Oracle® Key Manager 3

Security Guide

E49728-07
November 2019

Oracle Key Manager 3 Security Guide,

E49728-07

Contents

Preface

Documentation Accessibility vi
Related Documentation vi

1 Secure Installation and Configuration

General Security Principles 1-1
Understand Your Environment 1-2
Recommended Deployment Topologies 1-2
Securely Install the Key Management Appliance 1-3
- Considerations When Installing OKM 1-4
- Characteristics of Hardened KMAs 1-5

TCP/IP Connections and the KMA 1-6

2 Security Features

Authentication 2-1
Access Control 2-2
- Users and Role-Based Access Control 2-2
- Quorum Protection 2-2

Audits 2-3
Secure Communication 2-3
Hardware Security Module 2-4
AES Key Wrapping 2-4
Key Replication 2-4
Solaris FIPS 140-2 Security Policies 2-5
Software Upgrades 2-5
Remote Syslog 2-5
Hardware Management Pack 2-5

3 Encryption Endpoints (Agents)

Potential Threats 3-1

Encryption Endpoint Tools 3-1
Management Endpoint Tools 3-2

A Secure Deployment Checklist

List of Tables

1-1	KMA Port Connections	1-6
1-2	Other Services	1-6
1-3	ELOM/ILOM Ports	1-7

Preface

This guide describes the security features of Oracle Key Manager 3 (OKM 3). It is intended for anyone using the security features for installation and configuration. Refer to the *OKM Installation and Administration Guide* for an overview of the product.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

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.

Related Documentation

- Oracle Key Manager customer documentation: https://docs.oracle.com/en/storage/storage-software/oracle-key-manager/index.html
- *Oracle Key Manager 3 Installation and Service Manual* (internal only)
- Oracle Integrated Lights Out Manager (ILOM) documentation: http://docs.oracle.com/cd/E37444_01/
- SPARC T7-1 Server documentation: https://docs.oracle.com/cd/E54976_01/
- Netra SPARC T4-1 Server documentation: http://docs.oracle.com/cd/E23203_01/
- Oracle Hardware Management Pack documentation
  - Oracle Hardware Management Pack documentation library: http://docs.oracle.com/cd/E72066_01/
  - Oracle Single System Management: http://www.oracle.com/technetwork/server-storage/servermgmt/overview/index.html
- NIST documentation:
  - *National Institute of Standards and Technology Special Publication 800-60 Volume I Revision 1*: http://dx.doi.org/10.6028/NIST.SP.800-60v1r1
- Security policy documentation for Oracle products:
  - *Oracle Solaris Kernel Cryptographic Framework Security Policy*: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2698.pdf

  - *Oracle Solaris Userland Cryptographic Framework Security Policy*http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2699.pdf
  - *Oracle Solaris Kernel Cryptographic Framework with SPARC T4 and T5 Security Policy*: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2060.pdf
  - *Sun Cryptographic Accelerator 6000 FIPS 140-2 Security Policy*: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1050.pdf
  - *Oracle StorageTek T10000D Tape Drive Security Policy*: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2254.pdf
  - *Oracle StorageTek T10000C Tape Drive Security Policy*: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1561.pdf
  - *Oracle StorageTek T10000B Tape Drive Security Policy*: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1156.pdf
  - *Oracle StorageTek T10000A Tape Drive Security Policy*: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1157.pdf
  - *Oracle StorageTek T9480D Tape Drive Security Policy*: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1288.pdf
- FIPS validation certificates for Oracle products:
  - Sun Crypto Accelerator 6000 - Certificate #1026 (Expired) : http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1026.pdf
- Security policy documentation for nCipher nShield Solo Module
  - nCipher nShield HSM Security Policy: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp214.pdf

1

Secure Installation and Configuration

Plan for a secure installation and follow recommended deployment topologies when applicable.

- General Security Principles
- Understand Your Environment
- Recommended Deployment Topologies
- Securely Install the Key Management Appliance
- TCP/IP Connections and the KMA

General Security Principles

Follow these fundamental principles to securely use the application.

Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. The latest Oracle Key Manager upgrade packages and installers are available on the My Oracle Support website: `http://support.oracle.com`.

Restrict Network Access to Critical Services

Keep your business applications behind a firewall. The firewall provides assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls.

Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over-ambitious granting of responsibilities, roles, grants, and so on especially earlier on in an organization's life cycle when people are few and work must be done quickly, often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration, and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check the My Oracle Support website yearly for revisions.

