Oracle® ZFS Storage Appliance Security Guide

Part No: E41348-02

Oracle ZFS Storage Appliance Security Overview

This guide explores, reviews, and highlights the security considerations necessary to create a secure storage system and a team-wide understanding of your specific security goals. We recommend that you read this guide before you configure your appliance so you can take advantage of the available security features and create the levels of security that you need.

You can also use this guide as a reference to find more detailed information about security considerations of the various features and capabilities of the Oracle ZFS Storage Appliance (ZFSSA). For appliance configuration procedures, see the Oracle ZFS Storage System Administration Guide.

The following sections provide a description of the ZFSSA security features:

- **Initial installation** - Describes how to set up administrative access, how the root account is established, and the effects of a ZFSSA factory reset.
- **Physical Security** - Describes the physical security environment for the ZFSSA.
- **Administrative Model** - Describes restricting access to the CLI and BUI, the system patching model, deferred updates, support bundles, and configuration backup.
- **ZFSSA Users** - Describes administrative roles, who can administer the ZFSSA, and managing user authorizations.
- **Access Control Lists (ACL)** - Describes the mechanism that allows or denies access to files and directories.
- **Storage Area Network (SAN)** - Describes logical unit numbers (LUNs) and the associated initiator groups, as well as initiator authentication options and defaults.
- **Data Services** - Describes the data services supported by the ZFSSA and the security offered by the different data services.
- **Directory Services** - Describes the directory services that can be configured on the ZFSSA and their security ramifications.
- **System Settings** - Describes system settings; Phone Home, Service Tags, SMTP, SNMP, Syslog, System Identity, Disk Scrubbing, and Preventing Destruction.
- Remote Administrative Access - Describes remote access via the BUI and CLI. · Logs - Describes the log types pertinent to security.

Initial installation

The ZFSSA is delivered to customers with the ZFSSA software pre-installed. No software installation is required and no media is delivered.

The initial installation is accomplished with the default account name and password, the default root password must be changed after installation. If the ZFSSA is reset to factory defaults, the root password also resets to the default for both the ZFSSA and the service processor.

During the initial installation of a ZFSSA, there is a default account name and password that is associated with the system's Service Processor. It is this default account that allows a system administrator to gain first-time access to the ZFSSA, where the administrator is then required to perform the system's initial installation steps. One of the required steps is to set a new ZFSSA administrative password, which in turn also resets the default Service Processor password to the same value.

Physical Security

To control access to your system, you must maintain the physical security of your computing environment. For example, a system that is logged in and left unattended is vulnerable to unauthorized access. The computer's surroundings and the computer hardware must be physically protected from unauthorized access at all times.

The ZFSSA is intended for restricted access whereby access is controlled through the use of a means of security (for example, key, lock, tool, badge access) and personnel authorized for access have been instructed on the reasons for the restrictions and any precautions that need to be taken.

Administrative Model

This section describes security for the ZFSSA administrative models.

Restricted Access (CLI and BUI)

Administrative access to the Browser User Interface (BUI) and Command Line Interface (CLI) is limited to the root user, local administrators defined with the relevant privileges, and those authorized through identity servers such as Lightweight Directory Access Protocol (LDAP) and Network Information Service (NIS).

Administration is conducted over a Secure Sockets Layer (SSL) command-line login or an HTTP secure (HTTPS) browser session. HTTPS sessions are encrypted with a self-signed certificate that is uniquely generated for each ZFSSA at initial installation time. HTTPS sessions have a user-definable default session timeout of 15 minutes.

System Updates

System updates are applied as whole binary replacements of the system software. Before the update, a snapshot is taken of the running system pool. This lets an administrator roll back to the previous version if needed.

Deferred Updates

A deferred update is a feature or piece of functionality that is part of a system update which is not activated when the system update is performed. The administrator decides when or if to apply deferred updates. Updates not applied during a system update, are still available during successive system updates. You cannot select individual updates to apply, when you choose to apply deferred updates, you can apply all or none of the updates. After you apply an update, you cannot rollback to an earlier system software version.

