安全配置指南

2019 年 10 月 24 日

vRealize Automation 7.6

vmware®

您可以从 VMware 网站下载最新的技术文档：

https://docs.vmware.com/cn/。

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

威睿信息技术（中国）有限公司
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

1

安全配置有助于用户评估和优化 vRealize Automation 部署的安全配置。

“安全配置”介绍了如何确认和配置典型 vRealize Automation 环境的安全部署，并提供了帮助用户针对安全配置做出明智选择的信息和过程。

目标读者

本文档提供的信息主要面向 vRealize Automation 系统管理员以及负责维护和配置系统安全的其他用户。

VMware 技术出版物术语表

VMware 技术出版物提供了一个术语表，其中包含一些您可能不熟悉的术语。有关 VMware 技术文档中所使用的术语的定义，请访问 http://www.vmware.com/support/pubs。

vRealize Automation 安全基准概览

2

VMware 提供了许多综合全面的建议，帮助您验证并配置 vRealize Automation 系统的安全基准。

使用 VMware 指定的相应工具和过程，针对 vRealize Automation 系统验证并维护安全的强化基准配置。有些 vRealize Automation 组件已在强化或部分强化状态下安装，但您应根据 VMware 安全建议、公司安全策略和已知威胁检查并验证每个组件的配置。

vRealize Automation 安全状态

vRealize Automation 安全状态会根据系统和网络配置、组织安全策略和安全性最佳做法假定整体安全环境。

验证和配置 vRealize Automation 强化系统时，请考虑 VMware 强化建议中讨论的以下几个问题。

- 安全部署
- 安全配置
- 网络安全

要确保系统已安全强化，请考虑 VMware 强化建议以及您的本地安全策略，因它们与这些概念性问题紧密相关。

系统组件

考虑 vRealize Automation 系统强化和安全配置时，请确保您已了解所有组件及其如何协作以支持系统功能。

规划和实施安全系统时，请考虑以下组件。

- vRealize Automation 设备
- IaaS 组件

要了解 vRealize Automation 及其组件如何协同工作，请参见 VMware vRealize Automation 文档中心的《基础和概念》。有关典型 vRealize Automation 部署和架构的信息，请参见《参考架构》。文档可从 VMware vRealize Automation 文档获取。

确认安装介质的完整性

3

安装 VMware 产品之前，用户应始终确认安装介质的完整性。

在下载 ISO、脱机包或修补程序之后，始终确认 SHA1 哈希，确保已下载文件的完整性和真实性。如果从 VMware 获取物理介质，而安全封装已损坏，请将软件退回 VMware 进行替换。

下载介质后，请使用 MD5/SHA1 总和数值确认下载介质的完整性。将 MD5/SHA1 哈希输出与 VMware 网站上发布的值进行比较。SHA1 或 MD5 哈希应当匹配。

有关确认安装介质完整性的详细信息，请参见 http://kb.vmware.com/kb/1537。

强化 VMware 系统软件基础架构

4

在强化过程中，评估已部署的支持 VMware 系统的软件基础架构并确认符合 VMware 强化准则。

在强化 VMware 系统之前，请检查并解决支持软件基础架构中的安全缺陷，从而创建一个完全强化的安全环境。要考虑的软件基础架构元素包括操作系统组件、支持软件以及数据库软件。根据制造商的建议和其他相关安全协议，解决这些组件以及其他组件中的安全问题。

本章讨论了以下主题：

- 强化 VMware vSphere ® 环境
- 强化基础架构即服务主机
- 强化 Microsoft SQL Server
- 强化 Microsoft .NET
- 强化 Microsoft Internet Information Services (IIS)

强化 VMware vSphere ® 环境

评估 VMware vSphere ® 环境，并确认已执行和维护相应级别的 vSphere 强化指导。

有关更多强化指导，请参见 http://www.vmware.com/security/hardening-guides.html 。

在全面强化的环境中，VMware vSphere ® 基础架构必须符合 VMware 制定的安全准则。

强化基础架构即服务主机

确认已根据 VMware 准则强化基础架构即服务 Microsoft Windows 主机。

查看相应的 Microsoft Windows 强化和安全性最佳做法准则中的建议，并确保已正确强化 Windows Server 主机。不遵循强化建议可能会导致 Windows 版本上的不安全组件引发已知的安全漏洞。

要确认您的版本受支持，请参见 vRealize Automation 支持列表。

有关 Microsoft 产品的正确强化实践指导，请联系 Microsoft 供应商。

强化 Microsoft SQL Server

确认 Microsoft SQL Server 数据库符合 Microsoft 和 VMware 制定的安全准则。

查看相应的 Microsoft SQL Server 强化和安全性最佳做法准则中的建议。查看有关已安装的 Microsoft SQL Server 版本的所有 Microsoft 安全公告。不遵循强化建议可能会导致 Microsoft SQL Server 版本上的不安全组件引发已知的安全漏洞。

要确认您的 Microsoft SQL Server 版本受支持，请参见 vRealize Automation 支持列表。

有关 Microsoft 产品的强化实践指导，请联系 Microsoft 供应商。

强化 Microsoft .NET

在全面强化的环境中，Microsoft .NET 必须符合 Microsoft 和 VMware 制定的安全准则。

查看相应的 .NET 强化和安全性最佳做法准则中列出的建议。此外，查看有关正在使用的 Microsoft SQL Server 版本的所有 Microsoft 安全公告。不遵循强化建议可能会导致不安全的 Microsoft.NET 组件引发已知的安全漏洞。

要确认您的 Microsoft.NET 版本受支持，请参见 vRealize Automation 支持列表。

有关 Microsoft 产品的强化实践指导，请联系 Microsoft 供应商。

强化 Microsoft Internet Information Services (IIS)

确认 Microsoft Internet Information Services (IIS) 符合所有 Microsoft 和 VMware 安全准则。

查看相应的 Microsoft IIS 强化和安全性最佳做法准则中列出的建议。此外，查看有关所使用的 IIS 版本的所有 Microsoft 安全公告。不遵循强化建议可能会引发已知的安全漏洞。

要确认您的版本受支持，请参见 vRealize Automation 支持列表。

有关 Microsoft 产品的强化实践指导，请联系 Microsoft 供应商。

检查已安装的软件

5

由于第三方软件和未用软件中的漏洞会增加未授权系统访问和可用性中断风险，因此，请务必检查 VMware 主机上安装的所有软件并评估其用途，这一点至关重要。

仅应在 VMware 主机上安装系统安全操作所需的软件。请卸载未使用或无关的软件。

确认不受支持的已安装软件的清单

评估已安装产品的 VMware 部署和清单，确认未安装任何不受支持的无关软件。

有关第三方产品的支持策略的详细信息，请参见 VMware 支持文章，网址为：https://www.vmware.com/support/policies/thirdparty.html。

确认第三方软件

VMware 不支持或不建议安装未经测试或未确认的第三方软件。在 VMware 主机上安装不安全、未应用修补程序或未经身份验证的第三方软件，可能会导致系统面临未授权访问和可用性中断风险。如果必须使用不受支持的第三方软件，请咨询第三方供应商，了解安全配置和修补要求。

VMware 安全建议和修补程序

6

要保证系统的最大安全性，请遵循以下 VMware 安全建议并应用所有相关的修补程序。

VMware 发布了许多产品安全建议。请密切关注这些建议，确保您的产品免受已知威胁攻击。

评估 vRealize Automation 安装、修补和升级历史记录，确认已遵循并强制执行发布的 VMware 安全建议。

有关 VMware 最新安全建议的详细信息，请参见 http://www.vmware.com/security/advisories/。

安全配置

7

确认 vRealize Automation 虚拟设备和基础架构即服务组件的安全设置适用于您的系统配置并进行更新。此外，确认并更新其他组件和应用程序的配置。

安全配置 vRealize Automation 安装时，涉及到分别配置每个组件并使其协同工作。请考虑所有系统组件的配置，以实现合理的安全基准。

本章讨论了以下主题：

保护 vRealize Automation 设备的安全

根据系统配置需要确认和更新 vRealize Automation 设备的安全设置。

为虚拟设备及其主机操作系统配置安全设置。此外，设置或验证其他相关组件和应用程序的配置。在某些情况下，您需要验证现有设置；在其他情况下，您必须更改或添加相应的配置设置。

更改 Root 密码

您可以更改 vRealize Automation 设备的 root 密码。

步骤

1. 以 root 用户身份登录到 vRealize Automation 设备管理界面。

   https://*vrealize-automation-appliance-FQDN*:5480
2. 单击**管理**选项卡。
3. 单击**管理**子菜单。
4. 在**当前管理员密码**文本框中输入现有密码。
5. 在**新管理员密码**文本框中输入新密码。
6. 在**重新键入新管理员密码**文本框中输入新密码。
7. 单击**保存设置**。

确认 Root 密码哈希和复杂性

确认 root 密码符合您组织的公司密码复杂性要求。

必须确认 root 密码复杂性，这是因为 root 用户将绕过应用于用户帐户的 pam_cracklib 模块密码复杂性检查。

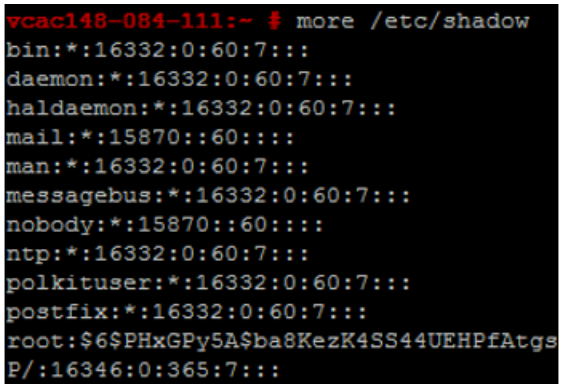
帐户密码必须以 `$6$`（表示 sha512 哈希）开头。这是所有强化设备的标准哈希。

步骤

1 要确认 root 密码的哈希，请以 root 用户身份登录并运行 `# more /etc/shadow` 命令。

将显示哈希信息。

图 7-1. 密码哈希结果



2 如果 root 密码不包含 sha512 哈希值，请运行 `passwd` 命令进行更改。

所有强化设备均针对 `/etc/pam.d/common-password` 文件中的 `pw_history` 模块启用 `enforce_for_root`。默认情况下，系统将记住最后五个密码。每个用户的旧密码存储在 `/etc/securetty/passwd` 文件中。

