Guia de configuração segura

03 de maio de 2018
vRealize Automation 7.3

vmware®

Você pode encontrar a documentação técnica mais atualizada no site da VMware, em:

https://docs.vmware.com/br/

Caso tenha comentários sobre esta documentação, envie seu feedback para:

docfeedback@vmware.com

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

Conteúdo

Configuração Segura

1

A Configuração Segura ajuda os usuários a avaliarem e otimizarem a configuração segura das implantações do vRealize Automation.

A Configuração Segura descreve a verificação e configuração de implantações seguras para ambientes típicos do vRealize Automation e oferece informações e procedimentos para ajudar os usuários a tomarem decisões baseadas em informações em reação à configuração de segurança.

Público-alvo

Estas informações são concebidas para administradores de sistema do vRealize Automation e outros usuários responsáveis pela manutenção e configuração de segurança do sistema.

Glossário de publicações técnicas da VMware

O documento Publicações técnicas da VMware fornece um glossário de termos que podem não ser familiares para você. Para conhecer definições de termos usados na documentação técnica da VMware, acesse http://www.vmware.com/support/pubs.

Informações atualizadas 2

Este *Guia de Configuração Segura* é atualizado a cada nova versão do produto ou quando necessário.

Esta tabela fornece o histórico de atualizações do *Guia de Configuração Segura*.

Revisão	Descrição
3 de maio de 2018	Edições secundárias.
5 de dezembro de 2017	Foi atualizado Ativar TLS na configuração do localhost
002535-01	Tempo limite de sessão do Appliance do vRealize Automation atualizado.
002535-00	Versão inicial.

Visão geral da linha de base segura do vRealize Automation 3

A VMware oferece recomendações abrangentes para ajudar você a verificar e configurar uma linha de base segura para o seu sistema vRealize Automation.

Use as ferramentas e procedimentos adequados conforme especificado pela VMware para verificar e manter uma configuração de linha de base segura e reforçada para o seu sistema vRealize Automation. Alguns componentes do vRealize Automation são instalados em estado reforçado ou semirreforçado, mas você deve rever e verificar a configuração de cada componente à luz das recomendações de segurança da VMware, políticas de segurança da empresa e ameaças conhecidas.

Postura de segurança do vRealize Automation

A postura de segurança do vRealize Automation presume um ambiente holisticamente seguro baseado nas configurações do sistema e rede, políticas de segurança organizacional e melhores práticas de segurança.

Ao verificar e configurar o reforço de um sistema vRealize Automation, considere cada uma das áreas conforme tratadas pelas recomendações de reforço da VMware.

- Implantação segura
- Configuração Segura
- Segurança da rede

Para garantir que seu sistema esteja reforçado de forma segura, considere as recomendações da VMware e suas políticas de segurança locais, conforme relacionadas a estas áreas conceituais.

Componentes do sistema

Ao considerar o reforço e a configuração segura do seu sistema vRealize Automation, certifique-se de entender todos os componentes e como eles trabalham juntos para garantir a funcionalidade do sistema.

Considere os seguintes componentes ao planejar e implementar um sistema seguro.

- Appliance do vRealize Automation
- Componentes de IaaS

Para se familiarizar com o vRealize Automation e como os componentes operam juntos, consulte *Fundamentos e conceitos* no centro de documentação do vRealize Automation da VMware. Para obter informações sobre implantações e arquitetura típicas do vRealize Automation, consulte *Arquitetura de referência*.

Verificar a integridade da mídia de instalação

4

Os usuários devem sempre verificar a integridade da mídia de instalação antes de instalar um produto VMware.

Sempre verifique o hash SHA1 após baixar um ISO, pacote off-line ou patch para assegurar a integridade e autenticidade dos arquivos baixados. Caso obtenha a mídia física da VMware e o lacre de segurança estiver rompido, retorne o software para a VMware para substituição.

Após baixar a mídia, use o valor de soma MD5/SHA1 para verificar a integridade do download. Compare a saída do hash MD5/SHA1 com o valor publicado no site da VMware. Os hashs SHA1 ou MD5 devem ser iguais.

Para mais informações sobre a verificação de integridade da mídia de instalação, consulte http://kb.vmware.com/kb/1537.

Reforçar infraestrutura de software do sistema da VMware 5

Como parte do processo de reforço, avalie a infraestrutura de software implantada que dá suporte ao sistema da VMware e verifique se ela atende às diretrizes de reforço da VMware.

Antes de reforçar o sistema da VMware, avalie e resolva falhas de segurança na infraestrutura de software de suporte para criar um ambiente totalmente reforçado e seguro. Elementos de infraestrutura de software para considerar incluem componentes do sistema operacional, software de suporte e software de banco de dados. Resolva preocupações de segurança nestes componentes e em outros de acordo com as recomendações do fabricante e outros protocolos de segurança relevantes.

Este capítulo inclui os seguintes tópicos:

Reforçar o ambiente do VMware vSphere ®

Avalie o ambiente do VMware vSphere ® e verifique se o nível adequado da recomendação de reforço do vSphere está sendo aplicado e mantido.

Para mais informações sobre reforço, consulte http://www.vmware.com/security/hardening-guides.html .

Como parte de um ambiente reforçado de forma abrangente, a infraestrutura do VMware vSphere ® deve atender às diretrizes de segurança estabelecidas pela VMware.

Reforçar o host de Infraestrutura como Serviço

Verifique se a máquina de host Microsoft Windows de Infraestrutura como Serviço está reforçada de acordo com as diretrizes da VMware:

Consulte as recomendações nas diretrizes de reforço e proteção do Microsoft Windows para garantir que o host do Windows Server esteja reforçado corretamente. Deixar de seguir as recomendações de reforço pode resultar em exposição a vulnerabilidades de segurança conhecidas em componentes inseguros nas versões do Windows.

Para verificar se a sua versão é compatível, consulte a Matriz de Suporte do vRealize Automation.

Entre em contato com o seu fornecedor Microsoft para obter a orientação adequada sobre práticas de reforço em produtos Microsoft.

Reforçar o Microsoft SQL Server

Verifique se o banco de dados do Microsoft SQL Server atende às diretrizes de segurança conforme estabelecido pela Microsoft e pela VMware.

Consulte as recomendações definidas nas diretrizes de reforço e proteção do Microsoft SQL Server. Consulte todos os boletins de segurança da Microsoft relacionados à versão instalada do Microsoft SQL Server. Deixar de seguir as recomendações de reforço pode resultar em exposição a vulnerabilidades de segurança conhecidas em componentes inseguros nas versões do Microsoft SQL Server.

Para verificar se a sua versão do Microsoft SQL Server é compatível, consulte a Matriz de Suporte do vRealize Automation.

Entre em contato com o seu fornecedor Microsoft para obter orientação sobre as práticas de reforço dos produtos Microsoft.

Reforçar o Microsoft .NET

Como parte de um ambiente reforçado de forma abrangente, o Microsoft .NET deve atender às diretrizes de segurança estabelecidas pela Microsoft e pela VMware.

Reveja as recomendações definidas nas diretrizes adequadas de reforço e proteção de .NET. Além disso, consulte todos os boletins de segurança da Microsoft relacionados à versão do Microsoft SQL Server que você está utilizando. Deixar de seguir as recomendações de reforço pode resultar em exposição a vulnerabilidades de segurança conhecidas em componentes inseguros do Microsoft.NET.

Para verificar se a sua versão do Microsoft.NET é compatível, consulte a Matriz de Suporte do vRealize Automation.

Entre em contato com o seu fornecedor Microsoft para obter orientação sobre as práticas de reforço dos produtos Microsoft.

Reforçar o Internet Information Services Microsoft (IIS)

Verifique se o Internet Information Services Microsoft (IIS) atendem a todas as diretrizes de segurança da Microsoft e da VMware,

Reveja as recomendações definidas nas diretrizes adequadas de reforço e proteção do Microsoft IIS. Além disso, consulte todos os boletins de segurança da Microsoft relacionados à versão do Microsoft IIS que você está utilizando. Deixar de seguir as recomendações de reforço pode resultar em exposição a vulnerabilidades de segurança conhecidas.

Para verificar se a sua versão é compatível, consulte a Matriz de Suporte do vRealize Automation.

Entre em contato com o seu fornecedor Microsoft para obter orientação sobre as práticas de reforço dos produtos Microsoft.

Revisar softwares instalados

6

Uma vez que vulnerabilidades em softwares de terceiros ou não utilizados aumentam o risco de acesso não autorizado ao sistema e disrupção da disponibilidade, é importante revisar todos os softwares instalados nas máquinas de host do VMware e avaliar seu uso.

Não instale softwares que não sejam necessários para a operação segura do sistema nas máquinas de host do VMware. Desinstale softwares não utilizados ou externos

Software não compatível instalado no inventário

Avalie sua implantação do VMware e o inventário dos produtos instalados para conferir se nenhum software não compatível externo está instalado.

Para mais informações sobre as políticas de compatibilidade para produtos de terceiros, consulte o artigo de suporte do VMware em https://www.vmware.com/support/policies/thirdparty.html.

Verificar softwares de terceiros

A VMware não oferece suporte nem recomenda a instalação de softwares de terceiros que não tenham sido testados e verificados. Softwares de terceiros inseguros, desatualizados ou não autenticados instalados nas máquinas de host do VMware podem colocar o sistema em risco de acesso não autorizado e disrupção da disponibilidade. Caso precise utilizar um software de terceiro não compatíveis, consulte o fornecedor terceiro para os requisitos de configuração segura e atualizações.

Avisos e patches de segurança da VMware

7

Para manter a máxima segurança em seu sistema, siga os avisos de segurança da VMware e aplique todos os patches relevantes.

A VMware emite avisos de segurança para os produtos. Acompanhe esses avisos para garantir que seu produto esteja protegido contra ameaças conhecidas.

Avale a instalação do vRealize Automation, histórico de patches e atualizações, e confirme se os Avisos de Segurança emitidos pela VMware são seguidos e aplicados.

Para mais informações sobre os avisos de segurança atuais da VMware, consulte http://www.vmware.com/security/advisories/.

Configuração Segura

8

Verifique e atualize as configurações de segurança dos appliances virtuais do vRealize Automation e o componente de Infraestrutura como Serviço conforme apropriado para a configuração do seu sistema. Além disso, verifique e atualize a configuração de outros componentes e aplicações.

Configurar uma instalação do vRealize Automation com segurança envolve tratar a configuração de cada componente individualmente e em seu funcionamento em conjunto. Considere a configuração de todos os componentes do sistema em conjunto para obter uma linha de base razoavelmente segura.

Este capítulo inclui os seguintes tópicos:

Protegendo o appliance do vRealize Automation

Verifique e atualize as configurações de segurança para o appliance do vRealize Automation conforme necessário para a configuração do sistema.

Defina as configurações de segurança para seus appliances virtuais e seus sistemas operacionais host. Além disso, defina ou verifique a configuração de outros componentes e aplicativos relacionados. Em alguns casos, você precisa verificar as configurações existentes, enquanto em outros casos você deve alterar ou adicionar configurações para obter uma definição apropriada.

Alterar a senha raiz

Você pode alterar a senha raiz do Appliance do vRealize Automation para atender aos requisitos de segurança aplicáveis.

Altere a senha raiz no Appliance do vRealize Automation usando a Virtual Appliance Management Interface. Verifique se a senha raiz atende aos requisitos de complexidade de senha corporativa da organização.

Procedimentos

1 Abra a Virtual Appliance Management Interface para o seu Appliance do vRealize Automation.

   https://*vRealizeAppliance-url*:5480

2 Selecione a guia **Administrador** na Virtual Appliance Management Interface.

3 Selecione o submenu **Administrador**.

4 Insira a senha existente na caixa de texto **Senha do administrador atual**.

5 Insira a nova senha na caixa de texto **Nova senha do administrador**.

6 Insira a nova senha na caixa de texto **Redigitar a nova senha do administrador**.

7 Clique em **Salvar configurações** para salvar suas alterações.

Verificar hash e complexidade da senha raiz

Verifique se a senha raiz atende aos requisitos de complexidade de senha corporativa da organização.

Validar a complexidade da senha raiz é necessário, já que o usuário raiz ignora a verificação de complexidade de senha do módulo pam_cracklib que é apicada a contas de usuário.

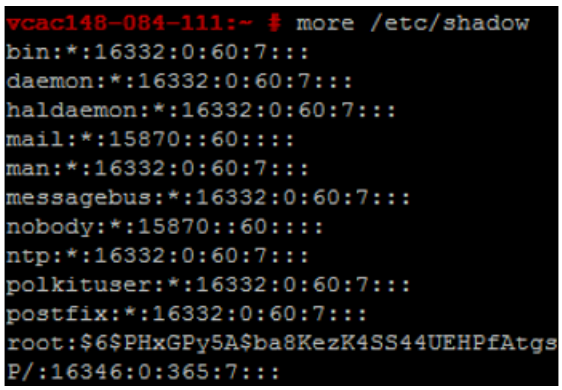
A senha da conta deve iniciar com `$6$`, que indica um hash sha512. Esse é o hash padrão para todos os appliances reforçados.