Support Bundles

When your system is registered for Phone Home support if it suffers a major fault, your system status is sent to My Oracle Support where it can be examined by engineering support personnel and a support bundle can be created. The system status information that is sent to My Oracle Support contains no user data; only configuration information is sent.

Configuration Backup

System configurations can be saved locally for later restore. These backups contain no user data; only configuration settings are saved.

ZFSSA Users

There are two types of ZFSSA users:

- **Data Services Users** – Clients who access file and block resources using the supported protocols such as NFS, SMB, Fibre Channel, iSCSI, http, and FTP.
- **Administrative Users** - Users who will manage the configuration and services on the ZFSSA. This section applies to administrative users only.

Administrative User Roles

Administrators can be granted privileges by assigning custom roles to them. A role is a collection of privileges that you can assign to an administrator. You may want to create various administrator and operator roles, with different authorization levels. Staff members should be assigned any role that is suitable for their needs, without assigning unnecessary privileges.

The use of roles is more secure than the use of shared full-access administrator passwords, such as giving everyone the root password. Roles restrict users to defined sets of authorizations. In addition, user roles are traceable to individual usernames in the audit logs. By default, a role called "Basic administration" exists, which contains a minimum of authorizations.

Administrative users can be:

- Local users – Where all account information is saved on the ZFSSA.
- Directory users – Where existing NIS or LDAP accounts are used and supplemental authorization settings are saved on the ZFSSA. This lets existing NIS/LDAP users log in and administer the ZFSSA but existing NIS/LDAP users cannot log into the ZFSSA by default. Access must be explicitly granted to the ZFSSA.

Administrative Scopes

Authorizations let users perform specific tasks, such as creating shares, rebooting the ZFSSA, and updating the system software. Groups of authorizations are called scopes. Each scope can have a set of optional filters that narrow the number of the authorizations. For example, rather than authorization to restart all services, a filter can be used such that the authorization can restart only the HTTP service.

Access Control Lists (ACL)

ZFSSA provides file access control through Access control lists (ACLs). An access control list is a mechanism that allows or denies access to a particular file or directory.

The ACL model provided by ZFSSA is based on the NFSv4 ACL model which is derived from the Windows ACL semantics. It is a rich ACL model that provides for fine grained access to files and directories. Every file and directory within the storage ZFSSA has an ACL and all access control decisions for both SMB and NFS go through the same algorithms for determining who is allowed or denied access to files and directories.

An ACL is composed of one or more ACEs (Access Control Entries). Each ACE contains an entry for the permissions the ACE grants or denies; who the ACE applies to and the inheritance level flags used.

ACL Inheritance

NFSv4 ACLs let individual ACEs be inherited by newly created file and directories. ACEs inheritance is controlled by several inheritance level flags that an administrator sets on the ACL when it is initially setup.

Determining ACL Access

NFSv4 ACLs are order dependent and are processed from top to bottom. Once a permission is granted, a subsequent ACE cannot take it away. Once a permission is denied, a subsequent ACE cannot grant it.

SMB Share Level ACL

An SMB share level ACL is an ACL which is combined with a file or directory ACL in the share to determine the file’s effective permissions. The share level ACL provides another layer of access control above the file ACLs and provides more sophisticated access control configurations. Share level ACLs are set when the file system is exported using the SMB protocol. If the file system is not exported using the SMB protocol, setting the share level ACL has no effect. By default, share level ACLs grant everyone full control.

ZFS ACL Properties

ACL Behavior and inheritance properties are applicable only for NFS clients. SMB clients use strict Windows semantics and take precedence over ZFS properties. The difference is that NFS utilizes POSIX semantics and SMB clients do not. The properties are mainly compatible with POSIX.

Storage Area Network (SAN)

In a SAN, target and initiator groups define sets of targets and initiators that can be associated with a Logical Unit Number (LUN). A LUN that is associated with a target group is only accessible via those group's targets. A LUN that is associated with an initiator group is only accessible by those group's initiators. You apply initiator groups and target groups to a LUN when you create a LUN. LUN creation cannot be completed successfully without defining at least one target group and one initiator group.

Aside from Challenge-Handshake Authentication Protocol (CHAP) authentication, which can be selected only for iSCSI/iSER initiator access, there is no authentication performed.

