Oracle SuperCluster M7 系列安全指南

文件号码 **E69649-01**
2016 年 2 月

文件号码 E69649-01

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

使用本文档

- **概述**－提供了有关为 Oracle SuperCluster M7 系列系统规划、配置和维护安全的环境的信息。
- **目标读者**－技术人员、系统管理员和授权服务提供商
- **必备知识**－UNIX 和数据库管理方面的丰富经验。

产品文档库

有关该产品及相关产品的文档和资源，可从以下网址获得：http://www.oracle.com/goto/sc-m7/docs。

反馈

可以通过以下网址提供有关本文档的反馈：http://www.oracle.com/goto/docfeedback。

了解安全原则

本指南提供了有关为 Oracle SuperCluster M7 系列系统规划、配置和维护安全的环境的信息。

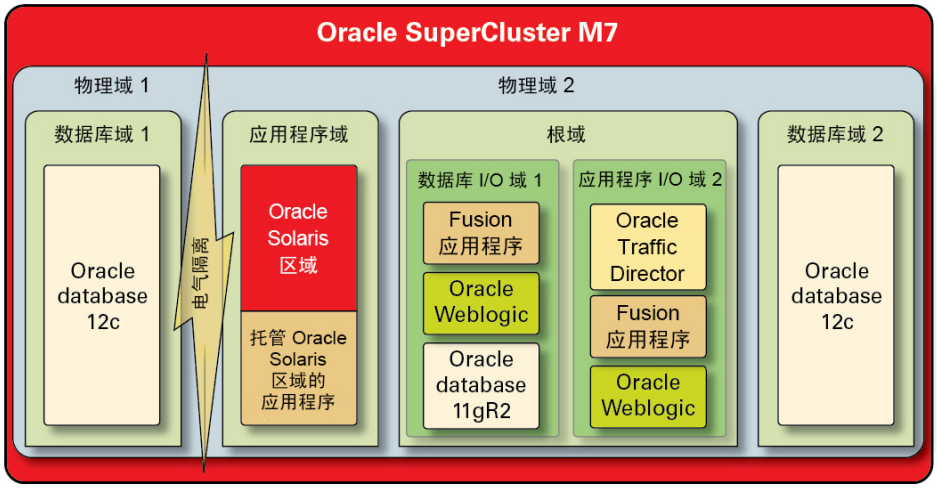
本部分介绍以下主题：

安全隔离

SuperCluster M7 支持各种隔离策略，云提供商可根据他们的安全和保障要求来选择隔离策略。此灵活性使得云提供商可创建根据其业务量身打造的安全的定制多租户体系结构。

SuperCluster M7 支持许多工作负荷隔离策略，每个策略都有一组独特的功能。尽管可以单独使用每个实施策略，但也可以在混合方法中将它们结合使用，以便云提供商部署的体系结构可以更有效地平衡其安全、性能、可用性需求和其他需求。

图 1 动态租户配置的安全隔离



在租户主机运行的应用程序和数据库必须与其他工作负荷物理隔离的情况下，云提供商可以使用物理域（也称为 PDomain）。由于对组织的重要性、所含信息的敏感性、符合性要求原因或者仅仅因为数据库或应用程序工作负荷将充分利用整个物理系统的资源，部署可能需要专用物理资源。

对于需要虚拟机管理程序协调式隔离的组织来说，Oracle VM Server for SPARC 域（称为专用域）用于创建将应用程序和/或数据库实例隔离的虚拟环境。专用域在安装 SuperCluster 的过程中创建，每个专用域都运行其唯一的 Oracle Solaris OS 实例。对物理资源的访问由 SPARC 处理器中内置的硬件协助式虚拟机管理程序协调。

此外，SuperCluster 允许您创建其他称为根域的域，这类域利用单一根 I/O 虚拟化 (single root I/O virtualization, SR-IOV) 技术。根域拥有一个或两个 IB HCA 和 10 GbE NIC。您可以选择在根域上动态创建其他域，称为 I/O 域。SuperCluster M7 包含基于浏览器的工具，可以创建和管理这些域。

然而，在每个域中，云使用者租户可以利用 Oracle Solaris Zones 技术创建其他隔离环境。使用区域，可以将单个应用程序或数据库实例或者应用程序或数据库实例组部署到一个或多个共同在单个 OS 内核上运行的虚拟容器中。此轻量级虚拟化方法用于围绕部署的服务创建安全性更高的边界。

在 SuperCluster 上托管多个应用程序和数据库的租户还可以选择采用混合方法，结合使用多种隔离策略基于 Oracle Solaris Zones、I/O 域和专用域来创建满足其云基础结构需求的灵活且具有弹性的体系结构。通过各种虚拟化选项，SuperCluster 使云托管的租户可

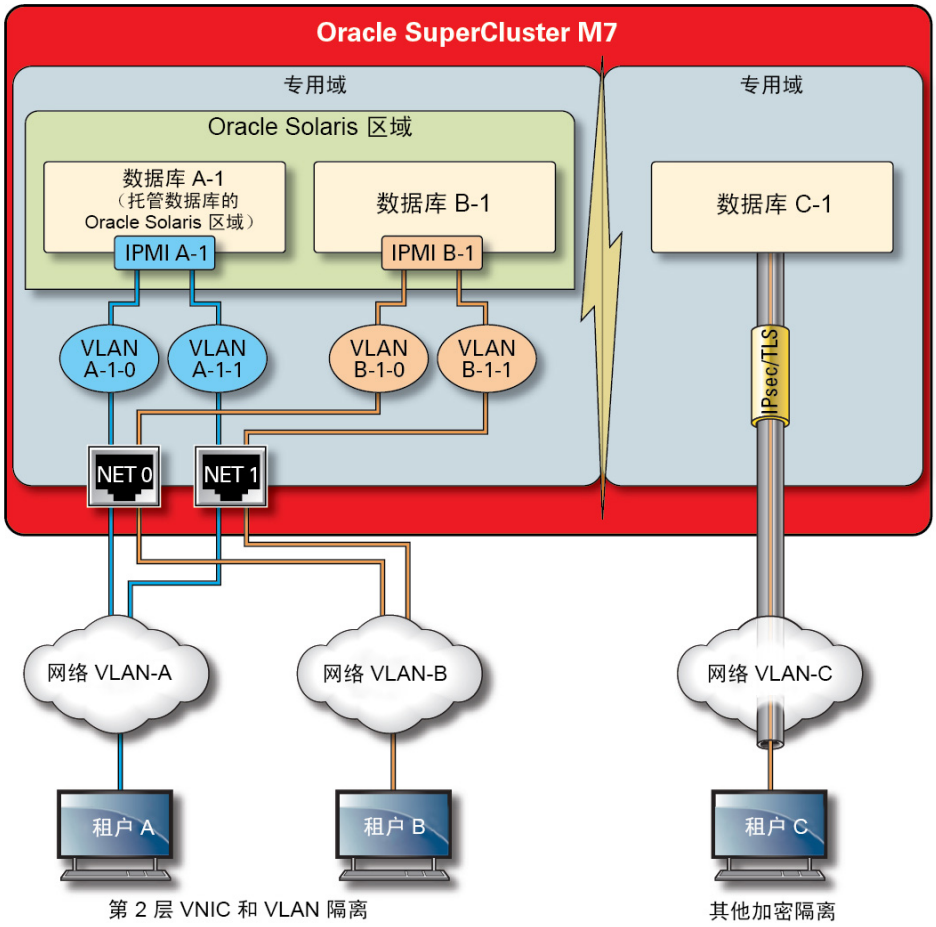
以在硬件层安全地隔离，并且它提供了 Oracle Solaris Zones 以在运行时环境中实现增强的安全性和进一步的隔离。

首先最好确保将单个应用程序、数据库、用户和流程在主机 OS 中正确隔离。然而，考虑在 SuperCluster 中使用的三个主要网络以及如何保护网络隔离功能和网络中的通信流同样重要。

- 10 GbE 客户机访问网络
- 专用 IB 服务网络
- 管理网络

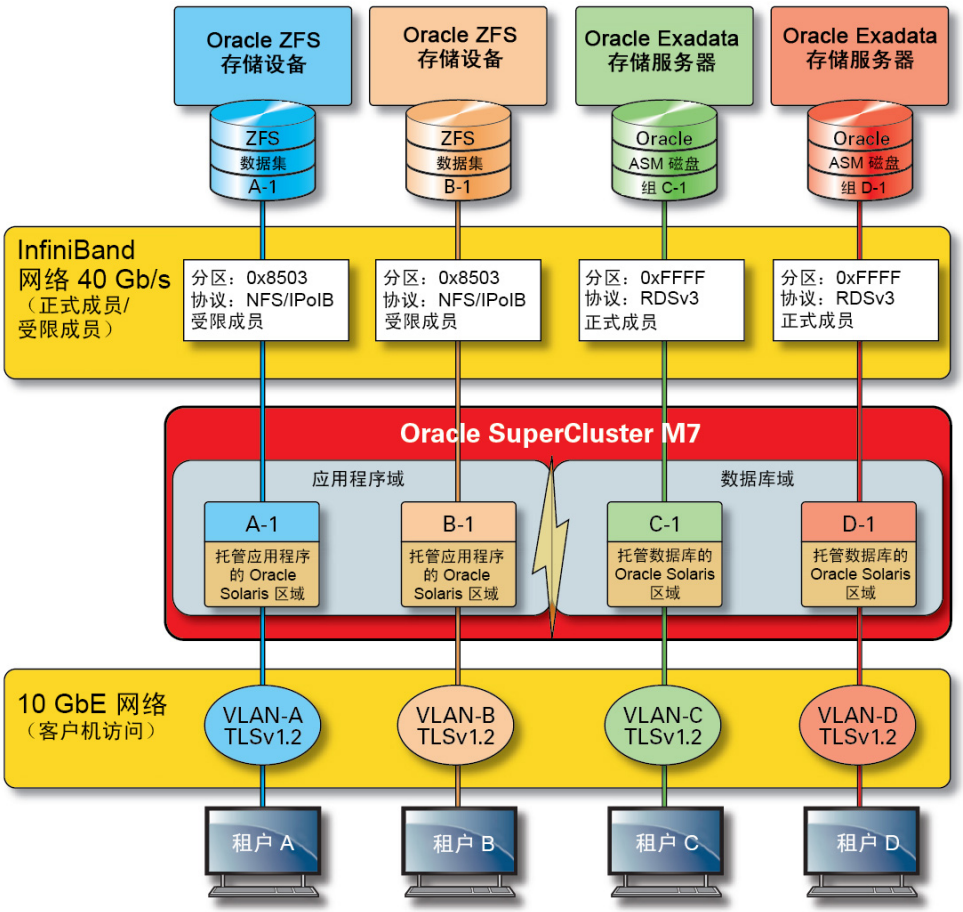
SuperCluster 客户机访问网络中的网络通信流可以通过许多技术隔离。下图显示了一种可行的配置，其中四个数据库实例配置为在三个不同的虚拟 LAN (virtual LAN, VLAN) 中运行。通过将 SuperCluster 的网络接口配置为使用 VLAN，可以在 Oracle VM Server for SPARC 专用域之间以及 Oracle Solaris Zones 之间隔离网络通信流量。

图 2 客户机访问网络中的安全网络隔离



SuperCluster 包含一个专用 IB 网络，数据库实例使用它来访问 Exadata 存储服务器和 ZFS 存储设备中存储的信息，并执行群集和高可用性所需的内部通信。此插图显示了 SuperCluster M7 上的安全网络隔离。

图 3 40 Gbs IB 网络上的安全网络隔离



默认情况下，在安装和配置过程中会将 SuperCluster IB 网络划分为六个不同的分区。尽管您无法更改默认分区，但 Oracle 却支持在需要将 IB 网络进一步细分的情况下创建和使用其他专用分区。此外，IB 网络支持受限和正式分区成员身份的概念。受限成员只能与正式成员通信，而正式成员可以与分区中的所有节点通信。可以将应用程序 I/O 域和 Oracle Solaris 11 区域配置为其各自 IB 分区的受限成员，以确保它们只能与配置为正式成员的 ZFS 存储设备通信，不能与可能存在于同一分区中的其他受限成员身份节点通信。

SuperCluster 还包含专用管理网络，通过它可以管理和监视其所有核心组件。此策略可将敏感的管理和监视功能与用于处理客户机请求的网络路径隔离。通过将管理功能隔离

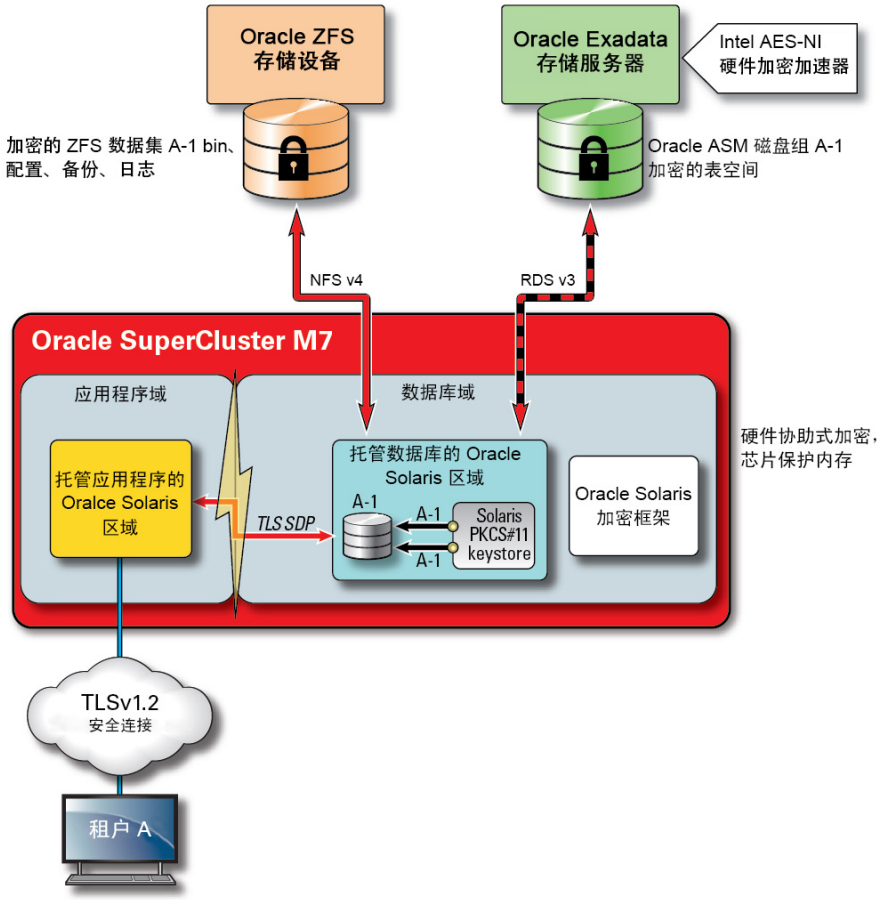
到此管理网络，SuperCluster 可以进一步减少通过客户机访问和 IB 网络公开的网络攻击面。强烈建议云提供商遵循此建议的做法并隔离管理、监视和其他相关功能，以便只能从管理网络访问它们。

数据保护

对于云提供商来说，数据保护是安全策略的核心。鉴于隐私和符合性要求的重要性，考虑使用多租户体系结构的组织应认真考虑使用加密技术来保护数据库的往来信息流。将系统地对数据保护应用加密服务，以便无论是在网络中流动时还是位于磁盘中时，都可以确保信息的机密性和完整性。

SuperCluster 中的 SPARC M7 处理器有助于实施硬件协助式高性能加密，以满足对安全性较为敏感的 IT 环境的数据保护需求。SPARC M7 处理器还采用了芯片保护内存技术，该技术可以防止恶意应用程序级别的攻击，例如内存抓取、无提示内存损坏、缓冲区溢出和相关攻击。

图 4 硬件协助式加密加速和内存入侵保护提供的数据保护



在安全的多租户体系结构（在其中数据保护几乎融入到了体系结构的每个方面）中，SuperCluster 及其支持软件使组织不用牺牲性能即可实现其安全性和符合性目标。SuperCluster 利用位于核心上的加密指令和芯片保护内存功能，这些功能内置在 SPARC M7 处理器中，设计用于在不影响性能的情况下加速加密操作和确保内存入侵保护。这些功能提高了加密性能并提供内存入侵检查，还提高了整体性能，因为有更多计算资源可以专用于处理租户工作负荷。

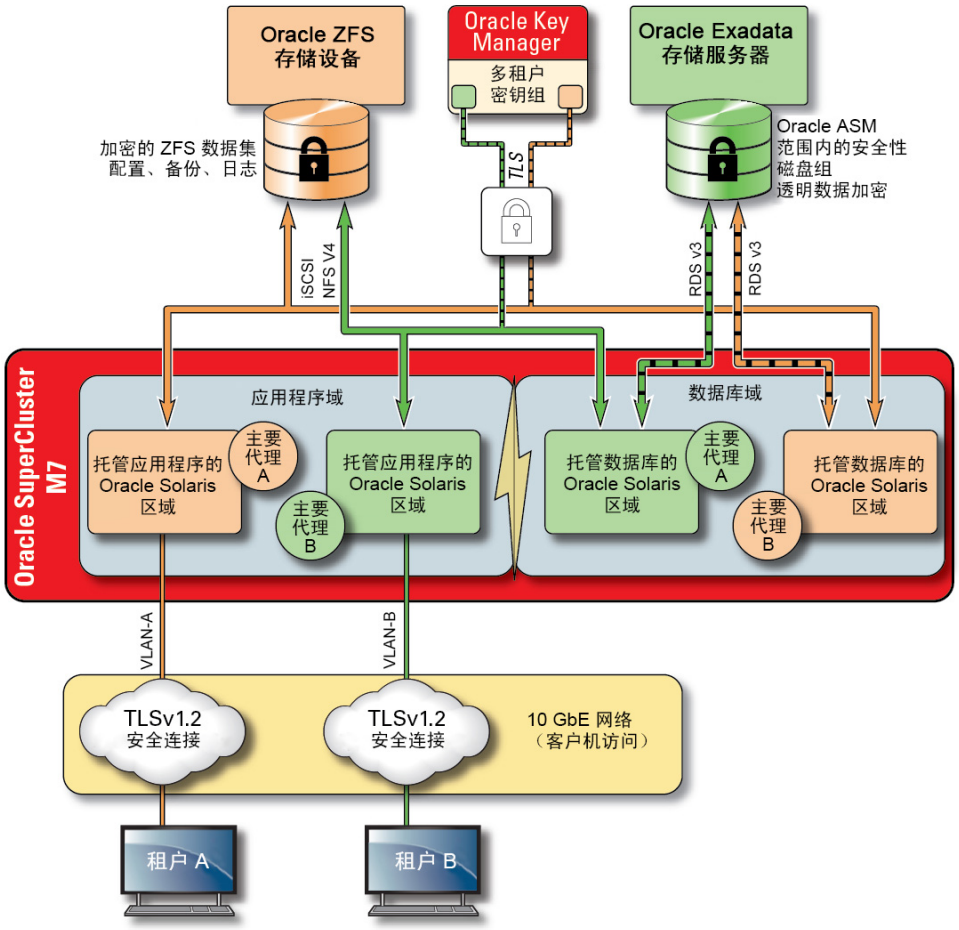
SPARC 处理器为超过 16 种行业标准加密算法提供硬件协助式加密加速支持。这些算法共同为新型加密需求提供支持，包括公钥加密、对称密钥加密、随机数生成以及计算和验证数字签名和消息摘要。此外，在 OS 级别，默认情况下会为大多数核心服务启用加密硬件加速，包括安全 Shell、IPSec/IKE 和加密的 ZFS 数据集。

Oracle Database 和 Oracle Fusion Middleware 自动识别 SuperCluster 使用的 Oracle Solaris OS 和 SPARC 处理器。这使得数据库和中间件可以自动将平台的硬件加密加速功能用于 TLS、WS-Security、表空间加密操作。它还使得它们可以使用芯片保护内存功能来确保内存保护，并且它无需最终用户进行配置即可确保应用程序数据完整性。为了保护 IB 网络中特定于租户并基于 IP 的区域间通信流的机密性和完整性，请使用 IPSec（IP Security，IP 安全）和 IKE（Internet Key Exchange，Internet 密钥交换）。

如果不讨论如何管理加密密钥，则任何关于加密技术的讨论都是不完整的。生成和管理加密密钥（特别是具有大量服务的情况）过去一直是组织面临的重大挑战，在基于云的多租户环境中挑战变得更加严峻。在 SuperCluster 上，ZFS 数据集加密和 Oracle Database 透明数据加密可以利用 Oracle Solaris PKCS#11 密钥库安全地保护主密钥。使用 Oracle Solaris PKCS#11 密钥库将自动对所有主密钥操作应用 SPARC 硬件协助式加密加速。这使得 SuperCluster 可以极大地提高与 ZFS 数据集、Oracle Database 表空间加密、加密数据库备份（使用 Oracle Recovery Manager [Oracle RMAN]）、加密数据库导出（使用 Oracle Database 的数据泵功能）和重做日志（使用 Oracle Active Data Guard）关联的加密和解密操作的性能。

使用共享 Wallet 方法的租户可以利用 ZFS 存储设备创建可以在群集中的所有节点之间共享的目录。使用共享的集中式密钥库有助于租户在群集数据库体系结构（例如 Oracle Real Application Clusters (Oracle RAC)）中更好地管理、维护和轮转密钥，因为密钥将在群集中的每个节点之间同步。

