Oracle® ZFS Storage Appliance 安全指南，发行版 OS8.6.x

文件号码 **E78552-01**
2016 年 9 月

ORACLE

文件号码 E78552-01

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

Oracle ZFS Storage Appliance 安全指南

本指南探讨、回顾并重点介绍了创建安全的存储系统和让整个团队理解组织的具体安全目标需要注意的安全事项。建议在配置设备之前阅读本指南，以便利用可用的安全功能并实现需要的安全级别。

您还可以将本指南用作参考，以便找到有关 Oracle ZFS Storage Appliance 各种特性和功能的安全注意事项的更多详细信息。有关设备配置过程，请参见《Oracle ZFS Storage Appliance 管理指南》。

以下各节介绍了 Oracle ZFS Storage Appliance 安全功能和建议：

- **初始步骤**－介绍设备初始安装期间的登录安全以及针对您系统物理安全的建议。
- **管理模型**－介绍通过 BUI 和 CLI 的远程访问、限制对 BUI 和 CLI 的访问、系统修补模型、延迟更新、支持包和配置备份。
- **设备用户**－介绍可管理设备的管理角色以及管理用户授权。
- **访问控制列表**－介绍允许或拒绝访问文件和目录的机制。
- **数据服务**－介绍设备所支持的数据服务以及不同数据服务所提供的安全性。
- **目录服务**－介绍可在设备上配置的目录服务及其对安全性的影响。
-
- **安全日志**－介绍与安全相关的日志类型。

初始步骤

本节介绍设备初始安装期间的登录安全以及针对您系统物理安全的建议。

初始安装

Oracle ZFS Storage Appliance 交付时已预安装了设备软件。因此无需软件安装或提供任何介质。

完成初始安装时使用的是默认帐户名和密码；必须在安装后更改默认 root 用户密码。如果 Oracle ZFS Storage Appliance 重置为出厂默认值，则该设备和服务处理器的 root 用户密码也都会重置为默认值。

在 Oracle ZFS Storage Appliance 的初始安装期间，存在与系统服务处理器关联的默认帐户名和密码。系统管理员可以使用该默认帐户首次访问设备，访问期间将要求管理员执行初始安装步骤。其中一个要求执行的步骤是设置新的设备管理密码，这进而也会将默认服务处理器密码重置为相同的值。

物理安全

要控制对系统的访问，必须维护好所在计算环境的物理安全。例如，如果系统已登录但却无人值守，则会很容易发生未经授权的访问。必须始终以物理方式保护好计算机的周围环境和计算机硬件，防止出现未经授权的访问。

Oracle ZFS Storage Appliance 用于限制访问，通过使用安全手段（例如，密钥、锁、工具以及标记访问）对访问进行控制，并且已为授权访问的人员指示限制的原因以及需要采取的任何防范措施。

管理模型

本节介绍了 Oracle ZFS Storage Appliance 管理模型的安全性。

远程管理访问

本节介绍了 Oracle ZFS Storage Appliance 远程访问安全性。

浏览器用户界面

浏览器用户界面 (Browser User Interface, BUI) 用于设备的常规管理。您可以使用 BUI 服务屏幕查看和修改远程访问服务和设置。

管理通过 HTTP 安全 (HTTPS) 浏览器会话进行。HTTPS 会话使用每个 Oracle ZFS Storage Appliance 初始安装时唯一生成的自签名证书进行加密。HTTPS 会话的用户可定义默认会话超时为 15 分钟。

命令行界面

命令行界面 (Command Line Interface, CLI) 可用于执行可在 BUI 中执行的大多数相同管理操作。

安全 Shell (Secure Shell, SSH) 允许用户通过与 CLI 的安全套接字层 (Secure Sockets Layer, SSL) 连接登录到 Oracle ZFS Storage Appliance。SSH 还可以用作从远程主机执行自动脚本的方式，例如用于检索每日日志或分析统计信息。

受限用户授权

管理访问仅限于 root 用户、定义有相关权限的本地管理员，以及通过标识服务器（如轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP) 和网络信息服务 (Network Information Service, NIS)）授权的用户。

Oracle ZFS Storage Appliance RESTful API

Oracle ZFS Storage Appliance RESTful API 可用于管理 Oracle ZFS Storage Appliance。RESTful 体系结构基于分层的客户机/服务器模型，此模型允许通过标准集线器、路由器和其他网络系统在没有客户机配置的情况下透明地重定向服务。

Oracle ZFS Storage Appliance RESTful API 使用与 BUI 和 CLI 相同的验证凭证。来自外部客户机的所有请求都单独使用设备凭证进行验证并在端口 215 上通过 HTTPS 连接来执行。RESTful API 支持用户可定义默认超时为 15 分钟的 HTTPS 会话。

有关使用 RESTful API 管理 Oracle ZFS Storage Appliance 的信息，请参见《Oracle ZFS Storage Appliance RESTful API 指南》。

系统更新

要利用最新的安全改进，Oracle 建议将系统软件保持最新。

系统更新将作为完整的系统软件二进制替换进行应用。更新之前，将对正在运行的系统池创建快照。这样可在需要时允许管理员回滚到先前的版本。

延迟更新

延迟更新是一项功能，属于系统更新的一部分，但不会在执行系统更新时激活。由管理员决定何时以及是否应用延迟更新。系统更新期间未应用的更新在连续系统更新期间仍可用。无法选择应用单个更新；选择应用延迟更新时，不是应用所有更新，就是不应用任何更新。应用更新后，将无法回滚到较早的系统软件版本。