NOTE: Using the default initiator group can result in exposure of the LUN to unwanted or conflicting initiators.

Data Services

TABLE 1 Data Services

SERVICE	DESCRIPTION	PORTS USED
NFS	Filesystem access via the NFSv3 and NFSv4 protocols	111 and 2049

SERVICE	DESCRIPTION	PORTS USED
iSCSI	LUN access via the iSCSI protocol	3260 and 3205
SMB	Filesystem access via the SMB protocol	SMB-over-NetBIOS 139
		SMB-over-TCP 445
		NetBIOS Datagram 138
		NetBIOS Name Service 137
FTP	Filesystem access via the FTP protocol	21
HTTP	Filesystem access via the HTTP protocol	80
NDMP	NDMP host service	10000
Remote Replication	Remote replication	216
Shadow Migration	Shadow data migration	
SFTP	Filesystem access via the SFTP protocol	218
SRP	Block access via the SRP protocol	
TFTP	Filesystem access via the TFTP protocol	
Virus Scan	Filesystem virus scanning	

Minimum Needed Ports:

To provide security on a network, you can create firewalls. Port numbers are used for creating firewalls and uniquely identify a transaction over a network by specifying the host and the service.

The following list shows the minimum ports required for creating firewalls:

Inbound Ports

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

Additional inbound ports if http file sharing is used (typically it is not)

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

Outbound Ports

- tcp/80 (WEB)

Note: For replication, use Generic Routing Encapsulation (GRE) tunnels where possible. This lets traffic run on the back end interfaces and avoid the firewall where traffic could be slowed. If GRE tunnels are not available on the NFS core, you must run replication over the front end interface. In this case, port 216 must also be open.

NFS Authentication and Encryption Options

NFS shares are allocated with AUTH_SYS RPC authentication by default. You can also configure them to be shared with Kerberos security. Using AUTH_SYS authentication, the client's UNIX uid and gid are

passed unauthenticated on the network by the NFS server. This authentication mechanism is easily defeated by anyone with root access on a client therefore it is best to use one of the other available security modes.

Additional access controls can be specified on a per share basis to allow or disallow access to the shares for specific hosts, DNS domains,or networks.

Security Modes

Security modes are set on per-share basis . The following list describes the available Kerberos security settings.

- krb5 - End-user authentication through Kerberos V5
- krb5i - krb5 plus integrity protection (data packets are tamper proof)
- krb5p - krb5i plus privacy protection (data packets are tamper proof and encrypted)

Combinations of Kerberos types may also be specified in the security mode setting. The combination security modes let clients mount with any Kerberos types listed.

Kerberos Types

- sys - System Authentication
- krb5 - Kerberos v5 only, clients must mount using this type.
- krb5:krb5i - Kerberos v5, with integrity, clients may mount using any type listed.
- krb5i - Kerberos v5 integrity only, clients must mount using this type.
- krb5:krb5i:krb5p - Kerberos v5, with integrity or privacy, clients may mount using any type listed.
- krb5p - Kerberos v5 privacy only, clients must mount using this type.

iSCSI

When you configure a LUN on the ZFSSA you can export that volume over an Internet Small Computer System Interface (iSCSI) target. The iSCSI service lets iSCSI initiators access targets using the iSCSI protocol.

This service supports discovery, management, and configuration using the iSNS protocol. The iSCSI service supports both unidirectional (target authenticates initiator) and bidirectional (target and initiator authenticate each other) authentication using CHAP. Additionally, the service supports CHAP authentication data management in a RADIUS database.

The system first performs authentication and then authorization, in two independent steps. If the local initiator has a CHAP name and a CHAP secret, the system performs authentication. If the local initiator does not have CHAP properties, the system does not perform any authentication and therefore all initiators are eligible for authorization.

The iSCSI service lets you specify a global list of initiators that you can use within the initiator groups. When using iSCSI and CHAP authentication, RADIUS can be used as the iSCSI protocol that defers all CHAP authentications to the selected RADIUS server.