图 5 通过多租户密钥管理方案使用 Oracle Key Manager 实现的数据保护



要解决与基于云的多租户环境中的多个主机和应用程序关联的密钥管理复杂性和问题，请使用可选的 Oracle Key Manager 作为集成到管理网络中的设备。Oracle Key Manager 集中授予对 Oracle Database、Oracle Fusion 应用程序、Oracle Solaris 和 ZFS 存储设备使用的加密密钥的访问权限，并保护和管理对它们的访问。Oracle Key Manager 还支持 Oracle 的 StorageTek 加密磁带机。通过在 ZFS 数据集（文件系统）级别实施加密策略和密钥管理，可以通过密钥销毁提供有保证的租户文件系统删除。

Oracle Key Manager 是完整的密钥管理设备，支持生命周期密钥管理操作和可信密钥存储。当配置有来自 Oracle 的附加 Sun Crypto Accelerator 6000 PCIe 卡时，Oracle Key

Manager 会提供经 FIPS 140-2 3 级认证的密钥存储（用于 AES 256 位加密密钥）以及符合 FIPS 186-2 的随机数生成。在 SuperCluster 中，所有数据库和应用程序域（包括其全局区域和非全局区域）都可以配置为使用 Oracle Key Manager 来管理与应用程序、数据库和加密的 ZFS 数据集关联的密钥。实际上，Oracle Key Manager 能够支持与单个或多个数据库实例、Oracle RAC、Oracle Active Data Guard、Oracle RMAN 和 Oracle Database 的数据泵功能关联的密钥管理操作。

最后，由 Oracle Key Manager 强制实施的职责分离使每个租户都能完全控制其加密密钥，并且针对任何密钥管理操作都能获得一致的视图。鉴于密钥对保护信息的重要性，租户基于角色实施所需级别的访问控制和审计以确保密钥在其整个生命周期中得到妥善的保护至关重要。

相关信息

- “Oracle Key Manager” [114]

访问控制

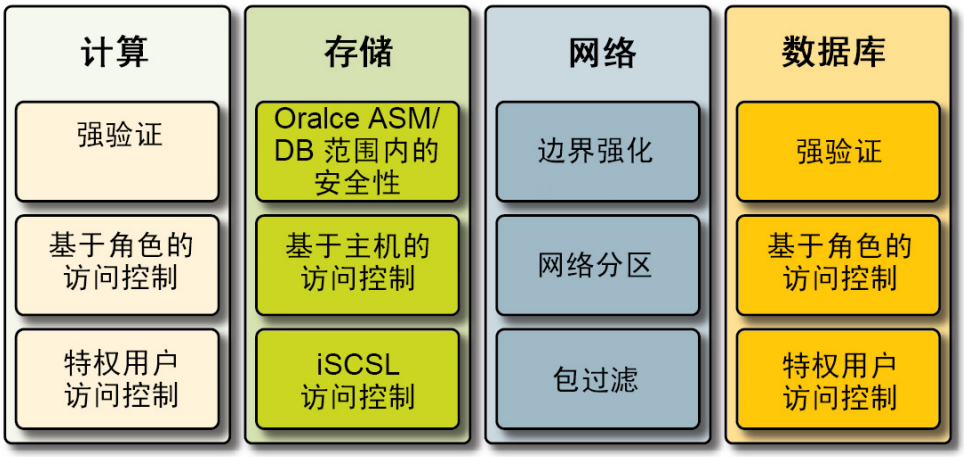
对于采用云托管环境策略的组织来说，访问控制是要解决的最大难题之一。租户必须保证存储在共享基础结构中的信息得到了保护并且仅对获得了授权的主机、服务、个人、组和角色可用。必须根据最小特权原则进一步约束获得了授权的主机、个人和服务，以便它们仅具有执行特定操作所需的权限和特权。

SuperCluster 便于实施灵活且分层的访问控制体系结构，该体系结构涵盖堆栈的每一层并支持各种角色，包括最终用户、数据库管理员和系统管理员。这使得组织可以分别定义保护主机、应用程序和数据库的策略并保护服务基于其运行的底层计算、存储和网络基础结构。

在虚拟化和 OS 层，首先通过减少在网络上公开的服务数来实施访问控制。这有助于控制对 Oracle VM Server for SPARC 控制台、域和区域的访问。通过减少可以访问系统的入口数，不仅可以减少访问控制策略数，还可以让在系统的生命周期内进行维护变得更加容易。

在 Oracle Solaris OS 中，访问控制结合使用 POSIX 权限与 Oracle Solaris 基于角色的访问控制 (role-based access control, RBAC) 工具来实施。同样重要的是，访问控制能够防止在 SuperCluster 上运行的主机、应用程序、数据库和相关服务遭受基于网络的攻击。为此，租户应首先确认仅获得批准的网络服务运行并侦听传入网络连接。最大限度地减小网络攻击面之后，租户然后应配置剩余服务，以便它们仅侦听获得批准的网络和接口上的传入连接。这种简单的做法有助于确保管理协议（如安全 Shell）无法从除管理网络以外的任何位置访问。

图 6 端到端访问控制摘要



此外，租户还可以选择实施基于主机的防火墙，例如 Oracle Solaris 的 IP 过滤器服务。基于主机的防火墙非常有用，因为它们在控制对网络服务的访问方面为主机提供了功能更加丰富的方法。例如，IP 过滤器支持有状态包过滤，并且它可以按照 IP 地址、端口、协议、网络接口以及通信方向对包进行过滤。这些功能对于管理许多网络接口并支持各种入站和出站网络通信的平台（例如 SuperCluster）非常重要。

在 SuperCluster 上，可以在 Oracle VM Server for SPARC 域中配置或者在 Oracle Solaris 区域中管理 IP 过滤器。这允许在提供数据库服务的 OS 容器内强制实施网络访问控制策略。在多租户方案中，出站网络活动量可能最小并且可以轻松地分类，以便可以创建策略以将通信对象限制为特定网络接口和目标。所有其他通信流量将遭拒并被记录在“默认拒绝”策略中，以阻止未经授权的通信，不管是入站还是出站通信。

Oracle End User Security 允许租户将其应用程序和数据库与其现有身份管理服务集成，以支持单点登录 (single sign-on, SSO) 以及集中式用户和角色管理。具体地说，Oracle End User Security 帮助对以下事项进行集中化处理：(1) 置备和取消置备数据库用户和管理员；(2) 密码管理和自助密码重置；(3) 使用全局数据库角色进行的授权管理。需要多重验证方法（例如的 Kerberos 或 PKI）的组织可以利用 Oracle Advanced Security。

Oracle Exadata 存储服务器技术支持一组预定义的用户帐户，每个用户帐户都具有不同的特权。执行 Oracle Exadata 存储服务器管理的管理员必须使用这些预定义的角色之一来访问系统。另一方面，ZFS 存储设备支持创建本地和远程管理帐户，这两类帐户都支持单独分配角色和特权。

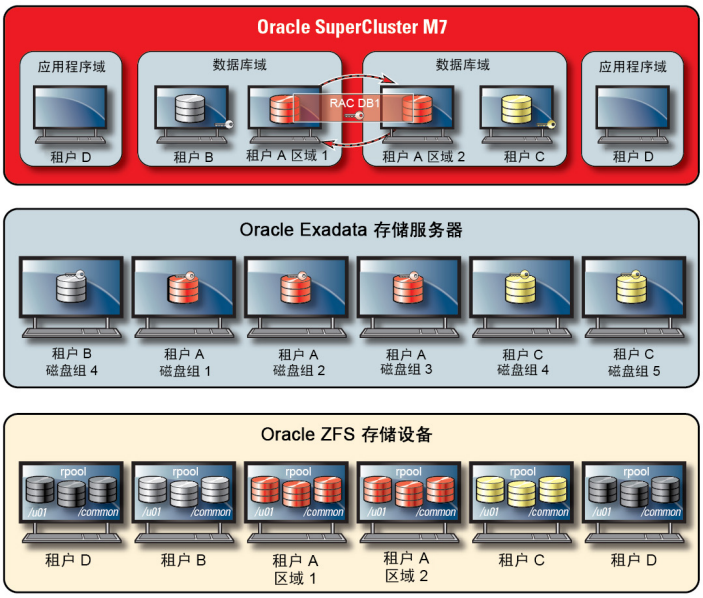
默认情况下，SuperCluster 中使用的 Oracle Exadata 存储服务器由数据库域通过 Oracle Automatic Storage Management 工具访问。此工具允许云提供商为每个租户创建能够

满足其容量、性能和可用性要求的不同磁盘组。在访问控制方面，Oracle Automatic Storage Management 支持三种访问控制模式：开放式安全性、Oracle Automatic Storage Management 范围内的安全性和数据库范围内的安全性。

在多租户方案中，建议使用数据库范围内的安全性，因为它可以提供最精细的访问控制。在此模式中，可以配置磁盘组，以便它们只能由单个数据库访问。具体地说，这意味着数据库管理员和用户都只能访问包含他们有权访问的信息的那些网格磁盘。在数据库整合方案中（在其中各个数据库可能支持不同的组织或租户），让每个租户都只能访问和处理其自己的存储非常重要。特别是，当与之前讨论的工作负荷和数据库隔离策略结合使用时，租户可以有效地分隔对各个数据库的访问。

数据库范围内的安全性是一种有效的工具，可以限制对 Oracle ASM 网格磁盘的访问。此图显示 Oracle ASM 范围内的安全性和 ZFS 安全性。如果在 SuperCluster 平台上部署了大量 Oracle Database 实例，则采用 Oracle ASM 范围内的每租户安全性可能更合适，因为它可以显著减少必须创建、分配和管理的密钥数。另外，由于数据库范围内的安全性要求为每个数据库创建独立磁盘组，因此，此方法还可以显著减少在 Exadata 存储服务器上必须创建的独立网格磁盘数。

图 7 Oracle ASM 范围内的每租户安全性



SuperCluster 利用 Oracle Solaris 数据链路保护来防止恶意租户虚拟机可能对网络造成的损坏。此集成的 Oracle Solaris 功能可以防御以下基本威胁：IP 和 MAC 地址欺骗以及 L2

帧欺骗（例如网桥协议数据单元攻击）。Oracle Solaris 数据链路保护必须单独应用于在多租户环境中部署的所有 Oracle Solaris 非全局区域。

由于单个租户任何时候都不需要对 Exadata 存储服务器进行管理或主机级别的访问，因此，强烈建议限制此类访问。应将 Exadata 存储服务器配置为禁止对租户的非全局区域和数据库 I/O 域进行直接访问，同时仍允许从 SuperCluster 数据库域（由云提供商管理）进行访问。这可以确保 Exadata 存储服务器只能从管理网络上的可信位置进行管理。

定义和实施租户的安全配置后，服务提供商可以考虑一个额外的步骤，即将特定于租户的全局和非全局区域作为只读环境配置为不可变。不可变区域创建有弹性且高度完整的操作环境，在其中租户可管理其自己的服务。不可变区域基于 Oracle Solaris 固有的安全功能构建，可确保部分（或所有）OS 目录和文件在无云服务提供商介入的情况下无法更改。强制实施这种只读环境有助于防止未经授权的更改、促进更强大的变更管理过程，并阻止基于内核和用户的恶意软件的注入。

监视和符合性审计

主动监视和登录在云环境中非常重要，在许多情况下可以帮助减少利用安全漏洞进行的攻击。无论是对于符合性报告还是事件响应来说，监视和审计对于云提供商都是至关重要的功能，租户组织必须强制实施定义明确的日志记录和审计策略，以便增进对托管环境的认识。在多大程度上进行监视和审计通常取决于风险大小和所保护环境的重要性。

SuperCluster 云体系结构使用 Oracle Solaris 审计子系统来收集、存储和处理审计事件信息。每个特定于租户的非全局区域将生成审计记录，它们被本地存储到每个 SuperCluster 专用域（全局区域）中。此方法将确保各个租户无法修改其审计策略、配置或记录的数据，因为这是云服务提供商的职责。Oracle Solaris 审计功能监视所有管理操作、命令调用，甚至租户区域和域中的各个内核级系统调用。该工具高度可配置，可提供全局、每区域甚至每用户审计策略。配置为使用租户区域时，每个区域的审计记录可以存储在全局区域中以防止被篡改。专用域和 I/O 域还利用本机 Oracle Solaris 审计工具来记录与虚拟化事件和域管理相关联的操作和事件。

Exadata 存储服务器和 ZFS 存储设备支持登录、硬件和配置审计。这使组织可以确定谁访问过设备以及执行过什么操作。尽管不直接向最终用户公开，但 Oracle Solaris 审计为 ZFS 存储设备显示的信息提供底层内容。

同样地，Exadata 存储服务器审计是一个丰富的系统事件集合，这些系统事件可以与 Exadata 存储服务器软件提供的硬件和配置警报信息结合使用。通过 Oracle Solaris 的 IP 过滤器功能，云提供商可以有选择地记录入站和出站网络通信，并且可以在域和非全局区域级别应用该功能。这有助于组织细分网络策略和验证活动记录。（可选）可以部署 Oracle Audit Vault and Database Firewall 设备，以安全地汇总和分析来自各种 Oracle 和非 Oracle 数据库的审计信息以及来自 Oracle Solaris 的审计信息。

通过与 Oracle Enterprise Manager 集成，SuperCluster 能够支持各种云自助操作。云提供商可以定义资源池、向单个租户分配池和配额、识别和发布服务目录，并最终支持监视和记录应用程序和数据库资源。

相关信息

- 符合性审计 [107]
- “监视安全性” [116]

有关 SuperCluster 安全性最佳做法的其他资源

有关 SuperCluster 安全性、体系结构和最佳做法的其他信息，请参阅以下资源：

- 《Oracle SuperCluster M7 - Platform Security Principles and Capabilities》（《Oracle SuperCluster M7－平台安全原则和功能》）

  `http://www.oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster/supercluster-t4-4/ssc-security-pac-1716580.pdf`
- 《Oracle SuperCluster M7 - Secure Private Cloud Architecture》（《Oracle SuperCluster M7－安全的专用云体系结构》）

  `http://www.oracle.com/technetwork/server-storage/engineered-systems/oracle-supercluster/documentation/supercluster-secure-multi-tenancy-2734706.pdf`
- 《Comprehensive Data Protection on Oracle SuperCluster》（《Oracle SuperCluster 上全面的数据保护》）

  `https://community.oracle.com/docs/DOC-918251`
- 《Secure Database Consolidation on Oracle SuperCluster》（《Oracle SuperCluster 上安全的数据库整合》）

  `http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf`
- 《Oracle SuperCluster and PCI Compliance》（《Oracle SuperCluster 和 PCI 符合性》）

  `http://www.oracle.com/technetwork/server-storage/engineered-systems/sparc-supercluster/supercluster-pci-dss-compliance-2372543.pdf`
- 《Oracle SuperCluster - Security Technical Implementation Guide (STIG) Validation and Best Practices》（《Oracle SuperCluster－安全技术实施指南 (STIG) 验证和最佳做法》）

  `http://www.oracle.com/technetwork/server-storage/hardware-solutions/stig-sparc-supercluster-1841833.pdf`

- 《Developer's Guide to Oracle Solaris 11 Security》（《Oracle Solaris 11 开发者安全性指南》）

  https://docs.oracle.com/cd/E36784_01/html/E36855/index.html
- 《Oracle Solaris 11 and PCI Compliance》（《Oracle Solaris 11 和 PCI 符合性》）

  http://www.oracle.com/us/products/servers-storage/solaris/solaris11/solaris11-pci-dss-wp-1937938.pdf
- 《Oracle Solaris 11 Audit Quick Start》（《Oracle Solaris 11 审计快速入门》）

  http://www.oracle.com/technetwork/articles/servers-storage-admin/sol-audit-quick-start-1942928.html
- 《Oracle Solaris 11 Security Guidelines》（《Oracle Solaris 11 安全准则》）

  http://docs.oracle.com/cd/E53394_01/html/E54807/index.html
- 《Oracle Database Security Guide 12c Release 1 (12.1)》（《Oracle Database 安全指南 12c 发行版 1 (12.1)》）

  https://docs.oracle.com/database/121/DBSEG/E48135-11.pdf

查看默认安全配置

以下主题介绍了 SuperCluster M7 的默认安全配置。

默认安全设置

SuperCluster M7 软件安装有许多默认安全设置。只要有可能，请使用默认安全设置：

- 密码策略强制实施最低密码复杂性。
- 失败的登录尝试会导致在失败尝试达到一定次数后锁定帐户。
- OS 中的所有默认系统帐户都被锁定，禁止登录。
- 配置了使用 `su` 命令的有限能力。
- 从 OS 内核中禁用了不必要的协议和模块。
- 引导装载程序受密码保护。
- 所有不必要的系统服务都已禁用，包括 `inetd`（Internet 服务守护进程）。
- 在存储单元上配置了软件防火墙。
- 在与密钥安全相关的配置文件和可执行文件上设置了限制性的文件权限。
- SSH 侦听端口限于管理和专用网络。
- SSH 限于 v2 协议。
- 禁用了不安全的 SSH 验证机制。
- 配置了特定加密密码。
- 交换机在系统中与网络上的数据通信流量分离。

默认用户帐户和密码

下表列出了 SuperCluster M7 的默认用户帐户和密码。有关各个组件的后续章节中提供了更改默认密码的其他说明。

组件	用户名	密码	用户帐户和密码信息
在以下系统上运行的 Oracle ILOM： ■ SPARC M7 系列服务器 ■ Exadata 存储服务器 ■ ZFS 存储设备	■ `root`	`welcome1`	请参阅 Oracle ILOM 文档集中的 "Configuration and Maintenance"（配置和维护），网址为：`http://docs.oracle.com/cd/E24707_01/html/E24528`
SPARC M7 系列服务器	■ `root` ■ `oracle` ■ `grid`	`welcome1` `welcome1` `welcome1`	请参见登录到计算服务器并更改默认密码 [49]。 另请参阅以下资源： ■ **Oracle Solaris 11**－请参阅 Oracle Solaris 11 的安全文档，网址为：`http://www.oracle.com/goto/Solaris11/docs` ■ **Oracle Solaris 10**－请参阅《*Oracle Solaris Administration: Basic Administration*》（《Oracle Solaris 管理：基本管理》），网址为：`http://docs.oracle.com/cd/E26505_01`

Exadata 存储服务器	■ `root`
	■ `celladmin`
	■ `cellmonitor`
		`welcome1`
		`welcome`
		`welcome`
			请参见更改存储服务器密码 [84]。

Oracle ZFS Storage ZS3-ES	■ `root`	`welcome1`	请参见更改 ZFS 存储设备 `root` 密码 [74]。 另请参阅《*Oracle ZFS Storage Appliance Administration Guide*》（《Oracle ZFS Storage Appliance 管理指南》）中的 "Users"（用户）部分，网址为：`http://www.oracle.com/goto/ZS3-ES/docs`
InfiniBand 交换机	■ `root` ■ `nm2user`	`welcome1` changeme	请参见更改 `root` 和 `nm2user` 密码 [99]。 另请参阅 *Sun Datacenter InfiniBand Switch 36 HTML Document Collection for Firmware Version 2.1* 中的 "Controlling the Chassis"，网址为：`http://docs.oracle.com/cd/E36265_01`
InfiniBand Oracle ILOM	■ `ilom-admin` ■ `ilom-operator`	ilom-admin ilom-operator	请参见更改 IB 交换机密码 (Oracle ILOM) [99]。 另请参阅 InfiniBand 文档，网址为：`http://docs.oracle.com/cd/E36265_01`
以太网管理交换机	■ `admin`	`welcome1`	请参见更改以太网交换机密码 [105]
Oracle I/O 域创建工具	■ `admin`	welcome1	请参阅《*Oracle I/O Domain Administration Guide*》（《Oracle I/O 域管理指南》），网址为：`http://www.oracle.com/goto/sc-m7/docs`。

组件	用户名	密码	用户帐户和密码信息
Oracle Engineered Systems Hardware Manager	■ admin ■ service	welcome1 welcome1	请参阅《*Oracle SuperCluster M7 Series Owner's Guide: Administration*》（《Oracle SuperCluster M7 系列所有者指南：管理》），网址为：http://www.oracle.com/goto/sc-m7/docs。

注 - 如果更改了此组件的 root 或 admin 密码，也必须在 Oracle Engineered Systems Hardware Manager 中进行更改。有关说明，请参阅《*Oracle SuperCluster M7 Series Owner's Guide: Administration*》。另请参见“Oracle Engineered Systems Hardware Manager 已知的密码” [31]

Oracle Engineered Systems Hardware Manager 已知的密码

Oracle Engineered Systems Hardware Manager 必须配置有下表中组件的帐户和密码。

注 - Oracle Engineered Systems Hardware Manager 不需要知道任何逻辑域或区域的密码。

组件	帐户
所有 Oracle ILOM	root
Exadata 存储服务器 OS	root
ZFS 存储控制器 OS	root
IB 交换机	root
以太网管理交换机	admin
PDU	admin

有关 Oracle Engineered Systems Hardware Manager 的更多信息，请参见“Oracle Engineered Systems Hardware Manager” [115]，并参阅《*Oracle SuperCluster M7 Series Administration Guide*》（《Oracle SuperCluster M7 系列管理指南》），网址为 http://www.oracle.com/goto/sc-m7/docs。

保护硬件

下面几部分介绍了保护硬件的安全准则：

限制人员接近

- 将 Oracle SuperCluster M7 系列系统和相关设备安装在带锁并限制随意出入的房间内。
- 锁上机架门，除非需要维修机架内的组件。这样做可以限制人员接近热插拔或热交换设备、USB 端口、网络端口和系统控制台。
- 将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) 存放在带锁的机柜中。仅允许经授权的人员接近带锁机柜。
- 定期检验机架和备用机柜上锁的状况和完整性，以防止或发现擅自换锁或者门意外未上锁等情况。
- 将机柜钥匙保存在不得随意接近的安全位置。
- 限制人员接近 USB 控制台。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。实际接近是操作组件的一种较安全的方法，因为不容易遭受网络攻击，但是，对可以实际接近的人员要加以限制。

