

Guida di Secure Configuration

24 ottobre 2019

vRealize Automation 7.5



vmware®

È possibile trovare la documentazione tecnica più aggiornata sul sito Web di VMware all'indirizzo:

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

In caso di commenti sulla presente documentazione, inviare un messaggio all'indirizzo:

docfeedback@vmware.com

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

VMware, Inc.
Centro Leoni Palazzo A
Via Spadolini 5
Ground Floor
Milan, MI 20121
tel: +39 02 30412700
fax: +39 02 30412701
www.vmware.com/it

Copyright © 2015-2019 VMware, Inc. Tutti i diritti sono riservati. [Informazioni sul copyright e sui marchi](#)

Sommario

1	Secure Configuration	5
2	Panoramica su baseline sicura per vRealize Automation	6
3	Verifica dell'integrità del supporto di installazione	8
4	Proteggere l'infrastruttura software del sistema VMware	9
	Proteggere l'ambiente VMware vSphere®	9
	Proteggere l'host Infrastructure as a Service	9
	Proteggere Microsoft SQL Server	10
	Proteggere Microsoft .NET	10
	Proteggere Microsoft Internet Information Services (IIS)	10
5	Revisione del software installato	12
6	Avvisi di sicurezza e patch di VMware	13
7	Secure Configuration	14
	Protezione dell'appliance vRealize Automation	14
	Modifica della password root	14
	Verifica dell'hash e della complessità della password root	15
	Verifica della cronologia delle password root	15
	Gestione della scadenza delle password	16
	Gestione degli account SSH e amministrativi	17
	Modifica dell'utente dell'interfaccia di gestione dell'appliance virtuale	21
	Impostazione dell'autenticazione del caricatore di avvio	22
	Configurazione del protocollo NTP	22
	Configurazione del protocollo TLS per i dati in transito dell'appliance vRealize Automation	23
	Verifica della protezione dei dati inattivi	32
	Configurazione delle risorse applicazione di vRealize Automation	33
	Personalizzazione della configurazione del proxy della console	35
	Configurazione delle intestazioni di risposta dei server	37
	Impostazione del timeout della sessione di Appliance vRealize Automation	39
	Gestione del software non essenziale	39
	Protezione del componente Infrastructure as a Service	44
	Configurazione di NTP	44
	Configurazione del protocollo TLS per i dati in transito di Infrastructure as a Service	44
	Configurazione dei pacchetti di crittografia TLS	47

Verifica della protezione del server host	48
Protezione delle risorse applicazione	49
Protezione della macchina host Infrastructure as a Service (IaaS)	50

8 Configurazione della sicurezza della rete host 51

Configurazione delle impostazioni di rete per le appliance VMware	51
Evitare il controllo delle interfacce di rete da parte degli utenti	51
Impostazione della dimensione della coda di backlog TCP	52
Negare le richieste eco ICMPv4 inviate a un indirizzo di broadcast	52
Disabilitare il protocollo ARP del proxy IPv4	53
Negare i messaggi di reindirizzamento IPv4 ICMP	53
Negare i messaggi di reindirizzamento IPv6 ICMP	54
Registrazione dei pacchetti martian IPv4	55
Uso del filtro del percorso inverso IPv4	55
Negare l'inoltro IPv4	56
Negare l'inoltro IPv6	57
Uso dei SYN cookie TCP IPv4	57
Negare gli annunci del router IPv6	58
Negare le richieste del router IPv6	59
Negare la preferenza del router IPv6 nelle richieste del router	59
Negare il prefisso del router IPv6	60
Negare le impostazioni del limite di hop degli annunci del router IPv6	61
Negare le impostazioni di configurazione automatica degli annunci del router IPv6	61
Negare le richieste del router adiacente IPv6	62
Limitazione del numero massimo di indirizzi IPv6	63
Configurazione delle impostazioni di rete per l'host IaaS	64
Configurazione di porte e protocolli	64
Porte richieste per gli utenti	64
Porte necessarie per l'amministratore	65

9 Controllo e registrazione 68

Secure Configuration

Secure Configuration consente agli utenti di valutare e ottimizzare la configurazione sicura delle distribuzioni di vRealize Automation.

Secure Configuration descrive la verifica e la configurazione di distribuzioni sicure per ambienti vRealize Automation tipici e fornisce informazioni e procedure per consentire agli utenti di prendere decisioni informate riguardanti la configurazione della protezione.

Destinatari

Queste informazioni sono destinate agli amministratori di sistema di vRealize Automation e agli altri utenti responsabili della manutenzione e della configurazione della protezione dei sistemi.

Glossario delle pubblicazioni tecniche di VMware

Il sito delle pubblicazioni tecniche di VMware Technical fornisce un glossario dei termini che potrebbero risultare non familiari. Per le definizioni dei termini utilizzati nella documentazione tecnica di VMware, consultare la pagina <http://www.vmware.com/support/pubs>.

Panoramica su baseline sicura per vRealize Automation

2

VMware fornisce una serie di raccomandazioni complete che consentono di verificare e configurare una baseline sicura per il sistema vRealize Automation.

Utilizzare gli strumenti appropriati e le procedure consigliate da VMware per verificare e mantenere una configurazione della baseline sicura e con protezione avanzata per il sistema vRealize Automation. Alcuni componenti di vRealize Automation sono installati in uno stato di protezione avanzata o protezione avanzata parziale, ma è opportuno riesaminare e verificare la configurazione di ciascun componente alla luce delle raccomandazioni di sicurezza di VMware, dei criteri di protezione dell'azienda e delle minacce note.

Comportamento della protezione di vRealize Automation

Il comportamento della protezione di vRealize Automation ipotizza un ambiente olisticamente sicuro, basato su configurazione di sistema e rete, criteri di protezione dell'organizzazione e procedure di sicurezza consigliate.

Quando si verifica e si configura la protezione avanzata di un sistema vRealize Automation, tenere in considerazione ognuna delle seguenti aree interessate dalle raccomandazioni di VMware relative alla protezione avanzata.

- Distribuzione sicura
- Secure Configuration
- Sicurezza della rete

Per garantire una protezione avanzata sicura del sistema, considerare le raccomandazioni di VMware e i criteri di protezione locali in relazione ad ognuna di queste aree concettuali.

Componenti del sistema

Quando si considera la protezione avanzata e la configurazione sicura del proprio sistema vRealize Automation, assicurarsi di comprendere tutti i componenti e come interagiscono per supportare le funzionalità del sistema.

Quando si pianifica e si implementa un sistema sicuro, tenere in considerazione i seguenti componenti.

- Appliance vRealize Automation

■ Componente IaaS

Per familiarizzare con vRealize Automation e con il modo in cui i componenti operano insieme, vedere *Nozioni fondamentali e concetti* nel centro documentazione di VMware vRealize Automation. Per informazioni sulle distribuzioni e sull'architettura tipiche di vRealize Automation, vedere *Architettura di riferimento*.

Verifica dell'integrità del supporto di installazione

3

Gli utenti dovrebbero sempre verificare l'integrità del supporto di installazione prima di installare un prodotto VMware.

Verificare sempre l'hash SHA1 dopo aver scaricato una ISO, un bundle offline o una patch per assicurarsi che i file scaricati siano integri e autentici. Se si ottiene un supporto fisico da VMware e il sigillo di sicurezza risulta danneggiato, restituire il software a VMware affinché venga sostituito.

Dopo aver scaricato il supporto, utilizzare il valore della somma MD5/SHA1 per verificare l'integrità del download. Confrontare l'output dell'hash MD5/SHA1 con il valore pubblicato sul sito Web di VMware. L'hash SHA1 o MD5 deve coincidere.

Per ulteriori informazioni sulla verifica dell'integrità del supporto di installazione, vedere <http://kb.vmware.com/kb/1537>.

Proteggere l'infrastruttura software del sistema VMware

4

Durante le operazioni di protezione, valutare l'infrastruttura del software distribuito che supporta il sistema VMware e verificare che soddisfi le linee guida per la protezione di VMware.

Prima di proteggere il sistema VMware, esaminare e risolvere le vulnerabilità della sicurezza nell'infrastruttura del software di supporto per creare un ambiente sicuro e completamente protetto. Gli elementi dell'infrastruttura software da considerare includono i componenti del sistema operativo, il software di supporto e il software del database. Provare a risolvere i problemi di sicurezza in questi e negli altri componenti seguendo i suggerimenti del produttore e utilizzando altri protocolli di sicurezza pertinenti.

Questo capitolo include i seguenti argomenti:

- [Proteggere l'ambiente VMware vSphere®](#)
- [Proteggere l'host Infrastructure as a Service](#)
- [Proteggere Microsoft SQL Server](#)
- [Proteggere Microsoft .NET](#)
- [Proteggere Microsoft Internet Information Services \(IIS\)](#)

Proteggere l'ambiente VMware vSphere®

Valutare l'ambiente VMware vSphere® e verificare che siano state applicate e mantenute le linee guida appropriate per la protezione di vSphere.

Per ulteriori istruzioni sulla protezione, vedere <http://www.vmware.com/security/hardening-guides.html>.

Essendo integrata in un ambiente completamente protetto, l'infrastruttura VMware vSphere® deve soddisfare le linee guida per la sicurezza stabilite da VMware.

Proteggere l'host Infrastructure as a Service

Verificare che la macchina host Infrastructure as a Service Microsoft Windows sia protetta in base alle linee guida di VMware.

Consultare i suggerimenti nelle linee guida pertinenti delle procedure consigliate di protezione e sicurezza di Microsoft Windows e verificare che l'host Windows Server sia protetto in modo appropriato. La mancata applicazione dei suggerimenti per la protezione potrebbe comportare l'esposizione a vulnerabilità della sicurezza note per i componenti non protetti delle versioni di Windows.

Per verificare che la versione in uso sia supportata, fare riferimento alla [Matrice di supporto di vRealize Automation](#).

Per istruzioni corrette sulle procedure di protezione dei prodotti Microsoft, contattare il rivenditore Microsoft.

Proteggere Microsoft SQL Server

Verificare che il database Microsoft SQL Server soddisfi le linee guida per la sicurezza stabilite da Microsoft e VMware.

Consultare i suggerimenti contenuti nelle linee guida pertinenti delle procedure consigliate di sicurezza e protezione di Microsoft SQL Server. Leggere tutti i bollettini di sicurezza Microsoft relativi alla versione installata di Microsoft SQL Server. La mancata applicazione dei suggerimenti per la protezione potrebbe comportare l'esposizione a vulnerabilità della sicurezza note per i componenti non protetti delle versioni di Microsoft SQL Server.

Per verificare che la versione di Microsoft SQL Server in uso sia supportata, fare riferimento alla [Matrice di supporto di vRealize Automation](#).

Per istruzioni sulle procedure di protezione per i prodotti Microsoft, contattare il rivenditore Microsoft.

Proteggere Microsoft .NET

Essendo integrato in un ambiente completamente protetto, Microsoft .NET deve soddisfare le linee guida per la sicurezza stabilite da Microsoft e VMware.

Consultare i suggerimenti contenuti nelle linee guida pertinenti delle procedure consigliate di sicurezza e protezione di .NET. Leggere inoltre tutti i bollettini Microsoft sulla sicurezza relativi alla versione di Microsoft SQL Server in uso. La mancata applicazione dei suggerimenti per la protezione potrebbe comportare l'esposizione a vulnerabilità della sicurezza note per i componenti Microsoft.NET non protetti.

Per verificare che la versione di Microsoft.NET in uso sia supportata, fare riferimento alla [Matrice di supporto di vRealize Automation](#).

Per istruzioni sulle procedure di protezione per i prodotti Microsoft, contattare il rivenditore Microsoft.

Proteggere Microsoft Internet Information Services (IIS)

Verificare che Microsoft Internet Information Services (IIS) rispetti tutte le linee guida per la sicurezza stabilite da Microsoft e VMware.

Consultare i suggerimenti contenuti nelle linee guida delle procedure consigliate per la sicurezza e la protezione di Microsoft IIS. Leggere inoltre tutti i bollettini Microsoft sulla sicurezza relativi alla versione di IIS in uso. La mancata applicazione dei suggerimenti per la protezione potrebbe comportare l'esposizione a vulnerabilità della sicurezza note.

Per verificare che la versione in uso sia supportata, fare riferimento alla [Matrice di supporto di vRealize Automation](#).

Per istruzioni sulle procedure di protezione per i prodotti Microsoft, contattare il rivenditore Microsoft.

Revisione del software installato

Poiché le vulnerabilità nel software di terze parti o inutilizzato aumentano il rischio di accessi non autorizzati al sistema e interruzione della disponibilità, è importante rivedere tutto il software installato nelle macchine host di VMware e valutarne l'utilizzo.

Non installare software che non è necessario per il funzionamento sicuro del sistema nelle macchine host di VMware. Disinstallare il software estraneo o inutilizzato.

Software non supportato installato in inventario

Valutare la propria distribuzione di VMware e l'inventario dei prodotti installati per verificare che non sia installato software estraneo non supportato.

Per ulteriori informazioni sui criteri di supporto per i prodotti di terze parti, vedere l'articolo sul supporto di VMware all'indirizzo <https://www.vmware.com/support/policies/thirdparty.html>.

Verificare il software di terze parti

VMware non supporta né consiglia l'installazione di software di terze parti che non sia stato testato e verificato. Software di terze parti non sicuro, senza le patch o non autenticato, installato in macchine host di VMware, può esporre il sistema al rischio di accessi non autorizzati e interruzione della disponibilità. Se è necessario utilizzare software di terze parti non supportato, consultare il fornitore terzo per conoscere la configurazione sicura e i requisiti di applicazione delle patch.