Understand Your Environment

Ask yourself these questions to better understand your security needs.

Which resources am I protecting?

Many resources in the production environment can be protected. Consider the resources you want to protect when deciding the level of security you must provide.

The primary resource to be protected is typically your data. Other resources are outlined here because they are associated with managing and protecting your data.Various concerns with protecting data include data loss (that is, data being unavailable) and data being compromised or disclosed to unauthorized parties.

Cryptographic keys are often used to protect data from unauthorized disclosure. Thus, they are another resource to be protected. Highly reliable key management is essential to maintaining highly available data.Another layer of resources to be protected includes the assets within the Oracle Key Manager Cluster itself, including the Key Management Appliances.

From whom am I protecting the resources?

These resources must be protected from everyone who does not have authority to access them. These resources should be physically protected. You should consider which of your employees should have access to these resources. Then identify which types of operations each employee should be able to issue in the Oracle Key Manager environment?

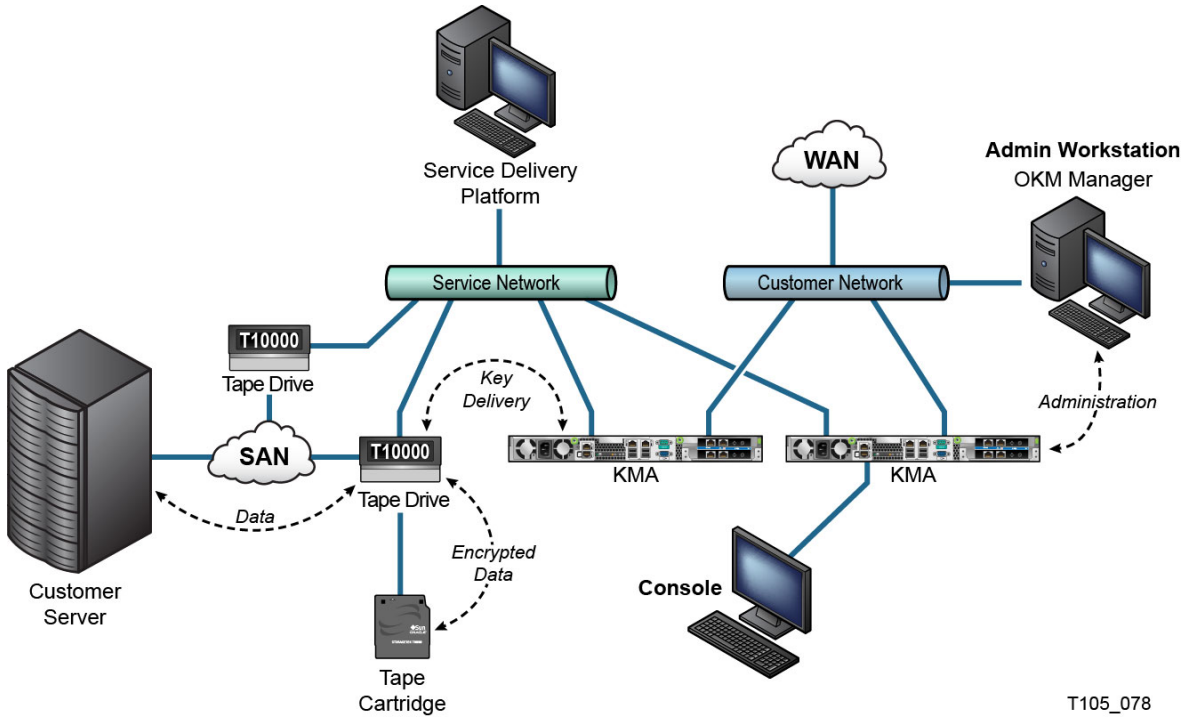
What will happen if the protections on strategic resources fail?

In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use your resources. Understanding the security ramifications of each resource will help you protect it properly.

Recommended Deployment Topologies

This figure shows a typical deployment of an Oracle Key Manager solution.

Figure 1-1 Typical Deployment of OKM Solution



Securely Install the Key Management Appliance

Follow the recommended installation and configuration process for the Key Management Appliance to ensure a secure installation.

Installing and configuring KMAs in an OKM Cluster include the following steps:

Install the KMA in a Rack

An Oracle Customer Service Engineer installs the KMA in a rack according to procedures outlined in the *Oracle Key Manager 3 Installation and Administration Guide*.

