安全配置

2018 年 10 月 11 日

vRealize Operations Manager 7.0

vmware®

您可以从 VMware 网站下载最新的技术文档：
https://docs.vmware.com/cn/。
VMware 网站还提供了最近的产品更新。
如果您对本文档有任何意见或建议，请将反馈信息发送至：
docfeedback@vmware.com

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

北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

目录

安全配置

安全配置的文档旨在充当 vRealize Operations Manager 的部署的安全基准。当您使用系统监控工具时，请参阅此文档，以确保持续监控安全基准配置出现的任何意外更改并对配置进行维护。

可以手动执行默认情况下尚未设置的强化活动。

目标受众

此信息面向 vRealize Operations Manager 的管理员。

vRealize Operations Manager 安全状态

1

vRealize Operations Manager 的安全状态基于系统和网络配置、组织安全策略和最佳实践假设了一个完全安全的环境。请务必根据您组织的安全策略和最佳实践执行强化活动。

文档分为以下各节：

- 安全部署
- 安全配置
- 网络安全
- 通信

该指南详细说明了虚拟应用程序的安装。

为确保您的系统得到安全强化，请根据您组织的安全策略和面临的风险检查和评估这些建议。

vRealize Operations Manager 安全部署

2

您必须在安装产品前验证安装媒体的完整性，以确保下载的文件的真实性。

本章讨论了以下主题：

验证安装媒体的完整性

在您下载媒体后，请使用 MD5/SHA1 和值验证下载的完整性。始终在下载 ISO、离线包或修补程序后验证 SHA1 散列值，以确保下载的文件的完整性和真实性。如果您从 VMware 获取物理介质且安全封条断开，请将软件退还给 VMware 进行更换。

步骤

- 将 MD5/SHA1 散列值输出结果与 VMware 网站上发布的值进行比较。

  SHA1 或 MD5 散列值应当匹配。

  注 vRealize Operations Manager `6.x-x.pak` 文件由 VMware 软件发布证书签署。vRealize Operations Manager 在安装前验证 PAK 文件签名。

强化已部署软件基础架构

作为强化过程的一部分，您必须对支持您的 VMware 系统的已部署软件基础架构进行强化。

在强化 VMware 系统之前，请检查并解决辅助软件基础架构的安全缺陷，以便创建完全强化的安全环境。需要考虑的软件基础架构要素包括操作系统组件、辅助软件以及数据库软件。根据制造商的建议以及其他相关安全协议解决这些组件以及其他组件中的安全问题。

强化 VMware vSphere 环境

vRealize Operations Manager 依靠安全的 VMware vSphere 环境实现诸多利益以及一个安全的基础架构。

评估 VMware vSphere 环境并验证是否强制实施并保持了适当级别的 vSphere 强化指导。

有关强化的更多指导，请参阅 http://www.vmware.com/security/hardening-guides.html。

检查已安装的和不受支持的软件

未使用的软件中的漏洞可能会增加未授权的系统访问和可用性中断的风险。检查 VMware 主机上安装的软件并评估其用途。

请勿在任何 vRealize Operations Manager 节点主机上安装系统的安全运行不需要的软件。卸载未使用的或不必要的软件。

在 vRealize Operations Manager 等基础架构产品上安装不受支持的、未经测试或未获批准的软件会对基础架构造成威胁。

要最大程度减少对基础架构造成的威胁，请勿在 VMWare 提供的主机上安装或使用不受 VMware 支持的任何第三方软件。

评估您的 vRealize Operations Manager 部署和已安装的产品清单，以确认没有安装任何不受支持的软件。

有关第三方产品支持策略的详细信息，请参阅 http://www.vmware.com/security/hardening-guides.html 处的 VMware 支持。

验证第三方软件

请勿使用 VMware 不支持的第三方软件。确认已根据第三方供应商的指导安全配置并修补所有第三方软件。

VMware 主机上安装的第三方软件所存在的不真实、不安全或 未修补的漏洞可能使系统面临未经授权的访问和可用性受损的风险。并非由 VMware 提供的所有软件必须获得适当的保护和修补。

如果您必须使用 VMware 不支持的第三方软件，请咨询第三方供应商以了解安全配置和修补要求。

VMware 安全通告和修补程序

VMware 有时会发布产品的安全通告。了解这些通告可确保您拥有最安全的基础产品，并确保产品不容易受到已知威胁攻击。

评估 vRealize Operations Manager 的安装、修补和升级历史记录，确认遵循并实施了已发布的 VMware 安全通告。

我们建议您始终维持最新的 vRealize Operations Manager 版本，因为此版本还将包含最新的安全修补程序。

有关最新的 VMware 安全通告的更多信息，请参阅 http://www.vmware.com/security/advisories/。

vRealize Operations Manager 的安全配置

3

作为最佳安全做法，您必须保护 vRealize Operations Manager 控制台并管理安全 Shell (SSH)、管理账户和控制台访问。确保使用安全传输通道部署您的系统。

您还必须遵循适用于运行 End Point Operations Management 代理的某些最佳安全做法。

本章讨论了以下主题：

保护 vRealize Operations Manager 控制台

安装 vRealize Operations Manager 后，您必须首次登录并保护群集中每个节点的控制台。

前提条件

安装 vRealize Operations Manager。

步骤

1 在 vCenter 中查找节点控制台或直接访问。

在 vCenter 中，按下 Alt+F1 访问登录提示。出于安全原因，默认情况下会禁用 vRealize Operations Manager 远程终端会话。

2 以 root 身份登录。

vRealize Operations Manager 不允许您访问命令提示符，直到您创建 root 密码为止。

3 在提示密码时，按 **Enter** 键。

4 在提示旧密码时，按 **Enter** 键。

5 当提示输入新密码时，输入所需的 root 密码，并记下它以供日后参考。

6 重新输入 root 密码。

7 从控制台注销。

更改 Root 密码

您可以通过使用控制台随时更改任何 vRealize Operations Manager 主节点或数据节点的 root 密码。

root 用户可绕过 `pam_cracklib` 模块密码复杂性检查（位于 `etc/pam.d/common-password` 中）。所有强化设备均为 `pw_history` 模块启用 `enforce_for_root`，该模块位于 `etc/pam.d/common-password` 文件中。系统会默认记住最后五个密码。每个用户的旧密码存储在 `/etc/security/opasswd` 文件中。

前提条件

确认设备的 root 密码符合您组织的公司密码复杂性要求。如果帐户密码开头为 `$6$`，它使用了 sha512 哈希。这是所有强化设备的标准哈希。

步骤

1 在设备的 root shell 中运行 `# passwd` 命令。

2 要验证 root 密码的哈希，以 root 身份登录并运行 `# more /etc/shadow` 命令。

将显示哈希信息。

3 如果 root 密码不包含 sha512 哈希，则运行 `passwd` 命令以对其进行更改。

管理密码到期日期

根据您组织的安全策略，配置所有帐户密码的到期日期。

默认情况下，所有强化 VMware 设备使用 60 天的密码到期日期。在大多数强化设备中，root 帐户设置为 365 天的密码到期日期。作为最佳实践，请确认所有帐户的到期日期符合安全和操作要求标准。

如果 root 密码到期，您不能将其恢复。您必须实施特定于站点的策略以防止管理密码和 root 密码到期。

步骤

1 以 root 身份登录到虚拟设备计算机，并运行 `# more /etc/shadow` 命令以验证所有帐户的密码到期日期。

2 要修改 root 帐户的到期日期，请运行 `# passwd –x 365 root` 命令。

在此命令中，365 指定了密码到期日期之前的天数。使用同一命令修改任意用户，用特定帐户替换 `root` 账户，并更换天数以满足组织的到期日期标准。

默认情况下，root 密码设置的有效期为 365 天。

管理安全 Shell、管理帐户和控制台访问

对于远程连接，所有强化设备包含安全 Shell (SSH) 协议。强化设备上默认禁用 SSH。

SSH 的交互式命令行环境，支持对 vRealize Operations Manager 节点进行远程连接。SSH 需要具有高权限的用户帐户凭据。SSH 活动通常会绕过 vRealize Operations Manager 节点的基于角色的访问控制（role-based access control，RBAC）和审核控制。

作为最佳实践，请在生产环境中禁用 SSH，仅在诊断或排除您无法通过其他方式解决的问题时才启用此协议。仅在需要将此功能用于特定用途时才将其启用，并且此行为须符合您组织的安全策略。如果您启用 SSH，请确保为其抵御攻击，并且仅在需要时才启用它。根据您的 vSphere 配置，您可以在部署开放虚拟化格式（Open Virtualization Format，OVF）模板时启用或禁用 SSH。

作为确定计算机上是否启用了 SSH 的简单测试，请尝试使用 SSH 打开一个连接。如果连接打开并请求凭据，则 SSH 已启用，且可用于进行连接。

安全 Shell Root 用户

由于 VMware 设备不包括预先配置的默认用户帐户，默认情况下，root 帐户可以使用 SSH 直接登录。尽可能以 root 身份禁用 SSH。

为了满足适用于不可否认性的法律合规标准，所有强化设备上的 SSH 服务器均预先配置了 AllowGroups wheel 条目以将 SSH 访问限制给次级组 wheel。为了实现职责分离，您可以修改 `/etc/ssh/sshd_config` 文件中的 AllowGroups wheel 条目以使用其他组，比如 sshd。

