Oracle® Key Manager 3

Disaster Recovery Reference Guide

Release 3.0

E49726-01

January 2014

ORACLE®

Oracle Key Manager 3 Disaster Recovery Reference Guide, Release 3.0

E49726-01

Contents

List of Figures

List of Tables

Preface

This guide is intended for StorageTek representatives, customers, and anyone responsible for planning disaster recovery processes and procedures using Oracle Key Manager.

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 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.

Summary of Changes

Date	Revision	Description
January 2014	01	Updates to this revision include: ■ Support for the Netra SPARC T4-1 server. ■ Support for the T10000C, T10000D, LTO5, and LTO6 drives.

1
Introduction

Encryption is based on the science of **cryptography** and is one of the most effective ways to achieve data security today. To read an encrypted file, you must have access to the key that will enable you to decipher the file.

Disaster recovery (DR) is the process, policies, and procedures that relate to and preparing for recovery or continuation of business critical information to an organization after a natural or human-induced disaster.

Disaster recovery is a subset of a larger process known as **business continuity planning** (BCP) and should include replacing hardware, re-establishing networks, resuming applications, and restoring data.

A business continuity plan also includes non-IT related aspects such as key personnel, facilities, and communications to restore the reputation and continuity of the business.

The Oracle Key Manager (OKM) supplies a comprehensive key management platform solution designed to address the rapidly growing enterprise commitment to storage-based data encryption. Compiling with open security standards, OKM provides the capacity, scalability and interoperability to centrally manage encryption keys over widely distributed and heterogeneous storage infrastructures.

OKM is specifically designed to meet the unique challenges of storage key management including:

- **Long-term key retention** – Securely retains encryption keys for the full data lifecycle, which can exceed a decade in length. For example, some sites have their key retention period set to over 50 years.
- **Interoperability** – Provides the level of interoperability to support a diverse range of storage devices that can attach to both mainframe or open systems platforms under a single storage key management system.
- **High Availability** – Provides high availability using active N-node clustering, dynamic load-balancing, and automated failover whether the appliances are together in the same room or distributed around the world.
- **High Capacity** – Manages large numbers of storage devices and even more storage keys. A single clustered appliance pair can provide key management services for thousands of storage devices and millions of storage keys.
- **State-of-the-Technology** – Supports StorageTek's T-Series, the Hewlett Packard (HP), and International Business Machines (IBM) LTOx encryption-capable tape drives.

This chapter provides a a high-level overview of components, user roles, and the method for enabling and disabling encryption for recovery.

Architecture

The architecture for the OKM encryption solution consists of:

- **Key Management Appliance** (KMA) – A security-hardened, dual-core processor with Solaris 10 (for X2100 M2, X2200 M2, X4170 M2) and Solaris 11 (for Netra SPARC T4-1) operating system that delivers policy-based key management and key provisioning services.

  Note: The KMAs can be installed with an SCA 6000 card, which is FIPS-compliant1 at Level 3.

- **OKM Graphical User Interface** (GUI) – A stand-alone application that users run on their own system, using either a Windows–based or Solaris–based platform.
- **OKM Cluster** – A full set of KMAs in the system. All KMAs in a Cluster are aware of the other KMAs in the system and replicate this information (active/active).

  This way, if any KMA should go down, encryption operations continue.
- **Agent** (tape drive) – A device that performs encryption using keys managed by the KMA Cluster and OKM.

  Note: With the KMS 2.1 or later OKM release and the latest tape drive firmware, the following drives are FIPS-compliant[1].

[1] **FIPS** = Federal Information Processing Standards are publicly announced standards and guidelines developed by the United States Federal government. Many FIPS standards are modified versions of standards used in the wider community (ANSI, NIST, IEEE, ISO, etc.).

Tape Drive	FIPS 140-2 Level
T10000A	1
T10000B	2
T10000C	1
T10000D	1
T9840D	1
LTO4 (HP and IBM)	No plans for FIPS
LTO5 (HP and IBM)	No plans for FIPS
LOT6 (HP)	No plans for FIPS

FIPS levels of security for the above tape drives includes Levels 1 and 2.

Level 1—The lowest level with production-grade requirements.

Level 2—Adds requirements for physical tamper evidence and role-based authentication. Built on a validated operating platform.

This selection provides a higher level of security for the KMAs and tape drives.

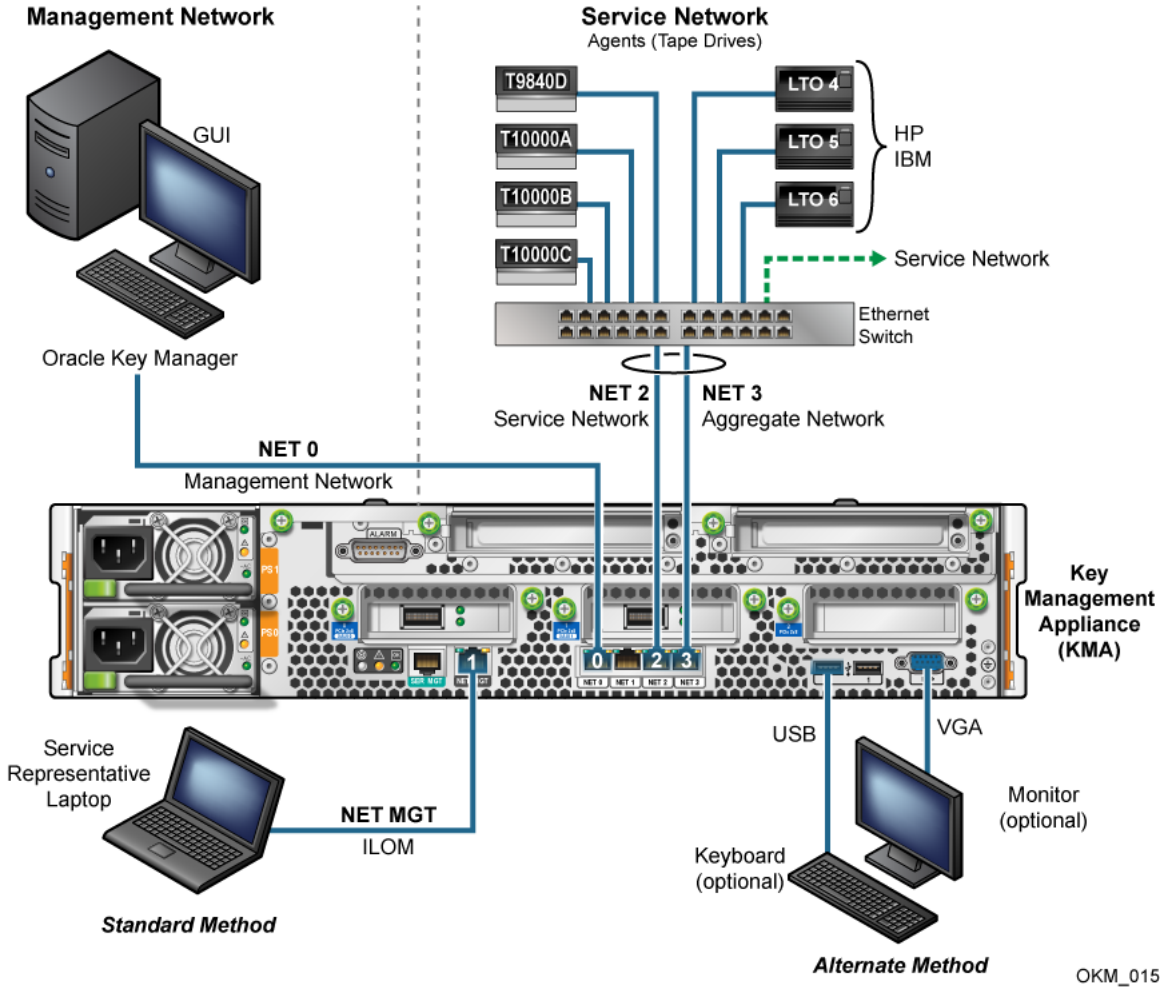
- **Data unit** – Media, a data cartridge.
- **Key Groups** – An organization for keys that associates them with a Key Policy.
- **Network connections** – The Key Management System consists of two networks:

- Management network: OKM GUI to KMAs.
- Service network: KMAs to encryption agents.