Procedimentos

1 Para verificar o hash da senha raiz, faça login como raiz e execute o comando `# more /etc/shadow`.

As informações de hash são exibidas.

Figura 8-1. Resultados de hash da senha



2 Se a senha raiz não contiver um hash sha512, execute o comando `passwd` para alterá-la.

Todos os appliances reforçados ativam `enforce_for_root` para o módulo `pw_history`, encontrado no arquivo `/etc/pam.d/common-password`. O sistema recorda as últimas cinco senhas por padrão. As senhas antigas são armazenadas para cada usuário no arquivo `/etc/securetty/passwd`.

Verificar histórico de senhas raiz

Verifique se o histórico de senhas é aplicado para a conta raiz.

Todos os appliances reforçados ativam `enforce_for_root` para o módulo pw_history, encontrado no arquivo `/etc/pam.d/common-password`. O sistema recorda as últimas cinco senhas por padrão. As senhas antigas são armazenadas para cada usuário no arquivo `/etc/securetty/passwd`.

Procedimentos

1 Execute o seguinte comando:

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

2 Certifique-se de que o `enforce_for_root` aparece nos resultados retornados.

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

Gerenciar expiração de senha

Configure todas as expirações de senhas de acordo com as políticas de segurança da sua organização.

Por padrão, todas as contas do appliance virtual reforçado do VMware utilizam uma expiração de senha de 60 dias. Na maioria dos appliances reforçados, a conta raiz é definida para uma expiração de senha de 365 dias. Como melhor prática, verifique se a expiração em todas as contas atende aos padrões dos requisitos de segurança e operação.

Se a senha raiz expirar, você não poderá reutilizá-la. Você deve implementar políticas específicas ao local para evitar que as senhas administrativas e raiz expirem.

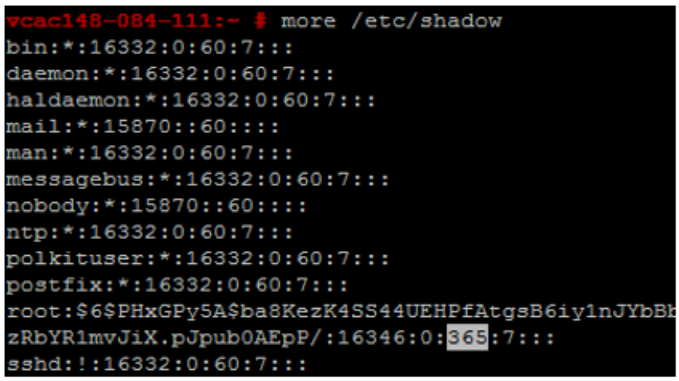
Procedimentos

1 Faça login nas máquinas do appliance virtual como raiz e execute o seguinte comando para verificar a expiração de senha em todas as contas.

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

A expiração de senha é o quinto campo (os campos são separados por vírgula) do arquivo sombra. A expiração da raiz é definida em dias.

Figura 8-2. Campo de expiração de senha



2 Para modificar a expiração da conta raiz, execute um comando no formato a seguir.

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

Neste comando, 365 especifica o número de dias até a expiração da senha. Use o mesmo comando para modificar qualquer usuário, substituindo "raiz" pela conta específica e substituindo o número de dias para atender aos padrões de expiração da organização.

Gerenciar Shell Seguro e contas administrativas

Para conexões remotas, todos os appliances reforçados incluem o protocolo Shell seguro (SSH). Use o SSH somente quando necessário e gerencie-o adequadamente para preservar a segurança do sistema.

O SSH é um ambiente interativo de linha de comando compatível com conexões remotas a appliances virtuais do VMware. Por padrão, o acesso do SSH requer credenciais de conta de usuário com alto privilégio. Em geral, as atividades de SSH do usuário raiz dispensam o controle de acesso baseado em função (RBAC) e controles de auditoria dos appliances virtuais.

Como melhor prática, desative o SSH em um ambiente de produção e ative-o somente para resolver problemas que não podem ser resolvidos por outros meios. Deixe-o habilitado somente quando for necessário para uma finalidade específica e em conformidade com as políticas de segurança da sua organização. O SSH está desabilitado por padrão no appliance do vRealize Automation. Dependendo da configuração do vSphere, você pode habilitar ou desabilitar o SSH ao implantar o modelo do Formato Aberto de Virtualização (OVF).

Como teste simples para determinar se o SSH está habilitado em uma máquina, tente abrir uma conexão usando SSH. Se a conexão abrir e solicitar credenciais, isso significa que o SSH está habilitado e disponível para conexões.

Conta de usuário raiz do Shell Seguro

Como appliances do VMware não incluem contas de usuário pré-configuradas, a conta raiz pode usar SSH para fazer login diretamente por padrão. Desative o SSH como raiz assim que possível.

Para atender aos padrões de conformidade de não repúdio, o servidor de SSH em todos os appliances reforçados é pré-configurado com a entrada de roda AllowGroups para restringir o acesso de SSH à roda do grupo secundário. Para separação de obrigações, você pode modificar a entrada de roda AllowGroups no arquivo `/etc/ssh/sshd_config` para usar outro grupo, como sshd.

O grupo de roda é habilitado com o módulo `pam_wheel` para acesso de superusuário, para que os membros do grupo da roda possam fazer o acesso como superusuário raiz, onde a senha raiz é exigida. A separação de grupos permite que os usuários usem SSH no appliance sem ter acesso de superusuário à raiz. Não remova ou modifique outras entradas no campo AllowGroups, que garante a funcionalidade correta do appliance. Após fazer uma alteração, você deve reiniciar o daemon do SSH executando o comando: `# service sshd restart`

Ativar ou desativar Shell Seguro nos appliances do vRealize Automation

Ative o Shell Seguro (SSH) no appliance do vRealize Automation somente para resolução de problemas. Desative o SSH nesses componentes durante a operação de produção normal.

Você pode ativar ou desativar o SSH no appliance do vRealize Automation usando o console de Gerenciamento do Appliance Virtual.

Procedimentos

1 Navegue até o Console de Gerenciamento do Appliance Virtual (VAMI) para o seu appliance do vRealize Automation.

: https://*vRealizeAppliance url*:5480

2 Clique na guia **Administração**.

3 Clique no submenu **Administração**.

4 Marque a caixa de seleção **Ativar serviço de SSH** para ativar o SSH ou desmarque-a para desativar o SSH.

5 Clique em **Salvar configurações** para salvar suas alterações.

Criar uma conta de administrador local para o Secure Shell

Como prática recomendada de segurança, crie e configure contas administrativas locais para o Secure Shell (SSH) nas suas máquinas host do appliance virtual. Além disso, remova o acesso SSH raiz depois de criar as contas apropriadas.

Crie contas administrativas locais para SSH ou membros do grupo wheel secundário, ou ambos. Antes de desativar o acesso raiz direto, teste se os administradores autorizados podem acessar o SSH usando o AllowGroups e se eles podem usar o comando su to root usando o grupo wheel.

Procedimentos

1 Faça login no appliance virtual como raiz e execute os seguintes comandos com o nome de usuário apropriado.

```
# useradd –g users <username> –G wheel –m –d /home/nome de usuário
             # passwd username
```

Wheel é o grupo especificado em AllowGroups para acesso ssh. Para adicionar vários grupos secundários, use `–G wheel,sshd`.

2 Mude para o usuário e forneça uma nova senha para reforçar a verificação de complexidade da senha.

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

Se a complexidade da senha for atendida, a senha será atualizada. Se a complexidade da senha não for atendida, a senha voltará para a senha original e será necessário executar novamente o comando de senha.

3 Para remover o login direto para SSH, modifique o arquivo `/etc/ssh/sshd_config` substituindo `(#)PermitRootLogin yes` por `PermitRootLogin no`.

   Como alternativa, você pode ativar/desativar o SSH na Virtual Appliance Management Interface (VAMI) marcando ou desmarcando a caixa de seleção **Login SSH de administrador ativado** na guia **Administrador**.

Próximo passo

Desative os logins diretos como raiz. Por padrão, os appliances protegidos permitem o login direto para raiz através do console. Depois de criar contas administrativas para não repúdio e testá-las para acesso à roda su-root, desative os logins de raiz diretos editando o arquivo `/etc/security` como root e substituindo a entrada `tty1` por `console`.

1 Abra o arquivo `/etc/securetty` em um editor de texto.

2 Localize `tty1` e substitua-o por `console`.

3 Salve o arquivo e feche-o.

Restringir acesso com shell seguro

Como parte do processo de reforço do seu sistema, restrinja o acesso com Shell Seguro (SSH) configurando o pacote cp_wrappers de forma correta em todas as máquinas de host do appliance virtual do VMware. Mantenha também as permissões de arquivo de chave SSH necessárias nesses appliances.

Todos os appliances virtuais do VMware incluem o pacote tcp_wrappers para permitir que daemons compatíveis com tcp controlem as sub-redes da rede capazes de acessar os daemons libwrapped. Por padrão, o arquivo `/etc/hosts.allow` contém uma entrada genérica, `Sshd: ALL : ALLOW`, que permite todos os acessos ao shell seguro. Restrinja esse acesso conforme adequado para sua organização.

Procedimentos

1 Abra o arquivo `/etc/hosts.allow` na máquina de host do appliance virtual em um editor de texto.

2 Altere a entrada genérica no ambiente de produção para incluir somente as entradas do host local e a sub-rede da rede de gerenciamento para operações seguras.

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

   Neste exemplo, todas as conexões do host local e conexões que os clientes fazem na sub-rede 10.0.0.0 são permitidas.

3 Adicione todas as identificações de máquina apropriadas; por exemplo, nome do host, endereço IP, nome de domínio totalmente qualificado (FQDN) e loopback.

4 Salve o arquivo e feche-o.

Reforçar a configuração do servidor de Shell Seguro

Quando possível, todos os appliances do VMware possuem uma configuração reforçada por padrão. Os usuários podem verificar se sua configuração está reforçada corretamente examinando as configurações do servidor e serviço do cliente na seção de opções globais do arquivo de configuração.

Se possível, restrinja o uso do servidor de SSH para uma sub-rede de gerenciamento no arquivo `/etc/hosts.allow`.

Procedimentos

1 Abra o arquivo de configuração do servidor `/etc/ssh/sshd_config` no appliance do VMware e verifique se as configurações estão corretas.

Configuração	Status
Protocolo do daemon do servidor	Protocolo 2
Cifras CBC	aes256-ctr e aes128-ctr
Encaminhamento TCP	AllowTCPForwarding no
Portas de gateway do servidor	Gateway Ports no
Encaminhamento X11	X11Forwarding no
Serviço de SSH	Use o campo AllowGroups e especifique um acesso permitido de grupo. Adicione os membros apropriados a esse grupo.
Autenticação GSSAPI	GSSAPIAuthentication no, if unused
Autenticação Keberos	KeberosAuthentication no, if unused
Variáveis locais (opção global AcceptEnv)	Defina como `desativado por comentário` ou `ativado para variáveis LC_* ou LANG`
Configuração de túnel	PermitTunnel no
Sessões de rede	MaxSessions 1
Conexões concorrentes do usuário	Defina como 1 para usuário raiz e qualquer outro usuário. O arquivo `/etc/security/limits.conf` também precisa ser definido com as mesmas configurações.
Verificação de modo restrito	Strict Modes yes
Separação de privilégios	UsePrivilegeSeparation yes
Autenticação RSA de rhosts	RhostsESAAuthentication no
Compressão	Compression delayed or Compression no
Código de autenticação da mensagem	MACs hmac-sha1
Restrição ao acesso do usuário	PermitUserEnvironment no

2 Salve suas alterações e feche o arquivo.

Reforçar a configuração do cliente de Shell Seguro

Como parte do processo de reforço do sistema, verifique o reforço do cliente de SSH examinando o arquivo de configuração do cliente de SSH nas máquinas de host do appliance virtual para garantir que ele está configurado de acordo com as diretrizes da VMware.

Procedimentos

1 Abra o arquivo de configuração do cliente de SSH, `/etc/ssh/ssh_config`, e verifique se as configurações da seção de opções globais estão corretas.

Configuração	Status
Protocolo do cliente	Protocolo 2
Portas de gateway do cliente	Gateway Ports no
Autenticação GSSAPI	GSSAPIAuthentication no
Variáveis locais (opção global SendEnv)	Fornecer somente variáveis LC_* ou LANG
Cifras CBC	Somente aes256-ctr e aes128-ctr
Códigos de autenticação da mensagem	Usados somente na entrada `MACs hmac-sha1`

2 Salve suas alterações e feche o arquivo.

Verificar permissões de arquivo da chave do shell seguro

Para minimizar a possibilidade de ataques maliciosos, mantenha permissões críticas de arquivo de chave de SSH nas máquinas de host do appliance virtual.

Após configurar ou atualizar suas configurações de SSH, sempre verifique se as permissões do arquivo de chave de SSH a seguir não foram alteradas.

