

Oracle® Server X6-2 安全指南



文件号码 E73676-01
2016 年 4 月

文件号码 E73676-01

版权所有 © 2016, Oracle 和/或其附属公司。保留所有权利。

本软件和相关文档是根据许可证协议提供的，该许可证协议中规定了关于使用和公开本软件和相关文档的各种限制，并受知识产权法的保护。除非在许可证协议中明确许可或适用法律明确授权，否则不得以任何形式、任何方式使用、拷贝、复制、翻译、广播、修改、授权、传播、分发、展示、执行、发布或显示本软件和相关文档的任何部分。除非法律要求实现互操作，否则严禁对本软件进行逆向工程设计、反汇编或反编译。

此文档所含信息可能随时被修改，恕不另行通知，我们不保证该信息没有错误。如果贵方发现任何问题，请书面通知我们。

如果将本软件或相关文档交付给美国政府，或者交付给以美国政府名义获得许可证的任何机构，则适用以下注意事项：

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

本软件或硬件是为了在各种信息管理应用领域内的一般使用而开发的。它不应被应用于任何存在危险或潜在危险的应用领域，也不是为此而开发的，其中包括可能会产生人身伤害的应用领域。如果在危险应用领域内使用本软件或硬件，贵方应负责采取所有适当的防范措施，包括备份、冗余和其它确保安全使用本软件或硬件的措施。对于因在危险应用领域内使用本软件或硬件所造成的一切损失或损害，Oracle Corporation 及其附属公司概不负责。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。其他名称可能是各自所有者的商标。

Intel 和 Intel Xeon 是 Intel Corporation 的商标或注册商标。所有 SPARC 商标均是 SPARC International, Inc 的商标或注册商标，并应按照许可证的规定使用。AMD、Opteron、AMD 徽标以及 AMD Opteron 徽标是 Advanced Micro Devices 的商标或注册商标。UNIX 是 The Open Group 的注册商标。

本软件或硬件以及文档可能提供了访问第三方内容、产品和服务的方式或有关这些内容、产品和服务的信息。除非您与 Oracle 签订的相应协议另行规定，否则对于第三方内容、产品和服务，Oracle Corporation 及其附属公司明确表示不承担任何种类的保证，亦不对其承担任何责任。除非您和 Oracle 签订的相应协议另行规定，否则对于因访问或使用第三方内容、产品或服务所造成的任何损失、成本或损害，Oracle Corporation 及其附属公司概不负责。

文档可访问性

有关 Oracle 对可访问性的承诺，请访问 Oracle Accessibility Program 网站 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>。

获得 Oracle 支持

购买了支持服务的 Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>；如果您听力受损，请访问 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>。

目录

基本安全	7
访问	7
验证	8
授权	8
记帐和审计	8
安全使用服务器配置和管理工具	9
Oracle ILOM 安全性	9
Oracle Hardware Management Pack 安全性	10
规划安全环境	13
密码保护	13
操作系统安全指南	14
网络交换机和端口	14
VLAN 安全性	15
InfiniBand 安全性	15
维护安全环境	17
电源控制	17
资产跟踪	17
软件和固件更新	18
网络安全性	18
数据保护和安全	19
日志维护	20

基本安全

本文档提供了若干一般安全准则，来帮助您保护 Oracle 服务器、服务器网络接口及其连接的网络交换机。

有关您所用系统和特定环境的其他安全要求，请联系您的 IT 安全主管。

在使用所有硬件和软件时，应遵循一些基本安全原则。本节介绍了以下四个基本安全原则：

- [“访问” \[7\]](#)
- [“验证” \[8\]](#)
- [“授权” \[8\]](#)
- [“记帐和审计” \[8\]](#)