Secure the ILOM of the KMA

The customer should secure the ILOM of a KMA (possibly with guidance from an Oracle Customer Service Engineer). Oracle Key Manager KMAs are manufactured with recent ILOM firmware. The ILOM should also be secured after the ILOM firmware is upgraded. Securing the ILOM consists of setting particular ILOM settings to prevent changes to the ILOM that may compromise security. For instructions, see the ILOM appendix of the *Oracle Key Manager 3 Installation and Administration Guide*.

Secure the OpenBoot PROM or BIOs of the KMA

The customer should secure the OpenBoot PROM or BIOS of a KMA (possibly with guidance from an Oracle Customer Service Engineer). Oracle Key Manager KMAs are manufactured with recent OpenBoot PROM or BIOS firmware. It should also be secured after the firmware is upgraded. Securing the OpenBoot PROM or BIOS consists of setting particular settings to prevent changes that may compromise

security. For instructions, see the *Oracle Key Manager 3 Installation and Administration Guide*.

Configure the First KMA in the Cluster

To configure the first KMA, you must identify the split credentials and user IDs and passphrases. Refer to Quorum Protection later in this document for more information. To initialize the OKM Cluster on this KMA, follow the configure cluster procedure described in the *Oracle Key Manager 3 Installation and Administration Guide*. The key split credentials and a user with Security Officer privileges are defined during this procedure. After the QuickStart procedure is completed, the Security Officer must log in to the KMA and define additional OKM users.

Add KMAs to the Cluster

Use the QuickStart program to add a KMA to the cluster.

1. Launch the host console of your SPARC KMA from its Service Processor web interface or CLI, depending on the server type of your KMA.
2. Launch the OKM QuickStart utility within the host console.
3. To add this KMA to the OKM Cluster, follow the Join Cluster procedure described in the *Oracle Key Manager 3 Installation and Administration Guide*.

Considerations When Installing OKM

To maximize security, follow key considerations when configuring and installing OKM.

Considerations When Defining Key Split Credentials

Defining fewer key split user IDs and passphrases and a lower threshold is more convenient but is less secure. Defining more key split user IDs and passphrases and a higher threshold is less convenient but is more secure. Find a balance between security and convience.

Considerations When Defining Additional OKM Users

Defining fewer OKM users, some of whom have multiple roles assigned to them, is more convenient but is less secure. Defining more OKM users, most of whom have only one role assigned to them, is less convenient but is more secure as it facilitates tracking operations performed by a given OKM user.

Considerations When Configuring Autonomous Unlock

Using Autonomous Unlock has important security implications. For maximum security, make sure this feature is disabled. OKM offers the convenient option of Autonomous Unlock for each KMA. This option is defined during the QuickStart procedure for the first and additional KMAs in a Cluster, and the Security Officer can modified it later.

If Autonomous Unlock is enabled, then the KMA will automatically unlock itself at startup and will be ready to provide keys without requiring quorum approval. If Autonomous Unlock is disabled, then the KMA will remain locked at startup and will not provide keys until the Security Officer issues a request to unlock it and a quorum approves this request.

For maximum security Oracle discourages enabling autonomous unlock. For more information about the Autonomous Unlock option, refer to the Oracle Key Manager

Version 2.x Security and Authentication White Paper at: http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf

Characteristics of Hardened KMAs

KMAs are manufactured as hardened appliances have these key characteristics.

- Unneeded network services are not enabled. For example, ftp and telnet access is not provided.
- A host-based firewall is installed and pre-configured for intrusion prevention.
- KMAs do not produce core files.
- Users are not permitted to log in to the KMA. Attempting to log in through the system console brings up the OKM Console utility.
- The ssh service is disabled by default. For customer support purposes, the Security Officer can enable the ssh service and define a support account for a limited amount of time. This support account is the only available account and has limited access and permissions. Solaris auditing tracks commands that the support account invokes.
- The DVD drive in a SPARC KMA is uncabled. Sun Fire KMAs are not equipped with a DVD drive.
- USB ports are disabled when a KMA is booted up.
- Non-executable stacks are enabled.
- Address space lookup randomization is configured.
- Non-executable heaps are enabled.
- Filesystem-level encryption is used for security sensitive filesystems.
- Solaris is configured in accordance with the Security Compliance Automation Protocol (SCAP) Basic Solaris and PCI-DSS benchmarks. Solaris is also configured for compliance with a current version of the Solaris 11 DISA STIG. See the *OKM Administration Guide* for how to produce STIG reports for compliance auditing.
- Unnecessary Solaris services are disabled.
- The optional nCipher nShield Solo Module – a Hardware Security Module – is certified to FIPS 140-2 Level 3, therefore providing both tamper evident and tamper resistant features in addition to certified cryptographic algorithms.
- Oracle Solaris Verified Boot is configurable on SPARC T7-1 based KMAs to secure the system boot process. You can configure this feature in the ILOM to warn about or prevent the loading of corrupted kernel modules, insertion of other malicious programs masquerading as legitimate kernel modules, or installation of unauthorized kernel modules. Refer to the *Oracle ILOM Administrators's Guide for Configuration and Maintenance Firmware Release 3.2* for more information about this feature.
- The newer KMAs based on SPARC T7-1 and Netra SPARC T4-1 servers are tamper evident (ILOM fault) when the chassis door is accessed while power is applied.
- The ILOM 3.2 firmware is FIPS 140-2 Level 1 certified and may be configured in FIPS mode.

