# Oracle® Key Vault Installation and Upgrade Guide





Oracle Key Vault Installation and Upgrade Guide, Release 21.10

G12111-06

Copyright © 2021, 2025, Oracle and/or its affiliates.

Primary Author: Puneet Rai

Contributing Authors: Monika Sharma, Sunil Surabhi, Prakash Jashnani, Mark Doran, Patricia Huey

Contributors: Alexis Abell, Bharathi Baskaran, Lalitha Chowdary, Shubham Goyal, Fahad Ibrar, Rahil Mir, Dongwon Park, Radhika Siravara, Ajay Srivastava, Peter Wahl

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

	Audience	V		
	Documentation Accessibility	V		
	Diversity and Inclusion	V		
	Related Documents	V		
	Conventions	vi		
	Changes in This Release for Oracle Key Vault			
	Changes for Oracle Key Vault Release 21.10	vii		
	Changes for Oracle Key Vault Release 21.6	Vİİ		
	Changes for Oracle Key Vault Release 21.4	i>		
	Changes for Oracle Key Vault Release 21.2	Х		
1	Introduction to Installing and Upgrading Oracle Key Vault			
	About Oracle Key Vault Installation and Upgrade	1-1		
	Oracle Key Vault Deployment Options	1-2		
	Privileges Required for Performing Oracle Key Vault Installations and Upgrades	1-2		
	Oracle Key Vault Pre-Installation Checklist	1-3		
2	Oracle Key Vault Installation Requirements			
	System Requirements	2-1		
	Additional or Third-Party Software	2-3		
	Network Port Requirements	2-3		
	Supported Endpoint Platforms	2-5		
	Endpoint Database Requirements	2-5		
3	Downloading Oracle Key Vault Software			
	Downloading the Oracle Key Vault Software for Fresh Installation	3-1		
	Downloading the Oracle Key Vault Software for Upgrade	3-2		



nstalling Oracle Key Vault	
ownloading the Oracle Key Vault Appliance Software	4-1
stalling the Oracle Key Vault Appliance Software	4-2
Requirements for root and support User Passwords	4-5
erforming Post-Installation Tasks	4-6
Cloning Oracle Key Vault Installation	
loning Oracle Key Vault Virtual Machines	5-1
uidelines for Cloning on Virtual Machines	5-2
Jpgrading a Standalone Oracle Key Vault Server	
bout Upgrading a Standalone Oracle Key Vault Server	6-1
tep 1: Back Up the Server Before You Upgrade	6-2
tep 2: Perform Pre-Upgrade Tasks for the Standalone Oracle Key Vault	6-2
tep 3: Add Disk Space to Extend the vg_root for the Release 21.10 Upgrad	de 6-6
tep 4: Upgrade the Oracle Key Vault Server	6-8
About Upgrading an Oracle Key Vault Server	6-8
Upgrading a Standalone Oracle Key Vault Server	6-8
tep 5: If Necessary, Add Disk Space to Extend Swap Space	6-11
tep 6: If Necessary, Remove Old Kernels	6-13
tep 7: If Necessary, Remove SSH-Related DSA Keys	6-15
tep 8: Upgrade the Endpoint Software	6-15
tep 10: Back Up the Upgraded Oracle Key Vault Server	6-19
Jpgrading Oracle Key Vault from an Earlier 21.x Relea Naster Cluster Environment	ase in a Multi-
bout Upgrading Oracle Key Vault from an Earlier 21.x Release in a Multi-Nnvironment	Master Cluster 7-1
tep 1: Perform Pre-Upgrade Tasks for the Upgrade from the Earlier 21.x R	
tep 2: Upgrade Each Multi-Master Cluster Node	7-6
tep 3: If Necessary, Change the Network Interface for Upgraded Nodes	7-9
tep 4: Check the Node Version and the Cluster Version	7-9
tep 5: If Necessary, Add Disk Space to Extend Swap Space	7-9
tep 6: If Necessary, Remove Old Kernels	7-12
tep 7: If Necessary, Remove SSH-Related DSA Keys	7-13
tep 8: Upgrade the Endpoint Software	7-13
top o. Opgrade the Enapolit Soltware	7-14



## Upgrading a Primary-Standby Oracle Key Vault Server 8 About Upgrading a Primary-Standby Oracle Key Vault Server 8-1 Step 1: Back Up the Server Before You Upgrade 8-2 Step 2: Perform Pre-Upgrade Tasks for the Primary-Standby Oracle Key Vault 8-2 Step 3: Add Disk Space to Extend the vg root for the Release 21.10 Upgrade 8-6 Step 4: Upgrade the Oracle Key Vault Primary-Standby Pair 8-8 About Upgrading an Oracle Key Vault Server Primary-Standby Pair 8-8 Upgrading a Pair of Primary-Standby Oracle Key Vault Servers 8-8 Step 5: If Necessary, Add Disk Space to Extend Swap Space 8-11 Step 6: If Necessary, Remove Old Kernels 8-13 Step 7: If Necessary, Remove SSH-Related DSA Keys 8-15 Step 8: Upgrade the Endpoint Software 8-16 Step 9: Back Up the Upgraded Oracle Key Vault Server 8-19 Getting Started Using Oracle Key Vault After the Installation or Upgrade 9 Logging In to the Oracle Key Vault Management Console 9-1 Overview of the Oracle Key Vault Management Console 9-1 Performing Actions and Searches 9-2 **Actions Menus** 9-2 Search Bars 9-2 Α Hyper-V Installation on Windows Hyper-V Installation A-1 Tablespace Encryption for Oracle Key Vault B Tablespace Encryption for Oracle Key Vault Upgraded from 12.2.0.3.0 or Before B-1 Index



## **Preface**

Welcome to *Oracle Key Vault Installation and Upgrade Guide*. This guide explains how to install and upgrade Oracle Key Vault.

- Audience
- Documentation Accessibility
- Diversity and Inclusion
- Related Documents
- Conventions

## **Audience**

*Oracle Key Vault Installation and Upgrade Guide* is written for Oracle Key Vault administrators who are responsible for installing or upgrading Oracle Key Vault.

# **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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

# **Diversity and Inclusion**

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

## **Related Documents**

For more information, see these resources:

- Oracle Key Vault Administrator's Guide
- Oracle Key Vault Root of Trust HSM Configuration Guide



- Oracle Key Vault RESTful Services Administrator's Guide
- Oracle Key Vault Developer's Guide
- Oracle Key Vault Licensing Information
- Oracle Key Vault Release Notes
- Key Management Interoperability Protocol Specification Version 1.1

To download the product data sheet, frequently asked questions, links to the latest product documentation, product download, and other collateral, visit Oracle Technical Resources (formerly Oracle Technology Network). You must register online before using Oracle Technical Services. Registration is free and can be done at

https://www.oracle.com/technical-resources/

## Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.



# Changes in This Release for Oracle Key Vault

This Oracle Key Vault release introduces new features that enhance the use of Oracle Key Vault in a large enterprise.

- Changes for Oracle Key Vault Release 21.10
   Oracle Key Vault release 21.10 introduces several new features.
- Changes for Oracle Key Vault Release 21.6
   Oracle Key Vault release 21.6 introduces new features that affect this guide.
- Changes for Oracle Key Vault Release 21.4
   Oracle Key Vault release 21.4 introduces new features that affect this guide.
- Changes for Oracle Key Vault Release 21.2
   Oracle Key Vault release 21.2 introduces new features that are related to installation and upgrade operations.

# Changes for Oracle Key Vault Release 21.10

Oracle Key Vault release 21.10 introduces several new features.

Configurable Oracle Key Vault Ports
 Starting with Oracle Key Vault release 21.10, you can now configure the ports used to communicate between read/write peers and connect to Oracle Key Vault remotely using SSH.

## Configurable Oracle Key Vault Ports

Starting with Oracle Key Vault release 21.10, you can now configure the ports used to communicate between read/write peers and connect to Oracle Key Vault remotely using SSH.

Oracle Key Vault uses port 1522 to communicate between read/write peers. The SSH service running on port 22 allows for remote administration of Oracle Key Vault. For certain deployments, it may not be possible to configure the network to allow ingress or egress traffic on these default ports. You can now configure these ports to non-default values for cluster operations and administrative maintenance.

# Changes for Oracle Key Vault Release 21.6

Oracle Key Vault release 21.6 introduces new features that affect this guide.

- Ability to Clone an Oracle Key Vault VM
   Starting with Oracle Key Vault release 21.6, a fresh installation of an Oracle Key Vault VM guest can be stored as a template, and the VM platform cloning capability can be used to clone Oracle Key Vault cluster nodes.
- Oracle Key Vault Operating System Upgrade to Oracle Linux 8
   In Oracle Key Vault release 21.6, the embedded operating system is upgraded to Oracle Linux 8.

## Ability to Clone an Oracle Key Vault VM

Starting with Oracle Key Vault release 21.6, a fresh installation of an Oracle Key Vault VM guest can be stored as a template, and the VM platform cloning capability can be used to clone Oracle Key Vault cluster nodes.

With Oracle Key Vault cluster, using the cloned template, the system administrator can significantly shorten the provisioning time, compared to performing a full installation of each individual cluster node.

Oracle Key Vault supports the cloning feature of the underlying virtualization platform. This eliminates the need to go through the full installation process for each individual cluster node. You can clone an Oracle Key Vault system (installed as a VM) after the installation is complete, but before performing post-installation tasks. When a clone is started up for the first time, it goes through a series of steps to regenerate system-specific configuration that makes it unique (and separate from all other clones). The (remote) cloning capability provided by virtualization platforms allows to clone from an Oracle Key Vault **Template**, which is an Oracle Key Vault installation that is stopped before this Oracle Key Vault is made unique. It regenerates all of the system-specific configuration; the clone becomes unique by completing the remaining installation steps.

## Oracle Key Vault Operating System Upgrade to Oracle Linux 8

In Oracle Key Vault release 21.6, the embedded operating system is upgraded to Oracle Linux 8.

Before attempting an Oracle Key Vault upgrade confirm with your vendor that your Oracle Key Vault servers (for installations on dedicated hardware) are compatible with Oracle Linux 8.

# Changes for Oracle Key Vault Release 21.4

Oracle Key Vault release 21.4 introduces new features that affect this guide.

- Ability to Control the Extraction of Symmetric Encryption Keys from Oracle Key Vault
  Starting in Oracle Key Vault release 21.4, to strengthen the protection of symmetric
  encryption keys, you now can restrict these keys from leaving the Oracle Key Vault cluster
  boundary.
- Ability to Restrict Oracle Key Vault Administrative Role Grants
   Starting in Oracle Key Vault release 21.4, you can control whether a grantee of an Oracle Key Vault administrative role can grant the role to other Oracle Key Vault users.

# Ability to Control the Extraction of Symmetric Encryption Keys from Oracle Key Vault

Starting in Oracle Key Vault release 21.4, to strengthen the protection of symmetric encryption keys, you now can restrict these keys from leaving the Oracle Key Vault cluster boundary.

This restriction applies to the key material of the symmetric keys, but not its metadata. For example, Transparent Database Encryption (TDE) master encryption keys are stored in Oracle Key Vault. When an endpoint needs to decrypt the key, the PKCS#11 library fetches the TDE master encryption key from Oracle Key Vault to perform the decryption. If your site requires that symmetric keys never leave Oracle Key Vault, then you can configure these keys to remain within Oracle Key Vault during operations. In this case, the PKCS#11 library will send



the encrypted data encryption key to Oracle Key Vault. Decryption is then performed within Oracle Key Vault and afterward, the plaintext data encryption key is returned to the PKCS#11 library. The Oracle Key Vault PKCS#11 library performs the encryption and decryption operation within Oracle Key Vault if the TDE master encryption key is restricted to leave Oracle Key Vault, or if it cannot be extracted from Oracle Key Vault.

To control whether symmetric encryption keys can be retrieved (extracted) from Oracle Key Vault, you can use the Oracle Key Vault management console, RESTful services utility commands, the C SDK APIs, and Java SDK APIs.

The following Oracle Key Vault RESTful services utility commands have been updated to accommodate this enhancement:

- okv managed-object attribute get
- okv managed-object attribute get-all
- okv managed-object attribute list
- okv managed-object attribute modify
- okv managed-object key create
- okv managed-object key register
- okv managed-object object locate

#### New APIs for the C SDK to manage extractable attribute:

- okvAttrAddExtractable
- okvAttrAddNeverExtractable
- okvAttrGetExtractable
- okvAttrGetNeverExtractable

#### New APIs for the Java SDK to manage extractable attribute:

- okvAttrAddExtractable
- okvAttrAddNeverExtractable
- okvAttrGetExtractable
- okvAttrGetNeverExtractable

#### **Related Topics**

- Managing the Extraction of Symmetric Keys from Oracle Key Vault
- Configuring the Global Default Extraction for New Symmetric Keys

## Ability to Restrict Oracle Key Vault Administrative Role Grants

Starting in Oracle Key Vault release 21.4, you can control whether a grantee of an Oracle Key Vault administrative role can grant the role to other Oracle Key Vault users.

In previous releases, the Oracle Key Vault administrative roles (System Administrator, Key Administrator, and Audit Manager) could be granted to another Oracle Key Vault user by any user who currently has the role. Starting with this release, when an administrator grants the role to another user, the administrator can restrict how the grantee user can in turn grant the role to other users. This enhancement improves overall user security and helps to adhere to good least privileges practices.



## **Related Topics**

· About Administrative Roles in Oracle Key Vault

# Changes for Oracle Key Vault Release 21.2

Oracle Key Vault release 21.2 introduces new features that are related to installation and upgrade operations.

 Changes in the Oracle Key Vault Management Console
 In Oracle Key Vault release 21.2, the Oracle Key Vault management console user interface has had minor changes throughout.

## Changes in the Oracle Key Vault Management Console

In Oracle Key Vault release 21.2, the Oracle Key Vault management console user interface has had minor changes throughout.

These changes are the result of modified terms, updates to the current release, and enhancements for better usability. The overall interface has not had major changes.



1

# Introduction to Installing and Upgrading Oracle Key Vault

Installing Oracle Key Vault entails ensuring that the environment meets the necessary requirements before you begin the installation and configuration.

- About Oracle Key Vault Installation and Upgrade
   Oracle Key Vault is a software appliance that is delivered as an ISO image.
- Oracle Key Vault Deployment Options
   You can deploy an Oracle Key Vault multi-master cluster on dedicated hardware or as VM quests.
- Privileges Required for Performing Oracle Key Vault Installations and Upgrades
   Oracle Key Vault requires users to have specific privileges to perform installations and upgrades.
- Oracle Key Vault Pre-Installation Checklist
   The pre-installation checklist covers all the requirements to successfully install Key Vault.

# About Oracle Key Vault Installation and Upgrade

Oracle Key Vault is a software appliance that is delivered as an ISO image.

The software appliance consists of a pre-configured operating system, an Oracle database, and the Oracle Key Vault application. You can install Oracle Key Vault on-premises on its own dedicated hardware, as a VM guest into your virtualization platform, or as a compute instance in your OCI tenancy (from the Oracle Cloud Marketplace at https://cloudmarketplace.oracle.com/marketplace/app/OracleKeyVault), and as a compute instance in Microsoft Azure and Amazon AWS.