确认 Root 密码历史记录

确认已为 root 帐户强制执行密码历史记录。

所有强化设备均针对 `/etc/pam.d/common-password` 文件中的 pw_history 模块启用 `enforce_for_root`。默认情况下，系统将记住最后五个密码。每个用户的旧密码存储在 `/etc/securetty/passwd` 文件中。

步骤

1 运行以下命令

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

2 确保返回的结果中显示 `enforce_for_root`。

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

管理密码到期

请根据您组织的安全策略配置所有帐户密码到期时间。

默认情况下，所有强化的 VMware 虚拟设备帐户使用 60 天的密码到期时间。在大多数强化设备上，root 帐户的密码设置为 365 天到期。最佳做法是确认所有帐户的到期同时符合安全和操作要求标准。

如果 root 密码到期，则无法将其恢复。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。

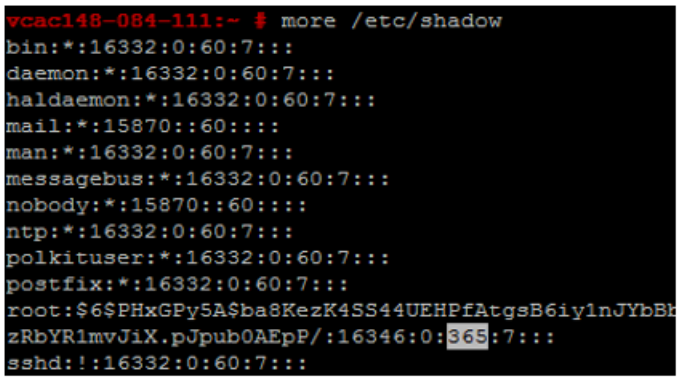
步骤

1 以 root 用户身份登录到虚拟设备计算机，然后运行以下命令确认所有帐户的密码到期时间。

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

密码到期时间是 shadow 文件的第五个字段（字段以冒号分隔）。root 到期时间以天为单位设置。

图 7-2. “密码到期”字段



2 要修改 root 帐户到期时间，请运行以下形式的命令。

```
# passwd –x 365 root
```

在此命令中，365 指定密码到期之前的天数。使用同一命令修改任何用户，用特定帐户代替“root”，然后替换天数以符合组织的到期标准。

管理安全 Shell 和管理帐户

对于远程连接，所有强化设备都包括安全 Shell (Secure Shell, SSH) 协议。仅在必要时使用 SSH，并适当进行管理以确保系统安全。

SSH 是一个交互式命令行环境，可支持远程连接到 VMware 虚拟设备。默认情况下，SSH 访问需要具有高度特权的用户帐户凭据。Root 用户的 SSH 活动通常会绕过虚拟设备基于角色的访问控制 (Role-Based Access Control, RBAC) 和审核控制。

最佳做法是在生产环境中禁用 SSH，仅在对无法通过其他方式解决的问题进行故障排除时将其激活。仅在出于特定需要时根据您组织的安全策略将其启用。默认情况下，vRealize Automation 设备会禁用 SSH。根据您的 vSphere 配置，可以在部署开放式虚拟化格式 (Open Virtualization Format, OVF) 模板时启用或禁用 SSH。

确定计算机是否已启用 SSH 的简单测试是尝试使用 SSH 打开连接。如果连接打开并请求凭据，则表示 SSH 已启用并且可用于连接。

安全 Shell root 用户帐户

由于 VMware 设备不包括预配置的用户帐户，因此默认情况下，root 帐户可以使用 SSH 直接登录。尽快以 root 用户身份禁用 SSH。

为了符合不可否认性合规标准，所有强化设备上的 SSH 服务器都预配置了 AllowGroups wheel 条目，用于限制对辅助 wheel 组的 SSH 访问。为了实现职责分离，可以在 `/etc/ssh/sshd_config` 文件中修改 AllowGroups wheel 条目，以便使用其他组（比如 sshd）。

wheel 组使用 `pam_wheel` 模块启用以提供超级用户访问权限，因此 wheel 组成员可以通过 su 命令成为 root 用户（需要 root 密码）。组分隔让用户能够通过 SSH 连接设备，但无法通过 su 命令成为 root 用户。为确保设备正常工作，请勿移除或修改 AllowGroups 字段中的其他条目。进行更改后，必须通过运行以下命令重新启动 SSH 守护进程：`# service sshd restart`。

在 vRealize Automation 设备上启用或禁用安全 Shell

在 vRealize Automation 设备上启用安全 Shell (SSH) 以仅用于故障排除。在正常生产操作中，请在这些组件上禁用 SSH。

您可以使用 vRealize Automation 设备管理界面在 vRealize Automation 设备上启用或禁用 SSH。

步骤

1 以 root 用户身份登录到 vRealize Automation 设备管理界面。

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

2 单击**管理**选项卡。

3 单击**管理**子菜单。

4 选中**启用 SSH 服务**复选框以启用 SSH，或者取消选中该复选框以禁用 SSH。

5 单击**保存设置**保存更改。

为安全 Shell 创建本地管理员帐户

作为安全性最佳做法，请在虚拟设备主机上为安全 Shell (Secure Shell, SSH) 创建和配置本地管理帐户。此外，在创建相应的帐户之后，移除 root 用户的 SSH 访问权限。

为 SSH 和/或辅助 wheel 组的成员创建本地管理帐户。禁用 root 用户直接访问之前，请测试授权管理员能否使用 AllowGroups 访问 SSH，以及能否使用 wheel 组通过 su 命令成为 root 用户。

步骤

1 以 root 用户身份登录到虚拟设备，并使用相应的用户名运行以下命令。

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

Wheel 是 AllowGroups 中指定可进行 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，以强制执行密码复杂性检查。

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

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

3 要移除 SSH 直接登录，请通过将 `(#)PermitRootLogin yes` 替换为 `PermitRootLogin no` 来修改 `/etc/ssh/sshd_config` 文件。

或者，您也可以通过在虚拟设备管理界面 (VAMI) 的**管理**选项卡上选中或取消选中**已启用管理员 SSH 登录**复选框来启用或禁用 SSH。

后续步骤

禁用 root 用户直接登录。默认情况下，强化设备允许通过控制台直接登录到 root。出于不可否认性目的创建管理帐户且测试是否具备 su-root wheel 访问权限之后，以 root 用户身份编辑 `/etc/security` 文件并将 `tty1` 条目替换为 `console` 可禁用 root 用户直接登录。

1 在文本编辑器中打开 `/etc/securetty` 文件。

2 找到 `tty1` 并将其替换为 `console`。

3 保存文件并关闭。

强化安全 Shell 服务器配置

如果可能，所有 VMware 设备都应具有默认强化配置。通过检查配置文件中全局选项部分中的服务器和客户端服务设置，用户可以确认其配置已正确强化。

步骤

1 在 VMware 设备上打开 `/etc/ssh/sshd_config` 服务器配置文件，然后确认设置正确。

设置	状态
服务器守护进程协议	协议 2
CBC 密码	aes256-ctr 和 aes128-ctr
TCP 转发	禁用 AllowTCPForwarding
服务器网关端口	禁用网关端口
X11 转发	禁用 X11Forwarding
SSH 服务	使用 AllowGroups 字段并指定具有访问权限的组。向此组添加相应成员。
GSSAPI 身份验证	如果未使用，则禁用 GSSAPIAuthentication
Keberos 身份验证	如果未使用，则禁用 KeberosAuthentication
局部变量（AcceptEnv 全局选项）	设置为“通过注释掉来禁用”或“通过 `LC_*` 或 `LANG` 变量启用”
隧道配置	禁用 PermitTunnel

设置	状态
网络会话	MaxSessions 为 1
用户并发连接数	针对 root 及任何其他用户，设置为 1。 `/etc/security/limits.conf` 文件也需要配置相同的设置。
严格模式检查	启用严格模式
特权分离	启用 UsePrivilegeSeparation
rhosts RSA 身份验证	禁用 RhostsESAAuthentication
压缩	延迟压缩或禁用压缩
消息身份验证代码	MACs hmac-sha1
用户访问限制	禁用 PermitUserEnvironment

2 保存更改并关闭文件。

强化安全 Shell 客户端配置

在系统强化过程中，检查虚拟设备主机上的 SSH 客户端配置文件以确认强化 SSH 客户端，从而确保其配置符合 VMware 准则。

步骤

1 打开 SSH 客户端配置文件 `/etc/ssh/ssh_config`，然后确认全局选项部分中的设置正确。

设置	状态
客户端协议	协议 2
客户端网关端口	禁用网关端口
GSSAPI 身份验证	禁用 GSSAPIAuthentication
局部变量（SendEnv 全局选项）	仅提供 LC_* 或 LANG 变量
CBC 密码	仅限 aes256-ctr 和 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。

确认安全 Shell 密钥文件权限

为了最大程度地减少恶意攻击，请在虚拟设备主机上保留关键 SSH 密钥文件权限。

配置或更新 SSH 配置之后，始终确认以下 SSH 密钥文件权限未更改。

- `/etc/ssh/*key.pub` 中的公有主机密钥文件由 root 用户所有，且其权限设置为 0644 (-rw-r--r--)。
- `/etc/ssh/*key` 中的私有主机密钥文件由 root 用户所有，且其权限设置为 0600 (-rw------)。

确认 SSH 密钥文件权限

确认将 SSH 权限应用于公钥和私钥文件。

步骤

1 通过运行以下命令来检查 SSH 公钥文件：`ls –l /etc/ssh/*key.pub`

2 确认所有者是 root，组所有者是 root，并且文件权限设置为 0644 (-rw-r--r--)。

3 通过运行以下命令来修复任何问题。

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

chgrp root /etc/ssh/*key.pub

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

4 通过运行以下命令来检查 SSH 私钥文件：`ls –l /etc/ssh/*key`

5 确认所有者是 root，组所有者是 root，并且文件权限设置为 0600 (-rw-------)。通过运行以下命令来修复任何问题。

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

chgrp root /etc/ssh/*key

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

更改虚拟设备管理界面用户

可以在虚拟设备管理界面上添加和删除用户以创建适当的安全级别。

虚拟设备管理界面的 root 用户帐户使用 PAM 进行身份验证，因此 PAM 设置的剪辑级别也适用。如果未正确隔离虚拟设备管理界面，当攻击者试图通过暴力攻击强制登录时，可能会锁定系统 root 帐户。此外，如果您组织中多人认为 root 帐户不足以提供不可否认性，可以选择更改管理界面的管理员用户。

