Oracle® ZFS Storage Appliance Security Guide, Release OS8.7.0

Part No: E78909-02
July 2017

ORACLE

Oracle ZFS Storage Appliance Security Guide, Release OS8.7.0

Part No: E78909-02

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Référence: E78909-02

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Oracle ZFS Storage Appliance Security Guide

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. For appliance configuration procedures, see the *Oracle ZFS Storage Appliance Administration Guide*.

The following sections provide a description of the Oracle ZFS Storage Appliance security features and recommendations:

- **First Steps** - Describes login security during the initial installation of the appliance and recommendations for the physical security of your system.
- **Administrative Model** - Describes remote access via the BUI and CLI, restricting access to the BUI and CLI, the system patching model, deferred updates, support bundles, and configuration backup.
- **Appliance Users** - Describes administrative roles, who can administer the appliance, and managing user authorizations.
- **Access Control Lists** - Describes the mechanism that allows or denies access to files and directories.
- **Data Services** - Describes the data services supported by the appliance and the security offered by the different data services.
- **Directory Services** - Describes the directory services that can be configured on the appliance and their security ramifications.
- **System Settings** - Describes system settings: Phone Home, Service Tags, Kerberos, SMTP, SNMP, syslog, system identity, disk scrubbing, and preventing destruction.
- **Security Logs** - Describes the log types pertinent to security.

First Steps

This section describes login security during the initial installation of the appliance and recommendations for the physical security of your system.

Initial Installation

The Oracle ZFS Storage Appliance is delivered with the appliance 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 Oracle ZFS Storage Appliance is reset to factory defaults, the root password also resets to the default for both the appliance and the service processor.

During the initial installation of an Oracle ZFS Storage Appliance, there is a default account name and password that is associated with the system service processor. This default account allows a system administrator to gain first-time access to the appliance, where the administrator is then required to perform the initial installation steps. One of the required steps is to set a new appliance 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 Oracle ZFS Storage Appliance 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 Oracle ZFS Storage Appliance administrative model.

Remote Administrative Access

This section describes Oracle ZFS Storage Appliance remote access security.

Browser User Interface

The Browser User Interface (BUI) is used for general administration of the appliance. You can use the BUI Services Screens to view and modify the remote access services and settings.

Administration is conducted over an HTTP secure (HTTPS) browser session. HTTPS sessions are encrypted with a self-signed certificate that is uniquely generated for each Oracle ZFS Storage Appliance at initial installation time. HTTPS sessions have a user-definable default session timeout of 15 minutes.

Command Line Interface

The Command Line Interface (CLI) can be used to perform most of the same administrative actions that can be performed in the BUI.

Secure Shell (SSH) lets users log in to the Oracle ZFS Storage Appliance over a Secure Sockets Layer (SSL) connection to the CLI. SSH can also be used as a means of executing automated scripts from a remote host, such as for retrieving daily logs or analytics statistics.

Restricted User Authorization

Administrative access 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).

In addition, the appliance can use Kerberos to authenticate users for administrative login using the BUI, CLI, and RESTful API, and for access to services, including NFS, HTTP, FTP, SFTP, and SSH. Kerberos can also be used to set security for individual shares that use the NFS protocol as described in “NFS Authentication and Encryption Options” on page 14.

Oracle ZFS Storage Appliance RESTful API

The Oracle ZFS Storage Appliance RESTful API can be used to manage the Oracle ZFS Storage Appliance. The RESTful architecture is based on a layered client-server model that lets services be transparently redirected through standard hubs, routers, and other network systems without client configuration.

The Oracle ZFS Storage Appliance RESTful API uses the same authentication credentials as the BUI and CLI. All requests from external clients are individually authenticated using the appliance credentials and are conducted over an HTTPS connection on port 215. The RESTful API supports HTTPS sessions that have a user-definable default timeout of 15 minutes.

For information on managing the Oracle ZFS Storage Appliance with the RESTful API, see the *Oracle ZFS Storage Appliance RESTful API Guide*.

System Updates

To take advantage of the latest security improvements, Oracle recommends keeping the system software up to date.

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 but 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 roll back to an earlier system software version.

Support Bundles

If your system is registered for Phone Home support and it suffers a major fault, your system status is sent to My Oracle Support, where it is 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 restoration. These backups contain no user data; only configuration settings are saved.

Appliance Users

There are two types of Oracle ZFS Storage Appliance users:

- **Data Services Users** – Clients who access file and block resources using the supported protocols such as Network File System (NFS), Server Message Block (SMB), Fibre Channel, Internet Small Computer System Interface (iSCSI), Hypertext Transfer Protocol (HTTP), and File Transfer Protocol (FTP).
- **Administrative Users** - Users who will manage the configuration and services on the appliance.