- The Solaris Basic Audit and Report Tool (BART) runs periodically to aid with forensics. These reports are included in OKM system dumps.
- The Solaris Cryptographic Security Framework is configured per the FIPS 140-2 Level 1 security policies (documented for Solaris 11.3) with or without the presence of a Hardware Security Module.

TCP/IP Connections and the KMA

If there is a firewall between the KMA and other OKM entities (such as OKM Manager, agents, and other KMAs in the same cluster), the firewall must allow the entities to establish TCP/IP connections with the KMA on specific ports.

- OKM Manager-to-KMA communication requires ports 3331, 3332, 3333, 3335.
- Agent-to-KMA communication requires ports 3331, 3332, 3334, 3335.
- KMA-to-KMA communication requires ports 3331, 3332, 3336.

> **Note:**
>
> For KMAs that use IPv6 addresses, configure IPv4-based edge firewalls to drop all outbound IPv4 protocol 41 packets and UDP port 3544 packets to prevent internet hosts from using any IPv6-over-IPv4 tunnelled traffic to reach internal hosts.
>
> Refer to your firewall configuration documentation for details. The table below lists ports KMAs explicitly use or ports on which KMAs provide services.

Table 1-1 KMA Port Connections

Port Number	Protocol	Direction	Description
22	TCP	Listening	SSH (only when Technical Support is enabled)
123	TCP/UDP	Listening	NTP
3331	TCP	Listening	OKM CA Service
3332	TCP	Listening	OKM Certificate Service
3333	TCP	Listening	OKM Management Service
3334	TCP	Listening	OKM Agent Service
3335	TCP	Listening	OKM Discovery Service
3336	TCP	Listening	OKM Replication Service

The table below shows other services listening on ports that might not be used.

Table 1-2 Other Services

Port Number	Protocol	Direction	Description
53	TCP/UDP	Connecting	DNS (only when KMA is configured to use DNS)

Table 1-2 (Cont.) Other Services

Port Number	Protocol	Direction	Description
68	UDP	Connecting	DHCP (only when KMA is configured to use DHCP)
111	TCP/UDP	Listening	RPC (KMAs respond to rpcinfo queries). This port is open to external requests only on KMS 2.1 and earlier
161	UDP	Connecting	SNMP (only when SNMP Managers are defined)
161	UDP	Listening	SNMP (only when Hardware Management Pack is enabled)
514	TCP	Connecting	Remote syslog (only when remote syslog servers are defined and configured to use TCP unencrypted)
546	UDP	Connecting	DHCPv6 (only when KMA is configured to use DHCP and IPv6)
4045	TCP/UDP	Listening	NFS lock daemon (KMS 2.0 only)
6514	TLS over TCP	Connecting	Remote syslog (only when remote syslog servers are defined and configured to use TLS)

Note:

Port 443 must be open to enable customers to access the Service Processor web interface and the OKM Console through the firewall. Refer to the *Oracle Key Manager 3 Service Manual* (internal only) to see ELOM and ILOM ports.

The table below lists the KMA ELOM/ILOM ports. These ports would be enabled if access to the ELOM/ILOM is required from outside the firewall; otherwise, they do not need to be enabled for the ELOM/ILOM IP address.

Table 1-3 ELOM/ILOM Ports

Port Number	Protocol	Direction	Description
22	TCP	Listening	SSH (for ELOM/ILOM command-line interface)
53	TCP/UDP	Connecting	DNS (only needed when DNS is configured)
68	UDP	Connecting	If DHCP is needed for the ELOM/ILOM. **Note**: Documentation for DHCP and the ELOM/ILOM is not available; although, it is supported.