  These two networks isolate the storage devices from heavy corporate network traffic and improves the response time for key requests.

Figure 1–1 shows the rear panel and connections of a Netra SPARC T4-1 Key Management Appliance.

Figure 1–1 KMA Connections and Components



Role-Based Operations

OKM defines and uses the following roles. Completing and assigning roles is a customer task, service representatives should only advise.

Security Officer	Manages security settings, users, sites, and Transfer Partners
Compliance Officer	Manages key policies and Key Groups and determines which agents and Transfer Partners can use Key Groups
Operator	Manages agents, data units, and keys
Backup Operator	Performs backups

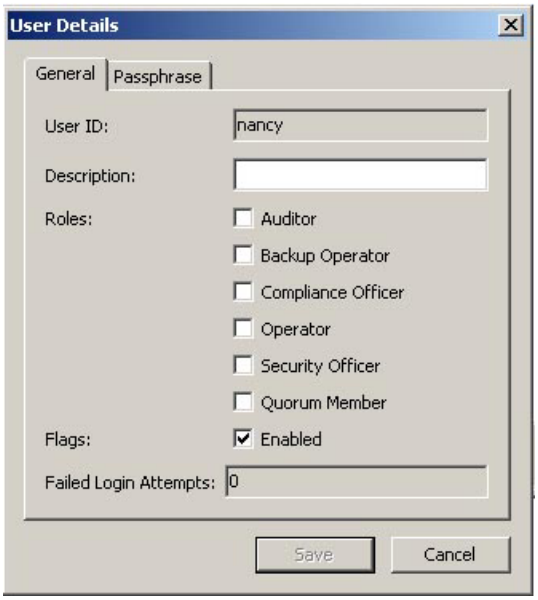
Auditor	Views information about the OKM Cluster
Quorum Member	Views and approves pending quorum operations.

Note: Each person or user may fulfill one or more of these roles. The KMA verifies that the requesting user has permission to execute an operation based on the role. Unavailable operations typically indicate the wrong role.

There are a number of basic operations a user/role can perform. Among these are: Create, Delete, Modify, and View.

Figure 1–2 shows an example of the User Detail screen.

Figure 1–2 User Roles Detail Screen



Tape Drive and Media Comparison

Table 1–1 Tape Drive and Media Comparisons

Specification	T10K-A	T10K-B	T10K-C	T10K-D	T9840D	HP LTO4	HP LTO5	HP LTO6	IBM LTO4	IBM LTO5	IBM LTO6
Capacity (native)	500 GB	1 TB	5 TB	8 TB	75 GB	800 GB	1.5 TB	2.5 TB	800 GB	1.5 TB	2.5 TB
Transfer rates (native)	120 MB/s	120 MB/s	252 MB/s	252 MB/s	30 MB/s	120 MB/s	140 MB/s	160 MB/s	120 MB/s	140 MB/s	160 MB/s
Buffer size	256 MB	256 MB	2 GB	2 GB	64 MB	256 MB	256 MB	512 MB	256 MB	256 MB	512 MB
Load Time (sec)	16	16	13.1	13	8.5	19	12	22	15	12	12
Access (sec)	46	46	57	50	8	72	60	50	46	60	96
Tape speed (m/s)	2-4.95	2-3.74	5.62	4.75	3.4	7.0	—	7.12	7.0	—	6.8

Table 1–1 (Cont.) Tape Drive and Media Comparisons

Specification	T10K-A	T10K-B	T10K-C	T10K-D	T9840D	HP LTO4	HP LTO5	HP LTO6	IBM LTO4	IBM LTO5	IBM LTO6
Rewind time (sec)	90	90	10-13	10-13	16/8	106/54	96/78	98/51	106/54	96/78	42
Unload Time (sec)	23	23	23	23	12	22	17	19	22	17	17
Interfaces											
Fibre Channel	2 & 4 Gb/s	4 Gb/s	4 Gb/s	16 Gb/s	4 Gb/s	4 Gb/s	8 Gb/s	8 Gb/s	4 Gb/s	8 Gb/s	8 Gb/s
SCSI/SAS	n/a	n/a	n/a	n/a	n/a	Ultra-320	n/a	6 Gb/s	Ultra-320	n/a	6 Gb/s
FICON FCoE	2 Gb/s	2 Gb/s	4 Gb/s	8 Gb/s 10 Gb/s	2 Gb/s	n/a	n/a	n/a	n/a	n/a	n/a
ESCON	no	no	no	no	2 Gb/s	n/a	n/a	n/a	n/a	n/a	n/a
Compatibility											
Tracks	768	1152	3,584	4,608	576	896	1,280	2,176	896	1,280	2,176
Length-usable	855 m (2805 ft)	855 m (2805 ft)	1,107 m (3,632 ft)	1,107 m (3,632 ft)	251 m (889 ft)	820 m (2690 ft)	850 m (2789 ft)	846 m (2776 ft)	820 m (2690 ft)	850 m (2789 ft)	846 m (2776 ft)
VolSafe—WORM	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes

T-Series Tape Drives

Table 1–2 shows the media compatibilities for the T-Series (T10000 and T9840) drives:

- Encryption-capable T-Series tape drives
- Non-encryption T-Series tape drives

Table 1–2 T-Series Tape Drive Media Compatibilities

Task	Enrolled for Encryption	Not Enrolled for Encryption
Write new data encrypted	Yes	No
Write new data not encrypted	No	Yes
Read encrypted data with key available	Yes	No
Read non-encrypted data	Yes	Yes
Append non-encrypted data to encrypted tape	No	No

Table 1–3 shows a comparison between the following:

- Encryption-enabled and non-encrypted tape drives
- Encrypted and non-encrypted media

Table 1–3 T-Series Tape Drive and Media Support

Tape Drive Types	Non-encrypted Media	Encrypted Media
Standard drive (non-encrypted)	■ Fully compatible ■ Read, write, and append	■ **Not capable** of reading, writing to or appending to this tape ■ Can re-write from the beginning of tape (BOT)

Table 1–3 (Cont.) T-Series Tape Drive and Media Support

Tape Drive Types	Non-encrypted Media	Encrypted Media
Encryption-capable drive	■ **Read** capability only ■ Not capable of appending to this tape ■ Can re-write from the beginning-of-tape (BOT)	■ Fully compatible ■ Read with correct keys ■ Write with current write keys

LTO Tape Drives

Both HP and IBM LTO tape drives are:

- Specified to interchange with un-encrypted data cartridges from other tape drives that comply to the LTO U-28, U-316 and U-416 specifications.
- Capable of interchanging encrypted data cartridges provided the correct encryption key is available.

Future compatibility:

In the future, LTO drives will be capable of:

- Reading and writing tapes from the current generation
- Reading and writing tapes from *one* earlier generation
- Reading tapes from *two* earlier generations

Note: Encryption is only supported with LTO4, LTO5, and LTO6 data cartridges on LTO4, LTO5, and LTO6 tape drives. To avoid problems, these drives will not write in normal or native modes once the drive is enabled for encryption.