访问

访问是指对硬件的物理访问，或对软件的物理或虚拟访问。

- 使用物理和软件控制措施来保护硬件和数据免遭入侵。
- 安装新系统时更改所有默认密码。大多数类型的设备都使用默认密码（如 changeme），这些密码广为人知，从而可能允许对硬件或软件进行未经授权的访问。
- 参阅软件随附的文档，启用可用于软件的任何安全功能。
- 在带锁的受限通道空间内安装服务器和相关设备。
- 如果设备安装在带有门锁的机架中，除非必须维修机架内的组件，否则请始终锁上机架门。
- 限制人员接近 USB 端口和控制台。一些设备（如系统控制器、配电设备 (Power Distribution Unit, PDU) 和网络交换机）具有 USB 连接，这些连接可以提供对系统的直接访问。由于物理访问不容易遭受网络攻击，因此是一种较安全的组件访问方法。
- 限制通过网络重新启动系统的能力。
- 尤其要限制人员接近热插拔或热交换设备，因为这些设备可以轻易被移除。
- 在带锁的机柜中存储备用现场可更换单元 (Field-Replaceable Unit, FRU) 和客户可更换单元 (Customer-Replaceable Unit, CRU)。仅限经授权的人员操作带锁机柜。

验证

验证就是识别用户的身份，通常是通过用户名和密码等保密信息来进行。验证可确保硬件或软件的用户与其表明的身份相符。

- 在平台操作系统中设置验证功能（如密码系统）以确保用户与其表明的身份相符。
- 确保人员正确使用员工胸卡进入机房。
- 对于用户帐户：酌情使用访问控制列表；对扩展会话设置超时；为用户设置特权级别。

授权

管理员可以通过授权来控制用户可执行或使用哪些任务或权限。用户只能执行为其分配的任务，并使用为其分配的权限。授权是指对人员使用硬件或软件施加的限制。

- 只允许员工使用他们经过培训并有资格使用的硬件和软件。
- 建立一套读/写/执行权限制度，以控制用户对命令、磁盘空间、设备和应用程序的访问。

记帐和审计

记帐和审计指的是维护用户在系统中执行的活动的记录。利用 Oracle 服务器的相关软件和硬件功能，管理员可以监视登录活动并维护硬件清单。

- 使用系统日志来监视用户登录。尤其要监视系统管理员和服务帐户，因为这些帐户可以访问一些特定的命令，如果这些命令使用不当，可能导致系统损坏或造成数据丢失。访问活动和命令应该通过系统日志进行细致监控。
- 记录所有硬件的序列号。使用组件序列号来跟踪系统资产。Oracle 部件号以电子方式记录在卡、模块和主板上，并可用于库存目的。
- 为了检测和跟踪组件，为计算机硬件的所有重要物项（如 FRU 和 CRU）提供安全标记。使用特殊的紫外线笔或压纹标签。
- 将硬件激活密钥和许可证保存在易于系统管理员获取的安全位置，尤其是在系统出现紧急情况期间。打印的文档可能是证明所有权的唯一证据。

安全使用服务器配置和管理工具

在使用软件和固件工具来配置和管理服务器时，请遵循以下各节中的安全准则：

- [“Oracle ILOM 安全性” \[9\]](#)
- [“Oracle Hardware Management Pack 安全性” \[10\]](#)

有关您所用系统和特定环境的其他安全要求，请联系您的 IT 安全主管。

Oracle ILOM 安全性

您可以使用 Oracle Integrated Lights Out Manager (ILOM) 管理固件（已嵌入到基于 x86 的 Oracle 服务器以及基于 SPARC 的 Oracle 服务器上）来主动保护、管理和监视系统组件。根据授予系统管理员的授权级别，这些功能可能包括关闭服务器电源、创建用户帐户、挂载远程存储设备等。

- **使用安全的内部可信网络。**
无论通过本地串行端口、专用网络管理端口、边带管理端口还是标准数据网络端口与 Oracle ILOM 建立物理管理连接，服务器上的此物理端口要始终连接到内部的可信网络或者专用安全管理或专用网络，这一点至关重要。
绝不要将 Oracle ILOM 服务处理器 (service processor, SP) 连接到公共网络，比如 Internet。应确保 Oracle ILOM SP 管理通信始终位于单独的管理网络上并仅授予系统管理员访问权限。
- **限制对默认管理员帐户的使用。**
将默认管理员帐户 (root) 限定为仅用于 Oracle ILOM 初始登录。提供此默认管理员帐户只是为了帮助进行服务器初始安装。因此，为了确保环境最安全，必须在最初设置系统的过程中更改此默认管理员的密码 (changeme)。如果获得了访问默认管理员帐户的权限，用户将可以无限制地访问 Oracle ILOM 的所有功能。此外，还要为每个新的 Oracle ILOM 用户设立新用户帐户并指定唯一密码和授权级别（用户角色）。
- **仔细考虑将串行端口连接到终端服务器的风险。**
终端设备并不能始终提供适当级别的用户验证或授权，而这些是保护网络免受恶意入侵所需的。为了保护系统免受意外的网络入侵，请不要通过任何类型的网络重定向设备（比如终端服务器）与 Oracle ILOM 建立串行连接（通过串行端口），除非服务器具有足够的访问控制能力。