Table 1-3 (Cont.) ELOM/ILOM Ports

Port Number	Protocol	Direction	Description
80	TCP	Listening	HTTP (for the ELOM/ILOM web interface) If HTTP is needed; otherwise, users can see instructions for how to connect to the remote console at: ELOM: http://docs.oracle.com/cd/E19121-01/sf.x2100m2/819-6588-14/819-6588-14.pdf ILOM: http://docs.oracle.com/cd/E37444_01
161	UDP	Listening / Connecting	SNMPv3 (configurable, this is the default port)
443	TCP /TLS	Listening	Embedded/Integrated Lights Out Manager Desktop Management Task Force (DMTF) Web services for Management Protocol (WS-Man) over Transport Layer Security (TLS)
623	UDP	Listening	Intelligent Platform Management Interface (IPMI)

2
Security Features

The OKM security features are designed to protect encrypted data from disclosure, minimize exposure to attacks, and provide sufficiently high reliability and availability.

Primary security features include:

- Authentication – Ensuring that only authorized individuals get access to the system and data
- Access Control – Control to system privileges and data; this access control builds on authentication to ensure that individuals only get appropriate access
- Audits – Allows administrators to detect attempted breaches of the authentication mechanism and attempted or successful breaches of access control.

In addition to the primary security features, there are other features to improve security of the OKM system:

- Secure Communication
- Hardware Security Module
- AES Key Wrapping
- Solaris FIPS 140-2 Security Policies
- Software Upgrades
- Remote Syslog

For more information about the security and authentication aspect of the Oracle Key Manager, refer to the *Oracle Key Manager Version 2.x Security and Authentication White Paper* at: `http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf`

Authentication

The OKM architecture provides for mutual authentication between all elements of the system: KMA to KMA, agent to KMA, and the OKM GUI or CLI to KMA for user operations.

Each element of the system (for example, a new encryption agent) is enrolled in the system by creating an ID and a passphrase in the OKM that is then entered into the element to be added. For example, when a tape drive is added to the system, the agent and KMA automatically run a challenge/response protocol based on the shared passphrase that results in the agent obtaining the Root Certificate Authority (CA) certificate and a new key pair and signed certificate for the agent. With the Root CA certificate, agent certificate, and key pair in place, the agent can run the Transport Layer Security (TLS) protocol for all subsequent communications with the KMAs. All certificates are X.509 certificates.

OKM 3.3.2 and above supports X.509v3 certificates. Renewing the OKM root CA certificate when using OKM 3.3.2+ will result in a X.509v3 certificate. For brand new

3.3.2+ OKM clusters, all entities will use X.509v3 certificates. The default signature hash algorithm used on X.509v3 certificates is SHA256.

The OKM behaves as a root certificate authority to generate a root certificate that KMAs use in turn to derive (self-sign) the certificates used by agents, users, and new KMAs. OKM 3.3.2+ allows you to reissue (renew) the root CA certificate with the existing RSA key pair.

Access Control

Access control consists of user role-based access and quorum protection.

- Users and Role-Based Access Control
- Quorum Protection

Users and Role-Based Access Control

A user's role determines their access to OKM functions.

The Oracle Key Manager provides the ability to define multiple users, each with a user ID and passphrase. Each user is given one or more pre-defined roles. These roles determine which operations a user is permitted to perform on an Oracle Key Manager system. These roles are:

- Security Officer – Performs Oracle Key Manager setup and management
- Operator – Performs agent setup and day-to-day operations
- Compliance Officer – Defines Key Groups and controls agent access to Key Groups
- Backup Operator – Performs backup operations
- Auditor – Views system audit trails
- Quorum Member – Views and approves pending quorum operations

A Security Officer is defined during the QuickStart process, which sets up a KMA in an OKM Cluster. Later, a user must log in to the Cluster as a Security Officer using the Oracle Key Manager GUI in order to define additional users. The Security Officer can choose to assign multiple roles to a particular user and can also choose to assign a particular role to multiple users.

For more information about the operations that each role allows and how a Security Officer creates users and assigns roles to them, refer to the *Oracle Key Manager Installation and Administration Guide.*

This role-based access control supports National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 operational roles to segregate operational functions.

Quorum Protection

Certain operations require the authentication of multiple users (a quorum). Requiring a quorum assures no single user can make a critical change.

Some operations are critical enough to require an additional level of security. These operations include adding a KMA to an OKM Cluster, unlocking a KMA, creating users,

and adding roles to users. To implement this security, the system uses a set of key split credentials in addition to the role-based access described above.