支持包

如果您的系统已注册到回拨支持并遭遇重大故障，则会向 My Oracle Support 发送您的系统状态，My Oracle Support 的工程支持人员会对其进行检查并创建支持包。向 My Oracle Support 发送的系统状态信息不包含任何用户数据；仅发送配置信息。

配置备份

可将系统配置保存到本地以供日后恢复。这些备份不包含任何用户数据；仅保存配置设置。

设备用户

有两种类型的 Oracle ZFS Storage Appliance 用户：

- **数据服务用户**－使用支持的协议（如网络文件系统 (Network File System, NFS)、Server Message Block (SMB)、光纤通道、Internet 小型计算机系统接口 (Internet Small Computer System Interface, iSCSI)、超文本传输协议 (Hypertext Transfer Protocol, HTTP) 和文件传输协议 (File Transfer Protocol, FTP)）访问文件和块资源的客户机。
- **管理用户**－管理设备上的配置和服务的用户。

本节仅适用于管理用户。

管理用户角色

您可以通过向管理员分配定制角色来授予其权限。角色是可分配给管理员的一组特权。可能需要创建多个授权级别不同的管理员和操作员角色。应为员工分配满足其需求的任何角色，而不为其分配不必要的特权。

使用角色比使用共享的完全访问管理员密码（例如向所有人提供 root 用户密码）更安全。角色可限制用户仅具有定义的几组授权。此外，还可在审计日志中将用户角色跟踪到各自的用户名。默认情况下，存在称为 "Basic administration"（基本管理）的角色，它包含最基本的授权。

管理用户可以是：

- **本地用户**－此时所有帐户信息都保存在 Oracle ZFS Storage Appliance 中。
- **目录用户**－使用现有的 NIS 或 LDAP 帐户，补充性的授权设置保存在设备中。必须向现有 NIS/LDAP 用户显式授予对设备的访问权限，这些用户才可以登录并管理设备。默认情况下，无法授予访问权限。

管理范围

通过授权，用户可执行特定任务，例如创建共享资源、重新引导设备和更新系统软件。授权组称为范围。每个范围可以有一组可选的过滤器，用于缩减授权的数目。例如，可使用过滤器使授权只能重新启动 HTTP 服务，而不是重新启动所有服务。

访问控制列表

Oracle ZFS Storage Appliance 通过访问控制列表 (access control list, ACL) 提供文件访问控制。ACL 是一种允许或拒绝访问特定文件或目录的机制。

Oracle ZFS Storage Appliance 提供的 ACL 模型以 NFSv4 ACL 模型为基础，派生于 Windows ACL 语义。这是一种丰富的 ACL 模型，可提供对文件和目录的细粒度访问。存储设备中的每个文件和目录都具有一个 ACL，SMB 和 NFS 的所有访问控制决定都会使用相同的算法，从而确定允许或拒绝哪些用户访问文件和目录。

一个 ACL 由一个或多个访问控制条目 (access control entry, ACE) 组成。每个 ACE 都包含 ACE 授予或拒绝的权限的条目、ACE 应用到的用户和所使用的继承级标志。

ACL 继承

通过 NFSv4 ACL，新创建的文件和目录即可继承单个 ACE。ACE 继承由初始配置 ACL 时管理员在其中设置的多个继承级标志控制。

确定 ACL 访问

NFSv4 ACL 具有一定的顺序，将从上到下进行处理。授予权限后，后续 ACE 将无法取消该权限。拒绝权限后，后续 ACE 将无法授予该权限。

SMB 共享资源级 ACL

SMB 共享资源级 ACL 是一种与共享资源中文件或目录 ACL 结合使用以确定该文件的有效权限的 ACL。共享资源级 ACL 在文件 ACL 之上又提供了一个访问控制层，以便提供更加复杂的访问控制配置。共享资源级 ACL 在使用 SMB 协议导出文件系统时进行设置。如果未通过 SMB 协议导出文件系统，则设置共享资源级 ACL 将不起任何作用。默认情况下，共享资源级 ACL 会向每个人授予完全控制权限。

ZFS ACL 属性

ACL 行为和继承属性仅适用于 NFS 客户机。SMB 客户机使用严格的 Windows 语义且优先于 ZFS 属性。区别在于 NFS 使用 POSIX 语义而 SMB 客户机不使用该语义。这些属性主要与 POSIX 兼容。

数据服务

下表提供了各个数据服务的说明和所用端口。

表 1 数据服务

服务	说明	所用端口
NFS	通过 NFSv3 和 NFSv4 协议的文件系统访问	111 和 2049
iSCSI	通过 iSCSI 协议的 LUN 访问	3260 和 3205
SMB	通过 SMB 协议的文件系统访问	SMB-over-NetBIOS 139 SMB-over-TCP 445 NetBIOS 数据报 138 NetBIOS 名称服务 137
病毒扫描	文件系统病毒扫描	
FTP	通过 FTP 协议的文件系统访问	21
HTTP	通过 HTTP 协议的文件系统访问	80
HTTPS	用于传入的安全连接	443
NDMP	NDMP 主机服务	10000
远程复制	远程复制	216 和 217
加密	文件系统和 LUN 的透明加密	
影子迁移	影子数据迁移	
SFTP	通过 SFTP 协议的文件系统访问	218
TFTP	通过 TFTP 协议的文件系统访问	
存储区域网络	存储区域网络目标和启动器组	