This section applies to administrative users only.

Administrative User Roles

You can grant administrators 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 Oracle ZFS Storage Appliance.
- **Directory Users** – Where existing NIS or LDAP accounts are used and supplemental authorization settings are saved on the appliance. Access to the appliance must be explicitly granted to existing NIS/LDAP users, who can then log in to and administer the appliance. Access cannot be granted by default.

Administrative Scopes

Authorizations let users perform specific tasks, such as creating shares, rebooting the appliance, 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 authorizations. For example, rather than

authorization to restart all services, a filter can be used to allow restarting of only the HTTP service.

Access Control Lists

The Oracle ZFS Storage Appliance provides file access control through access control lists (ACLs). An ACL is a mechanism that allows or denies access to a particular file or directory.

The ACL model provided by the Oracle ZFS Storage Appliance is based on the NFSv4 ACL model, which is derived from Windows ACL semantics. It is a rich ACL model that provides fine-grained access to files and directories. Every file and directory within the storage appliance 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 access control entries (ACEs). 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 files and directories. ACE inheritance is controlled by several inheritance-level flags that an administrator sets on the ACL when it is initially configured.

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 that 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.

Data Services

The following table provides a description and ports used for each data service.

TABLE 1 Data Services

SERVICE	DESCRIPTION	PORTS USED
NFS	Filesystem access via the NFSv3 and NFSv4 protocols	111 and 2049
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
Virus Scan	Filesystem virus scanning	
FTP	Filesystem access via the FTP protocol	21
HTTP	Filesystem access via the HTTP protocol	80
HTTPS	For incoming secure connections	443
NDMP	NDMP host service	10000
Remote Replication	Remote replication	216 and 217
Encryption	Transparent encryption for file systems and LUNs	
Shadow Migration	Shadow data migration	
SFTP	Filesystem access via the SFTP protocol	218
TFTP	Filesystem access via the TFTP protocol	
Storage Area Network	Storage Area Network target and initiator groups	

Minimum Needed Ports

To provide security on a network, you can create firewalls. Port numbers are used for creating firewalls, and they 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 and port 217 must also be open.

NFS Authentication and Encryption Options

In addition to the appliance's capability to use Kerberos to authenticate users for administrative login and for access to services, Kerberos can also be used to set security for individual shares that use the NFS protocol.

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 User ID (UID) and Group ID (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 a 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 Data Service

When you configure a LUN on the Oracle ZFS Storage Appliance, you can export that volume over an 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 Challenge-Handshake Authentication Protocol (CHAP). Additionally, the service supports CHAP authentication data management in a Remote Authentication Dial-In User Service (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

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 Oracle ZFS Storage Appliance to perform CHAP authentication using RADIUS, the following information must match:

- The appliance must specify the address of the RADIUS server and a secret to use when communicating with this RADIUS server.
- The RADIUS server must have an entry (for example, in its clients file) that gives the address of the appliance and specifies the same secret as above.
- The RADIUS server must have an entry (for example, in its users file) 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 appliance 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 appliance 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.

SMB Data Service

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 Domain Mode Authentication

In Domain Mode, users are defined in Microsoft Active Directory (AD). SMB clients can connect to the Oracle ZFS Storage Appliance using Kerberos or NTLM authentication.

When a user connects via a fully-qualified Oracle ZFS Storage Appliance 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 appliance, 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 the appliance via a fully-qualified hostname. For more information, see this Microsoft Developer Network 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 Oracle ZFS Storage Appliance. When an SMB client connects to an appliance in Workgroup Mode, that user's username 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 appliance is in Workgroup Mode.

The following list shows the Oracle ZFS Storage Appliance 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 appliance 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

To ensure that only the appropriate users have access to administrative operations, there are access restrictions on the operations performed remotely using the Microsoft Management Console (MMC).

The following list shows the users and their allowed operations:

- **Regular Users** - List shares.
- **Members of the Administrators Group** - List opened and closed files, disconnect user connections, and view services and event log. Members of the Administrators group can also set and modify share-level ACLs.

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 Oracle ZFS Storage Appliance contacts. The external engine is not included in the appliance 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 a delay engine to prevent timing attacks. It relies on the Oracle 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.

