

Oracle MiniCluster S7-2 安全指南

ORACLE®

文件号码 E78268-02
2016 年 10 月

文件号码 E78268-02

版权所有 © 2016, Oracle 和/或其附属公司。保留所有权利。

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

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

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

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

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

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

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

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

文档可访问性

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

获得 Oracle 支持

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

目录

使用本文档	7
产品文档库	7
反馈	7
了解安全原则	9
最少必需的安全任务	9
核心安全原则	10
安全的虚拟机	11
访问控制	12
数据保护	12
审计与遵从性	13
了解安全配置	15
内置的安全配置文件	15
▼ 验证 VM 安全配置文件 (CLI)	15
保护数据	19
采用 ZFS 数据集加密的数据保护	19
▼ 查看 ZFS 数据集加密密钥 (BUI)	19
安全 Shell 服务	20
▼ 更改 SSH 密钥 (BUI)	20
使用 IPsec 实现安全通信	22
▼ 配置 IPsec 和 IKE	22
控制访问	25
▼ 更改默认的 Oracle ILOM root 密码	25
▼ 配置 EEPROM 密码	26
用户置备	27
MCMU 用户审批流程	27
基于角色的访问控制	28

用户帐户	29
用户验证和密码策略	30
▼ 验证 Oracle Solaris 用户角色	30
VM 的安全删除	30
▼ 验证基于主机的防火墙规则	31
▼ 检验经验证的引导环境	32
▼ 限制对共享存储的访问	33
审计与遵从性报告	35
▼ 验证审计策略	35
▼ 查看审计日志	36
▼ 生成审计报告	37
▼ (如果需要) 启用以符合 FIPS-140 的模式运行 (Oracle ILOM)	39
FIPS-140-2 级别 1 遵从性	40
访问安全遵从性	43
安全遵从性基准测试	43
▼ 计划安全遵从性基准测试 (BUI)	43
▼ 查看基准测试报告 (BUI)	45
了解 SPARC S7-2 服务器安全控制	49
了解硬件安全	49
限制人员接近	49
序列号	50
硬盘驱动器	50
限制对 OpenBoot 的访问	50
▼ 进入 OpenBoot 提示符	51
▼ 检查失败的登录	51
▼ 提供通电横幅	51
索引	53

使用本文档

- 概述—提供了有关为 Oracle MiniCluster S7-2 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

可从以下网址获得有关该产品及相关产品的文档和资源：<http://www.oracle.com/goto/miniccluster-s7-2/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 MiniCluster S7-2 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：

- [“最少必需的安全任务” \[9\]](#)
- [“核心安全原则” \[10\]](#)
- [“安全的虚拟机” \[11\]](#)
- [“访问控制” \[12\]](#)
- [“数据保护” \[12\]](#)
- [“审计与遵从性” \[13\]](#)

最少必需的安全任务

作为一个工程系统，MiniCluster 在出厂时就默认配置为一个高度安全的系统，提供了以下安全功能：

- 为所有虚拟机 (virtual machine, VM) 预配置了完全自动化的安全控制。
- 默认情况下启用了加密，可以确保静态数据和传输中数据的安全。
- VM 自动配置了强化且最小化的 OS，该 OS 具有基于主机的防火墙。
- 访问控制要求使用基于角色且具有最小特权的访问权限。
- 所有 VM 都使用加密的 ZFS 存储。
- 提供了一个集中式密钥管理工具，它使用 PKCS#11 并且支持 FIPS。
- 系统中包括了采用集中式审计日志的全面审计策略。
- 系统和所有 VM 都配置有 PCI-DSS、CIS 等同或 DISA-STIG 安全配置文件。注意—后面的配置文件当前处于审核阶段。请仅在非生产环境中将 DISA-STIG 配置文件用于试验用途。
- 提供了易于查看的遵从性显示板，该显示板支持易于运行的遵从性基准。

安装 MiniCluster 后，安全管理员必须立即执行两个任务：

- 更改 Oracle ILOM root 密码。请参见[更改默认的 Oracle ILOM root 密码 \[25\]](#)

除此之外，请查看本指南中的安全信息来了解并验证 MiniCluster 安全功能。

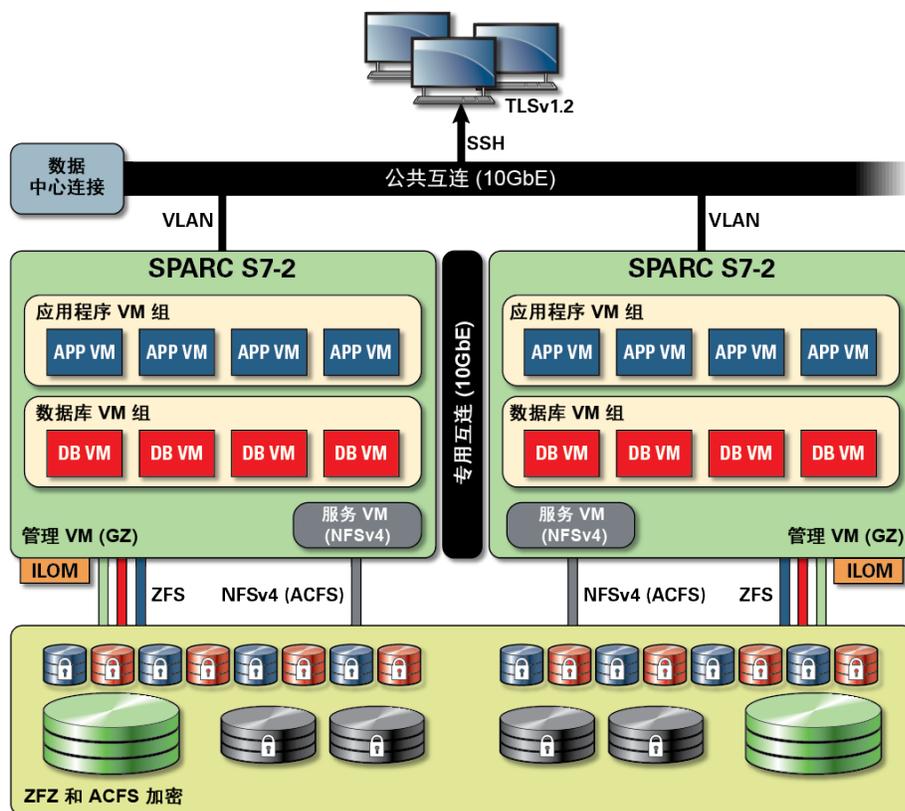
核心安全原则

MiniCluster 是一个安全的云基础结构平台，用于整合应用程序和数据库，并且非常适合用于提供专用的基于计算基础结构即服务 (infrastructure as a service, IaaS) 的云服务。作为一个多用途工程系统而构建，它组合利用了 Oracle SPARC S7 处理器的计算能力、SPARC Solaris 的高效虚拟化功能，以及集成了专用存储的 Oracle 数据库的优化数据库性能。此外，还采用了一个 10 GbE 网络，以允许客户机访问在 MiniCluster 上运行的服务。最后，另一个 10 GbE 网络提供了通道，SPARC S7 服务器上的虚拟机环境与托管的应用程序之间的所有交互通信均通过此通道。

SPARC S7 处理器具有始终生效的硬件辅助加密功能，可以帮助 MiniCluster 托管的实体使用高性能数据保护来保护其所有信息—包括静态的、使用中的和传输中的信息。该处理器还具有“芯片保护内存”功能，该功能可以检测并阻止与内存数据损坏和内存擦除相关的攻击，因此可以确保应用程序数据的完整性。

默认情况下，MiniCluster 预先配置有 250 个现成可用的安全控制，它们禁用了非绝对必要的服务、端口和协议并将公开的服务配置为仅接受可信连接，从而减少了系统的受攻击面。

该系统支持各种配置和部署选项。下图显示了一个整合了 Oracle 数据库和应用程序工作负荷的典型部署。



安全的虚拟机

MiniCluster 计算节点中的安全性是在多个层次中提供的。它从计算节点的安全验证引导开始，该引导采用强化且最小化的 OS，它作为隔离的虚拟机运行，以防止工作负荷和数据被未经授权的用户和系统访问。MiniCluster 使用 Oracle Solaris Zones 技术作为虚拟机来托管隔离的计算环境并高效地将同一操作系统上运行的各种应用程序置于沙盒中，从而使其免遭其他虚拟机中会发生的无意或恶意活动的危害。虽然在同一内核中运行，但是每个 Solaris 区域都有其自己的标识、资源、名称空间和进程隔离。实际上，Solaris 区域通过强大的隔离和灵活的资源控制提供了内置的虚拟化，但是 CPU 和内存占用要比在 1 型虚拟机管理程序上运行的传统虚拟机更少。每个虚拟机都配置有一个安全配置文件，该配置文件定义了在安装过程中自动应用的一组全面的安全控制和策略。使用 ZFS 池和数据集可以为虚拟机进一步将存储分隔并隔离为更细粒度的单元，并且可以具有其自己的安全策略。