Avvisi di sicurezza e patch di VMware

6

Per garantire la massima protezione del sistema, attenersi agli avvisi di sicurezza rilasciati da VMware e applicare tutte le patch pertinenti.

VMware rilascia avvisi di sicurezza per i prodotti. Monitorare questi avvisi per assicurarsi che il prodotto sia protetto dalle minacce note.

Esaminare la cronologia delle installazioni, delle applicazioni delle patch e degli aggiornamenti di vRealize Automation e verificare che gli avvisi di sicurezza rilasciati da VMware vengano seguiti e implementati.

Per ulteriori informazioni sugli avvisi di sicurezza correnti di VMware, vedere <http://www.vmware.com/security/advisories/>.

Secure Configuration

Verificare e aggiornare le impostazioni di sicurezza per le appliance virtuali di vRealize Automation e il componente Infrastructure as a Service nel modo appropriato in base alla configurazione del sistema. Inoltre, verificare e aggiornare la configurazione di altri componenti e applicazioni.

Per configurare in modo sicuro un'installazione di vRealize Automation, è necessario agire sia sulla configurazione di ciascun componente singolarmente, sia sull'interazione dei componenti. Considerare la configurazione di tutti i componenti del sistema nel loro insieme per ottenere una baseline ragionevolmente sicura.

Questo capitolo include i seguenti argomenti:

- [Protezione dell'appliance vRealize Automation](#)
- [Protezione del componente Infrastructure as a Service](#)

Protezione dell'appliance vRealize Automation

Verificare e aggiornare le impostazioni di sicurezza dell'appliance vRealize Automation in base alle esigenze della configurazione del sistema.

Configurare le impostazioni di sicurezza delle appliance virtuali e dei relativi sistemi operativi host. Inoltre, impostare o verificare la configurazione di altri componenti e applicazioni correlati. In alcuni casi è necessario verificare le impostazioni esistenti, mentre in altri è necessario modificare o aggiungere impostazioni per ottenere una configurazione appropriata.

Modifica della password root

È possibile modificare la password root dell'appliance vRealize Automation.

Procedura

- 1 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Fare clic sulla scheda **Amministrazione**.
- 3 Fare clic sul sottomenu **Amministrazione**.
- 4 Immettere la password esistente nella casella di testo **Password amministratore corrente**.
- 5 Immettere la nuova password nella casella di testo **Nuova password amministratore**.

6 Immettere la nuova password nella casella di testo **Ridigita la nuova password amministratore**.

7 Fare clic su **Salva impostazioni**.

Verifica dell'hash e della complessità della password root

Verificare che la password root soddisfi i requisiti aziendali di complessità delle password.

È necessario controllare la complessità della password root perché per l'utente root non viene eseguito il controllo di complessità della password del modulo pam_cracklib, applicato agli account utente.

La password dell'account deve iniziare con \$6\$, che indica un hash sha512. Questo è l'hash standard per tutte le appliance con protezione avanzata.

Procedura

- 1 Per verificare l'hash della password root, accedere come root ed eseguire il comando `# more /etc/shadow`.

Vengono visualizzate le informazioni dell'hash.

Figura 7-1. Risultati hash password

```
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 Se la password root non contiene un hash sha512, eseguire il comando `passwd` per modificarla.

Tutte le appliance con protezione avanzata abilitano `enforce_for_root` per il modulo `pw_history`, che si trova nel file `/etc/pam.d/common-password`. Per impostazione predefinita, il sistema ricorda le ultime cinque password. Le password precedenti di ciascun utente vengono memorizzate nel file `/etc/securetty/passwd`.

Verifica della cronologia delle password root

Verificare che per l'account root venga applicata la cronologia delle password.

Tutte le appliance con protezione avanzata abilitano `enforce_for_root` per il modulo `pw_history`, che si trova nel file `/etc/pam.d/common-password`. Per impostazione predefinita, il sistema ricorda le ultime cinque password. Le password precedenti di ciascun utente vengono memorizzate nel file `/etc/securetty/passwd`.

Procedura

- 1 Eseguire il comando seguente.

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

- 2 Assicurarsi che nei risultati restituiti sia presente `enforce_for_root`.

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

Gestione della scadenza delle password

Configurare le scadenze delle password di tutti gli account in base ai criteri di protezione dell'organizzazione.

Per impostazione predefinita, la protezione avanzata di tutti gli account dell'appliance virtuale VMware prevede una durata della password di 60 giorni. Nella maggior parte delle appliance con protezione avanzata, la durata della password impostata per l'account root è di 365 giorni. È consigliabile verificare che per tutti gli account la durata impostata soddisfi gli standard dei requisiti di sicurezza e di quelli operativi.

Se la password root scade, non è possibile ripristinarla. È necessario implementare criteri specifici per i siti per impedire la scadenza delle password degli account amministrativi e root.

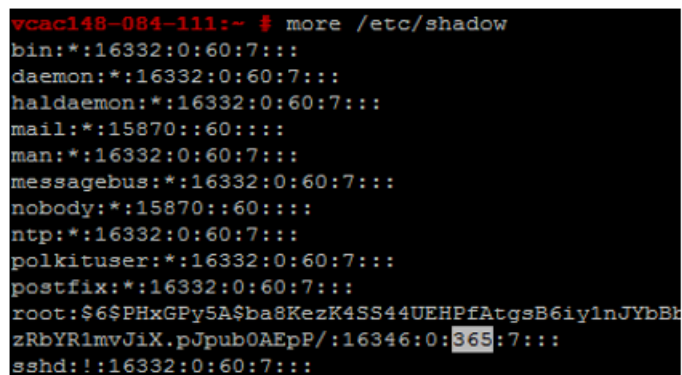
Procedura

- 1 Accedere alle macchine dell'appliance virtuale come utente root ed eseguire il seguente comando per verificare la scadenza delle password per tutti gli account.

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

La scadenza della password è specificata nel quinto campo (i campi sono separati da due punti) del file shadow. La scadenza dell'account root è impostata in giorni.

Figura 7-2. Campo scadenza password



```
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$ba8KczK4SS44UEHPfAtgsB6iy1nJYbBk
zRbYR1mvJiX.pJpub0AEpP/:16346:0:365:7:::
sshd:!:16332:0:60:7:::
```

- 2 Per modificare la scadenza dell'account root, eseguire un comando del tipo seguente.

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


In questo comando, il valore 365 specifica il numero di giorni della durata della password. Utilizzare lo stesso comando per modificare qualsiasi altro utente, sostituendo "root" con l'account specifico e il numero di giorni in base agli standard di scadenza stabiliti per l'organizzazione.

Gestione degli account SSH e amministrativi

Per le connessioni remote, tutte le appliance con protezione avanzata includono il protocollo Secure Shell (SSH). Utilizzare SSH solo se necessario e gestirlo in modo appropriato per preservare la sicurezza del sistema.

SSH è un ambiente interattivo da riga di comando che supporta le connessioni remote alle appliance virtuali VMware. Per impostazione predefinita, l'accesso a SSH richiede credenziali di account utente con privilegi elevati. In genere, le attività SSH dell'utente root escludono il controllo degli accessi in base al ruolo (RBAC) e i controlli delle appliance virtuali.

È consigliabile disattivare SSH negli ambienti di produzione e attivarlo solo per la risoluzione dei problemi che non possono essere risolti in altro modo. Lasciarlo abilitato solo per il tempo necessario a raggiungere uno scopo specifico e nel rispetto dei criteri di protezione dell'organizzazione. Nell'appliance vRealize Automation SSH è disabilitato per impostazione predefinita. In base alla configurazione di vSphere in uso, SSH può essere abilitato o disabilitato quando si distribuisce il proprio modello OVF (Open Virtualization Format).

Per sapere se in una macchina è abilitato SSH, è sufficiente provare ad aprire una connessione utilizzando il protocollo SSH. Se la connessione viene stabilita e vengono richieste le credenziali, significa che SSH è abilitato e disponibile per le connessioni.

Account utente root di SSH

Poiché le appliance VMware non includono account utente preconfigurati, l'account root può utilizzare SSH per accedere direttamente per impostazione predefinita. Disabilitare SSH come root non appena possibile.

Per rispettare gli standard di conformità per il non ripudio, il server SSH in tutte le appliance con protezione avanzata è preconfigurato con la voce AllowGroups wheel per limitare l'accesso SSH al gruppo wheel secondario. Per separare i compiti, è possibile modificare la voce AllowGroups wheel nel file `/etc/ssh/sshd_config` in modo che utilizzi un altro gruppo, ad esempio `sshd`.

Il gruppo wheel è abilitato con il modulo `pam_wheel` per l'accesso superuser, pertanto i membri del gruppo wheel possono utilizzare `su-root` quando è richiesta la password di root. La separazione dei gruppi consente agli utenti di connettersi all'appliance tramite SSH, ma non di utilizzare `su-to-root`. Non rimuovere o modificare le altre voci nel campo AllowGroups per assicurare il corretto funzionamento dell'appliance. Dopo aver apportato una modifica, è necessario riavviare il daemon SSH eseguendo il comando: `# service sshd restart`.

Abilitare o disabilitare il servizio SS nelle appliance di vRealize Automation

Abilitare il servizio SSH (Secure Shell) nell'appliance vRealize Automation solo per la risoluzione dei problemi. Durante le normali operazioni di produzione, disabilitare SSH in questi componenti.

È possibile abilitare o disabilitare SSH nell'appliance vRealize Automation utilizzando l'interfaccia di gestione dell'appliance vRealize Automation.

Procedura

- 1 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Fare clic sulla scheda **Amministrazione**.
- 3 Fare clic sul menu secondario **Amministrazione**.
- 4 Selezionare la casella di controllo di abilitazione del servizio SSH per abilitare SSH o deselezionarla per disabilitarlo.
- 5 Fare clic su **Salva impostazioni** per salvare le modifiche.

Creazione di un account amministratore locale per Secure Shell

Come procedura consigliata per la sicurezza, creare e configurare account amministrativi locali per Secure Shell nelle macchine host dell'appliance virtuale. Rimuovere inoltre l'accesso SSH root dopo aver creato gli account appropriati.

Creare account amministrativi locali per SSH o membri del gruppo wheel secondario o entrambi. Prima di disabilitare l'accesso root diretto, verificare che gli amministratori autorizzati possano accedere a SSH mediante AllowGroups e che possano eseguire su-to-root usando il gruppo wheel.

Procedura

- 1 Accedere all'appliance virtuale come root ed eseguire i seguenti comandi con il nome utente appropriato.

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

Wheel è il gruppo specificato in AllowGroups per l'accesso ssh. Per aggiungere più gruppi secondari, usare `-G wheel,sshd`.

- 2 Passare all'utente e fornire una nuova password per applicare il controllo della complessità della password.

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

Se i requisiti di complessità della password sono soddisfatti, la password viene aggiornata. Se i requisiti di complessità della password non sono soddisfatti, viene ripristinata la password originale ed è necessario eseguire di nuovo il comando della password.

- 3 Per rimuovere l'accesso diretto a SSH, modificare il file `/etc/ssh/sshd_config` sostituendo `(#)PermitRootLogin yes` con `PermitRootLogin no`.

In alternativa, è possibile abilitare/disabilitare SSH nell'interfaccia di gestione dell'appliance virtuale (Virtual Appliance Management Interface, VAMI) selezionando o deselezionando la casella di controllo **Accesso SSH amministratore abilitato** nella scheda **Amministrazione**.

Operazioni successive

Disabilitare gli accessi diretti come root. Per impostazione predefinita, le appliance con protezione avanzata consentono l'accesso diretto a root tramite la console. Dopo aver creato gli account amministrativi per il non ripudio e averli provati per l'accesso wheel su-root, disabilitare gli accessi root diretti modificando il file `/etc/security` come root e sostituendo la voce `tty1` con `console`.

- 1 Aprire il file `/etc/securetty` in un editor di testo.
- 2 Individuare `tty1` e sostituirlo con `console`.
- 3 Salvare il file e chiuderlo.

Proteggere la configurazione del server Secure Shell

Laddove possibile, tutte le appliance VMware hanno una configurazione protetta predefinita. Gli utenti possono verificare il livello di protezione della configurazione esaminando le impostazioni dei servizi del server e del client nella sezione delle opzioni globali del file di configurazione.

Procedura

- 1 Aprire il file di configurazione del server `/etc/ssh/sshd_config` nell'appliance VMware e verificare che le impostazioni siano corrette.

Impostazione	Stato
Server Daemon Protocol	Protocollo 2
CBC Ciphers	aes256-ctr e aes128-ctr
TCP Forwarding	AllowTCPForwarding - No
Server Gateway Ports	Porte gateway - No
X11 Forwarding	X11Forwarding - No
SSH Service	Utilizzare il campo AllowGroups e specificare un gruppo con autorizzazione di accesso. Aggiungere i membri corretti a questo gruppo.
GSSAPI Authentication	GSSAPIAuthentication - No, se inutilizzata
Keberos Authentication	KeberosAuthentication - No, se inutilizzata
Local Variables (AcceptEnv global option)	Impostare su <code>disabled</code> by <code>commenting out</code> o su <code>enabled</code> for <code>LC_*</code> or <code>LANG variables</code>
Tunnel Configuration	PermitTunnel - No
Network Sessions	MaxSessions 1

Impostazione	Stato
User Concurrent Connections	Impostare su 1 per l'utente root e qualsiasi altro utente. È necessario configurare anche il file <code>/etc/security/limits.conf</code> con la stessa impostazione.
Strict Mode Checking	Strict Modes - Yes
Privilege Separation	UsePrivilegeSeparation - Yes
rhosts RSA Authentication	RhostsESAAuthentication - No
Compression	Compression delayed o Compression no
Message Authentication code	MACs hmac-sha1
User Access Restriction	PermitUserEnvironment - No

2 Salvare le modifiche e chiudere il file.

Proteggere la configurazione del client Secure Shell

Durante le operazioni di potenziamento della protezione del sistema, verificare il livello di protezione del client SSH esaminandone il file di configurazione nelle macchine host dell'appliance virtuale per assicurarsi che sia configurato in base alle linee guida di VMware.

Procedura

- 1 Aprire il file di configurazione del client SSH, `/etc/ssh/ssh_config` e verificare che le impostazioni nella sezione delle opzioni globali siano corrette.

Impostazione	Stato
Client Protocol	Protocollo 2
Client Gateway Ports	Porte gateway - No
GSSAPI Authentication	GSSAPIAuthentication - No
Local Variables (SendEnv global option)	Specificare solo variabili <code>LC_*</code> o <code>LANG</code>
CBC Ciphers	Solo aes256-ctr e aes128-ctr
Message Authentication Codes	Utilizzati solo nella voce MACs hmac-sha1

2 Salvare le modifiche e chiudere il file.

Verifica delle autorizzazioni del file della chiave di SSH

Per ridurre al minimo la possibilità di attacchi dannosi, gestire in modo appropriato le autorizzazioni del file della chiave di Secure Shell (SSH) nelle macchine host dell'appliance virtuale.

Dopo aver configurato o aggiornato la configurazione di SSH, verificare sempre che le seguenti autorizzazioni del file della chiave di SSH non vengano modificate.

- I file delle chiavi degli host pubblici contenuti in `/etc/ssh/*key.pub` sono di proprietà dell'utente root e hanno le autorizzazioni impostate su 0644 (-rw-r--r--).

- I file delle chiavi degli host privati inclusi in `/etc/ssh/*key` sono di proprietà dell'utente root e hanno le autorizzazioni impostate su 0600 (`-rw-----`).

Verifica delle autorizzazioni dei file di chiave SSH

Verificare che le autorizzazioni SSH vengano applicate sia ai file di chiave privata che di chiave pubblica.

Procedura

- 1 Per verificare i file di chiave pubblica SSH, eseguire il comando seguente: `ls -l /etc/ssh/*key.pub`
- 2 Verificare che il proprietario sia di tipo root, che il proprietario del gruppo sia di tipo root e che le autorizzazioni dei file siano impostate su 0644 (`-rw-r--r--`).
- 3 Correggere eventuali problemi eseguendo i comandi riportati di seguito.