In this release, you can follow the upgrade paths:

• Oracle Key Vault release 21.x (for example, 21.2) to the current release, Oracle Key Vault 21.10.

Before you begin the installation or upgrade process for Oracle Key Vault, check the *Oracle Key Vault Release Notes* for any known issues that you should be aware of.



Introducing changes to the Oracle Key Vault underlying platform is not recommended. Any changes made to the core platform could prevent the Oracle key Vault software appliance to function effectively. If you make any changes, you are at your own risk and Oracle cannot guarantee proper functioning of the software appliance.

# Oracle Key Vault Deployment Options

You can deploy an Oracle Key Vault multi-master cluster on dedicated hardware or as VM guests.

- A standalone deployment is simplest to deploy. However, it does not provide continuous
  availability of the key service in the event an Oracle Key Vault server becomes unavailable.
  When you first install Oracle Key Vault, it is in a standalone environment. From there, you
  can configure Oracle Key Vault to be in a multi-master cluster configuration. Oracle
  recommends that you extend the OKV installation to a multi-master cluster with at least
  two nodes (one read/write pair).
- A multi-master cluster configuration allows for up to 16 nodes (an Oracle Key Vault server that has been converted to be a member of an Oracle Key Vault multi-master cluster) and is recommended for deployments requiring high availability. This is the recommended deployment for many reasons, such as data compatibility between nodes, fault tolerance, zero data loss, no passive machines in the system, scalability, and maintenance.
- Oracle Key Vault can be deployed on a physical server or a VM guest on a virtualized platform. Some capabilities of the virtualization platforms, such as (live) cloning of the Oracle Key Vault cluster nodes, or pausing of the cluster nodes, can lead to system instabilities and are therefore not supported.
- You can move an Oracle Key Vault server on a virtualized platform to a physical hardware using the below steps.

In a multi-master cluster environment:

- Install the Oracle Key Vault server (of the same version) on your preferred compatible hardware
- Add the new Oracle Key Vault server to the cluster as the new node
- Delete the existing cluster node that is on the virtualized platform.

For the standalone deployment:

 Use the backup to restore into a new standalone Oracle Key Vault server created on a physical hardware.

### **Related Topics**

Oracle Key Vault Administrator's Guide

# Privileges Required for Performing Oracle Key Vault Installations and Upgrades

Oracle Key Vault requires users to have specific privileges to perform installations and upgrades.

You should have the following privileges:

- For a fresh installation: Privileges to log in to the Oracle Software Delivery Cloud portal to download the current Oracle Key Vault installation software.
- The root privilege for the server where you will perform the installation or upgrade
- For upgrade of an existing Oracle Key Vault deployment: Privileges to log in to the Oracle Support portal to download the current Oracle Key Vault upgrade software.



 For performing upgrades, in addition to the preceding privileges, you must have the Oracle Key Vault System Administrator role to disable and re-enable the upgraded Oracle Key Vault cluster node.

# Oracle Key Vault Pre-Installation Checklist

The pre-installation checklist covers all the requirements to successfully install Key Vault.

Table 1-1 Oracle Key Vault Pre-Installation Checklist

Item#	Check	Task
1. [ x ]	New changes or issues that you should be aware of	See Oracle Key Vault Release Notes
2. [ x ]	System requirements	Confirm that you have enough CPU, memory, and disk as described in System Requirements.
3. [ x ]	Open all the required network ports in your firewall	For details on network ports, see Network Port Requirements.
4. [ x ]	Supported endpoint platforms	See Supported Endpoint Platforms.
5. [x]	Set the COMPATIBLE initialization parameter for the online master encryption key (previously TDE direct connect).	Guidance for setting this parameter for Oracle Database 12.1.0.2 or later is in Supported Endpoint Platforms.
6. [ x ]	Get a fixed IP address, network mask, gateway, and NTP addresses from your network administrator.	You will need this information for Step in Installing the Oracle Key Vault Appliance Software



# Oracle Key Vault Installation Requirements

The Oracle Key Vault installation requirements cover areas such as CPU, memory, disk space, network interfaces, and supported endpoint platforms.

#### System Requirements

System requirements include CPU, memory, disk, network interface, and hardware compatibility.

## Network Port Requirements

Network port requirements includes requirements for SSH/SCP, SNMP, HTTPS, listeners, KMIP, and TCP ports.

## Supported Endpoint Platforms

Oracle Key Vault supports both UNIX and Windows endpoint platforms.

#### Endpoint Database Requirements

Administrators can use online master encryption keys and the Oracle Database COMPATIBLE initialization parameter to manage Oracle Database endpoints.

# System Requirements

System requirements include CPU, memory, disk, network interface, and hardware compatibility.

The Oracle Key Vault installation removes existing software on a server.

You can install Oracle Key Vault on dedicated servers, as guests into your virtualization platform, or as a guest into a compute instance in your Oracle Cloud Infrastructure (OCI) tenancy, deployed in minutes from the Oracle Cloud Marketplace. Visit the following site:

https://cloudmarketplace.oracle.com/marketplace/app/OracleKeyVault

The minimum hardware requirements for deploying Oracle Key Vault on dedicated hardware or as VM guests are:

- **CPU**: Minimum: x86-64 16 cores. Recommended: 24-48 cores with cryptographic acceleration support (Intel AESNI).
- Memory: Minimum 16 GB of RAM. Recommended: 32–64 GB.

## Note:

- Oracle Key Vault does not support fiber channel storage with multipath for the boot disk.
- You can add more RAM to the Oracle Key Vault systems, but you cannot reduce the RAM size lower than the original system configuration. System memory reduction is not supported in Oracle Key Vault.
- Disk: Minimum 2 TB. Recommended: 6 TB.

Both BIOS and UEFI boot mode. For a system with a disk size greater than 2 TB, Oracle Key Vault supports booting in UEFI mode only.

- Network interface: One or two network interfaces.
- Hardware Compatibility: Any Intel x86 64-bit hardware platform supported by Oracle Key Vault's embedded operating system. Oracle Key Vault uses Oracle Linux 8 with the Unbreakable Enterprise Kernel (UEK) version 6. For a list of compatible hardware, refer to Hardware Certification List for Oracle Linux and Oracle VM in the Related Topics. This list contains the minimum version of Oracle Linux certified with the selected hardware. All Oracle Linux updates starting with Oracle Linux release 8 as the minimum are also certified unless otherwise noted. Refer to Oracle Linux documentation for more information on the operating system platform.

Oracle Key Vault supports both Legacy BIOS and UEFI boot modes. The support for UEFI boot mode allows the installation of Oracle Key Vault on servers that exclusively support UEFI, or when disks larger than 2 TB are used.

## Note:

- You can find the supported hardware from the hardware certification list for Oracle Linux and Oracle VM. Filter the results by selecting All Operating Systems and choosing Oracle Linux 8. However, be aware that Oracle Key Vault does not support the QLogic QL4\* family of network cards.
- For deployment with a large number of endpoints, the hardware requirement may need to scale to meet the workload.
- RAID: Oracle Key Vault does not support software RAID installations. If you require a RAID configuration, enable hardware RAID that presents one disk to Oracle Key Vault.
- **RESTful Services Utility**: If you plan to automate the onboarding of endpoints into Oracle Key Vault with the RESTful services, then ensure that the Java version on the future endpoint where the RESTful script will be executed is at release 1.7.0.21 or later.

The version of Java that is included in Oracle Database 12.2.0.1 and later is supported by Oracle Key Vault. For these releases, set <code>JAVA\_HOME</code> to <code>\$ORACLE\_HOME/jdk/jre</code> and add <code>JAVA\_HOME/bin</code> to your <code>PATH</code>.

For Oracle databases that are earlier than release 12.2.0.1, find the current Java installation as follows:

```
$ namei /usr/bin/java | grep "l java"
```

The output is similar to the following:

```
1 java -> /etc/alternatives/java
1 java -> /usr/java/jdk1.8.0 131/jre/bin/java
```

In this example, set <code>JAVA\_HOME=/usr/java/jdk1.8.0\_131/jre</code> and then add <code>JAVA\_HOME/bin</code> to <code>PATH: PATH=\$PATH:\$JAVA\_HOME/bin</code>.

OpenJDK is not supported.

Browser: Oracle Key Vault supports English as the browser display language.



#### Other Installation Considerations:

- Oracle recommends that you do not install a third-party software on an Oracle Key Vault appliance. For more information, see Additional or Third-Party Software.
- Oracle does not recommend to decrease CPU and RAM allocated to Oracle Key Vault as it
  is a software appliance. For the multi-master cluster deployment, if you need to decrease
  RAM or CPU without database endpoint downtime, add the new nodes with the required
  system configuration to the existing multi-master cluster, and then delete the old nodes.
  For other deployments, take the backup of Oracle Key Vault server, rebuild the server with
  required system configuration and restore using the backup with the recommended system
  configuration.
- Additional or Third-Party Software
   Oracle does not support Oracle Key Vault installations with any third-party software.

#### **Related Topics**

Hardware Certification List for Oracle Linux and Oracle VM

## Additional or Third-Party Software

Oracle does not support Oracle Key Vault installations with any third-party software.

- Oracle recommends that you do not install a third-party software on an Oracle Key Vault appliance. Oracle Key Vault is a security appliance and installing a third-party software interferes with the security of Oracle Key Vault. Installing a third-party software may also affect the operational integrity of the Oracle Key Vault appliance. For example:
  - Installing third-party software may cause an upgrade to fail.
  - Reboot or upgrade of the Oracle Key Vault may override the configuration changes made by a third-party software.
  - Third party software may affect the configuration and operations of Oracle Key Vault in unexpected ways.

# **Network Port Requirements**

Network port requirements includes requirements for SSH/SCP, SNMP, HTTPS, listeners, KMIP, and TCP ports.

Oracle Key Vault and its endpoints use a set of specific ports for communication. Network administrators must ensure that these ports are open.

The following table lists the required network ports for Oracle Key Vault:

Table 2-1 Ports Required for Oracle Key Vault

Port Number	Protocol	Port Type	Descriptions
22	SSH/SCP port	TCP	Used by Oracle Key Vault administrators and support personnel to remotely administer Oracle Key Vault. <b>Note</b> : You can change the default value of the port. After you change the default value on one node, apply the new port number to all the nodes of the cluster one-by-one.



Table 2-1 (Cont.) Ports Required for Oracle Key Vault

Port Number	Protocol	Port Type	Descriptions
161	SNMP port	UDP	Used by monitoring software to poll Oracle Key Vault for system information.
443	HTTPS port	TCP	Used by web clients such as browsers and RESTful Administrative commands to communicate with Oracle Key Vault.
5695	HTTPS port	TCP	Used by RESTful Key Management commands to communicate with Oracle Key Vault.
1522	Database TCPS listener ports	TCP	In a cluster configuration, listener ports used to communicate between read/ write peer nodes.
			<b>Note</b> : You can change the default value of this port. Oracle Key Vault automatically applies the new port number to all the cluster nodes.
7443	HTTPS port	TCP	The listener port used in a primary- standby configuration to run operating system commands. This port is also used when you add a new node to a cluster.
5696	KMIP port	TCP	Used by Oracle Key Vault endpoints and third party KMIP clients to communicate with the Oracle Key Vault KMIP server.
7093	TCP port	TCP	Used by Oracle GoldenGate for transmitting data in a multi-master cluster configuration.

If you are installing Oracle Key Vault in an OCI Marketplace instance or if you are creating a hybrid multi-master cluster between on-premises and OCI nodes, then consider the following network configuration:

- 1. Add rules to open the ports listed in the table.
- **2.** Add the following ingress rules:
  - ICMP Type 3, Code 4 (destination unreachable, fragmentation required and Don't Fragment flag is set).
  - ICMP Type 8, Code 0 (echo request, destination network is unreachable).
- 3. If you are using a site-to-site VPN or fastConnect, then ensure that your router allows traffic between the nodes of the multi-master cluster:
  - Add rules to open the ports.
  - In case of highly secured routers, add URL exceptions for your on-premises subnet at layers 3, 4, and 7.
  - Ensure that no packets are interpreted as threats by your routers.





Oracle Key Vault allows the configuration of network ports only for SSH/SCP (default port 22) and Database TCPS listener (default port 1522).

# Supported Endpoint Platforms

Oracle Key Vault supports both UNIX and Windows endpoint platforms.

Oracle supports 64-bit Linux endpoints, and only 64-bit endpoints are supported for Oracle databases that use the online master encryption key. The operating systems on which the endpoint runs must be compatible with Transport Layer Security (TLS) 1.2, either directly or with appropriate patches.

The supported endpoint platforms in this release are as follows:

- Oracle Linux (6, 7, 8, and 9)
- ARM64: Oracle Linux (7 and 8)
- Oracle Solaris x86 (10 and 11)
- Oracle Solaris SPARC (10 and 11)
- SUSE Linux Enterprise Server 15
- Red Hat Enterprise Linux 6, 7, and 8
- IBM AIX (7.1, 7.2, and 7.3)
- IBM zLinux (Red Hat Enterprise Server 7, 8, 9; SUSE Linux Enterprise Server 12, 15)
- HP-UX (IA) (11.31)
- Windows Server 2016, and 2019

# **Endpoint Database Requirements**

Administrators can use online master encryption keys and the Oracle Database COMPATIBLE initialization parameter to manage Oracle Database endpoints.

Administrators can use the online master encryption key to manage TDE master encryption keys for endpoints that are Oracle Database 12.1.0.2 or later. Administrators who want to use Oracle Key Vault for wallet management only or who are migrating existing wallets deployments to Oracle Key Vault can use the <code>okvutil upload</code> command to upload Oracle wallets to Oracle Key Vault.

Administrators who manage endpoints that are Oracle Database may need to set the COMPATIBLE initialization parameter.

For an endpoint that is Oracle Database release 12.1 or later, set the COMPATIBLE initialization parameter to 12.1.0.0 or later. A COMPATIBLE setting of 12.1.0.0 or later enables Transparent Data Encryption to work with Oracle Key Vault. For example:

```
SQL> ALTER SYSTEM SET COMPATIBLE = '12.1.0.0' SCOPE=SPFILE;
```

This applies to an Oracle Database endpoint that use the online master encryption key to manage TDE master encryption keys. This compatibility mode setting is not required for Oracle wallet upload or download operations.

Also note that after setting the COMPATIBLE parameter to 12.1.0.0, you cannot set it to a lower value such as 10.2. After you set the COMPATIBLE parameter, you must restart the database.

For Microsoft Windows endpoints, Oracle Key Vault supports the latest available database release versions at the time of the Oracle Key Vault release, including any associated Manufacturing Execution Systems (MES) libraries that may have been upgraded.



# Downloading Oracle Key Vault Software

To install or upgrade the Oracle Key Vault software download the binaries as described in the chapter.

- Downloading the Oracle Key Vault Software for Fresh Installation
   You can use the steps for fresh installation of Oracle Key Vault.
- Downloading the Oracle Key Vault Software for Upgrade
   You can use the steps for downloading and upgrading Oracle Key Vault.

# Downloading the Oracle Key Vault Software for Fresh Installation

You can use the steps for fresh installation of Oracle Key Vault.

