Oracle® Server X5-8

安全指南

文件号码 E65069-01
2015 年 7 月

文件号码 E65069-01

版权所有 © 2015, 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

概述 7
系统概述 7
安全原则 8

使用服务器配置和管理工具 11
Oracle System Assistant 安全性 11
Oracle ILOM 安全性 12
Oracle Hardware Management Pack 安全性 12

规划安全环境 15
操作系统安全指南 15
网络端口和交换机 16
VLAN 安全 16
Infiniband 安全 16
硬件物理安全 17
软件安全 17

维护安全环境 19
硬件电源控制 19
资产跟踪 19
软件和固件更新 20
网络安全性 20
数据保护和安全 21
日志维护 21

概述

本文档提供了若干一般安全准则，用于帮助您保护 Oracle Server X5-8、其网络接口及其连接的网络交换机。

本节包含以下主题：

- “系统概述” [7]
- “安全原则” [8]

系统概述

Oracle Server X5-8 支持以下组件：

- 四个或八个 CPU 模块，每个模块具有一个 Intel Xeon® E7-8895 V3 处理器。

  支持的配置：

  - 将四个 CPU 模块安装在插槽 0 至 3 中
  - 将八个 CPU 模块安装在插槽 0 至 7 中
- 最多 192 个 DIMM（每个 CPU 模块 24 个 DIMM）。

  8 GB、16 GB DDR3 ECC 寄存式 DIMM 或 32 GB DDR3 寄存式 ECC LRDIMM。

  最大内存容量为 6 TB。
- 八个双 PCIe 卡载体 (Dual PCIe Card Carrier, DPCC)，每个载体具有两个 PCIe 3.0 卡插槽。

  使用 DPCC 提供了十六个可热交换的 PCIe 3.0 插槽（八个 x8 插槽，八个 x16 插槽）

  有关可供客户订购的 I/O 卡列表，请访问 Oracle x86 服务器 Web 站点并导航到 Oracle Server X5-8 页面：

  `http://www.oracle.com/technetwork/server-storage/sun-x86/overview/index.html`
- 八个 2.5 英寸可从背面装卸的可热交换 SAS-3 硬盘驱动器 (hard disk drive, HDD) 或者八个 2.5 英寸 eMLC SATA-3 固态驱动器 (solid state drive, SSD)，内部存储容量最高可达 9.6 TB
- 四个可从正面装卸的冗余可热交换电源。
- 可以使用下列管理软件选件：
  - Oracle Integrated Lights Out Manager (ILOM)，位于服务处理器

  - Oracle System Assistant (OSA)，位于可选的内部 USB 闪存驱动器
  - Oracle Enterprise Management Ops Center，可从 Oracle 站点下载
- Oracle Integrated Lights Out Manager 提供：
  - 远程键盘、视频、鼠标重定向
  - 通过命令行、IPMI 和浏览器界面实现的全面远程管理
  - 远程介质功能（DVD、CD、ISO 映像）
  - 高级电源管理和监视
  - Active Directory、LDAP、RADIUS 支持
  - 双 ILOM 闪存
  - 签名 ILOM
- Oracle System Assistant 服务器设置工具，该工具嵌入在预安装的 USB 闪存驱动器中。

安全原则

有四个基本安全原则：访问、验证、授权和记帐。

- 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。
  - 请参阅软件随附的文档，启用可用于软件的任何安全功能。
  - 将服务器和相关设备安装在带锁并限制随意出入的房间内。
  - 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。
  - 限制人员接近连接器或端口，这些位置可以提供比 SSH 连接更强大的访问。系统控制器、配电设备 (power distribution unit, PDU) 和网络交换机之类的设备都有连接器和端口。
  - 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的现场可更换单元 (field-replaceable unit, FRU) 和客户可更换单元 (customer-replaceable unit, CRU)。仅限经授权的人员接近带锁机柜。
- 验证

  验证是指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；对冗长会话设置超时；为用户设置特权级别。
- 授权

授权是指对人员使用硬件或软件施加的限制。

- 只允许人员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

  记帐是指用于监视登录活动和维护硬件清单的软件和硬件功能。

  - 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功能强大的命令。
  - 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，并可用于盘点目的。
  - 为了检测和跟踪组件，为计算机硬件的所有重要物项（如 FRU）提供安全标记。使用特殊的紫外线笔或压纹标签。

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，请遵循以下安全准则。

- “Oracle System Assistant 安全性” [11]
- “Oracle ILOM 安全性” [12]
- “Oracle Hardware Management Pack 安全性” [12]