```
chown root /etc/ssh/*key.pub
```

```
chgrp root /etc/ssh/*key.pub
```

```
chmod 644 /etc/ssh/*key.pub
```

- 4 Per verificare i file di chiave privata SSH, eseguire il comando seguente: `ls -l /etc/ssh/*key`
- 5 Verificare che il proprietario sia di tipo root, che il proprietario del gruppo sia di tipo root e che le autorizzazioni dei file siano impostate su 0600 (`-rw-----`). Correggere eventuali problemi eseguendo i comandi riportati di seguito.

```
chown root /etc/ssh/*key
```

```
chgrp root /etc/ssh/*key
```

```
chmod 600 /etc/ssh/*key
```

Modifica dell'utente dell'interfaccia di gestione dell'appliance virtuale

È possibile aggiungere ed eliminare utenti nell'interfaccia di gestione dell'appliance virtuale per creare il livello appropriato di sicurezza.

L'account utente root per l'interfaccia di gestione dell'appliance virtuale utilizza PAM per l'autenticazione, pertanto vengono applicati anche i livelli di ritaglio impostati da PAM. Se non è stata isolata in modo corretto l'interfaccia di gestione dell'appliance virtuale, è possibile che si verifichi un blocco dell'account root di sistema se un utente malintenzionato tenta di accedere effettuando un attacco di forza bruta. Inoltre, quando l'account root è considerato insufficiente al non ripudio da parte di più persone nella propria organizzazione, si può scegliere di cambiare l'utente amministratore per l'interfaccia di gestione.

Prerequisiti

Procedura

- 1 Eseguire il comando seguente per creare un nuovo utente e aggiungerlo al gruppo dell'interfaccia di gestione dell'appliance virtuale.

```
useradd -G vami,root user
```

- 2 Creare una password per l'utente.

```
passwd user
```

- 3 (Facoltativo) Eseguire il comando seguente per disattivare l'accesso root nell'interfaccia di gestione dell'appliance virtuale.

```
usermod -R vami root
```

Nota La disattivazione dell'accesso root all'interfaccia di gestione dell'appliance virtuale disattiva anche la possibilità di aggiornare la password dell'amministratore, ovvero la password root, dalla scheda Amministrazione.

Impostazione dell'autenticazione del caricatore di avvio

Per fornire un livello di sicurezza adeguato, configurare l'autenticazione del caricatore di avvio nelle appliance virtuali VMware.

Se il caricatore di avvio del sistema non richiede alcuna autenticazione, gli utenti che dispongono dei diritti di accesso alla console del sistema possono alterare la configurazione di avvio del sistema o avviare il sistema in modalità utente singolo o in modalità di manutenzione, esponendolo al rischio di attacchi DoS (Denial of Service) o di accessi non autorizzati. Poiché l'autenticazione del caricatore di avvio non è impostata in modo predefinito nelle appliance virtuali VMware, è necessario creare una password GRUB per configurarla.

Procedura

- 1 Verificare se esiste una password di avvio individuando la riga `password --md5 <password-hash>` nel file `/boot/grub/menu.lst` nelle appliance virtuali.
- 2 Se non esiste alcuna password, eseguire il comando `# /usr/sbin/grub-md5-crypt` nell'appliance virtuale.

Viene generata una password MD5 e il comando fornisce come output l'hash md5.

- 3 Aggiungere la password al file `menu.lst` eseguendo il comando `# password --md5 <hash from grub-md5-crypt>`.

Configurazione del protocollo NTP

Per il reperimento critico dell'ora, disabilitare la sincronizzazione dell'ora dell'host e usare il protocollo NTP (Network Time Protocol) nell'appliance vRealize Automation.

Il daemon NTP nell'appliance vRealize Automation fornisce servizi orari sincronizzati. Poiché il protocollo NTP è disabilitato per impostazione predefinita, è necessario configurarlo manualmente. Se possibile, negli ambienti di produzione usare NTP per monitorare le azioni degli utenti, nonché rilevare intrusioni e attacchi potenzialmente dannosi mediante accurati controlli e compilazioni dei registri. Per informazioni sugli avvisi di sicurezza relativi a NTP, consultare il sito Web di NTP.

Il file di configurazione di NTP si trova nella cartella `/etc/` delle singole appliance. È possibile abilitare il servizio NTP per l'appliance vRealize Automation e aggiungere server orari nella scheda **Amministrazione** dell'interfaccia di gestione dell'appliance virtuale.

Procedura

- 1 Aprire il file di configurazione `/etc/ntp.conf` nella macchina host dell'appliance virtuale in un editor di testo.
- 2 Impostare la proprietà del file su **root:root**.
- 3 Impostare le autorizzazioni su **0640**.
- 4 Per ridurre il rischio di un attacco con amplificazione Denial of Service nel servizio NTP, aprire il file `/etc/ntp.conf` e verificare che siano presenti le righe di limitazione.

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

- 5 Salvare le eventuali modifiche e chiudere i file.

Configurazione del protocollo TLS per i dati in transito dell'appliance vRealize Automation

Assicurarsi che la distribuzione di vRealize Automation usi protocolli TLS complessi per proteggere i canali di trasmissione dei componenti dell'appliance vRealize Automation.

Per quanto riguarda le prestazioni, TLS non è abilitato per le connessioni localhost tra alcuni servizi delle applicazioni. Se è necessario applicare la difesa in profondità, abilitare TLS in tutte le comunicazioni localhost.

Importante Se si arresta TLS nel bilanciamento del carico, disabilitare i protocolli non sicuri, come SSLv2, SSLv3 e TLS 1.0, in tutti i bilanciamenti del carico.

Abilitare TLS nella configurazione localhost

Per impostazione predefinita, alcune comunicazioni localhost non utilizzano TLS. È possibile abilitare TLS in tutte le connessioni localhost per fornire una protezione avanzata.

Procedura

- 1 Connettersi all'Appliance vRealize Automation utilizzando il servizio SSH.

2 Impostare le autorizzazioni per l'archivio chiavi vcac eseguendo i comandi seguenti.

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

3 Aggiornare la configurazione HAProxy.

- a Aprire il file di configurazione HAProxy che si trova in `/etc/haproxy/conf.d` e scegliere il servizio `20-vcac.cfg`.

- b Individuare le righe contenenti la stringa seguente:

`server local 127.0.0.1...` e aggiungere quanto segue alla fine di queste righe: `ssl verify none`

Questa sezione contiene altre righe, ad esempio:

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

- c Modificare la porta di `backend-horizon` da 8080 a 8443.

4 Ottenere la password di `keystorePass`.

- a Individuare la proprietà `certificate.store.password` nel file `/etc/vcac/security.properties`.

Ad esempio `certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

- b Decrittografare il valore utilizzando il comando seguente:

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

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

5 Configurare il servizio vRealize Automation.

- a Aprire il file `/etc/vcac/server.xml`.
- b Aggiungere l'attributo seguente al tag `Connector`, sostituendo `certificate.store.password` con il valore della password dell'archivio di certificati disponibile 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 Configurare il servizio vRealize Orchestrator.

- a Aprire il file `/etc/vco/app-server.xml`
- b Aggiungere l'attributo seguente al tag `Connector`, sostituendo `certificate.store.password` con il valore della password dell'archivio di certificati disponibile 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 Riavviare vRealize Orchestrator, vRealize Automation e i servizi haproxy.

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

Nota Se il server vco non viene riavviato, riavviare il computer host.

8 Configurare l'interfaccia di gestione dell'appliance virtuale.

È possibile elencare lo stato dei servizi eseguendo il comando seguente nell'appliance virtuale 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)'"'
```

Nota Se si abilita SSL nell'interfaccia di gestione dell'appliance virtuale, la scheda Servizi non può elencare lo stato dei servizi vRealize Automation.

- a Aprire il file /opt/vmware/share/htdocs/service/café-services/services.py.
- b Sostituire la riga `conn = httplib.HTTP()` con `conn = httplib.HTTPS()` per una maggiore protezione.

Abilitare la conformità a FIPS (Federal Information Processing Standard) 140-2

L'appliance vRealize Automation ora utilizza la versione certificata FIPS (Federal Information Processing Standard) 140-2 di OpenSSL per i dati in transito su TLS in tutto il traffico di rete in entrata e in uscita.

È possibile abilitare o disabilitare la modalità FIPS nell'interfaccia di gestione dell'appliance vRealize Automation. È inoltre possibile configurare FIPS dalla riga di comando quando si accede come utente root, utilizzando i comandi seguenti:

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

Se FIPS è abilitato, per il traffico di rete dell'appliance vRealize Automation in entrata e in uscita sulla porta 443 viene utilizzata la crittografia conforme a FIPS 140–2. Indipendentemente dall'impostazione di FIPS, vRealize Automation utilizza AES–256 per tutelare i dati protetti archiviati nell'appliance vRealize Automation.

Nota Attualmente, vRealize Automation abilita solo in parte la conformità a FIPS, poiché alcuni componenti interni non utilizzano ancora i moduli di crittografia certificati. Nei casi in cui i moduli certificati non sono ancora stati implementati, viene utilizzata la crittografia basata su AES–256 in tutti gli algoritmi di crittografia.

Nota La procedura seguente consentirà di riavviare la macchina fisica quando si modifica la configurazione.

Procedura

- 1 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Selezionare **vRA > Impostazioni host**.
- 3 Fare clic sul pulsante sotto l'intestazione Azioni in alto a destra per abilitare o disabilitare la modalità FIPS.
- 4 Fare clic su **Sì** per riavviare l'appliance vRealize Automation.

Verifica dello stato di disabilitazione di SSLv3, TLS 1.0 e TLS 1.1

Nell'ambito del processo dell'applicazione della protezione avanzata, assicurarsi che Appliance vRealize Automation utilizzi canali di trasmissione sicuri.

Nota Non è possibile eseguire l'operazione di unione cluster una volta disabilitato TLS 1.0/1.1 e abilitato TLS 1.2

Prerequisiti

Completare la procedura [Abilitare TLS nella configurazione localhost](#).

Procedura

- 1 Verificare che SSLv3, TLS 1.0 e TLS 1.1 siano disabilitati nei gestori https HAProxy in Appliance vRealize Automation.

File da esaminare	Parametro che deve essere presente	Nella riga appropriata corrispondente
/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 Riavviare il servizio.

```
service haproxy restart
```

- 3 Aprire il file /opt/vmware/etc/lighttpd/lighttpd.conf e verificare che contenga le voci di disabilitazione corrette.

Nota Non sono disponibili direttive per la disabilitazione di TLS 1.0 o TLS 1.1 in Lighttpd. La restrizione sull'utilizzo di TLS 1.1 e TLS 1.0 può essere parzialmente mitigata facendo in modo che OpenSSL non utilizzi le suite di crittografia di TLS 1.0 e TLS 1.1.

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

- 4 Verificare che SSLv3, TLS 1.0 e TLS 1.1 siano disabilitati per il proxy della console in Appliance vRealize Automation.

- a Modificare il file /etc/vcac/security.properties aggiungendo o modificando la riga seguente:

```
consoleproxy.ssl.server.protocols = TLSv1.2
```

- b Riavviare il server eseguendo il comando seguente:

```
service vcac-server restart
```

- 5 Verificare che SSLv3, TLS 1.0 e TLS 1.1 siano disabilitati per il servizio vCO.