Key split credentials consist of a set of user ID and passphrase pairs. You must provide a minimum number of these pairs to the system to enable completion of certain operations. The key split credentials are also referred to as “the quorum" and the minimum number as “the quorum threshold."

Oracle Key Manager allows up to 10 key split user ID/passphrase pairs and a threshold to be defined. They are defined during the QuickStart process when the first KMA in an OKM Cluster is configured. The key split users IDs and passphrases are different from user IDs and passphrases that you use to log in to the system. When a user attempts an operation that requires quorum approval, the defined threshold of key split users and passphrases must approve this operation before the system performs this operation.

Audits

The KMA logs events for operations it performs. Use this log to view potential security violations.

Each KMA logs audit events for operations that it performs, including those issued by agents, users, and peer KMAs in the OKM Cluster. KMAs also log audit events whenever an agent, user, or peer KMA fails to authenticate itself. Audit events that indicate a security violation are noted. A failure to authenticate is an example of an audit event that indicates a security violation. If SNMP Agents are identified in the OKM Cluster, then KMAs also send SNMP INFORMs to these SNMP Agents should they encounter a security violation. If Remote Syslog is configured, then a KMA also forwards these audit messages to configured servers. See Remote Syslog.

A user must properly log in to the OKM Cluster and must have a role assigned to it before it is allowed to view audit events.

KMAs manage their audit events. KMAs remove older audit events based on retention terms and limits (counts). The Security Officer can modify these retention terms and limits as needed.

Secure Communication

OKM use TLS to secure communications.

The communication protocol between an agent and a KMA, a user and a KMA, and a KMA and a peer KMA is the same. In each case, the system uses the passphrase for the entity initiating the communication to perform a challenge/response protocol. If successful, the entity is provided with a certificate and its corresponding private key This certificate and private key can establish a Transport Layer Security (TLS) 1.0, 1.1, or 1.2 channel using 2048-bit RSA. The TLS protocol version is configurable for the management network and service network. Establishing this session results in the endpoints agreeing on an Advanced Encryption Standard (AES) 256-bit key. The TLS cipher suite is non-negotiable so KMA client endpoints may not negotiate a weaker suite. All subsequent communications are encrypted with this AES 256-bit key. Mutual authentication is performed; each end of any connection authenticates the other party. OKM KMAs running OKM 3.1 or later will always use TLS 1.2 for their peer-to-peer replication traffic.

Hardware Security Module

Optionally add a cryptographic card to provide a provide a FIPS 140-2 Level 3 certified cryptographic device.

KMAs can have an available Hardware Security Module (HSM), which is ordered separately. This HSM has been FIPS 140-2 Level 3 certified and provides Advanced Encryption Standard (AES) 256-bit encryption keys. Check the NIST site for certification status or contact Oracle as firmware levels change over time. The HSM supports a FIPS 140-2 Level 3 mode of operation and OKM always uses the HSM in this manner. When an HSM is installed in a KMA, encryption keys do not leave the cryptographic boundary of the HSM in unwrapped form. The HSM uses a FIPS-approved random number generator, as specified in FIPS 186-2 DSA Random Number Generator using SHA-1 for generating encryption keys.

When a KMA is not configured with an HSM card, cryptography is performed using the Solaris Cryptographic Framework (SCF) PKCS#11 soft token. Encryption keys do not leave the cryptographic boundary of the SCF in unwrapped form. The SCF is configured in FIPS 140 mode per the most recently published Solaris FIPS 140-2 security policies.

OKM release 3.3 supports two types of HSMs: the Sun Cryptographic Accelerator (SCA) 6000 card and nCipher nShield Solo Module. The SCA 6000 card was certified to FIPS 140-2 Level 3. However, this certification expired on 12/31/2015 and is not being renewed. The nCipher nShield Solo Module is available as an alternative HSM in OKM release 3.3. Either type of HSM can be installed in a SPARC KMA running this release, but a nCipher nShield Solo Module is not supported in a KMA running an older OKM release.

AES Key Wrapping

OKM uses AES Key Wrapping (RFC 3394) with 256-bit key encrypting keys to protect symmetric keys as they are created, stored on the KMA, transmitted to agents or within key transfer files.

Key Replication

When additional KMAs are added to the cluster, keys are replicated to the new KMAs.