RADIUS Support

Remote Authentication Dial-In User Service (RADIUS) is a system for using a centralized server to perform CHAP authentication on behalf of the storage nodes. When you use iSCSI and CHAP

authentication, you can select RADIUS for the iSCSI protocol, which applies both iSCSI and the iSCSI Extensions for RDMA (iSER), and sends all CHAP authentications to the selected RADIUS server.

To allow the ZFSSA to perform CHAP authentication using RADIUS, the following information must match:

- The ZFSSA must specify the address of the RADIUS server and a secret to use when communicating with this RADIUS server.
- The RADIUS server (for example, in its clients file) must have an entry that gives the address of the ZFSSA and specifies the same secret as above.
- The RADIUS server (for example, in its users file) must have an entry that supplies the CHAP name and matching CHAP secret for each initiator.
- If the initiator uses its IQN name as its CHAP name (this is the recommended configuration) and the ZFSSA does not need a separate Initiator entry for each Initiator box, the RADIUS server can perform all of the authentication steps.
- If the initiator uses a separate CHAP name, the ZFSSA must have an Initiator entry for the initiator that specifies the mapping from an IQN name to the CHAP name. This Initiator entry does NOT need to specify the CHAP secret for the initiator.

Server Message Block (SMB)

The SMB protocol (also known as Common Internet File System (CIFS)) primarily provides shared access to files on a Microsoft Windows network. It also provides authentication.

The following SMB options have security implications:

- **Restrict Anonymous Access to share list** - This option requires clients to authenticate using SMB before receiving a list of shares. If this option is disabled, anonymous clients can access the list of shares. This option is disabled by default.
- **SMB Signing Enabled** - This option enables interoperability with SMB clients using the SMB signing feature. If the option is enabled, a signed packet will have the signature verified. If the option is disabled, an unsigned packet will be accepted without signature verification. This option is disabled by default.
- **SMB Signing Required** - This option can be used when SMB signing is required. When the option is enabled, all SMB packets must be signed or they will be rejected. Clients that do not support SMB signing are unable to connect to the server. This option is off by default.
- **Enable Access-based Enumeration** - Setting this option filters directory entries based on the credentials of the client. When the client does not have access to a file or directory, that file will be omitted from the list of entries returned to the client. This option is disabled by default.

Active Directory (AD) Domain Mode Authentication

In Domain Mode, users are defined in Active Directory. SMB clients can connect to the ZFSSA using Kerberos or NTLM authentication.

When a user connects via a fully-qualified ZFSSA hostname, Windows clients in the same domain or a trusted domain use Kerberos authentication otherwise they use NTLM authentication.

When an SMB client uses NTLM authentication to connect to the ZFSSA, the user's credentials are forwarded to the AD Domain Controller for authentication. This is called pass-through authentication.

If Windows security policies restricting NTLM authentication are defined, Windows clients must connect to ZFSSA via a fully-qualified hostname. For more information, see this MSDN article: http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx.

After authentication a "security context" is established for the user's SMB session. The user represented by the security context has a unique Security Descriptor (SID). The SID denotes file ownership and is used to determine file access privileges.

Workgroup Mode Authentication

In Workgroup Mode, users are defined locally on the ZFSSA. When an SMB client connects to a ZFSSA in Workgroup Mode, that user's user name and password hashes are used to authenticate the user locally.

The LAN Manager (LM) compatibility level is used to specify the protocol used for authentication when the ZFSSA is in workgroup mode.

The following list shows the ZFSSA behavior for each LM compatibility level:

- Level 2: Accepts LM, NTLM and NTLMv2 authentication
- Level 3: Accepts LM, NTLM and NTLMv2 authentication
- Level 4: Accepts NTLM and NTLMv2 authentication
- Level 5: Accepts NTLMv2 authentication only.

Once the Workgroup user is successfully authenticated a security context is established. A unique SID is created for users defined on the ZFSSA using a combination of the machine's SID and the user's UID. All local users are defined as UNIX users.

Local Groups and Privileges

Local groups are domain user groups that provide additional privileges to those users. Administrators can bypass file permissions to change the ownership on files. Backup Operators can bypass file access controls to backup and restore files.

Administrative Operations via the Microsoft Management Console (MMC)

To ensure that only the appropriate users have access to administrative operations there are some access restrictions on the operations performed remotely using MMC.