访问控制

为保护应用程序数据、工作负荷以及这一切在其上运行的基础结构，MiniCluster 针对用户和管理员都提供了全面但仍然灵活的访问控制功能。MiniCluster 在针对访问系统服务的用户和应用程序实施的各种访问控制方法中都利用了 Oracle Solaris。虽然传统的用户名和密码对仍然被广泛使用，但是可以使用 Oracle Solaris 可插拔验证模块 (pluggable authentication module, PAM) 体系结构来轻松集成更强的验证方法，从而允许使用 LDAP、Kerberos 和公钥验证。MiniCluster 计算环境基于全面的基于角色的访问控制 (role-based access control, RBAC) 工具构建，允许组织根据需要灵活地委派用户和管理访问权限。抛弃了全能超级用户的概念，Oracle Solaris 中的 RBAC 功能实现了职责分离并且支持以下概念：管理角色、授权、细粒度特权和权限配置文件，所有这些元素集体用来为用户和管理员分配权限。RBAC 与其他核心 Oracle Solaris 服务（包括 Oracle Solaris 服务管理工具 (Service Management Facility, SMF) 和虚拟机）相集成，提供一致的体系结构来支持所有操作系统级访问控制需求。MiniCluster 利用 Oracle Solaris 的 RBAC 功能作为其访问控制体系结构的基础，允许组织从一个集中式机构来管理、控制和审计操作系统和虚拟化管理访问。所有重要操作都使用由多人授权工作流支持的职责分离原则来执行。对于每个安全敏感型操作，系统都要求由两个或更多人进行审批。这些功能可以共同用来针对用户身份和他们对重要业务操作的处理提供高度保证。

MiniCluster 系统中的所有设备都具有使用下述方法限制对服务进行网络访问的能力：使用体系结构方法（例如网络隔离）；或者使用数据包过滤和/或访问控制列表方法，以限制发往物理和虚拟设备、来自物理和虚拟设备和物理和虚拟设备之间的通信以及发往系统公开的服务的通信。MiniCluster 采用默认安全的模式，在此模式下，除了安全 (Secure Shell, SSH) 之外，不允许任何网络服务接受入站网络通信。其他已启用的网络服务在内部侦听 Oracle Solaris 操作系统（虚拟机或区域）内的请求。这可以确保所有网络服务默认情况下被禁用或者设置为仅侦听本地系统通信。组织可以根据其需求自由定制此配置。MiniCluster 预先配置有一个使用 Oracle Solaris IP 过滤器功能的网络和传输层（有状态）数据包过滤功能。IP 过滤器提供了广泛的基于主机的网络功能，包括有状态数据包过滤、网络地址转换和端口地址转换。

数据保护

MiniCluster 中的 SPARC S7 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。

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，在操作系统级别，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 MiniCluster 使用的 Oracle Solaris 操作系统和 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。MiniCluster 支持使用 IPSec (IP Security, IP 安全)，建议使用 IKE (Internet Key Exchange, Internet 密钥交换) 来保护通过公共和专用网络传输的 VM 特定和 VM 间通信的保密性和完整性。

在 MiniCluster 上，ZFS 数据集加密利用一个集中式 Oracle Solaris PKCS#11 密钥库来安全地保护包装密钥。使用 Oracle Solaris PKCS#11 密钥库将自动对所有加密操作应用 SPARC 硬件协助式加密加速。这使得 Oracle 可以极大地提高与 ZFS 数据集、Oracle Database 透明数据加密 (Transparent Data Encryption, TDE)、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。数据库虚拟机可以通过利用 Oracle Solaris PKCS#11 密钥库或者通过在 ACFs 共享存储上创建一个目录来使用共享钱包方式，以便可以在虚拟机上的数据库之间共享该钱包。在每个计算节点上使用共享的集中式密钥库可以使系统能够更好地在基于 Oracle 网络基础结构的群集数据库体系结构中管理、维护和轮转 Oracle TDE 的密钥，因为密钥将在群集中的每个节点之间同步。通过在 ZFS 数据集 (文件系统/ZVOL) 级别实施加密策略和密钥管理来通过密钥销毁提供有保证的删除，MiniCluster 还能够实现对虚拟机和关联 ZFS 数据集的安全删除。

审计与遵从性

MiniCluster 使用 Oracle Solaris 审计子系统来收集、存储和处理审计事件信息。每个虚拟机 (非全局区域) 都会生成审计记录，这些审计记录会被本地存储到每个 MiniCluster (全局区域) 审计存储中。此方法可确保各个虚拟机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，甚至虚拟机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。当配置为使用虚拟机时，可以将每个虚拟机的审计记录存储到全局区域中以防止它们被篡改。全局区域还利用本机 Oracle Solaris 审计工具来记录与虚拟化事件和 MiniCluster 管理关联的操作和事件。

MiniCluster 提供了相应的工具来评估和报告虚拟机上的 Oracle Solaris 运行时环境的遵从性。遵从性实用程序基于安全内容自动化协议 (Security Content Automation Protocol, SCAP) 实现。MiniCluster 支持两个安全遵从性基准测试配置文件：

- **默认安全配置文件**—一个 CIS 等同配置文件 (基于 Internet 安全中心基准)，更符合由规章规定的安全遵从性要求 (例如 HIPAA、FISMA、SOX，等等)。
- **PCI-DSS 配置文件**—支付卡行业数据安全标准
- **DISA STIG 配置文件**—国防信息系统局的安全技术实施指南标准。此配置文件以默认安全配置文件为基础，引入了额外的 75 项安全控制、FIPS-140-2 加密技术，并且

支持设置 S 密码。注意—此配置文件当前处于审核阶段。请仅在非生产环境中将此配置文件用于试验用途。

MiniCluster 管理员可以按需运行遵从性基准测试并验证环境的遵从性和异常。这些分析工具可以将安全控制映射到行业标准规定的遵从性要求。关联的遵从性报告可以显著降低审计时间和成本。

从 MiniCluster v.1.1.18 开始，系统包括以下审计功能：

- **审计员角色**—为 MCMU 用户指定了此角色时，该用户可以在 MCMU BUI 中访问审计员的审核页面。该用户不能查看或执行任何其他 MiniCluster 管理任务。
- **审计员审核页面**—这是一个特殊的 MCMU BUI 页面，只有具有审计员角色的用户才能查看。通过此页面，可以访问审计池状态，并且能够基于每个区域生成所有用户活动的审计记录。请参见[生成审计报告 \[37\]](#)。

了解安全配置

以下主题介绍了 MiniCluster 安全控制：

- [“内置的安全配置文件” \[15\]](#)
- [验证 VM 安全配置文件 \(CLI\) \[15\]](#)

内置的安全配置文件

MiniCluster 初始化是使用 MCMU BUI 或 CLI 执行的。在初始化期间，MCMU 会要求安装者选择下列安全配置文件之一：

- **默认安全配置文件**—满足与 Internet 安全中心 (Center for Internet Security, CIS) 和安全性技术实施准则 (Security Technical Implementation Guidelines, STIG) 评估规定的基准相当或等同的要求。
- **PCI-DSS 配置文件**—符合由支付卡行业安全标准委员会定义的支付卡行业数据安全标准 (Payment Card Industry Data Security Standard, PCI DSS)。
- **DISA STIG 配置文件**—国防信息系统局的安全技术实施指南标准。此配置文件以默认安全配置文件为基础，引入了额外的 75 项安全控制、FIPS-140-2 加密技术，并且支持设置 eeprom 密码。注意—此配置文件当前处于审核阶段。请仅在非生产环境中将此配置文件用于试验用途。

MCMU 根据所选的策略为全局区域和非全局区域配置超过 250 项安全控制。

初始化后，在创建虚拟机时，MCMU 会要求为每个虚拟机选择一个安全配置文件。您可以根据安全要求在虚拟机上混合使用多个安全配置文件。

▼ 验证 VM 安全配置文件 (CLI)

使用此过程验证或识别为区域和虚拟机配置的安全配置文件。

注 - 您必须使用具有 root 角色的用户帐户来访问系统以执行此过程。

注 - 要识别分配给全局区域的安全配置文件，请在 MCMU BUI 中查看 "System Setting" (系统设置) -> "User Input Summary" (用户输入摘要)。安全配置文件将显示在页面底部。

1. 以 `mcinstall` 身份登录到全局区域。

有关如何访问系统的说明，请参阅《Oracle MiniCluster S7-2 管理指南》。

2. 承担 `root` 角色。

示例：

```
# su root
```

3. 确定相关 VM 的日志文件名称。

在此示例中，每个 VM 有一个日志文件：

```
# cd /var/opt/oracle.minicluster/mcmubui/MCMU/verification_logs
# ls
verify_appvmg1-zone-1-mc4-n1.log  verify_dbvmg1-zone-3-mc4-n1.log
verify_appvmg1-zone-1-mc4-n2.log  verify_dbvmg1-zone-3-mc4-n2.log
verify_dbvmg1-zone-1-mc4-n2.log  verify_dbvmg1-zone-4-mc4-n1.log
verify_dbvmg1-zone-2-mc4-n1.log  verify_dbvmg1-zone-4-mc4-n2.log
verify_dbvmg1-zone-2-mc4-n2.log
#
```

4. 查看验证日志文件。

查看日志文件的最后几行。如果显示了 (PCI-DSS)，则 VM 的安全配置文件是 PCI-DSS。如果未列出任何配置文件，则 VM 的安全配置文件是 CIS 等同。