此外，诸如密码重置和 "Preboot" 菜单等某些 Oracle ILOM 功能只能通过物理串行端口使用。如果使用未经验证的终端服务器将串行端口连接到网络，则无需进行物理访问，并且会降低与这些功能相关的安全性。

- 访问 "Preboot" 菜单需要对服务器进行物理访问。

Oracle ILOM 的 "Preboot" 菜单是一个强大的实用程序，可将 Oracle ILOM 重置为默认值，或者在 Oracle ILOM 不响应时重置闪存固件。在 Oracle ILOM 重置之后，用户将需要按下服务器上的按钮（默认方式）或键入密码才能访问。Oracle ILOM 的 "Physical Presence" 属性可控制此行为 (`check_physical_presence= true`)。为了在访问 "Preboot" 菜单时实现最高的安全性，请不要更改该属性的默认设置 (`true`)，以便访问 "Preboot" 菜单时始终需要对服务器进行物理访问。

- 参阅 Oracle ILOM 文档。

请参阅 Oracle ILOM 文档，以更详细地了解如何设置密码、管理用户以及应用与安全相关的功能，包括安全 Shell (Secure Shell, SSH)、安全套接字层 (Secure Socket Layer, SSL) 和 RADIUS 验证。有关特定于 Oracle ILOM 的安全准则，请参阅 Oracle ILOM 文档库中的《Oracle ILOM 安全指南》。您可以在以下位置找到 Oracle ILOM 文档：

<http://www.oracle.com/goto/ilom/docs>

Oracle Hardware Management Pack 安全性

Oracle Hardware Management Pack 可用于您的服务器，以及许多基于 x86 的其他 Oracle 服务器和某些基于 SPARC 的 Oracle 服务器。Oracle Hardware Management Pack 采用两种组件（即 SNMP 监视代理和一系列跨操作系统的命令行界面工具 (command-line interface tools, CLI Tools)）来管理此服务器。您可以使用 Oracle Server CLI Tools 来配置 Oracle 服务器。CLI Tools 适用于 Oracle Solaris、Oracle Linux、Oracle VM、其他 Linux 变体以及 Microsoft Windows 操作系统。

- 使用 Hardware Management Agent SNMP Plugin。

SNMP 是用于监视或管理系统的标准协议。通过 Hardware Management Agent SNMP Plugin，您可以使用 SNMP 来监视数据中心中的 Oracle 服务器，其优点是不必连接到两个管理点，即主机和 Oracle ILOM。通过此功能，可以使用单个 IP 地址（主机的 IP 地址）来监视多个服务器。

SNMP Plugin 在 Oracle 服务器的主机操作系统上运行。SNMP Plugin 模块可扩展主机操作系统中的本机 SNMP 代理，以提供其他 Oracle MIB 功能。Oracle Hardware Management Pack 本身不包含 SNMP 代理。对于 Linux，模块将添加到 net-snmp 代理。对于 Oracle Solaris，模块将添加到 Oracle Solaris Management Agent。对于 Microsoft Windows，该插件可扩展本机 SNMP 服务。与 Oracle Hardware Management Pack 的 SNMP 相关的任何安全性设置均由本机 SNMP 代理或服务的设置（而不是插件）来决定。

请注意，SNMPv1 和 SNMPv2c 不提供加密，并且使用团体字符串作为验证形式。相比之下，SNMPv3 更为安全，是建议使用的版本，因为它使用加密来提供安全的通道并使用单独的用户名和密码。