- Os arquivos de chave do host público em `/etc/ssh/*key.pub` são de posse do usuário raiz e têm permissões definidas para 0644 (-rw-r--r--).
- Os arquivos de chave do host privado em `/etc/ssh/*key` são de posse do usuário raiz e têm permissões definidas para 0600 (-rw------).

Verificar permissões de arquivo de chave SSH

Verifique se permissões SSH estão aplicadas a ambos os arquivos de chave pública e particular.

Procedimentos

1 Verifique os arquivos de chave pública SSH executando o seguinte comando: `ls -l /etc/ssh/*key.pub`

2 Verifique se o proprietário é root, se o proprietário do grupo é root e se os arquivos têm permissões definidas como 0644 (-rw-r--r--).

3 Corrija problemas executando os seguintes comandos.

```
chown root /etc/ssh/*key.pub
chgrp root /etc/ssh/*key.pub
chmod 644 /etc/ssh/*key.pub
```

4 Verifique os arquivos de chave particular SSH executando o seguinte comando: `ls –l /etc/ssh/*key`

5 Corrija problemas executando os seguintes comandos.

```
chown root /etc/ssh/*key
chgrp root /etc/ssh/*key
chmod 644 /etc/ssh/*key
```

Alterar o usuário da Interface de Gerenciamento de Appliances Virtuais

Você pode adicionar e excluir usuários na Interface de Gerenciamento de Appliances Virtuais para criar o nível de segurança apropriado.

A conta de usuário raiz da Interface de Gerenciamento de Appliances Virtuais usa o PAM para autenticação e, portanto, os níveis de corte definidos pelo PAM também se aplicam. Se você não tiver isolado corretamente a Interface de Gerenciamento de Appliances Virtuais, um bloqueio da conta raiz do sistema poderá ocorrer se um invasor tentar forçar o login de forma bruta. Além disso, quando a conta raiz é considerada insuficiente para fornecer não repúdio por mais de uma pessoa na sua organização, você pode optar por alterar o usuário administrador da interface de gerenciamento.

Pré-requisitos

Procedimentos

1 Execute o seguinte comando para criar um novo usuário e adicioná-lo ao grupo da Interface de Gerenciamento de Appliances Virtuais.

```
useradd –G vami,root user
```

2 Crie uma senha para o usuário.

```
passwd user
```

3 (Opcional) Execute o seguinte comando para desativar o acesso raiz na Interface de Gerenciamento de Appliances Virtuais.

```
usermod –R vami root
```

Observação A ação de desativar o acesso raiz à Interface de Gerenciamento de Appliances Virtuais também desativa a capacidade de atualizar a senha do administrador, ou raiz, na guia Administração.

Definir autenticação do bootloader

Para oferecer um nível adequado de segurança, configure a autenticação do bootloader nos appliances virtuais do VMware.

Se o bootloader do sistema não exigir autenticação, os usuários com acesso ao console do sistema poderão alterar as configurações de inicialização do sistema, ou inicializar o sistema em modo de usuário único ou manutenção, o que pode resultar em negação do serviço ou em acesso não autorizado ao sistema. Como a autenticação do bootloader não é definida por padrão nos appliances virtuais do VMware, você deverá criar uma senha GRUB para configurá-la.

Procedimentos

1. Verifique se existe uma senha de inicialização localizando a linha `password --md5 <password-hash>` no arquivo `/boot/grub/menu.lst` nos appliances virtuais.
2. Se não existir nenhuma senha, execute o comando `# /usr/sbin/grub-md5-crypt` no appliance virtual.

   Uma senha MD5 será gerada e o comando fornecerá a saída de hash md5.
3. Anexe a senha ao arquivo `menu.lst` executando o comando `# password --md5 <hash from grub-md5-crypt>`.

Configurar o NTP

Para o fornecimento de horário crítico, desative a sincronização de data/hora do host e use o Network Time Protocol (NTP) no appliance do vRealize Automation.

O daemon NTP no appliance do vRealize Automation fornece serviços de hora sincronizados. O NTP está desativado por padrão; portanto, é necessário configurá-lo manualmente. Se possível, use o NTP em ambientes de produção para rastrear ações de usuários e detectar possíveis ataques e intrusões maliciosos por meio de auditoria e registro de manutenção precisos. Para obter informações sobre avisos de segurança do NTP, consulte o site do NTP.

O arquivo de configuração do NTP está localizado na pasta `/etc/` em cada appliance. Você pode ativar o serviço NTP para o appliance do vRealize Automation e adicionar servidores de horário na guia **Administrador** da Virtual Appliance Management Interface.

Procedimentos

1. Abra o arquivo de configuração `/etc/ntp.conf` na máquina host do appliance virtual usando um editor de texto.
2. Defina a propriedade do arquivo como **`root:root`**.
3. Defina as permissões para **`0640`**.

4 Para reduzir o risco de um ataque de amplificação de negação de serviço no NTP, abra o arquivo `/etc/ntp.conf` e verifique se as linhas de restrição aparecem no arquivo.

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

5 Salve as alterações e feche os arquivos.

Configurando o TLS para dados do appliance do vRealize Automation em trânsito

Certifique-se de que a implantação do seu vRealize Automation usa protocolos TLS fortes para proteger canais de transmissão para componentes do appliance do vRealize Automation.

Para considerações de desempenho, o TLS não está habilitado para conexões localhost entre alguns application services. Em locais onde a defesa em profundidade é preocupante, habilite o TLS em todas as comunicações localhost.

Importante Se você estiver finalizando o TLS no balanceador de carga, desative protocolos inseguros, como SSLv2, SSLv3 e TLS 1.0 em todos os balanceadores de carga.

Ativar TLS na configuração do localhost

Por padrão, algumas comunicações do localhost não usam TLS. Você pode ativar o TLS em todas as conexões do localhost para oferecer maior segurança.

Procedimentos

1 Conectar ao Appliance do vRealize Automation usando SSH.

2 Defina as permissões para o keystore vcac executando os seguintes comandos.

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

3 Atualize a configuração de HAProxy.

a Localize as linhas contendo a seguinte string

`server local 127.0.0.1`… e adicione o seguinte ao final dessas linhas: `ssl verify none`

Esta seção contém outras linhas semelhantes às linhas abaixo.

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

b Altere a porta de backend-horizon de 8080 para 8443.

4 Obtenha a senha de keystorePass.

   a Localize a propriedade `certificate.store.password` no arquivo `/etc/vcac/security.properties`.

   Por exemplo, `certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

   b Desencripte o valor usando o seguinte comando:

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

   Por exemplo, `vcac–config prop–util –d ––p s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

5 Configure o serviço vRealize Automation

   a Abra o arquivo `/etc/vcac/server.xml`.

   b Adicione o seguinte atributo à tag Connector, substituindo certificate.store.password pelo valor da senha do repositório de certificados encontrado em `etc/vcac/security.properties`.

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

6 Configure o serviço vRealize Orchestrator.

   a Abra o arquivo `/etc/vco/app/server.xml`

   b Adicione o seguinte atributo à tag Connector, substituindo certificate.store.password pelo valor da senha do repositório de certificados encontrado em `etc/vcac/security.properties`.

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

7 Reinicie o vRealize Orchestrator, vRealize Automation e serviços de haproxy.

```
service vcac–server restart
service vco–server restart
service haproxy restart
```

Observação Se o vco-server não reiniciar, reinicialize o computador host.

8 Configure a Interface de Gerenciamento do Appliance Virtual.

   a Abra o arquivo `/opt/vmware/share/htdocs/service/café–services/services.py`.

   b Altere a linha `conn = httplib.HTTP()` para `conn = httplib.HTTPS()` para aumentar a segurança.

Ativar conformidade com o Padrão Federal de Processamento de Informações (FIPS) 140-2

O appliance do vRealize Automation agora utiliza a versão do OpenSSL certificada conforme o Padrão Federal de Processamento de Informações (FIPS) 140-2 para dados em trânsito sobre TLS em todo o tráfego de entrada e saída da rede.

Você pode ativar ou desativar o modo FIPS na interface de gerenciamento do appliance do vRealize Automation. Você também pode configurar o FIPS a partir da linha de comando ao acessar como raiz, usando os seguintes comandos:

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

Quando o FIPS está ativado, o tráfego de rede de entrada e saída do Appliance do vRealize Automation na porta 443 usa a criptografia em conformidade com FIPS 140–2. Independentemente da configuração de FIPS, o vRealize Automation usa AES–256 para proteger os dados seguros armazenados no appliance do vRealize Automation.

Observação Atualmente, o vRealize Automation só pode ativar parcialmente a conformidade com FIPS, porque alguns componentes internos não usam ainda os módulos criptográficos certificados. Em casos onde módulos certificados ainda não tenham sido implantados, a criptografia baseada em AES–256 é usada em todos os algoritmos criptográficos.

Observação O procedimento a seguir vai reinicializar a máquina física quando você alterar a configuração.

Procedimentos

1. Faça login como raiz na interface de gerenciamento do appliance do vRealize Automation.

   `https:// vrealize-automation-appliance-FQDN:5480`

2. Selecione **Configurações do vRA > Configurações do Host**.
3. Clique no botão sob o cabeçalho Ações no canto superior direito para ativar ou desativar o FIPS.
4. Clique em **Sim** para reiniciar o appliance do vRealize Automation

Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados

Como parte do processo de reforço, certifique-se de que o Appliance do vRealize Automation implantado utilize canais seguros de transmissão.

Pré-requisitos

Conclua a Ativar TLS na configuração do localhost.

Procedimentos

1 Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados nos manipuladores https de HAProxy no Appliance do vRealize Automation.

Reveja este arquivo	Certifique-se de que o seguinte está presente	Na linha apropriada como mostrado
`/etc/haproxy/conf.d/20-vcac.cfg`	no-sslv3 no-tlsv10 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-sslv3 no-tlsv10 no-tlsv11`
`/etc/haproxy/conf.d/30-vro-config.cfg`	no-sslv3 no-tlsv10 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-sslv3 no-tlsv10 no-tlsv11`

2 Reinicie o serviço.

```
service haproxy restart
```

3 Abra o arquivo `/opt/vmware/etc/lighttpd/lighttpd.conf` e verifique se as entradas desativadas corretas aparecem.

Observação Não há uma diretiva para desativar o TLS 1.0 ou TLS 1.1 no Lighttpd. A restrição sobre o uso do TLS 1.0 e TLS 1.1 pode ser parcialmente atenuada ao forçar o OpenSSL a não usar conjuntos de cifras do TLS 1.0 e TLS 1.1.

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
```

4 Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados para o Proxy do Console no Appliance do vRealize Automation.

a Edite o arquivo `/etc/vcac/security.properties` adicionando ou modificando a seguinte linha:

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

b Reinicie o servidor executando o seguinte comando:

`service vcac-server restart`

5 Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados para o serviço vCO.

a Localize a tag <Connector> no arquivo /etc/vco/app-server/server.xml e adicione o seguinte atributo:

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

b Reinicie o serviço vCO executando o seguinte comando.

```
service vco-server restart
```

6 Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados para o serviço do vRealize Automation .

a Adicione os seguintes atributos à tag <Connector> no arquivo /etc/vcac/server.xml

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

b Reinicie o serviço vRealize Automation executando o seguinte comando:

```
service vcac-server restart
```

7 Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados para o RabbitMQ.

Abra o arquivo /etc/rabbitmq/rabbitmq.config e verifique se {versions, ['tlsv1.2', 'tlsv1.1']} está presente nas seções ssl e ssl_options.

```
[
  {ssl, [
      {versions, ['tlsv1.2', 'tlsv1.1']},
      {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', 'tlsv1.1']},
         {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 Reinicie o servidor RabbitMQ.

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

9 Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados para o serviço de vIDM.

Abra o arquivo `opt/vmware/horizon/workspace/conf/server.xml` para cada instância do conector contendo `SSLEnabled="true"` e certifique-se de que a linha a seguir esteja presente.

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

Desativar TLS 1.0

Desativar TLS 1.0 em componentes aplicáveis do vRealize Automation.

Não há uma diretiva para desativar o TLS 1.0 no Lighttpd. A restrição sobre o uso do TLS 1.0 pode ser parcialmente removida obrigando o OpenSSL a não usar conjuntos de cifras do TLS 1.0, conforme descrito na etapa 2 abaixo.

Procedimentos

1 Desative o TLS 1.0 no manipulador https do HAProxy no appliance do vRealize Automation.

a Acrescente `no-tlsv10` no fim da seguinte entrada no arquivo `/etc/haproxy/conf.d/20-vcac.cfg`.

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers TLSv1+HIGH:!aNULL:!eNULL:!3DES:!RC4:!CAMELLIA:!DH:!kECDHE:@STRENGTH no-sslv3 no-tlsv10
```

b Acrescente no-tlsv10 no fim da seguinte entrada no arquivo `/etc/haproxy/conf.d/30-vro-config.cfg`.

