Oracle® ZFS Storage Appliance 安全指南

ORACLE®

Oracle ZFS Storage Appliance 安全概述

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。

还可以将本指南用作参考资料，查找关于 Oracle ZFS Storage Appliance (ZFSSA) 的各项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 System 管理指南》。

以下各节介绍了 ZFSSA 安全功能：

- **初始安装** – 介绍如何设置管理访问权限，如何建立 root 帐户，以及重置 ZFSSA 出厂设置的影响。
- **物理安全** – 介绍 ZFSSA 的物理安全环境。
- **管理模型** – 介绍如何限制对 CLI 和 BUI 的访问、系统修补模型、延迟更新、支持包和配置备份。
- **ZFSSA 用户** – 介绍管理角色（可以管理 ZFSSA 的人）以及管理用户授权。
- **访问控制列表 (Access Control List, ACL)** – 介绍允许或拒绝访问文件和目录的机制。
- **存储区网络 (Storage Area Network, SAN)** – 介绍逻辑单元号 (logical unit number, LUN) 和关联的启动器组，以及启动器授权选项和默认值。
- **数据服务** – 介绍 ZFSSA 支持的数据服务以及各种数据服务提供的安全性。
- **目录服务** – 介绍可以在 ZFSSA 上配置的目录服务及其安全影响。
- **系统设置** – 介绍系统设置；回拨、服务标记、SMTP、SNMP、系统日志、系统标识、磁盘清理和防止销毁。
- **远程管理访问** – 介绍通过 BUI 和 CLI 的远程访问。
- **日志** – 介绍与安全性相关的日志类型。

初始安装

ZFSSA 提供给客户时预安装了 ZFSSA 软件。不需要执行软件安装并且没有提供介质。

初始安装是以默认帐户名和密码完成的，在安装后必须更改默认的 root 用户密码。如果 ZFSSA 重置为出厂默认值，则对于 ZFSSA 和服务处理器，root 用户密码也将重置为默认值。

在初始安装 ZFSSA 期间，有一个与系统的服务处理器关联的默认帐户名和密码。管理员可以使用此默认帐户对 ZFSSA 执行首次访问，在首次访问时会要求管理员执行系统的初始安装步骤。必须执行的步骤之一是设置新的 ZFSSA 管理密码，然后该密码也将默认服务处理器密码重设为相同的值。

物理安全

要控制对系统的访问，必须维护计算环境的物理安全性。例如，处于已登录状态且无人值守的系统容易受到未经授权的访问。必须为计算机环境和计算机硬件提供物理保护，始终防止其受到未经授权的访问。

ZFSSA 仅供受限访问，通过使用安全手段（例如，密钥、锁、工具以及识别卡访问）对访问进行控制，并且授权访问的人员已获悉限制访问的原因以及需要采取的防范措施。

管理模型

本节描述了 ZFSSA 管理模型的安全性。

受限访问（CLI 和 BUI）

对浏览器用户界面 (Browser User Interface, BUI) 和命令行界面 (Command Line Interface, CLI) 的管理访问仅限于 root 用户、定义有相关权限的本地管理员，以及那些通过身份服务器（例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)）获得了授权的用户。

管理是通过安全套接字层 (secure sockets layer, SSL) 命令行登录或 HTTP 安全 (HTTP secure, HTTPS) 浏览器会话进行的。HTTPS 会话由初始安装期间为每个 ZFSSA 生成的唯一自签名证书进行加密。HTTPS 会话的默认会话超时值为 15 分钟，但用户可以定义该值。

系统更新

将通过替换系统软件的整个二进制文件形式应用系统更新。在更新之前，将创建正在运行的系统池的快照。这样管理员在需要时可以回滚到以前的版本。

延迟更新

延迟更新是系统更新中的一项或一部分功能，它在执行系统更新时未激活。管理员可决定何时或是否应用延迟更新。在系统更新期间未应用的更新在后续的系统更新期间将仍然可用。无法选择单个更新进行应用，当选择应用延迟更新时，只能应用所有更新或者一个更新都不应用。在应用更新后，无法回滚到以前的系统软件版本。

支持包

如果系统注册了“回拨”支持，当系统遇到重大故障时，系统状态将被发送到 My Oracle Support，然后工程支持人员可以对其进行检查并且可以创建支持包。发送到 My Oracle Support 的系统状态信息不包含用户数据；只会发送配置信息。