When the first KMA of an OKM cluster is initialized, the KMA generates a large pool of keys. When additional KMAs are added to the cluster, the keys are replicated to the new KMAs and are then ready to be used to encrypt data. Each KMA that is added to the cluster generates a pool of keys and replicates them to peer KMAs in the cluster. All KMAs will generate new keys as needed to maintain the key pool size so that ready keys are always available for agents. When an agent requires a new key, the agent contacts a KMA in the cluster and requests a new key. The KMA draws a ready key from its key pool and assigns this key to the agent's default key group and to the data unit. The KMA then replicates these database updates across the network to the other KMAs in the cluster. Later, the agent can contact another KMA in the Cluster in order to retrieve the key. At no time is any clear text key material transmitted across the network.

Solaris FIPS 140-2 Security Policies

These FIPS security policies apply to the Solaris configuration used with OKM.

In August 2016, the National Institute of Standards and Technology (NIST) awarded FIPS 140-2 Level 1 validation certificate #2698 for the Oracle Solaris Kernel Cryptographic Framework module in Solaris 11.3 and awarded FIPS 140-2 Level 1 validation certificate #2699 for the Oracle Solaris Userland Cryptographic Framework. The Oracle Key Manager 3.3 KMA is based on Solaris 11.3. The Oracle Solaris Kernel Cryptographic Framework in an Oracle Key Manager 3.3 KMA is configured in accordance to the *Oracle Kernel Cryptographic Framework Security Policy*. Similarly, the KMA is also configured in accordance with the *Oracle Solaris Userland Cryptographic Framework Security Policy*. OKM will update to newer Solaris security policies as they become available.

Software Upgrades

All KMA software upgrade bundles are digitally signed to prevent loading rogue software from unapproved sources.

Remote Syslog

OKM provides support for remote syslog servers.

You can configure KMAs to send messages in RFC 3164 or RFC 5424 message format to a remote syslog server using TCP unencrypted or Transport Layer Security (TLS). RFC 5425 describes the use of TLS to provide a secure connection for the transport of syslog messages in RFC 5424 message format.

A Security Officer can configure a KMA to send messages through TCP unencrypted or TLS. It is more secure to use TLS, as TLS uses X.509 certificates to authenticate and to encrypt the communication between the KMA and a remote syslog server. The KMA authenticates the remote syslog server by requesting its certificate and public key. Optionally, you can configure the remote syslog server to use mutual authentication. Mutual authentication ensures that the remote syslog server accepts messages only from authorized clients (such as KMAs). When configured to use mutual authentication, the remote syslog server requests a certificate from the KMA to verify the identity of the KMA.

Hardware Management Pack

OKM supports the Oracle Hardware Management Pack (HMP) on SPARC T7-1, Netra SPARC T4-1 and Sun Fire X4170 M2 KMAs.

The HMP product is a member of Oracle Single System Management along with the ILOM. A Security Officer can enable the HMP on a KMA to use a management agent in Solaris to enable in-band monitoring of the KMA over SNMP. The HMP software is pre-installed but disabled with the SNMP agent configuration. Consequently, the SNMP agent listening port is not open until the HMP is enabled. The HMP is disabled by default.

Enabling the HMP provides you with:

- Event notification of hardware issues before they appear as Oracle Key Manager specific SNMP notifications or as a KMA outage.
- Ability to enable HMP on any, or all, supported KMAs in an OKM cluster.
- Ability to use read-only SNMP Get operations to SNMP MIBS on the KMA, including MIB-II, SUN-HW-MONITORING-MIB, and SUN-STORAGE-MIB.
- Oracle Red Stack integration with Oracle Enterprise Manager through SNMP Receivelets and SNMP Fetchlets.

You should keep the following security considerations in mind when you choose to enable the HMP on a KMA. When enabled, the HMP:

- Leverages any enabled, protocol v2c SNMP Managers configured in the Oracle Key Manager cluster. The SNMP v2c protocol does not have the security enhancements that appear in the SNMP v3 protocol.
- Enables a SNMP management agent on the KMA, allowing read-only network access to SNMP MIB information on this KMA.
- Security risks identified in the *Oracle Hardware Management Pack (HMP) Security Guide* (`http://docs.oracle.com/cd/E20451_01/pdf/E27799.pdf`) are mitigated by:
  - “System management products can be used to obtain a bootable root environment" - The hardening of KMAs disables root access to users of the system. SNMP is configured for read-only access. Therefore, SNMP Put operations are rejected.
  - “System management products include powerful tools that require administrator or root privileges to run" - root access to KMAs is disabled. Therefore, system users cannot run these tools.