```
bind :8283 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers TLSv1+HIGH:!aNULL:!eNULL:!3DES:!RC4:!CAMELLIA:!DH:!kECDHE:@STRENGTH no-sslv3 no-tls10
```

Observação Para reativar o TLS 1.0, remova `no-tlsv10` da diretiva vinculativa.

2 Verifique no Lighttpd se o OpenSSL não usa os conjuntos de cifras do TLS 1.0.

a Edite a linha `ssl.cipher-list` no arquivo `/opt/vmware/etc/lighttpd/lighttpd.conf` conforme mostrado a seguir.

```
ssl.cipher-list = "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256"
```

b Reinicie o lighttpd usando o comando a seguir:

```
service vami-lighttp restart
```

3 Desative o TLS 1.0 para o Proxy do Console no appliance do vRealize Automation.

a Adicione ou modifique a seguinte linha no arquivo `/etc/vcac/security.properties`.

```
consoleproxy.ssl.server.protocols = TLSv1.2, TLSv1.1
```

b Reinicie o servidor executando o seguinte comando:

```
service vcac-server restart
```

Observação Para reativar o TLS 1.0, adicione TLSv1 da seguinte maneira e reinicie o serviço vcac-server:

```
consoleproxy.ssl.server.protocols = TLSv1.2,TLSv1.1, TLSv1
```

4 Desative o TLS 1.0 para o serviço vCO.

a Localize a tag `<Connector>` no arquivo `/etc/vco/app-server/server.xml` e adicione o seguinte atributo a ela:

```
sslEnabledProtocols = "TLSv1.1,TLSv1.2"
```

b Reinicie o serviço vCO executando o seguinte comando:

```
service vco-server restart
```

5 Desative o TLS 1.0 para o serviço vRealize Automation.

a Localize a tag `<Connector>` no arquivo `/etc/vcac/server.xml` e adicione o seguinte atributo a ela:

```
sslEnabledProtocols = "TLSv1.1,TLSv1.2"
```

b Reinicie o serviço vRealize Automation executando os seguintes comandos.

```
service vcac-server restart
```

Observação Para reativar o TLS 1.0, adicione TLSv1 a sslEnabledProtocols. Por exemplo, `sslEnabledProtocols = "TLSv1.1,TLSv1.2,TLSv1"`

6 Desative o TLS 1.0 para RabbitMQ.

a Abra o arquivo `/etc/rabbitmq/rabbitmq.config` e verifique se tlsv1.2 e tlsv 1.1 estão adicionados às seções ssl e ssl_options conforme mostrado no exemplo a seguir.

```
[
   {ssl, [
      {versions, ['tlsv1.2', 'tlsv1.1']},
      {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', 'tlsv1.1']},
         {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}]}
].
```

b Reinicie o servidor do RabbitMQ executando o seguinte comando:

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

Configurando pacotes de codificação de TLS para componentes do vRealize Automation

Para obter segurança máxima, você deve configurar componentes do vRealize Automation para usar codificação forte.

A codificação de criptografia negociada entre o servidor e o navegador determina a força de criptografia que é usada em uma sessão TLS.

Para garantir que apenas codificações fortes sejam selecionadas, desative as codificações fracas nos componentes do vRealize Automation. Configure o servidor para permitir somente codificações fortes e usar tamanhos de chave suficientemente grandes. Além disso, configure todas as codificações em uma ordem adequada.

Desative pacotes de codificação que não ofereçam autenticação, como pacotes de codificação NULL, aNULL ou eNULL. Além disso, desative a troca de chaves Diffie-Hellman anônima (ADH), a codificação de nível de exportação (EXP, codificação contendo DES), os tamanhos de chave menores de 128 bits para criptografar tráfego de carga, o uso do MD5 como mecanismo de hashing para tráfego de carga, os pacotes de codificação IDEA e os pacotes de codificação RC4. Certifique-se também de que os pacotes de codificação que usam a troca de chaves Diffie-Hellman (DHE) estejam desativados.

Desativar cifras fracas no HA Proxy

Compare as cifras do serviço de HA Proxy do appliance do vRealize Automation com a lista de cifras aceitáveis e desative todas aquelas consideradas fracas.

Desative pacotes de codificação que não ofereçam autenticação, como pacotes de codificação NULL, aNULL ou eNULL. Além disso, desative a troca de chaves Diffie-Hellman anônima (ADH), a codificação de nível de exportação (EXP, codificação contendo DES), os tamanhos de chave menores de 128 bits para criptografar tráfego de carga, o uso do MD5 como mecanismo de hashing para tráfego de carga, os pacotes de codificação IDEA e os pacotes de codificação RC4.

Procedimentos

1 Consulte a entrada de cifras no arquivo `/etc/haproxy/conf.d/20-vcac.cfg` da diretiva vinculante e desative todas as que são consideradas fracas.

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers TLSv1+HIGH:!aNULL:!
eNULL:!3DES:!RC4:!CAMELLIA:!DH:!kECDHE:@STRENGTH no-sslv3 no-tlsv10
```

2 Consulte a entrada de cifras no arquivo `/etc/haproxy/conf.d/30-vro-config.cfg` da diretiva vinculante e desative todas as que são consideradas fracas.

```
bind :8283 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers TLSv1+HIGH:!
aNULL:!eNULL:!3DES:!RC4:!CAMELLIA:!DH:!kECDHE:@STRENGTH no-sslv3 no-tls10
```

Desativar as cifras fracas no serviço de proxy do console do appliance do Appliance do vRealize AutomationvRealize Automation

Compare as cifras do serviço de proxy do console do appliance do vRealize Automation com a lista de cifras aceitáveis e desative todas aquelas consideradas fracas.

Desative pacotes de codificação que não ofereçam autenticação, como pacotes de codificação NULL, aNULL ou eNULL. Além disso, desative a troca de chaves Diffie-Hellman anônima (ADH), a codificação de nível de exportação (EXP, codificação contendo DES), os tamanhos de chave menores de 128 bits para criptografar tráfego de carga, o uso do MD5 como mecanismo de hashing para tráfego de carga, os pacotes de codificação IDEA e os pacotes de codificação RC4.

Procedimentos

1 Abra o arquivo `/etc/vcac/security.properties` em um editor de texto.

2 Adicione uma linha ao arquivo para desativar os conjuntos de cifras indesejados.

Use uma variação da seguinte linha:

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

Por exemplo, para desativar os conjuntos de codificações AES 128 e AES 256, adicione a seguinte linha:

```
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 Reinicie o servidor usando o comando a seguir.

```
service vcac-server restart
```

Desativar cifras fracas no serviço vCO do Appliance do vRealize Automation

Compare as cifras do serviço vCO do Appliance do vRealize Automation com a lista de cifras aceitáveis e desative todas aquelas consideradas fracas.

Desative pacotes de codificação que não ofereçam autenticação, como pacotes de codificação NULL, aNULL ou eNULL. Além disso, desative a troca de chaves Diffie-Hellman anônima (ADH), a codificação de nível de exportação (EXP, codificação contendo DES), os tamanhos de chave menores de 128 bits para criptografar tráfego de carga, o uso do MD5 como mecanismo de hashing para tráfego de carga, os pacotes de codificação IDEA e os pacotes de codificação RC4.

Procedimentos

1 Localize a tag `<Connector>` no arquivo `/etc/vco/app-server/server.xml`.

2 Edite ou adicione o atributo de cifra para usar os conjuntos de cifras desejados.

Consulte o exemplo a seguir:

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_EC
DSA_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”
```

Desativar cifras fracas no serviço RabbitMQ do Appliance do vRealize Automation

Compare as cifras do serviço RabbitMQ do Appliance do vRealize Automation com a lista de cifras aceitáveis e desative todas aquelas consideradas fracas.

Desative pacotes de codificação que não ofereçam autenticação, como pacotes de codificação NULL, aNULL ou eNULL. Além disso, desative a troca de chaves Diffie-Hellman anônima (ADH), a codificação de nível de exportação (EXP, codificação contendo DES), os tamanhos de chave menores de 128 bits para criptografar tráfego de carga, o uso do MD5 como mecanismo de hashing para tráfego de carga, os pacotes de codificação IDEA e os pacotes de codificação RC4.

Procedimentos

1 Avalie os conjuntos de cifras compatíveis. executando o comando `# /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites().'`.

As cifras retornadas no exemplo a seguir representam somente as cifras compatíveis. O servidor do RabbitMQ não usa ou anuncia estas cifras exceto se configurado para tal no arquivo `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 Selecione as cifras compatíveis que atendem aos requisitos de segurança da sua organização.

Por exemplo, para permitir somente `ECDHE-ECDSA-AES128-GCM-SHA256 & ECDHE-ECDSA-AES256-GCM-SHA384`, abra o arquivo `/etc/rabbitmq/rabbitmq.config` e adicione a seguinte linha a ssl e ssl_options.

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

3 Reinicie o servidor do RabbitMQ usando o seguinte comando.

`service rabbitmq-server restart`

Verificar a segurança de dados em repouso

Verificar a segurança dos usuários do banco de dados e contas usadas com o vRealize Automation.

Usuário postgres

A conta de usuário Linux postgres está vinculada à função de conta de superusuário do banco de dados postgres e, por padrão, é uma conta bloqueada. Esta é a configuração mais segura para este usuário, pois só é acessível a partir da conta do usuário raiz. Não desbloqueie esta conta de usuário.

Funções de conta do usuário do banco de dados

As funções padrão de conta do usuário postgres não devem ser utilizadas além da funcionalidade da aplicação. Para compatibilidade com atividades não padrão de revisão ou relatórios do banco de dados, uma conta adicional deve ser criada e a senha protegida adequadamente.

Execute o seguinte script na linha de comando:

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

Isso vai adicionar um novo usuário e uma senha fornecida pelo usuário.

Observação Esse script deve ser executado contra um banco de dados postgres mestre nos casos onde a configuração de postgres mestre-escravo HA está configurada.

Configurar autenticação do cliente PostgreSQL

Certifique-se de que a autenticação de confiança local não esteja configurada no banco de dados PostgreSQL do appliance do vRealize Automation. Essa configuração permite que qualquer usuário local, incluindo o superusuário do banco de dados, conecte-se como qualquer usuário do PostgreSQL sem uma senha.

Observação A conta de superusuário do Postgres deve permanecer como confiança local.

O método de autenticação md5 é recomendado porque ele envia senhas criptografadas.

As configurações de autenticação do cliente estão localizadas no arquivo `/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
```

Caso você edite o arquivo `pg_hba.conf`, deverá reiniciar o servidor do Postgres executando os seguintes comandos antes que as alterações possam ser efetivadas.

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

Configurar recursos de aplicação do vRealize Automation

Revisar recursos de aplicação do vRealize Automation e restringir permissões de arquivo.

Procedimentos

1 Execute o seguinte comando para verificar se os arquivos com conjunto de bits SUID e GUID estão bem-definidos.

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

A seguinte lista deverá aparecer.

```
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 Execute o seguinte comando para verificar se todos os arquivos no appliance virtual têm um proprietário.

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

3 Reveja as permissões para todos os arquivos ao appliance virtual para verificar se nenhum deles é gravável globalmente executando o comando a seguir.

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

4 Execute o seguinte comando para verificar se somente o usuário vcac tem posse dos arquivos corretos.

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

Se nenhum resultado aparecer, isso significa que todos os arquivos corretos são de posse apenas do usuário vcac.

5 Verifique se os arquivos a seguir são graváveis somente pelo usuário 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`

Além disso, verifique os arquivos a seguir e seus subdiretórios

`/var/log/vcac/*`

`/var/lib/vcac/*`

`/var/cache/vcac/*`

6 Verifique se somente o usuário vcac ou raiz pode ler os arquivos corretos nos diretórios a seguir e seus subdiretórios.

`/etc/vcac/*`

`/var/log/vcac/*`

`/var/lib/vcac/*`

`/var/cache/vcac/*`

7 Verifique se os arquivos corretos são de posse somente do usuário vco ou raiz, conforme mostrado nos diretórios a seguir e seus subdiretórios.

   `/etc/vco/*`

   `/var/log/vco/*`

   `/var/lib/vco/*`

   `/var/cache/vco/*`

8 Verifique se os arquivos corretos são graváveis somente pelo usuário vco ou raiz, conforme mostrado nos diretórios a seguir e seus subdiretórios.

   `/etc/vco/*`

   `/var/log/vco/*`

   `/var/lib/vco/*`

   `/var/cache/vco/*`

9 Verifique se os arquivos corretos são legíveis somente pelo usuário vco ou raiz, conforme mostrado nos diretórios a seguir e seus subdiretórios.

   `/etc/vco/*`

   `/var/log/vco/*`

   `/var/lib/vco/*`

   `/var/cache/vco/*`

Personalizando a configuração do proxy do console

Você pode personalizar a configuração do console remoto para o vRealize Automation facilitar a solução de problemas e as práticas organizacionais.

Ao instalar, configurar ou manter o vRealize Automation, você pode alterar algumas configurações para ativar a solução de problemas e a depuração da sua instalação. Catalogue e faça auditoria de cada uma das alterações que você faz para garantir que os componentes aplicáveis estejam devidamente protegidos, de acordo com o uso necessário. Não continue a produção se você não tiver certeza de que as alterações de configuração estejam protegidas corretamente.