序列号

- 记录 SuperCluster M7 系列系统中组件的序列号。
- 为计算机硬件的所有重要物品（如更换部件）添加安全标记。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记录保存在系统出现紧急状况时易于系统管理员获取的安全位置。打印的文档可能是证明所有权的唯一证据。
- 安全地存放随系统提供的所有信息表。

驱动器

硬盘驱动器和固态驱动器通常用来存储敏感信息。为防止未经授权泄露这些信息，在重新使用、停止使用或处置驱动器之前，要对其进行净化处理。

- 使用 Oracle Solaris `format(1M)` 命令等磁盘擦除工具彻底删除驱动器上的所有数据。
- 组织应当参考其数据保护策略来确定最合适的硬盘驱动器净化方法。
- 如果需要，可以利用 Oracle 的客户数据和设备保留服务。请参阅此文档：`http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`

注意 - 由于新式驱动器控制数据访问的方式，磁盘擦除软件可能无法删除这些驱动器上的某些数据。

OBP

默认情况下，SPARC M7 系列 OBP 不受密码保护。您可以通过执行以下操作来限制访问 OBP，从而增强系统的安全性：

- 实施密码保护。
- 检查失败的 OBP 登录。
- 提供 OBP 打开电源标志。

其他硬件资源

《*SPARC M7 Series Servers Security Guide*》（《SPARC M7 系列服务器安全指南》）中概述的所有安全准则均适用于 SuperCluster 中的 SPARC M7 服务器。该安全指南可从以下位置获得：`http://www.oracle.com/goto/M7/docs`

保护 Oracle ILOM

Oracle ILOM 提供了先进的服务处理器硬件和软件，它们用于管理和监视 Oracle SuperCluster 组件，包括计算服务器、存储服务器、ZFS 存储设备和 IB 交换机。

通过 Oracle ILOM，您可以独立于 OS 状态有效管理和监视底层服务器和设备，从而提供可靠的快速远程管理功能。

为了全方位保护 SuperCluster M7 上的 Oracle ILOM，您必须单独将配置设置应用于各个启用了 Oracle ILOM 的组件。以下组件具有 Oracle ILOM：

- 计算服务器
- 存储服务器
- ZFS 存储设备
- IB 交换机

执行以下任务以保护 Oracle ILOM：

▼ 登录到 Oracle ILOM CLI

1. **在管理网络中，登录到 Oracle ILOM。**

   在此示例中，将 *ILOM_SP_ipaddress* 替换为您要访问组件的 Oracle ILOM 的 IP 地址：

   - 计算服务器
   - 存储服务器
   - ZFS 存储设备

- IB 交换机

您配置的 IP 地址在 Oracle 人员提供的 "Deployment Summary"（部署摘要）中列出。

```
% ssh root@ILOM_SP__ipaddress
```

2. **输入 Oracle ILOM root 密码。**
   请参见"默认帐户和密码 (Oracle ILOM)" [37]。

▼ 确定 Oracle ILOM 版本

要利用最新的特性、功能和安全增强功能，请将 Oracle ILOM 软件更新至受支持的最新版本。

1. **在管理网络中，登录到 Oracle ILOM。**
   请参见登录到 Oracle ILOM CLI [35]。

2. **显示 Oracle ILOM 版本。**
   在此示例中，Oracle ILOM 软件的版本为 3.2.4.1.b。

```
-> version
SP firmware 3.2.4.1.b
SP firmware build number: 94529
SP firmware date: Thu Nov 13 16:41:19 PST 2014
SP filesystem version: 0.2.10
```

注 - 要更新任何 SuperCluster 组件上的 Oracle ILOM 的版本，请安装最新的 SuperCluster Quarterly Full Stack Download Patch，该程序可从 My Oracle Support 上获得，网址为 https://support.oracle.com。

注 - Oracle 工程系统（如 SuperCluster）在可以使用哪些版本的 Oracle ILOM 和如何更新这些版本方面受到限制。要了解更多详细信息，请与 Oracle 代表联系。

▼ （如果需要）启用以符合 FIPS-140 的模式运行 (Oracle ILOM)

美国联邦政府客户需要使用经 FIPS 140 验证的加密。

默认情况下，Oracle ILOM 在运行时不使用经 FIPS 140 验证的加密。然而，如果需要，可以改为使用经 FIPS 140 验证的加密。

配置为以符合 FIPS 140 的模式运行时，一些 Oracle ILOM 特性和功能不可用。《*Oracle ILOM* 安全指南》中的“启用了 FIPS 模式时不受支持的功能”部分（请参见“其他 Oracle ILOM 资源” [48]）提供了此类功能的列表。

另请参见“FIPS-140-2 级别 1 符合性” [110]。

注意 - 此任务要求您重置 Oracle ILOM。重置会导致用户配置的所有设置丢失。因此，对 Oracle ILOM 进行其他任何特定于站点的更改之前，您必须启用以符合 FIPS 140 的模式运行。对于已做出特定于站点的配置更改的系统，请备份 Oracle ILOM 配置，以便可以在重置 Oracle ILOM 之后将其恢复，否则这些配置更改将丢失。

1. **在管理网络中，登录到 Oracle ILOM。**
   请参见登录到 Oracle ILOM CLI [35]。

2. **确定 Oracle ILOM 是否配置为以符合 FIPS 140 的模式运行。**

   ```
   -> show /SP/services/fips state status
   /SP/services/fips
   Properties:
   state = enabled
   status = enabled
   ```

   在 Oracle ILOM 中，符合 FIPS 140 的模式由 `state` 和 `status` 属性表示。`state` 属性表示 Oracle ILOM 中的已配置模式，而 `status` 属性表示 Oracle ILOM 中的运行模式。如果更改 FIPS `state` 属性，则在下一次 Oracle ILOM 重新引导之前，更改不会影响运行模式（FIPS `status` 属性）。

3. **启用以符合 FIPS 140 的模式运行。**

   ```
   -> set /SP/services/fips state=enabled
   ```

4. **重新启动 Oracle ILOM 服务处理器。**
   要使此更改生效，必须重新启动 Oracle ILOM SP。

   ```
   -> reset /SP
   ```

默认帐户和密码 (Oracle ILOM)

帐户	类型	默认密码	说明
`root`	管理员	`welcome1`	这是为此组件提供和启用的默认帐户。此帐户用于执行初始配置和允许创建其他非共享的管理帐户。

帐户	类型	默认密码	说明
			出于安全考虑，请更改默认密码。

默认公开的网络服务 (Oracle ILOM)

此表列出了 Oracle ILOM 公开的默认网络服务。

有关这些服务的其他信息，请参阅《*Oracle ILOM* 安全指南》（请参见"其他 Oracle ILOM 资源" [48]）。

服务名称	协议	端口	说明
SSH	TCP	22	由集成的安全 Shell 服务使用，用于允许使用 CLI 对 Oracle ILOM 进行管理访问。
HTTP (BUI)	TCP	80	由集成的 HTTP 服务使用，用于允许使用浏览器界面对 Oracle ILOM 进行管理访问。尽管 TCP/80 通常用于以明文形式进行访问，但默认情况下 Oracle ILOM 会自动将传入的请求重定向到此服务的安全版本（在 TCP/443 上运行）。
NTP	UDP	123	由集成的网络时间协议 (Network Time Protocol, NTP)（仅限客户机）服务使用，用于将本地系统时钟与一个或多个外部时间源同步。
SNMP	UDP	161	由集成的 SNMP 服务使用，用于提供管理接口以监视 Oracle ILOM 的运行状况和监视收到的陷阱通知。
HTTPS (BUI)	TCP	443	由集成的 HTTPS 服务使用，用于允许使用浏览器界面通过加密 (SSL/TLS) 通道对 Oracle ILOM 进行管理访问。
IPMI	TCP	623	由集成的智能平台管理接口 (Intelligent Platform Management Interface, IPMI) 服务使用，用于为各种监视和管理功能提供计算机接口。不应禁用此服务，因为 Oracle Enterprise Manager Ops Center 使用它来收集硬件清单数据、FRU 说明、硬件传感器信息和硬件组件状态信息。
远程 KVMS	TCP	5120 5121 5123 5555 5556 7578 7579	远程 KVMS 端口共同提供了一组协议，这些协议提供了可与 Oracle Integrated Lights Out Manager 一起使用的远程键盘、视频、鼠标和存储功能。
ServiceTag	TCP	6481	由 Oracle ServiceTag 服务使用。这是用于识别服务器和支持服务请求的 Oracle 搜索协议。Oracle Enterprise Manager Ops Center 等产品使用此服务搜索 Oracle ILOM 软件并与其他 Oracle 自动服务解决方案集成。
WS-Man over HTTPS	TCP	8888	由集成的 WS-Man 服务使用，用于提供基于标准的 Web 服务接口，该接口用于通过 HTTPS 协议管理 Oracle ILOM。禁用此服务时，无法使用此协议来管理 Oracle ILOM。从 Oracle ILOM 版本 3.2 开始，将不再包含此服务。
WS-Man over HTTP	TCP	8889	此端口由集成的 WS-Man 服务使用，用于提供基于标准的 Web 服务接口，该接口用于通过 HTTP 协议管理 Oracle ILOM。禁用此服务时，将无法使用此协议来管理 Oracle ILOM。从 Oracle ILOM 版本 3.2 开始，将不再包含此服务。

服务名称	协议	端口	说明
单点登录	TCP	11626	此端口由集成的单点登录功能使用，该功能可以减少用户必须输入用户名和密码的次数。禁用此服务时，如果不重新输入密码，则无法启动 KVMS。

强化 Oracle ILOM 安全配置

以下主题介绍了如何通过各种配置设置来保护 Oracle ILOM。

▼ 禁用不必要的服务 (Oracle ILOM)

禁用支持平台的运行和管理要求不需要的任何服务。

默认情况下，Oracle ILOM 采用网络“默认安全”配置，不必要的服务已被禁用。然而，根据您的安全策略和要求，可能需要禁用更多服务。

1. **在管理网络中，登录到 Oracle ILOM。**
   请参见登录到 Oracle ILOM CLI [35]。
2. **确定 Oracle ILOM 支持的服务列表。**

   ```
   -> show /SP/services
   ```
3. **确定特定服务是否处于启用状态。**
   将 *servicename* 替换为在步骤 2 中确定的服务名称。

```
-> show /SP/services/servicename servicestate
```

尽管大多数服务都可以识别 servicestate 参数并使用它来记录服务处于启用还是禁用状态，但一些服务（如 servicetag、ssh、sso 和 wsman）使用名为 state 的参数。无论使用的实际参数是什么，如果 servicestate 或 state 参数返回的值为 enabled，则表示服务处于启用状态，如以下示例中所示：

```
-> show /SP/services/https servicestate
/SP/services/https
Properties:
servicestate = enabled

-> show /SP/services/ssh state
/SP/services/ssh
Properties:
state = enabled
```

4. **要禁用不需要的服务，请将服务状态设置为 disabled。**

```
-> set /SP/services/http servicestate=disabled
```

5. **确定是否应禁用任何服务。**

   根据使用的工具和方法，如果不需要或不使用其他服务，则可以将其禁用：

   - **对于浏览器管理界面 (HTTP, HTTPS)，键入：**

     ```
     -> set /SP/services/http servicestate=disabled
     -> set /SP/services/http secureredirect=disabled
     -> set /SP/services/https servicestate=disabled
     ```

   - **对于键盘、视频、鼠标服务 (keyboard, video, mouse service, KVMS)，键入：**

     ```
     -> set /SP/services/kvms servicestate=disabled
     ```

   - **对于 Web 服务管理 (WS-Man over HTTP/HTTPS)－（Oracle ILOM 版本 3.1 和更早版本），键入：**

     ```
     -> set /SP/services/wsman state=disabled
     ```

   - **对于单点登录 (Single-Sign On, SSO) 服务，键入：**

     ```
     -> set /SP/services/sso state=disabled
     ```

▼ 配置指向 HTTPS 的 HTTP 重定向（Oracle ILOM）

默认情况下，Oracle ILOM 配置为将传入的 HTTP 请求重定向到 HTTPS 服务，以确保 Oracle ILOM 和管理员之间基于浏览器的所有通信均经过加密。

1. **在管理网络中，登录到 Oracle ILOM。**
   请参见登录到 Oracle ILOM CLI [35]。

2. **验证安全重定向是否已启用。**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **如果更改了默认设置，则您可以启用安全重定向。**

```
-> set /SP/services/http secureredirect=enabled
```

4. **通过再次执行步骤 2 来验证设置。**

禁用未获批准的协议

使用以下主题禁用未获批准的协议：

- 为 HTTPS 禁用 SSLv2 协议 [41]
- 为 HTTPS 禁用 SSLv3 协议 [42]

▼ 为 HTTPS 禁用 SSLv2 协议

默认情况下，会为 HTTPS 服务禁用 SSLv2 协议。

出于安全考虑，禁用 SSLv2 非常重要。

1. **在管理网络中，登录到 Oracle ILOM。**
   请参见登录到 Oracle ILOM CLI [35]。

2. **确定是否为 HTTP 服务禁用了 SSLv2 协议。**

```
-> show /SP/services/https sslv2
/SP/services/https
Properties:
sslv2 = disabled
```

3. **如果服务处于启用状态，则禁用 SSLv2 协议。**

```
-> set /SP/services/https sslv2=disabled
```

4. **通过再次执行步骤 2 来验证设置。**

▼ 为 HTTPS 禁用 SSLv3 协议

默认情况下，会为 HTTPS 服务启用 SSLv3 协议。

出于安全考虑，需要禁用 SSLv3 协议。

1. **在管理网络中，登录到 Oracle ILOM。**
请参见登录到 Oracle ILOM CLI [35]。

2. **确定是否为 HTTP 服务禁用了 SSLv3 协议。**

```
-> show /SP/services/https sslv3
/SP/services/https
Properties:
sslv3 = enabled
```

3. **禁用 SSLv3 协议。**

```
-> set /SP/services/https sslv3=disabled
```

4. **通过再次执行步骤 2 来验证设置。**

▼ 为 HTTPS 禁用未获批准的 TLS 协议

默认情况下，会为 HTTPS 服务启用 TLSv1.0、TLSv1.1 和 TLSv1.2 协议。

您可以禁用一个或多个不符合您安全策略的 TLS 协议版本。

出于安全考虑，请使用 TLSv1.2，除非需要支持较旧版本的 TLS 协议。

1. **在管理网络中，登录到 Oracle ILOM。**
请参见登录到 Oracle ILOM CLI [35]。

2. **确定为 HTTPS 服务启用的 TLS 协议版本的列表。**

```
-> show /SP/services/https tlsv1 tlsv1_1 tlsv1_2
/SP/services/https
```

```
Properties:
tlsv1 = enabled
tlsv1_1 = enabled
tlsv1_2 = enabled
```

3. **禁用 TLSv1.0。**

```
-> set /SP/services/https tlsv1_0=disabled
```

4. **禁用 TLSv1.1。**

```
-> set /SP/services/https tlsv1_1=disabled
```

5. **通过再次执行步骤 2 来验证设置。**

▼ 为 HTTPS 禁用较弱和中等强度的 SSL 密码

默认情况下，Oracle ILOM 会为 HTTPS 服务禁用较弱和中等强度的密码。

1. **在管理网络中，登录到 Oracle ILOM。**
请参见登录到 Oracle ILOM CLI [35]。

2. **确定是否禁用了较弱和中等强度的密码。**

```
-> show /SP/services/https weak_ciphers
/SP/services/https
Properties:
weak_ciphers = disabled
```

3. **如果更改了默认设置，则您可以禁用较弱和中等强度的密码。**

```
-> set /SP/services/https weak_ciphers=disabled
```

4. **通过再次执行步骤 2 来验证设置。**

▼ 禁用未获批准的 SNMP 协议 (Oracle ILOM)

默认情况下，仅为用于监视和管理 Oracle ILOM 的 SNMP 服务启用 SNMPv3 协议。确保禁用较旧版本的 SNMP 协议，除非需要使用它们。

一些 Oracle 和第三方产品在支持较新的 SNMP 协议版本方面受到限制。请参阅与这些组件相关的产品文档，以确认它们对特定 SNMP 协议版本的支持情况。确保 Oracle ILOM 配置为支持这些组件所需的任何协议版本。

注 - SNMP 协议版本 3 引入了对基于用户的安全模型 (User-based Security Model, USM) 的支持。此功能使用实际用户帐户取代了传统的 SNMP 团体字符串，可以为用户帐户配置特定权限、验证、隐私协议和密码。默认情况下，Oracle ILOM 不包含任何 USM 帐户。根据您自己的部署、管理和监视要求来配置 SNMPv3 USM 帐户。

1. **在管理网络中，登录到 Oracle ILOM。**
   请参见登录到 Oracle ILOM CLI [35]。

2. **确定每个 SNMP 协议的状态。**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = disabled
v2c = disabled
v3 = enabled
```

3. **如果需要，请禁用 SNMPv1 和 SNMPv2c。**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

4. **通过再次执行步骤 2 来验证设置。**

▼ 配置 SNMP v1 和 v2c 团体字符串 (Oracle ILOM)

此任务仅适用于启用并配置为使用 SNMP v1 或 SNMPv2c 的情况。

为了使 SNMP 可以正常运行，客户机和服务器必须就用于验证访问权限的团体字符串达成一致。因此，更改 SNMP 团体字符串时，请确保同时为 Oracle ILOM 和尝试使用 SNMP 协议与 Oracle ILOM 连接的所有组件配置新字符串。

由于 SNMP 通常用于监视设备的运行状况，因此将设备使用的默认 SNMP 团体字符串替换为客户定义的值非常重要。

1. **在管理网络中，登录到 Oracle ILOM。**
   请参见登录到 Oracle ILOM CLI [35]。

2. **创建新 SNMP 团体字符串。**
   在此示例中，替换命令行中的以下项：

   - *string*－替换为客户定义的值，客户定义的值要符合美国国防部有关 SNMP 团体字符串组成部分的要求。

- *access*－根据这是只读还是读写访问字符串，替换为 `ro` 或 `rw`。

```
-> create /SP/services/snmp/communities/string permission=access
```

创建新团体字符串之后，必须删除默认团体字符串。

3. **删除默认 SNMP 团体字符串。**

```
-> delete /SP/services/snmp/communities/public
-> delete /SP/services/snmp/communities/private
```

4. **验证 SNMP 团体字符串。**

```
-> show /SP/services/snmp/communities
```

▼ 替换默认自签名证书 (Oracle ILOM)

Oracle ILOM 使用自签名证书来允许直接使用 SSL 和 TLS 协议。如果可能，应将自签名证书替换为获准在您的环境中使用并由获得认可的证书颁发机构签名的证书。

Oracle ILOM 支持通过各种方法访问数字证书和私钥（包括 HTTPS、HTTP、SCP、FTP、TFTP），还支持直接将信息粘贴到 Web 浏览器界面中。有关更多信息，请参阅 *Oracle ILOM* 配置和维护指南（请参见“其他 Oracle ILOM 资源” [48]）。

1. **确定 Oracle ILOM 是否正在使用默认自签名证书。**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

2. **安装您组织的证书。**

```
-> set /SP/services/https/ssl/custom_cert load_uri=URI_method
-> set /SP/services/https/ssl/custom_key load_uri=URI_method
```

▼ 配置浏览器管理界面不活动超时

Oracle ILOM 支持在管理会话处于不活动状态超过预定义的分钟数后将其断开连接并注销。默认情况下，浏览器界面会话在 15 分钟后超时。

与 HTTPS 和 HTTP 服务关联的会话超时参数单独进行设置和管理。确保设置与每个服务关联的 `sessiontimeout` 参数。

1. **在管理网络中，登录到 Oracle ILOM。**
   请参见登录到 Oracle ILOM CLI [35]。

2. **检查与 HTTPS 服务关联的不活动超时参数。**

```
-> show /SP/services/https sessiontimeout
/SP/services/https
Properties:
sessiontimeout = 15
```

3. **设置不活动超时参数。**
   将 *n* 替换为以分钟为单位指定的值。

```
-> set /SP/services/https sessiontimeout=n
```

4. **检查与 HTTP 服务关联的不活动超时参数。**

```
-> show /SP/services/http sessiontimeout
/SP/services/http
Properties:
sessiontimeout = 15
```

5. **设置不活动超时参数。**
   将 *n* 替换为以分钟为单位指定的值。

```
-> set /SP/services/http sessiontimeout=n
```

6. **通过再次执行步骤 2 和步骤 4 来验证设置。**

▼ 配置管理界面超时 (Oracle ILOM CLI)

Oracle ILOM 支持在 CLI 管理会话处于不活动状态超过预定义的分钟数后将其断开连接并注销。

默认情况下，SSH CLI 未指定超时值，因此，访问此服务的管理用户始终保持登录状态。

出于安全考虑，设置此参数时，需要与浏览器用户界面关联的值相匹配。可以是 15 分钟或某个其他值。

1. **在管理网络中，登录到 Oracle ILOM。**
   请参见登录到 Oracle ILOM CLI [35]。

2. **检查与 CLI 关联的不活动超时参数。**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **设置不活动超时参数。**
   将 *n* 替换为以分钟为单位指定的值。