The following list shows the users and their allowed operations:

- Regular users - List shares
- Members of the Administrators group - List open files and close files, disconnect user connections, view services, and event log
- Members of the Administrators group can also set/modify share level ACLs
- Members of the Administrators group - List open files and close files, disconnect user connections, view services and event log

Virus Scan

The Virus Scan service scans for viruses at the file system level. When a file is accessed from any protocol, the Virus Scan service first scans the file, and both denies access and quarantines the file if a virus is found. The scan is performed by an external engine that the ZFSSA contacts. The external engine is not included in ZFSSA software.

Once a file has been scanned with the latest virus definitions, it is not rescanned until it is next modified. Virus scanning is provided mainly for SMB clients who are likely to introduce viruses. NFS clients can also

use virus scanning, but due to the way the NFS protocol works a virus may not be detected as quickly as with the SMB client.

Delay Engine for Timing Attacks

SMB does not implement any delay engine to prevent timing attacks. It relies on the Solaris cryptographic framework.

Data Encryption on the Wire

The SMB service uses version 1 of the SMB protocol, which does not support data encryption on the wire.

File Transfer Protocol (FTP)

FTP allows file system access from FTP clients. The FTP service does not allow anonymous logins and users must authenticate with the configured name service.

FTP supports the following security settings. These settings are shared for all file systems for which the FTP protocol access is enabled:

- Enable SSL/TLS - Allows SSL/TLS encrypted FTP connections and ensures that the FTP transaction is encrypted. This is disabled by default.
- Permit root login - Allows FTP logins for the root user. This is off by default because FTP authentication is with plain text, which poses a security risk from network sniffing attacks.
- Maximum number of allowable login attempts - The number of failed login attempts before an FTP connection is disconnected, and the user must reconnect to try again. The default is 3.
- Logging level - The verbosity of the log.

FTP supports the following logs:

- proftpd - FTP events including successful and unsuccessful login attempts
- proftpd_xfer - File transfer log
- proftpd_tls - FTP events related to SSL/TLS encryption

Hypertext Transfer Protocol (HTTP)

HTTP provides access to file systems using the HTTP and HTTPS protocols and the HTTP extension Web based Distributed Authoring and Versioning (WebDAV). This lets clients access shared file systems through a web browser or as a local file system if their client software supports it. The HTTPS server uses a self-signed security certificate.

The following properties are available:

- Require client login - Clients must authenticate before share access is allowed, and files they create will have their ownership. If this is not set, files created will be owned by the HTTP service with user "nobody”.
- Protocols - Select which access methods to support: HTTP, HTTPS, or both.
- HTTP Port (for incoming connections) - HTTP port, the default is port 80.
- HTTPS Port (for incoming secure connections) - HTTP port, the default port is 443.

When Require Client Login is enabled, the ZFSSA denies access to clients that do not supply valid authentication credentials for a local user, a NIS user, or an LDAP user. Active Directory authentication is

not supported. Only basic HTTP authentication is supported. Unless HTTPS is being used, this transmits the username and password unencrypted, which may not be appropriate for all environments. If Require Client Login is disabled, the ZFSSA does not try to authenticate.

Regardless of authentication, permissions are not masked from created files and directories. Newly created files have permissions read and write by everyone. Newly created directories have permissions read, write, and execute by everyone.

Network Data Management Protocol (NDMP)

NDMP enables the ZFSSA to participate in NDMP-based backup and restore operations controlled by a remote NDMP client called a Data Management Application (DMA). Using NDMP, ZFSSA user data (for example, data stored in administrator-created shares on the ZFSSA) can be backed up and restored to both locally attached devices such as tape drives and remote systems. Locally attached devices can also be backed up and restored via DMA.

Remote Replication

ZFSSA remote replication facilitates replication of projects and shares. This service lets you view ZFSSAs that have replicated data to this ZFSSA and configure the ZFSSAs to which this ZFSSA can replicate.

When this service is enabled, the ZFSSA receives replication updates from other ZFSSAs as well as send replication updates for local projects and shares according to their configured actions. When the service is disabled, incoming replication updates fail and no local projects and shares are replicated.