所需的最少端口数

要提供网络安全，可以创建防火墙。端口号用于创建防火墙并通过指定主机和服务在网络上唯一标识事务。

以下列表显示了创建防火墙所需的最少端口数：

传入端口

- icmp/0-65535 (PING)
- tcp/1920 (EM)
- tcp/215 (BUI)
- tcp/22 (SSH)
- udp/161 (SNMP)

如果使用了 HTTP 文件共享（通常不会使用），则还需要以下传入端口：

- tcp/443 (SSL WEB)
- tcp/80 (WEB)

传出端口

- tcp/80 (WEB)

注 - 对于复制，尽可能使用通用路由封装 (Generic Routing Encapsulation, GRE) 隧道。这样可以让流量在后端接口上运行，并避免在可能减慢流量的地方设置防火墙。如果 GRE 隧道在 NFS 核心上不可用，则您必须在前端接口运行复制。在这种情况下，端口 216 和端口 217 还必须是开放的。

NFS 验证和加密选项

默认情况下，NFS 共享资源通过 AUTH_SYS RPC 验证进行分配。也可以将其配置为通过 Kerberos 安全进行共享。使用 AUTH_SYS 验证，客户机的 UNIX 用户 ID (User ID, UID) 和组 ID (Group ID, GID) 在网络上传递时不会经过 NFS 服务器验证。此验证机制可被客户机上具有 root 访问权限的任何人轻松破解；因此，最好使用一个其他可用安全模式。

可以以共享资源为单位指定其他访问控制，从而允许或拒绝对特定主机、DNS 域或网络的共享资源的访问。

安全模式

安全模式以共享资源为单位进行设置。以下列表介绍了可用的 Kerberos 安全设置：

- **krb5**－通过 Kerberos V5 进行最终用户验证
- **krb5i**－krb5 加完整性保护（数据包是防篡改的）
- **krb5p**－krb5i 加隐私保护（数据包是防篡改而经过加密的）

Kerberos 类型的组合也可以在安全模式设置中指定。组合安全模式允许客户机使用所列出的任何 Kerberos 类型进行挂载。

Kerberos 类型

- **sys**－系统验证
- **krb5**－仅限 Kerberos v5，客户机必须使用此类型进行挂载
- **krb5:krb5i**－Kerberos v5，带有完整性，客户机可以使用所列出的任何类型进行挂载
- **krb5i**－仅限 Kerberos v5 完整性 ，客户机必须使用此类型进行挂载
- **krb5:krb5i:krb5p**－Kerberos v5，带有完整性或隐私，客户机可以使用所列出的任何类型进行挂载

- **krb5p**－仅限 Kerberos v5 隐私，客户机必须使用此类型进行挂载

iSCSI 数据服务

在 Oracle ZFS Storage Appliance 上配置 LUN 时，您可以通过 iSCSI 目标导出该卷。通过 iSCSI 服务，iSCSI 启动器可以使用 iSCSI 协议访问目标。

该服务支持使用 iSNS 协议进行搜索、管理和配置。iSCSI 服务支持使用质询握手验证协议 (Challenge-Handshake Authentication Protocol, CHAP) 的单向验证（目标对启动器进行验证）和双向验证（目标和启动器相互验证）。此外，该服务还支持远程验证拨入用户服务 (Remote Authentication Dial-In User Service, RADIUS) 数据库中的 CHAP 验证数据管理。

系统首先执行验证，然后进行授权，这在两个独立的步骤中进行。如果本地启动器具有 CHAP 名称和 CHAP 密钥，则系统将执行验证。如果本地启动器没有 CHAP 属性，则系统不会执行任何验证，因此所有启动器都将符合授权条件。

通过 iSCSI 服务，您可以指定能够在启动器组内使用的启动器的全局列表。使用 iSCSI 和 CHAP 验证时，RADIUS 可用作延迟选定 RADIUS 服务器的所有 CHAP 验证的 iSCSI 协议。

RADIUS 支持

RADIUS 是代表存储节点使用中央服务器执行 CHAP 验证的系统。使用 iSCSI 和 CHAP 验证时，可为 iSCSI 协议选择 RADIUS，这可同时应用 iSCSI 和 RDMA 的 iSCSI 扩展 (iSCSI Extensions for RDMA, iSER)，然后将所有 CHAP 验证发送到选定的 RADIUS 服务器。

为使 Oracle ZFS Storage Appliance 能够使用 RADIUS 执行 CHAP 验证，必须满足以下要求：

- 设备必须指定 RADIUS 服务器的地址，以及与该 RADIUS 服务器通信时要使用的密钥。
- RADIUS 服务器必须有一个条目（例如，在其客户机文件中）指明设备的地址并指定与上面相同的密钥。
- RADIUS 必须有一个条目（例如，在其用户文件中）提供 CHAP 名称并与每个启动器的 CHAP 密钥匹配。
- 如果启动器使用其 IQN 名称作为 CHAP 名称（这是建议的配置）且设备无需在每个 "Initiator"（启动器）框中分别输入启动器条目，则 RADIUS 服务器可执行所有验证步骤。
- 如果启动器使用单独的 CHAP 名称，则设备必须有一个启动器条目对应于该启动器并指定从 IQN 名称到 CHAP 名称的映射关系。该启动器条目无需指定启动器的 CHAP 密钥。