- a Individuare il tag <Connector> nel file /etc/vco/app-server/server.xml e aggiungere il seguente attributo:

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

- b Riavviare il servizio vCO con il seguente comando.

```
service vco-server restart
```

- 6 Verificare che SSLv3, TLS 1.0 e TLS 1.1 siano disabilitati per il servizio vRealize Automation.

- a Aggiungere i seguenti attributi al tag <Connector> nel file /etc/vcac/server.xml.

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

- b Riavviare il servizio vRealize Automation mediante il seguente comando:

```
service vcac-server restart
```

- 7 Verificare che SSLv3, TLS 1.0 e TLS 1.1 siano disabilitati per RabbitMQ.

Aprire il file /etc/rabbitmq/rabbitmq.config e verificare che solo {versions, ['tlsv1.2']} sia presente nelle sezioni ssl e 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 Riavviare il server RabbitMQ.

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

- 9 Verificare che SSLv3, TLS 1.0 e TLS 1.1 siano disabilitati per il servizio vIDM.

Aprire il file opt/vmware/horizon/workspace/conf/server.xml per ogni istanza del connettore contenente SSLEnabled="true" e assicurarsi che sia presente la seguente riga.

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

Configurazione di pacchetti di crittografia TLS per i componenti vRealize Automation

Per ottenere la massima protezione, è necessario configurare i componenti di vRealize Automation in modo che usino crittografie complesse.

L'algoritmo di crittografia negoziato tra il server e il browser determina la complessità della crittografia usata in una sessione TLS.

Per assicurare che vengano selezionate solo crittografie complesse, disabilitare le crittografie vulnerabili nei componenti di vRealize Automation. Configurare il server in modo che supporti solo crittografie complesse e utilizzi dimensioni di chiave sufficientemente grandi. Configurare inoltre tutte le crittografie in un ordine adeguato.

Disabilitare i pacchetti di crittografia che non offrono autenticazione, come i pacchetti di crittografia NULL, ovvero aNULL o eNULL. Disabilitare inoltre lo scambio di chiavi Diffie-Hellman anonimo (ADH), le crittografie a livello di esportazione (EXP, crittografie che contengono DES), le dimensioni di chiave inferiori a 128 bit per la codifica del traffico del payload, l'uso di MD5 come meccanismo di hashing per il traffico del payload, i pacchetti di crittografia IDEA e i pacchetti di crittografia RC4. Assicurarsi inoltre che i pacchetti di crittografia che usano lo scambio di chiavi Diffie-Hellman (DHE) siano disabilitati

Disabilitare i pacchetti di crittografia deboli nel proxy HA

Esaminare i pacchetti di crittografia del servizio proxy HA dell'appliance vRealize Automation facendo riferimento all'elenco di pacchetti accettabili e disabilitare tutti quelli considerati deboli.

Disabilitare i pacchetti di crittografia che non offrono autenticazione, come i pacchetti di crittografia NULL, ovvero aNULL o eNULL. Disabilitare inoltre lo scambio di chiavi Diffie-Hellman anonimo (ADH), le crittografie a livello di esportazione (EXP, crittografie che contengono DES), le dimensioni di chiave inferiori a 128 bit per la codifica del traffico del payload, l'uso di MD5 come meccanismo di hashing per il traffico del payload, i pacchetti di crittografia IDEA e i pacchetti di crittografia RC4.

Procedura

- 1 Esaminare la voce della direttiva di binding relativa ai pacchetti di crittografia del file `/etc/haproxy/conf.d/20-vcac.cfg` e disabilitare tutti quelli considerati deboli.

```
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-tls1 no-tls11
```

- 2 Esaminare la voce della direttiva di binding relativa ai pacchetti di crittografia del file `/etc/haproxy/conf.d/30-vro-config.cfg` e disabilitare tutti quelli considerati deboli.

```
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-tls1 no-tls11
```

Disabilitazione dei pacchetti di crittografia deboli nel servizio proxy della console dell'appliance vRealize Automation

Esaminare i pacchetti di crittografia del servizio proxy della console dell'appliance vRealize Automation facendo riferimento all'elenco di pacchetti accettabili e disabilitare tutti quelli considerati deboli.

Disabilitare i pacchetti di crittografia che non offrono autenticazione, come i pacchetti di crittografia NULL, ovvero aNULL o eNULL. Disabilitare inoltre lo scambio di chiavi Diffie-Hellman anonimo (ADH), le crittografie a livello di esportazione (EXP, crittografie che contengono DES), le dimensioni di chiave inferiori a 128 bit per la codifica del traffico del payload, l'uso di MD5 come meccanismo di hashing per il traffico del payload, i pacchetti di crittografia IDEA e i pacchetti di crittografia RC4.

Procedura

- 1 Aprire il file `/etc/vcac/security.properties` in un editor di testo.
- 2 Aggiungere una riga al file per disabilitare i pacchetti di crittografia indesiderati.

Utilizzare una variante della riga seguente:

```
consoleproxy.ssl.ciphers.disallowed=pacchetto_crittografia_1, pacchetto_crittografia_2 e così via
```

Ad esempio, per disabilitare i pacchetti di crittografia AES 128 e AES 256, aggiungere la riga seguente:

```
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 Riavviare il server con il comando seguente.

```
service vcac-server restart
```

Disabilitare i pacchetti di crittografia deboli nel servizio vCO di Appliance vRealize Automation

Esaminare i pacchetti di crittografia del servizio vCO di Appliance vRealize Automation facendo riferimento all'elenco di pacchetti accettabili e disabilitare tutti quelli considerati deboli.

Disabilitare i pacchetti di crittografia che non offrono autenticazione, come i pacchetti di crittografia NULL, ovvero aNULL o eNULL. Disabilitare inoltre lo scambio di chiavi Diffie-Hellman anonimo (ADH), le crittografie a livello di esportazione (EXP, crittografie che contengono DES), le dimensioni di chiave inferiori a 128 bit per la codifica del traffico del payload, l'uso di MD5 come meccanismo di hashing per il traffico del payload, i pacchetti di crittografia IDEA e i pacchetti di crittografia RC4.

Procedura

- 1 Individuare il tag `<Connector>` nel file `/etc/vco/app-server/server.xml`.
- 2 Modificare o aggiungere l'attributo di crittografia in modo che vengano utilizzati i pacchetti di crittografia desiderati.

Fare riferimento all'esempio seguente:

```
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"
```

Disabilitare i pacchetti di crittografia deboli nel servizio RabbitMQ di Appliance vRealize Automation

Esaminare i pacchetti di crittografia del servizio RabbitMQ di Appliance vRealize Automation facendo riferimento all'elenco di pacchetti di crittografia accettabili e disabilitare tutti quelli considerati deboli.

Disabilitare i pacchetti di crittografia che non offrono autenticazione, come i pacchetti di crittografia NULL, ovvero aNULL o eNULL. Disabilitare inoltre lo scambio di chiavi Diffie-Hellman anonimo (ADH), le crittografie a livello di esportazione (EXP, crittografie che contengono DES), le dimensioni di chiave inferiori a 128 bit per la codifica del traffico del payload, l'uso di MD5 come meccanismo di hashing per il traffico del payload, i pacchetti di crittografia IDEA e i pacchetti di crittografia RC4.

Procedura

- 1 Valutare i pacchetti di crittografia supportati eseguendo il comando `# /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites()'`.

I pacchetti di crittografia restituiti nell'esempio seguente sono solo quelli supportati. Il server RabbitMQ non utilizza né comunica questi pacchetti di crittografia, a meno che non sia stato configurato a questo scopo nel file `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 Selezionare i pacchetti di crittografia supportati che soddisfano i requisiti di protezione della propria organizzazione.

Ad esempio, per consentire solo la crittografia `ECDHE-ECDSA-AES128-GCM-SHA256` & `ECDHE-ECDSA-AES256-GCM-SHA384`, esaminare il file `/etc/rabbitmq/rabbitmq.config` e aggiungere la riga seguente a `ssl` e `ssl_options`:

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

- 3 Riavviare il server RabbitMQ eseguendo il comando seguente:

```
service rabbitmq-server restart
```

Verifica della protezione dei dati inattivi

Verificare la protezione degli utenti e degli account del database utilizzati con vRealize Automation.

Utente Postgres

L'account utente postgres di Linux è legato al ruolo dell'account superuser del database postgres ed è un account bloccato per impostazione predefinita. Questa è la configurazione più sicura per questo utente poiché è accessibile solo dall'account utente root. Non sbloccare questo account utente.

Ruoli degli account utente del database

I ruoli predefiniti degli account utente postgres non dovrebbero essere utilizzati per finalità esterne alle funzionalità dell'applicazione. Per poter supportare attività non predefinite di analisi e creazione report del database, è consigliabile creare un account e una password aggiuntivi, adeguatamente protetti.

Eseguire lo script seguente dalla riga di comando:

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

Verrà aggiunto un nuovo utente e una password fornita dall'utente.

Nota Lo script deve essere eseguito in relazione al database postgres master nei casi in cui è implementata una configurazione di postgres HA master-slave.

Configurazione dell'autenticazione del client PostgreSQL

Assicurarsi che nel database PostgreSQL dell'appliance vRealize Automation non sia configurata l'autenticazione trust locale. Questa configurazione consente a qualsiasi utente locale, incluso il superuser del database, di connettersi in qualità di qualsiasi utente PostgreSQL senza dover specificare una password.

Nota L'account superuser di Postgres deve rimanere come trust locale.

È consigliabile utilizzare il metodo di autenticazione md5 perché invia password crittografate.

Le impostazioni di configurazione dell'autenticazione del client si trovano nel file `/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

```

Se si modifica il file `pg_hba.conf`, è necessario riavviare il server Postgres utilizzando i comandi seguenti per rendere effettive le modifiche.

```

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

```

Configurazione delle risorse applicazione di vRealize Automation

Controllare le risorse applicazione di vRealize Automation e limitare le autorizzazioni per i file.

Procedura

- 1 Eseguire il comando seguente per verificare che i file con i bit SUID e GUID impostati siano definiti correttamente.

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

Dovrebbe venire visualizzato il seguente elenco.

```

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 Eseguire il comando seguente per verificare che tutti i file nell'appliance virtuale abbiano un proprietario.

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

- 3 Eseguire il comando seguente per rivedere le autorizzazioni per tutti i file nell'appliance virtuale e verificare che nessuno di essi sia scrivibile da chiunque.

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

- 4 Eseguire il comando seguente per verificare che solo l'utente vcac possieda i file corretti.

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

Se non viene visualizzato alcun risultato, tutti i file corretti appartengono unicamente all'utente vcac.

- 5 Verificare che i seguenti file siano scrivibili solo dall'utente vcac.

```
/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
```

Verificare anche i seguenti file e le relative sottodirectory

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

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

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

- 6 Verificare che solo l'utente vcac o l'utente root possa leggere i file corretti nelle seguenti directory e relative sottodirectory.