```
-> set /SP/cli timeout=n
```

4. **通过再次执行步骤 2 来验证设置。**

▼ 配置登录警告标题 (Oracle ILOM)

Oracle ILOM 支持在管理员连接到设备之前和之后显示特定于客户的消息。

Oracle ILOM 连接消息在验证之前显示，而登录消息在验证之后显示。

您可以选择将 Oracle ILOM 配置为要求接受登录消息才能授予对 Oracle ILOM 功能的访问权限。连接和登录消息以及可选的接受要求由浏览器和命令行访问界面实施。

Oracle ILOM 支持不超过 1,000 个字符的连接和登录消息。

1. **在管理网络中，登录到 Oracle ILOM。**
   请参见登录到 Oracle ILOM CLI [35]。

2. **确定是否配置了连接和登录消息。**

```
-> show /SP/preferences/banner connect_message login_message
/SP/preferences/banner
Properties:
connect_message = (none)
login_message = (none)
```

3. **设置连接或登录消息。**

```
-> set /SP/preferences/banner connect_message="Authorized Use Only"
-> set /SP/preferences/banner login_message="Authorized Use Only"
```

4. **确定是否启用了登录消息接受。**

```
-> show /SP/preferences/banner login_message_acceptance
/SP/preferences/banner
Properties:
login_message_acceptance = disabled
```

5. **（可选）强制实施登录消息接受。**

注意 - 要求接受登录消息可能会妨碍使用 SSH 的自动管理流程正常运行，因为它们可能无法或未配置为响应接受请求。因此，此类连接可能会挂起或超时，因为在满足消息接受要求之前，Oracle ILOM 不允许使用 CLI。

```
-> set /SP/preferences/banner login_message_acceptance=enabled
```

6. **通过再次执行步骤 2 和步骤 4 来验证设置。**

其他 Oracle ILOM 资源

有关 Oracle ILOM 管理和安全过程的更多信息，请参阅与在 SuperCluster M7 上运行的版本相对应的 Oracle ILOM 文档库：

- 《*Oracle ILOM Security Guide Firmware Releases 3.0, 3.1, and 3.2*》（《Oracle ILOM 安全指南（固件发行版 3.0、3.1 和 3.2）》）：

  http://docs.oracle.com/cd/E37444_01/html/E37451
- Oracle Integrated Lights Out Manager 版本 3.2.*x*：

  http://docs.oracle.com/cd/E37444_01
- Oracle Integrated Lights Out Manager 版本 3.1.*x*：

  http://docs.oracle.com/cd/E24707_01
- Oracle Integrated Lights Out Manager 版本 3.0.*x*：

  http://docs.oracle.com/cd/E19860-01

保护计算服务器

SuperCluster M7 中安装有一台或两台 SPARC M7 服务器（计算服务器）。每台计算服务器都划分为两个硬件分区（两个 PDomain）。每个 PDomian 包括机箱中一半的处理器、内存和 PCIe 扩展插槽。两个 PDomain 在同一机箱中作为单独的服务器运行。一对冗余的服务处理器模块 (service processor module, SPM) 管理每个分区。

您必须保护每个 PDomain。

下面几部分提供了计算服务器的一组安全控制。

▼ 登录到计算服务器并更改默认密码

要通过 Oracle ILOM 访问单个 PDomain，必须登录到控制该 PDomain 的活动 SPM。您可以在一个分区继续正常运行的同时打开、重新引导或管理另一个分区。

您可以采用多种方法登录到 SuperCluster 计算服务器。本任务中介绍的方法涉及在计算服务器的 SPM 上登录到 Oracle ILOM CLI。使用这种方法，您可以访问处于以下任何状态的服务器：

- 备用电源模式
- 系统已通电，但主机未在运行
- OS 正在引导
- 已完全通电，且 OS 正在运行

1. **在管理网络上，使用 `ssh` 命令登录。**

```
$ ssh root@compute_server_SPM_ILOM_IP-address
```

2. **出现提示时，输入密码。**
   出厂默认 root 密码为 welcome1。
   如果系统提示您更改密码，请更改密码。
   此时，您可以在计算服务器上执行在 Oracle ILOM 上执行的任何安全任务。

3. **如果要访问计算服务器的主机控制台，请启动该主机控制台。**

```
    -> start /Servers/PDomains/PDomain_0/HOST/console
Are you sure you want to start /Servers/PDomains/PDomain_0/HOST/console (y/n)? y

Serial console started.  To stop, type #.

root@system-identifier-pd0:~#
```

注 - 如果主机未在运行，则您不会看到 PDomain 提示符。

注 - 要切换回到 Oracle ILOM 提示符，请键入转义符（#. 是默认转义符）。

4. **如果需要，承担超级用户角色。**
   使用 su 命令切换为配置有 root 角色的用户。

默认帐户和密码（计算服务器）

帐户	默认密码	说明
root	welcome1	Oracle ILOM 要求在首次成功登录后立即更改默认密码。
oracle	welcome1	
grid	welcome1	

▼ 确定 SuperCluster 软件版本

1. **登录到某一台计算服务器并访问主机控制台。**

请参见登录到计算服务器并更改默认密码 [49]。

2. **键入以下命令。**

```
# svcprop -p configuration/build svc:/system/oes/id:default
```

在输出中，附加到 ssc 的数字表示软件版本。

要更新 SuperCluster 软件的版本，请安装最新的 SuperCluster Quarterly Full Stack Download Patch，该程序可从 My Oracle Support 上获得，网址为 https://support.oracle.com。

注 - 对于 SuperCluster，可能会有额外的限制，限制可使用哪些软件版本以及如何更新这些版本。在这些情况下，请与 Oracle 代表联系。

▼ 配置安全 Shell 服务

执行本任务有助于改进在 Oracle SuperCluster 中部署的安全 Shell 安全配置。

/etc/ssh/sshd_config 文件是一个系统范围的配置文件，您可以从中配置安全 Shell 服务的参数。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **编辑 `/etc/ssh/sshd_config` 文件。**

3. **配置 `ListenAddress` 参数，以确保仅接受源于 SuperCluster 客户机访问网络的连接。**
   确保将 ListenAddress IP 地址设置为客户机网络。
   这样可确保无法在管理或 IB 网络上成功发起组件之间的安全 Shell 连接。

4. **查看其他 `sshd_config` 参数，并根据站点要求设置这些参数。**
   以下设置可保护安全 Shell 服务：

```
Protocol 2
Banner /etc/issue
PermitEmptyPasswords no
PermitRootLogin no
StrictModes yes
IgnoreRhosts yes
PrintLastLog yes
X11Forwarding no
ClientAliveInterval 600
```

```
ClientAliveCountMax 0
```

5. **保存 `sshd_config` 文件。**

6. **重新启动该服务。**
   必须重新启动该服务才能使更改生效。

```
# svcadm restart ssh
```

▼ 验证 root 是否为角色

默认情况下，在 Oracle Solaris 中将 `root` 配置为一个角色而不是用户帐户。此外，SuperCluster 配置不允许匿名 `root` 用户登录。在承担 root 角色之前，所有用户都必须以一般用户身份登录。所有 SuperCluster 管理操作都必须使用 `root` 作为角色来执行。

1. **登录到某一台计算服务器并访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **验证 `root` 属性是否设置为 `type=role`。**

```
# grep root /etc/user_attr
root::::type=role
```

3. **（可选）将 `root` 角色分配给任意一般用户。**

```
# usermod -R root user_name
```

默认公开的网络服务（计算服务器）

下表列出了计算服务器上公开的默认网络服务。

服务名称	协议	端口	说明
SSH	TCP	22	由集成的安全 Shell 服务使用，用于允许使用 CLI 对计算服务器进行管理访问。
HTTP (BUI)	TCP	80	由集成的 HTTP 服务使用，用于允许使用浏览器界面对计算服务器进行管理访问。
HTTPS (BUI)	TCP	443	由集成的 HTTPS 服务使用，用于允许使用浏览器界面通过加密 (SSL/TLS) 通道对计算服务器进行管理访问。
SNMP	UDP	161	由集成的 SNMP 服务使用，用于提供管理接口以监视计算服务器的运行状况和监视收到的陷阱通知。

强化计算服务器安全配置

以下主题介绍了如何安全地配置计算服务器。

▼ 启用 intrd 服务

中断平衡器 (intrd) 服务可监视中断与 CPU 之间的分配以确保最佳性能。有关详细信息，请参阅 intrd(1M) 手册页。

该服务仅在全局区域中运行。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **启动该服务。**

```
# svcadm enable intrd
```

▼ 禁用不必要的服务（计算服务器）

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **如果系统不是 NFS 客户机或服务器，则禁用 NFS 状态监视器。**
   该服务与 `lockd(1M)` 进行交互来为 NFS 上的锁定服务提供崩溃恢复功能。

```
# svcadm disable svc:/network/nfs/status
```

3. **如果根本不使用 NFS 或使用的是 NFSv4，则禁用 NFS 锁定管理器服务。**
   NFS 锁定管理器在 NFSv2 和 NFSv3 中支持对 NFS 文件执行记录锁定操作。

```
# svcadm disable svc:/network/nfs/nlockmgr
```

4. **如果系统不会挂载文件，则可以禁用 NFS 客户机服务或卸载其软件包。**
   仅当系统从 NFS 服务器挂载文件时才需要 NFS 客户机服务。有关更多信息，请参阅 `mount_nfs(1M)` 手册页。

```
# svcadm disable svc:/network/nfs/client
```

5. **在不是 NFS 文件服务器的系统上禁用 NFS 服务器服务。**
   NFS 服务器服务通过 NFS 版本 2、3 和 4 处理客户机文件系统请求。如果系统不是 NFS 服务器，则禁用该服务。

```
# svcadm disable svc:/network/nfs/server
```

6. **如果不对 DNS SRV 记录使用 FedFS 或不使用基于 LDAP 的引用，则禁用该服务。**
   联合文件系统 (Federated file system, FedFS) 客户机服务为存储 FedFS 信息的 LDAP 服务器管理默认值和连接信息。

```
# svcadm disable svc:/network/nfs/fedfs-client
```

7. **禁用 `rquota` 服务。**
   `remote` 配额服务器为通过 NFS 挂载的本地文件系统的用户返回配额。结果由 `quota(1M)` 用来显示远程文件系统的用户配额。`rquotad(1M)` 守护进程通常由 `inetd(1M)` 调用。该守护进程提供有关潜在恶意用户的网络的信息。

```
# svcadm disable svc:/network/nfs/rquota
```

8. **禁用 `cbd` 服务。**

   `cbd` 服务管理 NFS 版本 4 协议的通信端点。`nfs4cbd(1M)` 守护进程在 NFS 版本 4 客户机上运行，并创建回调的侦听器端口。

   ```
   # svcadm disable svc:/network/nfs/cbd
   ```

9. **如果不使用 NFSv4，则禁用 `mapid` 服务。**

   NFS 用户和组 ID 映射守护进程服务可来回映射 NFS 版本 4 客户机和服务器使用的 NFS 版本 4 `owner` 和 `owner_group` 标识属性以及本地 UID 和 GID 编号。

   ```
   # svcadm disable svc:/network/nfs/mapid
   ```

10. **禁用 `ftp` 服务。**

    FTP 服务提供未加密文件传输服务，并使用纯文本验证。使用安全复制程序 `scp(1)` 代替 `ftp`，因为该程序提供加密验证和文件传输。

    ```
    # svcadm disable svc:/network/ftp:default
    ```

11. **禁用远程卷管理器服务。**

    可移除卷管理器是 HAL 感知型卷管理器，它能够自动挂载和卸载可移除的介质和可热插拔的存储器。用户可能会导入恶意程序或将敏感数据传输到系统以外。有关详细信息，请参阅 `rmvolmgr(1M)` 手册页。

    该服务仅在全局区域中运行。

    ```
    # svcadm disable svc:/system/filesystem/rmvolmgr
    ```

12. **禁用 `smserver` 服务。**

    `smserver` 服务用于访问可移除介质设备。

    ```
    # svcadm disable rpc/smserver:default
    ```

13. **对于 `/etc/pam.d` 目录中的 `r-protocol` 服务，指定 `pam_deny.so.1` 作为验证堆栈的模块。**

    默认情况下，不会安装传统服务，例如 `r-protocols`、`rlogin(1)` 和 `rsh(1)`。但是，会在 `/etc/pam.d` 中定义这些服务。如果从 `/etc/pam.d` 中删除了服务定义，在传统服务处于启用状态的情况下，这些服务将使用其他服务（例如 SSH）。

    ```
    # cd /etc/pam.d
    # cp rlogin rlogin.orig
    # pfedit rlogin
    ```

```
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
# cp rsh rsh.orig
# pfedit rsh
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
```

14. **编辑 `/etc/default/keyserv` 文件，将 `ENABLE_NOBODY_KEYS` 的值更改为 `NO`。**
    `keyserv` 服务无法使用 `nobody` 用户密钥。默认情况下，`ENABLE_NOBODY_KEYS` 的值为 YES。

```
# pfedit /etc/default/keyserv
. . .
ENABLE_NOBODY_KEYS=NO
```

15. **向 `ftpusers` 文件中添加用户以限制 `ftp` 访问。**
    FTP 文件传输不得提供给所有用户，必须要求符合条件的用户提供用户名和密码。一般来说，不得允许系统用户使用 FTP。这项检查可验证系统帐户是否包括在 `/etc/ftpd/ftpusers` 文件中，以便不允许他们使用 FTP。
    文件 `/etc/ftpd/ftpusers` 用于禁止用户使用 FTP 服务。至少要包括所有系统用户，例如 `root`、`bin`、`adm` 等。

```
# pfedit /etc/ftpd/ftpusers
....
root
daemon
bin
...
```

16. **为 FTP 服务器创建的文件设置强默认文件创建掩码。**
    FTP 服务器不一定会使用用户的系统文件创建掩码。设置 FTP umask 可确保通过 FTP 传输的文件使用强文件创建 umask。

```
# pfedit /etc/proftpd.conf
Umask          027
```

17. **禁用对网络拓扑查询的响应。**
    务必禁用对回显请求的响应。ICMP 请求使用 `ipadm` 命令进行管理。
    以下设置可防止散播有关网络拓扑的信息。

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip
```

18. **禁用重定向 ICMP 消息。**
    路由器使用 ICMP 重定向消息通知主机更多指向目标的直接路由。非法的 ICMP 重定向消息可能会导致 "man-in-the-middle"（中间人）攻击。

```
# ipadm set-prop -p _ignore_redirect=1 ipv4
```

19. **禁用 `mesg(1)` 以防止 `talk(1)` 和 `write(1)` 访问远程终端。**

```
# mesg -n
```

20. **（可选）查看并禁用在网络上侦听的不必要的服务。**
默认情况下，`ssh(1)` 是唯一一个可以发送和接收网络数据包的网络服务。

```
# svcadm disable FMRI_of_unneeded_service
```

▼ 启用严格多宿主

对于充当其他域的网关的系统（例如防火墙或 VPN 节点），必须启用严格多宿主。`hostmodel` 属性可控制多宿主系统上 IP 数据包的发送和接收行为。将严格多宿主设置为 `1`，以便不会在不同的接口上接受数据包。默认值为 `0`。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
请参见登录到计算服务器并更改默认密码 [49]。

2. **将严格多宿主设置为 `1`。**

```
# ipadm set-prop -p _strict_dst_multihoming=1 ipv4
```

▼ 启用 ASLR

注 - 请勿在数据库域或数据库区域中启用 ASLR。

Oracle Solaris 标记了许多用户二进制文件，以启用地址空间布局随机化 (address space layout randomization, ASLR)。ASLR 会对地址空间的关键部分的起始地址进行随机化处理。该安全防御机制可以导致返回导向编程 (Return Oriented Programming, ROP) 攻击在试图利用软件漏洞时失败。区域为其流程继承了该随机布局。由于 ASLR 的使用可能并非对于所有二进制文件都是最佳的，因此可以在区域级别和二进制文件级别配置 ASLR。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
请参见登录到计算服务器并更改默认密码 [49]。

2. **启用 ASLR。**

```
# sxadm delcust aslr
# sxadm info
EXTENSION    STATUS               CONFIGURATION
```

```
aslr         enabled (tagged-files) System default (default)
```

▼ 配置 TCP 连接

将每个端口的每个 IP 地址的最大半开 TCP 连接设置为 4096 有助于抵御 SYN 洪水式拒绝服务攻击。将最大排队传入 TCP 连接数设置为至少 1024 有助于防止某些分布式拒绝服务 (distributed denial of service, DDoS) 攻击。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **设置最大半开和排队传入 TCP 连接数。**

```
# ipadm set-prop -p _conn_req_max_q0=9096 tcp
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

▼ 为 PCI 符合性设置密码历史记录日志和密码策略

`/etc/default/passwd` 文件中的 `HISTORY` 参数使用 `HISTORY` 值防止用户使用类似的密码。

如果 `MINWEEKS` 设置为 3 且 `HISTORY` 设置为 `10`，则 10 个月内不能重用密码。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **编辑 `/etc/default/passwd` 文件并设置密码参数。**

```
# pfedit /etc/default/passwd
. . .
#Compliance to the PCI-DSS benchmark is 10
#HISTORY=0
HISTORY=10
MINDIFF=4
MINDIGIT=1
MINUPPER=1
MINWEEKS=3
MAXWEEKS=13
```

3. **编辑 `/etc/default/login` 文件以包括这些参数。**

```
# pfedit /etc/default/login
. . .
# Compliance edit
```

```
#PASSLENGTH=6
PASSLENGTH=14
. . .
```

▼ 确保用户主目录具有适当的权限

主目录必须可由其所有者写入和搜索。通常，其他用户无权修改这些文件或向用户的主目录中添加文件。要确保就是这样，请设置用户目录的权限。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **设置用户目录的权限。**

   ```
   # chmod 750 /export/home/user_home_directory
   ```

▼ 启用 IP 过滤器防火墙

IP 过滤器是一个基于主机的防火墙，可提供有状态包过滤和网络地址转换 (network address translation, NAT)。包过滤可提供基本的保护以防止基于网络的攻击。IP 过滤器还包括无状态包过滤，并且可以创建和管理地址池。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **启用 IP 过滤器防火墙。**

   ```
   # svcadm svc:/network/ipfilter:default
   ```

▼ 确保名称服务仅使用本地文件

OS 使用多个有关主机、ipnodes、用户 (passwd(4), shadow(4), user_attr(4)) 和 groups 的信息数据库。有关这些项目的数据有多种来源。例如，可以在 /etc/hosts、NIS、LDAP、DNS 或多点传送 DNS 中找到主机名和主机地址。如果只有本地文件条目用于这些项目，系统在受限制的环境中就会更加安全。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **将名称服务配置为仅使用本地文件。**

```
# svccfg -s name-service/switch setprop config/default = astring: "files"
# svccfg -s name-service/switch setprop config/host = astring: "files"
# svccfg -s name-service/switch setprop config/password = astring: "files"
# svccfg -s name-service/switch setprop config/group = astring: "files"
# svccfg -s name-service/switch:default refresh
```

▼ 启用 Sendmail 和 NTP 服务

Sendmail 服务必须正在运行，否则无法传送指向 `root` 的重要系统邮件。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**

   请参见登录到计算服务器并更改默认密码 [49]。

2. **启用 sendmail。**

```
# svcadm enable smtp:sendmail
```

3. **如果需要，安装 NTP 服务。**

   必须在需要确保安全性和符合性的所有系统上安装 `ntp` 服务。

```
# pkg install service/network/ntp
```

4. **将 NTP 服务配置为客户机并启用该服务。**

   必须启用网络时间协议守护进程并正确地将其配置为客户机。`/etc/inet/ntp.conf` 文件必须至少包括一个服务器定义。该文件还必须包含 `restrict default ignore` 一行，以防止客户机也充当服务器。

```
# vi /etc/inet/ntp.conf
. . .
server server_IP_address iburst
restrict default ignore ...
# svcadm enable ntp
```

▼ 禁用 GSS（除非使用 Kerberos）

通用安全服务 (`gss`) 管理通用安全服务应用编程接口 (Generic Security Service Application Program Interface, GSS-API) 安全令牌的生成和验证。`gssd(1M)` 守护进程在内核 `rpc` 与 GSS-API 之间运行。

注 - Kerberos 使用该服务。如果未配置且未使用 Kerberos，请禁用 rpc/gss 服务。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **启用 rpc/gss。**

```
# svcadm enable rpc/gss
```

3. **为 /tmpfs 设置大小限制。**
   默认情况下，tmpfs 文件系统的大小不受限制。为避免性能影响，您可以限制每个 tmpfs 挂载的大小。有关更多信息，请参阅 mount_tmpfs(1M) 和 vfstab(4) 手册页。

```
# pfedit /etc/vfstab
...
swap - /tmp tmpfs - yes size=sz
```

4. **重新引导计算服务器。**

```
# reboot
```

▼ 为全局可写文件设置 Sticky 位

目录上的 sticky 位可防止除文件所有者或 root 角色以外的任何人删除或移动全局可写目录中的文件。这在对许多用户通用的目录（例如 /tmp 目录）中非常有用。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **在 /tmp 上以及其他任何全局可写文件上设置 sticky 位。**

```
# chmod 1777 /tmp
```

▼ 保护核心转储

核心转储可能会包含敏感数据。保护可以包括文件权限和记录核心转储事件。请参阅 coreadm(1m) 和 chmod(1M) 手册页。

使用 coreadm 命令查看并设置当前的配置。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **查看当前的配置。**

```
# coreadm
global core file pattern: /var/share/cores/core.%f.%p
global core file content: default
init core file pattern: core
init core file content: default
global core dumps: enabled
per-process core dumps: enabled
global setid core dumps: disabled
per-process setid core dumps: disabled
global core dump logging: enabled
```

3. **配置核心文件并保护核心转储目录。**

```
# coreadm -g /var/cores/core_%n_%f_%u_%g_%t_%p \
           -e log -e global -e global-setid \
           -d process -d proc-setid
```

4. **检查权限。**