The root password for the remote ZFSSA is required to configure remote replication targets for the ZFSSA. These targets are used to setup a replication peer connection that enables the ZFSSAs to communicate.

During target creation, the root password is used to confirm request authenticity and to produce and exchange security keys that will be used to identify the ZFSSAs in subsequent communications.

The generated keys are stored persistently as part of ZFSSA configuration. The root password is never stored persistently. The root password is never transmitted in the clear. All ZFSSA communications, including this initial identity exchange, are protected with SSL.

Shadow Migration

Shadow migration permits automatic data migration from external or internal sources and controls automatic background migration. Regardless of whether the service is enabled or not, data is migrated synchronously for in-band requests. The primary purpose of the service is to allow tuning of the number of threads dedicated to background migration.

NFS mounts on an NFS source are not under control of the ZFSSA user. Shadow migration mounts cannot be secure therefore; if the server expects a Kerberos or similar request the source mount is rejected.

SSH File Transfer Protocol (SFTP)

SFTP allows file system access from SFTP clients. Anonymous logins are not allowed so users must authenticate with the configured name service.

When you create an SFTP key, you must include the user property with a valid user assignment. SFTP keys are grouped by user and are authenticated through SFTP with the user's name.

NOTE: For security, you should recreate existing SFTP keys that do not include the user property, even though they will authenticate.

Trivial File Transfer Protocol (TFTP)

TFTP is a simple protocol for transferring files. It is designed to be small and easy to implement but lacks most of the security features of FTP. TFTP only reads and writes files to and from a remote server. It cannot list directories, and currently has no provisions for user authentication.

Directory Services

Network Information Service (NIS)

NIS is a name service for centralized directory management. The ZFSSA can act as a NIS client for users and groups so that NIS users can login to FTP and HTTP/WebDAV. NIS users can also be granted privileges for ZFSSA administration. The ZFSSA supplements NIS information with its own privilege settings.

Lightweight Directory Access Protocol (LDAP)

The ZFSSA uses LDAP to authenticate both administrative users as well as some data services users (ftp, http). LDAP over SSL security is supported by the ZFSSA. LDAP is used to retrieve information about users and groups and is used in the following ways:

- Provides user interfaces that accept and display names for users and groups.
- Maps names to and from users and groups, for data protocols like NFSv4 that use names. · Defines group membership for use in access control.
- Optionally, to carry authentication data used for administrative and data access authentication.

LDAP connections can be used as an authentication mechanism. For example, when a user attempts to authenticate to the ZFSSA, the ZFSSA can attempt to authenticate to the LDAP server as that user as a mechanism for verifying the authentication.

There are a variety of controls for LDAP connection security:

- Appliance-to-server authentication:
  - Appliance is anonymous
  - Appliance authenticates using user's Kerberos credentials
  - Appliance authenticates using specified "proxy" user and password
- Server-to-appliance authentication (ensuring that the correct server has been contacted):
  1. Unsecured
  2. Server is authenticated using Kerberos
  3. Server is authenticated using a TLS certificate

Data carried over an LDAP connection is encrypted if Kerberos or TLS is used but otherwise is not encrypted. When TLS is used, the first connection at configuration time is not secured. The server's certificate is collected at that time and is used to authenticate later production connections.

It is not possible to import a Certificate Authority certificate to be used to authenticate multiple LDAP servers; neither is it possible to import a particular LDAP server's certificate manually.

Only raw TLS (LDAPS) is supported. STARTTLS connections, which start on an unsecured LDAP connection and then change over to a secured connection, are not supported. LDAP servers that require a client certificate are not supported.

Identity Mapping

Clients can access file resources on the ZFSSA using SMB or NFS and each has a unique user identifier. SMB/Windows users have Security Descriptors (SIDs) and UNIX/Linux users have User IDs (UIDs). Users can also be members of groups that are identified by Group SIDs (for Windows users) or Group IDs (GID) for UNIX/Linux users.

In environments where file resources are accessed using both protocols it is often desirable to establish identity equivalences where for example, a UNIX user is equivalent to an Active Directory user. This is important for determining access rights to file resources on the ZFSSA.