`pam_wheel` 模块的 wheel 组已启用了超级用户访问权限，因此 wheel 的成员可以使用 su-root 命令，其中，需要提供 root 密码。组分离允许用户使用 SSH 访问设备，但不能使用 su 命令以 root 身份登录。请勿删除或修改 AllowGroups 字段中的其他条目，该字段可以确保设备功能正确运行。实施更改后，通过运行 `# service sshd restart` 命令重新启动 SSH 守护程序。

在 vRealize Operations Manager 节点上启用或禁用安全 Shell

您可以在 vRealize Operations Manager 节点上启用安全 Shell (Secure Shell, SSH) 进行故障排除。例如，要对某服务器进行故障排除，您可能需要该服务器通过 SSH 的控制台访问权限。在 vRealize Operations Manager 节点上禁用 SSH 以进行正常操作。

步骤

1 从 vCenter 访问 vRealize Operations Manager 节点的控制台。

2 按 Alt + F1 访问登录提示，然后登录。

3 运行 `#chkconfig` 命令。

4 如果 sshd 服务关闭，请运行 `#chkconfig sshd on` 命令。

5 运行 `#service sshd start` 命令启动 sshd 服务。

6 运行 `#service sshd stop` 命令停止 sshd 服务。

您还可以从管理界面的 **SSH 状态**列 vRealize Operations Manager 启用或禁用安全 Shell。

为安全 Shell 创建本地管理帐户

在移除 root SSH 访问权限之前，必须创建本地管理帐户，这些帐户可以用作安全 Shell (Secure Shell, SSH)，并且是辅助 wheel 组的成员。

在禁用直接 root 访问之前，请测试授权管理员可以使用 `AllowGroups` 来访问 SSH，并且他们可以使用 wheel 组和 `su` 命令以 root 身份登录。

步骤

1 以 root 身份登录并运行以下命令。

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

其中 wheel 是 `AllowGroups` 中指定进行 SSH 访问的组。要添加多个辅助组，请使用 `–G wheel,sshd`。

2 切换到该用户并提供新密码以确保密码复杂性检查。

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

如果满足密码复杂性要求，该密码会更新。如果不满足密码复杂性要求，该密码恢复为原始密码，必须重新运行密码命令。

在您创建登录帐户以允许使用 wheel 访问权限进行 SSH 远程访问并使用 `su` 命令以 root 身份登录之后，您可以将 root 帐户从 SSH 直接登录中移除。

3 要移除 SSH 直接登录，请修改 `/etc/ssh/sshd_config` 文件，方法是将 `(#)PermitRootLogin yes` 替换为 `PermitRootLogin no`。

后续步骤

禁止以 root 身份直接登录。默认情况下，强化设备通过控制台直接登录到 root。在您创建管理帐户以获得不可否认性并测试它们能够进行 wheel 访问 (`su–root`) 之后，请禁用直接 root 登录，方法是以 root 身份编辑 `/etc/securetty` 文件，然后将 `tty1` 条目替换为 `console`。

限制安全 Shell 访问

作为系统强化过程的一部分，请在所有 VMware 虚拟设备主机上适当地配置 tcp_wrappers 程序包，从而限制安全 Shell (SSH) 访问。另外，请在这些设备上维护必要的 SSH 密钥文件权限。

所有 VMware 虚拟设备均包含 tcp_wrappers 程序包，以便允许 TCP 支持的守护程序控制可以访问 libwrapped 守护程序的网络子网。默认情况下，`/etc/hosts.allow` 文件包含一个通用条目，`sshd: ALL : ALLOW`，其允许对安全 Shell 的所有访问。针对您的组织适当地限制此访问。

步骤

1 在文本编辑器中打开虚拟设备主机上的 `/etc/hosts.allow` 文件。

2 更改您的生产环境中的通用条目，使其只包括本地主机条目和管理网络子网，以便实现安全的操作。

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

在本示例中，允许所有本地主机连接以及客户端在 10.0.0.0 子网上创建的连接。

3 添加所有适当的主机标识，例如主机名称、IP 地址、完全限定域名 (FQDN) 和回送。

4 保存并关闭该文件。

维护安全 Shell 密钥文件权限

要维护适当水平的安全性，请配置安全 Shell (SSH) 密钥文件权限。

步骤

1 查看公共主机密钥文件，这些文件位于 `/etc/ssh/*key.pub` 中。

2 确认这些文件都由 root 所拥有，组由 root 所拥有，并且文件将权限设置为 0644。

权限是 (-rw-r--r--)。

3 关闭所有文件。

4 查看私人主机密钥文件，这些文件位于 `/etc/ssh/*key` 中。

5 确认 root 拥有这些文件和组，以及文件将权限设置为 0600。

权限是 (-rw-------)。

6 关闭所有文件。

强化安全 Shell 服务器配置

在可能的情况下，虚拟应用程序安装 (Virtual Application Installation, OVF) 具有默认强化配置。用户可以通过检查配置文件的全局选项部分的服务器和客户端服务，验证其配置是否经过适当的强化。

如果可能，请在 `/etc/hosts.allow` 文件中仅限 SSH 服务器用于管理子网。

步骤

1 打开 `/etc/ssh/sshd_config` 服务器配置文件，验证设置是否正确。

设置	状态
服务器守护程序协议	Protocol 2
密码	Ciphers aes256-ctr,aes128-ctr
TCP 转发	AllowTCPForwarding no
服务器网关端口	Gateway Ports no
X11 转发	X11Forwarding no
SSH 服务	使用 AllowGroups 字段指定一个组，该组有权访问辅助组以及向其中添加成员，辅助组的成员是有权使用该服务的用户。
GSSAPI 身份验证	GSSAPIAuthentication no（如果未使用）
Kerberos 身份验证	KerberosAuthentication no（如果未使用）
本地变量（AcceptEnv 全局选项）	设置为 `disabled by commenting out` 或 `enabled for only LC_* or LANG variables`
隧道配置	PermitTunnel no
网络会话	MaxSessions 1
严格模式检查	Strict Modes yes
权限分离	UsePrivilegeSeparation yes
rhosts RSA 身份验证	RhostsRSAAuthentication no
压缩	Compression delayed 或 Compression no
消息身份验证代码	MACs hmac-sha1
用户访问限制	PermitUserEnvironment no

2 保存更改并关闭文件。

强化安全 Shell 客户端配置

作为系统强化监控过程的一部分，请确认 SSH 客户端的强化，方法是检查虚拟设备主机上的 SSH 客户端配置文件，以确保该客户端是根据 VMware 准则进行配置的。

步骤

1 打开 SSH 客户端配置文件 `/etc/ssh/ssh_config`，并验证全局选项部分的设置是否正确。

设置	状态
客户端协议	Protocol 2
客户端网关端口	Gateway Ports no
GSSAPI 身份验证	GSSAPIAuthentication no
本地变量（SendEnv 全局选项）	仅提供 LC_* 或 LANG 变量

设置	状态
CBC 密码	Ciphers aes256-ctr,aes128-ctr
消息身份验证代码	仅用于 `MACs hmac-sha1` 条目

2 保存更改并关闭文件。

禁止以 root 身份直接登录

默认情况下，强化设备允许您使用控制台以 root 身份直接登录。作为安全最佳做法，在您创建管理帐户以获得不可否认性并测试它能够使用 `su-root` 命令进行 wheel 访问之后，请禁用直接登录。

前提条件

- 完成称为 为安全 Shell 创建本地管理帐户 的主题中的步骤。
- 验证您在禁用直接 root 登录之前是否已测试过以管理员身份访问系统。

步骤

1 以 root 身份登录并导航到 `/etc/securetty` 文件。

您可以从命令提示符访问此文件。

2 将 `tty1` 条目替换为 `console`。

禁用管理员用户帐户的 SSH 访问

作为安全最佳做法，您可以禁用管理员用户帐户的 SSH 访问。vRealize Operations Manager 管理员帐户和 Linux 管理员帐户共享相同的密码。禁用管理员用户的 SSH 访问通过确保 SSH 的所有用户首先使用不同于 vRealize Operations Manager 管理员帐户的密码登录到较低特权服务帐户来强制实施纵深防御，然后将用户切换到较高特权（例如管理员或 root）。

步骤

1 编辑 `/etc/ssh/sshd_config` 文件。

您可以从命令提示符访问此文件。

2 将 `DenyUsers admin` 条目添加到文件中的任何位置并保存该文件。

3 要重新启动 sshd 服务器，请运行 `service sshd restart` 命令。

设置引导加载程序身份验证

为提供适当水平的安全性，请在您的 VMware 虚拟设备上配置引导加载程序身份验证。如果系统引导加载程序不需要身份验证，对系统具有控制台访问权限的用户也许能够更改系统引导配置或将系统引导至单用户或维护模式，这可能导致出现拒绝服务或未经授权的系统访问。

默认情况下，VMware 虚拟设备上未设置引导加载程序身份验证，因此，必须创建一个 GRUB 密码以对其进行配置。

步骤

1 确认是否存在引导密码，方法是在虚拟设备上的 `/boot/grub/menu.lst` 文件中查找 `password --md5 <password-hash>` 一行。

2 如果不存在任何密码，则在虚拟设备上运行 `# /usr/sbin/grub-md5-crypt` 命令。

将生成 MD5 密码，该命令可提供 MD5 散列值输出结果。

3 通过运行 `# password --md5 <hash from grub-md5-crypt>` 命令，将密码附加到 `menu.lst` 文件中。

单用户或维护模式身份验证

如果系统在引导到单用户或维护模式之前不需要有效的 root 身份验证，则调用单用户或维护模式的任何用户都将被授予特权以访问系统上的所有文件。

步骤

- 检查 `/etc/inittab` 文件，并确保存在以下两行：`ls:S:wait:/etc/init.d/rc S` 和 `~~:S:respawn:/sbin/sulogin`。