```
/etc/vcac/*
```

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

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

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

- 7 Verificare che i file corretti appartengano solo all'utente vco o all'utente root, come illustrato nelle seguenti directory e relative sottodirectory.

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

- 8 Verificare che i file corretti siano scrivibili solo dall'utente vco o dall'utente root, come illustrato nelle seguenti directory e relative sottodirectory.

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

- 9 Verificare che i file corretti siano leggibili solo dall'utente vco o dall'utente root, come mostrato nelle seguenti directory e relative sottodirectory.

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

Personalizzazione della configurazione del proxy della console

È possibile personalizzare la configurazione della console remota per vRealize Automation per semplificare la risoluzione dei problemi e le procedure organizzative.

Quando si installa, si configura o si gestisce vRealize Automation, è possibile modificare alcune impostazioni per abilitare la risoluzione dei problemi ed eseguire il debug dell'installazione. Catalogare e controllare ogni modifica apportata per assicurarsi che i componenti applicabili siano protetti in modo adeguato in base all'utilizzo che se ne deve fare. Non passare alla produzione se non si è sicuri che le modifiche della configurazione non siano opportunamente protette.

Personalizzazione della scadenza del ticket di VMware Remote Console

È possibile personalizzare il periodo di validità dei ticket della console remota usati per stabilire le connessioni di VMware Remote Console.

Quando un utente esegue connessioni di VMware Remote Console, il sistema crea e restituisce credenziali monouso che stabiliscono una connessione specifica a una macchina virtuale. È possibile impostare la scadenza del ticket per un intervallo di tempo specificato in minuti.

Procedura

- 1 Aprire il file `/etc/vcac/security.properties` in un editor di testo.

- 2 Aggiungere una riga al file del modulo `consoleproxy.ticket.validitySec=30`.

In questa riga, il valore numerico specifica il numero di minuti che devono trascorrere prima che il ticket scada.

- 3 Salvare il file e chiuderlo.
- 4 Riavviare il server `vcac` usando il comando `/etc/init.d/vcac-server restart`.

Il valore della scadenza del ticket viene reimpostato sull'intervallo di tempo specificato in minuti.

Personalizzazione della porta del server proxy della console

È possibile personalizzare la porta su cui il proxy della console di VMware Remote Console è in ascolto per i messaggi.

Procedura

- 1 Aprire il file `/etc/vcac/security.properties` in un editor di testo.
- 2 Aggiungere una riga al file del modulo `consoleproxy.service.port=8445`.

Il valore numerico specifica il numero della porta del servizio proxy della console, in questo caso 8445.

- 3 Salvare il file e chiuderlo.
- 4 Riavviare il server `vcac` usando il comando `/etc/init.d/vcac-server restart`.

La porta del servizio proxy ha ora il numero di porta specificato.

Configurazione dell'intestazione della risposta X-XSS-Protection

Aggiungere l'intestazione della risposta X-XSS-Protection al file di configurazione `haproxy`.

Procedura

- 1 Aprire `/etc/haproxy/conf.d/20-vcac.cfg` per modificarlo.
- 2 Aggiungere le seguenti righe in una sezione del front end:

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

- 3 Ricaricare la configurazione HAProxy utilizzando il comando seguente.
`/etc/init.d/haproxy reload`

Configurazione dell'intestazione X-Content-Type-Options

Aggiungere l'intestazione della risposta X-Content-Type-Options alla configurazione HAProxy.

Procedura

- 1 Aprire `/etc/haproxy/conf.d/20-vcac.cfg` per modificarlo.

- 2 Aggiungere le seguenti righe in una sezione del front end:

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

- 3 Ricaricare la configurazione HAProxy utilizzando il comando seguente.

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

Configurazione dell'intestazione della risposta HTTP Strict Transport Security

Aggiungere l'intestazione della risposta HTTP Strict Transport (HSTS) alla configurazione HAProxy.

Procedura

- 1 Aprire `/etc/haproxy/conf.d/20-vcac.cfg` per modificarlo.
- 2 Aggiungere le seguenti righe in una sezione del front end:

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

- 3 Ricaricare la configurazione HAProxy utilizzando il comando seguente.

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

Configurazione dell'intestazione della risposta X-Frame-Options

In alcuni casi, l'intestazione della risposta X-Frame-Options può essere visualizzata due volte.

L'intestazione della risposta X-Frame-Options può essere visualizzata due volte perché il servizio vIDM aggiunge questa intestazione al back end oltre che ad HAProxy. Una configurazione appropriata può evitare la doppia visualizzazione.

Procedura

- 1 Aprire `/etc/haproxy/conf.d/20-vcac.cfg` per modificarlo.
- 2 Individuare la riga seguente nella sezione front end:
- 3 Aggiungere le righe seguenti prima della riga individuata nel passaggio precedente:

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

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

- 4 Ricaricare la configurazione HAProxy utilizzando il comando seguente.

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

Configurazione delle intestazioni di risposta dei server

Come procedura di sicurezza consigliata, configurare il sistema vRealize Automation per limitare le informazioni disponibili per i potenziali utenti malintenzionati.

Per quanto possibile, ridurre al minimo la quantità di informazioni che il sistema condivide sulla sua identità e la sua versione. Gli utenti malintenzionati e i pirati informatici possono usare queste informazioni per creare attacchi mirati contro il server Web o una sua specifica versione.

Configurazione dell'intestazione della risposta del server Lighttpd

È consigliabile creare un'intestazione del server vuota per il server Lighttpd dell'appliance vRealize Automation.

Procedura

- 1 Aprire il file `/opt/vmware/etc/lighttpd/lighttpd.conf` in un editor di testo.
- 2 Aggiungere `server.tag = " "` al file.
- 3 Salvare le modifiche e chiudere il file.
- 4 Riavviare il server Lighttpd eseguendo il comando `# /opt/vmware/etc/init.d/vami-lighttpd restart`.

Configurazione dell'intestazione della risposta TCServer per l'appliance vRealize Automation

È consigliabile creare un'intestazione del server vuota personalizzata per l'intestazione della risposta TCServer utilizzata con l'appliance vRealize Automation per limitare la possibilità che un utente malintenzionato ottenga informazioni preziose.

Procedura

- 1 Aprire il file `/etc/vco/app-server/server.xml` in un editor di testo.
- 2 In ciascun elemento `<Connector>`, aggiungere `server=" "`.
Ad esempio: `<Connector protocol="HTTP/1.1" server="" />`
- 3 Salvare le modifiche e chiudere il file.
- 4 Riavviare il server con il comando seguente.
`service vco-server restart`

Configurazione dell'intestazione della risposta del server Internet Information Services

Come procedura consigliata, creare un'intestazione del server vuota personalizzata per il server Internet Information Services (IIS) usato con Identity Appliance per limitare la possibilità che utenti malintenzionati ottengano informazioni preziose.

Procedura

- 1 Aprire il file `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` in un editor di testo.
- 2 Cercare la voce `RemoveServerHeader=0` e sostituirla con `RemoveServerHeader=1`.
- 3 Salvare le modifiche e chiudere il file.

- 4 Riavviare il server eseguendo il comando `iisreset`.

Operazioni successive

Disabilitare l'intestazione IIS X-Powered By rimuovendo le intestazioni di risposta HTTP dall'elenco nella console Gestione IIS.

- 1 Aprire la console Gestione IIS.
- 2 Aprire l'intestazione della risposta HTTP e rimuoverla dall'elenco.
- 3 Riavviare il server eseguendo il comando `iisreset`.

Impostazione del timeout della sessione di Appliance vRealize Automation

Configurare l'impostazione del timeout della sessione in Appliance vRealize Automation in base al criterio di protezione dell'azienda.

Il timeout della sessione predefinito di Appliance vRealize Automation in caso di inattività dell'utente è 30 minuti. Per modificare questo valore di timeout e adattarlo al criterio di protezione della propria organizzazione, modificare il file `web.xml` nella macchina host di Appliance vRealize Automation.

Procedura

- 1 Aprire il file `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` in un editor di testo.
- 2 Trovare `session-config` e impostare il valore `session-timeout`. Vedere il seguente esempio di codice.

```
<!-- 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 Riavviare il server eseguendo il comando seguente.

```
service vcac-server restart
```

Gestione del software non essenziale

Per ridurre al minimo i rischi di sicurezza, rimuovere o configurare il software non essenziale dalle macchine host vRealize Automation.

Per ridurre al minimo la possibilità che crei problemi di sicurezza, configurare tutto il software che non si intende rimuovere in base alle raccomandazioni dei produttori e in conformità alle procedure di sicurezza consigliate.

Sicurezza del gestore di archiviazione di massa USB

Garantire la sicurezza del gestore di archiviazione di massa USB per impedirne l'uso come gestore dei dispositivi USB con le macchine host dell'appliance virtuale VMware. Utenti potenzialmente malintenzionati possono sfruttare questo gestore per compromettere il sistema.

Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga `install usb-storage /bin/true`.
- 3 Salvare il file e chiuderlo.

Sicurezza del gestore del protocollo Bluetooth

Garantire la sicurezza del gestore del protocollo Bluetooth nelle macchine host dell'appliance virtuale per evitare che utenti potenzialmente malintenzionati lo sfruttino.

Il binding del protocollo Bluetooth allo stack della rete non è necessario e può aumentare la superficie di attacco dell'host.

Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga seguente.

```
install bluetooth /bin/true
```
- 3 Salvare il file e chiuderlo.

Sicurezza di Stream Control Transmission Protocol

Impedire il caricamento predefinito di Stream Control Transmission Protocol (SCTP) nel sistema. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Configurare il sistema per evitare il caricamento di Stream Control Transmission Protocol (SCTP) a meno che non sia assolutamente necessario. SCTP è un protocollo di livello trasporto standard IETF inutilizzato. Il binding di questo protocollo allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il kernel carichi dinamicamente un gestore del protocollo utilizzando il protocollo per aprire un socket.

Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga seguente.

```
install sctp /bin/true
```
- 3 Salvare il file e chiuderlo.

Sicurezza di Datagram Congestion Protocol

Come parte delle attività di protezione avanzata del sistema, evitare il caricamento predefinito del protocollo Datagram Congestion Control Protocol (DCCP) nelle macchine host dell'appliance virtuale. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Evitare il caricamento del modulo Datagram Congestion Control Protocol (DCCP) a meno che non sia assolutamente necessario. DCCP è un protocollo del livello trasporto proposto, che non viene utilizzato. Il binding di questo protocollo allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il kernel carichi dinamicamente un gestore del protocollo utilizzando il protocollo per aprire un socket.

Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file siano presenti le righe DCCP.

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

- 3 Salvare il file e chiuderlo.

Sicurezza del bridging di rete

Impedire il caricamento predefinito del modulo di bridging di rete nel sistema. Utenti potenzialmente malintenzionati possono sfruttarlo per compromettere il sistema.

Configurare il sistema per evitare il caricamento della rete a meno che non sia assolutamente necessario. Utenti potenzialmente malintenzionati possono sfruttarlo per aggirare il partizionamento e la protezione della rete.

Procedura

- 1 Eseguire il comando seguente su tutte le macchine host dell'appliance virtuale VMware.

```
# rmmod bridge
```

- 2 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 3 Assicurarsi che nel file sia presente la riga seguente.

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

- 4 Salvare il file e chiuderlo.

Sicurezza del protocollo Reliable Datagram Sockets

Come parte delle attività di protezione avanzata del sistema, evitare il caricamento predefinito del protocollo Reliable Datagram Sockets (RDS) nelle macchine host dell'appliance virtuale. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Il binding del protocollo Reliable Datagram Sockets (RDS) allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il sistema carichi dinamicamente un gestore del protocollo utilizzando il protocollo per aprire un socket.

Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga `install rds /bin/true`.
- 3 Salvare il file e chiuderlo.

Sicurezza del protocollo Transparent Inter-Process Communication

Come parte delle attività di protezione avanzata del sistema, evitare il caricamento predefinito del protocollo Transparent Inter-Process Communication (TIPC) nelle macchine host dell'appliance virtuale. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Il binding del protocollo Transparent Inter-Process Communication (TIPC) allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il kernel carichi dinamicamente un gestore del protocollo utilizzando il protocollo per aprire un socket.

Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga `install tipc /bin/true`.
- 3 Salvare il file e chiuderlo.

Sicurezza di Internetwork Packet Exchange Protocol

Impedire il caricamento predefinito di Internetwork Packet Exchange (IPX) Protocol nel sistema. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Evitare il caricamento del modulo Internetwork Packet Exchange (IPX) Protocol a meno che non sia assolutamente necessario. Il protocollo IPX è un protocollo a livello di rete obsoleto. Il binding di questo protocollo allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il sistema carichi dinamicamente un gestore di protocollo utilizzando il protocollo per aprire un socket.

Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga seguente.
`install ipx /bin/true`
- 3 Salvare il file e chiuderlo.

Sicurezza di Appletalk Protocol

Impedire il caricamento predefinito di Appletalk Protocol nel sistema. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Evitare il caricamento del modulo Appletalk Protocol a meno che non sia assolutamente necessario. Il binding di questo protocollo allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il sistema carichi dinamicamente un gestore di protocollo utilizzando il protocollo per aprire un socket.

Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga seguente.

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

- 3 Salvare il file e chiuderlo.

Sicurezza di DECnet Protocol

Impedire il caricamento predefinito di DECnet Protocol nel sistema. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Evitare il caricamento del modulo DECnet Protocol a meno che non sia assolutamente necessario. Il binding di questo protocollo allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il sistema carichi dinamicamente un gestore di protocollo utilizzando il protocollo per aprire un socket.

Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` di DECnet Protocol in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga seguente.

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

- 3 Salvare il file e chiuderlo.

Sicurezza del modulo Firewire

Impedire il caricamento predefinito del modulo Firewire nel sistema. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Evitare il caricamento del modulo Firewire a meno che non sia assolutamente necessario.

Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga seguente.

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

- 3 Salvare il file e chiuderlo.

Protezione del componente Infrastructure as a Service

Quando si applica la protezione avanzata al sistema, garantire la sicurezza del componente Infrastructure as a Service (IaaS) di vRealize Automation e della sua macchina host per evitare che utenti potenzialmente malintenzionati lo sfruttino.

È necessario configurare le impostazioni di sicurezza per il componente Infrastructure as a Service (IaaS) di vRealize Automation e per l'host in cui si trova. È necessario impostare o verificare la configurazione degli altri componenti e applicazioni correlati. In alcuni casi, è possibile verificare le impostazioni esistenti, mentre in altri sarà necessario cambiare o aggiungere impostazioni per una configurazione appropriata.

Configurazione di NTP

Come procedura consigliata di sicurezza, utilizzare server di riferimento ora autorizzati anziché la sincronizzazione con l'ora dell'host in un ambiente di produzione di vRealize Automation.

In un ambiente di produzione, disabilitare la sincronizzazione con l'ora dell'host e utilizzare server di riferimento ora autorizzati per garantire il monitoraggio accurato delle azioni utente, nonché l'identificazione di intrusioni e attacchi potenzialmente dannosi tramite le funzionalità di auditing e registrazione.

Configurazione del protocollo TLS per i dati in transito di Infrastructure as a Service

Assicurarsi che la distribuzione di vRealize Automation usi protocolli TLS complessi per proteggere i canali di trasmissione dei componenti di Infrastructure as a Service.

Secure Sockets Layer (SSL) e Transport Layer Security (TLS) sviluppato più di recente, sono protocolli di crittografia che contribuiscono a garantire la sicurezza durante le comunicazioni di rete tra i diversi componenti del sistema. Il protocollo SSL è uno standard datato e molte delle sue implementazioni non forniscono più una protezione adeguata da potenziali attacchi. Sono state identificate gravi debolezze nei protocolli SSL precedenti, tra cui SSLv2 e SSLv3. Questi protocolli non sono più considerati sicuri.

In base ai criteri di sicurezza dell'organizzazione, potrebbe essere preferibile disabilitare anche TLS 1.0.

Nota Quando si interrompe TLS nel bilanciamento del carico, disabilitare anche i protocolli vulnerabili come SSLv2, SSLv3 e, se necessario, anche TLS 1.0 e 1.1.

Abilitazione dei protocolli TLS 1.1 e 1.2 per IaaS

Abilitazione e applicazione dei protocolli TLS 1.1 e 1.2 in tutte le macchine virtuali che ospitano i componenti IaaS.

Procedura

- 1 Fare clic su **Start** e quindi su **Esegui**.
- 2 Digitare regedit, quindi fare clic su **OK**.