Oracle System Assistant 安全性

Oracle System Assistant 是一种预安装的工具，可帮助您从本地或远程配置和更新服务器硬件，以及安装支持的操作系统。有关如何使用 Oracle System Assistant 的信息，请参阅《*Oracle X5* 系列服务器管理指南》，网址为：

http://www.oracle.com/goto/x86AdminDiag/docs

下列信息有助于您了解与 Oracle System Assistant 相关的安全问题。

- **Oracle System Assistant 包含一个可引导的根环境。**

  Oracle System Assistant 是一款在预安装的内部 USB 闪存驱动器上运行的应用程序。它构建于可引导的 Linux 根环境之上。Oracle System Assistant 还具有访问其底层 root shell 的功能。对系统具有物理访问权限的用户或通过 Oracle ILOM 对系统具有远程 KVMS（keyboard, video, mouse, and storage，键盘、视频、鼠标和存储）访问权限的用户，可以访问 Oracle System Assistant 和 root shell。

  根环境可以用来更改系统配置和策略，还可以用来访问其他磁盘上的数据。建议保护对服务器的物理访问权限，慎重为 Oracle ILOM 用户分配管理员和控制台特权。

- **Oracle System Assistant 挂载了可供操作系统访问的一个 USB 存储设备。**

  除作为可引导环境外，Oracle System Assistant 还作为 USB 存储设备（闪存驱动器）挂载，安装后主机操作系统可访问此设备。这在访问工具和驱动程序以进行维护和重新配置时很有用。Oracle System Assistant USB 存储设备既可读取又可写入，因而可能会被病毒利用。

  建议使用保护磁盘的方法来保护 Oracle System Assistant 存储设备，包括定期扫描病毒和检查完整性。

- **可以禁用 Oracle System Assistant。**

  Oracle System Assistant 是一种有用的工具，可帮助设置服务器、更新和配置固件以及安装主机操作系统。但是，如果您不能接受上述安全风险，或不需要此工具，可

以禁用 Oracle System Assistant。禁用 Oracle System Assistant 后，主机操作系统将不能再访问此 USB 存储设备。此外，也无法引导 Oracle System Assistant。

您可以通过 Oracle System Assistant 工具本身或通过 BIOS 禁用该工具。一旦禁用了 Oracle System Assistant，就只能从 BIOS 设置实用程序重新启用它。建议使用密码保护 BIOS 设置，以便只有授权用户才能重新启用 Oracle System Assistant。有关如何禁用和重新启用 Oracle System Assistant 的信息，请参阅《*Oracle X5 系列服务器管理指南*》，网址为：

http://www.oracle.com/goto/x86AdminDiag/docs

Oracle ILOM 安全性

您可以使用 Oracle Integrated Lights Out Manager (Oracle ILOM) 管理固件（已预先安装到此服务器、基于 x86 的其他 Oracle 服务器以及某些基于 SPARC 的 Oracle 服务器上）来主动保护、管理和监视系统组件。

对服务处理器 (Service Processor, SP) 使用专用内部网络，以将其与常规网络隔离。Oracle ILOM 可向系统管理员提供服务器控制和监视功能。根据授予管理员的授权级别，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。因此，要使 Oracle ILOM 环境保持最安全可靠，服务器上的专用网络管理端口或边带管理端口必须始终连接到可信的内部网络或专用的安全管理/专用网络。

默认管理员帐户 (`root`) 只能用于 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`)。除了更改默认管理员帐户的密码以外，还应为每个 Oracle ILOM 新用户建立新用户帐户，并为这些帐户指定唯一的密码和分配授权级别。

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 3.2 文档库中的《*Oracle Security Guide Firmware 3.0, 3.1, and 3.2*》。您可以在以下位置找到 Oracle ILOM 3.2 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 的其他服务器和某些 SPARC 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 (CLI Tools)）来管理服务器。

通过 Hardware Management Agent SNMP Plugins，您可以使用 SNMP 来监视数据中心中的 Oracle 服务器和服务器模块，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）来监视多个服务器和服务器模块。SNMP Plugins 在 Oracle 服务器的主机操作系统上运行。

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。

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

在安装和配置服务器及相关设备之前和期间，请遵循以下注意事项。

其中包括以下主题：

- “操作系统安全指南” [15]
- “网络端口和交换机” [16]
- “VLAN 安全” [16]
- “Infiniband 安全” [16]
- “硬件物理安全” [17]
- “软件安全” [17]

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://docs.oracle.com/cd/E23824_01/html/819-3195/index.html
Oracle Linux OS	http://linux.oracle.com
Oracle VM OS	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、Windows 和 VMware ESXi）的信息，请参阅供应商的文档。

网络端口和交换机

不同的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：

- 对交换机进行本地和远程访问时，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接入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，以便网络交换机可以基于当前连接设置安全性。

VLAN 安全

如果设置了虚拟局域网 (Virtual Local Area Network, VLAN)，请注意，VLAN 会分享网络带宽，且需要其他安全措施。

- 定义 VLAN 以将系统的敏感群集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。
- 限制使用可通过中继传输的 VLAN，只有绝对需要时才使用。
- 如果可能，禁用 VLAN 中继协议 (VLAN Trunking Protocol, VTP)。否则，为 VTP 设置以下项：管理域、密码和修剪。然后将 VTP 设置为透明模式。