Personalizar a expiração do tíquete do VMware Remote Console

Você pode personalizar o período de validade para os tíquetes do console remoto usados no estabelecimento de conexões no VMware Remote Console.

Quando um usuário faz conexões no VMware Remote Console, o sistema cria e retorna uma credencial única que estabelece uma conexão específica a uma máquina virtual. Você pode definir a expiração do tíquete por um período de tempo especificado em minutos.

Procedimentos

1 Abra o arquivo `/etc/vcac/security.properties` em um editor de texto.

2 Adicione uma linha ao arquivo do formulário `consoleproxy.ticket.validitySec=30`.

   Nesta linha, o valor numérico especifica o número de minutos antes de o tíquete expirar.

3 Salve o arquivo e feche-o.

4 Reinicie o servidor vcac usando o comando `/etc/init.d/vcac-server restart`.

O valor de expiração do tíquete é redefinido para o período de tempo especificado em minutos.

Personalizar a porta do servidor proxy do console

Você pode personalizar a porta na qual o proxy do console do VMware Remote Console escuta as mensagens.

Procedimentos

1 Abra o arquivo `/etc/vcac/security.properties` em um editor de texto.

2 Adicione uma linha ao arquivo do formulário `consoleproxy.service.port=8445`.

   O valor numérico especifica o número da porta de serviço do proxy do console, neste caso 8445.

3 Salve o arquivo e feche-o.

4 Reinicie o servidor vcac usando o comando `/etc/init.d/vcac-server restart`.

A porta de serviço do proxy é alterada para o número de porta especificado.

Configurar o cabeçalho de resposta do X-XSS-Protection

Adicione o cabeçalho de resposta do X-XSS-Protection ao arquivo de configuração haproxy.

Procedimentos

1 Abra `/etc/haproxy/conf.d/20-vcac.cfg` para edição.

2 Adicione as seguintes linhas em uma seção front-end:

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

3 Recarregue a configuração do HAProxy usando o seguinte comando.

   `/etc/init.d/haproxy reload`

Configurar o cabeçalho de resposta do HTTP Strict Transport Security

Adicione o cabeçalho de resposta do HTTP Strict Transport (HSTS) à configuração do HAProxy.

Procedimentos

1 Abra `/etc/haproxy/conf.d/20-vcac.cfg` para edição.

2 Adicione as seguintes linhas em uma seção front-end:

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

3 Recarregue a configuração do HAProxy usando o seguinte comando.

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

Configurar o cabeçalho de resposta do X-Frame-Options

O cabeçalho de resposta do X-Frame-Options pode aparecer duas vezes em alguns casos.

O cabeçalho de resposta do X-Frame-Options pode aparecer duas vezes porque o serviço vIDM adiciona esse cabeçalho ao back-end, bem como ao HAProxy. Você pode impedir que ele apareça duas vezes com uma configuração apropriada.

Procedimentos

1 Abra `/etc/haproxy/conf.d/20-vcac.cfg` para edição.

2 Localize a seguinte linha na seção front-end:

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

3 Adicione as seguintes linhas antes da linha localizada na etapa anterior:

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

4 Recarregue a configuração do HAProxy usando o seguinte comando.

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

Configurar cabeçalhos de resposta do servidor

Como melhor prática de segurança, configure o sistema do vRealize Automation para limitar as informações disponíveis para invasores em potencial.

Até onde possível, minimize a quantidade de informações que o sistema compartilha sobre sua identidade e versão. Hackers e agentes maliciosos podem usar essas informações para criar ataques direcionados contra o seu servidor web ou versão.

Configurar o cabeçalho de resposta do servidor Lighttpd

Como uma prática recomendada, crie um cabeçalho de servidor em branco para o servidor lighttpd do appliance do vRealize Automation.

Procedimentos

1 Abra o arquivo `/opt/vmware/etc/lighttpd/lighttpd.conf` em um editor de texto.

2 Adicione `server.tag = " "` ao arquivo.

3 Salve suas alterações e feche o arquivo.

4 Reinicie o servidor lighttpd executando o comando `# /opt/vmware/etc/init.d/vami-lighttp restart`.

Configurar o cabeçalho de resposta do TCServer para o appliance do vRealize Automation

Como uma prática recomendada, crie um cabeçalho de servidor em branco personalizado para o cabeçalho de resposta do TCServer usado com o appliance do vRealize Automation para limitar a possibilidade de um invasor mal-intencionado obter informações valiosas.

Procedimentos

1 Abra o arquivo `/etc/vco/app-server/server.xml` em um editor de texto.

2 Em cada elemento do `<Connector>`, adicione `server=" ".`

Por exemplo: `<Connector protocol="HTTP/1.1" server="" ........ />`

3 Salve suas alterações e feche o arquivo.

4 Reinicie o servidor usando o comando a seguir.

```
service vco-server restart
```

Configurar o cabeçalho de resposta do servidor Internet Information Services

Como uma prática recomendada, crie um cabeçalho de servidor em branco personalizado para o servidor Internet Information Services (IIS) usado com o Identity Appliance para limitar a possibilidade de invasores maliciosos obterem informações valiosas.

Procedimentos

1 Abra o arquivo `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` em um editor de texto.

2 Procure por `RemoveServerHeader=0` e altere para `RemoveServerHeader=1.`

3 Salve suas alterações e feche o arquivo.

4 Reinicie o servidor executando o comando `iisreset`.

Próximo passo

Desative o cabeçalho IIS X-Powered By removendo cabeçalhos de resposta HTTP da lista no Console do Gerenciador do IIS.

1 Abra o console do Gerenciador do IIS.

2 Abra o cabeçalho de resposta HTTP e remova-o da lista.

3 Reinicie o servidor executando o comando `iisreset`.

Tempo limite de sessão do Appliance do vRealize Automation

Ajuste a configuração de tempo limite de sessão no Appliance do vRealize Automation de acordo com a política de segurança da sua empresa.

O tempo limite de sessão padrão do Appliance do vRealize Automation para inatividade do usuário é de 30 minutos. Para ajustar o valor do tempo limite de acordo com a política de segurança da sua organização, edite o arquivo `web.xml` na máquina de host do Appliance do vRealize Automation.

Procedimentos

1. Abra o arquivo `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` em um editor de texto.
2. Localize `session-config` e ajuste o valor session-timeout. Consulte o código de exemplo a seguir.

```
<!-- 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. Reinicie o servidor executando o comando a seguir.

```
service vcac-server restart
```

Gerenciar softwares não essenciais

Para minimizar os riscos de segurança, remova ou configure os softwares não essenciais nas máquinas de host do vRealize Automation.

Configure todos os softwares não removidos de acordo com as recomendações do fabricante e melhores práticas de segurança para minimizar o potencial de criar brechas de segurança.

Proteger o manipulador de armazenamento em massa USB

Proteja o manipulador de armazenamento em massa USB para evitar seu uso, como o manipulador de dispositivo USB com as máquinas de host do appliance virtual do VMware. Invasores em potencial podem explorar este manipulador para comprometer o seu sistema.

Procedimentos

1. Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
2. Certifique-se de que a linha `install usb-storage /bin/true` aparece no arquivo.
3. Salve o arquivo e feche-o.

Proteger o Manipulador do Protocolo de Bluetooth

Proteja o Manipulador do Protocolo de Bluetooth nas máquinas de host do appliance virtual para evitar que invasores em potencial o explorem.

Vincular o protocolo de Bluetooth à pilha da rede é desnecessário e pode aumentar a superfície de ataque do host.

Procedimentos

1. Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
2. Certifique-se de que a seguinte linha aparace no arquivo.

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

3. Salve o arquivo e feche-o.

Proteger o Protocolo de Transmissão de Controle de Fluxo

Evite que o Protocolo de Transmissão de Controle de Fluxo (SCTP) carregue no sistema por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Configure o sistema para impedir que o módulo do Protocolo de Transmissão de Controle de Fluxo (SCTP) carregue exceto se for absolutamente necessário. O SCTP é um protocolo de camada de transporte com padrão IETF não utilizado. Vincular este protocolo à pilha da rede aumenta a superfície de ataque do host. Processos locais não privilegiados podem fazer com que o kernel carregue dinamicamente um manipulador de protocolo abrindo um soquete usando o protocolo.

Procedimentos

1. Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
2. Certifique-se de que a seguinte linha aparace no arquivo.

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

3. Salve o arquivo e feche-o.

Proteger o Protocolo de Controle de Congestionamento de Datagramas

Como parte das atividades de reforço do sistema, evite que o Protocolo de Controle de Congestionamento de Datagramas (DCCP) carregue em suas máquinas de host do appliance virtual por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Evite carregar o módulo do Protocolo de Controle de Congestionamento de Datagramas (DCCP), exceto se for absolutamente necessário. O DCCP é um protocolo proposto para a camada de transporte, que não é usado. Vincular este protocolo à pilha da rede aumenta a superfície de ataque do host. Os processos locais não privilegiados podem fazer com que o kernel carregue dinamicamente um manipulador de protocolo usando o protocolo para abrir um soquete.

Procedimentos

1. Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
2. Certifique-se de que as linhas do DCCP aparacem no arquivo.

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

3. Salve o arquivo e feche-o.

Proteger ponte de rede

Evite que o módulo de ponte de rede carregue no sistema por padrão. Invasores em potencial podem explorá-lo para comprometer seu sistema.

Configure o sistema para evitar o carregamento da ponte de rede, exceto se for absolutamente necessária. Invasores em potencial podem explorá-la para contornar o particionamento e segurança da rede.

Procedimentos

1. Execute o seguinte comando em todas as máquinas de host do appliance virtual do VMware.

   ```
   # rmmod bridge
   ```

2. Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
3. Certifique-se de que a seguinte linha aparace no arquivo.

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

4. Salve o arquivo e feche-o.

Proteger Protocolo de Soquetes Confiáveis de Datagramas

Como parte das atividades de reforço do sistema, evite que o Protocolo de Soquetes Confiáveis de Datagramas (RDS) carregue em suas máquinas de host do appliance virtual por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Vincular o Protocolo de Soquetes Confiáveis de Datagramas (RDS) à pilha da rede aumenta a superfície de ataque do host. Os processos locais não privilegiados podem fazer com que o sistema carregue dinamicamente um manipulador de protocolo usando o protocolo para abrir um soquete.

Procedimentos

1. Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
2. Certifique-se de que a linha `install rds /bin/true` aparace no arquivo.
3. Salve o arquivo e feche-o.

Proteger protocolo de comunicações transparentes interprocessos

Como parte das atividades de reforço do sistema, evite que o Protocolo de Comunicações Transparentes Interprocessos (TIPC) carregue em suas máquinas de host do appliance virtual por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Vincular o Protocolo de Comunicações Transparentes Interprocessos (TIPC) à pilha da rede aumenta a superfície de ataque do host. Os processos locais não privilegiados podem fazer com que o kernel carregue dinamicamente um manipulador de protocolo usando o protocolo para abrir um soquete.

Procedimentos

1. Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.

2 Certifique-se de que a linha `install tipc /bin/true` aparace no arquivo.

3 Salve o arquivo e feche-o.

Proteger o Protocolo de Troca de Pacotes Inter-Rede

Evite que o Protocolo de Troca de Pacotes Inter-Rede (IPX) carregue no sistema por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Evite carregar o módulo do Protocolo de Troca de Pacotes Inter-Rede (IPX) exceto se for absolutamente necessário. O protocolo IPX é um protocolo obsoleto de camada de rede. Vincular este protocolo à pilha da rede aumenta a superfície de ataque do host. Os processos locais não privilegiados podem fazer com que o sistema carregue dinamicamente um manipulador de protocolo usando o protocolo para abrir um soquete.

Procedimentos

1 Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.

2 Certifique-se de que a seguinte linha aparace no arquivo.