配置备份

可以将系统配置保存在本地供以后恢复使用。这些备份不包含用户数据；只会保存配置设置。

ZFSSA 用户

有两种类型的 ZFSSA 用户：

- **数据服务用户** – 使用受支持的协议（例如 NFS、SMB、光纤通道、iSCSI、http 和 FTP）访问文件和块资源的客户。
- **管理用户** – 将对 ZFSSA 上的配置和服务进行管理的用户。本节仅适用于管理用户。

管理用户角色

可以通过为管理员分配定制角色来向其授予权限。角色是可以分配给管理员的权限的集合。您可能希望创建具有不同授权级别的多种管理员和操作员角色。应当为员工分配适合其需求的角色，而不是为其分配不必要的权限。

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。角色限定用户只具有所定义的授权集。此外，在审计日志中，用户角色还可以跟踪到各个用户名。默认情况下，存在一个称作 "Basic administration" 的角色，它包含最少的授权。

管理用户可以是：

- 本地用户 – 所有帐户信息都保存在 ZFSSA 上。
- 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 ZFSSA 上。这允许现有 NIS/LDAP 用户登录并管理 ZFSSA，但是默认情况下，现有 NIS/LDAP 用户无法登录到 ZFSSA。必须显式授予对 ZFSSA 的访问权限。

管理范围

通过授权，用户可以执行特定任务，例如，创建共享资源、重新引导 ZFSSA 以及更新系统软件。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，可使用过滤器使某项授权只能重新启动 HTTP 服务，而不是重新启动所有服务。

访问控制列表 (Access Control List, ACL)

ZFSSA 通过访问控制列表 (Access Control List, ACL) 提供文件访问控制。访问控制列表是用于允许或拒绝访问特定目录或文件的一种机制。

ZFSSA 提供的 ACL 模型基于 NFSv4 ACL 模型，后者是从 Windows ACL 语义派生的。它是一个丰富的 ACL 模型，可对文件和目录提供细粒度的访问权限。ZFSSA 存储内的每个文件和目录都有一个 ACL，并且针对 SMB 和 NFS 的访问控制决策都将通过相同的算法来确定允许或拒绝谁访问文件和目录。

一个 ACL 由一个或多个 ACE（Access Control Entry，访问控制条目）组成。每个 ACE 都包含 ACE 授予或拒绝的权限的一个条目，以及 ACE 应用于的用户和所使用的继承级别标志。

ACL 继承

NFSv4 ACL 允许新创建的文件和目录继承各个 ACE。ACE 继承由多个继承级别标志进行控制，这些标志是管理员在初始设置 ACL 时在其上设置的。

确定 ACL 访问权限

NFSv4 ACL 考虑顺序，按照从上到下的顺序进行处理。授予某个权限后，后续的 ACE 无法将其剥夺。拒绝某个权限后，后续 ACE 无法授予该权限。

SMB 共享资源级 ACL

SMB 共享资源级 ACL 是与共享资源中的文件或目录 ACL 结合使用的 ACL，用于确定文件的有效权限。共享资源级 ACL 在文件 ACL 之上提供了另一层访问控制，可实现更复杂的访问控制配置。

共享资源级 ACL 是使用 SMB 协议导出文件系统时设置的。如果文件系统不是使用 SMB 协议导出的，则设置共享资源级 ACL 没有效果。默认情况下，共享资源级 ACL 向所有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 语义并且优先于 ZFS 属性。不同之处是 NFS 利用 POSIX 语义，而 SMB 客户机不是。这些属性大部分与 POSIX 兼容。

存储区域网络 (Storage Area Network, SAN)

在 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。

注意：使用默认启动器组可能会导致 LUN 暴露给不需要的或者冲突的启动器。

数据服务

表 1　　数据服务

服务	说明	使用的端口
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
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
NDMP	NDMP 主机服务	10000
远程复制	远程复制	216
影子迁移	影子数据迁移	
SFTP	通过 SFTP 协议的文件系统访问	218
SRP	通过 SRP 协议的块访问	
TFTP	通过 TFTP 协议的文件系统访问	
病毒扫描	文件系统病毒扫描	

所需的最少端口数：

要提供网络安全，您可以创建防火墙。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)

使用了 http 文件共享（通常不使用）时需要的其他传入端口

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

传出端口

- tcp/80 (WEB)