3 Individuare e aprire la seguente sottochiave del Registro di sistema.

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

4 Verificare quanto segue e creare nuove voci in base alle necessità.

- Se non è presente alcuna sottochiave con il nome TLS 1.1 in Protocols, crearne una.
- Se non è presente alcuna sottochiave con il nome Client in TLS 1.1, crearne una.
- Se nella sottochiave Client non è presente alcuna chiave con il nome DisabledByDefault, crearne una di tipo DWORD.
- Fare clic con il pulsante destro del mouse su DisabledByDefault, scegliere Modifica e impostare il valore su 0.
- Se nella sottochiave Client non è presente alcuna chiave denominata Enabled, crearne una di tipo DWORD.
- Fare clic con il pulsante destro del mouse su Enabled, scegliere Modifica e impostare il valore su 1.
- Se non è presente alcuna sottochiave denominata Server in TLS 1.1, crearne una.
- Se nella sottochiave Server non è presente alcuna chiave con il nome DisabledByDefault, crearne una di tipo DWORD.
- Fare clic con il pulsante destro del mouse su DisabledByDefault, scegliere Modifica e impostare il valore su 0.
- Se nella sottochiave Server non è presente alcuna chiave denominata Enabled, crearne una di tipo DWORD.
- Fare clic con il pulsante destro del mouse su Enabled, scegliere Modifica e impostare il valore su 1.

5 Ripetere il passaggio precedente per il protocollo TLS 1.2.

Nota Per applicare l'utilizzo di TLS 1.1 e 1.2, sono necessarie impostazioni aggiuntive come descritto nei passaggi successivi.

6 Individuare e aprire la seguente sottochiave del Registro di sistema.

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

7 Verificare quanto segue e creare nuove voci in base alle necessità.

- Se non è presente alcuna voce DWORD denominata SchUseStrongCrypto, crearla e impostarne il valore su 1.
- Se non è presente alcuna voce DWORD denominata SystemDefaultTlsVersions, crearla e impostarne il valore su 1.

8 Individuare e aprire la seguente sottochiave del Registro di sistema.

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

9 Verificare quanto segue e creare nuove voci in base alle necessità.

- Se non è presente alcuna voce DWORD denominata SchUseStrongCrypto, crearla e impostarne il valore su 1.
- Se non è presente alcuna voce DWORD denominata SystemDefaultTlsVersions, crearla e impostarne il valore su 1.

Disabilitazione di SSL 3.0 e TLS 1.0 per IaaS

Disabilitazione di SSL 3.0 e del protocollo obsoleto TLS 1.0 per i componenti IaaS.

Procedura

1 Fare clic su **Start** e quindi su **Esegui**.

2 Digitare Regedit, quindi fare clic su **OK**.

3 Individuare e aprire la seguente sottochiave del Registro di sistema.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

4 Verificare quanto segue e creare nuove voci in base alle necessità.

- Se non è presente alcuna sottochiave con il nome SSL 3.0 in Protocols, crearne una.
- Se non è presente una sottochiave denominata Client in SSL 3.0, crearne una.
- Se nella sottochiave Client non è presente alcuna chiave con il nome DisabledByDefault, crearne una di tipo DWORD.
- Fare clic con il pulsante destro del mouse su DisabledByDefault, scegliere Modifica e impostare il valore su 1.
- Fare clic con il pulsante destro del mouse su Enabled, scegliere Modifica e impostare il valore su 0.
- Se non è presente alcuna sottochiave denominata Server in SSL 3.0, crearne una.
- Se nella sottochiave Server non è presente alcuna chiave con il nome DisabledByDefault, crearne una di tipo DWORD.
- Fare clic con il pulsante destro del mouse su DisabledByDefault, scegliere Modifica e impostare il valore su 1.
- Se nel server non è presente alcuna chiave denominata Enabled, creare una di tipo DWORD.
- Fare clic con il pulsante destro del mouse su Enabled, scegliere Modifica e impostare il valore su 0.

5 Ripetere i passaggi precedenti per il protocollo TLS 1.0.

Disabilitare TLS 1.0 per IaaS

Per garantire la massima sicurezza, configurare IaaS in modo che utilizzi il pooling e disabilitare TLS 1.0.

Per ulteriori informazioni, vedere l'articolo della Knowledge Base di Microsoft all'indirizzo <https://support.microsoft.com/en-us/kb/245030>.

Procedura

- 1 Configurare IaaS per l'utilizzo del pooling anziché dei socket Web.
 - a Aggiornare il file di configurazione dei servizi di gestione C:\Programmi(x86)\VMware\vCAC\Server\ManagerService.exe.config aggiungendo i valori seguenti nella sezione <appSettings>:


```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```
 - b Riavviare il servizio di gestione (VMware vCloud Automation Center Service).
- 2 Verificare che TLS 1.0 sia disabilitato nel server IaaS.
 - a Eseguire l'editor del Registro di sistema come amministratore.
 - b Nella finestra del Registro di sistema, passare a HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\
 - c Fare clic con il pulsante destro del mouse su Protocolli e scegliere **Nuovo > Chiave**, quindi immettere **TLS 1.0**.
 - d Nell'albero di spostamento, fare clic con il pulsante destro del mouse sulla chiave TLS 1.0 appena creata e nel menu a comparsa scegliere **Nuovo > Chiave**, quindi immettere **Client**.
 - e Nell'albero di spostamento, fare clic con il pulsante destro del mouse sulla chiave TLS 1.0 appena creata e nel menu a comparsa scegliere **Nuovo > Chiave**, quindi immettere **Server**.
 - f Nell'albero di spostamento, sotto TLS 1.0, fare clic con il pulsante destro del mouse su **Client**, quindi fare clic su **Nuovo > Valore DWORD (32 bit)** e immettere **DisabledByDefault**.
 - g Nell'albero di spostamento, sotto TLS 1.0, selezionare **Client** e nel riquadro destro fare doppio clic su **DisabledByDefault** DWORD, quindi immettere **1**.
 - h Nell'albero di spostamento, sotto TLS 1.0, fare clic con il pulsante destro del mouse su **Server** e scegliere **Nuovo > Valore DWORD (32 bit)**, quindi immettere **Abilitato**.
 - i Nell'albero di spostamento, sotto TLS 1.0, selezionare **Server** e nel riquadro destro fare doppio clic su **Abilitato** DWORD, quindi immettere **0**.
 - j Riavviare Windows Server.

Configurazione dei pacchetti di crittografia TLS

Per ottenere la massima protezione, è necessario configurare i componenti di vRealize Automation in modo che usino crittografie complesse. L'algoritmo di crittografia negoziato tra il server e il browser determina la complessità della crittografia usata in una sessione TLS. Per assicurare che vengano selezionate solo crittografie complesse, disabilitare le crittografie vulnerabili nei componenti di vRealize

Automation. Configurare il server in modo che supporti solo crittografie complesse e utilizzi dimensioni di chiave sufficientemente grandi. Configurare inoltre tutte le crittografie in un ordine adeguato.

Pacchetti di crittografia non accettabili

Disabilitare i pacchetti di crittografia che non offrono autenticazione, come i pacchetti di crittografia NULL, ovvero aNULL o eNULL. Disabilitare inoltre lo scambio di chiavi Diffie-Hellman anonimo (ADH), le crittografie a livello di esportazione (EXP, crittografie che contengono DES), le dimensioni di chiave inferiori a 128 bit per la codifica del traffico del payload, l'uso di MD5 come meccanismo di hashing per il traffico del payload, i pacchetti di crittografia IDEA e i pacchetti di crittografia RC4. Assicurarsi inoltre che i pacchetti di crittografia che usano lo scambio di chiavi Diffie-Hellman (DHE) siano disabilitati.

Per informazioni sulla disabilitazione della crittografia con chiavi statiche in vRealize Automation, vedere [l'articolo 71094 della Knowledge Base](#).

Verifica della protezione del server host

Come procedura di sicurezza consigliata, verificare la configurazione della protezione delle macchine del server host di Infrastructure as a Service (IaaS).

Microsoft fornisce diversi strumenti che consentono di verificare gli aspetti legati alla sicurezza nelle macchine del server host. Per informazioni su come utilizzare al meglio questi strumenti, rivolgersi al proprio fornitore Microsoft.

Verifica della baseline sicura del server host

Eseguire lo strumento Microsoft Baseline Security Analyzer (MBSA) per verificare rapidamente che nel server siano stati installati gli aggiornamenti e gli hotfix più recenti. È possibile utilizzare MBSA per installare le patch di sicurezza mancanti rilasciate da Microsoft e mantenere aggiornato il server con le raccomandazioni di protezione fornite da Microsoft.

Scaricare la versione più recente dello strumento MBSA dal sito Web di Microsoft.

Verificare la configurazione della protezione del server host

Utilizzare Configurazione guidata impostazioni di sicurezza di Windows e il toolkit Microsoft Security Compliance Manager (SCM) per verificare che il server host sia configurato in modo sicuro.

Eseguire SCW dagli strumenti di amministrazione nel server Windows. Questo strumento è in grado di identificare i ruoli del server e le funzionalità installate, incluse le impostazioni di rete, del firewall di Windows e del Registro di sistema. Confrontare il report con le istruzioni più recenti per l'applicazione della protezione avanzata dal toolkit SCM relativo al server Windows in uso. In base ai risultati è possibile ottimizzare le impostazioni della protezione per ogni funzionalità, ad esempio i servizi di rete, le impostazioni degli account e i firewall di Windows, quindi applicare le impostazioni al server.

Sul sito Web di Microsoft Technet sono disponibili ulteriori informazioni sullo strumento SCW.

Protezione delle risorse applicazione

Come procedura di sicurezza consigliata, verificare che tutti i file di Infrastructure as a Service rilevanti dispongano delle autorizzazioni appropriate.

Esaminare i file Infrastructure as a Service rispetto all'installazione di Infrastructure as a Service. Nella maggior parte dei casi, sottocartelle e file per ogni cartella dovrebbero avere le stesse impostazioni della cartella.

Directory o file	Gruppo o utenti	Controllo completo	Modifica	Lettura ed esecuzione	Lettura	Scrittura
VMware\VCAC\Agents\ <nome_agente>\logs	SYSTEM	X	X	X	X	X
	Amministratore	X	X	X	X	X
	Amministratori	X	X	X	X	X
VMware\VCAC\Agents\ <nome_agente>\temp	SYSTEM	X	X	X	X	X
	Amministratore	X	X	X	X	X
	Amministratori	X	X	X	X	X
VMware\VCAC\Agents\	SYSTEM	X	X	X	X	X
	Amministratori	X	X	X	X	X
	Utenti			X	X	
VMware\VCAC\Distributed Execution Manager\	SYSTEM	X	X	X	X	X
	Amministratori	X	X	X	X	X
	Utenti			X	X	
VMware\VCAC\Distributed Execution Manager\DEM\Log	SYSTEM	X	X	X	X	X
	Amministratore	X	X	X	X	X
	Amministratori	X	X	X	X	X
VMware\VCAC\Distributed Execution Manager\DEO\Log	SYSTEM	X	X	X	X	X
	Amministratore	X	X	X	X	X
	Amministratori	X	X	X	X	X
VMware\VCAC\Management Agent\	SYSTEM	X	X	X	X	X
	Amministratori	X	X	X	X	X
	Utenti			X	X	
VMware\VCAC\Server\	SYSTEM	X	X	X	X	X
	Amministratori	X	X	X	X	X
	Utenti			X	X	
VMware\VCAC\Web API	SYSTEM	X	X	X	X	X
	Amministratori	X	X	X	X	X
	Utenti			X	X	

Protezione della macchina host Infrastructure as a Service (IaaS)

Come procedura consigliata per la sicurezza, esaminare le impostazioni di base nella macchina host Infrastructure as a Service (IaaS) per assicurarsi che sia conforme alle linee guida sulla sicurezza.

Proteggere vari account, applicazioni, porte e servizi nella macchina host Infrastructure as a Service (IaaS).

Verificare le impostazioni dell'account utente server

Verificare che non siano presenti account utente e impostazioni utente, di dominio o locali, non necessari. Limitare tutti gli account utente che non sono correlati alle funzionalità dell'applicazione a quelli necessari per l'amministrazione, la manutenzione e la risoluzione dei problemi. Limitare l'accesso remoto dagli account utente del dominio al minimo indispensabile per la manutenzione del server. Controllare e verificare con precisione questi account.

Eliminare le applicazioni non necessarie

Eliminare tutte le applicazioni non necessarie dai server host. Le applicazioni non necessarie aumentano il rischio di esposizione a causa delle loro vulnerabilità non note o prive di patch.

Disabilitare le porte e i servizi non necessari

Esaminare l'elenco delle porte aperte nel firewall del server host. Bloccare tutte le porte che non sono necessarie per il componente IaaS o per il funzionamento del sistema critico. Vedere [Configurazione di porte e protocolli](#). Controllare i servizi in esecuzione rispetto al server host e disabilitare quelli che non sono necessari.

Configurazione della sicurezza della rete host



Per offrire la massima protezione dalle minacce note alla sicurezza, configurare le impostazioni dell'interfaccia di rete e della comunicazione in tutte le macchine host VMware.

Nell'ambito di un piano di sicurezza completo, configurare le impostazioni di sicurezza dell'interfaccia di rete per le appliance virtuali VMware e i componenti Infrastructure as a Service in base alle linee guida stabilite per la sicurezza.

Questo capitolo include i seguenti argomenti:

- [Configurazione delle impostazioni di rete per le appliance VMware](#)
- [Configurazione delle impostazioni di rete per l'host IaaS](#)
- [Configurazione di porte e protocolli](#)

Configurazione delle impostazioni di rete per le appliance VMware

Per assicurarsi che le macchine host dell'appliance virtuale VMware supportino solo comunicazioni sicure ed essenziali, esaminare e modificare le impostazioni di comunicazione di rete corrispondenti.

Esaminare la configurazione del protocollo IP delle macchine host VMware e configurare le impostazioni di rete in base alle linee guida di sicurezza. Disabilitare tutti i protocolli di comunicazione non essenziali.

Evitare il controllo delle interfacce di rete da parte degli utenti

Come procedura di sicurezza consigliata, concedere agli utenti solo i privilegi di sistema di cui hanno strettamente bisogno per eseguire il proprio lavoro nelle macchine host dell'appliance VMware.

Concedendo agli account degli utenti i privilegi per manipolare le interfacce di rete, si espone la rete ad attacchi quali l'aggiornamento dei meccanismi di sicurezza della rete o DoS (Denial of Service). Consentire di modificare le impostazioni delle interfacce di rete solo agli utenti con privilegi.

Procedura

- 1 Eseguire il comando seguente in ogni macchina host dell'appliance VMware.

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

- 2 Assicurarsi che ogni interfaccia sia impostata su NO.

Impostazione della dimensione della coda di backlog TCP

Per fornire un livello di difesa contro gli attacchi dannosi, configurare una dimensione per la coda di backlog TCP predefinita nelle macchine host dell'appliance VMware.

Se si imposta la dimensione della coda di backlog TCP su un valore predefinito adeguato, è possibile mitigare l'impatto degli attacchi Denial of Service del protocollo TCP. L'impostazione predefinita consigliata è 1280.

Procedura

- 1 Eseguire il comando seguente in ogni macchina host dell'appliance VMware.

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```
- 2 Aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Impostare la dimensione della coda di backlog TCP predefinita aggiungendo la voce seguente al file.