For a fresh installation, you can download the Oracle Key Vault appliance software from Software Delivery Cloud. You cannot use this package to upgrade Oracle Key Vault. For an upgrade, you can download the Oracle Key Vault upgrade software from the My Oracle Support website.

1. Use a web browser to access the Oracle Software Delivery Cloud portal:

https://edelivery.oracle.com

- Click Sign In, and if prompted, enter your User ID and Password.
- In the All Categories menu, select Release. In the next field, enter Oracle Key Vault and then click Search.
- From the list that is displayed, select Oracle Key Vault 21.10.0.0.0 or click the + icon next to the Oracle Key Vault 21.10.0.0.0.

The download is added to your cart. (To check the cart contents, click **View Items** in the upper right of the screen.)

- Click Continue.
- On the next page, verify the details of the installation package, and then click Continue.
- 7. In the Oracle Standard Terms and Restrictions page, select I reviewed and accept the Oracle License Agreement., and click Continue.

The **Oracle Software Delivery Cloud** page appears, which lists the Vpart\_number.zip Oracle Key Vault archive file in **Download** window pane.

- B. Click **Download** and select a location to save the Vpart number.zip archive file.
- 9. Click Save.

The size of the ISO file is approximately 20 GB, and will take time to download, depending on the network speed. The estimated download time and speed are displayed in the **File Download** dialog box.

- **10.** Unzip the downloaded Vpart number.zip archive file.
- **11.** Transfer the Vpart number.iso file by using one of the following methods:

- Burn the .iso image onto a bootable DVD.
- Copy the .iso image onto a bootable USB stick.
- Mount the .iso image with your virtualization software, in order to run Oracle Key Vault as a virtual machine, booting from the .iso image.

You can now install Oracle Key Vault on the server.

# Downloading the Oracle Key Vault Software for Upgrade

You can use the steps for downloading and upgrading Oracle Key Vault.

1. Click the link: https://updates.oracle.com/download/36884675.html

Alternatively, you can use the steps below to search for a patch:

- a. Go to https://support.oracle.com sign in, and click on the Patches & Updates tab.
- **b.** Use the **Patch Search** box to find the patch.
- c. Select the Search tab.
- d. Ensure that Number/Name or Bug Number (Simple) is selected on the left.
- For the top search drop-down list, select Patch Name or Number and enter 36884675 in the search box.
- Click Search.
- g. In the Patch Name column on the search results page, click the number for the latest Bundle Patch ORACLE KEY VAULT 21.10.0.0.0 RELEASE (Patchset). A corresponding patch page appears
- h. Click the **View ReadMe** button to open the readme file in a browser.
- Click the **Download** button to open the **File Download** page.
- j. Click the **Download File** Metadata link on the bottom left, and then the **Download** button to download the XML metadata file.
  You can use the data in this file to verify the patch files once they are downloaded.
- k. Click the Return to File Window link to go back to the File Download page.
- I. Click the following .zip file to download them on your system:

```
p36884675 2110000 Linux-x86-64.zip
```

2. Unzip the downloaded .zip file to access the upgrade software.

After unzipping the downloaded zip file to your destination directory, you will see the following file:

The following ISO file includes all the files that are required to perform the upgrade:

```
okv-upgrade-21.10.0.0.iso
```

Refer to, Readme OKV 2110.html.



## Note:

Oracle Key Vault should be installed by  ${\tt iso}$  package only and not  ${\tt rpm}$  package due to many dependencies.

- 3. You can use the XML metadata file to verify the checksum of the downloaded .iso file.
- 4. On your Linux machine, generate a sha256 checksum for the ISO file.

```
sha256sum okv-upgrade-21.10.0.0.iso
```

## Ensure that the file checksum matches the following value:

05cec94755b9b63b65a448e04bd33f1f7ff4a821d380d4873871a24cf285c45d okv-upgrade-21.10.0.0.0.iso



# Installing Oracle Key Vault

You must download the Oracle Key Vault application software, and then you can perform the installation.

- Downloading the Oracle Key Vault Appliance Software
   You can download executable files for both a fresh Oracle Key Vault installation or an
   upgrade.
- Installing the Oracle Key Vault Appliance Software
   The Oracle Key Vault installation process installs all the required software components
   onto a dedicated server or virtual machine.
- Performing Post-Installation Tasks
   After you install Oracle Key Vault, you must complete a set of post-installation tasks.

# Downloading the Oracle Key Vault Appliance Software

You can download executable files for both a fresh Oracle Key Vault installation or an upgrade.

For a fresh installation, you can download the Oracle Key Vault appliance software from Software Delivery Cloud. You cannot use this package to upgrade Oracle Key Vault. For an upgrade, you can download the Oracle Key Vault upgrade software from the My Oracle Support website.

1. Use a web browser to access the Oracle Software Delivery Cloud portal:

https://edelivery.oracle.com

- 2. Click Sign In, and if prompted, enter your User ID and Password.
- In the All Categories menu, select Release. In the next field, enter Oracle Key Vault and then click Search.
- 4. From the list that is displayed, select **Oracle Key Vault 21.10.0.0.0** or click the **+Add to Cart** button next to the **Oracle Key Vault 21.10.0.0.0**.

The download is added to your cart. (To check the cart contents, click **View Cart** in the upper right of the screen.)

- Click Checkout.
- 6. On the next page, verify the details of the installation package, and then click **Continue**.
- In the Oracle Standard Terms and Restrictions page, select I have reviewed and accept the terms of the Commercial License, Special Programs License, and/or Trial License, and click Continue.

The download page appears, which lists the <code>Vpart\_number.zip</code> Oracle Key Vault archive file

- 8. Click **Download** and select a location to save the *Vpart number*.zip archive file.
- Click Save.



The size of the ISO file is approximately 20 GB, and will take time to download, depending on the network speed. The estimated download time and speed are displayed in the **File Download** dialog box.

- 10. Unzip the downloaded Vpart number.zip archive file.
- 11. Transfer the Vpart number.iso file by using one of the following methods:
  - Burn the .iso image onto a bootable DVD.
  - Copy the .iso image onto a bootable USB stick.
  - Mount the .iso image with your virtualization software, in order to run Oracle Key Vault as a virtual machine, booting from the .iso image.

You now can install Oracle Key Vault on the server.

### **Related Topics**

Downloading the Oracle Key Vault Software for Fresh Installation
 You can use the steps for fresh installation of Oracle Key Vault.

# Installing the Oracle Key Vault Appliance Software

The Oracle Key Vault installation process installs all the required software components onto a dedicated server or virtual machine.

The installation process may take from 30 minutes or longer to complete, depending on the server resources where you are installing Oracle Key Vault.

If you are installing Oracle Key Vault on VMware, then set the VMX configuration parameter <code>disk.EnableUUID</code> to <code>TRUE</code>. In addition, you must set your virtual machine to use EFI boot. In some versions of VMware this is done by selecting the **VM Options** tab, then expanding **Boot Options**, and then setting the firmware to EFI. You must disable secure boot. Without this setting, the Oracle Key Vault installation on VMware will fail.



#### **Caution:**

The Oracle Key Vault installation wipes the server, repartitions the disk, and installs a hardened Oracle Linux 8. The installation erases existing software and data on the server.

Ensure that you have met the following prerequisites.

- Ensure that the server meets the recommended requirements.
- Request a fixed IP address, network mask, and gateway address from your network administrator. You will need this information to configure the network.

To install the Oracle Key Vault appliance:

Make the .iso image available to the computer where you want to install it, and then
restart the computer.

The .iso image can be made available in any of these ways:

- Burned onto a bootable DVD
- Copied onto a bootable USB stick
- Mounted with your site's virtualization software



You may need to change the boot order of your server to boot from the USB-stick or the DVD. The initialization screen appears, showing the following options:

```
Oracle Key Vault 21.10.0.0.0

Press ENTER to start the installation of the Oracle Key Vault.

Press ENTER to start the installation of the Oracle Key Vault with F

IPS Mode

Press Tab for full configuration options on menu items.
```

2. Using the up and down arrow keys, select the desired installation option or the option to perform a memory test, and then press **Enter**.

Choosing the first option, **Press Enter to start the installation of Oracle Key Vault**, does not enable FIPS mode on the system.

Choosing the second option, **Press Enter to install the Oracle Key Vault with FIPS mode enabled**, automatically enables FIPS mode on the system.

The installation begins, and after several minutes, you will be asked to set the root user password (with a second time to confirm it). It is important to store the root user password securely. You will need it later to authenticate yourself at the Oracle Key Vault management console and complete the post-installation tasks.

```
Changing password for user root.
New password:
```

3. After you set the root user password, when prompted, log in as the root to observe the installation status. At the following prompt, enter root, press **Enter**, enter the root user password, and then press **Enter** again.

```
Please re-insert the installation ISO to continue.

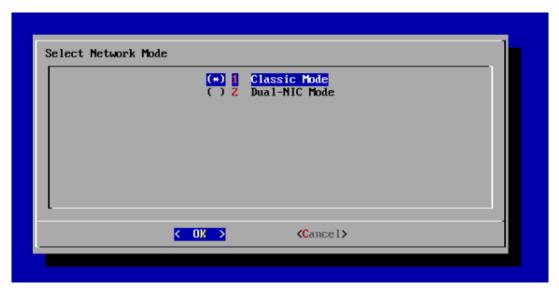
Log in as root to observe the current installation status.

Terminal:tty1

localhost login: _
```

When prompted, re-insert the ISO disk.

After you re-insert the ISO disk, the Select Network Mode window appears after a couple of minutes.



5. For the network mode, if you want Classic mode, then follow these steps:

Classic mode, used in previous releases of Oracle Key Vault, allows one network interface to be used. If you later decide to switch to dual NIC mode, then you can do so, but only if you are using a standalone configuration. In a multi-master cluster configuration, to switch to dual NIC mode for a cluster node, you must first delete the node from the cluster, configure the node to use dual NIC mode, and then re-induct the node back into the cluster.

- a. Select 1 to choose Classic mode and then select OK.
- In the Select default network interface screen, select from the available options, and then select OK.
- c. In the Network settings screen, enter the IP address, Network mask, and Gateway settings for the default network interface. The network administrator for your site can provide this information.
- d. Select OK.
- 6. If you want the dual NIC network mode, then follow these steps:

Dual NIC mode enables you to configure Oracle Key Vault to use two network interfaces, or ethernet ports. It is useful as a guard against physical or software failures and adds redundancy to the network layer. Select the dual NIC mode if there is a greater need for operational continuity and to avoid eviction from the cluster due to prolonged unavailability of the network. Dual NIC mode helps to prevent situations where a node may lose connectivity and risk missing changes that have been made to data in the cluster.

- a. Select 2 to select Dual-NIC mode and then select OK.
- **b.** In the Select Bond Mode screen, select from the bond mode choices for the two network interfaces that you plan to use, and then select **OK**.
  - Round Robin configures the network interfaces such that network packets are
    transmitted and received sequentially from the first available interface through the
    last. This bonding mode is the default. This mode provides fault tolerance and load
    balancing and requires the links to be connected to a network switch with
    EtherChannel support.
  - Active-Backup configures the network interfaces as active and backup. Only one interface in the bond is active. A different interface becomes active if, and only if, the active interface fails. The network communication happens over the active

interface. This mode provides fault tolerance and does not require any switch support.

- 802.3ad creates aggregation groups that share the same speed and duplex settings. Network packets are transmitted and received on all interfaces. This mode provides fault tolerance and load balancing and requires a switch that supports IEEE 802.3ad dynamic link aggregation.
- **c.** In the Select two network interfaces screen, select the two network interfaces that you want, and then select **OK**.
- d. In the Network settings screen, enter the IP address, Network mask, Gateway, and Hostname settings for the default network interface. The network administrator for your site can provide this information. For the host name, use only lowercase characters. The host name can be the fully qualified host name or the short host name.
- e. Select OK.
- 7. The installer installs and configures the operating system, database, and Oracle Key Vault on the server to make it a self-contained hardened appliance. The installation and configuration process can take an hour or longer.
- 8. When the installation is complete, on the Oracle Key Vault terminal console, log in as root, and set the password of the support.

```
passwd support
New password:
Retype new password
passwd: All authentication tokens updated successfully.
```

Once SSH has been enabled, the support user is the only user who can  ${\bf ssh}$  into Oracle Key Vault, .

SSH should be disabled, unless upgrade patches are applied, or directed by Oracle Support.

## Note:

- Oracle does not restrict customer to deploy Oracle Key Vault in virtual environment if the virtual environment reflects an Oracle Key Vault physical server. Some of the supported hypervisor products are Oracle VirtualBox, Hyper-V, VMware, and KVM.
- For installing Oracle Key Vault on Hyper-V, see Hyper-V Installation on Windows.
- Oracle key Vault does not support silent mode installation.
- Requirements for root and support User Passwords
   Ensure that you meet these requirements for root and support user passwords.

#### **Related Topics**

Requirements For Root And Support User Passwords

## Requirements for root and support User Passwords

Ensure that you meet these requirements for root and support user passwords.



- The password must have at least 15 characters.
- The password must contain at least one uppercase letter, one lowercase letter, one digit, and one special character.
- The same character cannot repeat consecutively more than 3 times in the password.
- Characters from the same class cannot repeat consecutively more than 4 times in the password. For example, more than 4 lowercase letters in a row.
- The new password must have at least 8 characters that are different from the old password.

# Performing Post-Installation Tasks

After you install Oracle Key Vault, you must complete a set of post-installation tasks.

These tasks include configuring the administrative user accounts and their one-time passwords, the recovery passphrase, as well as DNS and NTP settings.

1. Use a web browser to connect to the Oracle Key Vault server.

For example, to connect in to an Oracle Key Vault server whose IP address is 192.0.2.254, enter the following in the address bar:

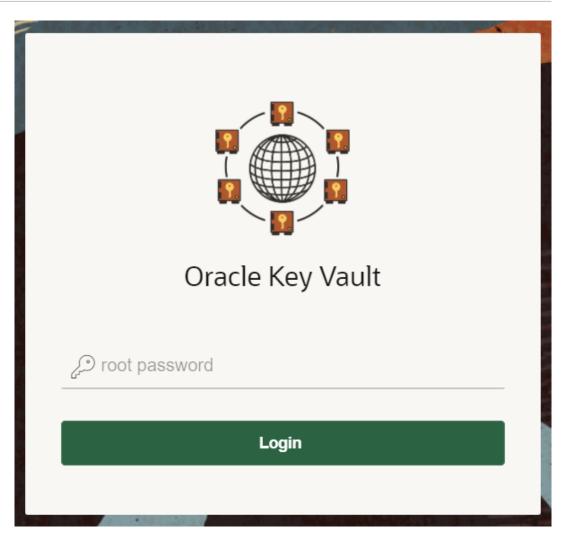
https://192.0.2.254

If the web browser displays a security warning message stating that you are connecting to a website with an untrusted or self-signed security certificate, accept the security warning message and proceed to connect to the Oracle Key Vault server.

This message is only temporary. When you configure third-party certificates, this message will no longer appear. After completing the post-installation tasks, you can upload a custom certificate or certificate chain that is trusted by the browser, so that you can connect to the Oracle Key Vault server without encountering the security warning message. For more information about uploading a custom certificate, see *Oracle Key Vault Administrator's Guide* .