Enabling and Disabling Encryption

The following are requirements that apply to encryption:

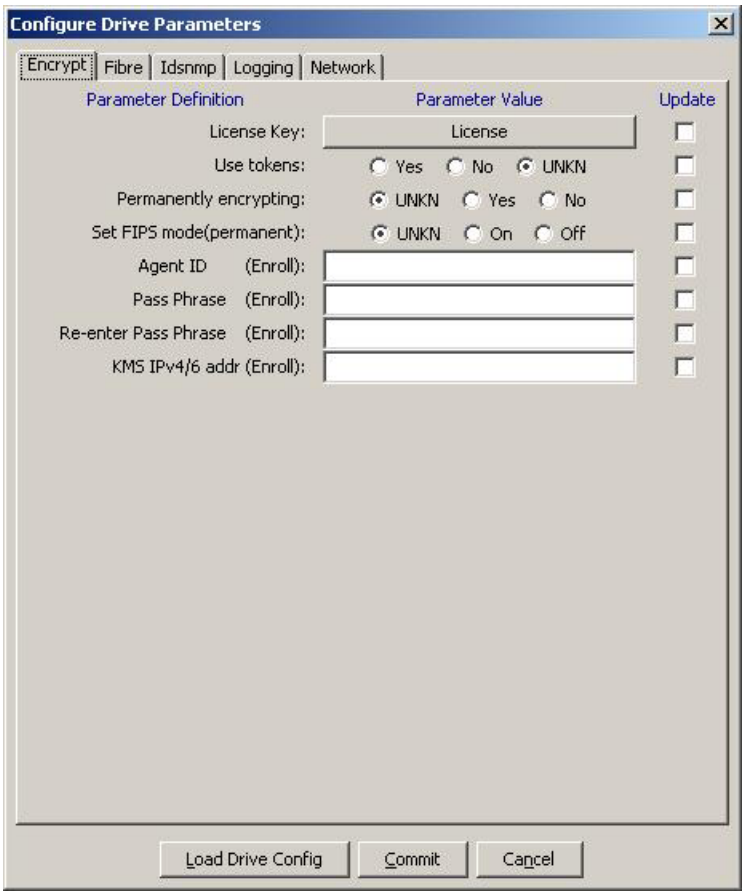
- The T10000 tape drives must be at a minimum firmware level of 1.37.114.
- The service representatives must install the Hardware Activation Keys for the tape drives, and have the required levels of the Virtual Operator Panel (VOP) available.
- The customers, partners, and disaster recovery (DR) sites must use the current Customer version of the virtual operator panel (VOP) 1.0.12 or higher.

Enrolling the T-Series Tape Drives

During the initial T-Series tape drive enrollment process, the customer has the chance to configure the tape drives to:

- Use Tokens, with an air gap configuration and KMS Version 1.x
- Select if the drive can be switched between encryption and non-encryption modes
- Select FIPS mode
- Enter Agent values for the Key Management System
- Enroll IPv4 and IPv6 addressing

Figure 1–3 T-Series Enrollment Selections



Use tokens
Select:

- Yes if using KMS Version 1.x
- No if using KMA Version 2.x or 3.x.

Permanently encrypting
Select:

- Yes if permanent (cannot disable)
- No, if switchable.

Set FIPS mode (Version 2.1 and later)
Enter the values for:

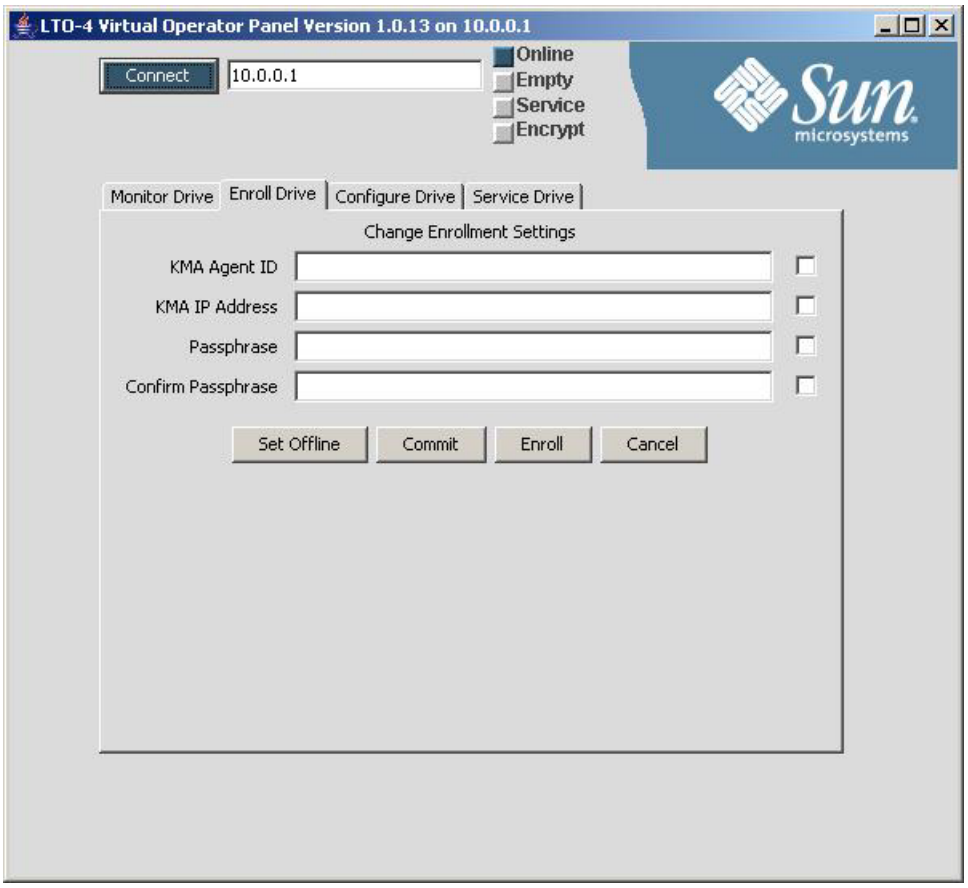
- Agent ID:
- Pass Phrase:
- OKM IP address of the appliance.

Enrolling the LTO Tape Drives

The enrollment process and the VOP screens are different for LTO tape drives. The Enroll Drive tab allows the initial enrollment of the tape drives.

Once enrolled, the tab and Enroll button change to Unenroll.

Figure 1–4 LTO Enrollment Selections



2

Component Recovery

OKM uses a Cluster design that requires at least two KMAs[1]. This design helps reduce the risk of disrupting business continuity.

In addition, some design and safe-guard requirements are in place to assist in component recovery.

Clustering KMAs allows for replication of database entries and workload balancing. In the unlikely event that a component should fail, it can be easily replaced and restored to operation.

While designing an encryption and archive strategy, an important design guideline is to make sure that critical data generated at any site is replicated and vaulted off-site. This is described in Chapter 3, "Data Recovery".

This chapter provides information about replacing components in the OKM.

KMA Outage

A single KMA can be recovered without any impact to the rest of the Cluster as long as at least one KMA remains operational. The following sections address scenarios that require recovery of a single KMA.

Software Upgrade

Software upgrades do not imply a repair or a recovery; however, sometime during this action a KMA will be out of service as the upgrade takes place.

An upgrade can be done without interrupting the active encryption agents.

- Downloading the new software can be done concurrently on all KMAs in the Cluster.
- Activating of the new software requires a reboot of the KMA server.

  Therefore, rebooting the KMAs in the Cluster must be staggered so that at least one KMA is active at all times.

As each KMA returns to an online status, any database updates done while the KMA was offline are replicated and all KMAs in the Cluster are re-synchronized.

[1] **Multiple Servers**: Exceptions to this standard configuration *must* be made with the approval of OKM Engineering and Global Support Services.

Network Disconnect

When a KMA is disconnected from the management network, such as when new software is activated, the remaining KMAs in the Cluster continue to attempt to contact it and report communication errors in the audit event log.

Agents continue to communicate with other KMAs across the network. Usually these are other KMAs attached to the same service network. However, because Agents may be attached to the management network, they first attempt to work with KMAs in their own configured site; but if need be, they will contact any reachable KMAs within the Cluster.

When the KMA is reconnected to the network, any database updates done while the KMA was disconnected are replicated and all KMAs in the Cluster are re-synchronized.

Hardware Failure

If a hardware failure occurs, first the KMA should be deleted from the Cluster so that the remaining KMAs will no longer attempt to communicate with it.