```
install ipx /bin/true
```

3 Salve o arquivo e feche-o.

Proteger protocolo Appletalk

Evite que o Protocolo Appletalk carregue no sistema por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Evite carregar o módulo do Protocolo Appletalk exceto se for absolutamente necessário. Vincular este protocolo à pilha da rede aumenta a superfície de ataque do host. Os processos locais não privilegiados podem fazer com que o sistema carregue dinamicamente um manipulador de protocolo usando o protocolo para abrir um soquete.

Procedimentos

1 Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.

2 Certifique-se de que a seguinte linha aparace no arquivo.

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

3 Salve o arquivo e feche-o.

Proteger protocolo DECnet

Evite que o Protocolo DECnet carregue no sistema por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Evite carregar o módulo do Protocolo DECnet exceto se for absolutamente necessário. Vincular este protocolo à pilha da rede aumenta a superfície de ataque do host. Os processos locais não privilegiados podem fazer com que o sistema carregue dinamicamente um manipulador de protocolo usando o protocolo para abrir um soquete.

Procedimentos

1. Abra o arquivo `/etc/modprobe.conf.local` do Protocoo DECnet em um editor de texto.
2. Certifique-se de que a seguinte linha aparace no arquivo.

   ```
   install decnet /bin/true
   ```
3. Salve o arquivo e feche-o.

Proteger módulo de Firewire

Evite que o módulo de Firewire carregue no sistema por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Evite carregar o módulo do Firewire exceto se for absolutamente necessário.

Procedimentos

1. Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
2. Certifique-se de que a seguinte linha aparace no arquivo.

   ```
   install ieee1394 /bin/true
   ```
3. Salve o arquivo e feche-o.

Proteger o componente de Infraestrutura como Serviço

Ao reforçar o sistema, proteja o componente de Infraestrutura como Serviço (IaaS) do vRealize Automation e sua máquina de host para evitar que potenciais invasores os explorem.

Você deve ajustar as configurações de segurança do componente de Infraestrutura como Serviço (IaaS) do vRealize Automation e o host onde ele reside. Você deve ajustar ou verificar a configuração de outros componentes e aplicações relacionados. Em alguns casos, você pode verificar as configurações existentes; em outros, você deve alterar ou adicionar configurações para uma configuração adequada.

Desativar serviço de tempo do Windows

Como melhor prática de segurança, use servidores de tempo autorizados em vez de sincronização de tempo com o host em um ambiente de produção do vRealize Automation.

Em um ambiente de produção, desative a sincronização de tempo do host e use servidores de tempo autorizados como suporte a um monitoramento preciso das ações do usuário, e à identificação de possíveis ataques maliciosos e invasão através de auditoria e logs.

Configurando o TLS para dados da Infraestrutura como Serviço em trânsito

Certifique-se de que a implantação do seu vRealize Automation use protocolos TLS fortes para proteger canais de transmissão para componentes da Infraestrutura como Serviço.

Secure Sockets Layer (SSL) e o mais recentemente desenvolvido Transport Layer Security (TLS) são protocolos criptográficos que ajudam a garantir a segurança do sistema durante as comunicações de rede entre os diferentes componentes do sistema. Como o SSL é um padrão mais antigo, muitos de seus implementos não fornecem mais segurança adequada contra possíveis ataques. Foram identificadas vulnerabilidades graves com protocolos SSL anteriores, incluindo o SSLv2 e o SSLv3. Esses protocolos não são mais considerados seguros.

Dependendo das políticas de segurança da sua organização, você também poderá desativar o TLS 1.0.

Observação Ao finalizar o TLS no balanceador de carga, desative também protocolos fracos, como o SSLv2, o SSLv3 e o TLS 1.0, se necessário.

Desativar o SSLV3 no Internet Information Services

Como melhor prática de segurança, desative o SSLv3 no Internet Information Services (IIS) na máquina do servidor de host de Infraestrutura como Serviço (IaaS).

Procedimentos

1. Execute o editor de registro do Windows como administrador.
2. Navegue até `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\` na janela de registro.
3. Clique com o botão direito em **Protocolos** e selecione **Novo > Chave**
4. Insira **`SSL 3.0`**.
5. Na árvore de navegação, clique com o botão direito na chave recém-criada de **SSL 3.0**, e no menu pop-up selecione **Novo > Chave** e insira **`Client`**.
6. Na árvore de navegação, clique com o botão direito na chave recém-criada de **SSL 3.0**, e no menu pop-up selecione **Novo > Chave** e insira **`Server`**.
7. Na árvore de navegação, em SSL 3.0, clique com o botão direito em **Cliente**, e selecione **Novo > Valor DWORD (32-bit)** e insira **`DisabledByDefault`**.
8. Na árvore de navegação, em SSL 3.0, selecione **Cliente**, e no painel à direita, clique duas vezes em **DisabledByDefault** e insira **`1`**.
9. Na árvore de navegação, em SSL 3.0, clique com o botão direito em **Servidor**, e selecione **Novo > Valor DWORD (32-bit)** e insira **`Enabled`**.
10. Na árvore de navegação, em SSL 3.0, selecione **Servidor**, e no painel à direita, clique duas vezes no **DWORD** habilitado e insira **`0`**.
11. Reinicie o Windows Server.

Desativar o TLS 1.0 para IaaS

Para oferecer máxima segurança, configure o IaaS para utilizar pooling e desative o TLS 1.0.

Para obter mais informações, consulte o artigo da base de dados de conhecimento Microsoft em https://support.microsoft.com/en-us/kb/245030.

Procedimentos

1 Configure o IaaS para usar pooling em vez de soquetes web.

   a Atualize o arquivo de configuração dos Serviços de Gerenciador `C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config` adicionando os seguintes valores na seção <appSettings>

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

   b Reinicie o Serviço de Gerenciador (VMware vCloud Automation Center Service).

2 Verifique se o TLS 1.0 está desativado no servidor IaaS.

   a Execute o editor de registro como administrador.

   b Na janela de registro, navegue até `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\`

   c Clique com o botão direito em Protocolos, selecione **Novo > Chave** e insira **`TLS 1.0`**.

   d Na árvore de navegação, clique com o botão direito na chave recém-criada do TLS 1.0, e no menu pop-up selecione **Novo > Chave** e insira **`Client`**.

   e Na árvore de navegação, clique com o botão direito na chave recém-criada do TLS 1.0, e no menu pop-up selecione **Novo > Chave** e insira **`Server`**.

   f Na árvore de navegação, em TLS 1.0, clique com o botão direito em **Cliente**, clique em **Novo > Valor DWORD (32-bit)** e insira **`DisabledByDefault`**.

   g Na árvore de navegação, em TLS 1.0, selecione **Cliente**, e no painel à direita, clique duas vezes em **DisabledByDefault** DWORD e insira **`1`**.

   h Na árvore de navegação, em TLS 1.0, clique com o botão direito em **Servidor**, e selecione **Novo > Valor DWORD (32-bit)** e insira **`Enabled`**.

   i Na árvore de navegação, em TLS 1.0, selecione **Servidor**, e no painel à direita, clique duas vezes em **Enabled** DWORD e insira **`0`**.

   j Reinicie o Windows Server.

Configurando pacotes de codificação TLS

Para obter segurança máxima, você deve configurar componentes do vRealize Automation para usar codificação forte. A codificação de criptografia negociada entre o servidor e o navegador determina a força de criptografia que é usada em uma sessão TLS. Para garantir que apenas codificações fortes sejam selecionadas, desative as codificações fracas nos componentes do vRealize Automation. Configure o servidor para permitir somente codificações fortes e usar tamanhos de chave suficientemente grandes. Além disso, configure todas as codificações em uma ordem adequada.

Pacotes de codificação que não são aceitáveis

Desative pacotes de codificação que não ofereçam autenticação, como pacotes de codificação NULL, aNULL ou eNULL. Além disso, desative a troca de chaves Diffie-Hellman anônima (ADH), a codificação de nível de exportação (EXP, codificação contendo DES), os tamanhos de chave menores de 128 bits para criptografar tráfego de carga, o uso do MD5 como mecanismo de hashing para tráfego de carga, os pacotes de codificação IDEA e os pacotes de codificação RC4. Certifique-se também de que os pacotes de codificação que usam a troca de chaves Diffie-Hellman (DHE) estejam desativados.

Verificar segurança do servidor do host

Como melhor prática de segurança, verifique a configuração de segurança das máquinas do servidor do host da Infraestrutura como Serviço (IaaS).

A Microsoft oferece diversas ferramentas para ajudar você a verificar a segurança das máquinas do servidor do host. Entre em contato com o seu fornecedor Microsoft para obter orientação sobre o uso mais adequado dessas ferramentas.

Verificar a linha de base segura do servidor do host

Execute o Analisador de Segurança de Linha de Base Microsoft (MBSA) para confirmar rapidamente se o servidor possui as atualizações e hot fixes mais recentes. Você pode usar o MBSA para instalar patches de segurança ausentes da Microsoft e manter o servidor atualizado em relação às recomendações de segurança da Microsoft.

Baixe a versão mais recente da ferramenta do MBSA no site da Microsoft.

Verificar configuração de segurança do servidor do host

Use o kit de ferramentas do Assistente de Configuração de Segurança (SCW) e o Gerente de Conformidade de Segurança Microsoft (SCM) para verificar se o servidor do host está configurado de forma segura.

Execute o SCW a partir das ferramentas administrativas do servidor Windows. Essa ferramenta pode identificar as funções do servidor e os recursos instalados, incluindo rede, firewalls do Windows e configurações de registro. Compare o relatório com a orientação mais recente sobre reforço do SCM relevante para o seu servidor Windows. Com base nos resultados, é possível ajustar as configurações de segurança para cada recurso como serviços de rede, configurações de conta e firewalls do Windows, e aplicar as configurações ao seu servidor.

Encontre mais informações sobre a ferramenta do SCW no site do Microsoft TechNet.

Proteger recursos da aplicação

Como melhor prática de segurança, certifique-se de que todos os arquivos relevantes de Infraestrutura como Serviço tenha permissões adequadas.

Compare os arquivos de Infraestrutura como Serviço com a sua instalação de Infraestrutura como Serviço. Na maioria dos casos, subpastas e arquivos de cada pasta devem ter as mesmas configurações da pasta.

Diretório ou arquivo	Grupo ou usuários	Controle total	Modificar	Ler e executar	Ler	Escrever
VMware\vCAC\Agents \<agent_name> \logs	SISTEMA	X	X	X	X	X
	Administrador	X	X	X	X	X
	Administradores	X	X	X	X	X
VMware\vCAC\Agents\ <agent_name> \temp	SISTEMA	X	X	X	X	X
	Administrador	X	X	X	X	X
	Administradores	X	X	X	X	X
VMware\vCAC\Agents\	SISTEMA	X	X	X	X	X
	Administradores	X	X	X	X	X
	Usuários			X	X	
VMware\vCAC\Distributed Execution Manager\	SISTEMA	X	X	X	X	X
	Administradores	X	X	X	X	X
	Usuários			X	X	
VMware\vCAC\Distributed Execution Manager\DEM\Logs	SISTEMA	X	X	X	X	X
	Administrador	X	X	X	X	X
	Administradores	X	X	X	X	X
VMware\vCAC\Distributed Execution Manager\DEO\Logs	SISTEMA	X	X	X	X	X
	Administrador	X	X	X	X	X
	Administradores	X	X	X	X	X
VMware\vCAC\Management Agent\	SISTEMA	X	X	X	X	X
	Administradores	X	X	X	X	X
	Usuários			X	X	

Diretório ou arquivo	Grupo ou usuários	Controle total	Modificar	Ler e executar	Ler	Escrever
VMware\vCAC\Server\	SISTEMA	X	X	X	X	X
	Administradores	X	X	X	X	X
	Usuários			X	X	
VMware\vCAC\Web API	SISTEMA	X	X	X	X	X
	Administradores	X	X	X	X	X
	Usuários			X	X	

Proteger a máquina host de Infraestrutura como Serviço

Como uma prática recomendada de segurança, revise as configurações básicas na sua máquina host de Infraestrutura como Serviço (IaaS) para garantir que ela esteja em conformidade com as diretrizes de segurança.

Proteja várias contas, aplicativos, portas e serviços na máquina host de Infraestrutura como Serviço (IaaS).

Verificar configurações de conta de usuário do servidor

Verifique se existem configurações e contas de usuário local e de domínio desnecessárias. Restrinja qualquer conta de usuário que não esteja relacionada às funções do aplicativo com aquelas necessárias para administração, manutenção e solução de problemas. Restrinja o acesso remoto das contas de usuário do domínio ao mínimo necessário para manter o servidor. Controle rigorosamente e faça auditoria dessas contas.

Excluir aplicativos desnecessários

Exclua todos os aplicativos desnecessários dos servidores host. Aplicativos desnecessários aumentam o risco de exposição por causa de suas vulnerabilidades desconhecidas ou não corrigidas.

Desativar portas e serviços desnecessários

Examine o firewall do servidor host para obter a lista de portas abertas. Bloqueie todas as portas que não são necessárias para o componente IaaS ou para a operação crítica do sistema. Consulte o Configurar portas e protocolos. Faça auditoria dos serviços em execução no seu servidor host e desative os que não são necessários.

Configurando a segurança de rede do host

9

Para fornecer proteção máxima contra ameaças de segurança conhecidas, configure a interface de rede e as configurações de comunicação em todas as máquinas host do VMware.

Como parte de um plano de segurança abrangente, defina as configurações de segurança da interface de rede para os appliances virtuais da VMware e para os componentes da Infraestrutura como Serviço de acordo com as diretrizes de segurança estabelecidas.

Este capítulo inclui os seguintes tópicos:

Definindo as configurações de rede para appliances da VMware

Para garantir que as suas máquinas host do appliance virtual da VMware ofereçam suporte a apenas comunicações seguras e essenciais, revise e edite as configurações de comunicação de rede.

Examine a configuração do protocolo de rede IP das suas máquinas host da VMware e defina as configurações de rede de acordo com as diretrizes de segurança. Desative todos os protocolos de comunicação não essenciais.

Prevenir controle do usuário de interfaces de rede

Como melhor prática de segurança, permita que os usuários utilizem somente os privilégios do sistema que precisam para realizar seu trabalho nas máquinas de host do appliance do VMware.

Permitir contas de usuário com privilégios para manipular as interfaces de rede pode resultar em evasão dos mecanismos de segurança da rede ou negação de serviço. Restrinja a capacidade de alterar as configurações de interface da rede a usuários privilegiados.

Procedimentos

1 Execute o seguinte comando em cada máquina de host do appliance do VMware.

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

2 Certifique-se de que todas as interfaces estejam definidas para `NO`.

Definir tamanho da fila de backlog de TCP

Para oferecer certo nível de defesa contra ataques maliciosos, configure um tamanho de fila de backlog de TCP padrão nas máquinas de host do appliance do VMware.