监视最低限度的必要用户帐户

您必须监视现有用户帐户，并确保删除任何不必要的用户帐户。

步骤

- 运行 *host*`:~ # cat /etc/passwd` 命令并验证最低限度的必要用户帐户：

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

监视最低限度的必要组

您必须监视现有组和成员，以确保删除所有不必要的组或组访问权限。

步骤

- 运行 `<host>:~ # cat /etc/group` 命令以验证最低限度的必要组和组成员身份。

```
audio:x:17:
bin:x:1:daemon
cdrom:x:20:
console:x:21:
daemon:x:2:
dialout:x:16:u1,tcserver,postgres
disk:x:6:
floppy:x:19:
haldaemon:!:102:
kmem:x:9:
mail:x:12:
man:x:62:
messagebus:!:101:
modem:x:43:
nobody:x:65533:
nogroup:x:65534:nobody
ntp:!:106:
polkituser:!:105:
public:x:32:
root:x:0:admin
shadow:x:15:
sshd:!:65:
suse-ncc:!:107:
sys:x:3:
tape:!:103:
trusted:x:42:
tty:x:5:
utmp:x:22:
uuidd:!:104:
video:x:33:u1,tcserver,postgres
wheel:x:10:root,admin
www:x:8:
xok:x:41:
maildrop:!:1001:
postfix:!:51:
users:x:100:
vami:!:1002:root
nginx:!:108:
admin:!:1003:
```

重置 vRealize Operations Manager 管理员密码 (Linux)

作为最佳安全做法，您可以在 Linux 群集上重置用于 vApp 或 Linux 安装的 vRealize Operations Manager 密码。

步骤

1 以 root 身份登录到主节点的远程控制台。

2 输入 `$VMWARE_PYTHON_BIN $VCOPS_BASE/../vmware-vcopssuite/utilities/sliceConfiguration/bin/vcopsSetAdminPassword.py --reset` 命令，然后按提示操作。

在 VMware 设备上配置 NTP

对于关键时间来源查找，请禁用主机时间同步并在 VMware 设备上使用网络时间协议 (Network Time Protocol, NTP)。您必须配置一个可信的远程 NTP 服务器以实现时间同步。NTP 服务器必须是权威时间服务器或者至少与权威时间服务器同步。

VMware 虚拟设备上的 NTP 守护程序提供同步时间服务。NTP 在默认情况下禁用，因此您需要手动进行配置。如有可能，请在生产环境中使用 NTP，以便通过准确的审核和日志保管来跟踪用户操作并检测潜在恶意攻击和入侵。有关 NTP 安全声明的信息，请参见 NTP 网站。

NTP 配置文件位于每台设备上的 `/etc/ntp.conf` 文件中。

步骤

1 导航到虚拟设备主机上的 `/etc/ntp.conf` 配置文件。

2 将文件所有者设置为 **`root:root`**。

3 将权限设置为 **`0640`**。

4 为降低对 NTP 服务的拒绝服务放大攻击风险，请打开 `/etc/ntp.conf` 文件并确保限制行出现在该文件中。

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

5 保存任何更改并关闭文件。

有关 NTP 安全声明的信息，请参阅 http://support.ntp.org/bin/view/Main/SecurityNotice。

在 Linux 上禁用 TCP 时间戳响应

使用 TCP 时间戳响应可以粗略估计远程主机的正常运行时间并有助于进一步的攻击。此外，可以根据某些操作系统的 TCP 时间戳对这些操作系统进行指纹采集。

步骤

- 在 Linux 上禁用 TCP 时间戳响应。
  a 要将 `net.ipv4.tcp_timestamps` 的值设置为 `0`，请运行 `sysctl -w net.ipv4.tcp_timestamps=0` 命令。
  b 在默认 `sysctl.conf` 文件中添加 `ipv4.tcp_timestamps=0` 值。

启用 FIPS 140-2 模式

vRealize Operations Manager 6.3 及更高版本附带的 OpenSSL 版本已通过 FIPS 140-2 认证。但是，默认情况下不启用 FIPS 模式。

如果存在安全合规性要求以在启用 FIPS 模式的情况下使用通过 FIPS 认证的加密算法，您可以启用 FIPS 模式。

步骤

1 要替换 `mod_ssl.so` 文件，请运行以下命令：

```
cd /usr/lib64/apache2-prefork/
cp mod_ssl.so mod_ssl.so.old
cp mod_ssl.so.FIPSON.openssl1.0.2 mod_ssl.so
```

2 通过编辑 `/etc/apache2/ssl-global.conf` 文件来修改 Apache2 配置。

3 搜索 `<IfModule mod_ssl.c>` 行并在其下添加 `SSLFIPS on` 指令。

4 要重置 Apache 配置，请运行 `service apache2 restart` 命令。

传输中的数据的 TLS

作为最佳安全做法，确保使用安全传输通道部署系统。

为 vRealize Operations Manager 配置强协议

SSLv2 和 SSLv3 等协议不再被视为是安全的。此外，建议您禁用 TLS 1.0。仅启用 TLS 1.1 和 TLS 1.2。

验证 Apache HTTPD 中协议的正确使用

vRealize Operations Manager 在默认情况下禁用 SSLv2 和 SSLv3。在将系统投入生产之前，您必须先禁用所有负载平衡器上的弱协议。

步骤

1 从命令提示符运行 `grep SSLProtocol /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf | grep -v '#'` 命令，以验证 SSLv2 和 SSLv3 是否被禁用。

如果协议被禁用，该命令将返回以下输出：`SSLProtocol All -SSLv2 -SSLv3`

2 要同时禁用 TLS 1.0 协议，请从命令提示符运行 `sed -i "/^[^#]*SSLProtocol/ c\SSLProtocol All -SSLv2 -SSLv3 -TLSv1" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` 命令。

3 要重新启动 Apache2 服务器，请从命令提示符运行 `/etc/init.d/apache2 restart` 命令。

验证 GemFire TLS 处理程序中协议的正确使用

vRealize Operations Manager 默认情况下禁用 SSLv3。在将系统投入生产之前，您必须先禁用所有负载平衡器上的弱协议。

步骤

1 验证协议是否已启用。要验证协议是否已启用，请在每个节点上运行以下命令：

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

以下结果是预期的：

```
cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.native.properties | grep -v '#'
```

以下结果是预期的：

```
cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties | grep -v '#'
```

以下结果是预期的：

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

2 禁用 TLS 1.0。

a 导航至 `url/admin` 处的管理员用户界面。

b 单击**脱机**。

c 要禁用 SSLv3 和 TLS 1.0，请运行以下命令：

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

为每个节点重复此步骤

d 导航到管理员用户界面。

e 单击**联机**。

3 重新启用 TLS 1.0。

a 导航到管理员用户界面以使群集脱机：`url/admin`。

b 单击**脱机**。

c 要确保 SSLv3 和 TLS 1.0 被禁用，请运行以下命令：

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

为每个节点重复此步骤。

d 导航到管理员用户界面以使群集联机。

e 单击**联机**。

配置 vRealize Operations Manager 以使用强密码

为最大程度地保证安全，必须配置 vRealize Operations Manager 组件以使用强密码。为确保只选择强密码，请禁止使用弱密码。将服务器配置为仅支持强密码并使用足够大的密钥大小。此外，请按合适的顺序配置密码。

vRealize Operations Manager 在默认情况下禁用那些使用 DHE 密钥交换的密码套件。在将系统投入生产之前，请确保在所有负载平衡器上禁用同样的弱密码套件。

使用强密码

服务器与浏览器之间协商的加密密码确定 TLS 会话中使用的密钥交换方法和加密强度。

验证 Apache HTTPD 中密码套件的正确使用

为获得最大安全性，请验证 Apache httpd 中密码套件的正确使用。

步骤

1 要验证 Apache httpd 中密码套件的正确使用，请从命令提示符运行 `grep SSLCipherSuite /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf | grep -v '#'` 命令。

如果 Apache httpd 使用正确的密码套件，该命令将返回以下输出：`SSLCipherSuite kECDH +AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:!aNULL!ADH:!EXP:!MD5:! 3DES:!CAMELLIA:!PSK:!SRP:!DH`

2 要配置密码套件的正确使用，请从命令提示符运行 `sed –i "/^[^#]*SSLCipherSuite/ c\SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA +AES:\!aNULL\!ADH:\!EXP:\!MD5:\!3DES:\!CAMELLIA:\!PSK:\!SRP:\! DH" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` 命令。

如果步骤 1 中的输出不是预期内容，请运行此命令。

此命令将禁用使用 DH 和 DHE 密钥交换方法的所有密码套件。

3 从命令提示符运行 `/etc/init.d/apache2 restart` 命令，以重新启动 Apache2 服务器。

4 要重新启用 DH，请通过从命令提示符处运行 `sed –i "/^[^#]*SSLCipherSuite/ c\SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:\!aNULL\!ADH:\!EXP:\!MD5:\!3DES:\!CAMELLIA:\!PSK:\!SRP" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` 命令来从密码套件中删除 `!DH`。