注意：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 还必须是开放的。

NFS 验证和加密选项

默认情况下，NFS 共享资源使用 AUTH_SYS RPC 验证分配。也可以将其配置为使用 Kerberos 安全性进行共享。使用 AUTH_SYS 验证时，客户机的 UNIX uid 和 gid 由 NFS 服务器通过网络传递且不进行验证。任何对客户机具有 root 访问权限的人很容易突破此验证机制，因此最好使用其他可用的安全模式。

可以按共享资源指定附加的访问控制，以允许或禁止特定的主机、DNS 域或网络访问共享资源。

安全模式

安全模式按共享资源设置。下面的列表描述了可用的 Kerberos 安全设置。

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

还可以在安全模式设置中指定 Kerberos 类型的组合。组合安全模式允许客户机使用所列出的任一种 Kerberos 类型进行挂载。

Kerberos 类型

- sys – 系统验证
- krb5 – 仅 Kerberos v5，客户机必须使用此类型进行挂载。
- krb5:krb5i – Kerberos v5 或加完整性保护，客户机可以使用所列出的任一种类型进行挂载。
- krb5i – 仅 Kerberos v5 加完整性保护，客户机必须使用此类型进行挂载。
- krb5:krb5i:krb5p – Kerberos v5、加完整性保护或加隐私保护，客户机可以使用所列出的任一种类型进行挂载。
- krb5p – 仅 Kerberos v5 加隐私保护，客户机必须使用此类型进行挂载。

iSCSI

当在 ZFSSA 上配置 LUN 时，您可以通过 Internet 小型计算机系统接口 (Internet Small Computer System Interface, iSCSI) 目标导出该卷。iSCSI 服务允许 iSCSI 启动器使用 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 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，该服务还支持在 RADIUS 数据库中进行 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。

iSCSI 服务允许指定一个启动器全局列表，其中包含可以在启动器组内使用的启动器。当使用 iSCSI 和 CHAP 验证时，可以使用 RADIUS 作为 iSCSI 协议，用于将所有 CHAP 验证推迟到选定的 RADIUS 服务器。

RADIUS 支持

远程验证拨入用户服务 (Remote Authentication Dial-In User Service, RADIUS) 是一个使用中央服务器代表存储节点执行 CHAP 验证的系统。当使用 iSCSI 和 CHAP 验证时，可以选择 RADIUS 作为 iSCSI 协议（同时应用于 iSCSI 和 iSCSI 的 RDMA 扩展 (iSER)），并将所有 CHAP 验证发送到选定的 RADIUS 服务器。

要使 ZFSSA 能够使用 RADIUS 执行 CHAP 验证，必须满足以下要求：

- ZFSSA 必须指定 RADIUS 服务器的地址，以及与该 RADIUS 服务器进行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）给出 ZFSSA 的地址并指定上述密钥。
- 对于每个启动器，RADIUS 服务器必须有一个条目（例如在其用户文件中）提供 CHAP 名称以及匹配的 CHAP 密钥。
- 如果启动器使用其 IQN 名称作为 CHAP 名称（这是建议的配置），ZFSSA 无需为每个启动器计算机包含一个单独的启动器条目，RADIUS 服务器就可执行所有验证步骤。
- 如果启动器使用单独的 CHAP 名称，则 ZFSSA 必须有一个启动器条目对应于该启动器，指定从 IQN 名称到 CHAP 名称的映射。该启动器条目无需指定启动器的 CHAP 密钥。

服务器消息块 (Server Message Block, SMB)

SMB 协议也称为通用 Internet 文件系统 (Common Internet File System, CIFS) 协议，主要用于为 Microsoft Windows 网络上的文件提供共享访问。它还提供验证功能。

下面的 SMB 选项具有安全影响：

- Restrict Anonymous Access to share list – 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。默认情况下此选项处于禁用状态。
- SMB Signing Enabled – 此选项对 SMB 客户机互操作启用 SMB 签名功能。如果启用了此选项，将对签名的包的签名进行验证。如果禁用了此选项，将接受未签名的包且不会对签名进行验证。默认情况下此选项处于禁用状态。
- SMB Signing Required – 当需要 SMB 签名时可以使用此选项。当启用了此选项时，所有 SMB 包都必须签名，否则它们将被拒绝。不支持 SMB 签名的客户机无法连接到服务器。默认情况下，此选项处于禁用状态。

- Enable Access-based Enumeration – 设置此选项将基于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省略该文件或目录。默认情况下此选项处于禁用状态。