前提条件

步骤

1 运行以下命令以创建新用户并将其添加到虚拟设备管理界面组。

```
useradd –G vami,root user
```

2 为该用户创建密码。

```
passwd user
```

3 （可选） 运行以下命令以禁用虚拟设备管理界面的 root 访问权限。

```
usermod –R vami root
```

注 禁用虚拟设备管理界面的 root 访问权限还会禁用从“管理”选项卡更新管理员或 root、密码的功能。

设置引导加载程序身份验证

要提供适当的安全性级别，请在 VMware 虚拟设备上配置引导加载程序身份验证。

如果系统的引导加载程序不需要身份验证，则具有系统控制台访问权限的用户可以更改系统引导配置或者引导系统进入单用户或维护模式，这可能会导致拒绝服务或未经授权的系统访问。由于默认情况下 VMware 虚拟设备上未设置引导加载程序身份验证，因此您必须创建 GRUB 密码才能对其进行配置。

步骤

1 通过在虚拟设备上的 `/boot/grub/menu.lst` 文件中找到 `password --md5 <password-hash>` 行，验证是否存在引导密码。

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

系统将生成 MD5 密码，且该命令将提供 md5 哈希输出。

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

配置 NTP

对于关键时间源，请在 vRealize Automation 设备上禁用主机时间同步并使用网络时间协议 (Network Time Protocol, NTP)。

vRealize Automation 设备上的 NTP 守护进程可提供同步时间服务。默认情况下，NTP 处于禁用状态，因此您需要手动对其进行配置。如果可能，请在生产环境中使用 NTP 跟踪用户操作，并通过准确的审核和日志保留数据来检测潜在的恶意攻击和入侵。有关 NTP 安全声明的信息，请参见 NTP 网站。

NTP 配置文件位于每个设备的 `/etc/` 文件夹中。您可以为 vRealize Automation 设备启用 NTP 服务，并在虚拟设备管理界面的**管理**选项卡上添加时间服务器。

步骤

1 使用文本编辑器打开虚拟设备主机上的 `/etc/ntp.conf` 配置文件。

2 将文件所有权设置为 **`root:root`**。

3 将权限设置为 **`0640`**。

4 要降低 NTP 服务上的拒绝服务放大攻击风险，请打开 `/etc/ntp.conf` 文件并确保该文件中存在限制行。

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

5 保存所有更改并关闭文件。

为正在传输的 vRealize Automation 设备数据配置 TLS

确保 vRealize Automation 部署使用强 TLS 协议保护 vRealize Automation 设备组件的传输通道。

出于性能方面的考虑，某些应用程序服务之间的 localhost 连接未启用 TLS。如果要进行深度防御，请在所有 localhost 通信上启用 TLS。

重要事项 如果要在负载平衡器上终止 TLS，请在所有负载平衡器上禁用 SSLv2、SSLv3 和 TLS 1.0 等不安全的协议。

在 localhost 配置上启用 TLS

默认情况下，某些 localhost 通信不使用 TLS。为了增强安全性，您可以在所有 localhost 连接中启用 TLS。

步骤

1 使用 SSH 连接到 vRealize Automation 设备。

2 通过运行以下命令为 vcac 密钥库设置权限。

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

3 更新 HAProxy 配置。

a 打开位于 `/etc/haproxy/conf.d` 中的 HAProxy 配置文件，然后选择 20-vcac.cfg 服务。

b 找到包含以下字符串的行：

`server local 127.0.0.1…`，并在这些行的末尾处添加以下内容：`ssl verify none`

本部分包含其他行，如下所示：

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

c 将 backend-horizon 端口从 8080 更改为 8443。

4 获取 keystorePass 的密码。

a 在 `/etc/vcac/security.properties` 文件中找到 `certificate.store.password` 属性。

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

b 使用以下命令解密值：

`vcac–config prop–util –d ––p VALUE`

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

5 配置 vRealize Automation 服务

a 打开 /etc/vcac/server.xml 文件。

b 将以下属性添加到 Connector 标记，使用在 etc/vcac/security.properties 中找到的证书存储密码值替换 certificate.store.password。

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

6 配置 vRealize Orchestrator 服务。

a 打开 /etc/vco/app-server.xml 文件

b 将以下属性添加到 Connector 标记，使用在 etc/vcac/security.properties 中找到的证书存储密码值替换 certificate.store.password。

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

7 重新启动 vRealize Orchestrator、vRealize Automation 和 haproxy 服务。

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

注 如果 vco-server 未重新启动，请重新引导主机。

8 配置虚拟设备管理界面。

可以通过在 vRealize Automation 虚拟设备上执行以下命令，列出服务的状态。

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

注 如果在虚拟设备管理界面上启用 SSL，则“服务”选项卡无法列出 vRealize Automation 服务的状态。

a 打开 /opt/vmware/share/htdocs/service/café-services/services.py 文件。

b 将 conn = httplib.HTTP() 行更改为 conn = httplib.HTTPS() 以增强安全性。

启用联邦信息处理标准 (FIPS) 140-2 合规性

vRealize Automation 设备现在使用联邦信息处理标准 (Federal Information Processing Standard, FIPS) 140-2 认证的 OpenSSL 版本处理所有入站和出站网络流量中通过 TLS 传输的数据。

您可以在 vRealize Automation 设备管理界面中启用或禁用 FIPS 模式。以 root 用户身份登录时，还可以从命令行使用以下命令配置 FIPS：

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

启用 FIPS 时，端口 443 上的入站和出站 vRealize Automation 设备网络流量使用符合 FIPS 140 - 2 的加密。无论 FIPS 设置如何，vRealize Automation 都会使用 AES - 256 保护存储在 vRealize Automation 设备上的安全数据。

注 目前，vRealize Automation 仅部分启用 FIPS 合规，因为有些内部组件尚未使用经认证的加密模块。如果尚未实施经认证的模块，则会在所有加密算法中使用基于 AES - 256 的加密。

注 更改配置后，以下过程将重新引导物理机。

步骤

1 以 root 用户身份登录到 vRealize Automation 设备管理界面。

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

2 选择 **vRA > 主机设置**。

3 单击右上方“操作”标题下的按钮以启用或禁用 FIPS。

4 单击**是**以重新启动 vRealize Automation 设备。

确认已禁用 SSLv3、TLS 1.0 和 TLS 1.1

在强化过程中，确保部署的 vRealize Automation 设备 使用安全传输通道。

注 禁用 TLS 1.0/1.1 并启用 TLS 1.2 后，无法运行加入群集操作

前提条件

完成 在 localhost 配置上启用 TLS。

步骤

1 确认已在 vRealize Automation 设备 上的 HAProxy https 处理程序中禁用 SSLv3、TLS 1.0 和 TLS 1.1。

查看以下文件	确保存在以下内容	在下述相应行中
/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 重新启动服务。

```
service haproxy restart
```

3 打开 /opt/vmware/etc/lighttpd/lighttpd.conf 文件，并确认显示正确的禁用条目。

注 没有任何指令用于在 Lighttpd 中禁用 TLS 1.0 或 TLS 1.1。通过强制 OpenSSL 不使用 TLS 1.0 和 TLS 1.1 的密码套件，可以部分缓解对 TLS 1.0 和 TLS 1.1 使用的限制。

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

4 确认已针对 vRealize Automation 设备 上的控制台代理禁用 SSLv3、TLS 1.0 和 TLS 1.1。

a 通过添加或修改以下行编辑 /etc/vcac/security.properties 文件：

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

b 通过运行以下命令重新启动服务器：

```
service vcac-server restart
```

5 确认已针对 vCO 服务禁用 SSLv3、TLS 1.0 和 TLS 1.1。

a 在 /etc/vco/app-server/server.xml 文件中找到 <Connector> 标记，并添加以下属性：

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

b 通过运行以下命令重新启动 vCO 服务。

```
service vco-server restart
```

6 确认已针对 vRealize Automation 服务禁用 SSLv3、TLS 1.0 和 TLS 1.1。

a 将以下属性添加到 `/etc/vcac/server.xml` 文件内的 `<Connector>` 标记中

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

b 通过运行以下命针对令重新启动 vRealize Automation 服务：

```
service vcac-server restart
```

7 确认已针对 RabbitMQ 禁用 SSLv3、TLS 1.0 和 TLS 1.1。

打开 `/etc/rabbitmq/rabbitmq.config` 文件，并确认 ssl 和 ssl_options 部分仅显示 `{versions, ['tlsv1.2']}`。

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

8 重新启动 RabbitMQ 服务器。

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

9 确认已针对 vIDM 服务禁用 SSLv3、TLS 1.0 和 TLS 1.1。

针对包含 `SSLEnabled="true"` 的连接器的每个实例，打开 `opt/vmware/horizon/workspace/conf/server.xml` 文件，并确保存在以下行。

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

为 vRealize Automation 组件配置 TLS 密码套件

为了确保最大安全性，您必须将 vRealize Automation 组件配置为使用强密码。

服务器与浏览器之间协商的加密密码确定了 TLS 会话中使用的加密强度。

要确保仅选择强密码，请在 vRealize Automation 组件中禁用弱密码。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，按合适的顺序配置所有密码。

禁用不提供身份验证的密码套件，如 NULL 密码套件、aNULL 或 eNULL。此外，禁用匿名 Diffie-Hellman 密钥交换 (ADH)、导出级别密码（EXP，包含 DES 的密码）、IDEA 密码套件和 RC4 密码套件，并禁止使用小于 128 位的密钥大小加密负载流量或将 MD5 用作负载流量的哈希机制。此外，还要确保使用 Diffie-Hellman (DHE) 密钥交换的密码套件处于禁用状态。

有关禁用 TLS 的详细信息，请参见知识库文章 2146570。

在 HA 代理中禁用弱密码

根据可接受的密码列表检查 vRealize Automation 设备 HA 代理服务密码，并禁用所有弱密码。

禁用不提供身份验证的密码套件，如 NULL 密码套件、aNULL 或 eNULL。此外，禁用匿名 Diffie-Hellman 密钥交换 (ADH)、导出级别密码（EXP，包含 DES 的密码）、IDEA 密码套件和 RC4 密码套件，并禁止使用小于 128 位的密钥大小加密负载流量或将 MD5 用作负载流量的哈希机制。

步骤

1 检查绑定指令的 `/etc/haproxy/conf.d/20-vcac.cfg` 文件密码条目，并禁用所有弱密码。

```
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
```