```
net.ipv4.tcp_max_syn_backlog=1280
```
- 4 Salvare le modifiche e chiudere il file.

Negare le richieste eco ICMPv4 inviate a un indirizzo di broadcast

Come procedura consigliata di sicurezza, verificare che le macchine host dell'appliance VMware ignorino le richieste echo inviate agli indirizzi di broadcast ICMP.

Le risposte alle richieste eco ICMP (Internet Control Message Protocol) inviate a un indirizzo di broadcast forniscono un vettore di attacco per gli attacchi con amplificazione e possono facilitare la mappatura della rete da parte di agenti dannosi. La configurazione delle macchine host dell'appliance in modo che ignorino le richieste eco ICMPv4 garantisce protezione da questi tipi di attacchi.

Procedura

- 1 Eseguire il comando `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` nelle macchine host dell'appliance virtuale VMware per verificare che siano configurate in modo da negare le richieste eco agli indirizzi di broadcast IPv4.

Se le macchine host sono configurate per negare i reindirizzamenti IPv4, questo comando restituirà il valore 0 per `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`.
- 2 Per configurare una macchina host dell'appliance virtuale in modo che neghi le richieste eco inviate agli indirizzi di broadcast ICMPv4, aprire il file `/etc/sysctl.conf` in un editor di testo nella macchina host Windows.
- 3 Individuare la voce `net.ipv4.icmp_echo_ignore_broadcasts=0`. Se il valore di questa voce non è impostato su 0 o se la voce non esiste, aggiungerla o aggiornare la voce esistente nel modo appropriato.
- 4 Salvare le modifiche e chiudere il file.

Disabilitare il protocollo ARP del proxy IPv4

Verificare che il protocollo ARP del proxy IPv4 sia disabilitato a meno che non sia necessario nelle macchine host dell'appliance VMware per impedire la condivisione non autorizzata delle informazioni.

Il protocollo ARP del proxy IPv4 consente a un sistema di inviare risposte alle richieste ARP in un'interfaccia per conto degli host connessi a un'altra interfaccia. Disabilitarlo se non è necessario per impedire la dispersione di informazioni di identificazione tra i segmenti di rete collegati.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | egrep "default|all"` nelle macchine host dell'appliance virtuale VMware per verificare che il protocollo ARP del proxy IPv4 sia disabilitato.

Se è disabilitato, questo comando restituisce il valore 0.

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

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare il protocollo ARP del proxy IPv6 nelle macchine host, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

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

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche apportate e chiudere il file.

Negare i messaggi di reindirizzamento IPv4 ICMP

Come procedura consigliata di sicurezza, verificare che le macchine host dell'appliance virtuale VMware neghino i messaggi di reindirizzamento IPv4 ICMP.

I router utilizzano i messaggi di reindirizzamento ICMP per comunicare agli host che per una determinata destinazione esiste una route più diretta. Un messaggio di reindirizzamento ICMP dannoso può favorire un attacco di tipo man-in-the-middle. Questi messaggi modificano la tabella di routing dell'host e non sono autenticati. Verificare che il sistema sia configurato in modo da ignorarli se non sono necessari.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare i messaggi di reindirizzamento IPv4.

Se le macchine host sono configurate per negare i reindirizzamenti IPv4, questo comando restituisce i seguenti valori:

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

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

- 2 Se è necessario configurare una macchina host dell'appliance virtuale in modo che neghi i messaggi di reindirizzamento IPv4, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare i valori delle righe che iniziano con `net.ipv4.conf`.

Se i valori delle voci elencate di seguito non sono impostati su 0 o se le voci non esistono, aggiungerle al file o aggiornare le voci esistenti nel modo appropriato.

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

- 4 Salvare le modifiche apportate e chiudere il file.

Negare i messaggi di reindirizzamento IPv6 ICMP

Come procedura consigliata di sicurezza, verificare che le macchine host dell'appliance virtuale VMware neghino i messaggi di reindirizzamento IPv6 ICMP.

I router utilizzano i messaggi di reindirizzamento ICMP per comunicare agli host che per una determinata destinazione esiste una route più diretta. Un messaggio di reindirizzamento ICMP dannoso può favorire un attacco di tipo man-in-the-middle. Questi messaggi modificano la tabella di routing dell'host e non sono autenticati. Verificare che il sistema sia configurato in modo da ignorarli a meno che non siano necessari.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` nelle macchine host dell'appliance virtuale VMware per verificare che siano configurate in modo da negare i messaggi di reindirizzamento IPv6.

Se le macchine host sono configurate per negare i reindirizzamenti IPv6, questo comando restituisce i seguenti valori:

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

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

- 2 Per configurare una macchina host dell'appliance virtuale in modo che neghi i messaggi di reindirizzamento IPv4, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare i valori delle righe che iniziano con `net.ipv6.conf`.

Se i valori delle voci elencate di seguito non sono impostati su 0 o se le voci non esistono, aggiungerle al file o aggiornare le voci esistenti nel modo appropriato.

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

- 4 Salvare le modifiche e chiudere il file.

Registrazione dei pacchetti martian IPv4

Come procedura di sicurezza consigliata, verificare che le macchine host dell'appliance virtuale VMware registrino i pacchetti martian IPv4.

I pacchetti martian contengono gli indirizzi che sono stati riconosciuti dal sistema come non validi. Configurare le macchine host per la registrazione di questi messaggi in modo da poter identificare le configurazioni errate e gli attacchi in corso.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians | grep "default|all"` nelle macchine host dell'appliance VMware per verificare che registrino i pacchetti martian IPv4.

Se le macchine virtuali sono configurate per registrare i pacchetti martian, restituiranno il seguente output:

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

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare le macchine virtuali per la registrazione dei pacchetti martian IPv4, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare i valori delle righe che iniziano con `net.ipv4.conf`.

Se i valori delle voci seguenti non sono impostati su 1 o se non esistono, aggiungerli al file o aggiornare le voci esistenti di conseguenza.

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

- 4 Salvare le modifiche e chiudere il file.

Uso del filtro del percorso inverso IPv4

Come procedura consigliata, verificare che le macchine host dell'appliance virtuale VMware utilizzino il filtro del percorso inverso IPv4.

Il filtro del percorso inverso protegge da indirizzi di origine falsificati facendo in modo che il sistema ignori i pacchetti con indirizzi di origine privi di percorso o con un percorso che non punta all'interfaccia di origine. Configurare le macchine host in modo che utilizzino il filtro del percorso inverso ogni volta che è possibile. In alcuni casi, a seconda del ruolo di sistema, il filtro del percorso inverso può fare in modo che il sistema ignori traffico lecito. Se si verificano tali problemi, potrebbe essere necessario usare una modalità più permissiva o disattivare del tutto il filtro del percorso inverso.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter | egrep "default|all"` nelle macchine host dell'appliance virtuale VMware per verificare che utilizzino il filtro del percorso inverso IPv4.

Se le macchine virtuali usano il filtro del percorso inverso IPv4, il comando restituisce quanto segue:

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

Se le macchine virtuali sono configurate correttamente, non sono richieste ulteriori azioni.

- 2 Se è necessario configurare il filtro del percorso inverso IPv4 nelle macchine host, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare i valori delle righe che iniziano con `net.ipv4.conf`.

Se i valori delle voci seguenti non sono impostati su 1 o se non esistono, aggiungerli al file o aggiornare le voci esistenti di conseguenza.

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

- 4 Salvare le modifiche e chiudere il file.

Negare l'inoltro IPv4

Verificare che le macchine host dell'appliance VMware neghino l'inoltro IPv4.

Se il sistema è configurato in modo da eseguire l'inoltro IP e non è un router designato, gli autori degli attacchi potrebbero utilizzarlo per aggirare la sicurezza della rete fornendo un percorso per le comunicazioni non filtrate dai dispositivi di rete. Per evitare questo rischio, configurare le macchine host dell'appliance virtuale in modo che neghino l'inoltro IPv4.

Procedura

- 1 Eseguire il comando `# cat /proc/sys/net/ipv4/ip_forward` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare l'inoltro IPv4.

Se le macchine host sono configurate per negare l'inoltro IPv4, questo comando restituirà il valore 0 per `/proc/sys/net/ipv4/ip_forward`. Se le macchine virtuali sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Per configurare una macchina host dell'appliance virtuale in modo che neghi l'inoltro IPv4, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Individuare la voce `net.ipv4.ip_forward=0`. Se il valore di questa voce non è impostato su 0 o se la voce non esiste, aggiungerla o aggiornare la voce esistente nel modo appropriato.
- 4 Salvare le modifiche e chiudere il file.

Negare l'inoltro IPv6

Come procedura consigliata di sicurezza, verificare che i sistemi host dell'appliance VMware neghino l'inoltro IPv6.

Se il sistema è configurato in modo da eseguire l'inoltro IP e non è un router designato, gli autori degli attacchi potrebbero utilizzarlo per aggirare la sicurezza della rete fornendo un percorso per le comunicazioni non filtrate dai dispositivi di rete. Per evitare questo rischio, configurare le macchine host dell'appliance virtuale in modo che neghino l'inoltro IPv6.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare l'inoltro IPv6.

Se le macchine host sono configurate per negare l'inoltro IPv6, questo comando restituisce i seguenti valori:

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

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare una macchina host in modo che neghi l'inoltro IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare i valori delle righe che iniziano con `net.ipv6.conf`.

Se i valori delle voci elencate di seguito non sono impostati su 0 o se le voci non esistono, aggiungerle o aggiornare le voci esistenti nel modo appropriato.

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

- 4 Salvare le modifiche apportate e chiudere il file.

Uso dei SYN cookie TCP IPv4

Verificare che le macchine host dell'appliance VMware utilizzino i SYN cookie TCP IPv4.

Un attacco flood SYN TCP può causare un Denial of Service riempiendo la tabella delle connessioni TCP di un sistema con connessioni nello stato SYN_RCVD. I SYN cookie impediscono il monitoraggio di una connessione finché non si riceve un ACK successivo, assicurandosi in tal modo che l'iniziatore stia tentando una connessione valida e non si tratti dell'origine di un attacco flood. Questa tecnica non funziona in modo pienamente conforme agli standard, ma viene attivata solo durante una condizione di flood e permette di difendere il sistema continuando a rispondere alle richieste valide.

Procedura

- 1 Eseguire il comando `# cat /proc/sys/net/ipv4/tcp_syncookies` nelle macchine host dell'appliance VMware per verificare che utilizzino i SYN cookie TCP IPv4.

Se le macchine host sono configurate per negare l'inoltro IPv4, il comando restituisce il valore 1 per `/proc/sys/net/ipv4/tcp_syncookies`. Se le macchine virtuali sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare un'appliance virtuale per l'utilizzo dei SYN cookie TCP IPv4, aprire il file `/etc/sysctl.conf` in un editor di testo.

- 3 Individuare la voce `net.ipv4.tcp_syncookies=1`.

Se il valore di questa voce non è attualmente impostato su uno o se la voce non esiste, aggiungere la voce o aggiornare quella esistente di conseguenza.

- 4 Salvare le modifiche apportate e chiudere il file.

Negare gli annunci del router IPv6

Verificare che le macchine host VMware neghino l'accettazione degli annunci del router e i reindirizzamenti ICMP a meno che non siano necessari per il funzionamento del sistema.

IPv6 consente ai sistemi di configurare i dispositivi di rete utilizzando automaticamente le informazioni fornite dalla rete. Dal punto di vista della sicurezza, configurare manualmente informazioni di configurazione importanti è preferibile rispetto ad accettarle dalla rete in modalità non autenticata.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare gli annunci del router.

Se le macchine host sono configurate per negare gli annunci del router IPv6, questo comando restituisce il valore 0.

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

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare una macchina host in modo che neghi gli annunci del router IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.

- 3 Controllare le voci seguenti:

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

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche apportate e chiudere il file.

Negare le richieste del router IPv6

Come procedura consigliata di sicurezza, verificare che le macchine host dell'appliance VMware neghino le richieste del router IPv6 a meno che non siano necessarie per il funzionamento del sistema.

L'impostazione relativa alle richieste del router determina quante richieste del router vengono inviate quando viene visualizzata l'interfaccia. Se gli indirizzi vengono assegnati in modo statico, non è necessario inviare alcuna richiesta.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations | grep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare le richieste del router IPv6.

Se le macchine host sono configurate per negare gli annunci del router IPv6, questo comando restituisce i seguenti valori:

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

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare le macchine host in modo che neghino le richieste del router IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

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

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche e chiudere il file.

Negare la preferenza del router IPv6 nelle richieste del router