- 以下示例显示了具有 PCI-DSS 配置文件的 VM 的最后 22 行：

```
# tail -22 verify_dbvmg1-zone-1-mc4-n2.log
```

```
(PCI-DSS) Checking /etc/cron.d/at.allow:
Passed/Configured
```

```
(PCI-DSS) Checking audit configuration (user audit flags):
Passed/Configured
```

```
(PCI-DSS) Checking audit configuration (non-attributable audit flags):
Passed/Configured
```

```
(PCI-DSS) Checking audit configuration (audit_binfile plugin):
Passed/Configured
```

```
(PCI-DSS) Checking audit flags on root and tadmin roles:
Passed/Configured
```

```
Check if tenant-key exists in keystore:  
Passed/Configured
```

```
Check if immutability is enabled:  
Failed/Not Configured
```

- 以下示例显示了具有 CIS 等同配置文件的 VM 的最后 22 行:

```
# tail -22 verify_dbvmg1-zone-1-mc4-n2.log
```

```
Checking if NDP routing daemon is disabled:  
Passed/Configured
```

```
Checking if r-protocol services are disabled:  
Passed/Configured
```

```
Checking if rpc/bind is enabled and configured correctly:  
Passed/Configured
```

```
Checking if NFS v2/v3 is disabled:  
Passed/Configured
```

```
Checking if GDM is enabled:  
Failed/Not Configured
```

```
Check if tenant-key exists in keystore:  
Passed/Configured
```

```
Check if immutability is enabled:  
Failed/Not Configured
```


保护数据

以下主题介绍了 MiniCluster 数据保护技术：

- [“采用 ZFS 数据集加密的数据保护” \[19\]](#)
- [查看 ZFS 数据集加密密钥 \(BUI\) \[19\]](#)
- [“安全 Shell 服务” \[20\]](#)
- [更改 SSH 密钥 \(BUI\) \[20\]](#)
- [“使用 IPsec 实现安全通信” \[22\]](#)
- [配置 IPsec 和 IKE \[22\]](#)

采用 ZFS 数据集加密的数据保护

在 MiniCluster 中，静态数据保护是使用 ZFS 数据集加密自动配置的。加密配置如下：

- 所有 ZFS 数据集都在虚拟机中进行加密，包括根文件系统和交换文件系统。
- 所有 ZFS 数据集都在全局区域中进行加密，但根文件系统和交换文件系统除外。

您可以通过查看加密密钥来验证加密配置。请参见[查看 ZFS 数据集加密密钥 \(BUI\) \[19\]](#)。

▼ 查看 ZFS 数据集加密密钥 (BUI)

可以使用此过程查看加密密钥详细信息。

1. 访问 **MCMU BUI**。
有关如何访问 MCMU BUI 的详细信息，请参阅《*Oracle MiniCluster S7-2 管理指南*》。
2. 在导航面板中，选择 **"System Settings"**（系统设置）-> **"Security"**（安全性）。

单击某个节点以显示详细信息。

Encryption Key Information
Encryption keys for all virtual machines and attached volumes

Node	VM Name	ZFS Pool	Key Label
Node 1			
	mc12-n1	rpool/common	gz_mc12-n1_zw.pinfile
	mc12-n1	rpool/audit_pool	gz_mc12-n1_zw.pinfile
	mc12ss01	rpool/common	kz_mc12ss01_zw.pinfile
	mc12ss01	rpool/audit_pool	kz_mc12ss01_zw.pinfile
	mc12ss01	rpool/u01	kz_mc12ss01_zw.pinfile
	mc12-n1	mcpool	mcpool-id-key
	mc12-n1	mcpool/dbzonetemplate	dbzonetemplate-id-key
	mc12-n1	mcpool/appzonetemplate	appzonetemplate-id-key
	mc12-n1	rpool/repo	repo-id-key
	mc12-n1	mcpool/mc12dbzg1-zone-1-mc12-n1u01	mc12dbzg1-zone-1-mc12-n1-id-key

安全 Shell 服务

MiniCluster 要求使用 SSH 网络协议以确保您安全登录到 MiniCluster 计算节点（全局区域）和虚拟机实例（非全局区域）。

当用户首次使用 SSH 登录时，系统会自动为用户生成一个新的 SSH 密钥对。

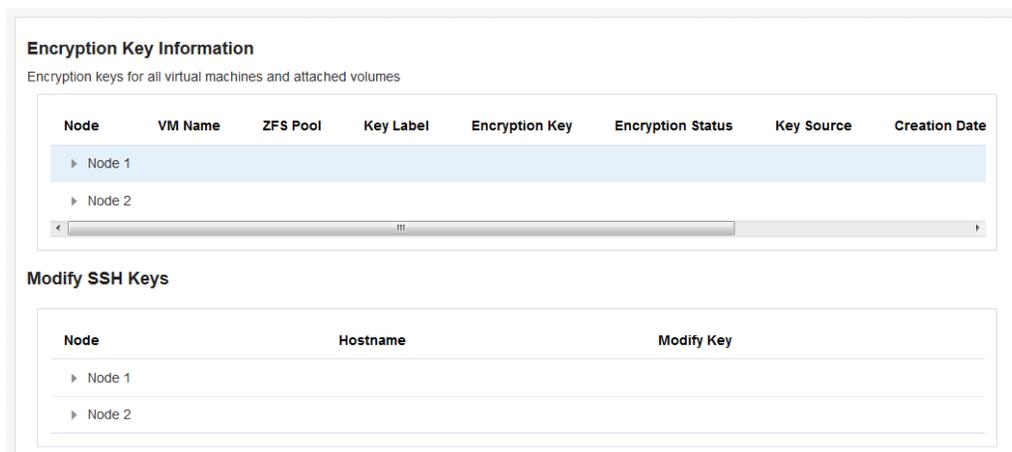
▼ 更改 SSH 密钥 (BUI)

可以使用此过程通过下列配置之一更改区域或 VM 的 SSH 密钥：

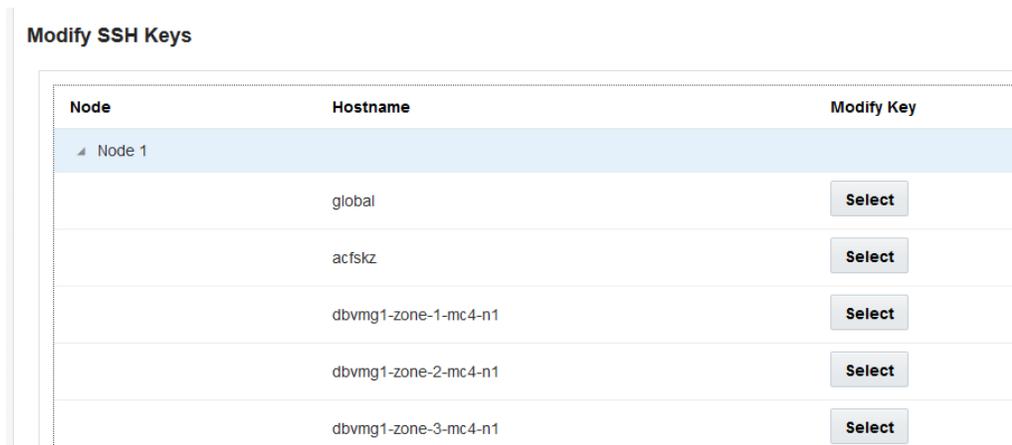
- 插入新密钥来对无密码 SSH 进行授权—要求您输入 VM 用户名、VM 机器名称，以及 RSA 公钥。
- 自动为 VM 生成新密钥

注 - 要使用 MCMU CLI 执行此过程，请参阅《Oracle MiniCluster S7-2 管理指南》。

1. 访问 MCMU BUI。
2. 在导航面板中，选择 "System Settings" (系统设置) -> "Security" (安全性)。



3. 在 "Modify SSH Keys" (修改 SSH 密钥) 面板中，单击某个节点以展开显示。



4. 对于您计划更改的 VM，单击 "Select" (选择)。
5. 从下拉菜单中选择一个选项，然后单击 "Next" (下一步)。选项如下：
 - Insert New Key to Authorize Passwordless SSH (插入新密钥以授权无密码 SSH)

- Auto Generate New Keys for Machines (自动为机器生成新密钥)
6. 单击 "Next" (下一步)。
 7. 如果您选择了对无密码 SSH 进行授权, 请输入以下信息, 然后单击 "Next" (下一步):
 - 机器的用户名
 - 机器的主机名
 - 机器的 RSA 公钥
 8. 单击 "Setup SSH" (设置 SSH)。
此时将应用更改。

使用 IPsec 实现安全通信

建议使用 IPsec (IP Security, IP 安全) 和 IKE (Internet Key Exchange, Internet 密钥交换) 来保护通过网络传输的区域间基于 IP 的通信和 NFS 通信的保密性和完整性。建议使用 IPsec, 因为它支持网络级对等验证、数据来源验证、数据保密性、数据完整性和重放保护。当在 Oracle MiniCluster 平台上使用时, IPsec 和 IKE 能够自动利用硬件协助式加密加速功能, 因此可以最大程度地降低使用加密技术保护流经网络通道的敏感信息对性能造成的影响。

▼ 配置 IPsec 和 IKE

必须先定义在通信对等节点之间使用的具体主机名和/或 IP 地址, 然后才能配置 IPsec。

对于此过程中的示例, IP 地址 10.1.1.1 和 10.1.1.2 用来指定由单个租户操作的两个 Solaris 非全局区域。这两个地址之间的通信将使用 IPsec 进行保护。此示例是从与 IP 地址 10.1.1.1 关联的非全局区域的角度讲述的。