Defina os tamanhos da fila de backlog de TCP conforme um tamanho padrão adequado para oferecer mitigação de ataques de negação de serviço de TCP. A configuração padrão recomendada é 1280.

Procedimentos

1. Execute o seguinte comando em cada máquina de host do appliance do VMware.

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

2. Abra o arquivo `/etc/sysctl.conf` em um editor de texto.
3. Defina o tamanho da fila de backlog de TCP padrão adicionando a seguinte entrada ao arquivo.

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

4. Salve suas alterações e feche o arquivo.

Negar ecos ICMPv4 para endereço de difusão

Como uma prática recomendada de segurança, verifique se as suas máquinas host do appliance da VMware ignoram solicitações de eco de endereço de difusão ICMP.

As respostas para ecos de Internet Control Message Protocol (ICMP) de difusão fornecem um vetor de ataque para ataques de amplificação e podem facilitar o mapeamento de rede por agentes maliciosos. Configurar as suas máquinas host do appliance para ignorar os ecos ICMPv4 fornece proteção contra esses ataques.

Procedimentos

1. Execute o comando `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` nas máquinas host do appliance virtual da VMware para confirmar se elas negam solicitações de eco de endereço de difusão IPv4.

   Se as máquinas host estiverem configuradas para negar redirecionamentos IPv4, este comando retornará um valor de 0 para `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`.

2. Para configurar uma máquina host do appliance virtual para negar solicitações de eco de endereços de difusão ICMPv4, abra o arquivo `/etc/sysctl.conf` nas máquinas host Windows em um editor de texto.
3. Localize a entrada que lê `net.ipv4.icmp_echo_ignore_broadcasts=0` . Se o valor para esta entrada não estiver definido como zero ou se a entrada não existir, adicione-a ou atualize a entrada existente em conformidade.
4. Salve as alterações e feche o arquivo.

Desativar IPv4 Proxy ARP

Verifique se o IPv4 Proxy ARP está desativado caso não seja necessário nas máquinas de host do appliance do VMware para impedir o compartilhamento não autorizado de informações.

O IPv4 Proxy ARP permite que um sistema envie respostas para solicitações de ARP em uma interface em nome de hosts conectados a outra interface. Desative se ele não for necessário para impedir o vazamento de informações de endereçamento enter os segmentos de rede anexos.

Procedimentos

1 Execute o comando `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp|egrep "default|all"` nas máquinas de host do appliance virtual do VMware para verificar se o IPv4 Proxy ARP está desativado.

   Se o IPv6 Proxy ARP estiver desativado nas máquinas de host, esse comando retornará o valor 0.

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

   Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2 Caso você precise configurar o IPv6 Proxy ARP nas máquinas de host, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Verifique as seguintes entradas.

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

   Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

4 Salve todas alterações feitas e feche o arquivo.

Negar mensagens de redirecionamento IPv4 ICMP

Como prática recomendada de segurança, verifique se as suas máquinas host do appliance virtual da VMware negam mensagens de redirecionamento IPv4 ICMP.

Os roteadores usam mensagens de redirecionamento ICMP para informar aos hosts que existe uma rota mais direta para um destino. Uma mensagem de redirecionamento ICMP maliciosa pode facilitar um ataque a intermediários. Essas mensagens modificam a tabela de rotas do host e não são autenticadas. Certifique-se de que o sistema esteja configurado para ignorá-las se não forem necessárias.

Procedimentos

1. Execute o comando `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep "default|all"` nas máquinas host do appliance da VMware para confirmar se elas negam as mensagens de redirecionamento IPv4.

   Se as máquinas host estiverem configuradas para negar redirecionamentos IPv4, este comando retornará o seguinte:

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

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

2. Se você precisa configurar uma máquina host do appliance virtual para negar as mensagens de redirecionamento ICMPv4, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3. Verifique os valores das linhas que começam com `net.ipv4.conf`.

   Se os valores para as entradas a seguir não forem definidos como zero ou se as entradas não existirem, adicione-as ao arquivo ou atualize as entradas existentes corretamente.

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

4. Salve as alterações feitas e feche o arquivo.

Negar mensagens de ICMP Redirect para IPv6

Como melhor prática de segurança, verifique se as máquinas de host do appliance virtual do VMware negam as mensagens de ICMP Redirect para IPv6.

Os roteadores usam mensagens de redirecionamento ICMP para informar aos hosts que existe uma rota mais direta para um destino. Uma mensagem de redirecionamento ICMP maliciosa pode facilitar um ataque a intermediários. Essas mensagens modificam a tabela de rotas do host e não são autenticadas. Certifique-se de que seu sistema esteja configurado para ignorá-las caso não sejam necessárias.

Procedimentos

1. Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects|egrep "default|all"` nas máquinas de host do appliance virtual do VMware para confirmar se eles negam mensagens Redirect para IPv6.

   Se as máquinas de host estiverem configuradas para negar Redirect de IPv6, esse comando retornará o seguinte:

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

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

2. Para configurar uma máquina de host do appliance virtual para negar mensagens Redirect para IPv4, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Verifique os valores das linhas que começam com `net.ipv6.conf`.

   Se os valores das seguintes entradas não estiverem definidos como zero, ou se as entradas não existirem, adicione-as ao arquivo ou atualize as entradas existentes conforme necessário.

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

4 Salve as alterações e feche o arquivo.

Log dos pacotes Martian de IPv4

Como melhor prática de segurança, verifique se as máquinas de host do appliance virtual do VMware fazem o log dos pacotes Martian de IPv4.

Os pacotes Martian contêm endereços que o sistema reconhece como inválidos. Configure as máquinas de host para fazer o log dessas mensagens de modo que você possa identificar falhas de configuração ou ataques em andamento.

Procedimentos

1 Execute o comando `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians|egrep "default|all"` nas máquinas de host do appliance do VMware para verificar se eles fazem o log de pacotes Martian de IPv4.

   Se as máquinas virtuais estiverem configuradas para fazer o log de pacotes Martian, elas retornarão o seguinte:

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

   Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2 Caso precise configurar um appliance virtual para fazer o log de pacotes Martian de IPv4, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Confira os valores das linhas iniciadas por `net.ipv4.conf`.

   Se o valor das seguintes entradas não estiverem definidos como 1, ou se as entradas não existirem, adicione-as ao arquivo ou atualize as entradas existentes conforme necessário.

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

4 Salve suas alterações e feche o arquivo.

Usar filtragem por caminho inverso IPv4

Como prática recomendada de segurança, verifique se as suas máquinas host do appliance virtual da VMware usam filtragem por caminho inverso IPv4.

A filtragem por caminho inverso protege contra endereços de origem falsos, fazendo com que o sistema descarte pacotes com endereços de origem que não têm rota ou com uma rota que não aponta para a interface de origem. Configure suas máquinas host para usar filtragem por caminho inverso sempre que possível. Em alguns casos, dependendo da função do sistema, a filtragem por caminho inverso pode fazer com que o sistema descarte o tráfego legítimo. Se você encontrar esses problemas, poderá precisar usar um modo mais permissivo ou desativar a filtragem por caminho inverso.

Procedimentos

1 Execute o comando `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"` nas máquinas host do appliance virtual da VMware para verificar se elas usam filtragem por caminho inverso IPv4.

   Se as máquinas virtuais usarem filtragem por caminho inverso IPv4, este comando retornará o seguinte:

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

   Se suas máquinas virtuais estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2 Se você precisar configurar a filtragem por caminho inverso IPv4 nas máquinas host, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Verifique os valores das linhas que começam com `net.ipv4.conf`.

   Se os valores para as entradas a seguir não forem definidos como 1 ou se eles não existirem, adicione-os ao arquivo ou atualize as entradas existentes em conformidade.

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

4 Salve as alterações e feche o arquivo.

Negar o encaminhamento IPv4

Verifique se as suas máquinas host do appliance da VMware negam o encaminhamento IPv4.

Se o sistema estiver configurado para encaminhamento IP e não for um roteador designado, os invasores poderão usá-lo para ignorar a segurança da rede, fornecendo um caminho para comunicação não filtrada por dispositivos de rede. Configure suas máquinas host do appliance virtual para negar o encaminhamento IPv4 para evitar esse risco.

Procedimentos

1. Execute o comando `# cat /proc/sys/net/ipv4/ip_forward` nas máquinas host do appliance da VMware para confirmar se elas negam o encaminhamento IPv4.

   Se as máquinas host estiverem configuradas para negar o encaminhamento IPv4, esse comando retornará um valor de 0 para `/proc/sys/net/ipv4/ip_forward`. Se as máquinas virtuais estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2. Para configurar uma máquina host do appliance virtual para negar o encaminhamento ICMPv4, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3. Localize a entrada que lê `net.ipv4.ip_forward=0`. Se o valor para esta entrada não estiver definido no momento como zero ou se a entrada não existir, adicione-a ou atualize a entrada existente em conformidade.

4. Salve todas as alterações e feche o arquivo.

Negar o encaminhamento IPv6

Como uma prática recomendada de segurança, verifique se os seus sistemas host do appliance da VMware negam o encaminhamento IPv6.

Se o sistema estiver configurado para encaminhamento IP e não for um roteador designado, os invasores poderão usá-lo para ignorar a segurança da rede, fornecendo um caminho para comunicação não filtrada por dispositivos de rede. Configure suas máquinas host do appliance virtual para negar o encaminhamento IPv6 para evitar esse risco.

Procedimentos

1. Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding|egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam o encaminhamento IPv6.

   Se as máquinas host estiverem configuradas para negar o encaminhamento IPv6, esse comando retornará o seguinte:

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

   Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2. Se você precisar configurar uma máquina host para negar o encaminhamento IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Verifique os valores das linhas que começam com `net.ipv6.conf`.

Se os valores para as entradas a seguir não estiverem definidos como zero ou se as entradas não existirem, adicione-as ou atualize as entradas existentes corretamente.

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

4 Salve todas alterações feitas e feche o arquivo.

Usar Syncookies IPv4 TCP

Verifique se suas máquinas de host do appliance do VMware usam Syncookies IPv4 TCP.

Um ataque de TCP SYN Flood pode causar uma negação de serviço ao preencher a tabela de conexão TCP do sistema com conexões no estado SYN_RCVD. Os Syncookies impedem o rastreamento de uma conexão até o recebimento de um ACK subsequente, verificando que o iniciador está tentando uma conexão válida e não é uma fonte de flood. Esta técnica não opera de forma totalmente em conformidade com os padrões, mas só é ativada durante uma condição de flood, e possibilita a defesa do sistema sem interromper o atendimento a solicitações válidas.

Procedimentos

1 Execute o comando `# cat /proc/sys/net/ipv4/tcp_syncookies` nas máquinas de host do appliance do VMware para verificar se eles usam Syncookies IPv4 TCP.

Se as máquinas de host estiverem configuradas para negar encaminhamento IPv4, esse comando retornará o valor 1 para `/proc/sys/net/ipv4/tcp_syncookies`. Se as máquinas virtuais estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2 Caso precise configurar um appliance virtual para utilizar os Syncookies IPv4 TCP, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Localize a entrada que lê `net.ipv4.tcp_syncookies=1`.

Se o valor desta entrada não estiver definido como 1 ou se a entrada não existir, adicione a entrada ou atualize a entrada existente conforme necessário.

4 Salve todas alterações feitas e feche o arquivo.

Negar anúncios do roteador IPv6

Verifique se as máquinas host da VMware negam a aceitação de anúncios do roteador e redirecionamentos ICMP, a menos que sejam necessários para a operação do sistema.

O IPv6 permite que os sistemas configurem seus dispositivos de rede automaticamente usando informações da rede. Do ponto de vista de segurança, a configuração manual de informações de configuração importantes é preferível para aceitá-la da rede de maneira não autenticada.

Procedimentos

1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra|egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam os anúncios do roteador.

   Se as máquinas host estiverem configuradas para negar os anúncios do roteador IPv6, esse comando retornará valores de 0:

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

   Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2 Se você precisar configurar uma máquina host para negar anúncios do roteador IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Verifique as seguintes entradas.

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

   Se essas entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

4 Salve todas alterações feitas e feche o arquivo.

Negar solicitações de roteador IPv6

Como uma prática recomendada de segurança, verifique se as suas máquinas host do appliance da VMware negam solicitações de roteador IPv6, a menos que sejam necessárias para operação do sistema.

A configuração de solicitações de roteador determina quantas solicitações de roteador são enviadas ao criar a interface. Se os endereços forem atribuídos estaticamente, não haverá necessidade de enviar solicitações.

Procedimentos

1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations|egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam as solicitações do roteador IPv6.