3. In the root password screen, enter the root password.

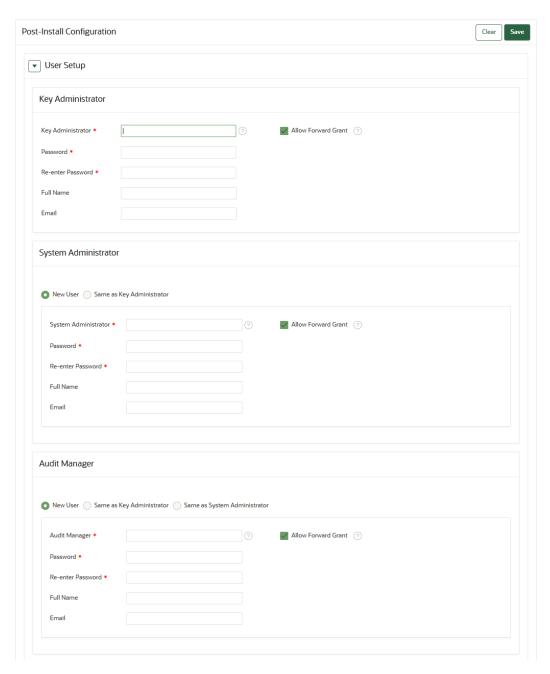




The root password screen is displayed when you connect to the Oracle Key Vault server for the first time, in order to complete the post-installation tasks. After you complete the post-installation tasks, the Oracle Key Vault login screen is displayed when you access the Oracle Key Vault management console through the web browser.

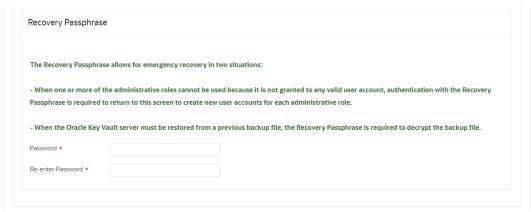
After you log in with the  $\mathtt{root}$  user password, the Post-Install Configuration screen is displayed.

 In the User Setup pane, create three administrative user accounts for the Key Administrator, System Administrator, and Audit Manager.



- Enter the user name and password, the full name (optional), and email (optional) for each administrative user account.
  - Note that the passwords are one-time use passwords which must be changed when the user logs in the first time.
- Ideally, create a different user account for each of these administrative roles for a strict separation of duties, or combine roles as necessary.
- Ensure that passwords are between 8 and 30 characters in length and contain at least one of each of the following: an uppercase letter, a lowercase letter, a number, and a special character from the set: period (.), comma (,), underscore (\_), plus sign (+), colon (:), exclamation mark (!). In addition, the passphrase may include a space character (\_) provided it is not used as the first or last character of the passphrase.
- If you want the user to be able to grant their role to other users, then select the Allow Forward Grant check box.

5. In the **Recovery Passphrase** section, create the recovery password.



The recovery passphrase must be between 8 and 30 characters in length and may only contain uppercase letters, lowercase letters, numbers, and special characters from the set: period (.), comma (,), underscore (\_), plus sign (+), colon (:), exclamation mark (!). Recovery passphrase must contain at least one of each of the following: an uppercase letter, a lowercase letter, a number, and a special character from the allowed set of special characters.

For greater security, Oracle recommends that you make the recovery passphrase longer and more complex. Because this is a critical password, you must properly secure and safeguard the recovery password. The recovery password is required in the following scenarios:

- In an emergency, when there are no administrative users available to access Oracle Key Vault
- To restore Oracle Key Vault data from a backup
- To reset the recovery password
- Induct a new node into a multi-master cluster
- To configure a hardware security module (HSM)

## lack

#### Caution:

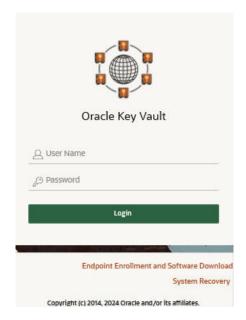
It is important to establish a secure process for the storage and retrieval of the recovery passphrase, including older recovery passphrases. The only way to recover from a lost recovery passphrase is to re-install Key Vault. Note also that the root and support user passwords expire after 365 days. If you log in to the Oracle Key Vault management console within 120 days before the expiration, you will see an alert that the password expires in remaining\_number\_of\_days days. If you log in after the expiration date, then you can use the old password only to log in and change the password to a new one.

6. Set the DNS IP addresses.

Oracle recommends that you set this IP address at this stage. Your network administrator can supply this address. You can only set the NTP server names after you save the changes on this page, including the DNS addresses.

Click Save in the upper right corner of the Post-Install Configuration screen.

The Oracle Key Vault management console login screen is displayed:



Configure the system time.

Oracle recommends that when you configure the system time, to configure all three NTP servers, using their host names. When you do so, ensure that you select the **Synchronize Periodically** option.

Configure system alerts, and if necessary, email so that the appropriate users can receive these alerts.

Oracle recommends that users who receive these alerts take action on them as soon as possible. For example, critical alerts, such as the Oracle Key Vault server certificate expiration alert, can result in downtime if they are not addressed in a timely fashion.

You can now log in to the Oracle Key Vault management console with the credentials of any of the user accounts that were created during the post-installation process.

## **Related Topics**

Oracle Key Vault Administrator's Guide



# Cloning Oracle Key Vault Installation

Perform the installation procedure for Oracle Key Vault before proceeding for VM cloning.

- Cloning Oracle Key Vault Virtual Machines
   Oracle Key Vault Vitual Machines (VM) can be cloned to reduce the installation time on each VM. You create a base VM to clone it to any number of VM's.
- Guidelines for Cloning on Virtual Machines
   Consider these Oracle Key Vault guidelines for managing Cloning on Virtual Machines.

# Cloning Oracle Key Vault Virtual Machines

Oracle Key Vault Vitual Machines (VM) can be cloned to reduce the installation time on each VM. You create a base VM to clone it to any number of VM's.

Create a base VM by performing the installation procedure for Oracle Key Vault following Installing the Oracle Key Vault Appliance Software, but do not go through the post-install steps.

 Install Oracle Key Vault as a base VM. The base VM refers to the VM that is used for cloning other VMs.



This process takes about 30 minutes or longer to get completed.

- 2. Log into terminal console of the **base VM** as a root user.
- 3. Run the script to set up the configuration to make sure that all system-specific configuration is regenerated on the next boot.

```
# /usr/local/okv/bin/okv enable vm clone
```

The script marks the **base VM** as the **clonable** and shuts down the system.

Note: This script sets up the configuration to make sure that all system-specific configuration is regenerated on the next boot. The system will be made **clonable**, and once the configuration completes the system automatically shuts down.

- 4. Start cloning the VM after the base VM shuts down.
- Access the terminal console of the cloned VM after the cloned VM is booted for the first time.
  - a. Set the password for the root user.
  - Configure the network (IP Address, gateway, network mask and host name).
- **6.** Oracle Key Vault begins the process of generating system-specific application configuration.
- Once completed the system gets rebooted automatically to complete the process.

The cloning is now marked as complete.

## Note:

If you access the Oracle Key Vault management console of the clone while the cloning process is in progress, the post-install tasks cannot be completed. Oracle Key Vault displays a message to log into the terminal console and follow directions to complete the post-clone configuration.

**8.** Complete the post-installation steps on the clone VM, see Performing Post-Installation Tasks.

# **Guidelines for Cloning on Virtual Machines**

Consider these Oracle Key Vault guidelines for managing Cloning on Virtual Machines.

- You can clone an Oracle Key Vault VM only if you have NOT completed the post-install tasks.
- The base VM serves as a template for cloning further VMs.
- Do not boot the base VM once you have marked the base VM as clonable and shut it down.
- In case, you do boot the base VM, it can no longer be used for cloning.
- It is recommended not to use the system again for cloning.
- When the cloned VM starts, you can change its IP address and root password (both are inherited from the base VM), and complete the post-install steps.



# Upgrading a Standalone Oracle Key Vault Server

This upgrade includes the Oracle Key Vault server software and utilities that control the associated endpoint software

- About Upgrading a Standalone Oracle Key Vault Server
   When you upgrade the Oracle Key Vault server software appliance, also upgrade the endpoint software to get access to the latest enhancements.
- Step 1: Back Up the Server Before You Upgrade
  Before you upgrade the Oracle Key Vault server, perform a one-time backup to a remote destination so that you can recover data in case the upgrade fails.
- Step 2: Perform Pre-Upgrade Tasks for the Standalone Oracle Key Vault
   To ensure a smooth upgrade to Oracle Key Vault, you should prepare the server you are
   upgrading.
- Step 3: Add Disk Space to Extend the vg\_root for the Release 21.10 Upgrade

  Before upgrading from Oracle Key Vault release 12.2 or 18 to 21, you need to extend the

  vg\_root to increase disk space.
- Step 4: Upgrade the Oracle Key Vault Server
   You can upgrade a standalone Oracle Key Vault server deployment.
- Step 5: If Necessary, Add Disk Space to Extend Swap Space
  If necessary, extend the swap space. Oracle Key Vault release 21.10 requires a hard disk size greater than or equal to 2 TB in size with approximately 64 GB of swap space.
- Step 6: If Necessary, Remove Old Kernels
   Oracle recommends that you clean up the older kernels that were left behind after the
   upgrade.
- Step 7: If Necessary, Remove SSH-Related DSA Keys
  You should remove SSH-related DSA keys left behind after the upgrade, because they can
  cause problems with some code analysis tools.
- Step 10: Back Up the Upgraded Oracle Key Vault Server
  You must perform server backup and user password tasks after completing a successful
  upgrade.

# About Upgrading a Standalone Oracle Key Vault Server

When you upgrade the Oracle Key Vault server software appliance, also upgrade the endpoint software to get access to the latest enhancements.

However, the endpoint software downloaded from the previous Oracle Key Vault release will continue to function with the upgraded Oracle Key Vault server. Be aware that while the old

endpoint software will continue to work with the upgraded Oracle Key Vault server, the new endpoint functionality may not work.

You must upgrade in the order shown: first perform a full backup of Oracle Key Vault, upgrade the Oracle Key Vault server, upgrade the endpoint software, and last, perform another full backup of the upgraded server. Note that upgrading requires a restart of the Oracle Key Vault server.

The Oracle Key Vault server is not available to endpoints for a limited duration during the upgrade. You can enable the persistent cache feature to enable endpoints to continue operation during the upgrade process.

Before you begin the upgrade, refer to *Oracle Key Vault Release Notes* for additional information about performing upgrades.

#### **Related Topics**

- Oracle Key Vault Release Notes
- Oracle Key Vault Administrator's Guide

# Step 1: Back Up the Server Before You Upgrade

Before you upgrade the Oracle Key Vault server, perform a one-time backup to a remote destination so that you can recover data in case the upgrade fails.



#### **Caution:**

Do not bypass this step. Back up the server before you perform the upgrade so that your data is safe and recoverable.

# Step 2: Perform Pre-Upgrade Tasks for the Standalone Oracle Key Vault

To ensure a smooth upgrade to Oracle Key Vault, you should prepare the server you are upgrading.

- 1. In the server where Oracle Key Vault is installed, log in as user support, and then switch to the root user.
- 2. Ensure that the server meets the minimum disk space requirements for an upgrade. For example, 6 GB of free space in the /usr/local/dbfw/tmp directory. See the Oracle Key Vault Readme for this release to determine the disk space requirements for the upgrade.
- 3. Ensure that you disable diagnostics and clean up disk space in /usr/local/dbfw/tmp before you upgrade by performing the following steps:
  - If the Oracle Key Vault system being upgraded is from release 21.6 or later, log in to the Oracle Key Vault management console as a user with the System Administrator role, and navigate to the **System** tab, and then click the **Diagnostics** button.

If the Diagnostics Package Files pane is displayed, then click **Clear** to disable diagnostics. Note that the **Diagnostics Package Files** pane will be displayed only if the diagnostics bundle was previously generated, and the files were not cleared.



If the Diagnostics Package Files pane is not displayed, or if the diagnostics bundle was previously generated using the **dbfw-diagnostics-package.rb** utility, then log in to the Oracle Key Vault system and run the following commands to disable diagnostics and clean up disk space in /usr/local/dbfw/tmp:

a. SSH into the Oracle Key Vault system as user support, then switch to user root:

```
ssh support@<OKV_IP_Address>
su - root
```

b. Delete the generated diagnostics zip file and remove the package using the following commands:

```
/usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --clean /usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --remove
```

- 4. Check the boot partition size. If any of the nodes in question have a boot partition that is less than 500 MB, then you cannot upgrade that system to the new release. You can check this size as follows:
  - a. Mount the /boot partition.

```
# mount /boot
```

b. Check the Size column given by the following command:

```
# df -h /boot
```

c. Unmount the /boot partition:

```
# umount /boot
```

If the boot partition given by this command shows less than 488 MB, then you cannot upgrade to the current release. Oracle recommends that you restore a backup of the current configuration to a freshly installed system of the same release as the current system, and upgrade that to the new release instead.

- 5. If Oracle Key Vault is using the BIOS boot mode, then ensure that the disk size is not greater than 2 TB. If this is the case, then you cannot upgrade to the current release. Oracle recommends that you restore a backup of the current configuration onto a system with a disk that is less than 2 TB in size, and upgrade that to the new release instead.
- 6. If you need to increase available disk space, then remove the temporary jar files located in /usr/local/okv/ssl. *Be careful in doing so.* If you accidentally delete any files other than the jar files in /usr/local/okv/ssl, then the Oracle Key Vault server becomes nonfunctional.
- 7. Increase your disk space by extending the vg root size:

You must increase the disk space by extending vg root before you perform the upgrade.

- 8. Ensure that no full or incremental backup jobs are running. Delete all scheduled full or incremental backup jobs before the upgrade.
- **9.** Plan for downtime according to the following specifications:



Oracle Key Vault Usage	Downtime required
Wallet upload or download	NO
Java Keystore upload or download	NO
Transparent Data Encryption (TDE) direct connect	YES (NO with persistent cache)
Primary Server Upgrade in a primary-standby deployment	YES (NO with persistent cache)

10. Plan for downtimes.

If Oracle Key Vault uses an online master encryption key, then plan for a downtime of 15 minutes during the Oracle Database endpoint software upgrades. Database endpoints can be upgraded in parallel to reduce total downtime.