```
# ls -ld /var/share/cores
drwx------ 2 root root 2 Aug 2 2015 cores/
```

5. **在目录上正确地设置权限。**

```
# chmod 700 /var/share/cores
```

▼ 强制实施不可执行堆栈

启用不可执行堆栈是一个非常有用的技巧，可以阻挠某些类型的缓冲区溢出攻击。启用 Oracle Solaris nxstack 后，会将进程堆栈内存段标记为不可执行。这项扩展可以抵御依靠注入恶意代码并在堆栈上执行该代码的攻击。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **启用 nxstack。**

```
# sxadm set model=all nxstack
```

3. 验证配置。

```
# sxadm get all nxstack
EXTENSION     PROPERTY     VALUE
nxstack         model        all
```

▼ 启用加密的交换空间

对交换空间进行加密，无论它是 ZFS 卷还是原始设备。加密可确保在系统需要将页面换出到磁盘时保护其中包含的所有敏感数据（例如用户密码）。

1. 登录到某一台计算服务器并以超级用户身份访问主机控制台。
   请参见登录到计算服务器并更改默认密码 [49]。

2. 编辑 **/etc/vfstab** 文件，并将 **swap** 设置为 **encrypted**。

```
# pfedit /etc/vfstab
...
/dev/zvol/dsk/rpool/swap - - swap - no encrypted
```

3. 创建并初始化 **PKCS #11** 密钥库。

```
# pktool setpin keystore=pkcs11
Enter token passphrase: changeme
Create new passphrase: welcome1
Re-enter new passphrase: welcome1
```

4. 生成一个对称密钥并将其存储在 **PKCS #11** 密钥库中。

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=globalzone-key
```

▼ 启用审计

确保审计日志捕获了所有管理操作，包括带有参数的命令。

1. 登录到某一台计算服务器并以超级用户身份访问主机控制台。
   请参见登录到计算服务器并更改默认密码 [49]。

2. 配置审计工具。

```
# auditconfig -setpolicy +argv
# auditconfig -setflags lo,ad,ex >& /dev/null
# auditconfig -setpolicy +zonename
```

▼ 在全局区域中启用数据链路（欺骗）保护

Oracle Solaris 数据链路保护可防止恶意来宾 VM 可能会对网络造成的潜在损害。

启用防窥探配置可以将虚拟环境的网络通信流量与主机系统接收或发送的更广泛的通信流量隔离开来，从而提高网络性能。链路保护可防止潜在恶意来宾 VM 可能会对网络造成的损害。该功能提供了针对以下基本威胁的保护：

- IP 和 MAC 欺骗
- L2 帧欺骗，例如网桥协议数据单元 (Bridge Protocol Data Unit, BPDU) 攻击

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **设置链路保护。**

```
# dladm set-linkprop -p protection=mac-nospoof,restricted,ip-nospoof,dhcp-
nospoof net0
```

3. **确认配置。**

```
# dladm show-linkprop -p protection net0
LINK         PROPERTY     PERM     VALUE         EFFECTIVE         DEFAULT     POSSIBLE
net0         protection     rw     mac-nospoof   mac-nospoof        --         mac-nospoof,
                                   restricted    restricted         --         restricted,
                                   ip-nospoof    ip-nospoof         --         ip-nospoof,

                                   dhcp-nospoof  dhcp-nospoof       --         dhcp-nospoof
```

4. **设置链路上允许的 IP。**

```
# dladm set-linkprop -p allowed-ips=10.0.0.1,10.0.0.2 net0
```

▼ 在非全局区域中启用数据链路（欺骗）保护

Oracle Solaris 数据链路保护也可以单独应用于在 SuperCluster 环境中部署的所有 Oracle Solaris 非全局区域。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **使用 `zonecfg(1M)` 命令在特定网络接口上强制实施数据链路保护。**
   确保允许的 IP 地址列表准确且完整。该列表必须包括 Oracle Solaris IPMP、Oracle Real Application Clusters 等使用的所有虚拟 IP 地址。另请注意，重新启动非全局区域后，对 SuperCluster 非全局区域配置所做的更改才会生效。

```
# zonecfg -z zonename
zonecfg:zonename> select anet linkname=network-link-name
zonecfg:zonename:anet> set allowed-address="list_of_allowed_IP_addresses"
zonecfg:zonename:anet>  set link-protection=mac-nospoof,ip-nospoof,restricted
zonecfg:zonename:anet>  set configure-allowed-address=false
zonecfg:zonename:anet>  end
zonecfg:zonename>  commit
zonecfg:zonename>  exit
```

▼ 创建加密的 ZFS 数据集

需要静态数据保护的组织可以选择使用加密的 ZFS 数据集来进一步保护区域部署的应用程序和信息。要确保每个非全局区域都能在没有管理员介入的情况下启动，应将加密的 ZFS 数据集配置为访问在各个数据库或应用程序域中本地存储的 ZFS 加密密钥。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**
   请参见登录到计算服务器并更改默认密码 [49]。

2. **创建 ZFS 加密密钥。**
   创建所需密钥的一种简单方法是使用类似于以下条目的命令：

```
# zfs createzfs_pool_name/zfskeystore
$ chown root:root /zfs_pool_name/zfskeystore
$ chmod 700 /zfs_pool_name/zfskeystore
$ pktool genkey keystore=file keytype=aes keylen=256 \
outkey=/zfs_pool_name/zfskeystore/zone_name.key
```

3. **创建加密的 ZFS 数据集。**

```
# zfs create -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zone_name.key \
zfs_pool_name/zone_name
```

4. **对 u01 和通用数据集进行加密。**
   可以采用同样的方法对 u01 和通用数据集进行加密，使用相同的（特定于 SuperCluster）密钥或每个数据集的唯一密钥，具体取决于特定于站点的要求和策略。

在本示例中，创建通用数据集所使用的密钥与在步骤 3 中创建的密钥相同。请注意，在创建这些额外数据集的过程中，也可以定义额外的 ZFS 配置参数，例如压缩。

```
# zfs create -o compression=on -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zfskeystore/zone_name.key \zfs_pool_name/u01
```

▼ （可选）为密钥库访问设置密码短语

前一项任务创建加密的 ZFS 数据集 [65]使用的是一个本地定义的（原始）密钥文件，该文件必须直接存储在文件系统上。另一个密钥存储技巧利用受密码短语保护的 PKCS#11 密钥库，称为 *Sun Software PKCS#11 Softtoken*。要使用这种方法，请执行本任务。

必须先手动解锁 PKCS#11 密钥库，然后密钥才能供 ZFS 使用。最终，这意味着需要手动管理介入来挂载加密的 ZFS 数据集（如果非全局区域也使用加密的 ZFS 数据集，那么还要启动该区域）。有关其他密钥存储策略的更多信息，请参阅 `zfs_encrypt(1M)` 手册页。

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**

   请参见登录到计算服务器并更改默认密码 [49]。

2. **设置访问密钥库所需的 PIN（密码短语）。**

   与新 PKCS#11 密钥库关联的默认 PIN 为 `changeme`。在本示例中第一个提示符处输入此密码短语。

   ```
   # pktool setpin keystore=pkcs11
   Enter token passphrase:
   Create new passphrase:
   Re-enter new passphrase:
   ```

3. **定义 `${SOFTTOKEN}` 环境变量，以将密钥存储在不同的位置。**

   默认情况下，PKCS#11 Softtoken 使用的密钥材料存储在 `/var/user/ ${USERNAME}/pkcs11_softtoken` 目录中。可以定义 `${SOFTTOKEN}` 环境变量，以将密钥材料存储在不同的位置。您可以使用此功能为受此密码短语保护的密钥材料启用特定于 SuperCluster 的存储。

   ```
   # export SOFTTOKEN=/<zfs_pool_name>/zfskeystore
   # pktool setpin keystore=pkcs11
   Enter token passphrase:
   Create new passphrase:
   Re-enter new passphrase:
   ```

4. **创建一个密钥。**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=zone_name_rpool
Enter PIN for Sun Software PKCS#11 softtoken:
```

5. **创建加密的 ZFS 数据集，使其引用在上一步中创建的密钥。**

```
# zfs create -o encryption=aes-256-ccm -o keysource=raw,pkcs11:
object=<zone_name>_rpool zfs_pool_name/zone_name
Enter PKCS#11 token PIN for 'zfs_pool_name/zone_name':
```

▼ 创建不可变全局区域

利用不变性防篡改可使全局区域和非全局区域创建高完整性弹性操作环境，SuperCluster 计算服务器可以在此环境中运行自己的服务。不可变区域基于 Oracle Solaris 全局区域和非全局区域固有的安全功能构建，可确保无法更改（部分或全部）OS 目录和文件（在没有管理员介入的情况下）。强制实施这种只读环境有助于防止未经授权的更改、促进更强大的变更管理过程，并阻止基于内核和用户的恶意软件的注入。

注 - 配置不可变区域后，除了通过可信路径登录或使用 `reboot -- -w` 在重新引导系统时利用可写模式以外，不能对该区域进行更新。

尽管始终都应该确认应用程序软件在不可变环境中按预期运行，但要知道，经验证，Oracle Database 实例和 Oracle RAC 群集可以在 Oracle Solaris 不可变非全局区域中正常运行。

1. **以超级用户身份登录到 Oracle Solaris 全局区域（专用域、根域或 I/O 域）。**

   请参见登录到计算服务器并更改默认密码 [49]。

2. **通过设置 `file-mac-profile` 属性来修改 Oracle Solaris 全局区域配置。**

```
# zonecfg -z global set file-mac-profile=fixed-configuration
zonecfg:global> commit
```

3. **重新引导 Oracle Solaris 全局区域以使更改生效。通过 ILOM 控制台登录到域。**

4. **启动不可变全局区域可信路径控制台。**

   配置不可变全局区域时，务必使用以下中断序列之一进入控制台登录：

   - **图形控制台**－F1-A
   - **串行控制台**－<Break> 或替代中断序列 (CR~ Ctrl-b)

```
trusted path console login:
```

5. **登录到 I/O 域的全局区域，承担 `root` 角色以对系统执行任何特定更新，然后重新引导系统使其返回只读模式。**

```
# reboot
```

▼ 配置不可变非全局区域

要将 Oracle Solaris 非全局区域配置为不可变区域，请执行本任务。

注 - 除本任务中指明的配置（固定配置）以外，Oracle Solaris 11 OS 还支持其他不可变区域配置。有关这些选项的更多信息，请参阅 `zonecfg(1M)` 手册页。但是，只有固定配置选项作为 SuperCluster 体系结构的一部分进行了测试。

注意 - 启用 Oracle Solaris 非全局区域不变性之后，不能添加、修改或删除区域用户帐户和密码，如本任务中所述。但是，可以部署一个 LDAP 目录，使其包含特定于区域的信息，例如用户、角色、组、权限配置文件等，由此解决这个问题。

注意 - Oracle Solaris 不可变区域功能限于默认情况下在 Oracle Solaris 非全局区域中实施的 ZFS 数据集。其他文件系统、池或数据集不遵循不可变区域策略，然而可以使用其他方式（例如，使用只读回送挂载）控制对这些文件元素的访问。

---

1. **登录到某一台计算服务器并以超级用户身份访问主机控制台。**

   请参见登录到计算服务器并更改默认密码 [49]。

2. **确保 Oracle Solaris 非全局区域已关闭。**

   如果以下命令返回一个值，表明 Oracle Solaris 非全局区域正在运行，您必须将其关闭。

注 - 尽管可以使用 `zoneadm(1M)` 命令停止区域，但是要遵循您的组织已建立的适当关闭过程，以避免潜在的服务中断和数据丢失。

```
# zoneadm list | grep -w "zone_name"
```

3. **通过设置 `file-mac-profile` 区域配置属性来调整 Oracle Solaris 非全局区域配置。**

```
# zonecfg -z zone_name set file-mac-profile=fixed-configuration
```

4. **如果需要，禁用非全局区域不可变配置。**

```
# zonecfg -z zone_name set file-mac-profile=none
```

5. **重新启动 Oracle Solaris 非全局区域以使更改生效。**

```
# zoneadm -z zone_name boot
```

▼ 启用安全验证的引导 (Oracle ILOM CLI)

执行本任务以通过 Oracle ILOM CLI 启用安全验证的引导。或者，您也可以使用 Oracle ILOM Web 界面。请参见"安全验证的引导（Oracle ILOM Web 界面）" [70]。

验证的引导是指使用数字签名在执行之前验证对象模块。Oracle Solaris 阻止装入行为异常的内核模块。验证的引导可以在执行之前验证内核模块，从而增强 Oracle Solaris 的安全性和稳健性。

启用后，Oracle Solaris 验证的引导将在装入并执行内核模块之前检查模块中出厂时签署的签名。这项检查可检测对模块的意外或恶意修改。执行的操作是可配置的，启用后，要么输出一条警告消息，继续装入并执行模块，要么操作失败，不会装入并执行模块。

1. **在计算服务器上访问 Oracle ILOM。**

   请参见登录到计算服务器并更改默认密码 [49]。

2. **启用验证的引导。**

```
-> set /HOST/verified_boot/ module_policy=enforce
Set 'module_policy' to 'enforce'
```

3. **访问并显示 Oracle 提供的证书。**

   预安装的验证的引导证书文件 `/etc/certs/ORCLS11SE` 作为 Oracle ILOM 的一部分提供。

```
# more /etc/certs/ORCLS11SE
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----
```

4. **启动证书的装入。**

```
-> set /HOST/verified_boot/user_certs/1 load_uri=console
```

5. **复制 `/etc/certs/ORCLS11SE` 文件的内容，并将其粘贴到 Oracle ILOM 控制台上。**

输入 Ctrl-z 保存并处理信息。

输入 Ctrl-c 退出并放弃更改。

```
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----^Z
Load successful.
```

6. 验证证书。

```
-> show /HOST/verified_boot/user_certs/1/
/HOST/verified_boot/user_certs/1
Targets:
Properties:
clear_action = (Cannot show property)
issuer = /C=US/O=Oracle Corporation/OU=VeriSign Trust Network/OU=Class 2 Managed PKI
 Individual
Subscriber CA/CN=Object Signing CA
load_uri = (Cannot show property)
subject = /O=Oracle Corporation/OU=Corporate Object Signing/OU=Solaris Signed Execution/
CN=Solaris 11
valid_from = Mar 1 00:00:00 2012 GMT
valid_until = Mar 1 23:59:59 2015 GMT
Commands:
cd
load
reset
show
->
```

7. 验证 **OBP `use-nvram` 参数是否设置为 `false`。**

使用验证的引导时，OBP `use-nvram` 参数必须设置为 `false`。这样可防止修改 OBP 以禁用验证的引导功能。默认值为 false。登录到 Oracle Solaris 并键入：

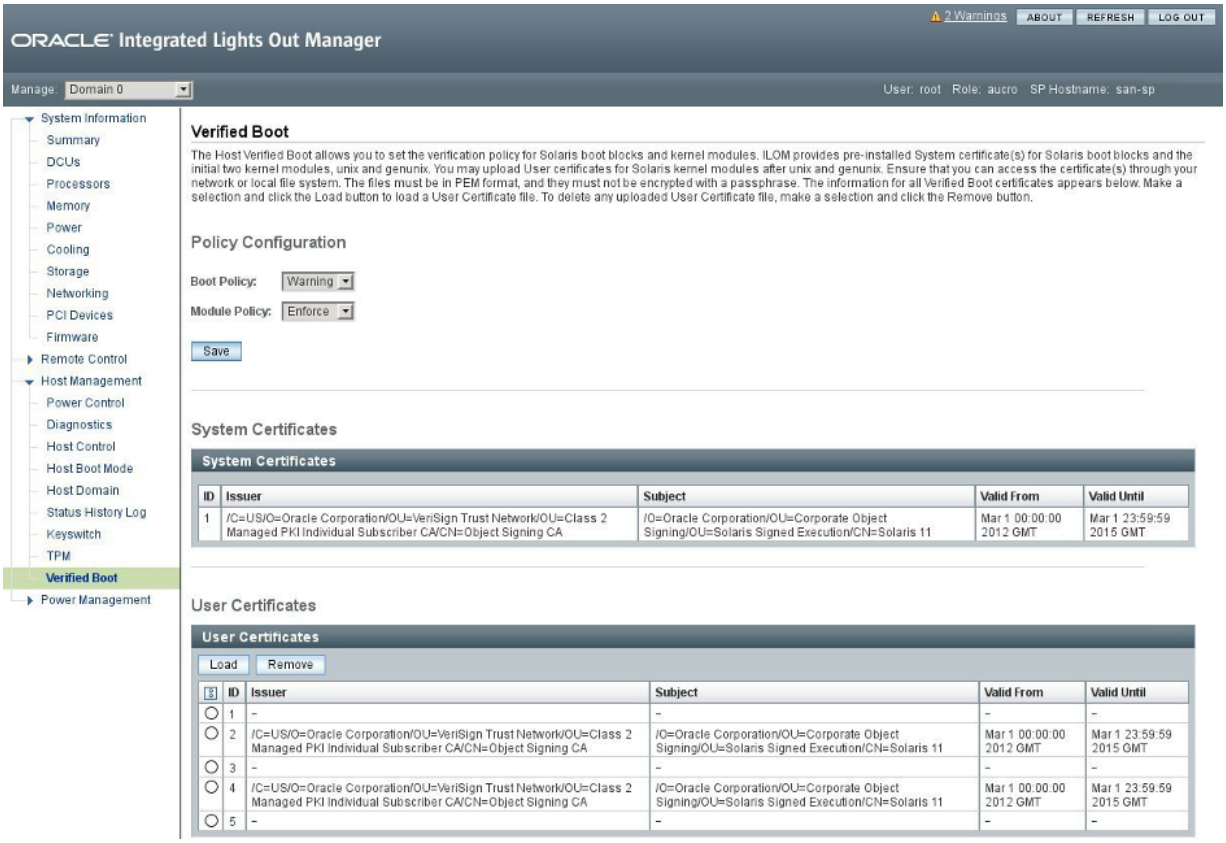
```
$ /usr/sbin/eeprom/eeprom use-nvramrc?

use-nvramrc?=false
```

安全验证的引导（Oracle ILOM Web 界面）

Oracle ILOM Web 界面也支持设置验证的引导策略变量和管理证书文件，提供的功能与 CLI 相同。导航到 "Host Management"（主机管理）导航菜单下的 "Verified Boot"（验证的引导）链接。

例如：



其他计算服务器资源

有关 Oracle Solaris OS 和 Oracle Solaris Cluster 安全指南，请参阅与您的 OS 版本对应的文档库。这些文档库位于 http:/docs.oracle.com/en/operating-systems。

有关 Oracle VM Server for SPARC 安全信息，请参阅位于 http://docs.oracle.com/cd/E62357_01 的安全指南。

有关计算服务器硬件的安全信息，请参阅位于 http://docs.oracle.com/cd/E55211_01 的安全指南。

保护 ZFS 存储设备

ZFS 存储设备是 SuperCluster 组件之一，用于在各种高要求工作负荷（包括商业智能、数据仓库、虚拟化、开发和测试以及数据保护）中为存储整合提供支持。

ZFS 存储设备配备两个冗余 ZFS 存储控制器。您必须保护这两个控制器。

下面几部分介绍了 ZFS 存储设备安全准则和功能：

▼ 登录到 ZFS 存储设备

要执行本部分中的安全任务，您需要通过管理网络登录到 ZFS 存储设备。

此任务介绍如何使用 CLI 登录。有关登录到 Oracle ILOM Web 界面的相应说明，请参阅《*Oracle ZFS Storage Appliance* 管理指南》。请参见“其他 ZFS 存储设备资源” [81]。

1. **在您的管理网络中，使用 SSH 连接到 ZFS 存储设备。**

   如果尚未配置其他用户来管理设备，则必须以 `root` 身份登录。

```
% ssh root@ZFS_Storage_App_IPaddress_or_hostname
Password:
Last login: Mon Oct 13 15:43:05 2015
hostname:>
```

2. **如有必要，请访问 CLI 帮助。**

   `help` 命令提供特定于上下文的帮助。有关特定主题的帮助可以通过将主题指定为 `help` 的参数来获得。通过使用 Tab 补齐 help 命令或键入 `help topics`，可显示现有的主题。

▼ 确定 ZFS 存储设备软件版本

使用以下过程确定 ZFS 存储设备上软件的版本。

1. **登录到 ZFS 存储设备。**
   请参见登录到 ZFS 存储设备 [73]。

2. **显示软件版本。**

```
hostname:> configuration version show
[...]
Appliance Product: Sun ZFS Storage 7320
Appliance Type: Sun ZFS Storage 7320
Appliance Version: 2013.06.05.2.10,1-2.1.1.1
[...]
```

在此示例中，ZFS 存储设备软件的版本为 `2013.06.05.2.10`。

要更新 ZFS 存储设备软件的版本，请安装最新的 SuperCluster Quarterly Full Stack Download Patch，该程序可从 My Oracle Support 上获得，网址为 `https://support.oracle.com`。

注 - 对于 SuperCluster 来说，一些附加限制条件可能会限制可以使用的 ZFS 存储设备软件版本并限制如何更新这些版本。在这些情况下，请与 Oracle 代表联系。

▼ 更改 ZFS 存储设备 root 密码

ZFS 存储设备本身未预配置默认 `root` 密码。ZFS 存储设备的初始配置通过控制台会话从嵌入式 Oracle ILOM 中执行。设备的 `root` 密码在此初始配置会话期间设置。

初次访问设备的控制台时，将显示 shell 接口配置屏幕。验证屏幕上的信息并输入所需的值。ZFS 存储设备的 `root` 密码在此过程中设置。

注 - 设备的 Oracle ILOM 具有默认 `root` 帐户，并且密码为 `welcome1`。请参见保护 Oracle ILOM [35]。

具有 `root` 帐户之后，您可以随时按此任务中所述更改密码。

注 - 如果为 Oracle Engineered Systems Hardware Manager 管理的任何 SuperCluster 组件（如 AFS 存储控制器 OS）更改了密码，您还必须在 Oracle Engineered Systems Hardware Manager 中更新密码。有关详细信息，请参阅《*Oracle SuperCluster M7* 系列管理指南》。

---

1. **登录到 ZFS 存储设备。**
   请参见登录到 ZFS 存储设备 [73]。

2. **更改 `root` 密码。**
   在此示例中，将 *password* 替换为符合美国国防部密码复杂性策略的密码。