SMB 数据服务

SMB 协议（也称为通用 Internet 文件系统 (Common Internet File System, CIFS)）主要提供对 Microsoft Windows 网络上文件的共享访问。另外，它还提供验证。

以下 SMB 选项具有安全隐患：

- **Restrict Anonymous Access to Share List（限制匿名访问共享资源列表）**－此选项要求客户机在接收共享资源列表之前使用 SMB 进行验证。如果禁用此选项，则匿名客户机可以访问共享资源列表。默认情况下禁用此选项。
- **SMB Signing Enabled（启用 SMB 签名）**－此选项可使用 SMB 签名功能启用与 SMB 客户机的互操作性。如果启用了此选项，则已签名的包将对签名进行验证。如果禁用了此选项，则不验证签名就接受未签名的包。默认情况下禁用此选项。
- **SMB Signing Required（需要 SMB 签名）**－需要 SMB 签名时可使用此选项。启用此选项时，必须对所有 SMB 包进行签名，否则会将其拒绝。不支持 SMB 签名的客户机将无法连接到服务器。默认情况下，此选项处于关闭状态。
- **Enable Access-based Enumeration（启用基于访问的枚举）**－设置此选项可根据客户机的凭证过滤目录条目。如果客户机无权访问某个文件或目录，则返回到客户机的条目列表中将忽略该文件或目录。默认情况下禁用此选项。

Active Directory 域模式验证

在域模式下，用户在 Microsoft Active Directory (AD) 中进行定义。SMB 客户机可以使用 Kerberos 或 NTLM 验证连接到 Oracle ZFS Storage Appliance。

用户通过全限定的 Oracle ZFS Storage Appliance 主机名进行连接时，同一域或可信域中的 Windows 客户机将使用 Kerberos 验证；否则，它们将使用 NTLM 验证。

当 SMB 客户机使用 NTLM 验证连接到设备时，用户的凭证将转发到 AD 域控制器以进行验证。这称为传递验证。

如果定义了限制 NTLM 验证的 Windows 安全策略，则 Windows 客户机必须通过全限定主机名连接到设备。有关更多信息，请参见以下 Microsoft 开发者网络文章：

`http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx`

验证后，即为用户的 SMB 会话建立“安全上下文”。由安全上下文表示的用户具有唯一的安全描述符 (Security Descriptor, SID)。SID 表示文件所有权，用于确定文件访问权限。

工作组模式验证

在工作组模式下，用户在 Oracle ZFS Storage Appliance 本地进行定义。 当某个 SMB 客户机连接到处于工作组模式的设备时，会在本地使用该用户的用户名和密码散列来验证用户。

LAN Manager (LM) 兼容性级别用于指定当设备处于工作组模式时所用的验证协议。

以下列表显示了每个 LM 兼容性级别的 Oracle ZFS Storage Appliance 行为：

- 级别 2：接受 LM、NTLM 和 NTLMv2 验证
- 级别 3：接受 LM、NTLM 和 NTLMv2 验证
- 级别 4：接受 NTLM 和 NTLMv2 验证
- 级别 5：仅接受 NTLMv2 验证

成功验证了工作组用户之后，就会建立安全语境。使用计算机的 SID 与用户的 UID 的组合为在设备上定义的用户创建一个唯一的 SID。所有本地用户都定义为 UNIX 用户。

本地组和特权

本地组是域用户组，可为这些用户提供附加特权。管理员可以绕过文件权限来更改文件的所有权。备份操作员可以绕过文件访问控制来备份和恢复文件。

通过 Microsoft 管理控制台执行的管理操作

为确保只有适当的用户有权执行管理操作，对于使用 Microsoft 管理管制台 (Microsoft Management Console, MMC) 远程执行的操作施加了一些访问限制。

以下列表显示了用户及其允许的操作：

- **一般用户**－列出共享资源。
- **Administrators 组成员**－列出打开的和关闭的文件，断开用户连接，以及查看服务和事件日志。Administrators 组成员还可以设置和修改共享资源级 ACL。

病毒扫描

病毒扫描服务在文件系统级别扫描病毒。通过任何协议访问文件时，病毒扫描服务都会先扫描文件，如果发现病毒，就会拒绝访问并隔离文件。扫描由 Oracle ZFS Storage Appliance 联系的外部引擎执行。外部引擎未包括在设备软件中。

使用最新的病毒定义扫描了文件之后，在下次修改之前不会再扫描该文件。主要为可能感染病毒的 SMB 客户机提供病毒扫描。NFS 客户机也可以使用病毒扫描，但由于 NFS 协议的工作方式的原因，病毒检测的速度可能不如 SMB 客户机快。

应对计时攻击的延迟引擎

SMB 不实施延时引擎来防止计时攻击。它依赖于 Oracle Solaris 加密框架。

线上数据加密

SMB 服务使用 SMB 协议的第 1 版；该版本不支持线上数据加密。

FTP 数据服务

FTP 允许从 FTP 客户机访问文件系统。FTP 服务不允许其名登录，用户必须通过配置的名称服务进行验证。

FTP 支持以下安全设置。这些设置在启用了 FTP 协议访问的所有文件系统间共享：

- **Enable SSL/TLS（启用 SSL/TLS）**－允许 SSL/TLS 加密的 FTP 连接，并确保将 FTP 事务加密。默认情况下，此选项处于禁用状态。FTP 服务器使用自签名安全证书或客户提供的证书。
- **Permit Root login（允许 Root 用户登录）**－允许 root 用户进行 FTP 登录。默认情况下，此选项处于禁用状态，因为 FTP 验证使用的是纯文本，会带来网络嗅探攻击的安全风险。
- **Maximum # of allowable login attempts（允许的最大登录尝试次数）**－FTP 连接断开之前的失败登录尝试次数；此后用户必须重新连接才能再次尝试。默认值为 3。
- **Logging level（登录级别）**－日志的详细级别。