If the KMA console is still accessible, you can reset the KMA. The reset operation will return the unit to its factory defaults. This operation offers the option to scrub the server's hard disk as an extra security precaution. Disposition of the failed server is handled by the customer.

A replacement KMA server is configured and added to the Cluster as described in the Oracle Key Manager System Installation and Service Manual, PN E48395-01.

Once the new KMA is added to the Cluster:

- The database is replicated.
- The KMAs in the Cluster are re-synchronized.
- The new KMA becomes an active member of the Cluster.

Component Configuration

Table 2–1 Component Configuration

Account Name:			
Security Officers:			
Quorum Members:			
Site Location:	KMA S/N:	KMA Name:	KMA Firmware Level:
KMA IP Address:		Service Network IP:	
OKM Manager IP:		ELOM/ILOM IP:	
NTP | Yes__No__IP:		DHCP | Yes__No__	
Gateway | Yes__No__IP:		DNS | Yes__No__IP:	
IPv6 Yes__No__		Domain:	
Address:		Hostname:	
KMA Number:		Number of KMAs in Cluster:	

Table 2–1 (Cont.) Component Configuration

KMA Location:		OKM Manager Location:	
Configuration Types:	SL8500 library SL3000 library SL500 library 9310 library L700/1400 library	Tape Drive Types:	T10000A tape drive T10000B tape drive T10000C tape drive T10000D tape drive T9840D tape drive HP LTO tape drive IBM LTO tape drive
Site Location:	KMA S/N:	KMA Name:	KMA Firmware Level:
KMA IP Address:		Service Network IP:	
OKM Manager IP:		ELOM/ILOM IP:	
NTP | Yes__No__IP:		DHCP | Yes__No__	
Gateway | Yes__No__IP:		DNS | Yes__No__IP:	
IPv6 Yes__No__		Domain:	
Address:		Hostname:	
KMA Number:		Number of KMAs in Cluster:	
KMA Location:		OKM Manager Location:	
Configuration Types:	SL8500 library SL3000 library SL500 library 9310 library L700/1400 library	Tape Drive Types:	T10000A tape drive T10000B tape drive T10000C tape drive T10000D tape drive T9840D tape drive HP LTO tape drive IBM LTO tape drive

3

Data Recovery

Disaster recovery is the process, policies, and procedures that relate to preparing for recovery or continuation of business critical information to an organization after a natural or human-induced disaster. This includes:

- **Recovery Point Objective** (RPO): The point in time to recover data as defined by a business continuity plan. This is generally a definition of what the business determines is an "acceptable loss" in a disaster situation. This could be in hours, days, or even weeks.
- **Recovery Time Objective** (RTO): The duration of time that a business process must be "restored" after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. This could be minutes when using a combined service network. See Figure 3–2.

The OKM can span multiple, geographically-separated sites. This greatly reduces the risk of a disaster destroying the entire Cluster. Clustering KMAs allows for replication of database entries and workload balancing. Although unlikely that an entire Cluster needs to be recreated, most of the key data can be recovered by recreating the OKM environment from a recent database backup.

When designing an encryption/archive strategy, one very important design element is that critical data generated at any site is replicated and vaulted at a recovery site.

If a site is lost, this backup data may be transferred to another operational site. Data units and keys associated with tape volumes will be known to the KMAs at the sister site, and encrypted data required to continue business operations will be available.

The damaged portion of the Cluster can be restored easily at the same or a different location once site operations resume.

Many companies employ the services of a third-party disaster recovery (DR) site to allow them to restart their business operations as quickly as possible. Periodic unannounced DR tests demonstrate the company's degree of preparedness to recover from a disaster, natural or human-induced. A number of possible scenarios exist, some are discussed here.

Shared resources	Provide cost-efficient elements for disaster recovery
Replication	Restoration through replication from intact KMAs
Scenario 1	Pre-positioning KMAs
Scenario 2	Sharing KMAs
Scenario 3	Key Transfers
Scenario 4	Restore from Backup

Backup Methodology	Some guidelines that might help

Backup and Key Sharing Considerations

OKM backups and key sharing (import/export) are database intensive and reduce response time on the KMA while it is performing the backup or key transfer operation.

If possible, reduce tape drive workloads during the OKM backup and transfer window.

If that is not possible, then consider the following options:

- OKM backups and key transfers can occur on any KMA but best practice would be to use the same KMA each time. Most likely this is how cron jobs invoking the OKM backup utility will get set up anyway.
- If the Cluster is large enough then a KMA may be dedicated as an administrative KMA.
  - This KMA should not have a service network connection so it would not be burdened with tape drive key requests at any time, especially during the backup or key transfer windows.
  - This KMA could also be used for OKM GUI sessions thus offloading the other KMAs from handling management related requests.
- The faster the management network connectivity of the backup and key transfer KMA, the better it will be able to keep up with the additional load during backup and key transfer windows.

  This is true for all KMAs, but especially for the KMA performing backups as it will fall behind on servicing replication requests during the backup window. Having a fast network connection will help to minimize the replication backlog, such as lag.
- Put the backup and key transfer KMA in a site that is not used by tape drives. The tape drives then preference other KMAs within the site that they have been assigned and avoid using the backup and key transfer KMA.
- Add more KMAs to the sites containing tape drives so that load balancing of key requests will occur across more KMAs. This reduces the number of key requests that the backup and key transfer KMA has to handle.

Key Pool Size Determination

OKM administrators should know the worst case number of keys they expect to be created per unit of time and the duration of the OKM backup windows or key transfer windows.

For this discussion we'll assume an hourly rate of key consumption has been calculated.

> **Note:** KMAs pre-generate keys so a key creation request from an agent does not actually cause a key to be created on the KMA until the key pool maintainer runs within the server. When the server is busy the key pool maintainer can be delayed in its operations.

The total Cluster keypool size must be large enough so that KMAs can hand out pre-generated keys from their key pool during the backup windows.

When the key pool size is too small, KMAs can get drained of pregenerated keys and start returning no ready key errors. Tape drives failover to other KMAs when this happens and it adds further disruption to the performance challenges of the backup/key transfer window.

The default key pool size of 1000 keys should be sufficient for most customers unless the estimated worst case key creation rate for the backup windows exceeds this.

The OKM backup window should be observed periodically as it will gradually grow as the database gets larger. Adjustments to the key pool size may be necessary when the backup window exceeds a threshhold. The key pool size should also be adjusted if the key consumption rate grows due to changes in the overall tape workload.

Shared Resources

Shared resources can provide cost-efficient elements for disaster recovery.

Companies that specialize in records management, data destruction, and data continuity and recovery, purchase equipment that several customers can use for various reasons including backup and archive.

For disaster recovery, the customer can use tape drives, libraries, and other resources of a shared resource site for short periods of time, either to do a disaster recovery test or an actual recovery from a disaster.

There are two approaches for disaster recovery and key management.

- The customer can place KMAs at the DR site and configure these into their production Cluster using a WAN connection. These KMAs are dedicated to the specific customer and allow the customer's keys to always be at the DR site and ready for use.

  With this approach, a recovery can begin once the customer enrolls the tape drives in the KMAs at the shared resource site and joins the OKM Cluster.

  This can be done by connecting the OKM GUI to the KMAs at the DR site. In a true disaster recovery scenario, these may be the only remaining KMAs from the customer's Cluster.

  Drive enrollment can be completed within minutes. Once the enrollment is complete, and the drives have been configured tape production can begin.

- Another method is to restore the backups of the customer's production OKM into KMAs provided by the shared resource site. This avoids the need for a wide area network (WAN) link and the on-site, dedicated KMAs but requires additional time to restore the database.

  With this approach, the restore operation requires both normal OKM backup files and a Core Security backup. This restore approach requires a quorum of the Key Split Credential members for the core security backup.

  Restore operations take about 20 minutes per 100,000 keys.

  After the restore is completed, the drives must be enrolled and configured.

  Three files are needed to take to a DR site:

  – Core Security backup file

  – .xml backup file

  – .dat backup file

  These files are created by a Backup Officer.