5 从命令提示符运行 `/etc/init.d/apache2 restart` 命令，以重新启动 Apache2 服务器。

验证 GemFire TLS 处理程序中密码套件的正确使用

为获得最大安全性，请验证 GemFire TLS 处理程序中密码套件的正确使用。

步骤

1 要验证密码套件是否已启用，请在每个节点上运行以下命令来验证协议是否已启用：

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

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

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

2 配置正确的密码套件。

a 导航至 *URL*`/admin` 处的管理员用户界面。

b 要使群集脱机，请单击**脱机**。

c 要配置正确的密码套件，请运行以下命令：

```
sed –i "/^[^#]*cluster-ssl-ciphers/ c\cluster-ssl-ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware-vcops/user/conf/gemfire.properties

sed –i "/^[^#]*cluster-ssl-ciphers/ c\cluster-ssl-ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware-vcops/user/conf/gemfire.native.properties

sed –i "/^[^#]*cluster-ssl-ciphers/ c\cluster-ssl-ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties
```

为每个节点重复此步骤。

d 导航至 *URL*`/admin` 处的管理员用户界面。

e 单击**联机**。

在 Localhost 连接上启用 TLS

默认情况下，localhost 到 PostgreSQL 数据库的连接不使用 TLS。要启用 TLS，您必须使用 OpenSSL 生成自签名证书或提供自己的证书。

要在 localhost 到 PostgreSQL 连接上启用 TLS，请完成以下步骤：

1 使用 OpenSSL 生成或提供您自己的自签名证书

2 安装适用于 PostgreSQL 的证书

3 在 PostgreSQL 上启用 TLS

使用 OpenSSL 生成或提供您自己的自签名证书

Localhost 到 PostgreSQL 数据库的连接不使用 TLS。要启用 TLS，您可以使用 OpenSSL 生成自己的自签名证书，或者提供自己的证书。

- 要使用 OpenSSL 生成自签名证书，请运行以下命令：

```
openssl req -new -text -out cert.req
 openssl rsa -in privkey.pem -out cert.pem
 openssl req -x509 -in cert.req -text -key cert.pem -out cert.cert
```

- 要提供您自己的证书，请完成以下步骤：
  - 将 `CAcerts.crt` 文件的所有权修改为 `postgres`。
  - 编辑 `postgresql.conf` 文件以包含指令 `ssl_ca_file = 'CAcerts.crt`。

    如果您使用带 CA 链的证书，则必须将包含中间和根 CA 证书的 `CAcerts.crt` 文件添加到同一目录。

安装适用于 PostgreSQL 的证书

在 localhost 至 PostgreSQL 连接上启用 TLS 后，您必须安装适用于 PostgreSQL 的证书。

步骤

1 将 `cert.pem` 文件复制到 `/storage/db/vcops/vpostgres/data/server.key`。

2 将 `cert.cert` 文件复制到 `/storage/db/vcops/vpostgres/data/server.crt`。

3 运行 `chmod 600 /storage/db/vcops/vpostgres/data/server.key` 命令。

4 运行 `chmod 600 /storage/db/vcops/vpostgres/data/server.crt` 命令。

5 运行 `chown postgres /storage/db/vcops/vpostgres/data/server.key` 和 `chown postgres /storage/db/vcops/vpostgres/data/server.crt` 命令，以将 `server.crt` 和 `server.key` 文件的所有权从 `root` 更改为 `postgres`。

在 PostgreSQL 上启用 TLS

您必须编辑 `postgresql.conf` 文件，以在 localhost 至 PostgreSQL 连接上启用 TLS。

步骤

- 编辑 /storage/db/vcops/vpostgres/data/ 处的 postgresql.conf 文件，并做以下更改：
  a 设置 ssl = on。
  b 设置 ssl_cert_file = 'server.crt'。
  c 设置 ssl_key_file = 'server.key'。

必须要保护的应用程序资源

作为最佳安全做法，请确保保护应用程序资源。

按照以下步骤操作，确保保护应用程序资源。

步骤

1 运行 Find / -path /proc -prune -o -type f -perm +6000 -ls 命令以验证这些文件是否具有充分定义的 SUID 和 GUID 位集。

将显示以下列表：

```
354131   24 -rwsr-xr-x   1 polkituser root 23176 /usr/lib/PolicyKit/polkit-set-default-helper
354126   20 -rwxr-sr-x   1 root     polkituser    19208 /usr/lib/PolicyKit/polkit-grant-helper
354125   20 -rwxr-sr-x   1 root     polkituser    19008 /usr/lib/PolicyKit/polkit-explicit-grant-
helper
354130   24 -rwxr-sr-x   1 root     polkituser    23160 /usr/lib/PolicyKit/polkit-revoke-helper
354127   12 -rwsr-x---   1 root     polkituser    10744 /usr/lib/PolicyKit/polkit-grant-helper-pam
354128   16 -rwxr-sr-x   1 root     polkituser    14856 /usr/lib/PolicyKit/polkit-read-auth-helper
 73886   84 -rwsr-xr-x   1 root     shadow      77848 /usr/bin/chsh
 73888   88 -rwsr-xr-x   1 root     shadow      85952 /usr/bin/gpasswd
 73887   20 -rwsr-xr-x   1 root     shadow      19320 /usr/bin/expiry
 73890   84 -rwsr-xr-x   1 root     root        81856 /usr/bin/passwd
 73799  240 -rwsr-xr-x   1 root     root       238488 /usr/bin/sudo
 73889   20 -rwsr-xr-x   1 root     root        19416 /usr/bin/newgrp
 73884   92 -rwsr-xr-x   1 root     shadow      86200 /usr/bin/chage
 73885   88 -rwsr-xr-x   1 root     shadow      82472 /usr/bin/chfn
 73916   40 -rwsr-x---   1 root     trusted     40432 /usr/bin/crontab
296275   28 -rwsr-xr-x   1 root     root        26945 /usr/lib64/pt_chown
353804  816 -r-xr-sr-x   1 root     mail       829672 /usr/sbin/sendmail
278545   36 -rwsr-xr-x   1 root     root        35792 /bin/ping6
278585   40 -rwsr-xr-x   1 root     root        40016 /bin/su
278544   40 -rwsr-xr-x   1 root     root        40048 /bin/ping
278638   72 -rwsr-xr-x   1 root     root        69240 /bin/umount
278637  100 -rwsr-xr-x   1 root     root        94808 /bin/mount
475333   48 -rwsr-x---   1 root     messagebus    47912 /lib64/dbus-1/dbus-daemon-launch-helper
 41001   36 -rwsr-xr-x   1 root     shadow      35688 /sbin/unix_chkpwd
 41118   12 -rwsr-xr-x   1 root     shadow      10736 /sbin/unix2_chkpwd
```

2 运行 find / -path */proc -prune -o -nouser -o -nogroup 命令以确认 vApp 中的所有文件都具有所有者。

如果没有结果，则所有文件都具有所有者。

3 运行 `find / -name "*.*" -type f -perm -a+w | xargs ls -ldb` 命令，通过检查 vApp 上所有文件的权限，确认没有文件是所有人都可写入的文件。

没有文件必须包含权限 `xx2`。

4 运行 `find / -path */proc -prune -o ! -user root -o -user admin -print` 命令以确认文件由正确的用户所拥有。

如果没有结果，则所有文件均属于 `root` 或 `admin`。

5 运行 `find /usr/lib/vmware-casa/ -type f -perm -o=w` 命令以确保 `/usr/lib/vmware-casa/` 目录中的文件不是所有人都可写入的文件。

必须不存在任何结果。

6 运行 `find /usr/lib/vmware-vcops/ -type f -perm -o=w` 命令以确保 `/usr/lib/vmware-vcops/` 目录中的文件不是所有人都可写入的文件。

必须不存在任何结果。

7 运行 `find /usr/lib/vmware-vcopssuite/ -type f -perm -o=w` 命令以确保 `/usr/lib/vmware-vcopssuite/` 目录中的文件不是所有人都可写入的文件。

必须不存在任何结果。

Apache 配置

禁用 Web 目录浏览

作为最佳安全做法，请确保用户无法通过目录进行浏览，因为这会增加面临目录遍历攻击的风险。

步骤

- 确认已为所有目录禁用 Web 目录浏览。
  a 在文本编辑器中打开 `/etc/apache2/default-server.conf` 和 `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` 文件。
  b 对于每个 `<Directory>` 列表，确认 `Options` 一行中已忽略相关标记的 `Indexes` 选项。

删除 Apache2 服务器的示例代码

Apache 包括两个示例通用网关接口 (CGI) 脚本：`printenv` 和 `test-cgi`。生产 Web 服务器必须仅包含操作必要的组件。这些组件可能会向攻击者披露有关系统的关键信息。

作为最佳安全做法，请从 `cgi-bin` 目录中删除 CGI 脚本。

步骤

- 要删除 `test-cgi` 和 `prinenv` 脚本，请运行 `rm /usr/share/doc/packages/apache2/test-cgi` 和 `rm /usr/share/doc/packages/apache2/printenv` 命令。

验证 Apache2 服务器的服务器令牌

作为系统强化过程的一部分，请验证 Apache2 服务器的服务器令牌。HTTP 响应的 Web 服务器响应标头可以包含多个信息字段。信息包括请求的 HTML 页面、Web 服务器类型和版本、操作系统和版本以及与 Web 服务器关联的端口。此信息提供恶意用户的重要信息，不包含广泛工具的使用。

指令 `ServerTokens` 必须设置为 `Prod`。例如 `ServerTokens Prod`。此指令控制发送回客户端的服务器响应标头字段是否包括操作系统描述和有关编译模块的信息。

步骤

1. 要验证服务器令牌，请运行 `cat /etc/apache2/sysconfig.d/global.conf | grep ServerTokens` 命令。
2. 要将 `ServerTokens OS` 修改为 `ServerTokens Prod`，请运行 `sed –i 's/\(ServerTokens\s\+\)OS/\1Prod/g' /etc/apache2/sysconfig.d/global.conf` 命令。