FTP 支持以下日志：

- **proftpd**－FTP 事件，包括成功登录和不成功的登录尝试
- **proftpd_xfer**－文件传输日志
- **proftpd_tls**－与 SSL/TLS 加密相关的 FTP 事件

HTTP 数据服务

通过 HTTP，可以使用 HTTP 和 HTTPS 协议以及 HTTP 扩展 Web 分布式创作和版本控制 (Web based Distributed Authoring and Versioning, WebDAV) 访问文件系统。这样一来，客户机便可通过 Web 浏览器访问共享文件系统；如果客户机软件支持，还可将其当作本地文件系统进行访问。

HTTPS 服务器使用自签名安全证书或客户提供的证书。要获得客户提供的证书，必须生成证书签名请求 (Certificate Signing Request, CSR) 并将该请求发送给证书颁发机构 (Certificate Authority, CA) 进行签名。签名的证书从 CA 返回后，可以在设备上安装该证书。如果证书是由非根 CA 签名的，您还必须从第二以及更高级别 CA 获得证书。有关证书管理的更多信息，请参阅《*Oracle ZFS Storage Appliance* 管理指南》。

可使用以下属性:

- **Require client login（需要客户机登录）**－客户机必须先进行验证才能访问共享资源，客户机对其创建的文件具有所有权。如果不设置此属性，则创建的文件将由 HTTP 服务用户 "nobody" 拥有。
- **Protocols（协议）**－选择支持 HTTP 和/或 HTTPS 的访问方法。
- **Port (for incoming connections)（端口（用于传入连接））**－HTTP 端口，默认端口为 80。
- **HTTPS Port (for incoming secure connections)（HTTPS 端口（用于传入的安全连接））**－ HTTP 端口，默认端口为 443。

如果启用了 "Require Client Login"（需要客户机登录），则 Oracle ZFS Storage Appliance 将拒绝访问不提供本地用户、NIS 用户或 LDAP 用户的有效验证凭证的客户机。不支持 Active Directory 验证。仅支持基本的 HTTP 验证。除非使用的是 HTTPS，否则将传输未加密的用户名和密码，这可能并不适合所有环境。如果禁用了 "Require Client Login"（需要客户机登录），则设备不会尝试验证凭据。

不管是否进行验证，都不会屏蔽已创建文件和目录的任何权限。新创建的文件允许所有人读取和写入。新创建的目录允许所有人读取、写入和执行。

NDMP 数据服务

通过网络数据管理协议 (Network Data Management Protocol, NDMP) 服务，Oracle ZFS Storage Appliance 可以参与由远程 NDMP 客户机（称为数据管理应用程序 (Data Management Application, DMA)）控制的基于 NDMP 的备份和恢复操作。通过使用 NDMP，可将设备用户数据（例如，存储在设备上管理员创建的共享资源中的数据）备份和恢复到本地连接的设备（例如，磁带设备）和远程系统。此外，还可以通过 DMA 备份和恢复本地连接的设备。

远程复制数据服务

Oracle ZFS Storage Appliance 远程复制为项目和共享资源的复制提供了便利。利用此服务，可以查看哪些设备将数据复制到了特定的设备，并可控制某个特定设备可以复制到哪些设备。

启用此服务时，设备将从其他设备接收复制更新以及发送本地项目和共享资源的复制更新（根据为其配置的操作）。禁用此服务时，传入的复制更新将会失败，且不会复制任何本地项目和共享资源。

配置设备的远程复制目标时，需要远程设备的 root 用户密码。这些目标用于设置实现设备通信的复制对等连接。

在目标创建期间，将使用 root 用户密码来确认请求的真实性，并生成和交换将用于在后续通信中标识设备的安全密钥。

生成的密钥将作为设备配置的内容永久存储。root 用户密码在任何时候都不会永久存储，也不会以未加密的方式传输。所有设备通信（包括此初始身份交换）都使用 SSL 进行保护。

在通过具有有限带宽的网络复制大的数据集时，Oracle ZFS Storage Appliance 脱机复制功能可以减少时间、资源以及可能的数据错误。脱机复制将复制流导出到 NFS 服务器上的文件，该文件能够以物理方式移至远程目标站点，或者可以选择性复制到外部介质以进行交付。在目标站点处，管理员将包含复制流的文件导入到目标设备。

要限制对导出的复制流的访问，请仅向源和目标设备的 IP 地址公开 NFS 共享资源。要加密数据，请在 NFS 服务器上为 NFS 共享资源启用磁盘上加密。有关更多信息，请参阅 NFS 服务器文档。请注意，设备永远不会加密导出的复制流。