- 11. If the Oracle Key Vault system has a syslog destination configured, ensure that the remote syslog destination is reachable from the Oracle Key Vault system, and that logs are being correctly forwarded. If the remote syslog destination is not reachable from the Oracle Key Vault system, then the upgrade process can become much slower than normal.
- **12.** If Oracle Audit Vault was integrated with Oracle Key Vault release 21.2 or earlier, then do the following to disable and remove the Oracle Audit Vault integration:
  - a. Disable the Oracle Audit Vault integration: Log into the Oracle Key Vault management console as a System Administrator, select the **System** tab and then **Settings** from the left navigation bar. In the Monitoring and Alerts pane, select Audit Vault. In the Audit Vault integration pane that appears, disable AVDF. Click **Save**.
  - **b.** Log in to the Oracle Key Vault server through SSH as user support, switch user su to root and then switch user su to oracle.
  - **c.** Stop the agent by executing the following command:

```
agent_installation_directory/bin/agentctl stop
```

- d. Log in to the Oracle Audit Vault Server console as an Oracle Audit Vault administrator.
- e. Delete the corresponding agent and target.
- f. Log in to the Oracle Key Vault server through SSH as user support, then switch user su to root.
- g. Delete the installation directory for the Oracle Audit Vault agent.
- 13. If you are performing an upgrade while using an HSM as a Root of Trust, then consult Oracle Key Vault Root of Trust HSM Configuration Guide for any additional steps that may be needed.
- **14.** Ensure that the Oracle Key Vault server certificate has not expired, nor is close to expiry, before you begin the upgrade.

You can find how much time the Oracle Key Vault server certificate has before it expires by checking the **OKV Server Certificate Expiration** setting on the Configure Alerts page in the Oracle Key Vault management console.





If you are upgrading from release 21.9.0.0.0 to release 21.10.0.0.0, Oracle recommends that you apply patch 37492574 before you start the upgrade. This patch corrects the configuration of certain processes internal to Oracle Key Vault, and prevents upgrades to 21.10.0.0.0 from failing. Apply this patch to all systems in the Oracle Key Vault 21.9.0.0.0 deployment before you start the upgrade to 21.10.0.0.0.

- 15. Ensure that the backup of the orapwdbfwdb file matches the original file.
  - a. SSH into the Oracle Key Vault system as user support, then switch to user root:

```
ssh support@<OKV_IP_Address>
su - root
```

**b.** Verify that the backup file exists:

```
su - oracle
ls -ltr /var/lib/oracle/okv orapwd backup dir/orapwdbfwdb
```

- **c.** If the backup file exists, then perform the following steps:
  - Compare the original file with the backup file:

```
diff /var/lib/oracle/dbfw/dbs/orapwdbfwdb /var/lib/oracle/
okv orapwd backup dir/orapwdbfwdb
```

• If there is a difference between the files, then update the backup file by copying the original file:

```
cp /var/lib/oracle/dbfw/dbs/orapwdbfwdb /var/lib/oracle/
okv orapwd backup dir/orapwdbfwdb
```

- **16.** If you are upgrading from Oracle Key Vault release 21.x to release 21.10.0.0.0, then Oracle recommends that you apply the following patches:
  - Patch 37688544, to be applied before you start the upgrade. This patch corrects any FIPS inconsistencies on the system and prevents upgrades from failing with the following error:

```
ODF-10001: Internal error: FAILED migration: okv_save_restore_orapwd_config["backup_orapwd_config"].
```

Apply this patch to all systems in the Oracle Key Vault deployment before you start the upgrade to 21.10.0.0.0.

Patch 37763976, to be applied after starting the upgrade with the ruby /images/upgrade.rb -confirm command but before resuming the upgrade with the /sbin/reboot command.

#### **Related Topics**

Step 3: Add Disk Space to Extend the vg\_root for the Release 21.10 Upgrade
Before upgrading from Oracle Key Vault release 12.2 or 18 to 21, you need to extend the
vg\_root to increase disk space.



Oracle Key Vault Administrator's Guide

# Step 3: Add Disk Space to Extend the vg\_root for the Release 21.10 Upgrade

Before upgrading from Oracle Key Vault release 12.2 or 18 to 21, you need to extend the vg root to increase disk space.

If you are upgrading from an earlier Oracle Key Vault release 21.x and have already extended the vg root, then you can bypass this step.

Before you start this procedure, ensure that all endpoints have persistent cache enabled and in use.

- 1. Log in to the server for which you will perform the upgrade and switch user as root.
- 2. Ensure that the persistent cache settings for Oracle Key Vault have been set.

You will need to ensure that the persistent cache has been enabled because in a later step in this procedure, you must shut down the server. Shutting down the Oracle Key Vault server will incur downtime. To avoid any downtime, Oracle recommends that you turn on persistent cache.

3. Run the vgs command to determine the free space.

vgs

The VFree column shows how much free space you have (for example, 21 GB).

Power off the server in order to add a new disk.

```
/sbin/shutdown -h now
```

- 5. Add a new disk to the server with a capacity of 100 GB or greater.
- 6. Start the server.
- 7. Log in to the Oracle Key Vault server through SSH as user support, then switch user su to root.

```
ssh support@okv_server_IP_address
su - root
```

8. Stop the Oracle Key Vault services.

```
service tomcat stop;
service httpd stop;
service kmipus stop;
service kmip stop;
service okvogg stop;
service javafwk stop;
service monitor stop;
service controller stop;
service dbfwlistener stop;
service dbfwdb stop;
service rsyslog stop;
```



9. Run the fdisk -1 command to find if there are any available partitions on the new disk.

```
fdisk -l
```

At this stage, there should be no available partitions.

10. Run the fdisk disk device to be added command to create the new partition.

For example, to create a disk device named /dev/sdb:

```
fdisk /dev/sdb
```

In the prompts that appear, enter the following commands in sequence:

- n for new partition
- p for primary
- 1 for partition number
- Accept the default values for cylinder (press Enter twice).
- w to write and exit
- 11. Use the pvcreate <code>disk\_device\_partition</code> command to add the newly added disk to the physical volume.

For example, for a disk device named /dev/sdb1, which is the name of the disk partition that you created (based on the name used for the disk device that was added).

```
pvcreate /dev/sdb1
```

Output similar to the following appears:

```
Physical volume "/dev/sdb1" successfully created
```

**12.** Use the vgextend vg\_root disk\_device\_partition command to extend the logical volume with this disk space that you just added.

For example, for the partition /dev/sdb1, you would run:

```
vgextend vg_root /dev/sdb1
```

Output similar to the following appears:

```
Volume group "vg_root" successfully extended
```

**13.** Run the vgs command again to ensure that VFree shows an increase of 100 GB or more (depending on the size of the disk that was added).

vgs

Output similar to the following appears:



#### 14. Restart the Oracle Key Vault server.

/sbin/reboot

#### **Related Topics**

Oracle Key Vault Administrator's Guide

## Step 4: Upgrade the Oracle Key Vault Server

You can upgrade a standalone Oracle Key Vault server deployment.

- About Upgrading an Oracle Key Vault Server
   In a standalone deployment you must upgrade a single Oracle Key Vault server.
- Upgrading a Standalone Oracle Key Vault Server
   A single Oracle Key Vault server in a standalone deployment is sometimes used in test and development environments for functional testing.

### About Upgrading an Oracle Key Vault Server

In a standalone deployment you must upgrade a single Oracle Key Vault server.

Note that persistent caching enables endpoints to continue to be operational during the upgrade process.



If you are upgrading from a system with 4 GB RAM, first add 12 GB or more of additional RAM, following instructions for your specific hardware, before upgrading. Ensure that the persistent cache is enabled and set to sufficiently large values before attempting such operations so as to not incur endpoint downtime.

#### **Related Topics**

Oracle Key Vault Administrator's Guide

### Upgrading a Standalone Oracle Key Vault Server

A single Oracle Key Vault server in a standalone deployment is sometimes used in test and development environments for functional testing.

- Ensure that you have backed up the server you are upgrading so your data is safe and recoverable.
  - Do not proceed without completing this step.
- Log into the Oracle Key Vault management console as a user who has the System Administrator role.
- 3. Ensure that SSH access is enabled.

Log in to the Oracle Key Vault management console as a user who has the System Administrator role. Select the **System** tab, then **Settings**. In the Network Details area, click **SSH Access**. Select **IP address(es)** and then enter only the IP addresses that you need, or select **All**. Click **Save**.



- 4. Ensure you have enough space in the destination directory for the upgrade ISO files.
  - Do not copy this file to any location other than the /var/lib/oracle directory.
- 5. Log in to the Oracle Key Vault server through SSH as user support, then switch user su to root.

```
ssh support@okv_server_IP_address
su - root
```

If the SSH connection times out while you are executing any step of the upgrade, then the operation will not complete successfully. Oracle recommends that you ensure that you use the appropriate values for the ServerAliveInterval and ServerAliveCountMax options for your SSH sessions to avoid upgrade failures. Using the tmux command prevents network disconnections interrupting the upgrade. If the session terminates, resume as follows:

```
root# tmux a
```

Copy the upgrade ISO file to the destination directory using Secure Copy Protocol or other secure transmission method.



The upgrade ISO file is **not** the installation ISO file that you downloaded from eDelivery. You can download the Oracle Key Vault 21.10 upgrade software from https://updates.oracle.com/download/36884675.html.

root# scp user\_name@remote\_host:remote\_path/okv-upgrade-21.10.0.0.0.iso /var/lib/ oracle/

#### In this specification:

- remote host is the IP address of the computer containing the ISO upgrade file.
- remote\_path is the directory of the ISO upgrade file. Do not copy this file to any location other than the /var/lib/oracle directory.
- 7. As root, make the upgrade accessible by using the mount command:

```
root# mount -o loop,ro /var/lib/oracle/okv-upgrade-21.10.0.0.0.iso /images
```

8. Clear the cache using the clean all command:

```
root# yum -c /images/upgrade.repo clean all
```

9. Apply the upgrade with the upgrade.rb command:

```
root# ruby /images/upgrade.rb --confirm
```

If the system is successfully upgraded, then the command will display the following message:

```
Reboot now to continue the upgrade process.
```

If you see an error message, then check the log file /var/log/messages for additional information.



#### Note:

If the upgrade of the Oracle Key Vault system fails with the following message: Failed to apply update: The Oracle Key Vault upgrade has detected issues with FIPS mode. Please consult the Oracle Key Vault upgrade documentation or contact Oracle Support.

Apply patch 37688544 to correct the FIPS inconsistencies, and attempt the upgrade again.

- **10.** Apply patch 37763976, following the instructions in the patch readme.
- 11. Restart the Oracle Key Vault server by running the reboot command:

# reboot

On the first restart of the computer after the upgrade, assuming that the upgrade ISO file was copied to the /var/lib/oracle directory, the system will automatically mount /var/lib/oracle/okv-upgrade-21.10.0.0.0.iso and finish the upgrade process. (If the ISO is not auto-mounted, then the upgrade process will prompt for the ISO to be reattached.) This can take a few hours. Do not shut down the system during this time.

The upgrade is complete when the screen shows the following text: Oracle Key Vault Server version. This appliance was upgraded from previous\_release\_version. The revision reflects the upgraded release.

- **12.** Confirm that Oracle Key Vault has been upgraded to the correct version.
  - a. Log in to the Oracle Key Vault management console as a user who has the System Administrator role.
  - **b.** Select the **System** tab, and then select **Status**.
  - **c.** Verify that the version displayed is the latest release number.

The release number is also at the bottom of each page, to the right of the copyright information.

- **13.** If your site uses the Commercial National Security Algorithm (CNSA) suite, then re-install these algorithms onto the standalone server.
- 14. Restart the Oracle Key Vault system.

root# /sbin/reboot

15. Delete the upgrade ISO from the Oracle Key Vault server that was just upgraded.

For example:

root# /bin/rm -f /var/lib/oracle/okv-upgrade-21.10.0.0.0.iso

16. Disable SSH access.

Log in to the Oracle Key Vault management console as a user who has the System Administrator role. Select the **System** tab, then **Settings**. In the Network Details area, click **SSH Access**. Select **Disabled**. Click **Save**.

#### **Related Topics**

- Oracle Key Vault Administrator's Guide
- Oracle Key Vault Root of Trust HSM Configuration Guide



# Step 5: If Necessary, Add Disk Space to Extend Swap Space

If necessary, extend the swap space. Oracle Key Vault release 21.10 requires a hard disk size greater than or equal to 2 TB in size with approximately 64 GB of swap space.

If your system does not meet this requirement, follow these instructions to extend the swap space. You can check how much swap space you have by running the <code>swapon -s</code> command. By default, Oracle Key Vault releases earlier than release 18.1 were installed with approximately 4 GB of swap space. After you complete the upgrade to release 18.1 or later, Oracle recommends that you increase the swap space allocation for the server on which you upgraded Oracle Key Vault. A new Oracle Key Vault installation is automatically configured with sufficient swap space. However, if you upgraded from a previous release, and your system does not have the desired amount of swap space configured, then you must manually add disk space to extend the swap space, particularly if the intention is to convert the upgraded server into the first node of a multi-master cluster.

- 1. Log in to the server in which you upgraded Oracle Key Vault and connect as root.
- 2. Check the current amount of swap space.

```
[root@my okv server support]# swapon -s
```

Output similar to the following appears. This example shows that the system has 4 GB of swap space.

```
Filename Type Size Used Priority /dev/dm-0 partition 4194300 3368 -1
```

There **must** be 64 GB of swap space if the disk is greater than 1 TB in size.

3. Run the vgs command to determine how much free space is available.

```
vgs
```

The VFree column shows how much free space you have (for example, 21 GB).

Power off the server in order to add a new disk.

```
/sbin/shutdown -h now
```

- 5. Add a new disk to the server of a size that will bring the VFree value to over 64 GB.
- **6.** Start the server.
- 7. Log in to the Oracle Key Vault server through SSH as user support, then switch user su to root.

```
ssh support@okv_server_IP_address
su - root
```

8. Run the fdisk -1 command to find if there are any available partitions on the new disk.

```
fdisk -l
```



At this stage, there should be no available partitions.

9. Run the fdisk disk device to be added command to create the new partition.

For example, to create a disk device named /dev/sdc:

```
fdisk /dev/sdc
```

In the prompts that appear, enter the following commands in sequence:

- n for new partition
- p for primary (the primary partition)
- 1 for partition number
- Accept the default values for cylinder (press Enter twice).
- w to write and exit
- **10.** Use the pvcreate <code>disk\_device\_partition</code> command to add the newly added disk to the physical volume.

For example, for a disk device named /dev/sdc1, which is the name of the disk partition that you created (based on the name used for the disk device that was added).

```
pvcreate /dev/sdc1
```

Output similar to the following appears:

```
Physical volume "/dev/sdc1" successfully created
```

**11.** Use the vgextend vg\_root disk\_device\_partition command to extend the logical volume with this disk space that you just added.

For example, for the partition /dev/sdc1, you would run:

```
vgextend vg root /dev/sdc1
```

Output similar to the following appears:

```
Volume group "vg root" successfully extended
```

12. Run the vgs command again to ensure that VFree shows an increase of 64 GB.

vgs

13. Disable swapping.

```
[root@my okv server support]# swapoff -v /dev/vg root/lv swap
```

**14.** To extend the swap space, run the lyresize command.

```
[root@my okv server support]# lvresize -L +60G /dev/vg root/lv swap
```



#### Output similar to the following appears:

```
Size of logical volume vg_root/lv_swap changed from 4.00 GiB (128 extents) to 64.00 GiB (2048 extents) Logical volume lv swap successfully resized.
```

**15.** Format the newly added swap space.

```
[root@my okv server support] # mkswap /dev/vg root/lv swap
```

#### Output similar to the following appears:

```
mkswap: /dev/vg_root/lv_swap: warning: don't erase bootbits sectors
on whole disk. Use -f to force.
Setting up swapspace version 1, size = 67108860 KiB
no label, UUID=fea7fc72-0fea-43a3-8e5d-e29955d46891
```

**16.** Enable swapping again.

```
[root@my okv server support] # swapon -v /dev/vg root/lv swap
```

17. Verify the amount of swap space that is available.

```
[root@my okv server support]# swapon -s
```

#### Output similar to the following appears:

```
Filename Type Size Used Priority /dev/dm-0 partition 67108860 0 -1
```

18. Restart the Oracle Key Vault server.

/sbin/reboot

## Step 6: If Necessary, Remove Old Kernels

Oracle recommends that you clean up the older kernels that were left behind after the upgrade.