Verificare che le macchine host dell'appliance VMware neghino le richieste del router IPv6 a meno che non siano necessarie per il funzionamento del sistema.

La preferenza del router nell'impostazione delle richieste determina le preferenze del router. Se gli indirizzi vengono assegnati in modo statico, non è necessario ricevere alcuna preferenza del router per le richieste.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare le richieste del router IPv6.

Se le macchine host sono configurate per negare gli annunci del router IPv6, questo comando restituisce i seguenti valori:

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

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare le macchine host in modo che neghino le richieste del router IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

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

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche apportate e chiudere il file.

Negare il prefisso del router IPv6

Verificare che le macchine host dell'appliance VMware neghino le informazioni sul prefisso del router IPv6 a meno che non siano necessarie per il funzionamento del sistema.

L'impostazione `accept_ra_pinfo` controlla se il sistema accetta informazioni sul prefisso dal router. Se gli indirizzi vengono assegnati in modo statico, non è necessario ricevere alcuna informazione sul prefisso del router.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare le informazioni sul prefisso del router IPv6.

Se le macchine host sono configurate per negare gli annunci del router IPv6, questo comando restituisce i seguenti valori:

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

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare le macchine host in modo che neghino le informazioni sul prefisso del router IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.

3 Controllare le voci seguenti:

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

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

4 Salvare le modifiche e chiudere il file.

Negare le impostazioni del limite di hop degli annunci del router IPv6

Verificare che le macchine host dell'appliance VMware neghino le impostazioni relative al limite di hop del router IPv6 a meno che non siano necessarie.

L'impostazione `accept_ra_defrtr` controlla se il sistema accetterà le impostazioni del limite di hop da un annuncio del router. Impostando il valore 0 si impedisce che un router modifichi il limite di hop IPv6 predefinito per i pacchetti in uscita.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare le impostazioni del limite di hop del router IPv6.

Se le macchine host sono configurate per negare le impostazioni del limite di hop del router IPv6, questo comando restituisce il valore 0.

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

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare una macchina host in modo che neghi le impostazioni del limite di hop del router IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

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

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche apportate e chiudere il file.

Negare le impostazioni di configurazione automatica degli annunci del router IPv6

Verificare che le macchine host dell'appliance VMware neghino le impostazioni di configurazione automatica del router IPv6 a meno che non siano necessarie.

L'impostazione `autoconf` controlla se gli annunci del router possono fare in modo che il sistema assegni un indirizzo unicast globale a un'interfaccia.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare le impostazioni di configurazione automatica del router IPv6.

Se le macchine host sono configurate per negare le impostazioni di configurazione automatica del router IPv6, questo comando restituisce il valore 0.

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

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare una macchina host in modo che neghi le impostazioni di configurazione automatica del router IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

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

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche apportate e chiudere il file.

Negare le richieste del router adiacente IPv6

Verificare che le macchine host dell'appliance VMware neghino le richieste del router adiacente IPv6 a meno che non siano necessarie.

L'impostazione `dad_transmits` determina quante richieste del router adiacente inviare per ogni indirizzo (globale e locale rispetto al collegamento) quando si visualizza un'interfaccia, per garantire che l'indirizzo desiderato sia univoco nella rete.

Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare le richieste del router adiacente IPv6.

Se le macchine host sono configurate per negare le richieste del router adiacente IPv6, questo comando restituisce il valore 0.

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

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare una macchina host in modo che neghi le richieste del router adiacente IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

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

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche apportate e chiudere il file.

Limitazione del numero massimo di indirizzi IPv6

Verificare che nelle impostazioni delle macchine host dell'appliance VMware, il numero massimo di indirizzi IPv6 sia limitato alla quantità minima necessaria per consentire il corretto funzionamento del sistema.

L'impostazione del numero massimo di indirizzi determina quanti indirizzi IPv6 unicast globali sono disponibili per ogni interfaccia. Il valore predefinito è 16, ma è consigliabile impostare il numero di indirizzi globali configurati statisticamente richiesti per il sistema specifico.

Procedura

- 1 Eseguire il comando `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che limitino in modo appropriato il numero massimo di indirizzi IPv6.

Se le macchine host sono configurate per limitare il numero massimo di indirizzi IPv6, il comando restituisce valori 1.

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

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare il numero massimo di indirizzi IPv6 nelle macchine host, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

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

Se le voci non esistono o se i loro valori non sono impostati su 1, aggiungere le voci o aggiornare le voci esistenti di conseguenza.

- 4 Salvare le modifiche apportate e chiudere il file.

Configurazione delle impostazioni di rete per l'host IaaS

Come procedura consigliata per la sicurezza, configurare le impostazioni di comunicazione di rete nella macchina host del componente Infrastructure as a Service (IaaS) VMware in base alle linee guida e ai requisiti di VMware.

Impostare la configurazione di rete della macchina host Infrastructure as a Service (IaaS) per il supporto completo delle funzioni di vRealize Automation con la protezione appropriata.

Vedere [Protezione del componente Infrastructure as a Service](#).

Configurazione di porte e protocolli

Come procedura di sicurezza consigliata, configurare le porte e i protocolli di tutti i componenti e le appliance vRealize Automation in conformità con le linee guida di VMware.

Configurare le porte in ingresso e uscita per i componenti di vRealize Automation come richiesto per il funzionamento in produzione dei componenti di sistema critici. Disabilitare tutte le porte e i protocolli non necessari. Vedere *Architettura di riferimento di vRealize Automation* in [Documentazione di VMware vRealize Automation](#).

Strumento Ports and Protocols

Lo strumento Ports and Protocols consente di visualizzare le informazioni sulle porte per una varietà di prodotti VMware e una combinazione di essi su un singolo dashboard. È inoltre possibile esportare i dati selezionati dallo strumento per l'accessibilità offline. Lo strumento Ports and Protocols supporta attualmente:

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

Lo strumento è disponibile all'indirizzo <https://ports.vmware.com/>.

Porte richieste per gli utenti

Come procedura di sicurezza consigliata, configurare le porte utente di vRealize Automation in base alle linee guida di VMware.

Esporre le porte necessarie solo in una rete sicura.

SERVER	PORTE
Appliance vRealize Automation	443, 8443

Porte necessarie per l'amministratore

Come procedura consigliata per la sicurezza, configurare le porte dell'amministratore di vRealize Automation in base alle linee guida di VMware.

Esporre le porte necessarie solo in una rete sicura.

SERVER	PORTE
Server vRealize Application Services	5480

Porte dell'appliance vRealize Automation

Come procedura di sicurezza consigliata, configurare le porte in ingresso e uscita per Appliance vRealize Automation in conformità alle raccomandazioni di VMware.

Porte in ingresso

Configurare il numero minimo di porte in ingresso richieste per Appliance vRealize Automation. Configurare porte facoltative se necessarie per la configurazione del sistema.

Tabella 8-1. Porte in ingresso minime richieste

PORTA	PROTOCOLLO	COMMENTI
443	TCP	Consente di accedere alla console di vRealize Automation e alle chiamate API.
8443	TCP	Proxy di VMware Remote Console
5480	TCP	Consente di accedere all'interfaccia di gestione dell'appliance vRealize Automation.
5488, 5489	TCP	Interne. Utilizzate da Appliance vRealize Automation per gli aggiornamenti.
5672	TCP	Messaggistica RabbitMQ.
		Nota Quando si configurano istanze di Appliance vRealize Automation in cluster, potrebbe essere necessario configurare le porte 4369 e 25672 aperte.
40002	TCP	Richiesta per il servizio vIDM. Questa porta è bloccata dal firewall per tutto il traffico esterno ad eccezione del traffico proveniente da altri nodi di Appliance vRealize Automation quando vengono aggiunti nella configurazione HA.

Se necessario, configurare le porte in ingresso facoltative.

Tabella 8-2. Porte in ingresso facoltative

PORTA	PROTOCOLLO	COMMENTI
22	TCP	(Facoltativa) SSH. In un ambiente di produzione, disabilitare il servizio SSH in ascolto sulla porta 22 e chiudere la porta 22.
80	TCP	(Facoltativa) Reindirizza a 443.

Porte in uscita

Configurare le porte in uscita richieste.

Tabella 8-3. Porte in uscita minime richieste

PORTA	PROTOCOLLO	COMMENTI
25, 587	TCP, UDP	SMTP per l'invio di notifiche via email in uscita.
53	TCP, UDP	DNS.
67, 68, 546, 547	TCP, UDP	DHCP.
110, 995	TCP, UDP	POP per la ricezione delle notifiche via email in entrata.
143, 993	TCP, UDP	IMAP per la ricezione delle notifiche via email in entrata.
443	TCP	Servizio di gestione di Infrastructure as a Service mediante protocollo HTTPS.

Se necessario, configurare le porte in uscita facoltative.

Tabella 8-4. Porte in uscita opzionali

PORTA	PROTOCOLLO	COMMENTI
80	TCP	(Facoltativa) Per il recupero degli aggiornamenti software. È possibile scaricare e applicare gli aggiornamenti separatamente.
123	TCP, UDP	(Facoltativa) Per la connessione diretta a NTP anziché utilizzare l'orario dell'host.

Strumento Ports and Protocols

Lo strumento Ports and Protocols consente di visualizzare le informazioni sulle porte per una varietà di prodotti VMware e una combinazione di essi su un singolo dashboard. È inoltre possibile esportare i dati selezionati dallo strumento per l'accessibilità offline. Lo strumento Ports and Protocols supporta attualmente:

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

Gli strumenti sono disponibili all'indirizzo <https://ports.vmware.com/>.

Porte Infrastructure as a Service

Come procedura consigliata di sicurezza, configurare le porte in ingresso e in uscita per i componenti Infrastructure as a Service (IaaS) in base alle linee guida di VMware.

Porte in ingresso

Configurare le porte in ingresso minime richieste per i componenti IaaS.

Tabella 8-5. Porte in ingresso minime richieste

COMPONENTE	PORTA	PROTOCOLLO	COMMENTI
Servizio di gestione	443	TCP	Comunicazione con i componenti di IaaS e con l'appliance vRealize Automation su protocollo HTTPS. In tutti gli host di virtualizzazione gestiti da agenti proxy deve essere aperta anche la porta TCP 443 per il traffico in ingresso.

Porte in uscita

Configurare le porte in uscita minime richieste per i componenti IaaS.

Tabella 8-6. Porte in uscita minime richieste

COMPONENTE	PORTA	PROTOCOLLO	COMMENTI
Tutto	53	TCP, UDP	DNS.
Tutto		TCP, UDP	DHCP.
Servizio di gestione	443	TCP	Comunicazione con l'appliance vRealize Automation su protocollo HTTPS.
Sito Web	443	TCP	Comunicazione con il servizio di gestione su protocollo HTTPS.
Distributed Execution Manager	443	TCP	Comunicazione con il servizio di gestione su protocollo HTTPS.
Agenti proxy	443	TCP	Comunicazione con il servizio di gestione e gli host di virtualizzazione su protocollo HTTPS.
Agente guest	443	TCP	Comunicazione con il servizio di gestione su protocollo HTTPS.
Servizio di gestione, sito Web	1433	TCP	MSSQL.

Se necessario, configurare le porte in uscita opzionali.

Tabella 8-7. Porte in uscita opzionali

COMPONENTE	PORTA	PROTOCOLLO	COMMENTI
Tutto	123	TCP, UDP	NTP è opzionale.

Controllo e registrazione

Come procedura consigliata per la sicurezza, configurare il controllo e la registrazione nel sistema vRealize Automation in base alle raccomandazioni di VMware.

La registrazione remota in un host di file di registro centrale fornisce un archivio sicuro per i file di registro. Raccogliendo i file di registro in un host centrale, è possibile monitorare l'ambiente con un solo strumento. È inoltre possibile eseguire analisi aggregate e cercare la prova di minacce quali attacchi coordinati a più entità all'interno dell'infrastruttura. La registrazione in un server di file di registro centralizzato e protetto può impedire la manomissione dei file di registro e fornisce inoltre una registrazione di controllo a lungo termine.

Assicurarsi che il server di registrazione remota sia protetto

Spesso, dopo aver violato la sicurezza del computer host, gli autori degli attacchi possono cercare e manomettere i file di registro per coprire le loro tracce e mantenere il controllo senza essere scoperti. Proteggere in modo adeguato il server di registrazione remota contribuisce a scoraggiare la manomissione del registro.

Utilizzare un server NTP autorizzato

Assicurarsi che tutte le macchine host utilizzino la stessa origine ora relativa, incluso lo stesso offset di localizzazione pertinente, e che sia possibile correlare l'origine ora relativa a uno standard orario concordato, come l'ora UTC (Coordinated Universal Time). Un approccio disciplinato alle origini ora consente di individuare rapidamente e correlare le azioni di un intruso quando si esaminano i file di registro pertinenti. Impostazioni orarie errate possono rendere difficoltosa l'ispezione e la correlazione dei file di registro allo scopo di rilevare gli attacchi e possono rendere imprecisi i controlli.

Usare almeno tre server NTP di origini ora esterne oppure configurare alcuni server NTP locali in una rete affidabile che a sua volta riceva l'ora da almeno tre origini ora esterne.