Active Directory (AD) 域模式验证

在域模式中，用户是在 Active Directory 中定义的。SMB 客户机可以使用 Kerberos 或 NTLM 验证连接到 ZFSSA。

当用户通过完全限定的 ZFSSA 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 ZFSSA 时，用户的凭证将转发到 AD 域控制器进行验证。这称为直通式验证。

如果定义了限制 NTLM 验证的 Windows 安全策略，则 Windows 客户机必须通过完全限定的主机名连接到 ZFSSA。有关更多信息，请参见此 MSDN 文章：http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx。

在验证之后，将为用户的 SMB 会话建立一个“安全上下文”。以安全上下文表示的用户具有唯一的安全描述符 (Security Descriptor, SID)。SID 指示文件所有权并用来确定文件访问权限。

工作组模式验证

在工作组模式中，用户是在 ZFSSA 本地定义的。当 SMB 客户机连接到处于工作组模式的 ZFSSA 时，将使用该用户的用户名和密码散列在本地对该用户进行验证。

当 ZFSSA 处于工作组模式时，将使用 LAN Manager (LM) 兼容性级别指定用于验证的协议。

下面的列表显示了每个 LM 兼容性级别的 ZFSSA 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。

在成功验证工作组用户后，将建立安全上下文，并使用计算机 SID 和用户 UID 的组合为 ZFSSA 上定义的用户创建唯一的 SID。所有本地用户都定义为 UNIX 用户。

本地组和权限

本地组是向用户提供额外权限的域用户组。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 (Microsoft Management Console, MMC) 执行管理操作

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

下面的列表显示了不同用户以及允许其执行的操作：

- 一般用户 – 列出共享资源
- 管理员组的成员 – 列出打开的文件以及关闭文件、断开用户连接、查看服务和事件日志
- 管理员组的成员还可以设置/修改共享资源级 ACL

- 管理员组的成员 – 列出打开的文件以及关闭文件、断开用户连接、查看服务和事件日志

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 ZFSSA 连接的外部引擎执行。外部引擎未包括在 ZFSSA 软件中。

使用最新的病毒定义扫描了文件之后，在下次修改文件之前不会再扫描该文件。病毒扫描主要是为可能会引入病毒的 SMB 客户机提供的。NFS 客户机也可以使用病毒扫描，但是由于 NFS 协议的工作方式，此类客户机无法像 SMB 客户机那样快速检测到病毒。

针对时序攻击的延迟引擎

SMB 没有实施任何延迟引擎来防止时序攻击。它依赖于 Solaris 加密框架。

传输中数据的加密

SMB 服务使用 SMB 协议的版本 1，它不支持传输中数据的加密。

文件传输协议 (File Transfer Protocol, FTP)

FTP 允许从 FTP 客户机访问文件系统。FTP 服务不允许匿名登录，用户必须使用所配置的名称服务进行验证。

FTP 支持以下安全设置。对于启用了 FTP 协议访问的所有文件系统，这些设置是共享的：

- Enable SSL/TLS – 允许 SSL/TLS 加密的 FTP 连接并确保 FTP 事务进行加密。默认情况下，此选项处于禁用状态。
- Permit root login – 允许 root 用户进行 FTP 登录。默认情况下此设置被禁用，因为 FTP 验证使用纯文本形式，会带来网络嗅探攻击的安全风险。
- Maximum number of allowable login attempts – 登录失败的最大次数，此后 FTP 连接断开，用户必须重新连接才能再次尝试。默认值为 3。
- Logging level – 日志的详细程度。

FTP 支持以下日志：

- proftpd – 包括成功和不成功的登录尝试在内的 FTP 事件
- proftpd_xfer – 文件传输日志
- proftpd_tls – 与 SSL/TLS 加密相关的 FTP 事件

超文本传输协议 (Hypertext Transfer Protocol, HTTP)

通过 HTTP，可以使用 HTTP 和 HTTPS 协议以及 HTTP 扩展 WebDAV（Web based Distributed Authoring and Versioning，Web 分布式创作和版本控制）访问文件系统。这允许客户机通过 Web 浏览器访问共享的文件系统，或者将其作为本地文件系统进行访问（如果客户机软件支持此功能）。HTTPS 服务器使用自签名安全证书。

具有以下属性可用：

- Require client login – 客户机必须先进行验证才允许访问共享资源，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 – 选择要支持的访问方法：HTTP、HTTPS 或两者。
- HTTP Port（用于传入的连接）– HTTP 端口，默认值为端口 80。
- HTTPS Port（用于传入的安全连接）– HTTPS 端口，默认端口为 443。