使用数据加密

许可声明：可以免费试用加密功能，但若要在生产环境中使用，必须为该功能购买单独的许可证。在 *Oracle ZFS Storage ZS5-4*、*Oracle ZFS Storage ZS5-2*、*Oracle ZFS Storage ZS4-4* 和 *Oracle ZFS Storage ZS3-4* 上，必须获取许可证才能使用加密功能。在试用期后，必须为该功能获取许可证或将其停用。*Oracle* 保留随时审计许可合规性的权利。有关详细信息，请参阅 *"Oracle Software License Agreement ("SLA") and Entitlement for Hardware Systems with Integrated Software Options"*。

Oracle ZFS Storage Appliance 为单个共享资源（文件系统和 LUN）以及在项目内部创建的共享资源提供透明数据加密。

管理加密密钥

该设备包括一个内置的 LOCAL（本地）密钥库，并可连接到 Oracle Key Manager (OKM) 系统。每个加密的项目或共享资源都需要一个来自 LOCAL（本地）或 OKM 密钥库的包装密钥。数据加密密钥由存储设备管理，并使用 LOCAL（本地）或 OKM 密钥库提供的包装密钥永久加密存储。

OKM 是综合密钥管理系统 (key management system, KMS)，可满足企业快速发展的、对基于存储的数据加密的需求。此功能的开发融合了多种开放标准，为集中管理分布在各地的异构存储基础结构上的加密密钥提供了相应的容量、可伸缩性和互操作性。

OKM 可应对存储密钥管理的独特挑战，包括：

- **密钥长期保留**－OKM 确保归档数据始终可用，它可在整个数据生命周期内安全保留加密密钥。
- **互操作性**－OKM 提供了支持在单一存储密钥管理系统下连接到大型机或开放系统的各种存储设备所需的互操作性。

- **高可用性**－借助主动的 N 节点群集、动态负载平衡和自动故障转移，OKM 提供了高可用性，而不管设备是位于一个站点中还是分布在世界各地。
- **大容量**－OKM 可以管理大量的存储设备以及更多的存储密钥。单个群集的设备对可以为数千个存储设备和以百万计的存储密钥提供密钥管理服务。
- **灵活的密钥配置**－对于每个 OKM 群集，可以自动生成密钥，也可以为某个 LOCAL（本地）或 OKM 密钥库单独创建密钥。安全管理员负责提供密钥名称；密钥名称与密钥库组合可以将指定的包装密钥与某个项目或共享资源关联。

维护密钥

使用处于未激活状态的 OKM 密钥的共享资源和项目仍可访问。要阻止使用 OKM 密钥，OKM 管理员必须显式删除密钥。

要确保加密的共享资源和项目可访问，请备份设备配置和 LOCAL（本地）密钥库密钥值。如果密钥变得不可用，则使用该密钥的所有共享资源或项目将变得不可访问。如果某个项目的密钥不可用，则无法在该项目中创建新共享资源。

在以下情况下，密钥可能会变得不可用：

- 删除密钥
- 回滚到不支持加密的版本
- 回滚到未配置密钥的版本
- 恢复出厂设置
- OKM 服务器不可用

加密密钥生命周期

加密密钥生命周期很灵活，因为可以随时在不将数据服务脱机的情况下更改密钥。

从密钥库中删除一个密钥时，所有使用它的共享资源都将卸载，其数据将变得不可访问。应使用 OKM 备份服务来执行对 OKM 密钥库中密钥的备份。LOCAL（本地）密钥库中密钥的备份包括在系统配置备份中。对于 LOCAL（本地）密钥库，还可以在创建时按值提供密钥，以允许将其托管在外部系统中，这可以提供备用的按密钥进行备份/恢复功能。

影子迁移数据服务

影子迁移允许从外部或内部来源自动迁移数据并控制自动的后台迁移。无论是否启用了该服务，都将以同步方式为带内请求迁移数据。该服务的主要用途是允许调整专用于后台迁移的线程数。

NFS 源上的 NFS 挂载不受 Oracle ZFS Storage Appliance 用户控制。因此无法对影子迁移挂载施加安全保护；如果服务器预计有 Kerberos 或类似的请求，则源挂载会被拒绝。

SFTP 数据服务

SSH 文件传输协议 (SSH File Transfer Protocol, SFTP) 支持从 SFTP 客户机访问文件系统。不允许匿名登录，因此，用户必须使用所配置的名称服务进行验证。

在创建 SFTP 密钥时，必须包括具有有效用户分配的 user 属性。SFTP 密钥按用户分组，并通过 SFTP 和用户的名称进行验证。

注 - 出于安全原因，您应当重新创建不包括 user 属性的现有 SFTP 密钥，尽管这些密钥仍将进行验证。

TFTP 数据服务

普通文件传输协议 (Trivial File Transfer Protocol, TFTP) 是一种传输文件的简单协议。它设计小巧且易于实施，但缺乏 FTP 的大多数安全功能。TFTP 仅从远程服务器读取/向其写入文件。它不能列出目录，目前没有针对用户验证的设置。

存储区域网络

在存储区域网络 (Storage Area Network, SAN) 中，目标组和启动器组定义可以与逻辑单元号 (Logical Unit Number, LUN) 关联的目标和启动器集。与某个目标组关联的 LUN 只能通过该组中的目标进行访问。与某个启动器组关联的 LUN 只能通过该组中的启动器进行访问。在创建 LUN 时，您将向 LUN 应用启动器组和目标组。必须定义至少一个目标组和一个启动器组，LUN 创建才能成功完成。