3
Encryption Endpoints (Agents)

OKM supports a variety of encryption endpoints (also referred to as agents).

- Encryption capable tape drives
- Oracle Transparent Database Encryption (TDE) 11g and higher
- Oracle ZFS Storage Appliance
- Oracle Solaris 11 ZFS file systems

Potential Threats

Customers with encryption-enabled agents should be aware of potential threats.

- Disclosure of information in violation of policy
- Loss or destruction of data
- Unacceptable delay in restoring data in case of catastrophic failure (for example, in a business-continuity site)
- Undetected modification of data.

Encryption Endpoint Tools

Encryption endpoint tools enable applications to obtain keys from an OKM cluster.

KMS PKCS#11 Provider

KMS PKCS#11 allows certain platforms to integrate with OKM.

A KMS PKCS#11 provider, known as pkcs11_kms, accompanies the Oracle Key Manager release. An administrator can download the Linux PKCS#11 KMS provider from the My Oracle Support website and install it on an Oracle Enterprise Linux server. The KMS PKCS#11 provider has the same security characteristics and authenticates with Oracle Key Manager appliances as other agents do.

The KMS PKCS#11 provider has been integrated with various Oracle products. It is available on the following platforms:

- Oracle Solaris 11
- Oracle Solaris 10 Update 10
- Oracle Linux Server 5.5, 5.6, 5.9, and 6.5
- Oracle Database 11.2.0.2 on a supported pkcs11_kms platform and mandatory patch 12626642
- Oracle Database 11.2.0.4 on a supported pkcs11_kms platform
- Oracle Database 12.1.0.1.0 on a supported pkcs11_kms platform
- Oracle ZFS Storage Appliance running 2013.06.05.1.3 or later

The KMS PKCS#11 provider stores a log file and profile information under a configuration directory. The user or administrator should manage this log file manually or by using a utility such as logrotate. Access control to the slot configuration directory should be restricted through appropriate permissions. Within the profile directory the authentication credentials for the agent are retained within a PKCS#12 file. The PKCS#12 file is secured with a password.

The default location of this slot configuration directory depends on the operating system, as follows:

- `/var/user/$USER/kms` (Oracle Solaris 11)
- `/var/kms/$USER` (Oracle Solaris 10)
- `/var/opt/kms/$USER` (Oracle Linux Server)

For more information about the KMS PKCS#11 provider, refer to the *Oracle Key Manager Installation and Administration Guide*.

OKM JCE Provider

JCE allows developers to implement a Java client application with OKM.

A Java Cryptographic Environment (JCE) Provider, known as the OKM JCE Provider, is available for developers wishing to implement Java client applications that can obtain keys from OKM. The OKM JCE Provider has the same security characteristics and authenticates with Oracle Key Manager appliances as do other agents. The OKM JCE Provider has been integrated with various Oracle products and is available from the My Oracle Support site. For more information about the OKM JCE Provider, refer to the white paper that is distributed with it.

Management Endpoint Tools

Management endpoint tools enable system administrators and Oracle Database administrators to monitor the KMAs in an OKM Cluster.

OKM Plub-in for Oracle Enterprise Manager

The plug-in for Oracle Enterprise Manager (OEM) Cloud Control provides monitoring for OKM clusters. Each KMA belonging to a cluster is monitored by the plug-in. Refer to the *Enterprise Manager Monitoring Plug-In for OKM Install and Admin Guide*, as well as the *Enterprise Manager Monitoring Plug-In for OKM Security Guide*.

A

Secure Deployment Checklist

This checklist includes guidelines that help secure your key management system:

1. Install each KMA in a physically secure environment.
2. Secure the OpenBoot PROM or BIOS on each KMA.
3. Secure the Lights Out Manager on each KMA.
4. Define the key split configuration for this Oracle Key Manager Cluster.
5. Set the autonomous unlock setting for each KMA as appropriate.
6. Define Oracle Key Manager users and their associated roles.
7. Practice the principle of least privilege.
    a. Grant each Oracle Key Manager user only those roles as needed.
8. Monitor activity on the Oracle Key Manager Cluster.
    a. Investigate any errors, especially Security Violations, that are logged in the Oracle Key Manager audit log.
9. Back up the core security when the key split configuration is initially defined and whenever the key split configuration is modified.
10. Perform Oracle Key Manager backups on a regular basis.
11. Store core security backup files and Oracle Key Manager backup files in a secure location.
12. Set the Export Format attribute of key transfer partners to `v2.1 (FIPS)` when key sharing is used.