如果启用了 "Require client login"，ZFSSA 将拒绝访问没有为本地用户、NIS 用户或 LDAP 用户提供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。此外，传输用户名和密码时都未加密（除非使用的是 HTTPS），这可能并不适合所有环境。如果禁用了 "Require Client Login"，则 ZFSSA 不会尝试进行验证。

不管是否进行验证，都不会对创建的文件和目录施加权限限制。任何人对新创建的文件都具有读取和写入权限。任何人对新创建的目录都具有读取、写入和执行权限。

网络数据管理协议 (Network Data Management Protocol, NDMP)

NDMP 允许 ZFSSA 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 ZFSSA 用户数据（例如存储在 ZFSSA 上由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（例如磁带机）和远程系统。还可以通过 DMA 备份和恢复本地连接的设备。

远程复制

ZFSSA 远程复制为项目和共享资源的复制提供了便利。此服务允许查看哪些 ZFSSA 将数据复制到此 ZFSSA 并配置此 ZFSSA 可以将数据复制到哪些 ZFSSA。

当启用了此服务时，ZFSSA 可从其他 ZFSSA 接收复制更新以及发送本地项目和共享资源的复制更新（根据其配置的操作）。当禁用了此服务时，传入的复制更新将失败，且不会复制任何本地项目和共享资源。

要为 ZFSSA 配置远程复制目标，需要有远程 ZFSSA 的 root 用户密码。这些目标用来设置支持 ZFSSA 通信的对等复制连接。

在创建目标期间，将使用 root 用户密码来确认请求真实性并生成和交换在后续通信中用来识别 ZFSSA 的安全密钥。

生成的密钥将永久性地存储为 ZFSSA 配置的一部分。root 用户密码从不会永久保存。root 用户密码从不会以明文形式传输。所有 ZFSSA 通信（包括此初始身份交换）都由 SSL 提供保护。

影子迁移

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。

对 NFS 源的 NFS 挂载不受 ZFSSA 用户的控制。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。

SSH 文件传输协议 (SSH File Transfer Protocol, SFTP)

SFTP 允许从 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。

注意：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。

简单文件传输协议 (Trivial File Transfer Protocol, TFTP)

TFTP 是一种用于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。

目录服务

网络信息服务 (Network Information Service, NIS)

NIS 是一种用于目录集中管理的名称服务。ZFSSA 可以充当用户和组的 NIS 客户机，以便 NIS 用户可以登录到 FTP 和 HTTP/WebDAV。还可以向 NIS 用户授予 ZFSSA 管理权限。ZFSSA 用自己的权限设置作为 NIS 信息的补充。

轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP)

ZFSSA 使用 LDAP 来验证管理用户以及某些数据服务用户（ftp、http）。ZFSSA 支持基于 SSL 的 LDAP 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（例如 NFSv4），在名称与用户和组之间建立映射关系。
- 定义用于访问控制的组成员关系。
- （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 ZFSSA 验证身份时，ZFSSA 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：
  - 设备作为匿名用户
  - 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）：
  1. 没有安全保护
  2. 使用 Kerberos 对服务器进行验证
  3. 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 ZFSSA 上的文件资源并且每个都具有唯一的用户标识符。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 ZFSSA 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。

IDMU

Microsoft 提供了一项称为 "Identity Management for UNIX" (IDMU) 的功能。Windows Server 2003 中提供了此软件，并且 Windows Server 2003 R2 和更高版本捆绑了此软件。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 RFC2307 （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，将通过临时映射为该用户提供临时凭证，除非其被拒绝映射阻止。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 ZFSSA 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 ZFSSA 与 Oracle 的清单门户相连接，您可以通过该门户管理您的 Oracle 设备。注册是使用回拨服务的先决条件。
- 回拨服务与 Oracle 支持系统进行通信来提供以下功能：
  - 故障报告 – 系统向 Oracle 报告活动问题以获得自动服务响应。根据故障的性质，可以创建支持案例。
  - 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。当一个已激活系统长时间未发送心跳时，Oracle 支持系统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 ZFSSA 获取以下数据，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 支持系统中注册服务标签，从而轻松跟踪您的 Oracle 设备，同时加速服务呼叫的处理。默认情况下，服务标签处于启用状态。