禁用 Apache2 服务器的跟踪方法

在标准生产操作中，使用诊断可以揭示导致数据受到威胁的未发现漏洞。要防止误用数据，请禁用 HTTP `Trace` 方法。

步骤

1. 要验证 Apache2 服务器的 `Trace` 方法，请运行以下命令 `grep TraceEnable /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf`。
2. 要禁用 Apache2 服务器的 `Trace` 方法，请运行以下命令 `sed –i "/^[^#]*TraceEnable/c\TraceEnable off" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf`。

禁用配置模式

作为最佳实践，当您安装、配置或维护 vRealize Operations Manager 时，您可以修改配置或设置以启用安装的故障排除和调试。

对您所做的每项更改进行编目和审核，以确保正确地对它们进行了安全保护。如果您不确定您的配置更改是否正确地进行了安全保护，请不要将这些更改应用于生产。

管理不必要的软件组件

要最大程度减少安全风险，请从您的 vRealize Operations Manager 主机删除或配置不必要的软件。

根据制造商的建议和最佳安全做法配置所有未移除的软件，从而最大程度减少造成安全违规的可能性。

保护 USB 大容量存储处理程序

保护 USB 大容量存储处理程序，防止在 vRealize 设备上默认加载该程序，并防止将其作为 vRealize 设备的 USB 设备处理程序。潜在的攻击者可能利用此处理程序来安装恶意软件。

步骤

1 在文本编辑器中打开 `/etc/modprobe.conf.local` 文件。

2 确保文件中出现 `install usb-storage /bin/true` 一行。

3 保存并关闭该文件。

保护蓝牙协议处理程序

保护 vRealize 设备上的蓝牙协议处理程序以防止潜在攻击者利用该程序发起攻击。

没有必要将蓝牙协议绑定到网络堆栈，这可能增大主机的攻击面。防止在 vRealize 设备上默认加载蓝牙协议处理程序模块。

步骤

1 在文本编辑器中打开 `/etc/modprobe.conf.local` 文件。

2 确保此文件中出现 `install bluetooth /bin/true` 一行。

3 保存并关闭该文件。

保护流控制传输协议

防止在 vRealize 设备上默认加载流控制传输协议（Stream Control Transmission Protocol，SCTP）模块。潜在的攻击者可能利用此协议破坏您的系统。

除非绝对必要，否则请配置您的系统以防止加载 SCTP 模块。SCTP 是一个未使用的 IETF 标准化传输层协议。将此协议绑定到网络堆栈会增大主机的攻击面。未授权的本地进程可能会使用协议打开套接字，从而导致内核动态加载协议处理程序。

步骤

1 在文本编辑器中打开 `/etc/modprobe.conf.local` 文件。

2 确保此文件中出现以下一行。

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

3 保存并关闭该文件。

保护数据报拥塞控制协议

作为系统强化活动的一部分，请防止在 vRealize 设备上默认加载数据报拥塞控制协议（Datagram Congestion Control Protocol，DCCP）模块。潜在的攻击者可能利用此协议破坏您的系统。

除非绝对必要，避免加载 DCCP 模块。DCCP 是建议的传输层协议，未使用该协议。将此协议绑定到网络堆栈会增大主机的攻击面。未授权的本地进程可能会使用协议打开套接字，从而导致内核动态加载协议处理程序。

步骤

1 在文本编辑器中打开 `/etc/modprobe.conf.local` 文件。

2 确保文件中出现 DCCP 文本行。

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

3 保存并关闭该文件。

保护可靠数据报套接字协议

作为系统强化活动的一部分，请防止在 vRealize 设备上默认加载可靠数据报套接字（Reliable Datagram Sockets，RDS）协议。潜在的攻击者可能利用此协议破坏您的系统。

将 RDS 协议绑定到网络堆栈会增大主机的攻击面。未授权的本地进程可能会使用协议打开套接字，从而导致内核动态加载协议处理程序。

步骤

1 在文本编辑器中打开 `/etc/modprobe.conf.local` 文件。

2 确保此文件中出现 `install rds /bin/true` 一行。

3 保存并关闭该文件。

保护透明进程间通信协议

作为系统强化活动的一部分，防止在虚拟设备主机中默认加载透明进程间通信协议（Transparent Inter-Process Communication protocol，TIPC）。潜在的攻击者可能利用此协议破坏您的系统。

将 TIPC 协议绑定到网络堆栈会增大主机的攻击面。未授权的本地进程可能会使用协议打开套接字，从而导致内核动态加载协议处理程序。

步骤

1 在文本编辑器中打开 `/etc/modprobe.conf.local` 文件。

2 确保此文件中出现 `install tipc /bin/true` 一行。

3 保存并关闭该文件。

保护 Internet 数据包交换协议

防止在 vRealize 设备上默认加载 Internet 数据包交换（Internetwork Packet Exchange，IPX）协议。潜在的攻击者可能利用此协议破坏您的系统。

除非绝对必要，避免加载 IPX 协议模块。IPX 协议是过时的网络层协议。将此协议绑定到网络堆栈会增大主机的攻击面。未授权的本地进程可能会使用协议打开套接字，从而导致系统动态加载协议处理程序。

步骤

1 在文本编辑器中打开 `/etc/modprobe.conf.local` 文件。

2 确保此文件中出现 `install ipx /bin/true` 一行。

3 保存并关闭该文件。

保护 AppleTalk 协议

防止在 vRealize 设备上默认加载 AppleTalk 协议。潜在的攻击者可能利用此协议破坏您的系统。

除非绝对必要，避免加载 AppleTalk 协议模块。将此协议绑定到网络堆栈会增大主机的攻击面。未授权的本地进程可能会使用协议打开套接字，从而导致系统动态加载协议处理程序。

步骤

1 在文本编辑器中打开 `/etc/modprobe.conf.local` 文件。

2 确保此文件中出现 `install appletalk /bin/true` 一行。

3 保存并关闭该文件。

保护 DECnet 协议

防止在您的系统上默认加载 DECnet 协议。潜在的攻击者可能利用此协议破坏您的系统。

除非绝对必要，避免加载 DECnet 协议模块。将此协议绑定到网络堆栈会增大主机的攻击面。未授权的本地进程可能会使用协议打开套接字，从而导致系统动态加载协议处理程序。

步骤

1 在文本编辑器中打开 DECnet 协议 `/etc/modprobe.conf.local` 文件。

2 确保此文件中出现 `install decnet /bin/true` 一行。

3 保存并关闭该文件。

保护 Firewire 模块

防止在 vRealize 设备上默认加载 Firewire 模块。潜在的攻击者可能利用此协议破坏您的系统。

除非绝对必要，避免加载 Firewire 模块。

步骤

1 在文本编辑器中打开 `/etc/modprobe.conf.local` 文件。

2 确保此文件中出现 `install ieee1394 /bin/true` 一行。

3 保存并关闭该文件。

内核消息日志记录

`/etc/sysctl.conf` 文件中的 `kernel.printk` 规范指定了内核打印日志记录规范。

指定了 4 个值：

- `console loglevel`. 打印到控制台的消息的最低优先级。
- `default loglevel`. 没有特定日志级别的消息的最低级别。

- 控制台日志级别的最低可能级别。
- 控制台日志级别的默认值。

每个值有八个可能的条目。

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

将 `kernel.printk` 值设为 **`3 4 1 7`** 并确保 `kernel.printk=3 4 1 7` 一行在 `/etc/sysctl.conf` 文件中存在。

End Point Operations Management 代理

End Point Operations Management 代理为 vRealize Operations Manager 增添基于代理的发现和监控功能。

End Point Operations Management 代理直接安装在主机上，信任级别可能与 End Point Operations Management 服务器相同，也可能不同。因此，您必须确认代理安全地进行安装。

适用于运行 End Point Operations Management 代理的最佳安全做法

使用用户帐户时，您必须遵循某些最佳安全做法。

- 对于静默安装，请删除 `AGENT_HOME/conf/agent.properties` 文件中存储的任何凭据和服务器证书指纹。
- 使用专门为 End Point Operations Management 代理注册保留的 vRealize Operations Manager 用户帐户。有关详情，请参阅 vRealize Operations Manager 帮助中的“vRealize Operations Manager 中的角色和权限”主题。
- 在安装完成之后，禁用您为代理注册使用的 vRealize Operations Manager 用户帐户。您必须为代理管理活动启用用户访问权限。有关详细信息，请参阅 vRealize Operations Manager 帮助中的在 vRealize Operations Manager 中配置用户和组主题。
- 如果运行代理的系统受到破坏，则可以使用 vRealize Operations Manager 用户界面，通过删除代理资源来撤销代理证书。请参阅“撤销代理”一节以了解更多详细信息。

代理功能最低所需的权限

您需要权限来安装和修改服务。如果要查找正在运行的进程，您用于运行代理的用户帐户还必须有权访问进程和程序。对于 Windows 操作系统安装，您需要权限来安装和修改服务。对于 Linux 安装，如果您使用 RPM 安装程序安装代理，您需要权限来将代理作为服务安装。

将代理注册到 vRealize Operations Manager 服务器所需的最低凭据指的是被授予“代理管理员”角色的用户具有的凭据，此类用户没有被分配给系统中的对象。

基于 Linux 的平台文件和权限

End Point Operations Management 代理完成安装后，所有者是安装代理的用户。

安装 End Point Operations Management 代理的用户提取 TAR 文件或安装 RPM 时，安装目录和文件权限（比如 600 和 700）设置为所有者。