Replication from Another Site

Figure 3–1 and Figure 3–2 show examples of two geographically separate sites, one OKM Cluster with four KMAs in the Cluster, two KMAs at each site.

During the initial install, after the first KMA is configured, any additional KMAs—new or replacements—self-replicate from the other KMAs in the Cluster.

Recovery of a single KMA can be accomplished with no impact to the rest of the Cluster as long as at least one KMA remains operational.

Figure 3–1 is an example of a Recovery Point Objective. In this example, a point in time to recover business continuity to an entire site could take months.

- If Site 1 were destroyed and Site 2 is still intact:

  The customer must replace all the destroyed equipment for the infrastructure, including the KMAs for the Cluster and the tape drives.

  Once the site is restored and functional:

  – Install and create the new KMAs (requires a Security Officer and Quorum).
  – Join the Existing Cluster, one at a time, for the new KMAs.
  – Install and activate the new tape drives.
  – Enroll the new tape drives, now called Agents.

  Site 1 then self-replicates from the surviving KMAs at the intact Site 2.

Figure 3–2 is an example of a Recovery Time Objective. In this example, the amount of time to recover business continuity is a matter of minutes.

- If the KMAs at Site 1 were destroyed, and the infrastructure at Site 2 is still intact:

  A Wide Area “Service” Network that connects the tape drives between the two sites allows the intact KMAs from Site B to continue tape operations between both sites.

  Once the KMAs are replaced at Site 1, they would then self-replicate from the surviving KMAs at the intact Site 2 similar to the description above.

  During the QuickStart program the customer selects:

  ```
  (2) Join Existing Cluster
  ```

  one at a time for each of the new KMAs.

Figure 3–1 Replication from Another Site—Recovery Point Objective

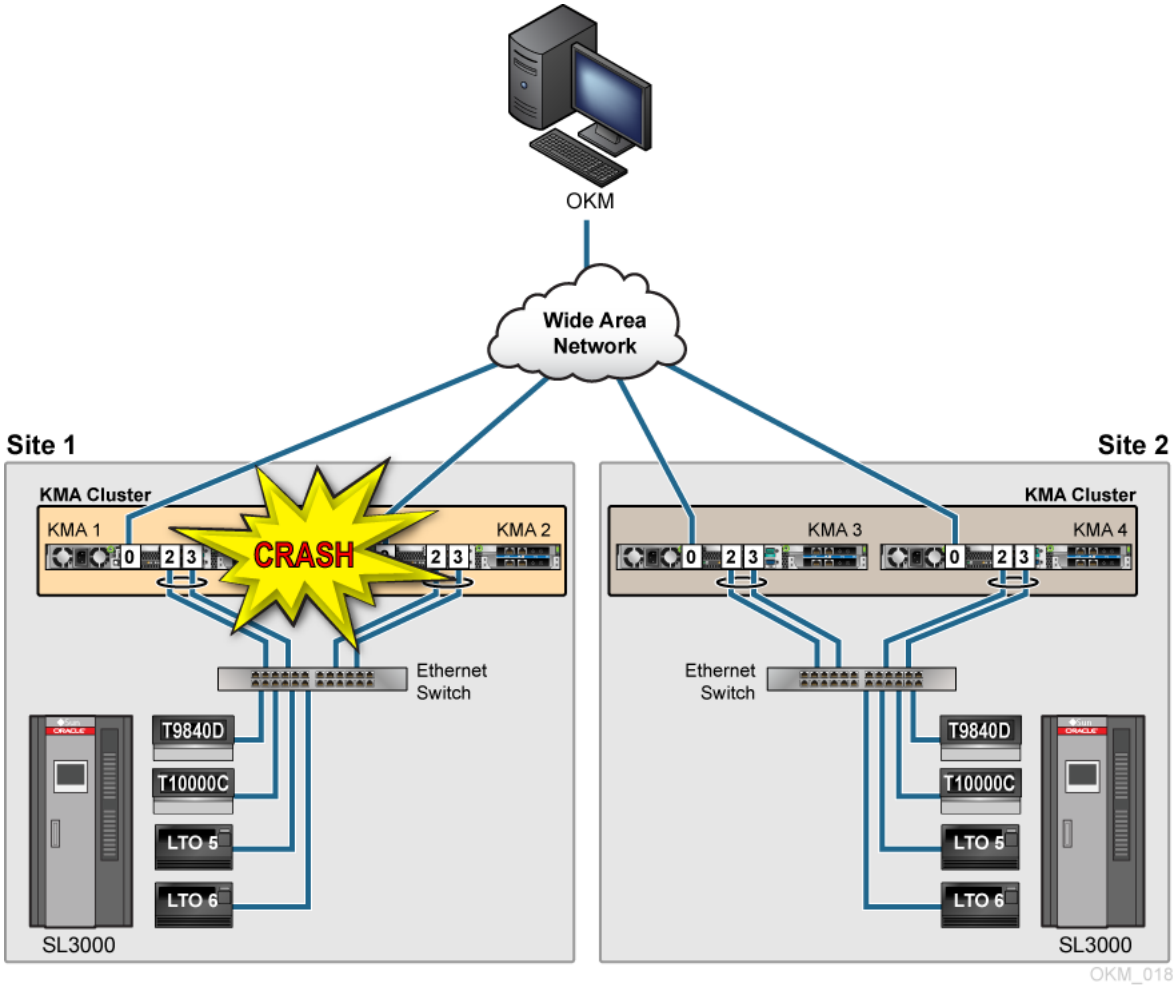
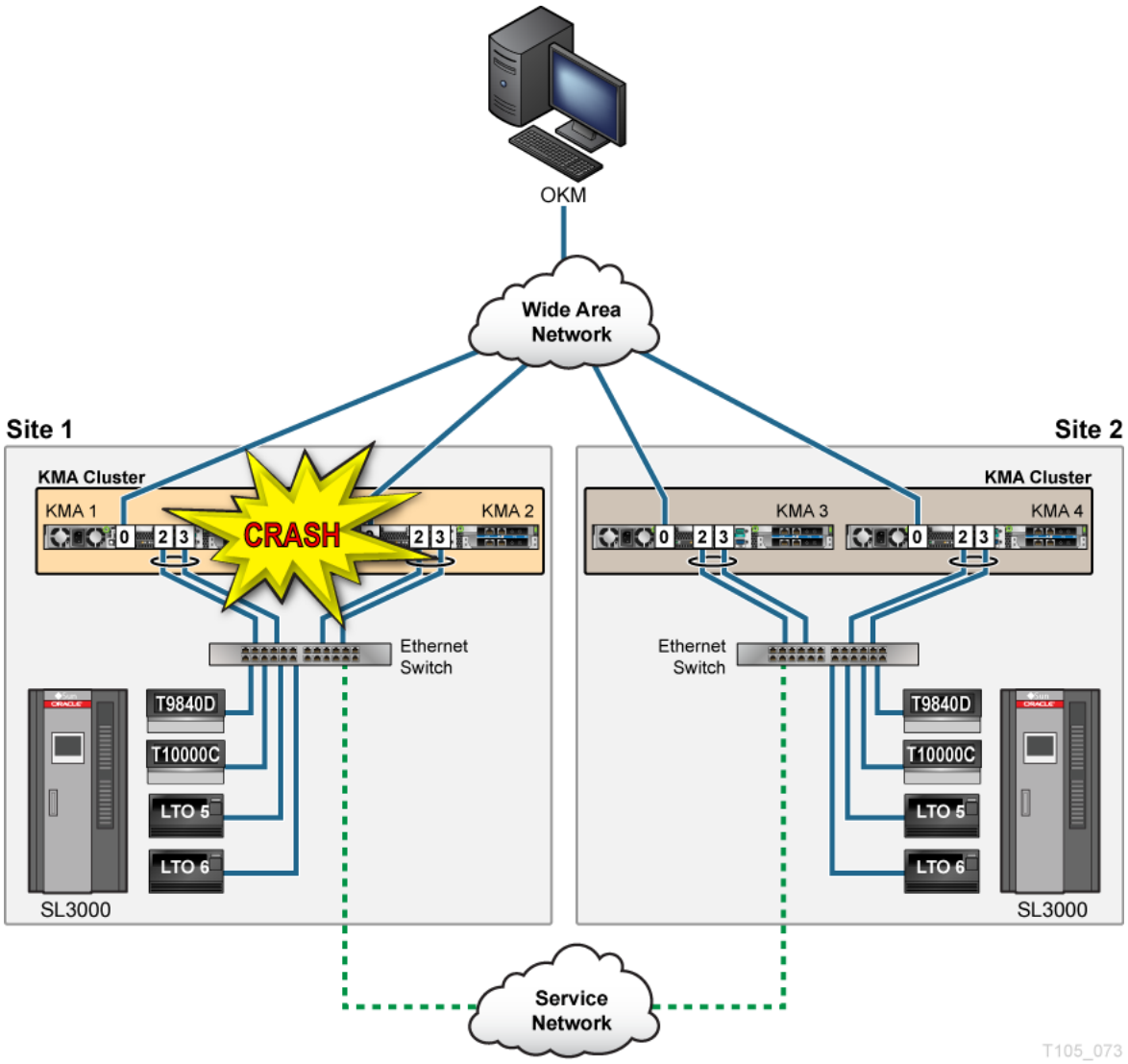