FTP Data Service

FTP allows filesystem 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 filesystems 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. The FTP server uses either a self-signed security certificate or a customer-supplied certificate.
- **Permit Root Login** - Allows FTP logins for the root user. This is off by default because FTP authentication uses 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

HTTP Data Service

HTTP provides access to filesystems using the HTTP and HTTPS protocols and the HTTP extension Web-based Distributed Authoring and Versioning (WebDAV). This lets clients access shared filesystems through a web browser or as a local filesystem, if their client software supports it.

The HTTPS server uses either a self-signed security certificate or a customer-supplied certificate. To obtain a customer-supplied certificate, you must generate a Certificate Signing Request (CSR) and send it to the Certificate Authority (CA) for signature. After the signed certificate is returned from the CA, it can be installed on the appliance. If a certificate is signed by a non-root CA, you must also obtain certificates from the second- and higher-level CAs. For more information on certificate management, please refer to the *Oracle ZFS Storage Appliance Administration Guide.*

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 Oracle ZFS Storage Appliance denies access to clients that do not supply valid authentication credentials for a local user, an 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 appliance does not try to authenticate credentials.

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.

NDMP Data Service

The Network Data Management Protocol (NDMP) enables the Oracle ZFS Storage Appliance to participate in NDMP-based backup and restore operations controlled by a remote NDMP client called a Data Management Application (DMA). Using NDMP, appliance user data (for example, data stored in administrator-created shares on the appliance) 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 Data Service

Oracle ZFS Storage Appliance remote replication facilitates replication of projects and shares. This service enables you to view which appliances have replicated data to a specific appliance, and to control to which appliances a specific appliance can replicate.

When this service is enabled, the appliance receives replication updates from other appliances and sends 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 appliance is required to configure remote replication targets for the appliance. These targets are used to set up a replication peer connection that enables the appliances 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 appliances in subsequent communications.

The generated keys are stored persistently as part of appliance configuration. The root password is never stored persistently nor transmitted unencrypted. All appliance communications, including this initial identity exchange, are protected with SSL.

The Oracle ZFS Storage Appliance offline replication feature reduces time, resources, and potential data errors when replicating a large dataset over a network with limited bandwidth. Offline replication exports the replication stream to a file on an NFS server, which can be physically moved to the remote target site, or optionally copied to external media for shipping. At the target site, the administrator imports the file containing the replication stream to the target appliance.

To limit access to the exported replication stream, expose the NFS share only to the IP address of the source and target appliances. To encrypt the data, enable on-disk encryption for the NFS share on the NFS server. Refer to your NFS server documentation for more information. Note that an exported replication stream is never encrypted by the appliance.

Working with Data Encryption

Note - Encryption is a licensed feature. For details, refer to the "Oracle Software License Agreement ("SLA") and Entitlement for Hardware Systems with Integrated Software Options" and the Licensing Information User Manual for the software release.

Oracle ZFS Storage Appliance offers transparent data encryption for individual shares (filesystems and LUNs) and shares created inside of projects.

Managing Encryption Keys

The appliance includes a built-in LOCAL keystore and the ability to connect to the Oracle Key Manager (OKM) system. Each encrypted project or share requires a wrapping key from either the LOCAL or OKM keystores. The data encryption keys are managed by the storage appliance and are stored persistently encrypted by the wrapping key from the LOCAL or OKM keystore.

OKM is a comprehensive key management system (KMS) that addresses the rapidly growing enterprise need for storage-based data encryption. Developed to comply with open standards, this feature provides the capacity, scalability, and interoperability to manage encryption keys centrally over widely distributed and heterogeneous storage infrastructures.

OKM meets the unique challenges of storage key management, including:

- **Long-term key retention** - OKM ensures that archive data is always available, and it securely retains encryption keys for the full data life cycle.
- **Interoperability** - OKM provides the interoperability needed to support a diverse range of storage devices attached to mainframe or open systems under a single storage key management service.
- **High availability** - With active N-node clustering, dynamic load balancing, and automated failover, OKM provides high availability, whether the appliances are sited together or distributed around the world.
- **High capacity** - OKM manages large numbers of storage devices and even more storage keys. A single clustered appliance can provide key management services for thousands of storage devices and millions of storage keys.
- **Flexible Key Configuration** - Per OKM cluster, keys can be generated automatically or created individually for a LOCAL or OKM keystore. Security administrators are responsible for providing the key names which, when combined with the keystore, associate a given wrapping key with a project or share.

Maintaining Keys

Shares and projects that use OKM keys that are in a deactivated state remain accessible. To prevent an OKM key from being used, the OKM administrator must explicitly delete the key.

To ensure encrypted shares and projects are accessible, back up your appliance configurations and LOCAL keystore key values. If a key(s) becomes unavailable, any shares or projects that use that key become inaccessible. If a project key is unavailable, new shares cannot be created in that project.