除了质询握手验证协议 (Challenge-Handshake Authentication Protocol, CHAP) 验证（只能为 iSCSI/iSER 启动器访问选择该验证机制）之外，不会执行其他验证。

注 - 使用默认启动器组可能导致不需要的或冲突的 LUN 启动器。

目录服务

本节介绍了可在设备上配置的目录服务及其对安全性的影响。

网络信息服务

网络信息服务 (Network Information Service, NIS) 是一种用于目录集中管理的名称服务。Oracle ZFS Storage Appliance 可以用作用户和组的 NIS 客户机，从而使 NIS 用户可以登录 FTP 和 HTTP/WebDAV。还可向 NIS 用户授予设备管理特权。设备使用自己的特权设置补充 NIS 信息。

轻量目录访问协议

Oracle ZFS Storage Appliance 使用轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP) 来验证管理用户以及某些数据服务用户（FTP、HTTP）。设备支持 LDAP-over-SSL 安全性。LDAP 用来检索关于用户和组的信息并通过以下方式使用：

- 提供用于接受和显示用户和组的名称的用户界面。
- 对于使用名称的数据协议（如 NFSv4），将名称映射到用户和组以及从用户和组映射名称。
- 定义供在访问控制中使用的组成员资格。
- （可选）传输用于管理和数据访问验证的验证数据。

LDAP 连接可以用作验证机制。例如，当用户尝试向 Oracle ZFS Storage Appliance 验证身份时，该设备可以尝试作为该用户向 LDAP 服务器验证身份（用作确认验证的一种机制）。

对于 LDAP 连接安全性，存在各种各样的控制：

- 设备到服务器的验证：
  - 设备是匿名的
  - 设备使用用户的 Kerberos 凭证进行验证
  - 设备使用指定的“代理”用户和密码进行验证
- 服务器到设备的验证（确保已连接了正确的服务器）：
  - 不安全
  - 使用 Kerberos 对服务器进行验证
  - 使用 TLS 证书对服务器进行验证

如果使用了 Kerberos 或 TLS，则通过 LDAP 连接传输的数据是加密的，但其他情况下不是加密的。使用 TLS 时，配置时的第一个连接不是安全的。此时会收集服务器的证书并使用它来验证以后的生产连接。

无法导入要用来验证多个 LDAP 服务器的证书颁发机构证书，也不能手动导入特定 LDAP 服务器的证书。

只支持原始 TLS (LDAPS)。不支持 STARTTLS 连接，此类连接在不安全的 LDAP 连接上启动，然后转移到安全连接。不支持需要客户机证书的 LDAP 服务器。

身份映射

客户机可以使用 SMB 或 NFS 访问 Oracle ZFS Storage Appliance 上的文件资源；每个客户机都有一个唯一的用户标识符。SMB/Windows 用户具有安全描述符 (Security Descriptor, SID)，UNIX/Linux 用户具有用户 ID (User ID, UID)。用户还可以是组的成员，这些组由组 SID 标识（对于 Windows 用户）或者由组 ID (Group ID, GID) 标识（对于 UNIX/Linux 用户）。

在同时使用这两种协议访问文件资源的环境中，通常最好建立身份对等关系，例如某个 UNIX 用户等效于某个 Active Directory 用户。这对于确定该设备上文件资源的访问权限非常重要。

有多种不同类型的身份映射，这涉及 Active Directory、LDAP 和 NIS 等目录服务。对于要使用的目录服务，应当小心遵循安全最佳做法。

UNIX 标识管理

Microsoft 提供了一项称为“UNIX 标识管理”(Identity Management for UNIX, IDMU) 的功能。此软件适用于 Windows Server 2003，且已与 Windows Server 2003 R2 和更高版本捆绑。此功能是之前称为 "Services for UNIX" 的功能的一部分（采用非捆绑形式）。

IDMU 的主要用途是支持将 Windows 作为 NIS/NFS 服务器。IDMU 允许管理员指定一组与 UNIX 相关的参数：UID、GID、登录 shell、起始目录，对于组也有类似的参数。这些参数是使用 AD 通过类似 RFC 2307（但不完全相同）的模式以及 NIS 服务提供的。

使用 IDMU 映射模式时，身份映射服务将使用这些 UNIX 属性在 Windows 身份与 UNIX 身份之间建立映射关系。此方法与基于目录的映射非常相似，但是身份映射服务会查询 IDMU 软件建立的属性模式，而不是允许使用定制模式。使用此方法时，无法使用任何其他基于目录的映射。

基于目录的映射

基于目录的映射涉及为 LDAP 或 Active Directory 对象加注有关如何将身份映射到对应平台上的对等身份的信息。必须配置这些与对象关联的额外属性。

基于名称的映射

基于名称的映射涉及创建各种按名称映射身份的规则。这些规则在 Windows 身份与 UNIX 身份之间建立对等关系。

临时映射

如果没有适用于特定用户的基于名称的映射规则，系统将通过临时映射为该用户提供临时凭证，除非这些临时凭证被拒绝映射阻止。当拥有临时 UNIX 名称的 Windows 用户在系统上创建一个文件时，使用 SMB 访问该文件的 Windows 客户机将认为该文件归该 Windows 身份所有。但是，NFS 客户机将认为该文件归 "nobody" 所有。

系统设置

以下各节描述了可用的系统安全设置。

回拨

回拨服务用于管理 Oracle ZFS Storage Appliance 注册以及回拨远程支持服务。这些消息中不传输任何用户数据或元数据。

注册将 Oracle ZFS Storage Appliance 与 Oracle 的清单门户相连接；可以通过该门户管理 Oracle 设备。注册是使用回拨服务的先决条件。