While the older kernel is not in use, it may be marked as an issue by some code analysis tools.

- 1. Log in to the Oracle Key Vault server as the support user.
- 2. Switch to the root user.

```
su - root
```

- 3. Mount /boot if it was not mounted on the system.
  - a. Check if the /boot is mounted. The following command should display /boot information if it was mounted.

```
df -h /boot;
```

**b.** Mount it if /boot is not mounted.

/bin/mount /boot;

For EFI-based systems, you may need to mount /boot/efi if it is not already mounted.

```
/bin/mount /boot/efi
```

- 4. Check the installed kernels and the running kernel.
  - Search for any kernels that are installed.

```
rpm -q kernel-uek | sort;
```

The following example output shows that two kernels are installed:

```
kernel-uek-5.4.17-2136.318.7.2.el8uek.x86_64
kernel-uek-5.4.17-2136.329.3.1.el8uek.x86_64
```

b. Check the latest kernel.

```
uname -r;
```

The following output shows an example of a kernel version that was installed at the time:

```
5.4.17-2136.329.3.1.el8uek.x86 64
```

This example assumes  $5.4.17-2136.329.3.1.e18uek.x86_64$  as the latest version (newer versions may be available by now). Based on the output from the commands above, remove the older kernel (kernel-uek- $5.4.17-2136.318.7.2.e18uek.x86_64$ ). You should remove all kernels that are older than the latest kernel.

Remove the older kernel and its associated RPMs.

```
For example, to remove the kernel-uek-5.4.17-2136.318.7.2.el8uek.x86_64
# yum --disablerepo=* remove `rpm -qa|grep kernel-uek-5.4.17-2136.318.7.2.el8uek`
```

Output similar to the following appears:

```
Resolving Dependencies
--> Running transaction check
---> Package kernel-uek.x86 64 0:4.14.35-2047.504.2.el7uek will be erased
---> Package kernel-uek-devel.x86 64 0:4.14.35-2047.504.2.el7uek will be erased
--> Finished Dependency Resolution
Dependencies resolved.
______
Package Arch Version Repository Size
______
Removina:
kernel-uek x86 64 5.4.17-2136.318.7.2.el8uek @avdf-base-os 135 M
Transaction Summary
______
Remove 1 Package
Freed space: 135 M
Is this ok [y/N]:
```

- **6.** Enter y to accept the deletion output.
- 7. Repeat these steps starting with Step 4 for all kernels that are older than the latest kernel.

# Step 7: If Necessary, Remove SSH-Related DSA Keys

You should remove SSH-related DSA keys left behind after the upgrade, because they can cause problems with some code analysis tools.

- Log in to the Oracle Key Vault management console as a user with the System Administrator role.
- 2. Enable SSH.

Log in to the Oracle Key Vault management console as a user who has the System Administrator role. Select the **System** tab, then **Settings**. In the Network Details area, click **SSH Access**. Select **IP address(es)** and then enter only the IP addresses that you need, or select **All**. Click **Save**.

3. Login to the Oracle Key Vault support account using SSH.

```
ssh support@OracleKeyVault serverIPaddress
```

Switch to the root user.

```
su - root
```

Change directory to /etc/ssh.

```
cd /etc/ssh
```

6. Rename the following keys.

```
mv ssh_host_dsa_key.pub ssh_host_dsa_key.pub.retire
mv ssh host dsa key ssh host dsa key.retire
```

7. Disable SSH access.

Log in to the Oracle Key Vault management console as a user who has the System Administrator role. Select the **System** tab, then **Settings**. In the Network Details area, click **SSH Access**. Select **Disabled**. Click **Save**.

# Step 8: Upgrade the Endpoint Software

As part of the upgrade, you must reenroll endpoints created in earlier releases of Oracle Key Vault, or update the endpoint software.

The easiest way to upgrade the Oracle Key Vault client software is to re-enroll an endpoint. Reenrolling generates a new <code>okvclient.jar</code> file, but maintains the relationship between the endpoint and its (default) wallet. Re-enrolling can be fully scripted using the <code>okv admin</code> endpoint re-enroll and <code>okv admin</code> endpoint provision commands.

Before an endpoint that uses Oracle Key Vault for TDE key management can take advantage of new Oracle Key Vault features, for example non-extractable TDE master keys, it must be upgraded to match the new Oracle Key Vault release.

- 1. If you are upgrading the endpoint software for an Oracle database configured for online TDE master encryption key management, then shut down the database.
- 2. Download the endpoint software (okvclient.jar) for your platform from the Oracle Key Vault server as follows:
  - a. Go to the Oracle Key Vault management console login screen.
  - b. Click the Endpoint Enrollment and Software Download link.
  - c. In the **Download Endpoint Software Only** section, select the appropriate platform from the drop-down list.

- Click the **Download** button.
- 3. Identify the path to your existing endpoint installation that you are about to upgrade (for example, /etc/ORACLE/KEYSTORES/okv (where /etc/ORACLE/KEYSTORES is WALLET\_ROOT of your database, or the softlink in \$ORACLE BASE/okv/\$ORACLE SID points to).
- 4. Install the endpoint software by executing the following command:

```
java -jar okvclient.jar -d existing endpoint directory path
```

#### For example:

```
java -jar okvclient.jar -d /etc/ORACLE/KEYSTORES/okv
```

5. Install the updated PKCS#11 library file.

This step is needed only for online TDE master encryption key management by Oracle Key Vault. If an endpoint uses online TDE master encryption key management by Oracle Key Vault, then you must upgrade the PKCS#11 library while upgrading the endpoint software.

• On UNIX/Linux platforms: Run root.sh from the bin directory of endpoint installation directory to copy the latest liborapkcs.so file for Oracle Database endpoints.

```
$ sudo /etc/ORACLE/KEYSTORES/okv/bin/root.sh
```

#### Or

```
$ su - root
# /etc/ORACLE/KEYSTORES/oky/bin/root.sh
```

On Windows platforms: Run root.bat from the bin directory of endpoint installation directory to copy the latest liborapkcs.dll file for Oracle Database endpoints. You will be prompted for the version of the database in use.

```
bin\root.bat
```

6. Update the SDK software.

If you have already deployed the SDK software, Oracle recommends that you redeploy the SDK software in the same location after you complete the upgrade to Oracle Key Vault release 21.10. This enables you to have access to the new SDK APIs that were introduced since the Oracle Key Vault version that you are upgrading from.

- a. Go to the Oracle Key Vault management console login screen.
- b. Click the Endpoint Enrollment and Software Download link.
- c. In the Download Software Development Kit section, select the appropriate language and platform for your site.
- d. Click the **Download** button to get the SDK zip file.
- Identify the existing location where SDK software was already deployed.
- f. Navigate to the directory in which you saved the SDK zip file.
- g. Unzip the SDK zip file.

For example, on Linux, to unzip the Java SDK zip file, use the following command:

```
unzip -o okv_jsdk.zip -d existing_endpoint_sdk_directory_path
```



For the C SDK zip file, use this command:

```
unzip -o okv csdk.zip -d existing endpoint sdk directory path
```

- h. Do not exit this page.
- 7. If you had deployed the RESTful services utility in the previous release, then redeploy the latest okvrestclipackage.zip file.

The latest <code>okvrestclipackage.zip</code> file enables you to have access to the new RESTful services utility commands that were introduced since the Oracle Key Vault version that you are upgrading from.

You can use wget or curl to download okvrestclipackage.zip.

```
wget --no-check-certificate https://Oracle_Key_Vault_IP_address:5695/
okvrestclipackage.zip
curl -O -k https://Oracle Key Vault IP address:5695/okvrestservices.jar
```

8. Start the Oracle databases if the upgrade of Oracle Key Vault endpoints for all of the TDE-enabled databases on this host machine is complete.

The easiest way to upgrade the Oracle Key Vault client software is to re-enroll an endpoint. Re-enrolling generates a new <code>okvclient.jar</code> file, but maintains the relationship between the endpoint and its (default) wallet.

- 9. If your site requires that you restrict TDE master encryption keys from leaving Oracle Key Vault and if you are using an Oracle Real Application Clusters (Oracle RAC) environment, then perform the following steps on each Oracle RAC node:
  - a. Perform the endpoint upgrade on each Oracle RAC node.
  - **b.** Set the extractable attribute value for symmetric keys.

By default, the extractable attribute value is true, which means that the key material of symmetric keys can be extracted from Oracle Key Vault during certain operations. If you want to prevent symmetric keys from being extracted, then you must set this value to false. You can set an extractable attribute value as follows:

- Set the default value for the extractable attribute of new symmetric keys in the endpoint settings. Endpoint-specific setting overrides the global endpoint settings.
- Explicitly specify the value of the extractable attribute when creating or registering a new symmetric key.
- Modify the extractable attribute of an existing symmetric key.

See Oracle Key Vault Administrator's Guide.

c. As a user who has the SYSDBA or SYSKM administrative privilege, perform a rekey operation on one Oracle RAC node. Use the following syntax:

```
ADMINISTER KEY MANAGEMENT SET [ENCRYPTION] KEY [FORCE KEYSTORE] [USING TAG 'tag_name'] IDENTIFIED BY [EXTERNAL STORE | keystore password;
```

See *Oracle Database Advanced Security Guide* for more information about rekeying a TDE master encryption key.

- 10. If your site requires that you restrict TDE master encryption keys from leaving Oracle Key Vault and if you are using an Oracle Data Guard environment, then do the following on the primary and standby databases:
  - a. Perform the endpoint upgrade on the primary and standby databases.
  - b. If your site requires it, then set the extractable attribute value for symmetric keys.

By default, the extractable attribute value is true, which means that the key material of symmetric keys can be extracted from Oracle Key Vault during certain operations. If you want to prevent symmetric keys from being extracted, then you must set this value to false. You can set an extractable attribute value as follows:

- Set the default value for the extractable attribute of new symmetric keys in the endpoint settings. Endpoint-specific setting overrides the global endpoint settings.
- Explicitly specify the value of the extractable attribute when creating or registering a new symmetric key.
- Modify the extractable attribute of an existing symmetric key.

See Oracle Key Vault Administrator's Guide.

c. As a user who has the SYSDBA or SYSKM administrative privilege, perform a rekey operation in the primary database.

```
ADMINISTER KEY MANAGEMENT SET [ENCRYPTION] KEY
[FORCE KEYSTORE]
[USING TAG 'tag_name']
IDENTIFIED BY [EXTERNAL STORE | keystore password;
```

See *Oracle Database Advanced Security Guide* for more information about rekeying a TDE master encryption key.

#### Note:

- You must run root.sh or root.bat script to install the latest Oracle Key Vault PKCS#11 library only once on a host machine that has multiple TDE-enabled Oracle databases that use Oracle Key Vault for master encryption key management.
- Ensure that you execute the root.sh or root.batscript only after the upgrade of Oracle Key Vault endpoints for all of the TDE-enabled databases on the same host machine is complete.
- Ensure that all of the TDE-enabled Oracle databases on this host have been shutdown.
- If you are upgrading the endpoint software for an Oracle database configured for online TDE master encryption key management, then shut down the database.

#### **Related Topics**

Oracle Key Vault Administrator's Guide



# Step 10: Back Up the Upgraded Oracle Key Vault Server

You must perform server backup and user password tasks after completing a successful upgrade.

- 1. Take a full backup of the upgraded Oracle Key Vault Server Database to a new remote destination. Avoid using the old backup destination for the new backups.
- 2. Schedule a new periodic incremental backup to the new destination defined in the preceding step.
- 3. Change the Oracle Key Vault administrative passwords.

Password hashing has been upgraded to a more secure standard than in earlier releases. This change affects the operating system passwords, support and root. You must change Oracle Key Vault administrative passwords after the upgrade to take advantage of the more secure hash.



7

# Upgrading Oracle Key Vault from an Earlier 21.x Release in a Multi-Master Cluster Environment

Similar to a standalone or primary-standby upgrade for release 21.x, this type of upgrade includes the Oracle Key Vault server software and endpoint software-related utilities.

- About Upgrading Oracle Key Vault from an Earlier 21.x Release in a Multi-Master Cluster Environment
  - To perform this upgrade, you must upgrade each multi-master cluster node.
- Step 1: Perform Pre-Upgrade Tasks for the Upgrade from the Earlier 21.x Release Similar to a standalone or primary-standby environment, you must perform pre-upgrade tasks such as backing up the Oracle Key Vault server.
- Step 2: Upgrade Each Multi-Master Cluster Node
   To upgrade the multi-master cluster, you must upgrade each multi-master cluster node, one after the other.
- Step 3: If Necessary, Change the Network Interface for Upgraded Nodes
   Nodes that were created in Oracle Key Vault releases earlier than release 21.1 use Classic mode, in which only one network interface was used.
- Step 4: Check the Node Version and the Cluster Version

  After you complete the upgrade of at least one node, you can log into any of the upgraded nodes to check the node and cluster versions.
- Step 5: If Necessary, Add Disk Space to Extend Swap Space
   If necessary, extend the swap space on each node. Oracle Key Vault release 21.10
   requires a hard disk size greater than or equal to 1 TB in size with approximately 64 GB of
   swap space.
- Step 6: If Necessary, Remove Old Kernels
   For each multi-master cluster node, Oracle recommends that you clean up the older kernels that were left behind after the upgrade.
- Step 7: If Necessary, Remove SSH-Related DSA Keys
   For each multi-master cluster node, you should remove SSH-related DSA keys left behind
   after the upgrade.
- Step 8: Upgrade the Endpoint Software
  After you have upgraded all the nodes in the cluster, you must reenroll endpoints that were
  created in earlier releases of Oracle Key Vault, or update the endpoint software.

# About Upgrading Oracle Key Vault from an Earlier 21.x Release in a Multi-Master Cluster Environment

To perform this upgrade, you must upgrade each multi-master cluster node.

For Oracle Key Vault 21.10 you need to upgrade to 21.x. If you are using the version earlier than 21.x, make sure to upgrade the version to 21.x first before proceeding with the version update to 21.10.

The upgrade process involves performing the upgrade on each multi-master cluster node. After you have begun a cluster upgrade, ensure that you upgrade all the nodes in the cluster one after the other, without too much intervening time between upgrades of two nodes.

Upgrading an Oracle Key Vault multi-master cluster includes upgrading each cluster node to the new later version. You must upgrade all nodes to the same Oracle Key Vault version. You should first upgrade the read-only nodes of the cluster, and then upgrade the read-write pairs. As each cluster node is upgraded, its node version is updated to the new version of the Oracle Key Vault. After you complete the upgrade of all cluster nodes, the cluster version is updated to the new version of the Oracle Key Vault. You can check the node version or the cluster version by selecting the **Cluster** tab, then in the left navigation bar, selecting **Management**. Oracle Key Vault multi-master cluster upgrade is considered complete when node version and cluster version at each cluster node is updated to the latest version of Oracle Key Vault.