使用以下步骤在一对指定的 (虚拟机) 非全局区域之间配置和使用 IPsec 和 IKE:

1. 定义 IPsec 安全策略。
定义在通信区域对之间将强制使用的安全策略。
在此示例中, 10.1.1.1 和 10.1.1.2 之间的所有网络通信都将加密:

```
{laddr 10.1.1.1 raddr 10.1.1.2}
ipsec{encr_algs aes encr_auth_algs sha256 sa shared}
```
2. 将策略存储在 /etc/inet/ipsecinit.conf 文件中。

3. 验证 IPsec 策略在语法上是否正确。

示例：

```
# ipsecconf -c -f ipsecinit.conf
```

4. 配置 Internet 密钥交换 (Internet Key Exchange, IKE) 服务。

按照 /etc/inet/ike/config 文件中的主机和算法设置配置该服务。

```
{ label "ipsec"
local_id_type ip
remote_addr 10.1.1.2
p1_xform { auth_method preshared oakley_group 5
auth_alg sha256 encr_alg aes } }
```

5. 配置预先共享的密钥。

必须先与两个对等节点共享密钥资料以便它们可以相互验证，然后才能启用 IPsec。

Oracle Solaris IKE 实现支持各种密钥类型，包括预先共享的密钥和证书。为简单起见，此示例使用 /etc/inet/secret/ike.preshared 文件中存储的预先共享的密钥。不过，希望使用更强验证形式的组织可以如下操作。

编辑 /etc/inet/secret/ike.preshared 文件，并输入预先共享的密钥信息。例如：

```
{
localidtype IP
localid 10.1.1.1
remoteid type IP
key "This is an ASCII phrAz, use str0ng p@sswords"
}
```

6. 在两个对等节点上启用 IPsec 和 IKE 服务。

必须先两个通信对等节点上启用这些服务，然后才能进行加密通信。

示例：

```
# svcadm enable svc:/network/ipsec/policy:default
# svcadm enable svc:/network/ipsec/ike:default
```


控制访问

以下主题介绍了 MiniCluster 中提供的访问控制功能：

- [更改默认的 Oracle ILOM root 密码 \[25\]](#)
- [配置 EEPROM 密码 \[26\]](#)
- [“用户置备” \[27\]](#)
- [“MCMU 用户审批流程” \[27\]](#)
- [“基于角色的访问控制” \[28\]](#)
- [“用户帐户” \[29\]](#)
- [“用户验证和密码策略” \[30\]](#)
- [验证 Oracle Solaris 用户角色 \[30\]](#)
- [“VM 的安全删除” \[30\]](#)
- [验证基于主机的防火墙规则 \[31\]](#)
- [检验经验证的引导环境 \[32\]](#)
- [限制对共享存储的访问 \[33\]](#)

▼ 更改默认的 Oracle ILOM root 密码

系统在出厂时在两个节点上都为 Oracle ILOM root 帐户分配了默认密码。这使得可以通过可预测的初始访问帐户执行安装过程。在安装后，请立即更改默认密码以确保最佳安全性。

1. 以 root 身份登录到节点 1 上的 Oracle ILOM。

使用 ssh 命令连接到 Oracle ILOM。

要获取 Oracle ILOM 的主机名，请在实用程序 BUI 中选择 "System Settings"（系统设置）-> "System Information"（系统信息）。主机名列在 ILOM 列下。

语法：

```
% ssh root@node1_ILOM_hostname_or_IPaddress
```

输入默认的 Oracle ILOM root 密码：welcome1

2. 更改 Oracle ILOM root 密码。

```
-> set /SP/users/root password
```

```
Enter new password: *****  
Enter new password again: *****
```

3. 在节点 2 上重复上述步骤来更改 Oracle ILOM root 密码。
4. 使用新密码更新 Oracle Engineered Systems Hardware Manager。
请参见《Oracle MiniCluster S7-2 管理指南》中的“更新组件密码”。

▼ 配置 EEPROM 密码

每个 MiniCluster 节点都有一个 EEPROM（有时称为 OpenBoot PROM），这是一个低级固件，其中包含便于引导系统的一些配置参数和驱动程序。默认情况下，EEPROM 密码功能处于禁用状态。

在安全环境中，使用此过程启用密码功能并设置密码。密码将自动启用并应用于两个节点。

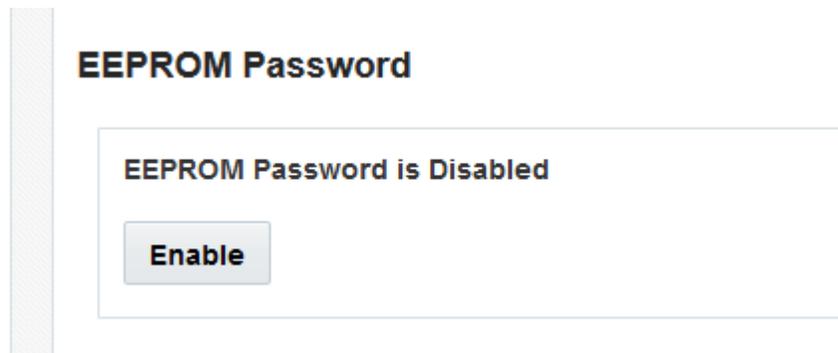
此过程取代了较旧的方法，在较旧的方法中，密码是在 OpenBoot ok 提示符下设置的，或者是在 Oracle Solaris 中通过 eeprom 命令设置的。



注意 - 请务必记住密码。如果忘记了密码，则必须呼叫支持服务来重新使您的系统可引导。

注 - 此过程介绍了如何使用 MCMU BUI 设置密码。另外，也可以使用 `mcmu security -e` 命令。

1. 以主管员身份（例如 `mcinstall`）登录到 MCMU。
2. 在导航面板中，选择 "System Settings"（系统设置）-> "Security"（安全性）



3. 执行以下操作之一：

- 要启用并设置密码—单击 "Enable"（启用），输入密码两次，然后单击 "Set Password"（设置密码）。
- 要禁用此功能—单击 "Disable"（禁用），然后单击 "Confirm"（确认）。
- 要更改现有密码—选择 "Change Password"（更改密码），两次输入新密码，然后单击 "Update"（更新）。

用户置备

在安装 MiniCluster 期间，安装过程会要求您创建并注册第一个 MCMU 用户（名为 mcinstall）。将收集该用户的人口信息，包括电子邮件地址和电话号码。mcinstall 用户是第一个主管员帐户。在 mcinstall 首次登录时，实用程序会要求 mcinstall 创建一个新密码，并且该密码必须符合与安全配置文件关联的 Oracle Solaris 密码策略。

在注册 mcinstall 用户期间，会要求您指定一个人来充当 MCMU 超级用户。只能通过名称和电子邮件地址来标识超级用户。超级用户不是 MCMU 用户，没有登录凭据。

超级用户和 mcinstall 用户都与实际的人员姓名和有效的电子邮件地址相关联。

当置备新的 MCMU 用户时，每个用户帐户都分配有一个主管员或辅助管理员角色（请参见[“基于角色的访问控制” \[28\]](#)）。在启用新帐户之前，mcinstall 用户和超级用户都必须通过他们在电子邮件中收到的 URL 来批准新用户帐户（请参见[“MCMU 用户审批流程” \[27\]](#)）。在首次登录时，会强制用户设置一个符合 MCMU 密码策略的密码。请参见[“用户验证和密码策略” \[30\]](#)。

MCMU 用户审批流程

所有 MCMU 用户帐户都需要由 MCMU 超级用户和主管员两个人批准。该流程的工作方式如下所述：

1. 预期的用户（或代表他们的 MCMU 管理员）访问 MCMU 注册页面并提供以下必需详细信息：
 - MCMU 用户名
 - 电子邮件地址
 - 全名
 - 电话号码
 - MCMU 角色
2. MCMU 向 MCMU 超级用户和主管员发送一封请求批准或拒绝的电子邮件。该电子邮件包含 MCMU 批准/拒绝功能的 URL 并且包含一个唯一的密钥标识符。

- 当超级用户和主管理员都批准了帐户时，该用户帐户便被启用，并且 MCMU 会向新用户发送一封确认帐户激活的电子邮件。用户将收到可以通过 MCMU BUI 或 CLI 访问的一个 MCMU 帐户。用户还将收到一个 Oracle Solaris 用户帐户。如果用户存在于公司 LDAP 中并且 MiniCluster 配置有 LDAP 客户机，则用户只能将 LDAP 用于 Oracle Solaris 帐户。

所有已注册的用户都存储在 MCMU 系统信息库中。MCMU 管理员可以通过查看 MCMU "System Settings" (系统设置) -> "User Accounts" (用户帐户) 来验证用户，包括其角色和超级用户。示例：

User Name ▲	Role	Date Joined	Last Login	Email	Phone	Supervisor
mcinstall	root	06-10-2016 02:02	07-10-2016 20:59	mr.smith@company.com	0000000000	mc5super
mc5super	supervisor	06-10-2016 02:03	06-10-2016 02:03	hr@company.com		
jr-admin	tadmin	07-10-2016 20:38	07-10-2016 20:51	jr.jones@company.com	4081111111	mc5super
sec-admin	auditor	07-10-2016 20:41	07-10-2016 20:41	security.boss@company.com	4082222222	mc5super
blue	root	07-10-2016 20:43	07-10-2016 20:43	blue.jeans@company.com	4083333333	mc5super
green	mcadmin	07-10-2016 20:44	07-10-2016 20:44	green.jeans@company.com	4084444444	mc5super