   Se as máquinas host estiverem configuradas para negar anúncios do roteador IPv6, esse comando retornará o seguinte:

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

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2 Se você precisar configurar máquinas host para negar solicitações de roteador IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Verifique as seguintes entradas.

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

Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

4 Salve todas as alterações e feche o arquivo.

Negar a preferência de roteador IPv6 em solicitações de roteador

Verifique se as suas máquinas host do appliance da VMware negam solicitações de roteador IPv6, a menos que sejam necessárias para operação do sistema.

A preferência de roteador na configuração de solicitações determina as preferências de roteador. Se os endereços forem atribuídos estaticamente, não haverá necessidade de receber qualquer preferência de roteador para solicitações.

Procedimentos

1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref|egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam as solicitações do roteador IPv6.

Se as máquinas host estiverem configuradas para negar anúncios do roteador IPv6, esse comando retornará o seguinte:

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

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2 Se você precisar configurar máquinas host para negar solicitações de roteador IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Verifique as seguintes entradas.

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

Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

4 Salve todas alterações feitas e feche o arquivo.

Negar o prefixo do roteador IPv6

Verifique se as suas máquinas host do appliance da VMware negam informações de prefixo do roteador IPv6, a menos que sejam necessárias para operação do sistema.

A configuração `accept_ra_pinfo` controla se o sistema aceita informações de prefixo do roteador. Se os endereços forem atribuídos estaticamente, não haverá necessidade de receber qualquer informação de prefixo do roteador.

Procedimentos

1. Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo|egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam as informações de prefixo do roteador IPv6.

   Se as máquinas host estiverem configuradas para negar anúncios do roteador IPv6, esse comando retornará o seguinte.

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

   Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2. Se você precisar configurar máquinas host para negar informações de prefixo do roteador IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3. Verifique as seguintes entradas.

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

   Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

4. Salve todas as alterações e feche o arquivo.

Negar configurações de limite de saltos do anúncio do roteador IPv6

Verifique se as suas máquinas host do appliance da VMware negam configurações de limite de saltos do roteador IPv6, a menos que sejam necessárias.

A configuração `accept_ra_defrtr` controla se o sistema aceitará as configurações de Limite de salto de um anúncio do roteador. Configurá-la como zero evita que um roteador altere seu limite de saltos IPv6 padrão para pacotes de saída.

Procedimentos

1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr|egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam as configurações de limite de saltos do roteador IPv6.

   Se as máquinas host estiverem configuradas para negar as configurações de limite de saltos do roteador IPv6, este comando retornará valores de 0.

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

   Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2 Se você precisar configurar uma máquina host para negar configurações de limite de saltos do roteador IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Verifique as seguintes entradas.

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

   Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

4 Salve todas alterações feitas e feche o arquivo.

Negar configurações do autoconf de anúncio do roteador IPv6

Verifique se as suas máquinas host do appliance da VMware negam configurações do autoconf do roteador IPv6, a menos que sejam necessárias.

A configuração `autoconf` controla se os anúncios do roteador podem fazer com que o sistema atribua um endereço de unicast global a uma interface.

Procedimentos

1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf|egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam as configurações do auconf do roteador IPv6.

   Se as máquinas host estiverem configuradas para negar as configurações de autoconf do roteador IPv6, esse comando retornará valores de 0.

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

   Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2 Se você precisar configurar máquinas host para negar configurações do autoconf do roteador IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Verifique as seguintes entradas.

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

Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

4 Salve todas alterações feitas e feche o arquivo.

Negar solicitações de vizinhança IPv6

Verifique se as suas máquinas host do appliance da VMware negam solicitações de vizinhança IPv6, a menos que sejam necessárias.

A configuração `dad_transmits` determina quantas solicitações de vizinhança são enviadas por endereço (global e link-local) ao criar uma interface para garantir que o endereço desejado seja exclusivo na rede.

Procedimentos

1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits|egrep "default|all"` nas máquinas host do appliance da VMware para confirmar se elas negam as solicitações de vizinhança IPv6.

Se as máquinas host estiverem configuradas para negar as solicitações de vizinhança IPv6, esse comando retornará valores de 0.

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

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2 Se você precisar configurar máquinas host para negar solicitações de vizinhança IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Verifique as seguintes entradas.

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

Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

4 Salve todas alterações feitas e feche o arquivo.

Restringir número máximo de endereços IPv6

Verifique se as máquinas de host do appliance do VMware restringem o número máximo de endereços IPv6 conforme o mínimo necessário para a operação do sistema.

A configuração de número máximo de endereços determina quantos endereços IPv6 unicast globais estão disponíveis para cada interface. O padrão é 16, mas você deve definir o número exato de endereços globais estaticamente configurados exigidos pelo seu sistema.

Procedimentos

1 Execute o comando `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses|egrep "default|all"` nas máquinas de host do appliance do VMware para verificar se eles restringem o número máximo de endereços IPv6 corretamente.

   Se as máquinas de host estiverem configuradas para restringir o número máximo de endereços IPv6, esse comando retornará o valor 1.

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

   Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

2 Caso você precise configurar o número máximo de endereços IPv6 nas máquinas de host, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Verifique as seguintes entradas.

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

   Se as entradas não existirem ou se os seus valores não estiverem definidos como 1, adicione as entradas ou atualize as entradas existentes conforme necessário.

4 Salve todas alterações feitas e feche o arquivo.

Definindo as configurações de rede para o host da Infraestrutura como Serviço

Como prática recomendada de segurança, defina as configurações de comunicação de rede na sua máquina host do componente de Infraestrutura como Serviço (IaaS) da VMware de acordo com os requisitos e diretrizes da VMware.

Defina a configuração de rede da máquina host de Infraestrutura como um Serviço (IaaS) para oferecer suporte a funções completas do vRealize Automation com a segurança apropriada.

Consulte Proteger o componente de Infraestrutura como Serviço.

Configurar portas e protocolos

Como melhor prática de segurança, configure portas e protocolos para todos os appliances e componentes do vRealize Automation de acordo com as diretrizes da VMware.

Configure as portas de entrada e saída para os componentes do vRealize Automation conforme exigido para os componentes críticos do sistema operarem em produção. Desative todas as portas e protocolos desnecessários. Consulte a *Arquitetura de Referência do vRealize Automation*.

Portas de usuário necessárias

Como melhor prática de segurança, configure as portas de usuário do vRealize Automation conforme as diretrizes da VMware.

Exponha as portas necessárias apenas por meio de uma rede segura.

SERVIDOR	PORTAS
Appliance do vRealize Automation	443, 8443

Portas necessárias do administrador

Como uma prática recomendada de segurança, configure as portas do administrador do vRealize Automation de acordo com as diretrizes da VMware.

Exponha as portas necessárias apenas por meio de uma rede segura.

SERVIDOR	PORTAS
Servidor do vRealize Application Services	5480

Portas do appliance do vRealize Automation

Como melhor prática de segurança, configure as portas de entrada e saída para o Appliance do vRealize Automation de acordo com as diretrizes da VMware.

Portas de entrada

Configure o número mínimo de portas de entrada necessárias para o Appliance do vRealize Automation. Configure portas opcionais se necessário para a configuração do seu sistema.

Tabela 9-1. Número mínimo de portas de entrada necessárias

PORTA	PROTOCOLO	COMENTÁRIOS
443	TCP	Acesso ao console do vRealize Automation e às chamadas de API.
8443	TCP	Proxy do console (VMRC).
5480	TCP	Acesso ao console de gerenciamento Web do appliance virtual
5488, 5489	TCP	Interna. Usado pelo Appliance do vRealize Automation para atualizações.

Tabela 9-1. Número mínimo de portas de entrada necessárias (Continuação)

PORTA	PROTOCOLO	COMENTÁRIOS
5672	TCP	Mensagens do RabbitMQ. **Observação** Ao clusterizar instâncias do Appliance do vRealize Automation, pode ser necessário configurar as portas abertas 4369 e 25672.
40002	TCP	Necessária para o serviço vIDM. Isto é colocado no firewall para todo tráfego externo, exceto o tráfego de outros nós do Appliance do vRealize Automation quando adicionados em configuração de HA.

Se necessário, configure as portas de entrada opcionais.

Tabela 9-2. Portas de entrada opcionais

PORTA	PROTOCOLO	COMENTÁRIOS
22	TCP	SSH (opcional) Em um ambiente de produção, desative a escuta do serviço de SSH na porta 22, e feche a porta 22.
80	TCP	Redireciona para 443 (opcional).

Portas de saída

Configure as portas de saída necessárias.

Tabela 9-3. Número mínimo de portas de saída necessárias

PORTA	PROTOCOLO	COMENTÁRIOS
25,587	TCP, UDP	SMTP para o envio de e-mails de notificação de saída.
53	TCP, UDP	DNS.
67, 68, 546, 547	TCP, UDP	DHCP.
110, 995	TCP, UDP	POP para receber e-mails de notificação de entrada.
143, 993	TCP, UDP	IMAP para receber e-mails de notificação de entrada.
443	TCP	Manager Service de Infraestrutura como Serviço sobre HTTPS.

Se necessário, configure as portas de saída opcionais.

Tabela 9-4. Portas de saída opcionais

PORTA	PROTOCOLO	COMENTÁRIOS
80	TCP	Para obter as atualizações de software (opcional). Você pode baixar e aplicar atualizações separadamente.
123	TCP, UDP	Para conexão direta com o NTP em vez de usar o tempo do host (Opcional).

Portas de Infraestrutura como Serviço

Como melhor prática de segurança, configure as portas de entrada e saída para os componentes de Infraestrutura como Serviço (IaaS) em conformidade com as diretrizes da VMware.

Portas de entrada

Configure o número mínimo de portas de entrada necessárias para os componentes de IaaS.

Tabela 9-5. Número mínimo de portas de entrada necessárias

COMPONENTE	PORTA	PROTOCOLO	COMENTÁRIOS
Manager Service	443	TCP	Comunicação com os componentes de IaaS e do appliance do vRealize Automation sobre HTTPS. Todos os hosts de virtualização gerenciados por agentes de proxy também devem ter a porta TCP 443 aberta para o tráfego de entrada

Portas de saída

Configure o número mínimo de portas de saída necessárias para os componentes de IaaS.

Tabela 9-6. Número mínimo de portas de saída necessárias

COMPONENTE	PORTA	PROTOCOLO	COMENTÁRIOS
Tudo	53	TCP, UDP	DNS.
Tudo		TCP, UDP	DHCP.
Manager Service	443	TCP	Comunicação com o appliance do vRealize Automation sobre HTTPS.
Site	443	TCP	Comunicação com o Manager Service sobre HTTPS.
Distributed Execution Managers	443	TCP	Comunicação com o Manager Service sobre HTTPS.
Agentes de proxy	443	TCP	Comunicação com o Manager Service e os hosts de virtualização sobre HTTPS.
Agente guest	443	TCP	Comunicação com o Manager Service sobre HTTPS.
Manager Service, Site	1433	TCP	MSSQL.

Se necessário, configure as portas de saída opcionais.

Tabela 9-7. Portas de saída opcionais

COMPONENTE	PORTA	PROTOCOLO	COMENTÁRIOS
Tudo	123	TCP, UDP	O NTP é opcional.

Auditoria e registro

10

Como uma prática recomendada de segurança, configure a auditoria e o registro no seu sistema do vRealize Automation de acordo com as recomendações da VMware.

O registro remoto em um host de registro central fornece um armazenamento seguro para arquivos de registro. Ao reunir arquivos de registro em um host central, você pode monitorar o ambiente com uma única ferramenta. Além disso, você pode executar a análise agregada e procurar provas de ameaças, como ataques coordenados em várias entidades dentro da infraestrutura. Fazer o registro em um servidor de registro seguro e centralizado pode ajudar a evitar a violação do registro e também fornece um registro de auditoria de longo prazo.

Garantir que o servidor de registro remoto é seguro

Muitas vezes, depois que os invasores violam a segurança da sua máquina host, eles tentam procurar e manipular arquivos de registro para apagar seus rastros e manter controle sem serem descobertos. Proteger adequadamente o servidor de registro remoto ajuda a desencorajar a adulteração do registro.

Usar um servidor NTP autorizado

Certifique-se de que todas as máquinas host usem a mesma fonte de tempo relativa, incluindo o deslocamento de localização relevante, e de que você possa correlacionar a fonte de tempo relativa com um padrão de tempo acordado, como o Tempo Universal Coordenado (UTC). Uma abordagem disciplinada das fontes de tempo permite que você rastreie e correlacione rapidamente as ações de um intruso ao revisar os arquivos de registro relevantes. Configurações de hora incorretas podem dificultar a inspeção e a correlação de arquivos de registro para detectar ataques e podem tornar a auditoria imprecisa.

Use pelo menos três servidores NTP de fontes de tempo externas ou configure alguns servidores NTP locais em uma rede confiável que, por sua vez, obtenha seu tempo de pelo menos três fontes de tempo externas.