Figure 3–2 Service Network Continuation—Recovery Time Objective



Scenario 1: Pre-positioned KMAs

In this scenario, the customer has a big environment with multiple sites. Each site uses:

- A pair of KMAs and the infrastructure to support automated tape encryption
- A single Cluster where all KMAs share keys.

Along with the multiple sites, this customer also maintains and uses equipment at a Disaster Recovery (DR) site that is part of the customer's OKM Cluster.

See Figure 3–3 for this scenario.

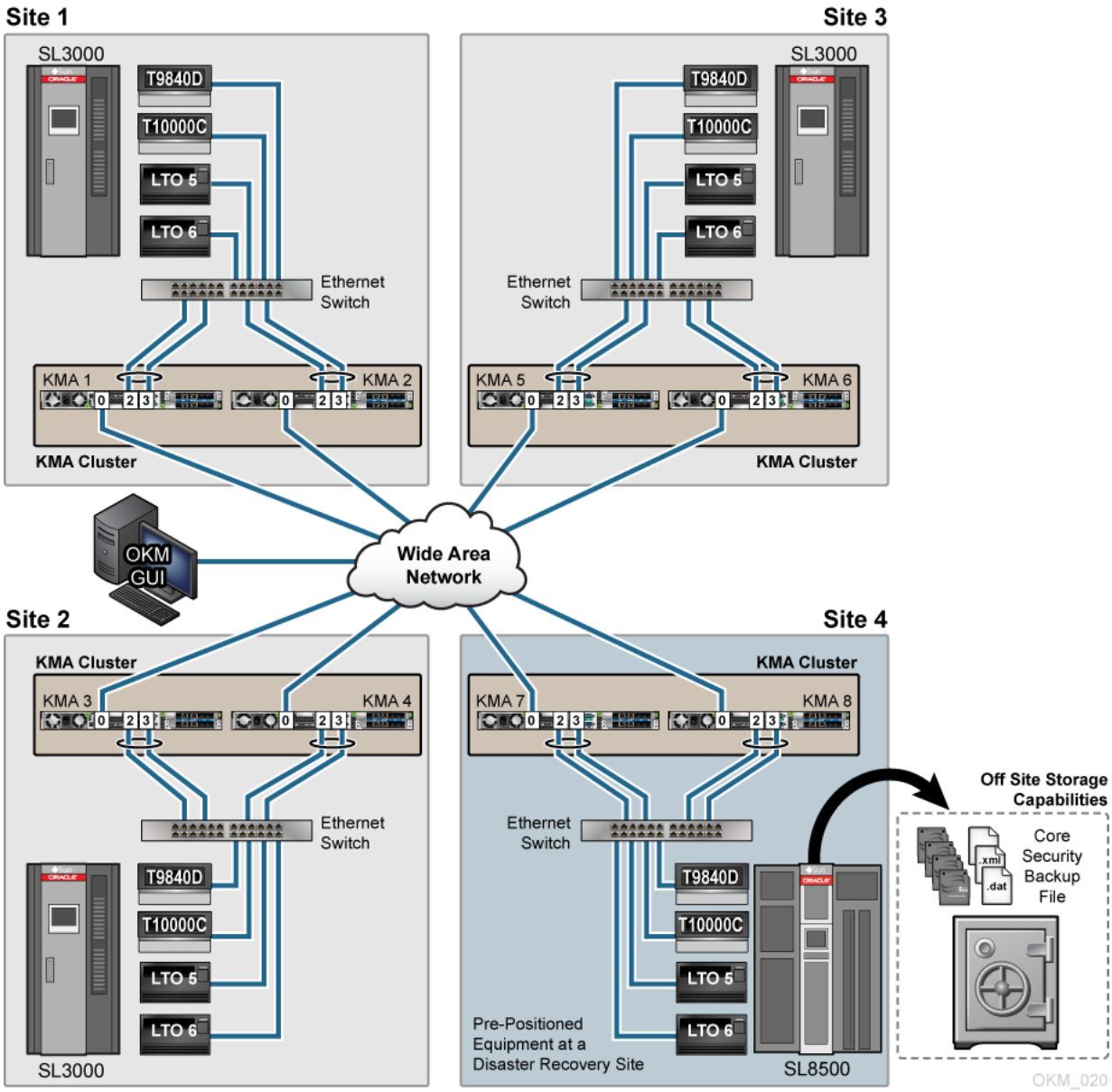
This customer uses a simple backup scheme that consists of:

- Daily incremental backups
- Weekly differential backups
- Monthly full backups.

The monthly backups are duplicated at the DR site and sent to an off-site storage facility for 90 days. After the 90-day retention period, the tapes are recycled.

Because the customer owns the equipment at the DR site, this site is just an extension of the customer that strictly handles the back-up and archive processes.

Figure 3–3 Pre-positioned Equipment



Scenario 2: Shared KMAs

This scenario is very similar to Scenario 1: Pre-positioned KMAs; however, the Disaster Recovery site owns the equipment and is sharing the resources with several other customers.

See Figure 3–4 for this scenario.

Because this Disaster Recovery site supports other DR clients, you cannot assume the site is always configured for encryption-capable processes.

Note: The KMAs must be reset to factory settings before creating a configuration for a different customer.

At the DR site,

- The customer selects the appropriate equipment from the DR site inventory.
- The DR site configures the equipment and infrastructure accordingly.