```
hostname:> configuration users select root set initial_password=password initial_password
 = *************
hostname:configuration users> done
```

有关 ZFS 存储设备的初始安装和配置的更多信息，请参阅《*Oracle ZFS Storage Appliance* 安装指南》。请参见"其他 ZFS 存储设备资源" [81]。

默认公开的网络服务（ZFS 存储设备）

此表列出了 ZFS 存储设备公开的默认网络服务。

服务	协议	端口	说明
SSH	TCP	22	由安全 Shell 服务使用，用于允许使用 CLI 对 ZFS 存储设备进行管理访问。
PORTMAP	TCP/UDP	111	由远程过程调用 (Remote Procedure Call, RPC) 端口映射守护进程（名为 `rpcbind` 或 `portmap`）使用。需要此服务，才能支持 NFS 版本 3。
NTP	UDP	123	由集成的网络时间协议 (Network Time Protocol, NTP) 服务（仅限客户机）使用，用于将本地系统时钟与一个或多个外部时间源同步。
HTTPS (BUI)	TCP	215	由集成的 HTTPS 服务使用，用于允许使用浏览器界面通过加密 (SSL/TLS) 通道对 ZFS 存储设备进行管理访问。
远程复制	TCP	216	由集成的远程数据复制服务使用。远程数据复制服务复制和同步项目并通过加密 (SSL/TLS) 通道在 ZFS 存储设备之间共享。
NFS	TCP/UDP	2049 4045 许多	由网络文件系统 (network file system, NFS) 服务使用。NFS 提供网络文件共享服务。实际端口数取决于使用哪个版本的 NFS 协议。NFS 版本 3 依靠 RPC 端口映射守护进程（已在上文中列出）和动态分配的端口来提供挂载、状态、配额和相关服务。然而，NFS 版本 4 仅依靠 TCP/2049。NFS 锁定服务使用 TCP/4045。
iSCSI/iSNS	TCP	3260	由 iSCSI 服务使用，该服务为链路数据存储工具提供基于 IP 的存储联网协议。ZFS 存储设备可以配置为与联网的客户机共享 iSCSI 设备（称为 LUN）。
服务标签	TCP	6481	由 Oracle ServiceTag 服务使用。这是用于识别服务器和支持服务请求的 Oracle 搜索协议。Oracle Enterprise Manager Ops Center 等产品使用此服务搜索 ZFS 存储设备软件并与其他 Oracle 自动服务解决方案集成。
NDMP	TCP	10000	由网络数据管理协议 (Network Data Management Protocol, NDMP) 服务使用，该服务允许 ZFS 存储设备参与远程协调的备份。

ZFS 存储设备还支持其他许多默认情况下处于禁用状态的服务，包括 HTTP、FTP、SFTP、TFTP、WebDAV 等。如果在安装后启用这些服务，则可能会公开其他网络端口。

强化 ZFS 存储设备安全配置

以下主题介绍了如何强化 ZFS 存储设备的安全配置：

▼ 实施 Oracle ILOM 安全配置强化

ZFS 存储设备将 Oracle ILOM 嵌入到了产品中。与其他 Oracle ILOM 实施一样，您可以实施与安全相关的配置更改，以改进设备的默认安全配置。

- **通过执行保护 Oracle ILOM [35] 中的过程来保护 ZFS 存储设备 Oracle ILOM 界面。**

▼ 禁用不必要的服务（ZFS 存储设备）

禁用支持平台的运行和管理要求不需要的任何服务。

默认情况下，ZFS 存储设备采用网络默认安全配置，不必要的服务会被禁用。然而，根据您的安全策略和要求，可能需要启用或禁用更多服务。

1. **登录到 ZFS 存储设备。**
   请参见登录到 ZFS 存储设备 [73]。

2. **显示 ZFS 存储设备支持的服务列表。**

   hostname:> **configuration services**

3. **确定特定服务是否处于启用状态。**
   将 *servicename* 替换为在步骤 2 中确定的服务名称。

   ```
   hostname:> configuration services servicename get <status>
   ```

   如果服务状态参数返回值 `enabled`，则表明服务处于启用状态。例如：

   ```
   hostname:> configuration services iscsi get <status>
   <status> = online
   ```

4. **禁用不再需要的服务。**
   将服务状态设置为 disable。例如：

   ```
   hostname:> configuration services iscsi disable
   ```

▼ 禁用动态路由

ZFS 存储设备默认情况下配置为运行动态路由协议。

在禁用动态路由服务之前，请确保 ZFS 存储设备已直接连接到它可以与之通信的任何网络，或者确保已将其配置为使用静态路由或默认路由。为了确保禁用动态路由后连接不会中断，需要执行此步骤。

1. **登录到 ZFS 存储设备。**
   请参见登录到 ZFS 存储设备 [73]。

2. **禁用动态路由。**

   ```
   hostname:> configuration services dynrouting disable
   ```

3. **要确定动态路由是否处于启用状态，请键入：**

   ```
   hostname:> configuration services dynrouting get <status>
   ```

▼ 限制 root 使用安全 Shell 执行远程访问

默认情况下，ZFS 存储设备配置为允许 `root` 帐户使用安全 Shell (SSH) 服务执行远程管理访问。

使用以下过程可禁止 root 使用 SSH 执行远程访问。

作出此配置更改后，root 帐户不能再使用 SSH 访问系统。然而，root 帐户能够使用 HTTPS 管理界面访问此系统。

1. **登录到 ZFS 存储设备。**
   请参见登录到 ZFS 存储设备 [73]。

2. **禁止 root 执行远程访问。**

```
hostname:> configuration services ssh set permit_root_login=false
```

3. **确认不再允许 root 帐户使用 SSH 访问系统。**

```
hostname:> configuration services ssh get permit_root_login
```

4. **如果需要执行 SSH 管理访问，请至少创建一个非 root 帐户。**
   有关说明，请参阅与 ZFS 存储设备上运行的发行版相对应的《*Oracle ZFS Storage Appliance* 管理指南》。请参见"其他 ZFS 存储设备资源" [81]。

▼ 配置管理界面不活动超时 (HTTPS)

ZFS 存储设备支持在管理会话处于不活动状态达到预定义的分钟数后将其断开连接并注销。默认情况下，浏览器用户界面 (HTTPS) 在 15 分钟后将会话设为超时。

注 - ZFS 存储设备的 SSH 命令行界面中无等效的参数可强制实施不活动超时。

使用以下过程将不活动超时参数设置为定制值。

1. **登录到 ZFS 存储设备。**
   请参见登录到 ZFS 存储设备 [73]。

2. **查看当前与浏览器界面关联的不活动超时参数。**

```
hostname:> configuration preferences get session_timeout
session_timeout = 15
```

3. **配置超时参数。**
   session_timeout 值以分钟为单位指定（在此示例中为 10 分钟）。

```
hostname:> configuration preferences set session_timeout=10
session_timeout = 10
```

4. **通过再次执行步骤 2 来验证超时参数。**

▼ 禁用未获批准的 SNMP 协议

默认情况下，会在 ZFS 存储设备上启用 SNMPv1 和 SNMPv2c。ZFS 存储设备的所有受支持的产品版本均支持 SNMPv1/v2c。从版本 2013.1.2 开始，ZFS 存储设备还支持 SNMPv3。

注 - SNMP 协议版本 3 引入了对基于用户的安全模型 (User-based Security Model, USM) 的支持。此功能使用实际用户帐户取代了传统的 SNMP 团体字符串，可以为用户帐户配置特定权限、验证、隐私协议和密码。默认情况下，ZFS 存储设备未包含集成（只读）USM 帐户的用户名或密码。出于安全考虑，请基于部署、管理和监视要求配置 USM 凭证和协议。

确保禁用未使用或较旧的 SNMP 协议版本，除非需要使用它们。

1. **登录到 ZFS 存储设备。**
   请参见登录到 ZFS 存储设备 [73]。

2. **确定设备使用哪个版本的 SNMP 协议。**

```
hostname:> configuration services snmp get version
version = v2
```

3. **启用 SNMPv3（如果可用）。**
   使用 SNMPv1/v2c 和 SNMPv3 是互斥的，因此在您启用 SNMPv3 时，SNMPv1/v2c 会被禁用。

```
hostname:> configuration services snmp set version=v3
version = v3
```

4. **验证 SNMP 的版本。**

```
hostname:> configuration services snmp get version
version = v3
```

▼ 配置 SNMP 团体字符串

仅当 ZFS 存储设备配置为使用 SNMPv1 或 v2 时才执行此任务。

由于 SNMP 通常用于监视设备的运行状况，因此将设备使用的默认 SNMP 团体字符串更改为客户定义的值非常重要。

1. **登录到 ZFS 存储设备。**

   请参见登录到 ZFS 存储设备 [73]。

2. **更改 SNMP 团体字符串。**

   在此示例中，将 *string* 替换为符合美国国防部有关 SNMP 团体字符串组成部分的要求的值。

```
hostname:> configuration services snmp set community=string
community = value
```

3. **验证 SNMP 团体字符串。**

```
hostname:> configuration services snmp get community
```

▼ 配置 SNMP 授权网络

仅当 ZFS 存储设备配置为使用 SNMPv1 或 v2 时才执行此任务。

为了最大限度地降低泄露系统配置信息的可能性，应该仅接受来自已获批准的网络或主机来源的 SNMP 查询。

1. **登录到 ZFS 存储设备。**

   请参见登录到 ZFS 存储设备 [73]。

2. **配置 SNMP 授权网络参数。**

```
hostname:> configuration services snmp set network=127.0.0.1/8
network = 127.0.0.1/8
```

3. **检查 SNMP 授权网络参数的值。**

   在此示例中，网络参数设置为 `127.0.0.1/8`，这样将有效地阻止所有基于网络的 SNMP 查询。应根据需要调整此值，以允许已获批准的主机和网络。

   如果值为 `0.0.0.0/0`，将允许来自任何网络位置的查询。

```
hostname:> configuration services snmp get network
network = 127.0.0.1/8
```

▼ 限制管理网络访问

除了上述安全强化过程之外，还必须在专用的隔离管理网络中部署 ZFS 存储设备公开的管理接口。此步骤有助于 ZFS 存储设备防御未经授权或不必要的管理网络通信流量。您必须严格控制对管理网络的访问，仅将访问权限授予需要进行此级别访问的管理员。

另外，可以将 ZFS 存储设备配置为允许或禁止通过特定网络接口进行管理访问。此更改可以通过以下过程来实施。

1. **登录到 ZFS 存储设备。**

   请参见登录到 ZFS 存储设备 [73]。

2. **配置管理网络接口。**

   在此示例中，将 *interface* 的值替换为此设置应用于的实际网络接口的名称。

   hostname:> **configuration net interfaces select** *interface* **set admin=false**

其他 ZFS 存储设备资源

有关 ZFS 存储设备的其他安全准则，请参阅与 ZFS 存储设备上运行的发行版相对应的安全指南。请参见确定 ZFS 存储设备软件版本 [74]。

以下指南提供了有关产品安全特性、功能和配置选项的其他信息：

- 《*Oracle ZFS Storage Appliance Security Guide, Release 2013.1.4.0*》（《Oracle ZFS Storage Appliance 发行版安全指南，发行版 2013.1.4.0》）

  http://docs.oracle.com//cd/E56047_01
- 《*Oracle ZFS Storage Appliance Security Guide*》（《Oracle ZFS Storage Appliance 安全指南》）（发行版 2013.1.3.0）

  http://docs.oracle.com/cd/E56021_01
- 《*Oracle ZFS Storage Appliance Security Guide*》（《Oracle ZFS Storage Appliance 安全指南》）（发行版 2013.1.2.0）

  http://docs.oracle.com/cd/E51475_01

保护 Exadata 存储服务器

Exadata 存储服务器（以下简称存储服务器）是 SuperCluster 的存储构建块。每台存储服务器在交付时都已预安装并作为 SuperCluster M7 的一部分与其所有必要的计算、存储和软件组件相集成。

注 - 只允许您应用批准的方法、修补程序或更新对配置进行更改。不得以其他任何方式更改存储服务器软件。

SuperCluster M7 至少有三个存储服务器。可以在 SuperCluster 主机架和可选的扩展机架中安装额外的存储服务器。您必须保护每个存储服务器。

以下主题介绍了如何保护存储服务器：

▼ 登录到存储服务器 OS

- **在管理网络上，以 `celladmin` 身份登录到某一台存储服务器。**
  有关默认密码，请参见“默认帐户和密码” [83]。

```
# ssh celladmin@Storage_Server_IP_address
```

默认帐户和密码

下表列出了存储服务器的默认帐户和密码。

帐户名称	类型	默认密码	说明
root	管理员	welcome1	用于访问存储服务器 OS 以执行常规管理操作并更新存储服务器软件。
celladmin	单元管理员	welcome	用于执行存储服务器设置和配置。此外，平台上的所有存储服务都使用此帐户运行。
cellmonitor	监视员	welcome	仅用于监视目的。此帐户使用受限 shell 以确保无法从此帐户修改存储服务器上的配置和对象。

▼ 更改存储服务器密码

有关默认帐户和密码的列表，请参见"默认帐户和密码" [83]。

注 - 如果更改了 Oracle Engineered Systems Hardware Manager 管理的任何 SuperCluster 组件（例如 Exadata 存储服务器 OS）的密码，也必须在 Oracle Engineered Systems Hardware Manager 中更新密码。有关详细信息，请参阅《*Oracle SuperCluster M7* 系列管理指南》。

1. **以 `celladmin` 身份登录到存储服务器。**
   请参见登录到存储服务器 OS [83]。
2. **使用以下方法之一更改默认密码。**
   - **在您登录到的服务器上更改一个帐户的密码。**

     ```
     # passwd account_name
     ```

   - **在所有存储服务器上更改一个帐户密码。**
     `cell_group` 是一个简单的文本文件，列出了所有存储服务器的主机名（每行一个）。
     在本示例中，将以下命令行项目：
     - *new_password*－替换为符合站点策略的新密码。
     - *account_name*－替换为 Oracle Linux 帐户的名称。

     ```
     # dcli -g cell_group -l root "echo new_password | passwd --stdin account_name"
     ```

▼ 确定 Exadata 存储服务器软件版本

1. **登录到某一台存储服务器。**

请参见登录到存储服务器 OS [83]。

2. **键入以下命令。**

   在本示例中，存储服务器软件版本为 12.1.2.1.1.150316.2。

   ```
   # imageinfo -ver
   12.1.2.1.1.150316.2
   ```

   要更新软件的版本，请安装最新的 SuperCluster Quarterly Full Stack Download Patch，该程序可从 My Oracle Support 上获得，网址为 `https://support.oracle.com`。

   注 - 对于 SuperCluster，可能会有额外的限制，限制可使用哪些软件版本以及如何更新这些版本。在这些情况下，请与 Oracle 代表联系。

默认公开的网络服务（存储服务器）

服务名称	协议	端口	说明
SSH	TCP	22	由安全 Shell 服务使用，该服务集成到存储服务器软件中，使用 CLI 提供对系统的管理访问。 默认情况下，安全 Shell 服务器配置为仅响应管理 (NET 0) 和 IB (BONDIB0) 网络上的连接请求。

存储服务器还使用可靠数据报套接字 (RDSv3) 协议通过远程直接内存访问 (remote direct memory access, RDMA) 接口与 SuperCluster 上的 Oracle 数据库域进行通信。这种点对点通信不使用 TCP/IP，并且限于 SuperCluster 上的 Oracle 数据库域和存储服务器所在的内部 IB 网络分区。

强化存储服务器安全配置

注 - 存储服务器包括一个嵌入式 Oracle ILOM 作为产品的一部分。与其他 Oracle ILOM 实施一样，也可以实施与安全性相关的配置更改，对设备的默认安全配置加以改进。有关更多信息，请参见保护 Oracle ILOM [35]。

以下主题介绍了如何强化存储服务器的安全性：

- “安全配置限制” [86]
- 使用 `host_access_control` 显示可用安全配置 [86]

安全配置限制

要在存储服务器上实施安全配置更改，host_access_control 实用程序是唯一一种经允许且受支持的方法。按照 Oracle 技术支持公告 1068804.1，不允许您对这些设备的配置进行手动更改。另外，在使用此工具之前，您必须先获得 Oracle SuperCluster 技术支持的明确批准，然后才能更改存储服务器的安全配置。要申请这项批准，请向 Oracle 技术支持开立服务请求。

host_access_control 命令自 Exadata 软件版本 11.2.3.3.0 起提供，用于实施有限的一组访问和安全配置设置：

- 限制远程 root 访问。
- 限制对某些帐户的网络访问。
- 实施密码生命期和复杂性策略。
- 实施登录警告标题。
- 定义帐户锁定和会话超时策略。

▼ 使用 host_access_control 显示可用安全配置

要查看 host_access_control 实用程序中提供的内容，请执行以下步骤。

1. **登录到存储服务器 OS。**
   请参见登录到存储服务器 OS [83]。

2. **（可选）显示 host_access_control 帮助，查看详细信息。**

```
# /opt/oracle.cellos/host_access_control --help
```

▼ 配置系统引导装载程序密码

您可以将存储服务器配置为每当管理员尝试访问引导装载程序 (GRUB) 编辑器或命令接口时都要求提供系统引导装载程序密码。

1. **以 `celladmin` 身份登录到存储服务器。**

   请参见登录到存储服务器 OS [83]。

2. **配置系统引导装载程序密码。**

```
# /opt/oracle.cellos/host_access_control grub-password
New GRUB password: password
Retype new GRUB password: password
[...]
```

3. **验证设置。**

   如果命令返回了一个与本示例类似的值，表明已安装引导装载程序密码。

```
# grep "^password" /etc/grub.conf
password --md5 $1$Hdner/$Q2VoiZeTJwmNQsFnH9oFy.
```

▼ 禁用 Oracle ILOM 系统控制台访问

每台存储服务器都包括一个嵌入式 Oracle ILOM 以实现远程监视和管理。Oracle ILOM 也可用于提供对存储服务器系统控制台的远程访问。

如果要禁用通过 Oracle ILOM 对存储服务器的访问，请执行以下过程。

1. **以 `celladmin` 身份登录到存储服务器。**

   请参见登录到存储服务器 OS [83]。

2. **禁用 Oracle ILOM 系统控制台访问。**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --lock
```

3. **验证设置。**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --status
```

▼ 限制使用 SSH 进行远程 root 访问

默认情况下，允许 root 用户远程访问每台存储服务器。

1. **以 celladmin 身份登录到存储服务器。**
   请参见登录到存储服务器 OS [83]。

2. **禁用通过 SSH 进行远程 root 访问。**

```
# /opt/oracle.cellos/host_access_control rootssh --lock
```

3. **验证设置。**

```
# /opt/oracle.cellos/host_access_control rootssh --status
```

▼ 配置系统帐户锁定

默认情况下，存储服务器配置为在连续五次尝试验证失败后锁定系统帐户。

要更改该阈值，请执行以下过程。

1. **以 celladmin 身份登录到存储服务器。**
   请参见登录到存储服务器 OS [83]。

2. **更改该阈值。**
   按照美国国防部的安全要求，应指定值 3。如有必要，将该值替换为符合您的本地站点策略的值。

```
# /opt/oracle.cellos/host_access_control pam-auth --deny 3
```

3. **验证设置。**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep deny=
```

▼ 配置密码复杂性规则

默认情况下，存储服务器不实施任何重要的限制来管控系统帐户密码的复杂性。

1. **以 `celladmin` 身份登录到存储服务器。**
   请参见登录到存储服务器 OS [83]。

2. **定义密码复杂性策略。**
   语法：

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc N0,N1,N2,N3,N4
```

将 *N0,N1,N2,N3,N4* 替换为以逗号分隔的五个值。这五个值共同设置实际系统密码复杂性策略。这些值如下所示（也在 `passwdqc.conf(5)` 手册页中列出）：

- *N0*－用于仅包含一个字符分类（数字、小写字符、大写字符和特殊字符）的密码。一般来说，此参数设置为 `disabled`，因为简单的密码不安全。
- *N1*－用于包含两个字符分类的不符合密码短语要求的密码。要使此规则适用，密码长度必须至少为 N1 个字符。
- *N2*－用于包含一个密码短语的密码。要使此规则适用，密码长度必须至少为 N2 个字符且必须符合密码短语要求。
- *N3*－用于至少包含三个字符分类的密码。要使此规则适用，密码长度必须至少为 N3 个字符。
- *N4*－用于至少包含四个字符分类的密码。要使此规则适用，密码长度必须至少为 *N4* 个字符。

按照美国国防部的安全要求，应将 *N0,N1,N2,N3,N4* 参数设置为 `disabled,disabled,disabled,disabled,15`。这样可确保仅接受至少包含四个字符分类（大写、小写、数字和特殊字符）且长度至少为 15 个字符的密码。

注 - 计算字符分类数时，密码开头的大写字符和密码结尾的数字不计算在内。

例如，要设置符合美国国防部要求的密码复杂性，请键入：

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc
 disabled,disabled,disabled,disabled,15
```