- 参阅 Oracle Hardware Management Pack 文档。

有关这些功能的更多信息，请参阅 Oracle Hardware Management Pack 文档。有关特定于 Oracle Hardware Management Pack 的安全准则，请参阅 Oracle Hardware Management Pack 文档库中的《*Oracle Hardware Management Pack (HMP)* 安全指南》。您可以在以下位置找到 Oracle Hardware Management Pack 文档：

<http://www.oracle.com/goto/ohmp/docs>

规划安全环境

安全准则应在系统到位之前制定就绪。系统到位之后，应定期审核和调整安全准则，以便与组织当前的安全要求保持同步。

在对服务器及相关设备进行安装和配置之前和期间，请利用以下各节中提供的信息。

- [“密码保护” \[13\]](#)
- [“操作系统安全指南” \[14\]](#)
- [“网络交换机和端口” \[14\]](#)
- [“VLAN 安全性” \[15\]](#)
- [“InfiniBand 安全性” \[15\]](#)

有关您所用系统和特定环境的其他安全要求，请联系您的 IT 安全主管。

密码保护

密码是安全性的一个重要方面，因为如果选择的密码不安全，可能会导致有人未经授权便访问公司资源。实施密码管理最佳做法可以确保用户遵守创建和保护密码的一组准则。密码策略典型的几个部分应该定义以下内容：

- 密码长度和强度
- 密码期限
- 密码的常见做法

强制实施以下标准做法以创建强安全性的复杂密码：

- 不要创建包含用户名、员工姓名或家庭成员姓名的密码。
- 不要选择易于猜测的密码。
- 不要创建包含连续数字字符串（例如 12345）的密码。
- 创建的密码不得包含通过简单的 Internet 搜索便可轻松发现的单词或字符串。
- 不允许用户在多个系统中重复使用相同的密码。
- 不允许用户重复使用旧密码。

定期更改密码。这样有助于防止恶意行为，并且可以确保密码符合当前的密码策略。

操作系统安全指南

有关下列内容的信息，请参阅 Oracle 操作系统 (Operating System, OS) 文档：

- 配置系统时如何使用安全功能。
- 将应用程序和用户添加到系统时如何安全操作。
- 如何保护基于网络的应用程序。

受支持的 Oracle 操作系统的安全指南文档包含在该操作系统的文档库中。要获得某个 Oracle 操作系统的安全指南文档，请转到该 Oracle 操作系统文档库：

操作系统	链接
Oracle Solaris OS	http://www.oracle.com/technetwork/documentation/solaris-11-192991.html
Oracle Linux OS	http://www.oracle.com/technetwork/documentation/ol-1-1861776.html
Oracle VM	http://www.oracle.com/technetwork/documentation/vm-096300.html

有关其他供应商提供的操作系统（例如 Red Hat Enterprise Linux、SUSE Linux Enterprise Server、Microsoft Windows 和 VMware ESXi）的信息，请参阅相应供应商的文档。

网络交换机和端口

网络交换机提供不同级别的端口安全功能。请参阅交换机文档，了解如何执行下列操作：

- 针对交换机的本地和远程访问，使用验证、授权和记帐功能。
- 对于默认情况下可能有多个用户帐户和密码的网络交换机，更改其上的每个密码。
- 带外管理交换机（与数据通信隔开）。如果带外管理不可行，则专门使用一个单独的虚拟局域网 (Virtual Local Area Network, VLAN) 号进行带内管理。
- 对入侵检测系统 (Intrusion Detection System, IDS) 访问使用网络交换机的端口镜像功能。
- 脱机维护一份交换机配置文件，并且只限授权的管理员访问。该配置文件应包含每个设置的描述性注释。
- 实施端口安全性，以基于 MAC 地址限制访问。对所有端口禁用自动中继。
- 如果您的交换机具有以下端口安全功能，请使用这些功能：
 - **MAC 绑定 (MAC Locking)** – 涉及将一个或多个连接设备的介质访问控制 (Media Access Control, MAC) 地址与交换机的物理端口相关联。如果将交换机端口绑定到特定的 MAC 地址，超级用户将无法利用非法访问点在您的网络中创建后门。
 - **MAC 锁定 (MAC Lockout)** – 会禁止将指定的 MAC 地址连接到交换机。