本部分中的后续主题将介绍如何执行这些任务。

基于角色的访问控制

MiniCluster 中没有 root 用户。相反，root 是一个角色并且分配给注册为主管理员的 MCMU 用户。

创建 MCMU 用户时，您将为用户分配下列角色之一：

- **主管理员 (root 角色)** — root 角色定义 MiniCluster 系统 (包括其所有计算节点、网络、数据库和存储) 的主管理员的权限和特权。具有 root 角色的用户可以执行所有安装和所有重要管理操作，没有任何限制。作为主管理员，他们可以委派操作并且可以批准添加和删除用户，包括新的主管理员和辅助管理员。用户必须使用其自己的凭据进行登录。执行的所有操作都将基于用户标识符而非角色标识符进行记录和审计。
- **辅助管理员 (mcadmin 角色)** — 此角色定义 MiniCluster 域和非全局区域的辅助管理员的权限和特权。默认情况下，此角色仅启用对 MCMU 的只读访问权限。执行的所有操作都将基于用户标识符而非角色标识符进行记录和审计。

- **租户管理员 (tadmin 角色)** — 此角色定义 MiniCluster VM 的管理员的权限和特权。此角色定义参与日常管理操作来为应用程序安装和部署提供支持的 VM 管理员的权限和特权。所有操作都将基于用户标识符而非角色标识符进行审计。
- **审计员 (auditor 角色)** — 具有此角色的用户只能访问 MCMU BUI 审计审核页面，他们可以在该页面上查看审计池状态以及生成关于用户活动的报告。只有具有此角色的用户可以访问审计审核页面。审计员不能访问 MCMU (审计页面除外)，也不能登录到内核区域或 VM。

用户帐户

MiniCluster 中包括此表中列出的用户帐户。

用户	密码	角色	说明
mcinstall	此密码是在安装期间配置的。它可以通过 MCMU 重置和更改。	root	<p>安装过程要求您将 mcinstall 创建为 MCMU 主管员并创建密码。此帐户计划用作 MCMU 的主管理员。</p> <p>此用户帐户用于以下活动：</p> <ul style="list-style-type: none"> ■ 通过运行 installmc 在安装时执行系统初始化。 ■ 使用 MCMU BUI 和 mcmu CLI 对系统 (包括 VM) 进行管理。 ■ 在应用程序 VM 上和全局区域及内核区域中承担 root 角色 (su 到 root) 以获取超级用户特权。
MCMU 超级用户—安装时确定的帐户名	不适用	不适用	<p>在 MiniCluster 软件中，超级用户只是一个用户名和电子邮件地址。它不是登录凭据。可以使用此帐户在 MCMU 用户审批流程中提供一个额外的层次。</p> <p>每次创建了新的 MCMU 用户时，此用户都会收到电子邮件。新用户必须由超级用户和主管员批准，该用户帐户才能启用。</p> <p>可以使用此帐户通过将主管员之外的人员指定为超级用户在 MCMU 用户审批流程中提供一个额外的层。</p>
(可选) 租户管理员—用户注册时确定的帐户名	初始登录时确定。	tadmin	<p>此用户只能在 VM 上执行所有安装后活动。</p> <p>此用户不能访问全局或内核区域，也不能运行 MCMU BUI 或 CLI。</p>
(可选) 辅助管理员—用户注册时确定的帐户名	初始登录时确定。	mcadmin	<p>当创建一个 MCMU 用户并将其指定为辅助管理员时，该用户对非全局区域具有只读访问权限。</p>
oracle	此密码与 mcinstall 密码相同。	root	<p>此用户帐户用于以下活动：</p> <ul style="list-style-type: none"> ■ 用作数据库 VM 的初始登录帐户，可以通过该帐户配置包含数据库、数据的数据库 VM，还可以根据需要配置其他帐户。 ■ 在数据库 VM 上承担 root 角色 (su 到 root) 以获取超级用户特权。

首次登录时使用的默认 MCMU 密码是 welcome1。在输入 welcome1 后，实用程序将强制用户输入一个符合密码策略的新密码。请参见“[用户验证和密码策略](#)” [30]。

所有 MCMU 用户执行的所有操作都将基于用户的标识符进行记录。有关审计报告的信息，请参见[审计与遵从性报告 \[35\]](#)。

注 - MCMU 用户帐户不用于系统的例行使用，例如使用应用程序和数据库。这些用户帐户通过 VM 上的 Oracle Solaris、应用程序和数据库进行管理，以及通过站点的名称服务进行管理。

用户验证和密码策略

在 MiniCluster 中置备的所有用户都分配有一个角色，该角色具有严格的密码策略和由安全配置文件强制实施的密码加密。

默认的安全策略设定了以下 MCMU 密码要求：

- 必须包含至少 14 个字符
- 必须具有至少一个数字字符
- 必须具有至少一个大写的字母字符
- 必须至少有三个字符不同于以前的密码
- 不能与之前的十个密码匹配

所有用户都必须仅使用用户自己的密码登录到其 Oracle Solaris 帐户。

▼ 验证 Oracle Solaris 用户角色

1. 登录到 MiniCluster 全局区域并承担 root 角色。
有关进一步的详细信息，请参阅《Oracle MiniCluster S7-2 管理指南》。

2. 验证可用角色的列表。

```
# logins -r
```

3. 检验进行验证必需的用户角色和密码：

```
# grep root /etc/user_attr
root:::audit_flags=10\::no:type=role;roleauth=user
mcinstall:::auths=solaris.system.maintenance;roles=root
```

VM 的安全删除

只有 MCMU 主管理员可以删除 VM 和 VM 组。当删除某个 VM 组件时，将自动删除对应的密钥，并且会向主管理员发送电子邮件。

要验证此功能，请在删除 VM 组件之前以主管理员身份登录到 MCMU BUI，然后查看加密密钥 ("System Settings" (系统设置) -> "Security" (安全性))。删除 VM 组件，然后再次查看密钥。已删除组件的 VM 和关联的密钥标签将不再显示。

▼ 验证基于主机的防火墙规则

所有计算环境（包括全局区域、内核区域和非全局区域）都自动配置有 IPFilter 防火墙。不需要手动配置。

要验证 IPFilter 是否正在使用，请执行以下步骤。

1. 以 `mcinstall` 身份登录到节点 1 上的全局区域，并承担 `root` 角色。
有关 Oracle ILOM 登录说明，请参阅《*Oracle MiniCluster S7-2 管理指南*》。

```
% ssh mcinstall@mc4-n1
Password: *****
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3      June 2016
Minicuster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: *****
#
```

2. 检查 IPFilter 配置。

确保 `/etc/ipf/ipf.conf` 文件中的规则与以下屏幕输出匹配。

```
# cat /etc/ipf/ipf.conf
block in log on all
block out log on ipmppub0 all
pass in quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 443 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1159 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1158 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port 5499 >< 5550 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1522 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1523 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp/udp from any to any port = domain keep state
pass in quick on ipmppub0 proto icmp icmp-type echo keep state
pass out quick on ipmppub0 proto icmp icmp-type echo keep state
pass in quick on ipmppub0 proto udp from any to any port = 123 keep state
pass out quick on ipmppub0 proto udp from any to any port = 123 keep state
block return-icmp in proto udp all
```

3. 验证 IPF 服务是否处于联机状态。

```
# svcs | grep svc:/network/ipfilter:default
```

```

online          22:13:55 svc:/network/ipfilter:default
# ipfstat -v
bad packets:           in 0    out 0
  IPv6 packets:        in 0 out 0
  input packets:        blocked 2767 passed 884831 nomatch 884798 counted 0 short 0
output packets:        blocked 0 passed 596143 nomatch 595516 counted 0 short 0
  input packets logged: blocked 0 passed 0
output packets logged: blocked 0 passed 0
  packets logged:       input 0 output 0
  log failures:         input 0 output 0
fragment state(in):    kept 0  lost 0  not fragmented 0
fragment reassembly(in): bad v6 hdr 0    bad v6 ehdr 0  failed reassembly 0
fragment state(out):   kept 0  lost 0  not fragmented 0
packet state(in):      kept 0  lost 0
packet state(out):     kept 0  lost 0
ICMP replies:         0      TCP RSTs sent: 0
Invalid source(in):   0
Result cache hits(in): 0      (out): 0
IN Pullups succeeded: 0      failed: 3462
OUT Pullups succeeded: 0      failed: 0
Fastroute successes:  0      failures: 0
TCP cksum fails(in):  0      (out): 0
IPF Ticks:             92894
Packet log flags set: (0)
                    none

```

4. 确保不需要更改防火墙规则便可访问您的数据库和应用程序。

▼ 检验经验证的引导环境

Oracle Solaris 验证的引导是一项反恶意软件和完整性保障功能，降低了恶意或意外修改重要引导和内核组件的风险。此功能检查固件、引导系统和内核的出厂签署加密签名。

默认情况下，MiniCluster 全局区域配置有 Oracle Solaris 验证的引导。如果要验证系统是否配置有验证的引导，请执行以下步骤。

1. 登录到其中一个节点上的 **Oracle ILOM**。
2. 在 **Oracle ILOM** 中检查验证的引导配置。

有关 Oracle ILOM 登录说明，请参阅《*Oracle MiniCluster S7-2 管理指南*》。

确保 boot_policy 设置为 warning。

```

-> show /HOST/verified_boot

/HOST/verified_boot
Targets:
  system_certs
  user_certs

Properties:
  boot_policy = warning

Commands:
  cd
  show