SMTP

SMTP 会发送 ZFSSA 生成的所有邮件，通常是根据配置对警报进行响应。SMTP 不接受外部邮件；它仅发送由 ZFSSA 自身自动生成的邮件。

默认情况下，SMTP 服务使用 DNS（MX 记录）确定将邮件发送到何处。如果没有为 ZFSSA 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 ZFSSA 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 (Simple Network Management Protocol, SNMP)

在 ZFSSA 上提供了两种 SNMP 功能；可以由 SNMP 发送 ZFSSA 状态信息，并且可以配置警报来发送 SNMP 陷阱。可以使用 SNMP 版本 1 和 2c。

系统日志

系统日志消息是从 ZFSSA 传输到一个或多个远程系统的小型事件消息。ZFSSA 提供了两种系统日志功能：

- 可以配置警报来向一个或多个远程系统发送系统日志消息。
- ZFSSA 上支持系统日志的服务可以将系统日志消息转发到远程系统。

系统日志可以配置为使用 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。系统日志消息作为 UDP 数据报进行传输。因此，它们可能会被网络丢弃，如果发送系统内存不足或网络非常拥堵，则可能根本不发送这些消息。因此，管理员应该认识到在网络发生复杂故障的情况下，一些消息可能缺失或被丢弃。

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 ZFSSA 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 ZFSSA 移到另一个网络位置或者改变了用途，可能需要更改这些配置。

磁盘清理

应当定期执行磁盘清理，以便 ZFSSA 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 ZFSSA 上销毁的某个共享资源是复制源，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。

远程管理访问

本节描述了 ZFSSA 远程访问安全。

浏览器用户界面 (Browser User Interface, BUI)

可以使用 BUI 服务屏幕查看和修改远程访问服务和设置。

安全 Shell (Secure Shell, SSH)

SSH 允许用户通过命令行界面 (Command Line Interface, CLI) 登录到 ZFSSA 并执行可以在 BUI 中执行的大多数管理操作。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。

日志

本节描述了与安全相关的日志记录功能。

审计

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
2009-10-12 05:20:24	root	galaxy	Disabled ftp service	
2009-10-12 03:17:05	root	galaxy	User logged in	
2009-10-11 22:38:56	root	galaxy	Browser session timed out	
2009-10-11 21:13:35	root	<console>	Enabled ftp service	

回拨

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
2009-10-12 05:24:09	Uploaded file 'cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz' to Oracle support	OK

更多信息

在每个 ZFSSA 浏览器用户界面 (Browser User Interface, BUI) 页面中，您可以通过单击页面左上角的 "Help" 按钮查找特定于上下文的联机帮助。

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

www.oracle.com/cn/products/servers-storage/storage/nas/overview

文档对应关系

可使用下表查找 ZFSSA 的每项服务、配置或其他功能的详细文档。使用 BUI 配置 ZFSSA 时，您可以在任何屏幕中单击右上角的 "HELP" 链接来显示针对该屏幕的帮助信息。

表 4 服务

服务	文档位置
Active Directory	服务:Active_Directory
身份映射	服务:Identity_Mapping
DNS	服务:DNS

服务	文档位置
动态路由	服务:Dynamic_Routing
IPMP	服务:IPMP
NTP	服务:NTP
回拨	服务:Phone_Home
服务标签	服务:Service_Tags
SMTP	服务:SMTP
SNMP	服务:SNMP
系统日志	服务:Syslog
系统标识	服务:System_Identity
SSH	服务:SSH

表 5 配置

配置	文档位置
SAN	配置:SAN
SAN:FC	配置:SAN:FC
SAN:iSCSI	配置:SAN:iSCSI
SAN:SRP	配置:SAN:SRP
群集	配置:群集
用户	配置:用户
首选项	配置:首选项
警报	配置:警报
存储	配置:存储

表 6 存储

存储	文档位置
共享资源	共享资源
概念	共享资源:概念
Shadow_Migration	共享资源:Shadow_Migration
Space_Management	共享资源:Space_Management
File system_Namespace	共享资源:File system_Namespace
共享资源	共享资源:共享资源
常规	共享资源:共享资源:常规
协议	共享资源:共享资源:协议
访问权限	共享资源:共享资源:访问
快照	共享资源:共享资源:快照
项目	共享资源:项目
项目:常规	共享资源:项目:常规

存储	文档位置
项目:协议	共享资源:项目:协议
项目:复制	共享资源:项目:复制
模式	共享资源:模式

ORACLE