Important: The customer must provide the DR site with the three OKM back-up files:

- Core Security backup file
- .xml backup file
- .dat backup file

At the DR sites, the customer

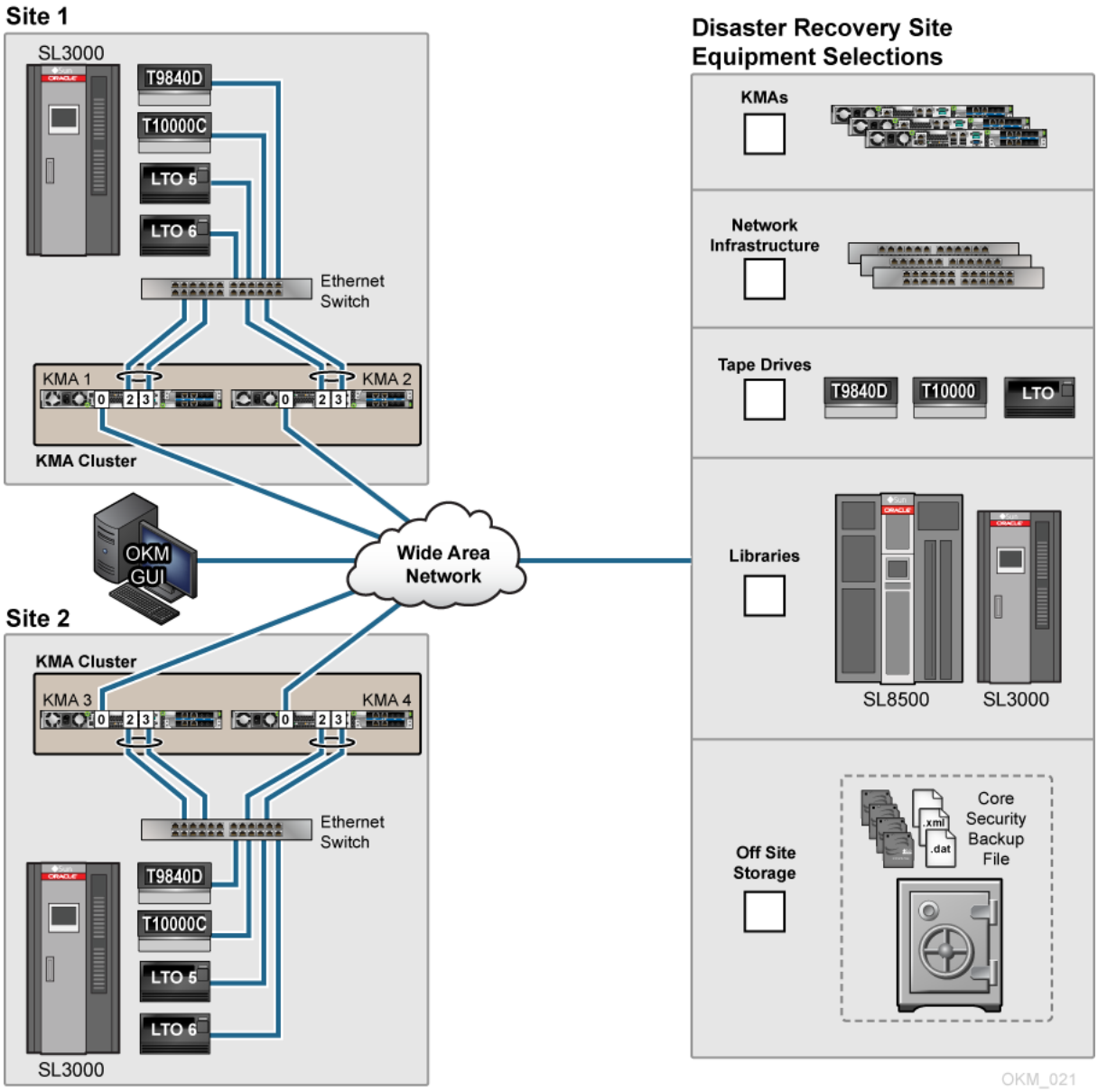
- Configures an initial KMA using the QuickStart Wizard
- Restores the KMA from the OKM back-up files
- Activates, enables, or switches the drives to encryption-capable (DR representatives)
- Enrolls the tape drives into the DR site KMA Cluster.

Once the job is done, the Disaster Recovery site needs to:

- Switch-off encryption from the Agents
- Remove the tape drives from the Cluster or reset the drives passphrase
- Reset the KMAs to factory default.

Disconnect the infrastructure and network.

Figure 3–4 Shared KMAs



Scenario 3: Key Transfer Partners

Key Transfer is also called Key Sharing. Transfers allow keys and associated data units to be securely exchanged between Partners or independent Clusters and is required if you want to exchange encrypted media.

> **Note:** A DR site may also be configured as a Key Transfer Partner.

This process requires each party in the transfer to establish a public/private key pair. Once the initial configuration is complete:

- The sending party uses Export Keys to generate a file transfer.
- The receiving party then uses Import Keys to receive the keys and associated data

As a practice, it is not recommended to use Key Transfer Partners for Disaster Recovery. However, if or when DR sites create keys during the backup process, doing a key transfer can incrementally add the DR sites keys to the already existing data base.

The Key Transfer process requires each user to configure a Transfer Partner for each OKM Cluster.

- One Transfer Partner *exports* Keys from their OKM Cluster.
- The other Transfer Partner *imports* Keys into their OKM Cluster.

When configuring Key Transfer Partners, administrators must perform tasks in a specific order that requires several roles, including:

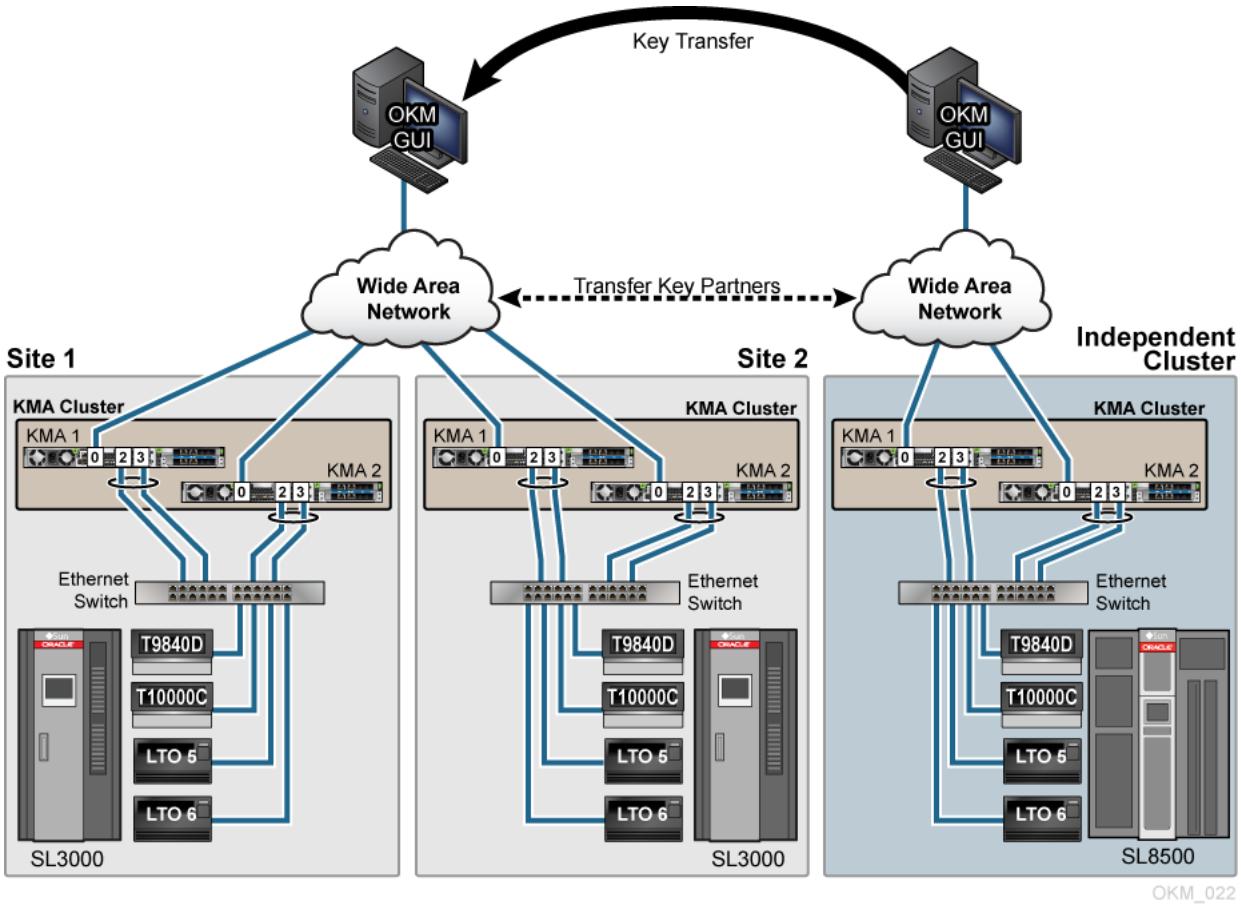
- Security Officer role
- Compliance Officer role
- Operator role.