There are different types of identity mapping that involve Directory Services such as Active Directory, LDAP, and NIS. Care should be taken to follow the security best practices for the directory service being used.

IDMU

Microsoft offers a feature called Identity Management for UNIX (IDMU). This software is available for Windows Server 2003, and is bundled with Windows Server 2003 R2 and later. This feature is part of what was formerly called Services for UNIX in its unbundled form.

The primary use of IDMU is to support Windows as a NIS/NFS server. IDMU lets the administrator specify a number of UNIX-related parameters: UID, GID, login shell, home directory, and similar for groups. These parameters are made available using AD through a schema similar to but not the same as RFC2307, and through the NIS service.

When the IDMU mapping mode is used, the identity mapping service uses these UNIX attributes to establish mappings between Windows and UNIX identities. This approach is very similar to directory-based mapping, except the identity mapping service queries the property schema established by the IDMU software instead of allowing a custom schema. When this approach is used, no other directory-based mapping can be used.

Directory-based Mapping

Directory-based mapping involves annotating an LDAP or Active Directory object with information about how the identity maps to an equivalent identity on the opposite platform. These extra attributes associated with the object must be configured.

Name-based Mapping

Name-based mapping involves creating various rules that map identities by name. These rules establish equivalences between Windows identities and UNIX identities.

Ephemeral Mapping

If no name-based mapping rule applies for a particular user, that user is given temporary credentials through an ephemeral mapping unless they are blocked by a deny mapping. When a Windows user with an

ephemeral UNIX name creates a file on the system, Windows clients accessing the file using SMB see that the file is owned by that Windows identity. However, NFS clients see that the file is owned by “nobody”.

System Settings

The following sections describe the available system security settings.

Phone Home

The Phone Home service is used to manage the ZFSSA registration as well as the Phone Home remote support service. No user data or metadata is transmitted in these messages.

- Registration connects your ZFSSA with Oracle's inventory portal, through which you can manage your Oracle equipment. Registration is a prerequisite for using the Phone Home service.
- The Phone Home service communicates with Oracle support to provide:
  - Fault reporting - The system reports active problems to Oracle for automated service response. Depending on the nature of the fault, a support case may be opened.
  - Heartbeats - Daily heartbeat messages are sent to Oracle to indicate that the system is up and running. Oracle support may notify the technical contact for an account when one of the activated systems fails to send a heartbeat for too long.
  - System configuration - Periodic messages are sent to Oracle describing current software and hardware versions and configuration as well as storage configuration.

Service Tags

Service Tags are used to facilitate product inventory and support, by allowing the ZFSSA to be queried for data such as:

- System serial number
- System type
- Software version numbers

You can register the service tags with Oracle support, allowing you to easily keep track of your Oracle equipment and also expedite service calls. The service tags are enabled by default.

SMTP

SMTP sends all mail generated by the ZFSSA, typically in response to alerts as configured. SMTP does not accept external mail; it only sends mail generated automatically by the ZFSSA itself.

By default, the SMTP service uses DNS (MX records) to determine where to send mail. If DNS is not configured for the ZFSSA's domain, or the destination domain for outgoing mail does not have DNS MX records set up properly, the ZFSSA can be configured to forward all mail through an outgoing mail server.

Simple Network Management Protocol (SNMP)

SNMP provides two functions on the ZFSSA; ZFSSA status information can be served by SNMP and alerts can be configured to send SNMP traps. Both SNMP versions 1 and 2c are available.

Syslog

A Syslog message is a small event message transmitted from the ZFSSA to one or more remote systems. Syslog provides two ZFSSA functions:

- Alerts can be configured to send Syslog messages to one or more remote systems
- Services on the ZFSSA that are Syslog capable can have their Syslog messages forwarded to remote systems

The Syslog can be configured to use the classic output format described by RFC 3164, or the newer, versioned output format described by RFC 5424. Syslog messages are transmitted as UDP datagrams. Therefore they are subject to being dropped by the network, or may not be sent at all if the sending system is low on memory or the network is sufficiently congested. Administrators should therefore assume that in complex failure scenarios in a network some messages may be missing and were dropped.