Keys can become unavailable in the following ways:

- Keys are deleted
- Rollback to a release that does not support encryption
- Rollback to a release where the keys are not configured
- Factory reset
- The OKM server is not available

Encryption Key Life Cycle

The encryption key life cycle is flexible because you can change keys at any time without taking data services offline.

When a key is deleted from the keystore, all the shares that use it are unmounted and their data becomes inaccessible. Backing up keys in the OKM keystore should be performed using the OKM backup services. Backup of keys in the LOCAL keystore is included as part of the System Configuration Backup. For the LOCAL keystore, it is also possible to supply the key by value at creation time to allow it to be escrowed in an external system, which provides an alternative per-key backup/restore capability.

Shadow Migration Data Service

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 the control of the Oracle ZFS Storage Appliance user. Shadow migration mounts cannot be secure; therefore, if the server expects a Kerberos or similar request, the source mount is rejected.

SFTP Data Service

The SSH File Transfer Protocol (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.

TFTP Data Service

The Trivial File Transfer Protocol (TFTP) is a simple protocol for transferring files. It is designed to be small and easy to implement, but it 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 it currently has no provisions for user authentication.

Storage Area Network

In a storage area network (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 could result in unwanted or conflicting LUN initiators.

Directory Services

This section describes the directory services that can be configured on the appliance and their security ramifications.

Network Information Service

Network Information Service (NIS) is a name service for centralized directory management. The Oracle ZFS Storage Appliance can act as an NIS client for users and groups so that NIS users can log in to FTP and HTTP/WebDAV. NIS users can also be granted privileges for appliance administration. The appliance supplements NIS information with its own privilege settings.

Lightweight Directory Access Protocol

The Oracle ZFS Storage Appliance uses Lightweight Directory Access Protocol (LDAP) to authenticate both administrative users as well as some data services users (FTP, HTTP). LDAP-over-SSL security is supported by the appliance. 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, carries 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 Oracle ZFS Storage Appliance, the appliance 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):
  - Unsecured
  - Server is authenticated using Kerberos
  - 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, nor 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 Oracle ZFS Storage Appliance 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 (GIDs) 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 appliance.

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.

Identity Management for UNIX

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 RFC 2307, 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 a name-based mapping rule does not apply 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 Oracle ZFS Storage Appliance registration, as well as the Phone Home remote support service. No user data or metadata is transmitted in these messages.

Registration connects your Oracle ZFS Storage Appliance 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 Oracle ZFS Storage Appliance to be queried for such data 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 to expedite service calls. The Service Tags are enabled by default.

Kerberos Service

The Kerberos service offers authentication for appliance administrative login, and access to such services as NFS, HTTP, FTP, SFTP, and SSH when used in conjunction with a Kerberos environment. An appliance user must have a Kerberos principal by the same name to use Kerberos authentication for these services. Kerberos can also be used to set security for individual shares that use the NFS protocol as described in "NFS Authentication and Encryption Options" on page 14.

Both Kerberos and Active Directory can be enabled at the same time because they have distinct realms and keys. When both are active, the Kerberos realm is the default. When only Active Directory is active, its realm is the default.

Simple Mail Transport Protocol

The Simple Mail Transport Protocol (SMTP) sends all mail generated by the Oracle ZFS Storage Appliance, typically in response to configured alerts. SMTP does not accept external mail; it only sends mail generated automatically by the appliance itself.

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

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) provides two functions on the Oracle ZFS Storage Appliance: appliance status information can be served by SNMP, and alerts can be

configured to send SNMP traps. SNMP versions v1, v2c, and v3 are available when this service is enabled. The appliance supports a maximum of 128 physical and logical network interfaces.

Syslog Message

A syslog message is a small event message transmitted from the Oracle ZFS Storage Appliance to one or more remote systems. Syslog provides two appliance functions:

- Alerts can be configured to send syslog messages to one or more remote systems.
- Services on the appliance 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 appliance
- 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. The system name and location may need to be changed if the Oracle ZFS Storage Appliance is moved to a different network location or is repurposed.

Disk Scrubbing

Disk scrubbing should be performed on a regular basis to allow the Oracle ZFS Storage Appliance 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 an Oracle ZFS Storage Appliance 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.

Security Logs

This section describes logging features related to security.

Audit Log

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
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	
2013-10-11 21:13:35	root	<console>	Enabled ftp service	

Phone Home Log

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

More Information

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

https://docs.oracle.com

When you are using the BUI to configure the Oracle ZFS Storage Appliance, you can click the Help link in the top right of any screen to display the help for that screen.