```

3. 检查验证的引导策略设置。

确保 `module_policy` 设置为 `enforce`。

```
-> show /HOST/verified_boot module_policy
```

```
/HOST/verified_boot
Properties:
  module_policy = enforce
```

4. 启动主机控制台以访问全局区域。

以 `mcinstall` 身份登录。

```
-> start /HOST/console
```

```
Are you sure you want to start /HOST/console (y/n)? y
```

```
Serial console started. To stop, type #.
```

```
Miniclustert Setup successfully configured
mc4-n1 console login: mcinstall
Password: *****
Last login: Tue Jun 28 10:17:38 2016 on rad/47
Oracle Corporation SunOS 5.11 11.3 June 2016
Miniclustert Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall %
```

5. 在全局区域中查找表明系统以验证的引导配置引导的证据。

在 `messages` 文件中查找字符串 `NOTICE: Verified boot enabled; policy=warning`。

```
mcinstall % cat /var/adm/messages | grep Verified
Jun 29 11:39:15 mc4-n1 unix: [ID 402689 kern.info] NOTICE: Verified boot enabled;
policy=warning
```

▼ 限制对共享存储的访问

MiniCluster 包含一个混合使用了 SSD 和 HDD 的存储阵列。可以对 HDD 进行配置来向 VM 提供共享存储。

MiniCluster 提供了共享存储隔离功能，这是一个便于对仅应用于全局和内核区域的共享存储进行隔离的切换开关。这有助于实现 VM 组环境的安全性和遵从性，使其不与全局和内核区域共享文件。这可确保 VM 组不再附加到 NFS 挂载并确保禁用 NFS 服务。

要实现高度安全的环境，请不要为数据库 VM 和应用程序 VM 启用共享存储。如果启用了共享存储，则文件系统必须仅可供 VM 进行只读访问。有关如何启用或禁用共享存储的说明，请参阅《Oracle MiniCluster S7-2 Administration Guide》（《Oracle MiniCluster S7-2 管理指南》），网址为：http://docs.oracle.com/cd/E69469_01。

`/sharedstore` 目录是共享存储的挂载点：

- 根据您的安全需求，牢记以下建议来配置共享存储：

- 确保共享存储不可供数据库 VM 和应用程序 VM 使用，或者确保它是只读的。
- 在生产部署中，请确保两个内核区域都不可通过公共网络访问，也不可供客户机直接访问。必须终止从公共网络或客户机对共享存储服务的所有直接访问和使用。如果虚拟机需要通过 NFS 访问 /sharedstore 文件系统，请确保通过 IPSEC/IKE 通道为虚拟机提供便利。

审计与遵从性报告

以下主题介绍了 MiniCluster 中提供的审计与遵从性报告功能：

- [验证审计策略 \[35\]](#)
- [查看审计日志 \[36\]](#)
- [生成审计报告 \[37\]](#)
- [（如果需要）启用以符合 FIPS-140 的模式运行 \(Oracle ILOM\) \[39\]](#)
- [“FIPS-140-2 级别 1 遵从性” \[40\]](#)

▼ 验证审计策略

审计策略是在安装全局区域和非全局区域期间选择遵从性配置文件（默认的 CIS 等同或 PCI-DSS）时配置的。

要验证审计策略是否已启用，请执行以下步骤。

1. 以 `mcinstall` 身份登录到全局区域，并承担 `root` 角色。

有关 Oracle ILOM 登录说明，请参阅《*Oracle MiniCluster S7-2 管理指南*》。

```
% ssh mcinstall@mc4-n1
Password: *****
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3      June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: *****
#
```

2. 验证审计服务是否处于联机状态。

```
# svcs | grep svc:/system/auditd
online          22:14:37 svc:/system/auditd:default
```

3. 验证审计插件是否处于活动状态。

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile (active)
Attributes: p_age=0h;p_dir=/var/audit;p_fsize=0;p_minfree=1
```

4. 验证处于活动状态的审计策略。

```
# auditconfig -getpolicy
configured audit policies = argv,cnt,perzone,zonename
active audit policies = argv,cnt,perzone,zonename
```

5. 验证为 `cusa` 审计策略捕获的所有角色。

```
# userattr audit_flags root
cusa:no
# userattr audit_flags mcadmin
fw,fc,fd,ps,lo,ex,ua,as,cusa:no
```

▼ 查看审计日志

1. 以 `mcinstall` 身份登录到全局区域，并承担 `root` 角色。

有关 Oracle ILOM 登录说明，请参阅《Oracle MiniCluster S7-2 管理指南》。

```
% ssh mcinstall@mc4-n1
Password: *****
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3      June 2016
Minicuster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: *****
#
```

2. 如下所示使用 `auditreduce` 命令。

下面是用于查看审计日志的语法：

```
auditreduce -z vm_name audit_file_name | praudit -s
```

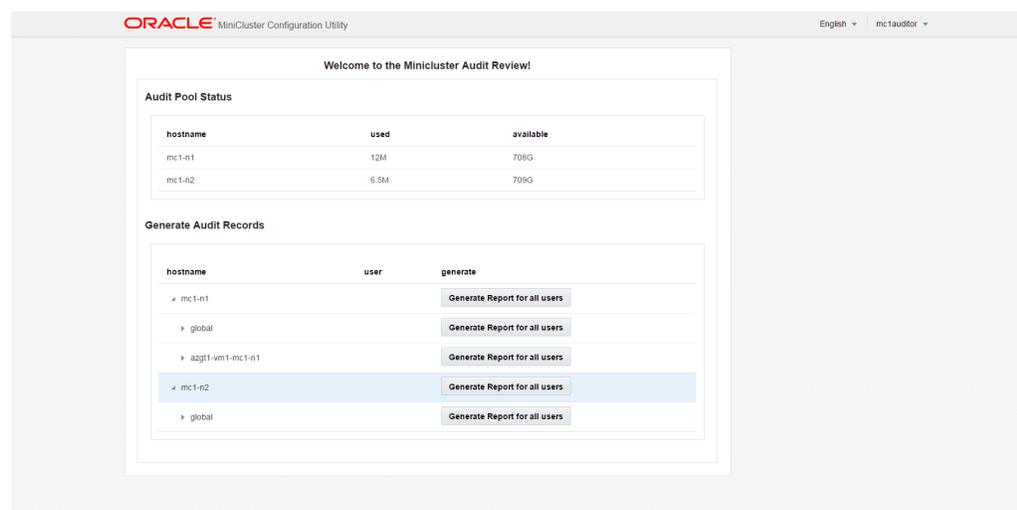
```
# cd /var/share/audit
#
# ls
20160628051437.not_terminated.mc4-n1
#
# auditreduce -z dbvmg1-zone-1-mc4-n1 20160628051437.not_terminated.mc4-n1 |
praudit -s
file,2016-06-27 22:58:53.000 -07:00,
header,127,2,AUE_zone_state,,mc4-n1.us.oracle.com,2016-06-27 22:58:53.354 -07:00
subject,mcinstall,root,root,root,root,26272,415120213,9462 65558 mc4-n1.us.oracle.com
text,boot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
header,88,2,AUE_zone_state,na,mc4-n1.us.oracle.com,2016-06-27 23:02:30.767 -07:00
text,reboot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
file,2016-06-27 23:02:30.000 -07:00,
```

▼ 生成审计报告

使用此过程为节点或者为各个 VM 和全局区域生成审计报告。

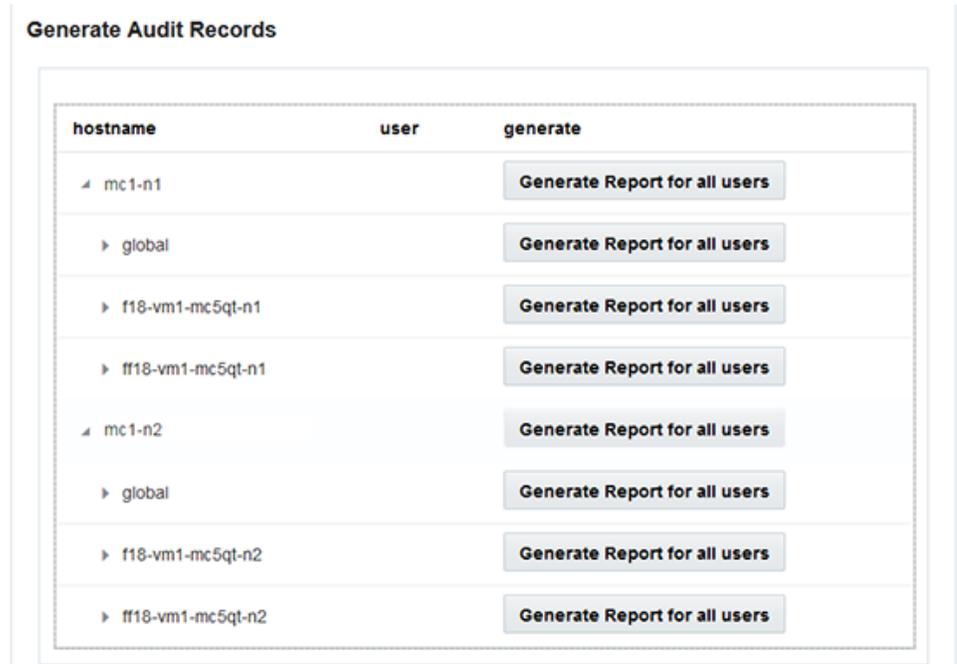
1. 以分配有审计员角色的用户的身份登录到 **MCMU**。
有关 MCMU 用户和角色的信息，请参阅《Oracle MiniCluster S7-2 Administration Guide》（《Oracle MiniCluster S7-2 管理指南》），网址为：http://docs.oracle.com/cd/E69469_01。
2. 在导航面板中，选择 **"System Settings"（系统设置）** -> **"Security"（安全性）**。
此时将显示 **"Audit Review"（审计审核）** 页面。

注 - 只有分配有审计员角色的 MCMU 用户可以显示此页面。

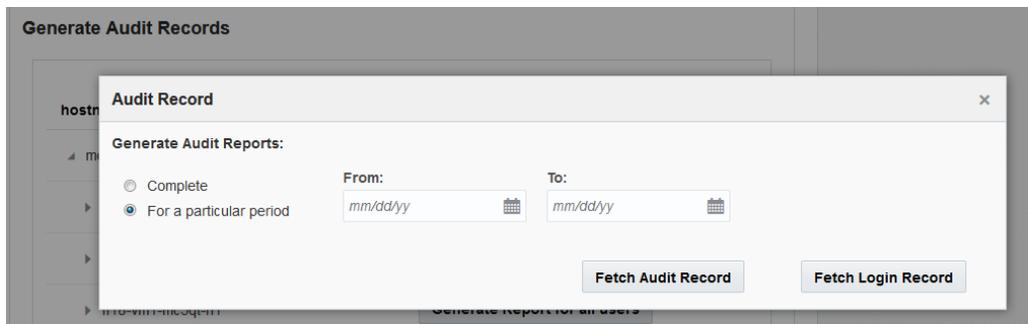


3. 检查 **"Audit Pool Status"（审计池状态）** 部分。
此部分列出了每个节点上的审计池已使用的空间量和可用的空间量。
4. 要为整个节点生成报告，请单击其中一个节点的 **"Generate"（生成）** 按钮，然后转到 **步骤 6**
另外，还可以为特定的 VM 或区域生成报告。请参见 **步骤 5**
5. 要为特定的 VM 或全局区域生成报告，请执行以下步骤。

- a. 单击节点旁边的三角形以展开视图。



- b. 对于 VM 或全局区域，单击 "Generate Report for all users"（为所有用户生成报告）。
6. 在 "Audit Record"（审计记录）对话框中，配置审计记录参数。



下面是可供选择的选项：

- **Complete (完整)** — 如果希望获得包括所有审计记录的报告，请选择此项。
- **For a particular period (针对特定期间)** — 如果希望指定特定的时间段，则输入开始日期和结束日期。

7. 单击其中一个 **"Fetch" (提取)** 按钮。

下面是可供选择的选项：

- **Fetch Audit Record (提取审计记录)** — 生成完整的审计记录。
- **Fetch Login Record (提取登录记录)** — 生成用户活动，例如登录、注销和用户操作。

8. 单击 **"Click Here" (单击此处)** 按钮并选择 **"download XML file" (下载 XML 文件)**。

可以将 XML 文件导入到审计分析应用程序（例如 Oracle Audit Vault）中。

9. 单击 **"Close" (关闭)**。

▼ (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。不过，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》中标题为“当 FIPS 模式处于启用状态时不受支持的功能”的一节涵盖了这些功能的列表。

另请参见“[FIPS-140-2 级别 1 遵从性](#)” [40]。



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**。
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。

要使其更改生效，必须重新启动 Oracle ILOM SP。