- **MAC 学习 (MAC Learning)** – 使用有关每个交换机端口的直接连接的知识，以便可以基于当前连接设置网络交换机的安全性。

VLAN 安全性

如果设置了虚拟局域网 (Virtual Local Area Network, VLAN)，请记住，VLAN 会分享网络带宽，且需要其他安全措施。对于其他安全措施，请遵守以下准则：

- 使用 VLAN 时，请将敏感的系统群与网络的其余部分隔开。这样可以降低用户访问这些客户机和服务器上信息的可能性。
- 为中继端口指定唯一的本机 VLAN 号。
- 将可通过中继传输的 VLAN 限定为仅用于必需的那些 VLAN。
- 如果可能，禁用 VLAN 中继协议 (VLAN Trunking Protocol, VTP)。否则，为 VTP 设置以下内容：管理域、密码和删改。然后将 VTP 设置为透明模式。
- 如果可能，使用静态 VLAN 配置。
- 禁用未使用的交换机端口，并为其指定未使用的 VLAN 号。

InfiniBand 安全性

要在使用 InfiniBand 时提高安全性，请遵循以下准则：

- 确保 InfiniBand 主机安全。InfiniBand 光纤网络的安全程度取决于其安全程度最低的 InfiniBand 主机。
- 请注意，分区不会保护 InfiniBand 光纤网络。分区只会使主机上各虚拟机之间的 InfiniBand 通信相互隔离。

维护安全环境

初始安装和设置之后，可以使用 Oracle 硬件和软件安全功能继续控制硬件和跟踪系统资产。

可使用以下各节中的信息维护安全的环境：

- “电源控制” [17]
- “资产跟踪” [17]
- “软件和固件更新” [18]
- “网络安全性” [18]
- “数据保护和安全” [19]
- “日志维护” [20]

有关您所用系统和特定环境的其他安全要求，请联系您的 IT 安全主管。

电源控制

可以使用软件来打开和关闭某些 Oracle 系统的电源。某些系统机柜的配电设备 (Power Distribution Unit, PDU) 可以远程进行启用和禁用。这些命令的授权通常在系统配置期间设置，并且通常仅限系统管理员和服务人员使用这些命令。

有关详细信息，请参阅系统或机柜文档。

资产跟踪

可使用序列号来跟踪清单。Oracle 在选件卡和系统主板上的固件中嵌入了序列号。可以通过局域网 (local area network, LAN) 连接读取这些序列号。

还可以使用无线射频识别 (wireless radio frequency identification, RFID) 读取器来进一步简化资产跟踪。可从以下位置获取 Oracle 白皮书《*How to Track Your Oracle Sun System Assets by Using RFID*》（《如何使用 RFID 跟踪 Oracle Sun 系统资产》）：

<http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf>

软件和固件更新

安全增强功能是通过新的软件发行版和修补程序引入的。有效、主动的修补程序管理是系统安全的重要部分。最佳的安全措施是，使用最新的软件发行版以及所有必要的安全修补程序对系统进行更新。

- 定期检查是否有软件或固件更新以及安全修补程序。
- 始终在设备上安装软件或固件的最新发行版本。
- 为您的软件安装所有必要的安全修补程序。
- 请记住，网络交换机之类的设备也包含固件，因此也可能需要修补程序和固件更新。