注 解压缩 ZIP 文件时，可能未正确应用权限。验证并确保权限正确。

代理创建和写入的所有文件将被授予 700 权限，所有者是运行代理的用户。

表 3-1. Linux 文件和权限

目录或文件	权限	组或用户	读取	写入	执行
agent directory/bin	700	所有者	是	是	是
		组	否	否	否
		全部	否	否	否
agent directory/conf	700	所有者	是	是	是
		组	否	否	否
		全部	否	否	否
agent directory/log	700	所有者	是	是	否
		组	否	否	否
		全部	否	否	否
agent directory/data	700	所有者	是	是	是
		组	否	否	否
		全部	否	否	否
agent directory/bin/ep-agent.bat	600	所有者	是	是	否
		组	否	否	否
		全部	否	否	否
agent directory/bin/ep-agent.sh	700	所有者	是	是	是
		组	否	否	否
		全部	否	否	否

表 3-1. Linux 文件和权限 （续）

目录或文件	权限	组或用户	读取	写入	执行
agent directory/conf/*（conf 目录中的所有文件）	600	所有者	是	是	是
		组	否	否	否
		全部	否	否	否
agent directory/log/*（log 目录中的所有文件）	600	所有者	是	是	否
		组	否	否	否
		全部	否	否	否
agent directory/data/*（data 目录中的所有文件）	600	所有者	是	是	否
		组	否	否	否
		全部	否	否	否

基于 Windows 的平台文件和权限

对于 Windows 上安装的 End Point Operations Management 代理，安装代理的用户必须具有权限才能安装和修改服务。

End Point Operations Management 代理完成安装后，安装文件夹（包括所有子目录和文件）应仅可由 SYSTEM、管理员组和安装用户访问。当您使用 `ep-agent.bat` 安装 End Point Operations Management 代理时，确保成功完成强化过程。作为安装代理的用户，建议您记下任何错误消息。如果强化过程失败，用户可以手动应用这些权限。

表 3-2. Windows 文件和权限

目录或文件	组或用户	完全控制	修改	读取和执行	读取	写入
<agent directory>/bin	SYSTEM	是	-	-	-	-
	管理员	是	-	-	-	-
	安装用户	是	-	-	-	-
	用户		-	-	-	-
<agent directory>/conf	SYSTEM	是	-	-	-	-
	管理员	是	-	-	-	-
	安装用户	是	-	-	-	-
	用户		-	-	-	-
<agent directory>/log	SYSTEM	是	-	-	-	-
	管理员	是	-	-	-	-
	安装用户	是	-	-	-	-
	用户		-	-	-	-
<agent directory>/data	SYSTEM	是	-	-	-	-
	管理员	是	-	-	-	-
	安装用户	是	-	-	-	-

表 3-2. Windows 文件和权限 （续）

目录或文件	组或用户	完全控制	修改	读取和执行	读取	写入
	用户		-	-	-	-
<agent directory>/bin/hq-agent.bat	SYSTEM	是	-	-	-	-
	管理员	是	-	-	-	-
	安装用户	是	-	-	-	-
	用户		-	-	-	-
<agent directory>/bin/hq-agent.sh	SYSTEM	是	-	-	-	-
	管理员	是	-	-	-	-
	安装用户	是	-	-	-	-
	用户		-	-	-	-
<agent directory>/conf/*（conf 目录中的所有文件）	SYSTEM	是	-	-	-	-
	管理员	是	-	-	-	-
	安装用户	是	-	-	-	-
	用户		-	-	-	-
<agent directory>/log/*（log 目录中的所有文件）	SYSTEM	是	-	-	-	-
	管理员	是	-	-	-	-
	安装用户	是	-	-	-	-
	用户		-	-	-	-
<agent directory>/data/*（data 目录中的所有文件）	SYSTEM	是	-	-	-	-
	管理员	是	-	-	-	-
	安装用户	是	-	-	-	-
	用户		-	-	-	-

代理主机上打开的端口

代理进程侦听可配置的两个端口（127.0.0.1:2144 和 127.0.0.1:32000）上的命令。可能会强行分配这些端口，因此，确切的端口号可能会有所不同。代理不打开外部接口上的端口。

表 3-3. 最少所需的端口

端口	协议	方向	备注
443	TCP	出站	代理使用此端口来建立通过 HTTP、TCP 或 ICMP 的出站连接。
2144	TCP	侦听	仅限内部使用。可配置。用于代理与加载并配置代理的命令行之间的进程间通信。代理进程侦听此端口。 **注** 任意分配端口号，可能会有所不同。
32000	TCP	侦听	仅限内部使用。可配置。用于代理与加载并配置代理的命令行之间的进程间通信。代理进程侦听此端口。 **注** 任意分配端口号，可能会有所不同。

撤销代理

如果由于某种原因您需要撤销代理，例如，正在运行代理的系统受到破坏时，您可以从系统中删除代理资源。任何后续请求将无法通过验证。

使用 vRealize Operations Manager 用户界面，通过删除代理资源来撤销代理证书。有关详细信息，请参见 删除代理资源。

再次确保系统安全时，您可以恢复代理。有关详细信息，请参见 恢复代理资源。

删除代理资源

您可以使用 vRealize Operations Manager，通过删除代理资源来撤销代理证书。

前提条件

要通过之前记录的指标数据保护资源的连续性，请记录资源详细信息中显示的 End Point Operations Management 代理令牌。

步骤

1. 导航到 vRealize Operations Manager 用户界面中的清单资源管理器。
2. 打开“适配器类型”树。
3. 打开“EP Ops 适配器”列表。
4. 选择 **EP Ops 代理 - *HOST_DNS_NAME***。
5. 单击**编辑对象**。
6. 记录代理 ID，这是代理令牌字符串。
7. 关闭“编辑对象”对话框。
8. 选择 **EP Ops 代理 - *HOST_DNS_NAME*** 并单击**删除对象**。

恢复代理资源

恢复系统的安全状态时，您可以恢复已撤销的代理。这可确保该代理继续在相同的资源上报告，而不会丢失历史数据。要执行此操作，必须使用删除代理资源前记录的令牌创建新的 End Point Operations Management 令牌文件。请参阅“删除代理资源”一节。

前提条件

- 确保您拥有记录的 End Point Operations Management 令牌字符串。
- 使用从 vRealize Operations Manager 服务器删除代理资源前记录的资源令牌。
- 确保您拥有“管理代理”特权。

步骤

1 通过运行代理的用户创建代理令牌文件。

例如，运行命令以创建一个包含 123-456-789 令牌的令牌文件。

- 在 Linux 上：

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

- 在 Windows 上：

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

在本示例中，令牌文件写入到该平台的默认令牌位置

2 安装新代理并将它注册到 vRealize Operations Manager 服务器。确保代理加载您插入到令牌文件中的令牌。

您必须具有“管理代理”权限才能执行此操作。

代理证书撤销和更新证书

通过使用 `setup` 命令行参数从代理发起重新颁发流程。当已注册的代理使用 `setup` 命令行参数 `ep-agent.sh setup` 并填写必要凭据时，新的 `registerAgent` 命令被发送到服务器。

服务器检测到已注册代理，其会向代理发送新的客户端证书，而不会创建另一个代理资源。在代理端上，新的客户端证书将取代旧证书。如果修改了服务器证书并且您运行 `ep-agent.sh setup` 命令，您将看到一条消息，请求您信任新证书。您也可以在 `agent.properties` 文件中提供新的服务器证书指纹，然后再运行 `ep-agent.sh setup` 命令，以使该过程静默执行。

前提条件

管理代理权限以撤销和更新证书。

步骤

◆ 在基于 Linux 的操作系统上， 在代理主机上运行 `ep-agent.sh setup` 命令。在基于 Windows 的操作系统上，运行 `ep-agent.bat setup` 命令。

如果代理检测到服务器证书已被修改，将显示一条消息。如果您信任新证书且证书有效，则接受该证书。

修补和更新 End Point Operations Management 代理

如果需要，新的 End Point Operations Management 代理包可独立于 vRealize Operations Manager 版本提供。

End Point Operations Management 代理没有修补或更新。您必须安装该代理的最新可用版本，该版本包含最新安全修复程序。关键安全修复程序将按照 VMware 安全通报指南进行传达。请参见有关安全通报的主题。

其他安全配置活动

验证服务器用户帐户并从主机服务器中删除不必要的应用程序。阻止不必要的端口，禁用正在您的主机服务器上运行的不需要的服务。

验证服务器用户帐户设置

建议您验证本地和域用户帐户与设置中是否存在任何不必要的用户帐户。

将与应用程序的正常运行不相关的任何用户帐户限制为管理、维护和故障排除所需的帐户。将域用户帐户的远程访问权限限制为维护服务器所需的最低权限。严格控制和审核这些帐户。

删除和禁用不必要的应用程序

从主机服务器中删除不必要的应用程序。每个附加或不必要的应用程序由于其未知或未修补漏洞，都会增加暴露风险。

禁用不必要的端口和服务

根据允许通信的开放端口列表确认主机服务器的防火墙。

阻止未在本文档配置端口和协议部分作为 vRealize Operations Manager 最低要求列出或不需要的所有端口。此外，审核主机服务器上运行的服务并禁用不需要的服务。

网络安全和安全通信

4

作为最佳安全做法，请检查和编辑您的 VMware 虚拟设备和主机的网络通信设置。您还必须为 vRealize Operations Manager 配置最低限度的入站和出站端口 。