回拨服务与 Oracle 支持进行通信来提供：

- **故障报告**－系统向 Oracle 报告现存问题以获得自动服务响应。根据故障的性质，可以打开支持案例。
- **心跳**－向 Oracle 发送每日心跳消息来指示系统是否启动并且正在运行。当一个已激活系统很长时间无法发送心跳时，Oracle 支持可能会通知帐户的技术联系人。
- **系统配置**－向 Oracle 发送定期消息，描述当前软件和硬件版本和配置以及存储配置。

服务标签

使用服务标签可以查询 Oracle ZFS Storage Appliance 获取如下数据，从而为产品清单和支持提供便利：

- 系统序列号
- 系统类型
- 软件版本号

可以在 Oracle 支持中注册服务标签，从而轻松跟踪您的 Oracle 设备，以及可以加速服务调用。默认情况下，启用服务标签。

简单邮件传输协议

简单邮件传输协议 (Simple Mail Transfer Protocol, SMTP) 发送 Oracle ZFS Storage Appliance 生成的所有邮件，通常是为了响应配置的警报。SMTP 不接受外部邮件；它仅发送由该设备自身自动生成的邮件。

默认情况下，SMTP 服务使用 DNS（MX 记录）确定邮件发送到的位置。如果没有为该设备的域配置 DNS，或者外发邮件的目标域未正确设置 DNS MX 记录，可以将该设备配置为通过外发邮件服务器转发所有邮件。

简单网络管理协议

简单网络管理协议 (Simple Network Management Protocol, SNMP) 在 Oracle ZFS Storage Appliance 上提供两个功能：SNMP 可以处理设备状态信息，可以配置警报来发送 SNMP 陷阱。启用此服务时可以使用 SNMP 版本 v1、v2c 和 v3。设备最多支持 128 个物理和逻辑网络接口。

Syslog 消息

syslog 消息是从 Oracle ZFS Storage Appliance 传输到一个或多个远程系统的小事件消息。Syslog 提供了两种设备功能：

- 可以配置警报来向一个或多个远程系统发送 syslog 消息。
- 设备上支持 syslog 的服务会将其 syslog 消息转发到远程系统。

syslog 可以配置为使用 RFC 3164 描述的经典输出格式，或者是 RFC 5424 描述的更新的版本化输出格式。Syslog 消息作为 UDP 数据报传输。因此，它们可能会被网络丢弃，或者如果发送系统内存不足或网络非常拥塞，则可能根本不发送这些消息。因此，管理员应该认为在网络中发生复杂故障的情况下，一些消息可能已缺失或已被丢弃。

消息包含以下元素：

- 设备，描述发出消息的系统组件的类型
- 严重性，描述与消息关联的状况的严重程度
- 时间戳，描述关联事件的时间（以 UTC 时间表示）
- 主机名，描述设备的规范名称
- 标签，描述发出消息的系统组件的名称
- 消息，描述事件本身

系统标识

此服务提供系统名称和位置的配置。如果将 Oracle ZFS Storage Appliance 移到不同的网络位置或者改变用途，则可能需要更改系统名称和位置。

磁盘清理

应当定期执行磁盘清理，以便 Oracle ZFS Storage Appliance 检测并更正磁盘上损坏的数据。磁盘清理是一个后台进程，它在空闲期间读取磁盘来检测不常访问的扇区中无法纠正的读取错误。及时检测到这类潜在扇区错误对于减少数据丢失非常重要。

防止销毁

当启用了防止销毁功能时，无法销毁共享资源或项目。这包括通过从属克隆销毁共享资源，销毁项目内的共享资源或销毁复制数据包。不过，这不会影响通过复制更新销毁的共享资源。如果销毁了 Oracle ZFS Storage Appliance 中某个作为复制源的共享资源，即使设置了此属性，目标设备上的对应共享资源也将被销毁。

要销毁共享资源，首先必须要做的是显式禁用此属性。默认情况下，此属性处于禁用状态。

安全日志

本节描述了与安全相关的日志记录功能。

审计日志

审计日志记录了用户活动事件（包括登录和注销 BUI 和 CLI）和管理操作。下表显示了 BUI 中可能会显示的审计日志条目示例：

表 2 审计日志记录

时间	用户	主机	摘要	会话注释
2013-10-12 05:20:24	root	galaxy	Disabled ftp service	
2013-10-12 03:17:05	root	galaxy	User logged in	
2013-10-11 22:38:56	root	galaxy	Browser session timed out	

时间	用户	主机	摘要	会话注释
2013-10-11 21:13:35	root	<console>	Enabled ftp service	

回拨日志

如果使用了回拨，则此日志将显示与 Oracle 技术系统之间的通信事件。下面是 BUI 中可能会显示的回拨条目示例：

表 3 回拨日志记录

时间	说明	结果
2013-10-12 05:24:09	Uploaded file 'cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz' to Oracle support	OK（正常）

更多信息

您可以在以下位置查找 Oracle ZFS Storage Appliance 的完整产品信息：

https://docs.oracle.com

使用 BUI 配置 Oracle ZFS Storage Appliance 时，您可以在任何屏幕中单击右上方的 "Help"（帮助）链接来显示针对该屏幕的帮助信息。