2 检查绑定指令的 `/etc/haproxy/conf.d/30-vro-config.cfg` 文件密码条目，并禁用所有弱密码。

```
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
```

在 vRealize Automation 设备 vRealize Automation 设备控制台代理服务中禁用弱密码

根据可接受的密码列表检查 vRealize Automation 设备控制台代理服务密码，并禁用所有弱密码。

禁用不提供身份验证的密码套件，如 NULL 密码套件、aNULL 或 eNULL。此外，禁用匿名 Diffie-Hellman 密钥交换 (ADH)、导出级别密码（EXP，包含 DES 的密码）、IDEA 密码套件和 RC4 密码套件，并禁止使用小于 128 位的密钥大小加密负载流量或将 MD5 用作负载流量的哈希机制。

步骤

1 在文本编辑器中打开 `/etc/vcac/security.properties` 文件。

2 在文件中添加一行以禁用不需要的密码套件。

使用以下行的变化形式：

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

例如，要禁用 AES 128 和 AES 256 密码套件，请添加以下行：

```
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 使用以下命令重新启动服务器。

```
service vcac-server restart
```

在 vRealize Automation 设备 vCO 服务中禁用弱密码

根据可接受的密码列表，检查 vRealize Automation 设备 vCO 服务密码，并禁用所有弱密码。

禁用不提供身份验证的密码套件，如 NULL 密码套件、aNULL 或 eNULL。此外，禁用匿名 Diffie-Hellman 密钥交换 (ADH)、导出级别密码（EXP，包含 DES 的密码）、IDEA 密码套件和 RC4 密码套件，并禁止使用小于 128 位的密钥大小加密负载流量或将 MD5 用作负载流量的哈希机制。

步骤

1 在 `/etc/vco/app-server/server.xml` 文件中找到 `<Connector>` 标记。

2 编辑或添加密码属性以使用所需的密码套件。

请参考以下示例：

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_E
CDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GC
M_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_R
SA_WITH_AES_256_CBC_SHA384”
```

在 vRealize Automation 设备 RabbitMQ 服务中禁用弱密码

根据可接受的密码列表，检查 vRealize Automation 设备 RabbitMQ 服务密码，并禁用所有弱密码。

禁用不提供身份验证的密码套件，如 NULL 密码套件、aNULL 或 eNULL。此外，禁用匿名 Diffie-Hellman 密钥交换 (ADH)、导出级别密码（EXP，包含 DES 的密码）、IDEA 密码套件和 RC4 密码套件，并禁止使用小于 128 位的密钥大小加密负载流量或将 MD5 用作负载流量的哈希机制。

步骤

1 评估受支持的密码套件，方法是运行 `# /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites().'` 命令。

下述示例中返回的密码仅表示受支持的密码。RabbitMQ 服务器不使用或通告这些密码，除非在 `rabbitmq.config` 文件中配置为执行此操作。

```
["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 选择满足您组织安全要求的受支持密码。

例如，要仅允许 `ECDHE-ECDSA-AES128-GCM-SHA256 & ECDHE-ECDSA-AES256-GCM-SHA384`，请检查 `/etc/rabbitmq/rabbitmq.config` 文件并将以下行添加到 ssl 和 ssl_options。

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

3 使用以下命令重新启动 RabbitMQ 服务器。

```
service rabbitmq-server restart
```

确认静态数据安全

确认与 vRealize Automation 结合使用的数据库用户和帐户的安全。

Postgres 用户

Postgres Linux 用户帐户已绑定到 postgres 数据库的超级用户帐户角色。默认情况下，该帐户已锁定。这是此用户最安全的配置，因为它只能通过 root 用户帐户访问。请勿解锁此用户帐户。

数据库用户帐户角色

外部使用应用程序功能时，不得利用默认的 postgres 用户帐户角色。要支持非默认数据库检查或报告活动，应创建其他帐户并相应地进行密码保护。

在命令行中运行以下脚本：

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

这将添加该用户提供的新用户和密码。

注 配置主-从属 HA postgres 设置时，必须针对主 postgres 数据库运行此脚本。

配置 PostgreSQL 客户端身份验证

确保 vRealize Automation 设备 PostgreSQL 数据库未配置本地信任身份验证。通过此配置，任何本地用户（包括数据库超级用户）无需密码即可以任何 PostgreSQL 用户身份进行连接。

注 Postgres 超级用户帐户应保持为本地信任。

建议使用 md5 身份验证方法，因为它发送加密密码。

客户端身份验证配置设置位于 /storage/db/pgdata/pg_hba.conf 文件中。

```
# 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
```

如果编辑 pg_hba.conf 文件，则通过运行以下命令重新启动 Postgres 服务器后更改才会生效。

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

配置 vRealize Automation 应用程序资源

检查 vRealize Automation 应用程序资源并限制文件权限。

步骤

1 运行以下命令，确认设置了 SUID 和 GUID 位的文件已明确定义。

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

将显示以下列表。

```
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 运行以下命令，确认虚拟设备上的所有文件都具有所有者。

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

3 通过运行以下命令，检查虚拟设备的所有文件的权限，以确认它们都处于全局不可写状态。

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

4 运行以下命令，确认只有 vcac 用户拥有正确的文件。

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

如果没有显示任何结果，则所有正确文件仅由 vcac 用户所有。

5 确认以下文件仅可由 vcac 用户写入。

```
/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
```

还要确认以下文件及其子目录

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

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

6 确认只有 vcac 或 root 用户可以读取以下目录及其子目录中的正确文件。

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

7 确认正确文件仅由 vco 或 root 用户所有，如以下目录及其子目录中所示。

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

8 确认正确文件仅可由 vco 或 root 用户写入，如以下目录及其子目录中所示。

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

9 确认正确文件仅可由 vco 或 root 用户读取，如以下目录及其子目录中所示。

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

自定义控制台代理配置

您可以自定义 vRealize Automation 的远程控制台配置以便进行故障排除和组织实践。

安装、配置或维护 vRealize Automation 时，您可以更改某些设置，以便对安装进行故障排除和调试。对每次所做的更改进行编录和审核，确保根据所需用途有效保护应用程序组件。如果您不确定配置更改是否已得到有效保护，请不要应用到生产环境。

自定义 VMware Remote Console 票证到期

您可以自定义用于建立 VMware Remote Console 连接的远程控制台票证的有效期。

当用户建立 VMware Remote Console 连接时，系统将创建并返回一次性凭据，以便与虚拟机建立特定连接。您可以将票证到期设置指定的时间范围（以分钟为单位）。

步骤

1 在文本编辑器中打开 `/etc/vcac/security.properties` 文件。

2 在文件中添加一行，形式为 `consoleproxy.ticket.validitySec=30`。

此行中的数值指定票证到期之前的分钟数。

3 保存文件并关闭。

4 使用 `/etc/init.d/vcac-server restart` 命令重新启动 vcac-server。

票证到期值重置为指定的时间范围（以分钟为单位）。

自定义控制台代理服务器端口

您可以自定义 VMware Remote Console 控制台代理侦听消息的端口。

步骤

1 在文本编辑器中打开 `/etc/vcac/security.properties` 文件。

2 在文件中添加一行，形式为 `consoleproxy.service.port=8445`。

数值指定控制台代理服务端口号，本例中为 8445。

3 保存文件并关闭。

4 使用 `/etc/init.d/vcac-server restart` 命令重新启动 vcac-server。

代理服务端口将更改为指定的端口号。

配置 X-XSS-Protection 响应标头

将 X-XSS-Protection 响应标头添加到 HAProxy 配置文件。

步骤

1 打开 `/etc/haproxy/conf.d/20-vcac.cfg` 进行编辑。

2 在前端部分添加以下行：

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

3 使用以下命令重新加载 HAProxy 配置。

`/etc/init.d/haproxy reload`

配置 X-Content-Type-Options 响应标头

将 X-Content-Type-Options 响应标头添加到 HAProxy 配置。

步骤

1 打开 `/etc/haproxy/conf.d/20-vcac.cfg` 进行编辑。

2 在前端部分添加以下行：

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

3 使用以下命令重新加载 HAProxy 配置。

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

配置 HTTP 强制传输安全响应标头

将 HTTP 强制传输 (HSTS) 响应标头添加到 HAProxy 配置。

步骤

1 打开 `/etc/haproxy/conf.d/20-vcac.cfg` 进行编辑。

2 在前端部分添加以下行：

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

3 使用以下命令重新加载 HAProxy 配置。

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

配置 X-Frame-Options 响应标头

在某些情况下，X-Frame-Options 响应标头可能会重复出现。

由于 vIDM 服务将 X-Frame-Options 响应标头添加到后端和 HAProxy，因此该标头可能会重复出现。您可以进行相应配置以防止其重复出现。

步骤

1 打开 `/etc/haproxy/conf.d/20-vcac.cfg` 进行编辑。

2 在前端部分中找到以下行：

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

3 在上一步中找到的行前面添加以下行：

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

4 使用以下命令重新加载 HAProxy 配置。

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

配置服务器响应标头

作为安全性最佳做法，请将 vRealize Automation 系统配置为限制潜在攻击者可访问的信息。

在可能的范围内，最大程度地减少系统共享有关其标识和版本的信息。黑客和恶意操作者可以使用此信息针对您的 Web 服务器或版本发动攻击。

配置 Lighttpd 服务器响应标头

最佳做法是。为 vRealize Automation 设备 lighttpd 服务器创建一个空白服务器标头。

步骤

1 在文本编辑器中打开 `/opt/vmware/etc/lighttpd/lighttpd.conf` 文件。

2 在文件中添加 `server.tag = " "`。

3 保存更改并关闭文件。

4 通过运行 `# /opt/vmware/etc/init.d/vami-lighttp restart` 命令重新启动 lighttpd 服务器。

为 vRealize Automation 设备配置 TCServer 响应标头

最佳做法是，为用于 vRealize Automation 设备的 TCServer 响应标头创建一个自定义空白服务器标头，以便限制恶意攻击者获取重要信息。

步骤

1 在文本编辑器中打开 `/etc/vco/app-server/server.xml` 文件。

2 在每个 `<Connector>` 元素中添加 `server=" ".`

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

3 保存更改并关闭文件。

4 使用以下命令重新启动服务器。

```
service vco-server restart
```

配置 Internet Information Services 服务器响应标头

最佳做法是为与 Identity Appliance 结合使用的 Internet Information Services (IIS) 服务器创建一个自定义空白服务器标头，以便限制恶意攻击者获取重要信息。