To configure Key Transfer Partners, refer to the OKM Administration Guide and:

1. Configure a Key Transfer Partner for both OKM Clusters participating in key exchange.
2. Establish a public/private key exchange to communicate with the OKM Clusters. For example, in case of sending an e-mail, two sites can use an established communication method to secure an e-mail exchange and authenticate its source and recipient.

   There are mechanisms, such as the fingerprint, in place to prevent modification of this information during transit.
3. Gather a quorum to approve the creation of the new Transfer Partner.
4. Assign the Transfer Partner to one or more Key Groups.
5. Export keys from one OKM Cluster and import them into another. This can be done many times.

Figure 3–5 Transfer Key Partners



Scenario 4: Restore From Backup

A backup refers to making copies of data so that they can be used to restore the original after a disaster or other event where the data has been lost.

These copies are typically called "backups," which serve to:

- Restore a site following a disaster (disaster recovery)
- Restore files after they have been accidentally deleted or corrupted

It is important to recognize and use a backup scheme that works for each a department, group, organization, or business. It is also important to have confidence that the backup process is working as expected.

For the OKM, the following are available to help create, and, when necessary, restore the OKM.

- Backup

  A file created during the backup process that contains all the information needed to restore a KMA. This file is encrypted with a "key" generated specifically for the backup. This key is contained in the corresponding backup key file.

- Backup Key File

  A file generated during the backup process that contains a key used to encrypt the backup file. This file is encrypted using a system "master key." The master key is

extracted from the Core Security backup file using a quorum for the key split credentials.

- Backup Operator

  A user role that is responsible for securing and storing data and keys.

> **Note:** See "Backup Methodology" on page 3-13 for more information.

Backup Locations:

Keep in mind that the OKM backup location should be at a site that is safely located at a suitable distance, such that a single building fire does not destroy all the data. The distance should also take into account natural disasters.

For example, if all the backup sites are located in buildings across New Orleans, the destruction of data is unavoidable in a Katrina-like disaster.

Restore:

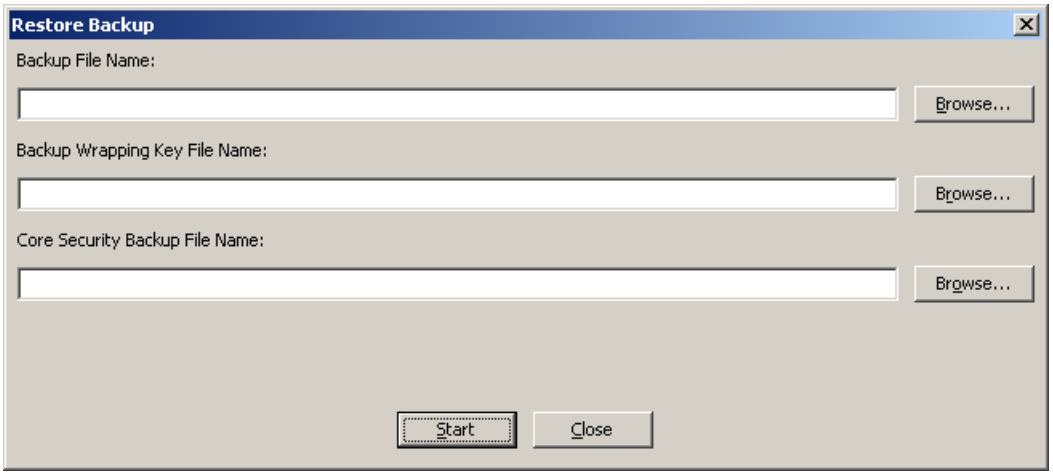
A restore from backup is only required if all KMAs in the Cluster have failed, such as if a site is destroyed by fire.

> **Note:** Restoring the OKM from a backup requires a Quorum. The Backup Operator creates and maintains backups and the Security Officer restores them. Make sure the required number of Quorum users are available.

To restore the system from a backup, refer to the *OKM Administration Guide* and:

1. Select Secure Information Management > Backup List. This allows you to view the history and details of the backup files.
2. From the Backup List screen, highlight the Backup you want to restore from and double-click the Backup entry. The Backup Details dialog box is displayed.
3. Click on the Restore button. The Restore Backup dialog box is displayed.

Figure 3–6 Restore from Backup



4. Click on the Start button.

When the upload completes, the Key Split Quorum Authentication dialog box appears.

The Core Security Backup Quorum must type their user names and pass phrases to authenticate the operation.

5. Click on the OK button. A progress display of the restore is indicated.

Backup Methodology

Remember, each customer and each situation is different. Here are some guidelines that might help:

Backup frequency. There are two types of backups handled differently:

- **Core Security Backup**, which must be secured using special tactics.
- **Database Backup** of the Key Data, which needs to be protected.

Core Security Backup

The Core Backup contains a primary component for the OKM, the Root Key Material. It is this key material that is generated when a Cluster is initialized. The Root Key Material protects the Master Key, a symmetric key that protects the Data Unit Keys stored on the KMA.

The Core Security backup is protected with a key split scheme that requires a quorum of users defined in the Key Split Credentials. This quorum of users must provide their usernames and passphrases to unwrap the Root Key Material.

Methodology:

The Core Backup must precede the first Database Backup and then this core backup only needs to be repeated when members of the Key Split change (quorum). This is a security item handled and protected specially. This is required to restore any backup of the OKM.

As a best practice, keep two copies of this backup in two secure locations on a portable media of the customers choice, such as CDs, USB memory sticks, or external hard drives.

When a new Core Backup is created and secured, the old ones should be destroyed.

Database Backup

Note: Backup Operators are responsible for securing and storing data and their keys.

A Database Backup consists of two files: a Backup file and a Backup Key file. These filenames are automatically generated, however, you can edit the names.

Each KMA creates 1000 keys (default) when created. This may vary during installation. Each KMA controls and assigns its own keys. After issuing 10 keys the KMA creates 10 keys to replenish them.

Keys are then replicated to all KMAs in the OKM.

Database Backups are encrypted with AES-256; and therefore, secure.

Methodology:

Example One: Database Backup — Multiple Sites in the OKM Cluster

- Keys are protecting keys against corruption.
- Keys are being protected by replication.

The customer should never need a total disaster recovery of the Cluster because of the geographically placed data centers. Creating backups for this customer are not as critical as Example Two; however, create a core security backup, then database backups before all generated keys from a single KMA are issued to Data Units.

Example Two: Database Backup — One Physical Site in a OKM Cluster

- A localized disaster may destroy the entire OKM.
- Database backups are the only protection for the keys.

Maintain offsite copies of the Core Security and Database backups. For bare minimum protection:

Table 3–1 Database Backup Calculations

1.	Calculate how many tapes will be initially encrypted using one key per tape.	
2.	How many hours, days, or weeks will it take to issue the initially created keys? Note: Each KMA creates 1000 keys (default) when created	
3.	Calculate how many tapes mounted will have an expired key encryption period?	
4.	Add these two calculations together	
5.	Assume only one KMA issues all the keys and backup the database before the initial keys are all issued. This provides a 50% safety factor to the calculation.	
6.	Repeat this calculation based on new tape influx and Re-use the encryption period expiration.	

Things to consider:

- Archive copies or do not archive copies.
- Remember old backups contain users, passwords, and other sensitive data you may not want to keep.
- Make and archive two current database backups in case of backup media failure.
- Because you computed a 50 percent safety factor assuming that only one KMA was issuing keys, either backup contains all the active keys.
- Never archive old copies of Database.
- If you routinely delete keys for policy or compliance reasons, the deleted keys can be recovered from prior backups.
- Keep redundant copies. Do not create two backups.
- Make two identical copies to protect against backup media failure. This scheme also ensures another key was not issued during the backup, making the two copies different.