Before you perform the upgrade, note the following:

- Perform the entire upgrade process on all multi-master cluster nodes, without interruption. That is, after you have started the cluster upgrade process, ensure that you try and upgrade all nodes, individually one after the other or in read-write pairs. Do not perform any critical operations or make configuration changes to Oracle Key Vault until you have completed upgrading all the nodes in your environment.
- Be aware that you cannot use any new features that were introduced in this release until
  you have completed upgrading all of the multi-master cluster nodes. An error is returned
  when such features are used from the node that has been upgraded. Oracle recommends
  that you plan the upgrade of all cluster nodes close to each other to ensure availability of
  the new features sooner.
- Starting in Oracle Key Vault release 21.2, expiration alerts for deactivated or destroyed objects are not generated. If you are upgrading from Oracle Key Vault release 21.1 or earlier, then the following behavior is expected:
  - As each cluster node is upgraded, Oracle Key Vault deletes all expiration alerts for any certificate and secret objects, as well as for key objects that have been revoked or destroyed.
  - Cluster nodes that have not been upgraded yet will continue to generate alerts for these same objects, and also send email notifications for these alerts. This behavior that results in deletion and recreation of alerts may repeat until the last cluster node is upgraded.
  - After the upgrade is complete, expiration alerts for the certificate and secret objects will have the alert type of Certificate Object Expiration and Secret Object Expiration, respectively.

#### **Related Topics**

Step 4: Check the Node Version and the Cluster Version
 After you complete the upgrade of at least one node, you can log into any of the upgraded nodes to check the node and cluster versions.



# Step 1: Perform Pre-Upgrade Tasks for the Upgrade from the Earlier 21.x Release

Similar to a standalone or primary-standby environment, you must perform pre-upgrade tasks such as backing up the Oracle Key Vault server.

If you plan to perform an upgrade of the Oracle Key Vault server, then disable the diagnostics packaging utility by ensuring that there are no files available to download. This can be confirmed by checking if the **Diagnostics** page has a section called **Diagnostics Package Files**. If it does, click **Clear** to disable the utility.

- In the server where Oracle Key Vault is installed, log in as user support, and then switch to the root user.
- 2. Back up the server so that you can recover data in case the upgrade fails.
- 3. Ensure that no full or incremental backup jobs are running. Delete all scheduled full or incremental backup jobs before the upgrade.
- 4. Ensure that the server meets the minimum disk space requirements for an upgrade. For example, 6 GB of free space in the /usr/local/dbfw/tmp directory. See the Oracle Key Vault Readme for this release to determine the disk space requirements for the upgrade.
- 5. Ensure that you disable diagnostics and clean up disk space in /usr/local/dbfw/tmp before you upgrade by performing the following steps:

If the Oracle Key Vault system being upgraded is from release 21.6 or later, log in to the Oracle Key Vault management console as a user with the System Administrator role, and navigate to the **System** tab, and then click the **Diagnostics** button.

If the Diagnostics Package Files pane is displayed, then click **Clear** to disable diagnostics. Note that the **Diagnostics Package Files** pane will be displayed only if the diagnostics bundle was previously generated, and the files were not cleared.

If the Diagnostics Package Files pane is not displayed, or if the diagnostics bundle was previously generated using the **dbfw-diagnostics-package.rb** utility, then log in to the Oracle Key Vault system and run the following commands to disable diagnostics and clean up disk space in /usr/local/dbfw/tmp:

a. SSH into the Oracle Key Vault system as user support, then switch to user root:

```
ssh support@<OKV_IP_Address>
su - root
```

b. Delete the generated diagnostics zip file and remove the package using the following commands:

```
/usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --clean /usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --remove
```

6. Plan for downtime according to the following specifications:

Oracle Key Vault Usage	Downtime required
Wallet upload or download	NO
Java Keystore upload or download	NO



Oracle Key Vault Usage	Downtime required
Transparent Data Encryption (TDE) direct connect	YES (NO with persistent cache)
Primary Server Upgrade in a primary-standby deployment	YES (NO with persistent cache)

The Oracle Key Vault client software is backward-compatible. Older Oracle Key Vault client software versions are completely functional with the upgraded Oracle Key Vault server, the new features of Oracle Key Vault are only available with the current client software. TDE-enabled databases before 21c need to restart to load the updated Oracle Key Vault PKCS#11 library that is deployed as part of the Oracle Key Vault client software upgrade. Oracle Database 21c and later can dynamically load the new Oracle Key Vault PKCS#11 library, without downtime. Database endpoints can be upgraded in parallel to reduce total downtime.

- 7. If the Oracle Key Vault system has a syslog destination configured, ensure that the remote syslog destination is reachable from the Oracle Key Vault system, and that logs are being correctly forwarded. If the remote syslog destination is not reachable from the Oracle Key Vault system, then the upgrade process can become much slower than normal.
- 8. Check the disk size before you begin the upgrade. If any of the nodes in question have a disk size that is greater than 2 TB and uses BIOS boot mode, then you cannot upgrade that system to the new release. Oracle recommends that you remove the node from the cluster and if possible, replace it with a node whose disk is less than 2 TB in size.
- 9. If you need to increase available disk space, then remove the temporary jar files located in /usr/local/okv/ssl. Be careful in doing so. If you accidentally delete any files other than the jar files in /usr/local/okv/ssl, then the Oracle Key Vault server becomes non-functional.
- 10. Check the boot partition size. If any of the nodes in question have a boot partition that is less than 500 MB, then you cannot upgrade that system to the new release. You can check this size as follows:
  - a. Mount the /boot partition.

/bin/mount /boot

b. Check the Size column given by the following command:

/bin/df -h /boot

c. Unmount the /boot partition:

/bin/umount /boot

If the boot partition given by this command shows less than 488 MB, then you cannot upgrade to the current release. Oracle recommends that you remove the node from the cluster and if possible, replace it with a node that has been freshly installed with the same Oracle Key Vault version as the rest of the cluster nodes.

- 11. Increase the Maximum Disable Node Duration setting as appropriate so that any disabled cluster nodes have sufficient time to be upgraded then enabled back into the cluster. Note that increasing the Maximum Disable Node Duration setting also increases disk space usage.
- 12. Plan to disable one node at a time.
- **13.** If Oracle Audit Vault was integrated with Oracle Key Vault in Oracle Key Vault release 21.2 or earlier, then do the following to disable and remove the Oracle Audit Vault integration:



- a. Disable the Oracle Audit Vault integration: Log into the Oracle Key Vault management console as a System Administrator, select the **System** tab and then **Settings** from the left navigation bar. In the Monitoring and Alerts pane, select Audit Vault. In the Audit Vault integration pane that appears, disable Oracle Audit Vault. Click **Save**.
- **b.** Log in to the Oracle Key Vault server through SSH as user support, switch user su to root and then switch user su to oracle.
- **c.** Stop the agent by executing the following command:

```
agent installation directory/bin/agentctl stop
```

- d. Log in to the Oracle Audit Vault Server console as an Oracle Audit Vault administrator.
- e. Delete the corresponding agent and target.
- f. Log in to the Oracle Key Vault server through SSH as user support, then switch user su to root.
- g. Delete the installation directory for the Oracle Audit Vault agent.
- **14.** Ensure that the Oracle Key Vault server certificate has not expired, nor is close to expiry, before you begin the upgrade.

You can find how much time the Oracle Key Vault server certificate has before it expires by checking the **OKV Server Certificate Expiration** setting on the Configure Alerts page in the Oracle Key Vault management console.

**15.** If you are performing an upgrade while using an HSM as a Root of Trust, then consult *Oracle Key Vault Root of Trust HSM Configuration Guide* for any additional steps that may be needed.

#### Note:

If you are upgrading from release 21.9.0.0.0 to release 21.10.0.0.0, Oracle recommends that you apply patch 37492574 before beginning the upgrade. This patch corrects the configuration of certain processes internal to Oracle Key Vault, and prevents upgrades to 21.10.0.0.0 from failing. Apply this patch to all systems in the Oracle Key Vault 21.9.0.0.0 deployment before beginning upgrade to 21.10.0.0.0.

- 16. Ensure that the backup of the orapwdbfwdb file matches the original file.
  - a. SSH into the Oracle Key Vault system as user support, then switch to user root:

```
ssh support@<OKV_IP_Address>
su - root
```

**b.** Verify that the backup file exists:

```
su - oracle
ls -ltr /var/lib/oracle/okv_orapwd_backup_dir/orapwdbfwdb
```

c. If the backup file exists, then perform the following steps:



Compare the original file with the backup file:

```
diff /var/lib/oracle/dbfw/dbs/orapwdbfwdb /var/lib/oracle/
okv_orapwd_backup_dir/orapwdbfwdb
```

• If there is a difference between the files, then update the backup file by copying the original file:

```
cp /var/lib/oracle/dbfw/dbs/orapwdbfwdb /var/lib/oracle/
okv_orapwd_backup_dir/orapwdbfwdb
```

- **17.** If you are upgrading from Oracle Key Vault release 21.x to release 21.10.0.0.0, then Oracle recommends that you apply the following patches:
  - Patch 37688544, to be applied before you start the upgrade. This patch corrects any FIPS inconsistencies on the system and prevents upgrades from failing with the following error:

```
ODF-10001: Internal error: FAILED migration: okv save restore orapwd config["backup orapwd config"].
```

Apply this patch to all systems in the Oracle Key Vault deployment before you start the upgrade to 21.10.0.0.0.

Patch 37763976, to be applied after starting the upgrade with the ruby /images/upgrade.rb -confirm command but before resuming the upgrade with the /sbin/reboot command.

#### **Related Topics**

- Step 3: Add Disk Space to Extend the vg\_root for the Release 21.10 Upgrade
  Before upgrading from Oracle Key Vault release 12.2 or 18 to 21, you need to extend the
  vg\_root to increase disk space.
- Step 2: Perform Pre-Upgrade Tasks for the Standalone Oracle Key Vault To ensure a smooth upgrade to Oracle Key Vault, you should prepare the server you are upgrading.
- Oracle Key Vault Administrator's Guide

### Step 2: Upgrade Each Multi-Master Cluster Node

To upgrade the multi-master cluster, you must upgrade each multi-master cluster node, one after the other.

Do not use other Oracle Key Vault features until you have completed upgrading *all* multi-master cluster nodes. Ensure that you have successfully backed up Oracle Key Vault before you begin the upgrade of the multi-master cluster nodes.

- **1.** Ensure that you have performed the pre-upgrade steps.
- 2. Disable the multi-master cluster node.
  - Log into the cluster node that you want to upgrade as a user with the System Administrator role.
  - b. Select the **Cluster** tab, and then select **Management** from the left navigation bar.
  - c. Under Cluster Details, in the Select Node column, select the check box of the node to disable.

d. Click Disable.

In the node's **Management** page (under the **Cluster** tab), the node's status will change from DISABLING to DISABLED.

3. Ensure that SSH access is enabled for the node.

Select the **System** tab, then **Settings**. In the Network Details area, click **SSH Access**. Select **IP address(es)** and then enter only the IP addresses that you need, or select **All**. Click **Save**.

- 4. Ensure that you have enough space in the destination directory for the upgrade ISO files.
- 5. Log in to the Oracle Key Vault server through SSH as user support, then switch user su to root.

```
ssh support@okv_server_IP_address
su - root
```

If the SSH connection times out while you are executing any step of the upgrade, then the operation will not complete successfully. Oracle recommends that you ensure that you use the appropriate values for the <code>ServerAliveInterval</code> and <code>ServerAliveCountMax</code> options for your SSH sessions to avoid upgrade failures.

Using the tmux command prevents network disconnections interrupting the upgrade. If the session terminates, resume as follows:

```
tmux a
```

Copy the upgrade ISO file to the destination directory using SCP or other secure transmission method.

```
scp remote_host:remote_path/okv-upgrade-disc-
new_software_release.iso /var/lib/oracle
```

#### In this specification:

- remote host is the IP address of the computer containing the ISO upgrade file.
- remote\_path is the directory of the ISO upgrade file. Do not copy this file to any location other than the /var/lib/oracle directory.
- 7. Make the upgrade accessible by using the mount command:

```
/bin/mount -o loop,ro /var/lib/oracle/okv-upgrade-disc-new_software_release.iso /images
```

8. Clear the cache using the clean all command:

```
yum -c /images/upgrade.repo clean all
```

**9.** Apply the upgrade with the upgrade.rb command:

```
root# ruby /images/upgrade.rb --confirm
```



If the system is successfully upgraded, then the command will display the following message:

Reboot now to continue the upgrade process.

If you see an error message, then check the log file /var/log/messages for additional information.



If the upgrade of the Oracle Key Vault system fails with the following message: Failed to apply update: The Oracle Key Vault upgrade has detected issues with FIPS mode. Please consult the Oracle Key Vault upgrade documentation or contact Oracle Support

Apply patch 37688544 to correct the FIPS inconsistencies, and attempt the upgrade again.

- **10.** Apply patch 37763976, following the instructions in the patch readme.
- 11. Restart the Oracle Key Vault server by running the reboot command:

# reboot

On the first restart of the computer after the upgrade, the system will apply the necessary changes. This can take a few hours. Do not shut down the system during this time. The upgrade of the cluster node is completed when the screen with heading: Oracle Key Vault Server new\_software\_release appears, with new\_software\_release reflecting the release number of the upgraded version. Following the heading appears the menu item **Display Appliance Info**. Select **Display Appliance Info** and press the **Enter** key to see the IP address settings for the appliance.

- **12.** If you are performing an HSM upgrade using Entrust (formerly nCipher), then perform the additional steps described in *Oracle Key Vault Root of Trust HSM Configuration Guide*.
- 13. After the node has been successfully upgraded, re-enable it.
  - a. Log into the Oracle Key Vault node that you just upgraded as a user who has the System Administrator role.
  - b. Select the **Cluster** tab, and then select **Management** from the left navigation bar.
  - In the Cluster Details section, under Name, click the name of the node that you had disabled.
  - d. Click Enable.

After you re-enable the disabled multi-master cluster node, its status changes from DISABLED to ENABLING, then to ACTIVE. The status of the node will remain at ENABLING and will not change to ACTIVE unless bidirectional replication between it and all other nodes is occurring successfully.

14. As necessary, disable SSH access on this node.

Select the **System** tab, then **Settings**. In the Network Details area, click **SSH Access**. Select **Disabled**. Click **Save**.

**15.** After you have successfully completed this procedure, repeat these upgrade steps on all multi-master cluster nodes.



# Step 3: If Necessary, Change the Network Interface for Upgraded Nodes

Nodes that were created in Oracle Key Vault releases earlier than release 21.1 use Classic mode, in which only one network interface was used.

If you prefer to use dual NIC network mode, which supports the use two network interfaces, then you can switch the node to use this mode, from the command line.