步骤

1 在文本编辑器中打开 `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` 文件。

2 搜索 `RemoveServerHeader=0` 并将其更改为 `RemoveServerHeader=1.`

3 保存更改并关闭文件。

4 通过运行 `iisreset` 命令重新启动服务器。

后续步骤

通过从 IIS Manager 控制台的列表中移除 HTTP 响应标头，可以禁用 IIS X-Powered-By 标头。

1 打开 IIS Manager 控制台。

2 打开 HTTP 响应标头，然后将其从列表中移除。

3 通过运行 `iisreset` 命令重新启动服务器。

设置 vRealize Automation 设备会话超时

根据您公司的安全策略，在 vRealize Automation 设备上配置会话超时设置。

vRealize Automation 设备在用户不活动时的默认会话超时为 30 分钟。要调整此超时值以符合您组织的安全策略，请编辑 vRealize Automation 设备主机上的 `web.xml` 文件。

步骤

1 在文本编辑器中打开 `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` 文件。

2 查找 `session-config` 并设置会话超时值。请参见以下代码示例。

```
<!-- 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 通过运行以下命令重新启动服务器。

```
service vcac-server restart
```

管理不重要的软件

要最大程度地降低安全风险，请在 vRealize Automation 主机中移除或配置不重要的软件。

请根据制造商的建议和安全性最佳做法配置未移除的所有软件，从而最大限度地降低出现安全漏洞的可能性。

保护 USB 海量存储处理程序

保护 USB 海量存储处理程序，防止在使用 VMware 虚拟设备主机时它用作 USB 设备处理程序。潜在攻击者可能利用此处理程序破坏您的系统。

步骤

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

2 确保此文件中显示 `install usb-storage /bin/true` 行。

3 保存文件并关闭。

保护蓝牙协议处理程序

保护您虚拟设备主机上的蓝牙协议处理程序，防止潜在的攻击者利用它。

不必将蓝牙协议绑定到网络堆栈，这可能会增加主机的攻击面。

步骤

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

2 确保此文件中显示以下行。

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

3 保存文件并关闭。

保护流控制传输协议

默认情况下，阻止您的系统加载流控制传输协议 (Stream Control Transmission Protocol, SCTP)。潜在攻击者可能利用此协议破坏您的系统。

除非绝对需要，否则请将系统配置为阻止加载流控制传输协议 (SCTP) 模块。SCTP 是未使用的 IETF 标准化传输层协议。将此协议绑定到网络堆栈会增加主机的攻击面。未授权的本地进程可能会导致内核通过使用协议打开套接字来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 确保此文件中显示以下行。

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

3 保存文件并关闭。

保护数据报拥堵协议

在系统强化活动中，默认情况下，阻止您的虚拟设备主机加载数据报拥堵协议 (Datagram Congestion Protocol, DCCP)。潜在攻击者可能利用此协议破坏您的系统。

除非绝对需要，否则避免加载数据报拥堵协议 (DCCP) 模块。DCCP 是建议的传输层协议，目前未使用。将此协议绑定到网络堆栈会增加主机的攻击面。未授权的本地进程可能会导致内核通过使用协议打开套接字来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 确保文件中显示 DCCP 行。

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

3 保存文件并关闭。

保护网络桥接

默认情况下，阻止您的系统加载网络桥接模块。潜在攻击者可能利用此模块破坏您的系统。

除非绝对需要，否则请将系统配置为阻止加载网络。潜在攻击者可能利用它来绕过网络分区和安全措施。

步骤

1 在所有 VMware 虚拟设备主机上运行以下命令。

```
# rmmod bridge
```

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

3 确保此文件中显示以下行。

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

4 保存文件并关闭。

保护可靠数据报套接字协议

在系统强化活动中，默认情况下，阻止您的虚拟设备主机加载可靠数据报套接字协议 (Reliable Datagram Sockets Protocol, RDS)。潜在攻击者可能利用此协议破坏您的系统。

将可靠数据报套接字 (RDS) 协议绑定到网络堆栈会增加主机的攻击面。未授权的本地进程可能会导致系统通过使用协议打开套接字来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 确保此文件中显示 `install rds /bin/true` 行。

3 保存文件并关闭。

保护透明进程间通信协议

在系统强化活动中，默认情况下，阻止您的虚拟设备主机加载透明进程间通信协议 (Transparent Inter-Process Communication Protocol, TIPC)。潜在攻击者可能利用此协议破坏您的系统。

将透明进程间通信 (TIPC) 协议绑定到网络堆栈会增加主机的攻击面。未授权的本地进程可能会导致内核通过使用协议打开套接字来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 确保此文件中显示 `install tipc /bin/true` 行。

3 保存文件并关闭。

保护 Internet 数据包交换协议

默认情况下，阻止您的系统加载 Internet 数据包交换 (IPX) 协议。潜在攻击者可能利用此协议破坏您的系统。

除非绝对需要，否则避免加载 Internet 数据包交换 (IPX) 协议模块。IPX 协议是废弃的网络层协议。将此协议绑定到网络堆栈会增加主机的攻击面。未授权的本地进程可能会导致系统通过使用协议打开套接字来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 确保此文件中显示以下行。

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

3 保存文件并关闭。

保护 Appletalk 协议

默认情况下，阻止您的系统加载 Appletalk 协议。潜在攻击者可能利用此协议破坏您的系统。

除非绝对需要，否则避免加载 Appletalk 协议模块。将此协议绑定到网络堆栈会增加主机的攻击面。未授权的本地进程可能会导致系统通过使用协议打开套接字来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 确保此文件中显示以下行。

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

3 保存文件并关闭。

保护 DECnet 协议

默认情况下，阻止您的系统加载 DECnet 协议。潜在攻击者可能利用此协议破坏您的系统。

除非绝对需要，否则避免加载 DECnet 协议模块。将此协议绑定到网络堆栈会增加主机的攻击面。未授权的本地进程可能会导致系统通过使用协议打开套接字来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 确保此文件中显示以下行。

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

3 保存文件并关闭。

保护 Firewire 模块

默认情况下，阻止您的系统加载 Firewire 模块。潜在攻击者可能利用此协议破坏您的系统。

除非绝对需要，否则避免加载 Firewire 协议模块。

步骤

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

2 确保此文件中显示以下行。

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

3 保存文件并关闭。

保护基础架构即服务组件

强化系统时，需保护 vRealize Automation 基础架构即服务 (Infrastructure as a Service, IaaS) 组件及其主机，防止潜在攻击者利用它。

必须为 vRealize Automation 基础架构即服务 (IaaS) 组件及其所在主机配置安全设置。您必须设置或确认其他相关组件和应用程序的配置。在某些情况下，您可以验证现有设置；在其他情况下，您必须更改或添加相应的配置设置。

配置 NTP

作为安全性最佳做法，请在 vRealize Automation 生产环境中使用授权时间服务器，而不是主机时间同步。

在生产环境中，请禁用主机时间同步并使用授权时间服务器，以便准确跟踪用户操作以及通过审核和日志记录识别潜在的恶意攻击和入侵。

为正在传输的基础架构即服务数据配置 TLS

确保 vRealize Automation 部署使用强 TLS 协议保护基础架构即服务组件的传输通道。

安全套接字层 (SSL) 和最近开发的传输层安全 (TLS) 是加密协议，可帮助确保在不同系统组件之间进行网络通信时的系统安全。SSL 是一项旧标准，其诸多实施无法再针对潜在攻击提供足够的安全防御。已确定早期 SSL 协议（包括 SSLv2 和 SSLv3）存在严重漏洞。这些协议不再是安全协议。

根据您组织的安全策略，您可能还希望禁用 TLS 1.0。

注 在负载平衡器终止 TLS 时，还可以根据需要禁用 SSLv2、SSLv3 以及 TLS 1.0 和 1.1 等弱协议。

为 IaaS 启用 TLS 1.1 和 1.2 协议

在托管 IaaS 组件的所有虚拟机上启用并强制使用 TLS 1.1 和 1.2 协议。

步骤

1 单击**开始**，然后单击**运行**。

2 键入 Regedit，然后单击**确定**。

3 找到并打开以下注册表子项。

```
HKEY LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols
```

4 验证以下内容，并根据需要创建新条目。

- 如果“Protocols”下没有名称为“TLS 1.1”的子项，则创建一个。
- 如果“TLS 1.1”下没有名称为“Client”的子项，则创建一个。
- 如果“Client”子项中没有名称为“DisabledByDefault”的项，则创建一个类型为 DWORD 的项。
- 右键单击“DisabledByDefault”，选择“修改”，然后将其值设置为 0。
- 如果“Client”子项中没有名称为“Enabled”的项，则创建一个类型为 DWORD 的项。

- 右键单击“Enabled”，选择“修改”，然后将其值设置为 1。
- 如果“TLS 1.1”下没有名称为“Server”的子项，则创建一个。
- 如果“Server”子项中没有名称为“DisabledByDefault”的项，则创建一个类型为 DWORD 的项。
- 右键单击“DisabledByDefault”，选择“修改”，然后将其值设置为 0。
- 如果“Server”子项中没有名称为“Enabled”的项，则创建一个类型为 DWORD 的项。
- 右键单击“Enabled”，选择“修改”，然后将其值设置为 1。

5 对 TLS 1.2 协议重复上述步骤。

注 要强制使用 TLS 1.1 和 1.2，需要执行其他设置，如后续步骤中所述。

6 找到并打开以下注册表子项。

```
HKEY LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFrmework\v4.0.30319
```

7 验证以下内容，并根据需要创建新条目。

- 如果没有名称为“SchUseStrongCrypto”的 DWORD 条目，则创建该条目并将其值设置为 1。
- 如果没有名称为“SystemDefaultTlsVersions”的 DWORD 条目，则创建该条目并将其值设置为 1。

8 找到并打开以下注册表子项。

```
HKEY LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFrmework\v4.0.30319
```

9 验证以下内容，并根据需要创建新条目。

- 如果没有名称为“SchUseStrongCrypto”的 DWORD 条目，则创建该条目并将其值设置为 1。
- 如果没有名称为“SystemDefaultTlsVersions”的 DWORD 条目，则创建该条目并将其值设置为 1。

为 IaaS 禁用 SSL 3.0 和 TLS 1.0

为 IaaS 组件禁用 SSL 3.0 和废弃的 TLS 1.0 协议。

步骤

1 单击**开始**，然后单击**运行**。

2 键入 `Regedit`，然后单击**确定**。

3 找到并打开以下注册表子项。