本章讨论了以下主题：

为虚拟应用程序安装配置网络设置

为确保 VMware 虚拟设备和主机仅允许安全的必要通信，请检查和编辑它们的网络通信设置。

防止用户控制网络接口

作为最佳安全做法，将更改网络接口设置的能力仅限制给具有权限的用户。如果用户操纵网络接口，则可能导致绕过网络安全机制或出现拒绝服务。确保没有为网络接口配置用户控制。

步骤

1. 要验证用户控制设置，请运行 `#grep –i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*` 命令。
2. 确保每个接口设置为 `NO`。

设置 TCP 积压的队列大小

作为最佳安全做法，请在 VMware 设备主机上配置默认 TCP 积压队列大小。为缓解 TCP 拒绝服务攻击，请为 TCP 积压队列大小设置适当的默认大小。建议的默认设置为 1280。

步骤

1. 在每个 VMware 设备主机上运行 `# cat /proc/sys/net/ipv4/tcp_max_syn_backlog` 命令。

2 设置 TCP 积压的队列大小。

a 在文本编辑器中打开 `/etc/sysctl.conf` 文件。

b 通过向文件添加以下条目来设置默认的 TCP 积压队列大小。

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

c 保存更改并关闭文件。

拒绝 ICMPv4 广播地址回显

Internet 控制消息协议 (Internet Control Message Protocol, ICMP) 广播回显响应为放大攻击提供攻击途径，并且有利于恶意代理的网络映射。将系统配置为忽略 ICMPv4 回显可防止此类攻击。

步骤

1 运行 `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` 命令以指定系统不向 ICMP 广播地址回显请求发送响应。

2 将主机系统配置为拒绝 ICMPv4 广播地址回显请求。

a 在文本编辑器中打开 `/etc/sysctl.conf` 文件。

b 如果此条目的值未设置为 `1`，请添加 `net.ipv4.icmp_echo_ignore_broadcasts=1` 条目。

c 保存更改并关闭文件。

将主机系统配置为禁用 IPv4 代理 ARP

IPv4 代理 ARP 允许系统代表连接到某个接口的主机向另一个接口上的 ARP 请求发送响应。必须禁用 IPv4 代理 ARP 以防止未经授权的信息共享。禁用该设置以防止连接的网络区段之间寻址信息泄露。

步骤

1 运行 `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp|egrep "default|all"` 命令以验证代理 ARP 是否禁用。

2 将主机系统配置为禁用 IPv4 代理 ARP。

a 在文本编辑器中打开 `/etc/sysctl.conf` 文件。

b 如果值未设置为 `0`，请添加条目或相应地更新现有条目。将值设置为 `0`。

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

c 保存您所做的任何更改并关闭文件。

将主机系统配置为忽略 IPv4 ICMP 重定向消息

作为安全最佳做法，请确认主机系统忽略 IPv4 Internet 控制消息协议 (Internet Control Message Protocol, ICMP) 重定向消息。恶意 ICMP 重定向消息可以允许中间人攻击发生。路由器使用 ICMP 重定向消息来通知服务器，某个目标存在更直接的路由。这些消息修改主机的路由表并且未经身份验证。

步骤

1 在主机系统上运行 `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep "default|all"` 命令以检查主机系统是否忽略 IPv4 重定向消息。

2 将主机系统配置为忽略 IPv4 ICMP 重定向消息。

   a 打开 `/etc/sysctl.conf` 文件。

   b 如果值未设置为 `0`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `0`。

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

   c 保存更改并关闭文件。

将主机系统配置为忽略 IPv6 ICMP 重定向消息

作为安全最佳做法，请确认主机系统忽略 IPv6 Internet 控制消息协议 (Internet Control Message Protocol, ICMP) 重定向消息。恶意 ICMP 重定向消息可能允许中间人攻击发生。路由器使用 ICMP 重定向消息来告诉服务器，某个目标存在更直接的路由。这些消息修改主机的路由表并且未经身份验证。

步骤

1 在主机系统上运行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects|egrep "default|all"` 命令以检查主机系统是否忽略 IPv6 重定向消息。

2 将主机系统配置为忽略 IPv6 ICMP 重定向消息。

   a 打开 `/etc/sysctl.conf` 将主机系统配置为忽略 IPv6 重定向消息。

   b 如果值未设置为 `0`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `0`。

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

   c 保存更改并关闭文件。

将主机系统配置为拒绝 IPv4 ICMP 重定向

作为安全最佳做法，请确认主机系统拒绝 IPv4 Internet 控制消息协议 (Internet Control Message Protocol, ICMP) 重定向。路由器使用 ICMP 重定向消息来通知服务器，某个特定目标存在直接路由。这些消息包含来自系统的路由表的信息，可能会透露网络拓扑的某些部分。

步骤

1 在主机上运行 `# grep [01] /proc/sys/net/ipv4/conf/*/send_redirects|egrep "default|all"` 以验证它是否拒绝 IPv4 ICMP 重定向。

2 将主机系统配置为拒绝 IPv4 ICMP 重定向。

a 打开 `/etc/sysctl.conf` 文件以配置主机系统。

b 如果值未设置为 `0`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `0`。

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

c 保存更改并关闭文件。

配置主机系统以记录 IPv4 Martian 数据包

作为最佳安全做法，请确认主机系统可记录 IPv4 Martian 数据包。Martian 数据包包含系统知道无效的地址。配置主机系统以记录消息，以便您可以确定错误配置或正在进行的攻击。

步骤

1 运行 `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians|egrep "default|all"` 命令以检查主机是否会记录 IPv4 Martian 数据包。

2 配置主机系统以记录 IPv4 Martian 数据包。

a 打开 `/etc/sysctl.conf` 文件以配置主机系统。

b 如果值未设置为 `1`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `1`。

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

c 保存更改并关闭文件。

将主机系统配置为使用 IPv4 反向路径过滤

作为安全最佳做法，请将您的主机配置为使用 IPv4 反向路径过滤。反向路径过滤可防止仿冒源地址，如果数据包的源地址没有路由，或者路由没有指向原始接口，它会导致系统丢弃这些数据包。

将系统配置为尽可能使用反向路径过滤。根据系统角色，反向路径过滤可能会导致合法通信被丢弃。在此情况下，可能需要使用更宽容的模式或完全禁用反向路径过滤。

步骤

1 在主机系统上运行 `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"` 命令以检查系统是否使用 IPv4 反向路径过滤。

2 将主机系统配置为使用 IPv4 反向路径过滤。

a 打开 `/etc/sysctl.conf` 文件以配置主机系统。

b 如果值未设置为 `1`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `1`。

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

c 保存更改并关闭文件。

将主机系统配置为拒绝 IPv4 转发

作为安全最佳做法，请确认主机系统拒绝 IPv4 转发。如果系统配置为进行 IP 转发并且不是指定的路由器，它可用来绕过网络安全，因为它提供一条不会被网络设备过滤的通信路径。

步骤

1 运行 `# cat /proc/sys/net/ipv4/ip_forward` 命令以验证主机是否拒绝 IPv4 转发。

2 将主机系统配置为拒绝 IPv4 转发。

a 打开 `/etc/sysctl.conf` 以配置主机系统。

b 如果该值未设置为 `0`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `0`。

```
net.ipv4.ip_forward=0
```

c 保存更改并关闭文件。

配置主机系统以拒绝转发 IPv4 源路由数据包

源路由数据包允许数据包的源建议路由器沿着与路由器上配置的路径不同的路径转发数据包，这可以用来绕过网络安全措施。

此要求仅适用于源路由通信的转发，例如当 IPv4 转发启用并且系统用作路由器时。

步骤

1 运行 `# grep [01] /proc/sys/net/ipv4/conf/*/accept_source_route|egrep "default|all"` 命令以验证系统是否未使用 IPv4 源路由数据包

2 配置主机系统以拒绝转发 IPv4 源路由数据包

a 使用文本编辑器打开 `/etc/sysctl.conf` 文件。

b 如果值未设置为 `0`，请确保 `net.ipv4.conf.all.accept_source_route=0` 和 `et.ipv4.conf.default.accept_source_route=0` 设置为 `0`。

c 保存并关闭文件。

将主机系统配置为拒绝 IPv6 转发

作为安全最佳做法，请确认主机系统拒绝 IPv6 转发。如果系统配置为进行 IP 转发并且不是指定的路由器，它可用来绕过网络安全，因为它提供一条不会被网络设备过滤的通信路径。

步骤

1 运行 `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding|egrep "default|all"` 命令以验证主机是否拒绝 IPv6 转发。

2 将主机系统配置为拒绝 IPv6 转发。

a 打开 `/etc/sysctl.conf` 以配置主机系统。

b 如果值未设置为 `0`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `0`。

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

c 保存更改并关闭文件。

将主机系统配置为使用 IPv4 TCP SYN Cookie

作为最佳安全做法，请确认主机系统使用 IPv4 传输控制协议 (TCP) SYN Cookie。通过占据系统的 TCP 连接表并使连接处于 SYN_RCVD 状态，TCP SYN 洪水攻击可能导致出现拒绝服务。通过使用 SYN Cookie 可以在收到后续 ACK 之后才跟踪连接，从而确认启动器正在尝试有效的连接，而不是洪水攻击源。

这种方法并非以完全符合标准的方式运行，而只是在检测到洪水攻击状况时才会激活，其可以在实现系统防御的同时，继续为有效请求提供服务。

步骤

1 运行 `# cat /proc/sys/net/ipv4/tcp_syncookies` 命令以确认主机系统是否使用 IPv4 TCP SYN Cookie。