3. **验证此设置的当前状态。**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep min=
```

▼ 配置密码历史记录策略

默认情况下，存储服务器会定义一个密码历史记录策略，以防止用户重用他们过去的十 (10) 个密码。

1. **以 `celladmin` 身份登录到存储服务器。**
   请参见登录到存储服务器 OS [83]。

2. **查看当前的设置。**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep remember=
```

3. **更改密码历史记录。**
   按照美国国防部的安全要求和 PCI-DSS 要求，应将密码历史记录策略设置为 5。这样可确保帐户无法重用分配给该帐户的前五个密码中的任何一个。如有必要，将该值替换为符合您的本地站点策略的值。

```
# /opt/oracle.cellos/host_access_control pam-auth --remember 5
```

4. **要验证设置，请重复执行步骤 2。**

▼ 配置验证失败锁定延迟

默认情况下，存储服务器实施一项策略，规定在任何一次尝试验证失败后都将系统帐户锁定 10 分钟。

要更改该阈值，请执行以下过程。

1. **以 `celladmin` 身份登录到存储服务器。**
   请参见登录到存储服务器 OS [83]。

2. **查看当前的设置。**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep lock_time=
```

3. **更改该阈值。**
   按照美国国防部的安全要求，应将值设置为 4（秒）。如有必要，将该值替换为符合您的本地站点策略的值。

```
# /opt/oracle.cellos/host_access_control pam-auth --lock 4
```

4. **要验证设置，请重复执行步骤 2。**

▼ 配置密码生命期控制策略

存储服务器支持多种密码生命期控制，包括用于控制以下几点的参数：使用密码的最大天数、更改密码的最短间隔天数以及在密码到期前警告用户的提前天数。

按照美国国防部的安全要求和 PCI-DSS 要求，应使用下表中美国国防部的值：

策略	Oracle 默认值	DOD 值
最长密码生命周期	90 天	60 天
最短密码生命周期	1 天	1 天
最短密码长度	8 个字符	15 个字符
密码到期警告	7 天	7 天

要更改其中任何参数，请执行以下过程。

1. **以 `celladmin` 身份登录到存储服务器。**
   请参见登录到存储服务器 OS [83]。

2. **查看当前的设置。**

   ```
   # /opt/oracle.cellos/host_access_control password-policy --status
   ```

3. **根据您的站点密码策略配置这些策略。**

   - **要更改最长密码生命周期参数，请键入：**

     ```
     # /opt/oracle.cellos/host_access_control password-policy --PASS_MAX_DAYS 60
     ```

   - **要更改最短密码生命周期参数，请键入：**

     ```
     # /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_DAYS 1
     ```

   - **要更改最短密码长度参数，请键入：**

     ```
     # /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_LEN 15
     ```

   - **要更改密码到期警告参数，请键入：**

     ```
     # /opt/oracle.cellos/host_access_control password-policy --PASS_WARN_AGE 7
     ```

4. **要验证设置，请重复执行步骤 2。**

▼ 配置管理接口不活动超时（登录 Shell）

存储服务器支持终止处于不活动状态超过预定义秒数的管理会话的功能。

要为系统帐户登录 shell 定义管理接口不活动超时，请执行以下过程。

1. **以 `celladmin` 身份登录到存储服务器。**
   请参见登录到存储服务器 OS [83]。

2. **查看当前的设置。**

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --status | grep Shell
   ```

3. **定义管理接口不活动超时。**
   按照美国国防部的安全要求和 PCI-DSS 要求，应指定值 `900`（秒）。如有必要，将该值替换为符合您的本地站点策略的值。

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --shell 900
   ```

4. **要验证设置，请重复执行步骤 2。**

▼ 配置管理接口不活动超时（安全 Shell）

存储服务器支持终止处于不活动状态超过预定义秒数的管理 SSH 会话的功能。

要为 SSH 会话定义管理接口不活动超时，请执行以下过程。

1. **以 `celladmin` 身份登录到存储服务器。**
   请参见登录到存储服务器 OS [83]。

2. **查看当前的设置。**

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --status | grep SSH
   ```

3. **为 SSH 会话定义管理接口不活动超时。**
   按照美国国防部的安全要求，应指定值 `900`（秒）。如有必要，将该值替换为符合本地站点策略的值。

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --client 900
   ```

4. **要验证设置，请重复执行步骤 2。**

▼ 配置登录警告标题（存储服务器）

存储服务器支持在用户成功向系统验证之前显示特定于客户的消息的功能。

要定义验证前登录警告标题，请执行以下过程。

1. **以 `celladmin` 身份登录到存储服务器。**
   请参见登录到存储服务器 OS [83]。

2. **确定当前的设置。**

   ```
   # /opt/oracle.cellos/host_access_control banner --status
   ```

3. **创建一个包含批准的登录警告标题消息的文本文件。**

4. **定义验证前登录警告标题。**
   按照美国国防部的安全要求，应将 *filename* 替换为包含批准的登录警告标题消息的文件的路径和名称。

   ```
   # /opt/oracle.cellos/host_access_control banner --file filename
   ```

5. **要验证设置，请重复执行步骤 2。**

限制远程网络访问

您可以通过实施过滤规则集来限制对存储服务器的入站远程网络访问。您还可以通过定义定制规则集来微调网络访问。

使用以下过程来限制远程访问。

- “存储服务器管理网络隔离” [93]
- 限制远程网络访问 [94]

存储服务器管理网络隔离

存储服务器部署在一个隔离的专用管理网络上。这有助于存储服务器防御未经授权或不必要的网络通信流量。对管理网络的访问必须严格控制，只将访问权限授予需要该级别访问权限的管理员。

▼ 限制远程网络访问

您可以采用多种方法限制存储服务器上的远程网络访问。您可以通过实施自上而下的过滤规则集（按用户帐户和起源定义访问权限）来限制对存储服务器的入站网络访问。您还可以定义定制规则集，按照美国国防部和 PCI-DSS 要求允许或拒绝访问。

注意 - 实施非默认策略时务必小心，以确保对系统的访问不会中断。添加各个新规则时，更改立即生效。

要实施规则集，请执行以下过程。

1. **以 `celladmin` 身份登录到存储服务器。**
   请参见登录到存储服务器 OS [83]。

2. **检查有效的规则集。**

   ```
   # /opt/oracle.cellos/host_access_control access --status
   ```

3. **将当前的规则集导出到一个文件中，并将其另存为备份副本。**
   以下命令可将规则集导出到一个 ASCII 文本文件中：

   ```
   # /opt/oracle.cellos/host_access_control access-export --file filename
   ```

4. **根据您希望用来创建规则集的方法，通过执行下面的一个或多个命令来配置规则集：**

   - **要实施一个消除入站网络限制的开放式规则集，请键入：**

     ```
     # /opt/oracle.cellos/host_access_control access --open
     ```

   - **要实施一个仅允许使用 SSH 进行入站访问的闭合式规则集，请键入：**

     ```
     # /opt/oracle.cellos/host_access_control access --close
     ```

   - **要修改现有规则集，请键入：**
     将当前的规则集导出到一个 ASCII 文本文件中：

     ```
     # /opt/oracle.cellos/host_access_control access-export --file filename
     ```

     使用编辑器编辑该文本文件以配置规则集。
     从该文本文件导入规则集，从而覆盖当前的规则集：

     ```
     # /opt/oracle.cellos/host_access_control access-import --file filename
     ```

- **单独添加特定规则：**

  这种方法包括根据以下参数允许和拒绝访问：

  - **用户名**－有效值包括关键字 `all` 或者一个或多个有效的本地帐户用户名。
  - **起源**－有效值包括关键字 `all` 或者描述系统访问来源的各个条目，来源包括控制台、虚拟控制台、Oracle ILOM、IP 地址、网络地址、主机名或 DNS 域。

  在本示例中，当从 `trustedhost.example.org` 主机或 `.trusted.domain.com` 域中的任何主机发起连接时，将对存储服务器的访问权限授予 `celladmin` 用户。

```
# /opt/oracle.cellos/host_access_control access --add --user celladmin \
--origins trustedhost.example.org,.trusted.domain.com
```

其他存储服务器资源

请参阅《Exadata Database Machine Security Guide》（《Exadata Database Machine 安全指南》），网址为 http://docs.oracle.com/cd/E50790_01/welcome.html。

保护 IB 和以太网交换机

SuperCluster 使用的 Oracle Sun Data Center InfiniBand Switch 36 为所有内部组件依赖的高性能、高度可扩展和完全冗余底板奠定了网络基础。

IB 交换机用于连接计算服务器、存储单元和 ZFS 存储设备。IB 交换机包含嵌入式 Oracle ILOM，以提供高级管理和监视功能。特别是，Oracle ILOM 允许监视和控制用户、硬件、服务、协议和其他配置参数。

SuperCluster M7 至少具有两个 IB 交换机，还可以安装更多 IB 交换机以满足更高配置的需求。您必须保护每个 IB 交换机。

以下主题介绍了如何保护 SuperCluster M7 中的 IB 交换机：

▼ 登录到 IB 交换机

此任务介绍如何登录到交换机上的 Oracle ILOM 界面，可以通过该界面执行大多数管理任务。

- **在管理网络上，以 `ilom-admin` 身份登录到 IB 交换机上的 Oracle ILOM。**

  有关默认密码，请参见“默认帐户和密码（IB 交换机）” [98]。

```
% ssh ilom-admin@IB_Switch_ILOM_IPaddress
->
```

▼ 确定 IB 交换机固件版本

要利用最新特性、功能和安全增强功能，请确保使用受支持的最新固件版本更新 IB 交换机。

1. **以 `ilom-admin` 身份登录到 IB 交换机。**

   请参见登录到 IB 交换机 [97]。

2. **显示固件版本。**

   在此示例中，IB 交换机固件的版本为 `2.1.5-1`。

```
-> version
SP firmware 2.1.5-1
SP firmware build number: 47111
SP firmware date: Sat Aug 24 16:59:14 IST 2013
SP filesystem version: 0.1.22
```

要更新 IB 交换机固件的版本，请安装最新的 SuperCluster Quarterly Full Stack Download Patch，该程序可从 My Oracle Support 上获得，网址为 `https://support.oracle.com`。

注 - 对于 SuperCluster M7 来说，其他限制条件可能会限制可以使用的 IB 交换机软件版本。这些限制条件还决定固件的更新方式。在这些情况下，请与 Oracle 代表联系。

默认帐户和密码（IB 交换机）

帐户名称	类型	默认密码	说明
`root`	管理员	`welcome1`	用于访问 IB 交换机 OS。一般不使用此帐户，而是使用 `ilom-admin`、`ilom-operator` 或客户定义的帐户。
`ilom-admin`	管理员	`ilom-admin`	用于通过嵌入式 Oracle ILOM 软件执行管理功能、执行软件升级、配置用户和服务，以及执行 IB 交换机诊断和结构管理功能。
`ilom-operator`	操作员	`ilom-operator`	仅用于执行 Oracle ILOM 监视和 IB 结构诊断功能。
`nm2user`	只读	`changeme`	此帐户仅对 IB 交换机的命令行管理界面具有只读特权。Oracle Enterprise Manager 通常使用此帐户来支持交换机硬件和软件监视。

▼ 更改 root 和 nm2user 密码

IB 交换机在两个位置维护系统帐户。root 和 nm2user 帐户由交换机的底层 OS 配置和公开。不支持在该层添加、删除或更改帐户，但您必须更改默认密码。

对于其他帐户和密码，请参见更改 IB 交换机密码 (Oracle ILOM) [99]。

IB 交换机不支持定义或强制实施密码复杂性、生命期、历史记录或其他规则。您必须确保指定的密码符合美国国防部提出的密码复杂性要求，并实施用于确保根据美国国防部政策更新密码的流程。

有关 IB 交换机帐户管理的更多信息，包括如何创建新帐户、为现有帐户指定权限或删除帐户，请参阅《*Oracle Sun Data Center InfiniBand Switch 36 Hardware Security Guide*》和《*Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36*》。请参见"其他 IB 交换机资源" [105]。

注 - 如果为 Oracle Engineered Systems Hardware Manager 管理的任何 SuperCluster 组件（如 IB 交换机）更改了密码，您还必须在 Oracle Engineered Systems Hardware Manager 中更新密码。有关详细信息，请参阅《*Oracle SuperCluster M7* 系列管理指南》。

---

1. **以 root 身份登录到 IB 交换机。**

   ```
   # ssh root@IB_Switch_IP_address
   ```

   有关默认密码，请参见"默认帐户和密码（IB 交换机）" [98]。

2. **更改 root 密码。**

   ```
   $ passwd root
   ```

3. **更改 nm2user 密码。**

   ```
   $ passwd nm2user
   ```

▼ 更改 IB 交换机密码 (Oracle ILOM)

IB 交换机在两个位置维护系统帐户。本部分介绍如何在 IB 交换机的 Oracle ILOM 界面中更改密码。有关其他帐户和密码，请参见更改 root 和 nm2user 密码 [99]。

默认 IB 交换机帐户和所有客户定义的帐户都通过 IB 交换机上的嵌入式 Oracle ILOM 进行管理。

要查看帐户和更改密码，请执行以下过程。

1. **以 `ilom-admin` 身份登录到 IB 交换机。**

   请参见登录到 IB 交换机 [97]。

   有关默认密码，请参见“默认帐户和密码（IB 交换机）” [98]。

2. **查看在 IB 交换机上配置的 Oracle ILOM 帐户。**

   ```
   -> show /SP/users
   ```

3. **更改 `ilom-admin` 帐户的密码。**

   ```
   -> set /SP/users/ilom-admin password=password
   ```

IB 交换机网络隔离

IB 交换机的管理接口部署在专用的隔离管理网络中。这有助于 IB 交换机防御未经授权或不必要的网络通信流量。

对此管理网络的访问必须受到严格控制，仅将访问权限授予需要进行此级别访问的管理员。

默认公开的网络服务（IB 交换机）

服务名称	协议	端口	说明
SSH	TCP	22	由集成的安全 Shell 服务使用，用于允许使用 CLI 对 IB 交换机进行管理访问。
HTTP (BUI)	TCP	80	由集成的 HTTP 服务使用，用于允许使用浏览器界面对 IB 交换机进行管理访问。尽管 TCP/80 通常用于以明文形式进行访问，但默认情况下 IB 交换机会自动将传入的请求重定向到此服务的安全版本（在 TCP/443 上运行）。
NTP	UDP	123	由集成的网络时间协议 (Network Time Protocol, NTP)（仅限客户机）服务使用，用于将本地系统时钟与一个或多个外部时间源同步。
SNMP	UDP	161	由集成的 SNMP 服务使用，用于提供管理接口以监视 IB 交换机的运行状况和监视收到的陷阱通知。
HTTPS (BUI)	TCP	443	由集成的 HTTPS 服务使用，用于允许使用浏览器界面通过加密 (SSL/TLS) 通道对 IB 交换机进行管理访问。
IPMI	TCP	623	由集成的智能平台管理接口 (Intelligence Platform Management Interface, IPMI) 服务使用，用于为各种监视和管理功能提供计算机接口。请勿禁用此服务，因为 Oracle Enterprise Manager Ops Center 使用它来收集硬件清单数据、现场可更换单元说明、硬件传感器信息和硬件组件状态信息。

服务名称	协议	端口	说明
ServiceTag	TCP	6481	由 Oracle ServiceTag 服务使用。这是用于识别服务器和支持服务请求的 Oracle 搜索协议。Oracle Enterprise Manager Ops Center 等产品使用此服务搜索 IB 交换机软件并与其他 Oracle 自动服务解决方案集成。

强化 IB 交换机配置

以下主题介绍了如何通过各种配置设置来保护 IB 交换机。

▼ 禁用不必要的服务（IB 交换机）

禁用支持平台的运行和管理要求不需要的任何服务。默认情况下，IB 交换机采用网络“默认安全”配置，不必要的服务已被禁用。然而，根据客户的安全策略和要求，可能需要禁用更多服务。

1. **以 `ilom-admin` 身份登录到 IB 交换机。**

   请参见登录到 IB 交换机 [97]。

2. **确定 IB 交换机支持的服务列表。**

   ```
   -> show /SP/services
   ```

3. **确定特定服务是否处于启用状态。**

   将 *servicename* 替换为步骤 2 中的服务名称。

   ```
   -> show /SP/services/servicename servicestate
   ```

   尽管大多数服务都可以识别 `servicestate` 参数并使用它来记录服务处于启用还是禁用状态，但一些服务（如 `servicetag`、`ssh`、`sso` 和 `wsman`）使用名为 `state` 的参数。无论使用的实际参数是什么，如果服务状态参数返回的值为 `enabled`，则表示服务处于启用状态，如以下示例中所示：

```
-> show /SP/services/https servicestate
/SP/services/https
Properties:
servicestate = enabled

-> show /SP/services/ssh state
/SP/services/ssh
Properties:
state = enabled
```

4. **要禁用不再需要的服务，请将服务状态设置为 `disabled`。**

```
-> set /SP/services/http servicestate=disabled
```

5. **确定是否应禁用任何服务。**

   根据使用的工具和方法，如果不需要或不使用 HTTP 和 HTTPS 浏览器服务，则可以将其禁用。键入：

```
-> set /SP/services/http servicestate=disabled
-> set /SP/services/http secureredirect=disabled
-> set /SP/services/https servicestate=disabled
```

   - 浏览器管理界面 (HTTP, HTTPS)：

     -> set /SP/services/http servicestate=disabled

     -> set /SP/services/http secureredirect=disabled

     -> set /SP/services/https servicestate=disabled

▼ 配置指向 HTTPS 的 HTTP 重定向（IB 交换机）

默认情况下，IB 交换机配置为将传入的 HTTP 请求重定向到 HTTPS 服务，以确保交换机和管理员之间基于浏览器的所有通信均经过加密。

1. **以 `ilom-admin` 身份登录到 IB 交换机。**

   请参见登录到 IB 交换机 [97]。

2. **验证安全重定向是否已启用。**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **如果更改了默认设置，则您可以启用安全重定向。**

```
-> set /SP/services/http secureredirect=enabled
```

▼ 禁用未获批准的 SNMP 协议（IB 交换机）

默认情况下，会同时为用于监视和管理 IB 交换机的 SNMP 服务启用 SNMPv1、SNMPv2c 和 SNMPv3 协议。确保禁用较旧版本的 SNMP 协议，除非需要使用它们。

注 - SNMP 协议版本 3 引入了对基于用户的安全模型 (User-based Security Model, USM) 的支持。此功能使用实际用户帐户取代了传统的 SNMP 团体字符串，可以为用户帐户配置特定权限、验证、隐私协议和密码。默认情况下，IB 交换机不包含任何 USM 帐户。根据您自己的部署、管理和监视要求来配置 SNMPv3 USM 帐户。

---

1. **以 `ilom-admin` 身份登录到 IB 交换机。**

   请参见登录到 IB 交换机 [97]。

2. **确定每个 SNMP 协议的状态。**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = enabled
v2c = enabled
v3 = enabled
```

3. **如果需要，请禁用 SNMPv1 和 SNMPv2c。**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

▼ 配置 SNMP 团队字符串（IB 交换机）

此任务仅适用于启用并配置为使用 SNMP v1 或 SNMPv2c 的情况。

由于 SNMP 通常用于监视设备的运行状况，因此将设备使用的默认 SNMP 团体字符串替换为客户定义的值非常重要。

1. **以 `ilom-admin` 身份登录到 IB 交换机。**

   请参见登录到 IB 交换机 [97]。

2. **创建新 SNMP 团体字符串。**

在此示例中，替换命令行中的以下项：

- *string*－替换为客户定义的值，客户定义的值要符合美国国防部有关 SNMP 团体字符串组成部分的要求。
- *access*－根据这是只读还是读写访问字符串，替换为 `ro` 或 `rw`。

```
-> create /SP/services/snmp/communities/string permission=access
```

创建新团体字符串之后，必须删除默认团体字符串。

3. **删除默认 SNMP 团体字符串。**

```
-> delete /SP/services/snmp/communities/public
-> delete /SP/services/snmp/communities/private
```

4. **验证 SNMP 团体字符串。**

```
-> show /SP/services/snmp/communities
```

▼ 替换默认自签名证书（IB 交换机）

IB 交换机使用自签名证书来允许直接使用 HTTPS 协议。作为最佳做法，应将自签名证书替换为获准在您的环境中使用并由获得认可的证书颁发机构签名的证书。

IB 交换机支持通过各种方法访问 SSL/TLS 证书和私钥（包括 HTTPS、HTTP、SCP、FTP、TFTP），还支持直接将信息粘贴到 Web 浏览器界面中。有关更多信息，请参阅《*Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36*》文档。请参见“其他 IB 交换机资源” [105]。

1. **以 `ilom-admin` 身份登录到 IB 交换机。**
   请参见登录到 IB 交换机 [97]。

2. **确定 IB 交换机是否正在使用默认自签名证书。**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

3. **安装您组织的证书。**

```
-> load -source URI /SP/services/https/ssl/custom_cert
-> load -source URI /SP/services/https/ssl/custom_key
```

▼ 配置 CLI 管理会话超时（IB 交换机）

IB 交换机支持在 CLI 管理会话处于不活动状态超过预定义的分钟数后将其断开连接并注销。

默认情况下，CLI 在 15 分钟后超时。

1. **以 `ilom-admin` 身份登录到 IB 交换机。**
   请参见登录到 IB 交换机 [97]。

2. **检查与 CLI 关联的不活动超时参数。**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **设置不活动超时参数。**
   将 *n* 替换为以分钟为单位指定的值。

```
-> set /SP/cli timeout=n
```