```
HKEY LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols
```

4 验证以下内容，并根据需要创建新条目。

- 如果“Protocols”下没有名称为“SSL 3.0”的子项，则创建一个。
- 如果“SSL 3.0”下没有名称为“Client”的子项，则创建一个。

- 如果“Client”子项中没有名称为“DisabledByDefault”的项，则创建一个类型为 DWORD 的项。
- 右键单击“DisabledByDefault”，选择“修改”，然后将其值设置为 1。
- 右键单击“Enabled”，选择“修改”，然后将其值设置为 0。
- 如果“SSL 3.0”下没有名称为“Server”的子项，则创建一个。
- 如果“Server”子项中没有名称为“DisabledByDefault”的项，则创建一个类型为 DWORD 的项。
- 右键单击“DisabledByDefault”，选择“修改”，然后将其值设置为 1。
- 如果“Server”中没有名称为“Enabled”的项，则创建一个类型为 DWORD 的项。
- 右键单击“Enabled”，选择“修改”，然后将其值设置为 0。

5 对 TLS 1.0 协议重复上述步骤。

对 IaaS 禁用 TLS 1.0

为安全起见，请将 IaaS 配置为使用池化，并禁用 TLS 1.0。

有关详细信息，请参见 Microsoft 知识库文章 https://support.microsoft.com/en-us/kb/245030。

步骤

1 将 IaaS 配置为使用池化而不是 Web 套接字。

a 更新 Manager Services 配置文件 `C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config`，方法是在 <appSettings> 部分添加以下值：

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

b 重新启动 Manager Service（VMware vCloud Automation Center 服务）。

2 确认已在 IaaS 服务器上禁用 TLS 1.0。

a 以管理员身份运行注册表编辑器。

b 在注册表窗口中，导航到 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\`

c 右键单击“Protocols”并选择**新建 > 项**，然后输入 **`TLS 1.0`**。

d 在导航树中，右键单击刚创建的 TLS 1.0 项，并在弹出菜单中选择**新建 > 项**，然后输入 **`Client`**。

e 在导航树中，右键单击刚创建的 TLS 1.0 项，并在弹出菜单中选择**新建 > 项**，然后输入 **`Server`**。

f 在导航树的 TLS 1.0 下，右键单击 **Client**，然后单击**新建 > DWORD (32 位) 值** 并输入 **`DisabledByDefault`**。

g 在导航树的 TLS 1.0 下，选择 **Client**，并在右窗格中双击 **DisabledByDefault** DWORD，然后输入 **`1`**。

h 在导航树的 TLS 1.0 下，右键单击 **Server**，并选择**新建 > DWORD (32 位) 值**，然后输入 **Enabled**。

i 在导航树的 TLS 1.0 下，选择 **Server**，并在右窗格中双击 **Enabled** DWORD，然后输入 **0**。

j 重新启动 Windows Server。

配置 TLS 密码套件

为了确保最大安全性，您必须将 vRealize Automation 组件配置为使用强密码。服务器与浏览器之间协商的加密密码确定了 TLS 会话中使用的加密强度。要确保仅选择强密码，请在 vRealize Automation 组件中禁用弱密码。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，按合适的顺序配置所有密码。

不可接受的密码套件

禁用不提供身份验证的密码套件，如 NULL 密码套件、aNULL 或 eNULL。此外，禁用匿名 Diffie-Hellman 密钥交换 (ADH)、导出级别密码（EXP，包含 DES 的密码）、IDEA 密码套件和 RC4 密码套件，并禁止使用小于 128 位的密钥大小加密负载流量或将 MD5 用作负载流量的哈希机制。此外，还要确保使用 Diffie-Hellman (DHE) 密钥交换的密码套件处于禁用状态。

有关在 vRealize Automation 中禁用静态密钥密码的信息，请参见知识文库文章 71094。

确认主机服务器安全

作为安全性最佳做法，请确认基础架构即服务 (Infrastructure as a Service, IaaS) 主机服务器的安全配置。

Microsoft 提供了几种工具，帮助您确认主机服务器的安全。有关这些工具的最佳用法的相关指导，请联系 Microsoft 供应商。

确认主机服务器的安全基准

运行 Microsoft Baseline Security Analyzer (MBSA)，快速验证您的服务器是否具有最新的更新或热修补程序。您可以使用 MBSA 通过 Microsoft 安装缺少的安全修补程序，确保服务器始终使用 Microsoft 安全建议的最新版本。

从 Microsoft 网站下载最新版本的 MBSA 工具。

确认主机服务器的安全配置

使用 Windows 安全配置向导 (SCW) 和 Microsoft Security Compliance Manager (SCM) 工具包，确认已安全配置主机服务器。

从 Windows Server 的管理工具中运行 SCW。此工具可确定您的服务器角色和已安装的功能，包括网络连接、Windows 防火墙和注册表设置。将报告与 Windows Server 相关 SCM 的最新强化指导进行对比。根据结果，您可以精确调整每项功能的安全设置，例如，网络服务、帐户设置和 Windows 防火墙，并将这些设置应用到服务器。

您可以在 Microsoft Technet 网站上查找有关 SCW 工具的详细信息。

保护应用程序资源

作为安全性最佳做法，请确保所有相关的基础架构即服务文件均具有适当的权限。

针对基础架构即服务安装，检查基础架构即服务文件。在大多数情况下，每个文件夹的子文件夹和文件应与文件夹具有相同的设置。

目录或文件	组或用户	完全控制	修改	读取和执行	读取	写入
VMware\vCAC\Agents \<agent_name> \logs	系统	X	X	X	X	X
	管理员	X	X	X	X	X
	管理员	X	X	X	X	X
VMware\vCAC\Agents\ <agent_name> \temp	系统	X	X	X	X	X
	管理员	X	X	X	X	X
	管理员	X	X	X	X	X
VMware\vCAC\Agents\	系统	X	X	X	X	X
	管理员	X	X	X	X	X
	用户			X	X	
VMware\vCAC\Distributed Execution Manager\	系统	X	X	X	X	X
	管理员	X	X	X	X	X
	用户			X	X	
VMware\vCAC\Distributed Execution Manager\DEM\Logs	系统	X	X	X	X	X
	管理员	X	X	X	X	X
	管理员	X	X	X	X	X
VMware\vCAC\Distributed Execution Manager\DEO\Logs	系统	X	X	X	X	X
	管理员	X	X	X	X	X
	管理员	X	X	X	X	X
VMware\vCAC\Management Agent\	系统	X	X	X	X	X
	管理员	X	X	X	X	X
	用户			X	X	
VMware\vCAC\Server\	系统	X	X	X	X	X
	管理员	X	X	X	X	X
	用户			X	X	
VMware\vCAC\Web API	系统	X	X	X	X	X
	管理员	X	X	X	X	X
	用户			X	X	

保护基础架构即服务主机

作为安全性最佳做法，请检查基础架构即服务 (IaaS) 主机上的基本设置，确保符合安全准则。

保护基础架构即服务 (IaaS) 主机上的其他帐户、应用程序、端口和服务。

确认服务器用户帐户设置

确认不存在不必要的本地和域用户帐户和设置。将与应用程序功能无关的所有用户帐户限制为管理、维护和故障排除所需的用户帐户。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访问权限。严格控制并审核这些帐户。

删除不必要的应用程序

从主机服务器中删除所有不必要的应用程序。不必要的应用程序包含未知或未修补的漏洞，会增加风险。

禁用不必要的端口和服务

检查主机服务器的防火墙，查看已打开的端口的列表。阻止 IaaS 组件或关键系统操作不需要的所有端口。请参见配置端口和协议。审核针对主机服务器运行的服务并禁用不必要的服务。

配置主机网络安全

8

为了最大限度地防御已知的安全威胁，请在所有 VMware 主机上配置网络接口和通信设置。

作为全面安全计划的一部分，请根据既定安全准则为 VMware 虚拟设备和基础架构即服务组件配置网络接口安全设置。

本章讨论了以下主题：

为 VMware 设备配置网络设置

要确保 VMware 虚拟设备主机仅支持安全通信和必要通信，请检查并编辑其网络通信设置。

检查 VMware 主机的网络 IP 协议配置，并根据安全准则配置网络设置。禁用所有不必要的通信协议。

防止用户控制网络接口

作为安全性最佳做法，请仅允许具有所需系统特权的用户在 VMware 设备主机上执行作业。

允许有特权的用户帐户操作网络接口可能会导致绕过网络安全机制或拒绝服务。限定只有特权用户才能更改网络接口设置。

步骤

1 在每个 VMware 设备主机上运行以下命令。

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

2 确保将每个接口设置为 NO。

设置 TCP 积压队列大小

要提供一定程度的防御以防止恶意攻击，请在 VMware 设备主机上配置默认的 TCP 积压队列大小。

请将 TCP 积压队列大小设置为适当的默认大小，以便消除 TCP 拒绝或服务攻击。建议的默认设置为 1280。

步骤

1 在每个 VMware 设备主机上运行以下命令。

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

2 在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 通过在文件中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
```

4 保存更改并关闭文件。

拒绝 ICMPv4 广播地址回显

作为安全性最佳做法，请确认 VMware 设备主机将忽略 ICMP 广播地址回显请求。

广播 Internet 控制消息协议 (ICMP) 回显的响应为放大攻击提供了攻击途径，使得恶意代理能够进行网络映射。将设备主机配置为忽略 ICMPv4 回显可防御此类攻击。

步骤

1 在 VMware 虚拟设备主机上运行 `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` 命令，确认这些主机拒绝 IPv4 广播地址回显请求。

如果主机已配置为拒绝 IPv4 重定向，此命令将为 `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` 返回值 0。

2 要将虚拟设备主机配置为拒绝 ICMPv4 广播地址回显请求，请在文本编辑器中打开 Windows 主机上的 `/etc/sysctl.conf` 文件。

3 找到 `net.ipv4.icmp_echo_ignore_broadcasts=0` 条目。如果此条目的值未设置为零或者不存在，请在文件中添加此条目或相应地更新现有条目。