您可以在 My Oracle Support Web 站点上找到软件更新和安全修补程序，网址为：

<https://support.oracle.com>

网络安全性

在根据安全原则对网络进行配置后，需要定期进行检查和维护。

要保护对系统的本地和远程访问，请遵循以下准则：

- 使用 SSH（而非 Telnet）将远程配置限定为只有特定的 IP 地址才可以执行。Telnet 以明文形式传递用户名和密码，这可能使局域网 (Local Area Network, LAN) 段上的每个人都能看到登录凭据。为 SSH 设置强密码。
- 使用简单网络管理协议 (Simple Network Management Protocol, SNMP) 版本 3 来提供安全传输。SNMP 的早期版本不安全，它们以未加密文本形式传输验证数据。SNMPv3 使用加密提供安全的通道和单独的用户名和密码。
- 如果必须使用 SNMPv1 或 SNMPv2，请将默认的 SNMP 团体字符串更改为加强的团体字符串。某些产品将 PUBLIC 设置为默认 SNMP 团体字符串。攻击者可以查询团体以绘制非常完整的网络图，并可能修改管理信息库 (Management Information Base, MIB) 值。
- 如果系统控制器使用浏览器界面，请始终在使用后进行注销。
- 启用必要的网络服务并以安全方式配置这些服务。禁用不必要的网络服务，如传输控制协议 (Transmission Control Protocol, TCP) 或超文本传输协议 (Hypertext Transfer Protocol, HTTP)。
- 使用 LDAP 访问系统时，请使用 LDAP 安全措施。
- 创建在登录时显示的标题消息，声明禁止未经授权的访问。您可以向用户告知任何重要的策略或规则。可以使用标题向用户警示给定系统的特殊访问限制，或者向用户提醒密码策略及正确使用方式。
- 在适用情况下，使用访问控制列表实施限制。
- 设置扩展会话超时，并设置特权级别。

- 针对交换机的本地和远程访问，使用验证、授权和记帐功能。
- 在非常安全的环境中使用这些网络服务，因为它们由证书和其他形式的强加密保护，可以保护通道：
 - Active Directory
 - LDAP/SSL (Lightweight Directory Access Protocol/Secure Socket Layer，轻量目录访问协议/安全套接字层)
- 在没有可疑恶意用户的专用安全网络上使用这些网络服务：
 - RADIUS (Remote Authentication Dial In User Service，远程身份验证拨入用户服务)
 - TACACS+ (Terminal Access Controller Access-Control System，终端访问控制器访问控制系统)
- 对入侵检测系统 (Intrusion Detection System, IDS) 访问使用交换机的端口镜像功能。
- 实施端口安全性，以基于 MAC 地址限制访问。对所有端口禁用自动中继。

有关网络安全的更多信息，请参阅 Oracle ILOM 文档库中的《Oracle ILOM 安全指南》。您可以在以下位置找到 Oracle ILOM 文档：

<http://www.oracle.com/goto/ilom/docs>

数据保护和安全

请遵循以下准则以最大限度地确保数据安全：

- 使用外部硬盘驱动器或 USB 存储设备等设备备份重要数据。将备份的数据存储在另一个不在现场的安全位置。
- 使用数据加密软件确保硬盘驱动器上的机密信息安全。
- 处置旧硬盘驱动器时，请物理销毁该驱动器或彻底清除该驱动器上的所有数据。删除一个驱动器中的文件或者将其重新格式化后，仍可恢复该驱动器上的信息。删除文件或重新格式化驱动器只会删除驱动器中的地址表。使用磁盘擦除软件可完全清除驱动器上的所有数据。
- 硬盘驱动器通常用来存储敏感信息。要防止这些信息遭受未经授权的泄漏，在重新使用、停止使用或处置硬盘驱动器之前，应该对其进行净化处理。
 - 使用 Oracle Solaris `format(1M)` 命令等磁盘擦除工具彻底删除硬盘驱动器上的所有数据。此外，还可以使用物理消磁工具（如果有且适合）。
 - 在某些情况下，硬盘驱动器上包含的信息非常敏感，唯一适合的净化方法是以物理方式销毁硬盘驱动器：粉碎或焚化。
 - 强烈建议组织参阅其数据保护策略，以确定最合适的硬盘驱动器净化方法。



注意 - 由于新式硬盘驱动器（尤其是固态硬盘 (Solid State Drive, SSD)）控制数据访问的方式，磁盘擦除软件可能无法删除这些硬盘驱动器上的某些数据。

日志维护

请定期检查和维护日志文件。使用以下方法来保证日志文件的安全：

- 启用日志记录并将系统日志发送至专用安全日志主机。
- 使用网络时间协议 (Network Time Protocol, NTP) 和时间戳配置日志记录以包含准确的时间信息。
- 对网络设备日志执行定期调度的扫描，查看有无异常的网络活动或访问。
- 查看日志以发现可能的事件，并根据安全策略将它们归档。
- 当日志文件超出合理大小时，定期对这些日志文件进行归档，然后重置日志。您可以复制要作废的文件，将副本用于将来参考或统计分析。