2 将主机系统配置为使用 IPv4 TCP SYN Cookie。

a 打开 `/etc/sysctl.conf` 以配置主机系统。

b 如果该值未设置为 `1`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `1`。

```
net.ipv4.tcp_syncookies=1
```

c 保存更改并关闭文件。

将主机系统配置为拒绝 IPv6 路由器播发

作为安全最佳做法，请确认主机系统拒绝接受路由器播发和 Internet 控制消息协议 (Internet Control Message Protocol, ICMP) 重定向（除非必要）。IPv6 的一个功能是让系统可以自动使用来自网络的信息来配置其网络设备。从安全的角度来看，最好手动设置重要配置信息，而不是以未经身份验证的方式接受来自网络的信息。

步骤

1 在主机系统上运行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra|egrep "default|all"` 命令以验证系统是否拒绝接受路由器播发和 ICMP 重定向（除非必要）。

2 将主机系统配置为拒绝 IPv6 路由器播发。

   a 打开 `/etc/sysctl.conf` 文件。

   b 如果值未设置为 `0`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `0`。

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

   c 保存更改并关闭文件。

将主机系统配置为拒绝 IPv6 路由器请求

作为安全最佳做法，请确认主机系统拒绝 IPv6 路由器请求（除非必要）。路由器请求设置确定在启用接口时发送多少个路由器请求。如果地址是静态分配的，则不需要发送任何请求。

步骤

1 运行 `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations|egrep "default|all"` 命令以验证主机系统是否拒绝 IPv6 路由器请求（除非必要）。

2 将主机系统配置为拒绝 IPv6 路由器请求。

   a 打开 `/etc/sysctl.conf`。

   b 如果值未设置为 `0`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `0`。

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

   c 保存更改并关闭文件。

将主机系统配置为拒绝路由器请求中的 IPv6 路由器首选项

作为安全最佳做法，请确认您的主机系统拒绝 IPv6 路由器请求（除非必要）。请求中的路由器首选项设置确定路由器首选项。如果地址是静态分配的，则不需要接收请求的路由器首选项。

步骤

1 在主机系统上运行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref|egrep "default|all"` 命令以验证主机系统是否拒绝 IPv6 路由器请求。

2 将主机系统配置为拒绝路由器请求中的 IPv6 路由器首选项。

a 打开 `/etc/sysctl.conf` 文件。

b 如果值未设置为 `0`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `0`。

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

c 保存更改并关闭文件。

将主机系统配置为拒绝 IPv6 路由器前缀

作为安全最佳做法，请确认主机系统拒绝 IPv6 路由器前缀信息（除非必要）。`accept ra pinfo` 设置用于控制系统是否接受来自路由器的前缀信息。如果地址是静态分配的，则系统不接收任何路由器前缀信息。

步骤

1 运行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo|egrep "default|all"` 以验证系统是否拒绝 IPv6 路由器前缀信息。

2 将主机系统配置为拒绝 IPv6 路由器前缀。

a 打开 `/etc/sysctl.conf` 文件。

b 如果值未设置为 `0`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `0`。

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

c 保存更改并关闭文件。

将主机系统配置为拒绝 IPv6 路由器播发跃点限制设置

作为最佳安全做法，请确认主机系统会在非必要的情况下拒绝来自路由器播发的 IPv6 路由器播发跃点限制设置。`accept_ra_defrtr` 设置可控制系统是否将接受来自路由器播发的跃点限制设置。将该设置设为 `0` 可防止路由器为后续的出站数据包更改默认 IPv6 跃点限制。

步骤

1 运行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr|egrep "default|all”` 命令以确认主机系统会拒绝 IPv6 路由器跃点限制设置。

2 如果值未设置为 `0`，请将主机系统配置为拒绝 IPv6 路由器播发跃点限制设置。

a 打开 `/etc/sysctl.conf` 文件。

b 如果值未设置为 `0`，请将以下条目添加到文件或相应地更新现有条目。将值设置为 `0`。

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

c 保存更改并关闭文件。

将主机系统配置为拒绝 IPv6 路由器播发 Autoconf 设置

作为安全最佳做法，请确认主机系统拒绝 IPv6 路由器播发 autoconf 设置。autoconf 设置用于控制路由器播发是否可以导致系统为接口分配全局单播地址。

步骤

1 运行 `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf|egrep "default|all"` 命令以验证主机系统是否拒绝 IPv6 路由器播发 autoconf 设置。

2 如果值未设置为 0，请将主机系统配置为拒绝 IPv6 路由器播发 autoconf 设置。

   a 打开 /etc/sysctl.conf 文件。

   b 如果值未设置为 0，请将以下条目添加到文件或相应地更新现有条目。将值设置为 0。

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

   c 保存更改并关闭文件。

将主机系统配置为拒绝 IPv6 邻居请求

作为安全最佳做法，请确认主机系统拒绝 IPv6 邻居请求（除非必要）。当您启用某个接口以确保所需地址在网络上唯一时，dad_transmits 设置确定每个地址要发送多少个邻居请求。

步骤

1 运行 `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits|egrep "default|all"` 命令以验证主机系统是否拒绝 IPv6 邻居请求。

2 如果值未设置为 0，请将主机系统配置为拒绝 IPv6 邻居请求。

   a 打开 /etc/sysctl.conf 文件。

   b 如果值未设置为 0，请将以下条目添加到文件或相应地更新现有条目。将值设置为 0。

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

   c 保存更改并关闭文件。

配置主机系统以限制 IPv6 地址最大数量

作为最佳安全做法，确认主机能够限制可以分配的 IPv6 地址的最大数量。最大地址数量设置决定了多少个全局单播 IPv6 地址可以分配给每个接口。默认值为 16，但您必须将此数字设置为所需的静态配置全局地址数。

步骤

1 运行 `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses|egrep "default|all"` 命令以验证主机系统是否能够限制可以分配的 IPv6 地址的最大数量。

2 如果值未设置为 1，则配置主机系统以限制可以分配的 IPv6 地址的最大数量。

a 打开 `/etc/sysctl.conf` 文件。

b 将以下条目添加到文件中或相应地更新现有条目。将值设置为 1。

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

c 保存更改并关闭文件。

配置端口和协议

作为安全最佳做法，请禁用所有非必要端口和协议。

为 vRealize Operations Manager 组件配置最少的入站和出站端口，只要能满足重要系统组件在生产中运行的要求即可。

最少所需的默认入站端口

作为最佳安全做法，请配置 vRealize Operations Manager 在生产环境中运行所需的入站端口。

表 4-1. 最少所需的入站端口

端口	协议	备注
443	TCP	用于访问 vRealize Operations Manager 用户界面和 vRealize Operations Manager 管理员界面。
123	UDP	供 vRealize Operations Manager 使用，以与主节点进行网络时间协议 (NTP) 同步。
5433	TCP	启用了高可用性功能时，主节点和副本节点使用此端口来复制全局数据库 (vPostgreSQL)。
7001	TCP	由 Cassandra 用于实现安全的节点间群集通信。 请勿将此端口连接到互联网。将此端口添加到防火墙。
9042	TCP	Cassandra 使用此端口在节点之间实现安全的客户端相关通信。 请勿将此端口连接到互联网。将此端口添加到防火墙。
6061	TCP	由客户端用于连接到 GemFire 定位器以获取到分布式系统中服务器的连接信息。此外，还监控要从客户端发送到负载最小的服务器的服务器负载。
10000-10010	TCP 和 UDP	对等分布式系统中用于单播 UDP 消息和 TCP 故障检测的 GemFire 服务器极短端口范围。
20000-20010	TCP 和 UDP	对等分布式系统中用于单播 UDP 消息和 TCP 故障检测的 GemFire 定位器极短端口范围。

表 4-2. 可选的入站端口

端口	协议	备注
22	TCP	可选。安全 Shell (SSH)。必须在生产环境中禁用侦听端口 22 或任何其他端口的 SSH 服务，并且必须关闭端口 22。
80	TCP	可选。重定向到 443。
3091-3101	TCP	在安装了 Horizon View 时，用于从 Horizon View 访问 vRealize Operations Manager 的数据。

vRealize Operations Manager 系统上的审核和日志记录

5

作为安全最佳做法，请设置 vRealize Operations Manager 系统上的审核和日志记录。

审核和日志记录的详细实施不在本文档的范围之内。

向中央日志主机进行的远程日志记录提供日志的安全存储。通过将日志文件收集到中央主机，使用一个工具就可以轻松地监控环境。您还可以对基础架构内的多个实体执行综合分析并搜索协同攻击。向安全的集中日志服务器进行的日志记录有助于防止日志篡改，并且还提供长期审核记录。

本章讨论了以下主题：

保证远程登录服务器安全

作为安全最佳做法，请确保远程登录服务器只能由授权用户进行配置，并且是安全的。

侵犯主机安全的攻击者可能会搜索并试图篡改日志文件，以便掩盖他们的攻击并保持控制而不会被发现。

使用授权的 NTP 服务器

确保所有主机系统使用相同的相对时间源，包括相关的本地化偏移。您可以将相对时间源关联到一致同意的时间标准，比如协调世界时（Coordinated Universal Time，UTC）。

在查阅相关的日志文件时，您可以轻松跟踪和关联入侵者的操作。错误的时间设置可能会导致难以检查和关联日志文件，从而难以检测攻击，并且可能使审核变得不准确。您可以使用至少三个来自外部时间源的 NTP 服务器，或在受信任的网络上配置一些本地 NTP 服务器，这些服务器可从至少三个外部时间源获取时间。

客户端浏览器注意事项

作为最佳安全做法，请勿通过不受信任或未应用修补程序的客户端或使用浏览器扩展的客户端使用 vRealize Operations Manager。