4 保存更改并关闭文件。

禁用 IPv4 代理 ARP

如果 VMware 设备主机未要求，请确认禁用 IPv4 代理 ARP 以防止未经授权的信息共享。

IPv4 代理 ARP 允许系统代表连接到一个接口的主机在另一个接口上发送 ARP 请求响应。如果不需要，请将其禁用，以防泄漏连接网络段之间的寻址信息。

步骤

1 请在 VMware 虚拟设备主机上运行 `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp|egrep "default|all"` 命令，确认已禁用 IPv4 代理 ARP。

如果已在主机上禁用 IPv6 代理 ARP，则此命令将返回值 0。

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

如果主机配置正确，则不需要进一步操作。

2 如果需要在主机上配置 IPv6 代理 ARP，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 查找以下条目。

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

如果条目不存在或其值未设置为零，请在文件中添加这些条目或相应地更新现有条目。

4 保存您所做的任何更改并关闭文件。

拒绝 IPv4 ICMP 重定向消息

作为安全性最佳做法，请确认 VMware 虚拟设备主机拒绝 IPv4 ICMP 重定向消息。

路由器使用 ICMP 重定向消息告知主机某个目标存在更直接的路由。恶意的 ICMP 重定向消息可为中间人攻击提供便利。这些消息未经身份验证，并且会修改主机的路由表。确保系统已配置为在不需要这些消息时忽略消息。

步骤

1 在 VMware 设备主机上运行 `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep "default|all"` 命令，确认这些主机拒绝 IPv4 重定向消息。

如果主机已配置为拒绝 IPv4 重定向，此命令将返回以下内容：

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

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

2 如果需要将虚拟设备主机配置为拒绝 IPv4 重定向消息，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 检查以 `net.ipv4.conf` 开头的行的值。

如果以下条目的值未设置为零或者不存在，请在文件中添加这些条目或相应地更新现有条目。

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

4 保存所做的更改并关闭文件。

拒绝 IPv6 ICMP 重定向消息

作为安全性最佳做法，请确认 VMware 虚拟设备主机拒绝 IPv6 ICMP 重定向消息。

路由器使用 ICMP 重定向消息告知主机某个目标存在更直接的路由。恶意的 ICMP 重定向消息可为中间人攻击提供便利。这些消息未经身份验证，并且会修改主机的路由表。确保系统已配置为在不需要时忽略这些消息。

步骤

1 在 VMware 虚拟设备主机上运行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects|egrep "default|all"` 命令，确认这些主机拒绝 IPv6 重定向消息。

如果主机已配置为拒绝 IPv6 重定向，此命令将返回以下内容：

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

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

2 要将虚拟设备主机配置为拒绝 IPv4 重定向消息，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 检查以 `net.ipv6.conf` 开头的行的值。

如果以下条目的值未设置为零或者不存在，请在文件中添加这些条目或相应地更新现有条目。

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

4 保存更改并关闭文件。

记录 IPv4 Martian 数据包

作为安全性最佳做法，请确认 VMware 虚拟设备主机记录 IPv4 Martian 数据包。

Martian 数据包中包含系统已知无效的地址。将主机配置为记录这些消息，以便识别配置错误或正在进行的攻击。

步骤

1 在 VMware 设备主机上运行 `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians|egrep "default|all"` 命令，确认这些主机记录 IPv4 Martian 数据包。

如果虚拟机已配置为记录 Martian 数据包，它们将返回以下内容：

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

如果主机配置正确，则不需要进一步操作。

2 如果需要将虚拟机配置为记录 IPv4 martian 数据包，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 查看以 `net.ipv4.conf` 开头的行的值。

如果以下条目的值未设置为 1 或者条目不存在，请在文件中添加这些条目或相应地更新现有条目。

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

4 保存更改并关闭文件。

使用 IPv4 反向路径筛选

作为安全性最佳做法，请确认 VMware 虚拟设备主机使用 IPv4 反向路径筛选。

反向路径筛选可使系统丢弃源地址无路由或路由不指向原始接口的数据包，从而防止假冒的源地址。将主机配置为尽可能使用反向路径筛选。在某些情况下，反向路径筛选可能会因系统角色而导致系统丢弃合法流量。如果遇到此类问题，您可能需要使用限制性更弱的模式或完全禁用反向路径筛选。

步骤

1 请在 VMware 虚拟设备主机上运行 `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"` 命令，确认这些主机使用 IPv4 反向路径筛选。

如果虚拟机使用 IPv4 反向路径筛选，此命令将返回以下内容：

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

如果虚拟机配置正确，则不需要进一步操作。

2 如果需要在主机上配置 IPv4 反向路径筛选，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 检查以 `net.ipv4.conf` 开头的行的值。

如果以下条目的值未设置为 1 或者不存在，请在文件中添加这些条目或相应地更新现有条目。

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

4 保存更改并关闭文件。

拒绝 IPv4 转发

确认 VMware 设备主机拒绝 IPv4 转发。

如果系统已配置为使用 IP 转发且不是指定的路由器，则攻击者可将其用于为网络设备未筛选的通信提供路径，从而绕过网络安全措施。要避免此风险，请将虚拟设备主机配置为拒绝 IPv4 转发。

步骤

1 在 VMware 设备主机上运行 `# cat /proc/sys/net/ipv4/ip_forward` 命令，确认这些主机拒绝 IPv4 转发。

如果主机已配置为拒绝 IPv4 转发，此命令将为 `/proc/sys/net/ipv4/ip_forward` 返回值 0。如果虚拟机配置正确，则不需要进一步操作。

2 要将虚拟设备主机配置为拒绝 IPv4 转发，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 找到 `net.ipv4.ip_forward=0` 条目。如果此条目的值当前未设置为零或者不存在，请在文件中添加此条目或相应地更新现有条目。

4 保存所有更改并关闭文件。

拒绝 IPv6 转发

作为安全性最佳做法，请确认 VMware 设备主机系统拒绝 IPv6 转发。

如果系统已配置为使用 IP 转发且不是指定的路由器，则攻击者可将其用于为网络设备未筛选的通信提供路径，从而绕过网络安全措施。要避免此风险，请将虚拟设备主机配置为拒绝 IPv6 转发。

步骤

1 在 VMware 设备主机上运行 `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding|egrep "default|all"` 命令，确认这些主机拒绝 IPv6 转发。

如果主机已配置为拒绝 IPv6 转发，此命令将返回以下内容：

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

如果主机配置正确，则不需要进一步操作。

2 如果需要将主机配置为拒绝 IPv6 转发，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 检查以 `net.ipv6.conf` 开头的行的值。

如果以下条目的值未设置为零或者条目不存在，请在文件中添加这些条目或相应地更新现有条目。

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

4 保存您所做的任何更改并关闭文件。

使用 IPv4 TCP Syncookies

确认 VMware 设备主机使用 IPv4 TCP Syncookies。

TCP SYN 洪水攻击会使系统的 TCP 连接表被 SYN_RCVD 状态的连接填充，导致服务被拒绝。Syncookies 会持续阻止跟踪连接，直到收到后续应答，确认启动器正尝试进行有效连接且不是洪水攻击源。此方法不会以完全符合标准的方式运行，而是仅在洪水状况下激活，它允许保护系统并能够继续处理有效请求。

步骤

1 请在 VMware 设备主机上运行 `# cat /proc/sys/net/ipv4/tcp_syncookies` 命令，确认这些主机使用 IPv4 TCP Syncookies。

如果主机已配置为拒绝 IPv4 转发，此命令将为 `/proc/sys/net/ipv4/tcp_syncookies` 返回值 1。如果虚拟机配置正确，则不需要进一步操作。

2 如果需要将虚拟设备配置为使用 IPv4 TCP Syncookies，请在文本编辑器中打开 `/etc/sysctl.conf`。

3 找到 `net.ipv4.tcp_syncookies=1` 条目。

如果此条目的值当前未设置为 1 或者不存在，请添加该条目或相应更新现有条目。

4 保存您所做的任何更改并关闭文件。

拒绝 IPv6 路由器通告

确认 VMware 主机仅在系统操作需要时接受路由器通告和 ICMP 重定向。

IPv6 使系统能够自动使用网络信息来配置其网络设备。从安全角度来说，手动配置重要的配置信息比以未经身份验证的方式接受这些信息安全。

步骤

1 在 VMware 设备主机上运行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra|egrep "default|all"` 命令，确认这些主机拒绝路由器通告。

如果主机已配置为拒绝 IPv6 路由器通告，此命令将返回值 0：

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

如果主机配置正确，则不需要进一步操作。

2 如果需要将主机配置为拒绝 IPv6 路由器通告，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 查找以下条目。

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

如果这些条目不存在或其值未设置为零，请在文件中添加这些条目或相应地更新现有条目。

4 保存您所做的任何更改并关闭文件。

拒绝 IPv6 路由器请求

作为安全性最佳做法，请确认 VMware 设备主机仅在系统操作需要时接受 IPv6 路由器请求。

路由器请求设置将确定打开接口时发送的路由器请求数。如果地址是静态分配的，则无需发送任何请求。

步骤

1 在 VMware 设备主机上运行 `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations|egrep "default|all"` 命令，确认这些主机拒绝 IPv6 路由器请求。

如果主机已配置为拒绝 IPv6 路由器通告，此命令将返回以下内容：

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

如果主机配置正确，则不需要进一步操作。

2 如果需要将主机配置为拒绝 IPv6 路由器请求，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 查找以下条目。

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

如果条目不存在或其值未设置为零，请在文件中添加这些条目或相应地更新现有条目。

4 保存所有更改并关闭文件。

拒绝路由器请求中的 IPv6 路由器首选项

确认 VMware 设备主机仅在系统操作需要时接受 IPv6 路由器请求。

请求设置中的路由器首选项将确定路由器首选项。如果地址是静态分配的，则无需接收请求的任何路由器首选项。

步骤

1 在 VMware 设备主机上运行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref| egrep "default|all"` 命令，确认这些主机拒绝 IPv6 路由器请求。

如果主机已配置为拒绝 IPv6 路由器通告，此命令将返回以下内容：

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

如果主机配置正确，则不需要进一步操作。

2 如果需要将主机配置为拒绝 IPv6 路由请求，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 查找以下条目。

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

如果条目不存在或其值未设置为零，请在文件中添加这些条目或相应地更新现有条目。

4 保存您所做的任何更改并关闭文件。

拒绝 IPv6 路由器前缀

确认 VMware 设备主机仅在系统操作需要时接受 IPv6 路由器前缀信息。

`accept_ra_pinfo` 设置控制系统是否接受路由器前缀信息。如果地址是静态分配的，则无需检索任何路由器前缀信息。

步骤

1 在 VMware 设备主机上运行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo| egrep "default|all"` 命令，确认这些主机拒绝 IPv6 路由器前缀信息。