```
-> reset /SP
```

FIPS-140-2 级别 1 遵从性

在 MiniCluster 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 遵从性进行了验证。Oracle Solaris 加密框架是 Oracle Solaris 的中央加密存储库，它提供了两个经 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 遵从性进行了验证，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 \(Oracle ILOM\) \[39\]](#)。

下表列出了 FIPS 认可的且 Oracle Solaris 在 MiniCluster 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

密钥或 CSP	证书编号	
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
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。

访问安全遵从性

以下主题介绍了 MiniCluster 安全基准测试功能：

- [“安全遵从性基准测试” \[43\]](#)
- [计划安全遵从性基准测试 \(BUI\) \[43\]](#)
- [查看基准测试报告 \(BUI\) \[45\]](#)

安全遵从性基准测试

安装系统时，会选择一个安全配置文件（PCI-DSS、CIS 等同，以及 DISA-STiG），并且会自动将系统配置为符合该安全配置文件。为确保系统继续根据安全配置文件运行，MCMU 提供了相应的方法来运行安全基准测试和访问基准测试报告。您可以使用 MCMU BUI 和 CLI 来管理基准测试。

运行安全基准测试提供了以下优点：

- 允许您评估数据库和应用程序 VM 的当前安全状态。
- 安全遵从性测试支持 PCI-DSS、CIS 等同标准（默认）和 DISA-STiG，具体取决于在安装期间配置的安全级别。
- 安全遵从性测试在系统引导时自动运行，并且可以按需或按计划的间隔运行。
- 可以轻松从 MCMU BUI 访问遵从性分数和报告，但仅可供 MCMU 主管管理员访问。
- 遵从性报告可提供纠正建议。

注 - DISA-STIG 配置文件当前处于审核阶段。请仅在非生产环境中将此配置文件用于试验用途。

▼ 计划安全遵从性基准测试 (BUI)

可以使用此过程通过 MCMU BUI 计划安全基准测试。要改用 MCMU CLI，请参阅《*Oracle MiniCluster S7-2 管理指南*》中的说明。

1. 以主管管理员身份登录到 **MCMU BUI**。
有关说明，请参阅《*Oracle MiniCluster S7-2 管理指南*》。

2. 在主页中，向下滚动到 **"Compliance Information"**（遵从性信息）面板。
3. 单击某个节点以展开其详细信息。
每个区域和 VM 都配置有一个安全配置文件（CIS 等同或 PCI-DSS）。在计划基准测试时，请选择与组件的安全配置文件对应的基准测试。

Compliance Information
Assess and Report Compliance for the virtual machines in the system

Update Reports

Node	Hostname	Benchmark Type	Compliance Score	Date & Time	Remarks	View Report
Node 1						
	global	pci-dss			No Reports Found	
	global	cis.equivalent			No Reports Found	
	dbvmg1-zone-1-mc4-n1	pci-dss			No Reports Found	
	dbvmg1-zone-1-mc4-n1	cis.equivalent			No Reports Found	
	dbvmg1-zone-2-mc4-n1	pci-dss			No Reports Found	
	dbvmg1-zone-2-mc4-n1	cis.equivalent			No Reports Found	
	dbvmg1-zone-3-mc4-n1	pci-dss			No Reports Found	
	dbvmg1-zone-3-mc4-n1	cis.equivalent			No Reports Found	

4. 向右滚动并单击其中一个 VM 的 **"Schedule"**（计划）按钮。
此时将显示 "Schedule Compliance Run"（计划遵从性运行）页面。

Schedule Compliance Run

Schedule: dbvmg1-zone-1-mc4-n1/cis.equivalent

24 hours format, eg: 18:00, 04:50, later than the default time shown

Time to run compliance(in 24 hours format): 14:15

Select a Frequency of run: only once

Cancel Start

- 指定时间和频率，然后单击 **"Start"**（开始）。
在安全遵从性测试按计划的时间运行后，查看报告。请参见[查看基准测试报告 \(BUI\) \[45\]](#)。

▼ 查看基准测试报告 (BUI)

下面是可接受的遵从性结果：

	CIS 等同	PCI-DSS
全局区域	大约 88%	大约 88%
VM	大约 90%	大约 93%

下面是因为 Oracle Solaris 问题而导致的已知遵从性测试错误：

- 软件包完整性（核心 OS、rad-python）
- GDM
- 路由守护进程
- SSH 回送地址—迁移不能修复此问题。
- 命名服务无法识别 DNS
- LDAP 客户机

下面是因为 MiniCluster 客户必需配置问题而导致的已知遵从性测试错误：

- NFS 客户机服务—选择需要可用的服务。
- 设置 eeprom 密码—可选设置

- 登录到 **MCMU BUI**。
- 在主页中，向下滚动到 **"Compliance Information"**（遵从性信息）面板。
- 单击 **"Update Reports"**（更新报告）。
更新过程需要大约一分钟才能完成。
- 展开节点显示并找到遵从性报告。

e-1-mc4-n1	cis.equivalent	89.83/100	2016-06-20,14:21	-	View Report
------------	----------------	-----------	------------------	---	-----------------------------

- 向右滚动并单击 **"View Report"**（查看报告）。

此时将显示基准测试报告。

在 "Rule Overview" 下，您可以选择要基于其结果显示的测试类型。您还可以在搜索字段中指定一个搜索字符串。



Compliance Report

Oracle Solaris Security Policy

with profile **Solaris Recommended Security Policy**

Oracle Solaris Compliance baseline and recommended settings for general purpose operating systems installations.

Evaluation Characteristics

Target machine	appvmg1-zone-1-mc4-n1
Benchmark Title	Oracle Solaris Security Policy
Benchmark Version	1.13749
Benchmark Description	Oracle Solaris Compliance baseline and recommended settings for general purpose operating systems installations.
Profile ID	Recommended
Started at	2016-06-20T14:21:21
Finished at	2016-06-20T14:22:10
Performed by	

CPE Platforms

- cpe:/o:oracle:solaris:11

Addresses

Compliance and Scoring

The target system did not satisfy the conditions of 11 rules! Please review rule results and consider applying remediation.

Rule results

174 passed 11 failed

Severity of failed rules

1 other 4 low 5 medium 1 high

6. 根据报告，您可以验证安全控制、遵从性分数、异常和纠正措施过程。
7. 单击某个测试的名称可以获取详细信息和建议的纠正措施信息。

注 - 您可以通过单击报告底部的 "Show all Result Details" 来显示所有测试的所有详细信息。

×
Package integrity is verified

Rule ID	OSC-54005
Result	fail
Time	2016-06-20T14:21:46
Severity	high
Identifiers and References	
Description	Run 'pkg verify' to check that all installed Oracle Solaris software matches the packaging database and that ownership, permissions and content are correct.

SCE stdout

The following packages showed errors

pkg://solaris/system/core-os	ERROR
pkg://solaris/system/management/rad/client/rad-python	ERROR

Run 'pkg verify' to determine the nature of the errors.

Remediation description:

'pkg verify' has produced errors. Rerun the command and evaluate the errors. As appropriate, based on errors found, you should run 'pkg fix <package-fmri>' See the pkg(1) man page.

Remediation script:

```
# pkg verify
followed by
# pkg fix <package-fmri>
```

Service svc:/system/pkg is enabled in global zone
medium
pass

了解 SPARC S7-2 服务器安全控制

以下主题介绍了针对硬件和 OpenBoot 环境的安全控制。

- [“了解硬件安全” \[49\]](#)
- [“限制对 OpenBoot 的访问” \[50\]](#)

了解硬件安全

应该将安全体系结构建立在物理隔离和访问控制的基础之上。确保物理服务器安装在安全的环境中，防止其遭受未经授权的访问。同样，记录所有序列号有助于防止被盗、转售或供应链风险（即仿冒或危及安全的组件注入到组织供应链中）。

以下几部分提供了有关 MiniCluster 的一般硬件安全准则。

- [“限制人员接近” \[49\]](#)
- [“序列号” \[50\]](#)
- [“硬盘驱动器” \[50\]](#)

限制人员接近

- 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，则除非必须在机架内维修组件，否则应始终锁上机架门。锁上机架门还可以限制人员接近热插拔或热交换设备。
- 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。仅限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。由于物理访问不容易遭受网络攻击，因此这是一种较安全的组件访问方法。

- 将控制台连接到外部 KVM 以实现远程控制台访问。KVM 设备通常支持双重验证、集中访问控制和审计。有关 KVM 的安全准则和最佳实践的更多信息，请参阅 KVM 设备随附的文档。

序列号

- 保留所有硬件的序列号记录。
- 为计算机硬件的所有重要物项（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。

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

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

硬盘驱动器

硬盘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、停止使用或处置硬盘驱动器之前，应对其进行净化处理。

- 使用 Oracle Solaris format (1M) 命令等磁盘擦除工具彻底删除硬盘驱动器上的所有数据。
- 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，利用 Oracle 的客户数据和设备保留服务

<http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf>

限制对 OpenBoot 的访问

以下主题介绍了如何在 OpenBoot 提示符下限制访问。

有关如何为 OpenBoot 配置密码的说明，请参见[配置 EEPROM 密码 \[26\]](#)。

- [进入 OpenBoot 提示符 \[51\]](#)
- [检查失败的登录 \[51\]](#)

- [提供通电横幅 \[51\]](#)

有关设置 OpenBoot 安全变量的信息，请参阅 OpenBoot 文档，网址为：

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

▼ 进入 OpenBoot 提示符

此过程介绍了在 MiniCluster 计算节点上如何进入 OpenBoot 提示符来配置安全控制。

必须关闭系统才能到达 OpenBoot 提示符。请执行用于干净地关闭 VM 的合适过程，如《*Oracle MiniCluster S7-2 管理指南*》中所述。

1. 登录到一个节点上的 **Oracle ILOM** 并发出以下命令。

```
-> set /HOST/bootmode script="setenv auto-boot? false
-> start /HOST/console
```

以 mcinstall 用户身份登录到主机控制台并 su 到 root。

2. 在所有 VM 都关闭后，以 **root** 角色停止全局区域。

```
# init 0
.
.
.
{0} ok
```

▼ 检查失败的登录

1. 确定是否有人尝试使用 `security-#badlogins` 参数访问 OpenBoot 环境且访问失败，如以下示例所示。

```
{0} ok printenv security-#badlogins
```

如果此命令返回任何大于 0 的值，则记录了访问 OpenBoot 环境失败的尝试。

2. 通过键入以下命令重置参数。

```
{0} ok setenv security-#badlogins 0
```

▼ 提供通电横幅

虽然横幅不是直接预防或检测控件，但会出于以下原因使用它：

- 传达所有权。
 - 警告用户可接受的服务器用法。
 - 指明仅限经授权的人员访问或修改 OpenBoot 参数。
- 使用以下命令启用定制警告消息。

```
{0} ok setenv oem-banner banner-message  
{0} ok setenv oem-banner? true
```

横幅消息最多可以为 68 个字符。接受所有可输出的字符。

索引

A

安全

- 原则, 9, 10

- 查看信息 (BUI), 19

- 查看基准测试报告 (BUI), 45

- 遵从性基准测试, 43

- 遵从性基准测试, 计划 (BUI), 43

- 配置文件, 15

- 安全 Shell 服务, 20

- 安全的虚拟机, 11

- 安全配置文件

 - 验证, 15

- 安全任务, 最少必需的, 9

- 安全散列标准, 40

- 安全性

 - 更改 Oracle ILOM 密码, 25

B

- 保护数据, 19

- 必需的安全任务, 9

C

- 采用 ZFS 数据集加密的数据保护, 19

- 策略, 安全, 10

- 查看

 - 安全基准测试报告 (BUI), 45

 - 系统安全信息 (system security information, BUI), 19

- 查看审计日志, 36

- 超级用户帐户, 29

D

- 登录, 检查失败的 OBP, 51

- 对称密钥, 40

- DISA STIG 配置文件, 15

E

- EEPROM, 配置密码, 26

F

- 防火墙规则, 验证, 31

- 访问 OpenBoot 提示符, 51

- 访问控制, 12

- 非对称密钥, 40

- 辅助管理员帐户, 29

- FIPS-140

 - 以符合标准的模式运行 (Oracle ILOM), 启用, 39

 - 级别 1 遵从性, 40

 - 认可的算法, 40

G

- 概述

 - MCMU 用户帐户, 29

 - 用户审批流程, 27

- 更改 SSH 密钥, 20

- 共享存储, 限制访问, 33

H

- 横幅, 提供, 51

I

- IKE, 配置, 22

- IPsec, 22

IPsec, 配置, 22

J

基于散列的消息验证, 40
计划安全基准测试, 43
加密, 12, 19
加密加速, 12
检查失败的 OBP 登录, 51

M

密码
 MCMU 的默认密码, 29
 在 Oracle ILOM 中更改, 25
 策略, 30
默认安全配置文件, 15
mcinstall 用户帐户, 29
MCMU 用户
 审批流程, 27
MCMU 用户帐户, 29
MCMU 用户帐户的角色, 28

O

OpenBoot
 访问, 51
 配置密码, 26
 限制对 OpenBoot 的访问, 50
Oracle ILOM, 更改 root 密码, 25
Oracle Solaris 用户角色, 验证, 30

P

配置
 EEPROM 密码, 26
 IPsec 和 IKE, 22
配置文件, 安全, 15
PCI-DSS 配置文件, 15
PKCS#11, 12

Q

启用 以符合 FIPS-140 的模式运行 (Oracle ILOM), 39

R

root, 更改密码
 , 25

S

审计报告, 生成, 37
审计策略, 验证, 35
审计和遵从性, 13
审计日志, 查看, 36
生成审计报告, 37
使用 IPsec 实现安全通信, 22
数据保护, 12
随机数生成器, 40
SSH 密钥, 更改, 20
SSH 网络协议, 20

T

特权, 28
提供通电横幅, 51

V

VM 的安全删除, 30
VM, 安全删除, 30

X

限制对共享存储的访问, 33
虚拟机, 安全, 11
序列号, 50

Y

验证
 Oracle Solaris 用户角色, 30
 基于主机的防火墙规则, 31
 安全配置文件, 15
 审计策略, 35
 验证的引导环境, 32
验证的引导环境, 验证, 32
验证日志文件, 15

硬件

- 序列号, 50
- 访问限制, 49
- 硬件安全, 了解, 49
- 硬件的访问限制, 49
- 硬盘驱动器, 50
- 用户
 - 审批流程, 27
 - 置备, 27
- 用户帐户, 29
- 用户帐户角色, 28
- 原则, 安全, 9, 10

Z

- 置备用户, 27
- 主管理员帐户, 29
- 租户管理员帐户, 29
- 最少必需的安全任务, 9
- 遵从性和审计, 13
- 遵从性基准测试
 - 概述, 43
- ZFS 数据集加密, 19