Infiniband 安全

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。
- 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。

硬件物理安全

保护物理硬件的方式非常简单：限制对硬件的接近和记录序列号。

- 限制接近
  - 将服务器和相关设备安装在带锁并限制随意出入的房间内。
  - 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。在进行设备维修之后将门锁上。
  - 限制人员接近 USB 控制台，该控制台可提供比 SSH 连接更强大的访问功能。系统控制器、配电设备 (power distribution unit, PDU) 和网络交换机之类的设备都可能有 USB 连接。
  - 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) 或客户可更换单元 (customer-replaceable unit, CRU)。仅限经授权的人员接近带锁机柜。
- 记录序列号
  - 对计算机硬件的所有重要物项（如 FRU）添加安全标记。使用特殊的紫外线笔或压纹标签。
  - 记录所有硬件的序列号。
  - 将硬件激活密钥和许可证保存在一个安全位置，在系统出现紧急状况时系统管理员可以轻松访问该位置。打印的文档可能是证明所有权的唯一证据。

软件安全

大多数硬件安全都通过软件方法实现。

- 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，从而有可能对设备进行未经授权的访问。
- 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。
- 默认管理员帐户 (root) 只能供一个管理员用户使用。对于每个新用户，始终创建新的 Oracle ILOM 帐户。确保始终为每个 Oracle ILOM 用户帐户指定唯一的密码和分配合适的授权级别（操作员、管理员等）。
- 对服务处理器使用专用网络，从而将其与常规网络隔离。
- 保护对 USB 控制台的访问。一些设备（如系统控制器、配电设备 (Power Distribution Unit, PDU) 和网络交换机）可能有 USB 连接，这些连接可以提供比 SSH 连接更强大的访问。

- 请参阅软件随附的文档，启用可用于软件的任何安全功能。
- 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。

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。

- “硬件电源控制” [19]
- “资产跟踪” [19]
- “软件和固件更新” [20]
- “网络安全性” [20]
- “数据保护和安全” [21]
- “日志维护” [21]

硬件电源控制

可以使用软件来打开和关闭某些 Oracle 系统的电源。可以远程启用和禁用某些系统机柜的配电设备 (power distribution unit, PDU)。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维护人员使用这些命令。

有关详细信息，请参阅系统或机柜文档。

资产跟踪

可使用序列号跟踪清单。Oracle 将序列号嵌入到选件卡和系统主板上的固件中。可以通过局域网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*》：

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

软件和固件更新

请保持服务器设备上的软件和固件为最新版本。

- 定期检查更新。
- 始终在您的设备上安装软件或固件的最新发行版本。
- 为您的软件安装任何必要的安全修补程序。
- 请注意，网络交换机和 Express 模块之类的设备也包含固件，可能需要修补程序和固件更新。

网络安全性

请遵循以下准则来保护对系统的本地和远程访问：

- 只允许使用 SSH（而非 Telnet）从特定 IP 地址进行远程配置。Telnet 以明文形式传递用户名和密码，这可能使 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。
- 如果必须使用 SNMP，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，请始终在使用后将其注销。
- 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)。启用必要的网络服务并以安全方式配置这些服务。
- 使用 LDAP 访问系统时，遵循 LDAP 安全措施。请参阅 Oracle ILOM 3.2 文档库中的《*Oracle Security Guide Firmware 3.0, 3.1, and 3.2*》，网址为：`http://www.oracle.com/goto/ILOM/docs`。
- 创建标题以指出禁止未经授权的访问。
- 在适用的情况下使用访问控制列表。
- 设置扩展会话的超时时间，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 (Authentication, Authorization, and Accounting, AAA) 功能。
- 如果可能，使用 RADIUS 和 TACACS+ 安全协议：
  - RADIUS（Remote Authentication Dial In User Service，远程验证拨入用户服务）是一种客户机/服务器协议，可保护网络免受未经授权的访问。
  - TACACS+（Terminal Access Controller Access-Control System，终端访问控制器访问控制系统）是一种协议，它允许远程访问服务器与验证服务器通信，以确定用户是否有权访问网络。

- 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。
- 实施端口安全以基于 MAC 地址限制访问。对所有端口禁用自动中继。

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，请以物理方式销毁该驱动器或彻底清除该驱动器上的所有数据。删除驱动器中的文件或重新格式化驱动器后，仍可从该驱动器恢复信息。删除文件或重新格式化驱动器只会删除该驱动器中的地址表。使用磁盘擦除软件可彻底清除驱动器上的所有数据。

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。
- 查看日志以发现可能的事件，并根据安全策略将它们归档。
- 定期将超出合理大小的日志文件作废。您可以复制要作废的文件，将这些副本用于将来参考或统计分析。