其他 IB 交换机资源

有关 IB 交换机管理和安全过程的更多信息，请参阅 Sun Datacenter InfiniBand Switch 36 文档库，网址为 http://docs.oracle.com/cd/E36265_01。

▼ 更改以太网交换机密码

注 - 如果为 Oracle Engineered Systems Hardware Manager 管理的任何 SuperCluster 组件（如以太网交换机）更改了密码，您还必须在 Oracle Engineered Systems Hardware Manager 中更新密码。有关详细信息，请参阅《*Oracle SuperCluster M7* 系列管理指南》。

---

1. **用串行电缆将以太网交换机控制台连接到手提电脑或类似的设备。**
   默认串行端口速度为 9600 波特、8 位、无奇偶校验、1 个停止位并且无握手。

```
sscsw-adm0 con0 is now available
Press RETURN to get started.
```

2. **将交换机置于启用模式。**

```
sscsw-adm0> enable
```

3. **设置密码。**

```
sscsw-adm0# configure terminal
Enter configuration commands,one per line.End with CNTL/Z.
sscsw-adm0(config)# enable password *******
sscsw-adm0(config)# enable secret *******
sscsw-adm0(config)# end
sscsw-adm0# write memory
*Apr 24 14:25:05.893:%SYS-5-CONFIG_I:Configured from console by
console
Building configuration...
Compressed configuration from 2502 bytes to 1085 bytes [OK ]
```

4. **保存配置。**

```
sscsw-adm0# copy running-config startup-config
```

5. **退出会话。**

```
sscsw-adm0# exit
```

6. **断开手提电脑与以太网交换机的连接。**

符合性审计

使用 Oracle Solaris 符合性实用程序可以评估和报告系统是否符合某项已知基准。

Oracle Solaris `compliance` 命令可将基准的各项要求映射到代码、文件或命令输出，然后由后者验证是否符合特定要求。Oracle SuperCluster 当前支持两个安全符合性基准配置文件：

- **Recommended**－基于 Internet 安全中心基准的配置文件。
- **PCI-DSS**－验证支付卡行业数据安全标准 (Payment Card Industry Data Security Standard, PCI DSS) 符合性要求的配置文件。

这些分析工具可将安全控制映射到符合性要求，生成的符合性报告可减少大量的审计时间。此外，符合性功能还提供了指南，其中包含每项安全检查的基本原理以及未通过的检查的修复步骤。这些指南对培训会很有用，也可用作日后测试的准则。默认情况下，安装时会创建每个安全配置文件的指南。SuperCluster Solaris 管理员可添加或更改基准并创建新指南。

以下主题介绍了如何运行符合性报告并说明了 FIPS-140 符合性：

- 生成符合性评估 [107]
- （可选）使用 `cron` 作业运行符合性报告 [109]
- “FIPS-140-2 级别 1 符合性” [110]

▼ 生成符合性评估

要执行本任务，您必须分配有 "Software Installation"（软件安装）权限配置文件才能将软件包添加到系统。您必须分配有管理权限才能执行大多数 compliance 命令。

1. **安装 compliance 软件包。**

```
# pkg install compliance
```

以下消息指示软件包已安装：

```
No updates necessary for this image.
```

有关更多信息，请参阅 pkg(1) 手册页。

注 - 在计划运行符合性测试的每个区域中安装该软件包。

---

2. **列出可用的基准、配置文件和以前的任何评估。**

   在本示例中，有两个基准。

   - **pci-dss**－包括一个配置文件，称为 Solaris_PCI-DSS
   - **solaris**－包括两个配置文件，称为 Baseliine 和 Recommended

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
No assessments available
```

3. **生成符合性评估。**

   使用以下语法运行 compliance 命令：

compliance assess -b *benchmark* -p *profile*

-b	指定特定基准。如果未指定，则默认值为 solaris。
-p	指定配置文件。配置文件名称区分大小写。如果未指定，则默认值为第一个配置文件。

   示例：

   - 使用 Recommended 配置文件：

```
# compliance assess -b solaris -p Recommended
```

     该命令会在 /var/share/compliance/assessments 中创建一个目录，其中包含三个评估文件，分别是一个日志文件、一个 XML 文件和一个 HTML 文件。

   - 使用 PCI-DSS 配置文件：

```
# compliance assess -b pci-dss
```

注 - pci-dss 基准只有一个配置文件，所以无需在命令行上指定配置文件选项 (-p)。

---

4. **验证是否已创建符合性文件。**

```
# cd /var/share/compliance/assessments/filename_timestamp
# ls
recommended.html
recommended.txt
recommended.xml
```

注 - 如果再次运行同一 compliance 命令，将不会替换这些文件。必须先删除这些文件，然后才能重复使用评估目录。

5. **（可选）创建定制报告。**

   可以重复运行定制报告。但是，只能在原始目录中运行一次评估。

   在本示例中，-s 选项用于选择哪些结果类型应该显示在报告中。

   默认情况下，除了 notselected 或 notapplicable 之外，所有结果类型都将显示在报告中。结果类型指定为除了默认类型之外要显示的逗号分隔列表。可以通过在各个结果类型前加上 - 来隐藏相应的结果类型，而使列表以 = 开头则可以确切地指定应当包括哪些结果类型。结果类型有：pass、fixed、notchecked、notapplicable、notselected、informational、unknown、error 或 fail。

   ```
   # compliance report -s -pass,fail,notselected
   /var/share/compliance/assessments/filename_timestamp/report_A.html
   ```

   此命令会以 HTML 格式创建包含未通过项和未选定项的报告。该报告针对最近的评估运行。

6. **查看完整报告。**

   可以在文本编辑器中查看日志文件，在浏览器中查看 HTML 文件，或者在 XML 查看器中查看 XML 文件。例如，要查看先前步骤所生成的定制 HTML 报告，请键入以下浏览器条目：

   file:///var/share/compliance/assessments/*filename_timestamp***/report_A.html**

7. **修复安全策略要求必须通过的未通过项。**

   如果修复步骤包括重新引导系统，请先重新引导系统，然后再次运行评估。

8. **重复评估，直到没有未通过项为止。**

▼ （可选）使用 cron 作业运行符合性报告

- **以超级用户身份，使用 crontab -e 命令将适当的条目添加到 crontab 文件中。**

  以下列表提供了 crontab 条目的示例：

  - 在凌晨 2:30 运行每日符合性评估

    ```
    30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
    ```

  - 在星期日凌晨 1:15 运行每周符合性评估

    ```
    15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
    ```

  - 在每月第一天凌晨 4:00 运行每月评估

```
0 4 1 * * /usr/bin/compliance assess -b pci-dss
```

- 在每月第一个星期一凌晨 3:45 运行评估

```
45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
```

FIPS-140-2 级别 1 符合性

在 SuperCluster 上托管的加密应用程序依赖于 Oracle Solaris 的加密框架功能，该功能已针对 FIPS 140-2 级别 1 符合性进行了验证。Oracle Solaris 加密框架是 Oracle Solaris 的中央加密存储库，它提供了两个 FIPS 140 验证的模块，它们支持用户空间和内核级进程。这些库模块为应用程序提供加密、解密、散列、签名生成和验证、证书生成和验证以及消息验证功能。调用这些模块的用户级应用程序在 FIPS 140 模式下运行。

除 Oracle Solaris 加密框架之外，与 Oracle Solaris 捆绑在一起的 OpenSSL 对象模块也针对 FIPS 140-2 级别 1 符合性进行了验证，该模块支持基于安全 Shell 和 TLS 协议对应用程序进行加密。云服务提供商可选择在符合 FIPS 140 的模式下启用租户主机。在符合 FIPS 140 的模式下运行时，Oracle Solaris 和 OpenSSL（FIPS 140-2 提供者）会强制使用 FIPS 140 验证的加密算法。

另请参见（如果需要）启用以符合 FIPS-140 的模式运行 (Oracle ILOM) [36]。

下表列出了 FIPS 认可的且 Oracle Solaris 在 SuperCluster M7 上支持的算法。

密钥或 CSP	证书编号	
	v1.0	v1.1
对称密钥		
AES：ECB、CBC、CFB-128、CCM、GMAC、GCM 和 CTR 模式，针对 128、192 和 256 位密钥大小	#2311	#2574
AES：XTS 模式，针对 256 和 512 位密钥大小	#2311	#2574
TripleDES：CBC 和 ECB 模式，针对密钥选项 1	#1458	#1560
非对称密钥		
RSA PKCS#1.5 签名生成/验证：1024 和 2048 位（SHA-1、SHA-256、SHA-384 和 SHA-512）	#1194	#1321
ECDSA 签名生成/验证：P-192、-224、-256、-384 和 -521；K-163、-233、-283、-409 和 -571；B-163、-233、-283、-409 和 -571	#376	#446
安全散列标准 (Secure Hashing Standard, SHS)		
SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512	#1425	#1596
（加密）散列消息验证		
HMAC SHA-1、HMAC SHA-224、HMAC SHA-256、HMAC SHA-384 和 HMAC SHA-512	#1425	#1596
随机数生成器		
swrand FIPS 186-2 随机数生成器	#1154	#1222

密钥或 CSP	证书编号	
n2rng FIPS 186-2 随机数生成器	#1152	#1226

Oracle Solaris 提供了两个针对 FIPS 140-2 级别 1 进行了验证的加密算法提供者。

- Oracle Solaris 的加密框架功能是 Oracle Solaris 系统上的中央加密存储库，它提供了两个 FIPS 140 模块。用户级模块为在用户空间中运行的应用程序提供加密，内核模块为内核级进程提供加密。这些库模块为应用程序提供加密、解密、散列、签名生成和验证、证书生成和验证以及消息验证功能。调用这些模块的用户级应用程序在 FIPS 140 模式下运行，例如 `passwd` 命令和 IKEv2。内核级使用者（例如 Kerberos 和 IPsec）使用专有 API 调用内核加密框架。
- OpenSSL 对象模块为 SSH 和 Web 应用程序提供加密。OpenSSL 是安全套接字层 (Secure Sockets Layer, SSL) 和传输层安全 (Transport Layer Security, TLS) 协议的开源工具包，提供加密库。在 Oracle Solaris 中，SSH 和 Apache Web 服务器是 OpenSSL FIPS 140 模块的使用者。Oracle Solaris 11.2 随附 OpenSSL 的 FIPS 140 版本，该版本可供所有使用者使用，但是 Oracle Solaris 11.1 随附的版本只能由 Solaris SSH 使用。因为 FIPS 140-2 提供者模块占用大量 CPU，所以默认情况下不启用它们。作为管理员，您负责在 FIPS 140 模式下启用提供者并配置使用者。

有关在 Oracle Solaris 上启用 FIPS-140 提供者的更多信息，请参阅 "Securing the Oracle Solaris 11 Operating System"（确保 Oracle Solaris 11 操作系统安全）标题下名为《*Using a FIPS 140 Enabled System in Oracle Solaris 11.2*》（《在 Oracle Solaris 11.2 中使用支持 FIPS 140 的系统》）的文档，网址为：`http://docs.oracle.com/cd/E36784_01`。

确保 SuperCluster M7 系列系统安全

以下主题介绍了您可用来在系统的整个生命周期内维护安全性的 SuperCluster M7 系列功能：

管理 SuperCluster 安全性

SuperCluster M7 利用多种产品的安全管理功能，包括 Oracle ILOM、Oracle Enterprise Manager Ops Center、Oracle Enterprise Manager 和 Oracle Identity Management Suite。下面几部分进行了详细介绍：

Oracle ILOM 安全管理

Oracle ILOM 是嵌入许多 SuperCluster M7 组件的服务处理器。使用 Oracle ILOM 可以执行以下带外管理活动：

- 提供安全的访问以对 SuperCluster 组件执行安全的快速远程管理。访问包括受 SSL 保护的基于 Web 的访问、使用安全 Shell 的命令行访问以及 IPMI v2.0 和 SNMPv3 协议。

- 使用 RBAC 模型分离职责要求。为各个用户分配特定角色，以限制他们可执行的功能。
- 提供有关所有登录和配置更改事项的审计记录。每个审计日志条目都会列出执行操作的用户和时间戳。借助此功能，您可以检测未经授权的活动或更改，并确定执行这些操作的特定用户。

有关更多信息，请参阅 Oracle Integrated Lights Out Manager 文档，网址为：`http://docs.oracle.com/en/hardware/?tab=4`

Oracle Identity Management Suite

Oracle Identity Management Suite 管理一个组织内用户身份和帐户的端到端生命周期。该套件支持单点登录、基于 Web 的访问控制、Web 服务安全性、身份管理、强验证以及身份和访问管控。

Oracle Identity Management 可以提供一个管理身份的平台，不仅能够访问在 Oracle SuperCluster 上运行的应用程序和服务，而且还能访问管理 Oracle SuperCluster 的底层基础结构和服务。

有关更多信息，请参阅 Oracle Identity Management 文档，网址为：

`http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html`

Oracle Key Manager

Oracle Key Manager 是一个全面的密钥管理系统 (key management system, KMS)，可以简化用来保护静态信息的加密密钥的管理和监视。

Oracle Key Manager 凭借高度可扩展且高度可用的体系结构支持企业级环境，可以管理数千台设备和数百万个密钥。此功能在强化的操作环境中运行，对密钥管理和监视操作强制实施强访问控制和角色分离，并选择性地支持 Oracle 的 Sun Crypto Accelerator 6000 PCIe 卡（一个 FIPS 140-2 额定硬件安全模块）中密钥的安全存储。

在 SuperCluster 的环境中，Oracle Key Manager 可以授权、保护和管理对 Oracle StorageTek 加密磁带机、使用透明数据加密功能加密的 Oracle Database 以及 Oracle Solaris 11 OS 上加密的 ZFS 文件系统使用的加密密钥的访问。

有关更多信息，请参阅 Oracle Key Manager 文档，网址为：

`http://docs.oracle.com/cd/E26076_02`

Oracle Engineered Systems Hardware Manager

Oracle Engineered Systems Hardware Manager 是基于 BUI 的机架级别的硬件管理工具，供 Oracle 服务人员使用。有关详细信息，请参阅《*Oracle SuperCluster M7 Series Owner's Guide: Administration*》。

Oracle Engineered Systems Hardware Manager 包括两组验证信息：

- **SuperCluster M7 组件密码**

  Oracle Engineered Systems Hardware Manager 可以安全地存储所有 SuperCluster M7 硬件的所有出厂帐户的密码。软件使用这些密码来管理 SuperCluster M7 组件。

  当任何密码发生更改时，您必须使用新密码更新 Oracle Engineered Systems Hardware Manager 应用程序。
- **本地验证**

  Oracle Engineered Systems Hardware Manager 具有两个本地用户帐户。一个帐户由客户用来针对他们的环境定制 Oracle Engineered Systems Hardware Manager 并管理服务帐户。另一个帐户由 Oracle 服务人员用来配置、支持和维修 SuperCluster M7 硬件。

Oracle Engineered Systems Hardware Manager 提供以下本地管理资源。

- **密码策略**－能够根据您的企业政策配置应用程序密码，从而确保密码符合您的企业标准。

  注 - 有关密码策略设置，请咨询您的企业安全官。

- **证书**－Oracle Engineered Systems Hardware Manager 使用证书保护计算服务器与 Oracle Engineered Systems Hardware Manager 服务器和 BUI 之间的通信。这些证书在安装期间自动创建，对于每个 SuperCluster 实例是唯一的。但是，它们可以替换为客户提供的证书和密钥。
- **端口**－如果 Oracle Engineered Systems Hardware Manager 使用的网络端口与您的企业政策冲突，可以对其进行配置。使用的是端口 8001 到 8004（包含 8001 和 8004）。

有关配置说明，请参阅《*Oracle SuperCluster M7 Series Owner's Guide: Administration*》。

Oracle Enterprise Manager

Oracle Enterprise Manager 套件是一个全面的集成式云管理解决方案，着重于应用程序、中间件、数据库以及物理和虚拟基础结构的生命周期管理（使用 Oracle Enterprise Manager Ops Center）。Oracle Enterprise Manager 提供以下管理技术：

- 支持应用程序、中间件和数据库的详细监视、事件通知、修补、变更管理、持续配置、符合性管理和报告。
- 使您可以集中维护安全性配置设置以及数据库组的访问控制和审计策略。对这些功能的访问可以限于授权人员，从而确保管理访问支持对职责分离、最小特权和应负责任的符合性要求。
- 支持使用各种方法进行强验证、细粒度访问控制和全面的审计，从而确保能以安全的方式完成 SuperCluster 环境的管理。

有关更多信息，请参阅 Oracle Enterprise Manager 文档，网址为：http://www.oracle.com/technetwork/oem/grid-control/documentation/oem-091904.html

Oracle Enterprise Manager Ops Center（可选）

Oracle Enterprise Manager Ops Center 是一项可选的技术，可用于管理 Oracle SuperCluster 的一些安全性方面。

作为 Oracle Enterprise Manager 套件的一部分，Oracle Enterprise Manager Ops Center 是一个聚合硬件管理解决方案，为服务器、OS、固件、虚拟机、区域、存储和网络结构提供了一个管理界面。

您可以使用 Oracle Enterprise Manager Ops Center 分配对物理和虚拟系统集合的管理访问权限、监视管理员活动、检测故障以及配置和管理警报。Oracle Enterprise Manager Ops Center 支持多种报告，使您可以对照已知的配置基准、修补程序级别和安全漏洞比较系统。

有关更多信息，请参阅 Oracle Enterprise Manager Ops Center 文档，网址为：http://docs.oracle.com/cd/E27363_01/index.htm

---

注 - 对于以前的 Oracle Enterprise Manager Ops Center 版本，Ops Center 软件从 SuperCluster 系统上安装和运行。从 Oracle Enterprise Manager Ops Center 12c Release 2 (12.2.0.0.0) 发行版开始，Ops Center 软件必须在 SuperCluster 系统以外的系统上安装和运行。

监视安全性

无论是对于符合性报告还是事件响应来说，监视和审计都是至关重要的功能，您必须使用这些功能来增进对 IT 环境的认识。监视和审计的应用程度通常基于环境的风险或危急性质。

SuperCluster M7 系列系统在服务器、网络、数据库和存储层提供了全面的监视和审计功能，从而确保可以获得信息来满足审计和符合性要求。

下面几部分介绍了工作负荷和数据库的监视和审计：

工作负荷监视

Oracle Solaris OS 具有一个全面的审计工具，它可以监视管理操作、命令行调用甚至个别的内核级系统调用。该工具高度可配置，可提供全局、每区域甚至每用户审计策略。

将系统配置为使用 Oracle Solaris Zones 时，每个区域的审计记录可存储在全局区域中，以防止对其进行篡改。

Oracle Solaris 审计提供了使用系统日志 (`syslog`) 工具将审计记录发送至远程收集点的功能。许多商业入侵检测和预防服务可以使用 Oracle Solaris 审计记录作为附加输入进行分析和报告。

Oracle VM Server for SPARC 利用本机 Oracle Solaris 审计工具来记录与虚拟化事件和域管理关联的操作和事件。

有关更多信息，请参阅 Oracle Solaris 安全准则中的“监视和维护 Oracle Solaris 安全性”部分，网址为：

`http://docs.oracle.com/cd/E26502_01`

数据库活动监视和审计

借助 Oracle Database 对细粒度审计的支持，您可以建立策略来选择性地确定是在何时生成的审计记录。此功能可帮助您把精力集中在其他数据库活动上，并减少通常与审计活动关联的开销。

Oracle Audit Vault and Database Firewall 可以集中管理数据库审计设置，并自动将审计数据整合到安全系统信息库中。该软件包括内置报告功能来监视大量的活动，包括特权用户活动和数据库结构的更改。Oracle Audit Vault and Database Firewall 生成的报告列明了各种应用程序和管理数据库活动，并提供了详细信息来支持操作的责任追查。

利用 Oracle Audit Vault and Database Firewall，可以对可能表明未经授权的访问尝试或滥用系统特权的活动进行主动检测和警报。这些警报可以同时包括系统和用户定义的事件和条件，例如创建特权用户帐户或修改包含敏感信息的表。

Oracle Audit Vault and Database Firewall Remote Monitor 可以提供实时数据库安全性监视。此功能查询数据库连接来检测恶意通信流量，例如应用程序绕过、未经授权的活动、SQL 注入及其他威胁。此软件使用基于准确 SQL 语法的方法，可帮助您快速识别可疑的数据库活动。

有关更多信息，请参阅 Oracle Audit Vault and Database Firewall 文档，网址为：http://docs.oracle.com/cd/E37100_01/index.htm

网络监视

根据安全准则对网络进行配置后，需要定期进行检查和维护。

请遵循以下准则以确保对系统的本地和远程访问的安全性：

- 查看日志以发现可能的事件，并根据您组织的安全策略将其归档。
- 对客户机访问网络执行定期检查，以确保主机和 Oracle ILOM 设置保持不变。

有关更多信息，请参阅 Oracle Solaris OS 的安全指南：

- Oracle Solaris 11 OS－http://www.oracle.com/goto/Solaris11/docs
- Oracle Solaris 10 OS－http://www.oracle.com/goto/Solaris10/docs

软件和固件更新

SuperCluster M7 系列系统的更新在 QFSDP 中提供。安装 QFSDP 会同时更新所有组件。此做法可确保所有组件继续在 Oracle 已一起充分测试的软件版本组合上运行。

请从 My Oracle Support 获取最新的 QFSDP，网址为：http://support.oracle.com

有关受支持的软件和固件的详细信息，请参阅《*Oracle SuperCluster M7* 系列产品说明》。MOS 简讯 1605591.1 介绍了如何获取此产品说明。

注 - 只能按照 Oracle 支持人员的建议，孤立地升级、更新或修补单个组件进行反应性维护。

索引

S

T

W

X

Y

Z