The message contains the following elements:

- A facility describing the type of system component that emitted the message
- A severity describing the severity of the condition associated with the message
- A timestamp describing the time of the associated event in UTC
- A hostname describing the canonical name of the ZFSSA
- A tag describing the name of the system component that emitted the message
- A message describing the event itself

System Identity

This service provides configuration for the system name and location. There may be a need to change these if the ZFSSA is moved to a different network location, or is repurposed.

Disk Scrubbing

Disk scrubbing should be performed on a regular basis to allow the ZFSSA to detect and correct damaged data on the disk. Disk scrubbing is a background process that reads disks during idle periods to detect irremediable read errors in infrequently accessed sectors. Timely detection of such latent sector errors is important to reduce data loss.

Preventing Destruction

When the Prevent Destruction feature is enabled, the share or project cannot be destroyed. This includes destroying a share through dependent clones, destroying a share within a project, or destroying a replication package. However, it does not affect shares destroyed through replication updates. If a share is destroyed on a ZFSSA that is the source for replication, the corresponding share on the target will be destroyed, even if this property is set.

To destroy the share, the property must first be explicitly turned off as a separate step. This property is off by default.

Remote Administrative Access

This section describes ZFSSA remote access security.

Browser User Interface (BUI)

You use the BUI Services screens to view and modify the remote access services and settings.

Secure Shell (SSH)

SSH lets users log in to the ZFSSA through the Command Line Interface (CLI) and perform most of the same administrative actions that can be performed in the BUI. SSH can also be used as means of executing automated scripts from a remote host, such as for retrieving daily logs or analytics statistics.

Logs

This section describes logging features related to security.

Audit

The audit log records user activity events, including login and logout to the BUI and CLI, and administrative actions. The following table shows example audit log entries as they would appear in the BUI:

TABLE 2 Audit Log Record

Time	User	Host	Summary	Session Annotation
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	

Phone Home

If Phone Home is used, this log will show communication events with Oracle support. The following table is an example Phone Home entry as it would appear in the BUI:

TABLE 3 Phone Home Log Record

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

More Information

You can find context specific online help for each ZFSSA Browser User Interface (BUI) page by clicking on the Help button located at the top left of each page.

You can find complete product information for the Oracle ZFS Storage appliance at the following location:

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

Documentation Mapping

Use the tables below to locate detailed documentation for each of the services, configurations, or other features of the ZFSSA. When you are using the BUI to configure an ZFSSA, you can click the HELP link in the top right of any screen to display the help for that screen.

TABLE 4 Services

Service	Documentation Location
Active Directory	Services:Active_Directory
Identity Mapping	Services:Identity_Mapping
DNS	Services:DNS
Dynamic Routing	Services:Dynamic_Routing
IPMP	Services:IPMP
NTP	Services:NTP
Phone Home	Services:Phone_Home
Service Tags	Services:Service_Tags
SMTP	Services:SMTP
SNMP	Services:SNMP
Syslog	Services:Syslog
System Identity	Services:System_Identity
SSH	Services:SSH

TABLE 5 Configuration

Configuration	Documentation Location
SAN	Configuration:SAN
SAN:FC	Configuration:SAN:FC
SAN:iSCSI	Configuration:SAN:iSCSI
SAN:SRP	Configuration:SAN:SRP
Cluster	Configuration:Cluster
Users	Configuration:Users
Preferences	Configuration:Preferences
Alerts	Configuration:Alerts
Storage	Configuration:Storage

TABLE 6 Storage

Storage	Documentation Location
Shares	Shares

Storage	Documentation Location
Concepts	Shares:Concepts
Shadow_Migration	Shares:Shadow_Migration
Space_Management	Shares:Space_Management
File system_Namespace	Shares:File system_Namespace
Shares	Shares:Shares
General	Shares:Shares:General
Protocols	Shares:Shares:Protocols
Access	Shares:Shares:Access
Snapshots	Shares:Shares:Snapshots
Projects	Shares:Projects
Projects:General	Shares:Projects:General
Projects:Protocols	Shares:Projects:Protocols
Projects:Replication	Shares:Projects:Replication
Schema	Shares:Schema