如果主机已配置为拒绝 IPv6 路由器通告，此命令将返回以下内容：

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

如果主机配置正确，则不需要进一步操作。

2 如果需要将主机配置为拒绝 IPv6 路由器前缀信息，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 查找以下条目。

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

如果条目不存在或其值未设置为零，请在文件中添加这些条目或相应地更新现有条目。

4 保存所有更改并关闭文件。

拒绝 IPv6 路由器通告跃点限制设置

确认 VMware 设备主机仅在必要时接受 IPv6 路由器跃点限制设置。

`accept_ra_defrtr` 设置控制系统是否接受路由器通告跃点限制设置。将其设置为零可防止路由器更改出站数据包的默认 IPv6 跃点限制。

步骤

1 在 VMware 设备主机上运行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr|egrep "default|all"` 命令，确认这些主机拒绝 IPv6 路由器跃点限制设置。

如果主机已配置为拒绝 IPv6 路由器跃点限制设置，此命令将返回值 0。

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

如果主机配置正确，则不需要进一步操作。

2 如果需要将主机配置为拒绝 IPv6 路由器跃点限制设置，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 查找以下条目。

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

如果条目不存在或其值未设置为零，请在文件中添加这些条目或相应地更新现有条目。

4 保存您所做的任何更改并关闭文件。

拒绝 IPv6 路由器通告 Autoconf 设置

确认 VMware 设备主机仅在必要时接受 IPv6 路由器 autoconf 设置。

`autoconf` 设置控制路由器通告是否可能会导致系统为接口分配全局单播地址。

步骤

1 在 VMware 设备主机上运行 `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf|egrep "default|all"` 命令，确认这些主机拒绝 IPv6 路由器 autoconf 设置。

如果主机已配置为拒绝 IPv6 路由器 autoconf 设置，此命令将返回值 0。

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

如果主机配置正确，则不需要进一步操作。

2 如果需要将主机配置为拒绝 IPv6 路由器 autoconf 设置，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 查找以下条目。

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

如果条目不存在或其值未设置为零，请在文件中添加这些条目或相应地更新现有条目。

4 保存您所做的任何更改并关闭文件。

拒绝 IPv6 邻居请求

确认 VMware 设备主机仅在必要时接受 IPv6 邻居请求。

`dad_transmits` 设置将确定打开接口时每个地址（全局和本地链接）发出的邻居请求数，确保网络上的所需地址唯一。

步骤

1 在 VMware 设备主机上运行 `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits|egrep "default|all"` 命令，确认这些主机拒绝 IPv6 邻居请求。

如果主机已配置为拒绝 IPv6 邻居请求，此命令将返回值 0。

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

如果主机配置正确，则不需要进一步操作。

2 如果需要将主机配置为拒绝 IPv6 邻居请求，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 查找以下条目。

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

如果条目不存在或其值未设置为零，请在文件中添加这些条目或相应地更新现有条目。

4 保存您所做的任何更改并关闭文件。

限制 IPv6 最大地址数

确认 VMware 设备主机将 IPv6 最大地址设置限制为系统操作所需的最小值。

最大地址数设置将确定每个接口可使用的全局单播 IPv6 地址数。默认值为 16，但您应准确设置为系统所需的静态配置全局地址数。

步骤

1 请在 VMware 设备主机上运行 `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses|egrep "default|all"` 命令，确认这些主机已相应限制 IPv6 最大地址数。

如果主机已配置为限制 IPv6 最大地址数，则此命令将返回值 1。

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

如果主机配置正确，则不需要进一步操作。

2 如果需要在主机上配置 IPv6 最大地址数，请在文本编辑器中打开 `/etc/sysctl.conf` 文件。

3 查找以下条目。

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

如果条目不存在或其值未设置为 1，请在文件中添加这些条目或相应地更新现有条目。

4 保存您所做的任何更改并关闭文件。

为基础架构即服务主机配置网络设置

作为安全性最佳做法，请根据 VMware 要求和准则为 VMware 基础架构即服务 (IaaS) 组件主机配置网络通信设置。

采用适当的安全措施配置基础架构即服务 (IaaS) 主机的网络配置，使其支持完整的 vRealize Automation 功能。

请参见保护基础架构即服务组件。

配置端口和协议

作为安全性最佳做法，请根据 VMware 准则为所有 vRealize Automation 设备和组件配置端口和协议。

根据需要为 vRealize Automation 组件配置入站和出站端口，以便关键系统组件在生产环境中正常运行。禁用所有不需要的端口和协议。请参见 VMware vRealize Automation 文档中的《vRealize Automation 参考架构》。

“端口和协议”工具

通过“端口和协议”工具，您可以在单个仪表板上查看各种 VMware 产品及其组合的端口信息。您还可以从该工具中导出选定的数据，以便进行脱机访问。“端口和协议”工具当前支持：

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

该工具可在 https://ports.vmware.com/ 上找到。

用户所需的端口

作为安全性最佳做法，请根据 VMware 准则配置 vRealize Automation 用户端口。

只能通过安全网络公开所需的端口。

服务器	端口
vRealize Automation 设备	443、8443

管理员所需的端口

作为安全性最佳做法，请根据 VMware 准则配置 vRealize Automation 管理员端口。

只能通过安全网络公开所需的端口。

服务器	端口
vRealize Application Services 服务器	5480

vRealize Automation 设备端口

作为安全性最佳做法，请根据 VMware 建议为 vRealize Automation 设备 配置入站和出站端口。

入站端口

为 vRealize Automation 设备 配置所需的最少入站端口数。配置可选端口数（如果系统配置需要）。

表 8-1. 所需的最少入站端口数

端口	协议	备注
443	TCP	访问 vRealize Automation 控制台和 API 调用。
8443	TCP	VMware Remote Console 代理。
5480	TCP	访问 vRealize Automation 设备管理界面。
5488, 5489	TCP	内部。由 vRealize Automation 设备 用于更新。
5672	TCP	RabbitMQ 消息传递。 注 将 vRealize Automation 设备 实例加入群集时，您可能需要配置打开的端口 4369 和 25672。
40002	TCP	vIDM 服务所必需的端口。这是所有外部流量的防火墙，但在 HP 配置中添加的其他 vRealize Automation 设备 节点的流量除外。

如有必要，请配置可选的入站端口。

表 8-2. 可选的入站端口

端口	协议	备注
22	TCP	（可选）SSH。在生产环境中，禁用端口 22 上的 SSH 服务侦听并关闭端口 22。
80	TCP	（可选）重定向到 443。

出站端口

配置所需的出站端口。

表 8-3. 所需的最少出站端口数

端口	协议	备注
25,587	TCP、UDP	用于发送出站通知电子邮件的 SMTP。
53	TCP、UDP	DNS。
67, 68, 546, 547	TCP、UDP	DHCP。
110, 995	TCP、UDP	用于接收入站通知电子邮件的 POP。
143, 993	TCP、UDP	用于接收入站通知电子邮件的 IMAP。
443	TCP	通过 HTTPS 的基础架构即服务 Manager Service。

如有必要，请配置可选的出站端口。

表 8-4. 可选的出站端口

端口	协议	备注
80	TCP	（可选）用于获取软件更新。您可以单独下载并应用更新。
123	TCP、UDP	（可选）用于直接连接到 NTP，而非使用主机时间。

“端口和协议”工具

通过“端口和协议”工具，您可以在单个仪表板上查看各种 VMware 产品及其组合的端口信息。您还可以从该工具中导出选定的数据，以便进行脱机访问。“端口和协议”工具当前支持：

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

这些工具可在 https://ports.vmware.com/ 上找到。

基础架构即服务端口

作为安全性最佳做法，请根据 VMware 准则为基础架构即服务 (Infrastructure as a Service, IaaS) 组件配置入站和出站端口。

入站端口

配置 IaaS 组件所需的最少入站端口数。

表 8-5. 所需的最少入站端口数

组件	端口	协议	备注
Manager Service	443	TCP	通过 HTTPS 与 IaaS 组件和 vRealize Automation 设备通信。代理程序管理的所有虚拟化主机还必须对入站流量打开 TCP 端口 443

出站端口

配置 IaaS 组件所需的最少出站端口数。

表 8-6. 所需的最少出站端口数

组件	端口	协议	备注
全部	53	TCP、UDP	DNS。
全部		TCP、UDP	DHCP。
Manager Service	443	TCP	通过 HTTPS 与 vRealize Automation 设备通信。
网站	443	TCP	通过 HTTPS 与 Manager Service 通信。
Distributed Execution Manager	443	TCP	通过 HTTPS 与 Manager Service 通信。
代理程序	443	TCP	通过 HTTPS 与 Manager Service 和虚拟化主机通信。
客户机代理	443	TCP	通过 HTTPS 与 Manager Service 通信。
Manager Service、Website	1433	TCP	MSSQL。

需要时，配置可选的出站端口。

表 8-7. 可选的出站端口

组件	端口	协议	备注
全部	123	TCP、UDP	NTP 是可选的。

9 审核和日志记录

作为安全性最佳做法，请根据 VMware 建议在 vRealize Automation 系统上设置审核和日志记录。

将日志远程记录到中央日志主机可以安全地存储日志文件。通过将日志文件收集到中央主机，可以通过单个工具监控环境。此外，还可以执行汇总分析和搜索威胁痕迹，例如对基础架构内多个实体的协同攻击。将日志记录到安全的集中式日志服务器不但有助于防止日志被篡改，而且能够提供长期的审核记录。

确保远程日志记录服务器安全可靠

通常，攻击者在破坏主机安全之后，会尝试搜索并篡改日志文件，以掩盖其攻击行为并保持控制而不被发现。保护远程日志记录服务器有助于防止日志被篡改。

使用授权的 NTP 服务器

确保所有主机均使用相同的相对时间源（包括相关本地化偏移），且相对时间源可与商定的时间标准（如协调世界时 (UTC)）相互关联。使用规范时间源可以在检查相关日志文件时快速跟踪和关联入侵者的操作。不正确的时间设置可能难以检查和关联日志文件以检测攻击，且可能使得审核不准确。

至少使用三个外部时间源 NTP 服务器，或在受信任的网络上配置一些本地 NTP 服务器，以便至少从三个外部时间源获取时间。