#### **Related Topics**

Oracle Key Vault Administrator's Guide

# Step 4: Check the Node Version and the Cluster Version

After you complete the upgrade of at least one node, you can log into any of the upgraded nodes to check the node and cluster versions.

Oracle Key Vault tracks the version information of each cluster node as well as the version of the cluster as a whole. The node version represents the version of the Oracle Key Vault software on a given node. When a node is upgraded, its node version is updated to the new version of the Oracle Key Vault software. The cluster version is derived from the version information of the cluster nodes and is set to the minimum version of any cluster node. During cluster upgrade, node version is updated as each cluster node is upgraded to the later version. When all of the cluster nodes have been upgraded, the cluster version is then updated to the new version. (The Cluster Version and Node Version fields are available in Oracle Key Vault release 18.2 or later.)

- 1. Log in to the Oracle Key Vault management console as a user who has the System Administrator role.
- 2. Select the Cluster tab.
- 3. In the left navigation bar, select Management.
- 4. Check the following areas:
  - To find the node version, check the Cluster Details area.
  - To find the cluster version, check the Cluster Information area.

# Step 5: If Necessary, Add Disk Space to Extend Swap Space

If necessary, extend the swap space on each node. Oracle Key Vault release 21.10 requires a hard disk size greater than or equal to 1 TB in size with approximately 64 GB of swap space.

If your system does not meet this requirement, follow these instructions to extend the swap space. You can check how much swap space you have by running the <code>swapon -s</code> command. By default, Oracle Key Vault releases earlier than release 18.1 were installed with approximately 4 GB of swap space. After you complete the upgrade to release 18.1 or later, Oracle recommends that you increase the swap space allocation for the server on which you upgraded Oracle Key Vault. A new Oracle Key Vault installation is automatically configured with sufficient swap space. However, if you upgraded from a previous release, and your system does not have the desired amount of swap space configured, then you must manually add disk space to extend the swap space, particularly if the intention is to convert the upgraded server into the first node of a multi-master cluster.



- 1. Log in to the server in which you upgraded Oracle Key Vault and connect as root.
- Check the current amount of swap space.

```
[root@my_okv_server support]# swapon -s
```

Output similar to the following appears. This example shows that the system has 4 GB of swap space.

```
Filename Type Size Used Priority /dev/dm-0 partition 4194300 3368 -1
```

There **must** be 64 GB of swap space if the disk is greater than 1 TB in size.

3. Run the vgs command to determine how much free space is available.

vgs

The VFree column shows how much free space you have (for example, 21 GB).

4. Power off the server in order to add a new disk.

```
/sbin/shutdown -h now
```

- 5. Add a new disk to the server of a size that will bring the VFree value to over 64 GB.
- 6. Start the server.
- 7. Log in to the Oracle Key Vault server through SSH as user support, then switch user su to root.

```
ssh support@okv_server_IP_address
su - root
```

8. Run the fdisk -1 command to find if there are any available partitions on the new disk.

```
fdisk -l
```

At this stage, there should be no available partitions.

Run the fdisk disk device to be added command to create the new partition.

For example, to create a disk device named /dev/sdc:

```
fdisk /dev/sdc
```

In the prompts that appear, enter the following commands in sequence:

- n for new partition
- p for primary
- 1 for partition number
- Accept the default values for cylinder (press Enter twice).
- w to write and exit



**10.** Use the pvcreate <code>disk\_device\_partition</code> command to add the newly added disk to the physical volume.

For example, for a disk device named /dev/sdc1, which is the name of the disk partition that you created (based on the name used for the disk device that was added).

```
pvcreate /dev/sdc1
```

#### Output similar to the following appears:

```
Physical volume "/dev/sdc1" successfully created
```

11. Use the vgextend vg\_root disk\_device\_partition command to extend the logical volume with this disk space that you just added.

For example, for the partition /dev/sdc1, you would run:

```
vgextend vg root /dev/sdc1
```

#### Output similar to the following appears:

```
Volume group "vg root" successfully extended
```

12. Run the vgs command again to ensure that VFree shows an increase of 64 GB.

vgs

13. Disable swapping.

```
[root@my okv server support]# swapoff -v /dev/vg root/lv swap
```

**14.** To extend the swap space, run the lyresize command.

```
[root@my okv server support]# lvresize -L +60G /dev/vg root/lv swap
```

#### Output similar to the following appears:

```
Size of logical volume vg_root/lv_swap changed from 4.00 GiB (128 extents) to 64.00 GiB (2048 extents) Logical volume lv swap successfully resized.
```

**15**. Format the newly added swap space.

```
[root@my_okv_server support]# mkswap /dev/vg_root/lv_swap
```

#### Output similar to the following appears:

```
mkswap: /dev/vg_root/lv_swap: warning: don't erase bootbits sectors
on whole disk. Use -f to force.
Setting up swapspace version 1, size = 67108860 KiB
no label, UUID=fea7fc72-0fea-43a3-8e5d-e29955d46891
```



Enable swapping again.

```
[root@my okv server support]# swapon -v /dev/vg root/lv swap
```

17. Verify the amount of swap space that is available.

```
[root@my okv server support]# swapon -s
```

Output similar to the following appears:

```
Filename Type Size Used Priority /dev/dm-0 partition 67108860 0 -1
```

18. Restart the Oracle Key Vault server.

```
/sbin/reboot
```

For primary-standby deployments, ensure that the primary and standby nodes sync up before proceeding further with next steps.

## Step 6: If Necessary, Remove Old Kernels

For each multi-master cluster node, Oracle recommends that you clean up the older kernels that were left behind after the upgrade.

While the older kernel is not in use, it may be marked as an issue by some code analysis tools.

- Log in to the Oracle Key Vault server as the support user.
- 2. Switch to the root user.

```
su - root
```

- 3. Mount /boot if it was not mounted on the system.
  - a. Check if the /boot is mounted. The following command should display /boot information if it was mounted.

```
df -h /boot;
```

**b.** Mount it if /boot is not mounted.

```
/bin/mount /boot;
```

- Check the installed kernels and the running kernel.
  - a. Search for any kernels that are installed.

```
rpm -q kernel-uek | sort
```

The following example output shows that two kernels are installed:

```
kernel-uek-4.14.35-2047.504.2.el7uek.x86_64
kernel-uek-5.4.17-2136.329.3.1.el8uek.x86_64
```

b. Check the latest kernel.

```
uname -r
```

The following output shows an example of a kernel version that was installed at the time:

```
5.4.17-2136.304.4.5.el7uek.x86 64
```

This example assumes  $5.4.17-2136.304.4.5.e17uek.x86_64$  as the latest version (newer versions may be available by now). Based on the output from the commands above, remove the older kernel (kernel-uek- $4.14.35-2047.504.2.e17uek.x86_64$ ). You should remove all kernels that are older than the latest kernel.

Remove the older kernel and its associated RPMs.

```
For example, to remove the kernel-uek-4.14.35-2047.504.2.el7uek.x86_64 kernel:

yum --disablerepo=* remove `rpm -qa|grep 4.14.35-2047.504.2.el7uek`
```

#### Output similar to the following appears:

```
Resolving Dependencies
--> Running transaction check
---> Package kernel-uek.x86 64 0:4.14.35-2047.504.2.el7uek will be erased
---> Package kernel-uek-devel.x86 64 0:4.14.35-2047.504.2.el7uek will be erased
--> Finished Dependency Resolution
Dependencies Resolved
Package
                 Arch
                          Version
Repository
                           Size
______
_____
Removing:
kernel-uek x86_64
@anaconda/7.7
                          4.14.35-2047.504.2.el7uek
                            58 M
kernel-uek-devel x86_64 4.14.35-2047.504.2.el7uek
                                                    @avs-ol-
dependencies
                   63 M
Transaction Summary
Remove 2 Package(s)
Installed size: 121 M
Is this ok [y/N]:
```

- **6.** Enter y to accept the deletion output.
- 7. Repeat these steps starting with Step 4 for all kernels that are older than the latest kernel.

# Step 7: If Necessary, Remove SSH-Related DSA Keys

For each multi-master cluster node, you should remove SSH-related DSA keys left behind after the upgrade.

- Log in to the Oracle Key Vault management console as a user with the System Administrator role.
- 2. Enable SSH.

Log in to the Oracle Key Vault management console as a user who has the System Administrator role. Select the **System** tab, then **Settings**. In the Network Details area, click **SSH Access**. Select **IP address(es)** and then enter only the IP addresses that you need, or select **All**. Click **Save**.

3. Login to the Oracle Key Vault support account using SSH.

 $\verb| ssh support@OracleKeyVault\_serverIPaddress| \\$ 

4. Switch to the root user.

```
su - root
```

5. Change directory to /etc/ssh.

```
cd /etc/ssh
```

6. Rename the following keys.

```
mv ssh_host_dsa_key.pub ssh_host_dsa_key.pub.retire
mv ssh host dsa key ssh host dsa key.retire
```

7. Disable SSH access.

Log in to the Oracle Key Vault management console as a user who has the System Administrator role. Select the **System** tab, then **Settings**. In the Network Details area, click **SSH Access**. Select **Disabled**. Click **Save**.

# Step 8: Upgrade the Endpoint Software

After you have upgraded all the nodes in the cluster, you must reenroll endpoints that were created in earlier releases of Oracle Key Vault, or update the endpoint software.

If you are upgrading from an earlier release to the latest release of Oracle Key Vault, then you must reenroll the endpoint instead of upgrading the endpoint software. Reenrolling the endpoint automatically updates the endpoint software.

Before an endpoint can take advantage of new features introduced in an Oracle Key Vault upgrade (for example non-extractable TDE master keys in Oracle Key Vault 21.4, or non-extractable private keys in Oracle Key Vault 21.6), it must be upgraded to Oracle Key Vault current release.

- Ensure that you have upgraded the Oracle Key Vault servers. If you are upgrading the endpoint software for an Oracle database configured for online TDE master encryption key management, then shut down the database.
- Download the endpoint software (okvclient.jar) for your platform from the Oracle Key Vault server as follows:
  - a. Go to the Oracle Key Vault management console login screen.
  - b. Click the Endpoint Enrollment and Software Download link.
  - c. In the **Download Endpoint Software Only** section, select the appropriate platform from the drop-down list.
  - d. Click the **Download** button.
- 3. Identify the path to your existing endpoint installation that you are about to upgrade (for example, /etc/ORACLE/KEYSTORES/okv (where /etc/ORACLE/KEYSTORES is WALLET\_ROOT of your database, or the softlink in \$ORACLE BASE/okv/\$ORACLE SID points to).
- 4. Install the endpoint software by executing the following command:

```
java -jar okvclient.jar -d existing_endpoint_directory_path
```

#### For example:

```
java -jar okvclient.jar -d /etc/ORACLE/KEYSTORES/okv
```



If you are installing the <code>okvclient.jar</code> file on a Windows endpoint system that has Oracle Database release 11.2.0.4 **only**, then include the <code>-db112</code> option. (This option is not necessary for any other combination of endpoint platform or Oracle Database version.) For example:

```
java -jar okvclient.jar -d /home/oracle/okvutil -v -db112
```

5. Install the updated PKCS#11 library file.

This step is needed only for online TDE master encryption key management by Oracle Key Vault. If an endpoint uses online TDE master encryption key management by Oracle Key Vault, then you must upgrade the PKCS#11 library while upgrading the endpoint software.

• On UNIX/Linux platforms: Run root.sh from the bin directory of endpoint installation directory to copy the latest liborapks.so file for Oracle Database endpoints.

```
$ sudo /etc/ORACLE/KEYSTORES/okv/bin/root.sh
```

#### Or

```
$ su - root
# /etc/ORACLE/KEYSTORES/okv/bin/root.sh
```

On Windows platforms: Run root.bat from the bin directory of endpoint installation directory to copy the latest liborapkcs.dll file for Oracle Database endpoints. You will be prompted for the version of the database in use.

```
bin\root.bat
```

6. Update the SDK software.

If you have already deployed the SDK software, Oracle recommends that you redeploy the SDK software in the same location after you complete the upgrade to Oracle Key Vault current release. This enables you to have access to the new capabilities of the SDK software that was introduced since the Oracle Key Vault version that you are upgrading from.

- a. Go to the Oracle Key Vault management console login screen.
- b. Click the Endpoint Enrollment and Software Download link.
- c. In the Download Software Development Kit section, select the appropriate language and platform for your site.
- d. Click the **Download** button to get the SDK zip file.
- e. Identify the existing location where SDK software was already deployed.
- f. Navigate to the directory in which you saved the SDK zip file.
- g. Unzip the SDK zip file.

For example, on Linux, to unzip the Java SDK zip file, use the following command:

```
unzip -o okv_jsdk.zip -d existing_endpoint_sdk_directory_path
```

For the C SDK zip file, use this command:

```
unzip -o okv_csdk.zip -d existing_endpoint_sdk_directory_path
```

7. If you had deployed the RESTful services utility in the previous release, then re-deploy the latest <code>okvrestclipackage.zip</code> file.



The latest <code>okvrestclipackage.zip</code> file enables you to have access to the new RESTful service that was introduced since the Oracle Key Vault version that you are upgrading from.

You can use wget or curl to download okvrestclipackage.zip.

```
wget --no-check-certificate https://Oracle_Key_Vault_IP_address:5695/
okvrestclipackage.zip
curl -0 -k https://Oracle_Key_Vault_IP_address:5695/okvrestclipackage.zip
```

8. Start the Oracle databases if the upgrade of Oracle Key Vault endpoints for all of the TDE-enabled databases on this host machine is complete.

At this stage, the endpoint will be fully upgraded.

- 9. If your site requires that you restrict TDE master encryption keys from leaving Oracle Key Vault and if you are using an Oracle Real Application Clusters (Oracle RAC) environment, then perform the following steps on each Oracle RAC node:
  - a. Perform the endpoint upgrade on each Oracle RAC node.
  - **b.** Set the extractable attribute value for symmetric keys.

By default, the extractable attribute value is true, which means that the key material of symmetric keys can be extracted from Oracle Key Vault during certain operations. If you want to prevent symmetric keys from being extracted, then you must set this value to false. You can set an extractable attribute value as follows:

- Set the default value for the extractable attribute of new symmetric keys in the endpoint settings. Endpoint-specific setting overrides the global endpoint settings.
- Explicitly specify the value of the extractable attribute when creating or registering a new symmetric key.
- Modify the extractable attribute of an existing symmetric key.

See Oracle Key Vault Administrator's Guide.

c. As a user who has the SYSDBA or SYSKM administrative privilege, perform a rekey operation in the Oracle RAC node. Use the following syntax:

```
ADMINISTER KEY MANAGEMENT SET [ENCRYPTION] KEY [FORCE KEYSTORE] [USING TAG 'tag_name'] IDENTIFIED BY [EXTERNAL STORE | keystore_password] ;
```

See *Oracle Database Advanced Security Guide* for more information about rekeying a TDE master encryption key.

- 10. If your site requires that you restrict TDE master encryption keys from leaving Oracle Key Vault and if you are using an Oracle Data Guard environment, then do the following on the primary and standby databases:
  - a. Perform the endpoint upgrade on the primary and standby databases.
  - **b.** Set the extractable attribute value for symmetric keys.

By default, the extractable attribute value is true, which means that the key material of symmetric keys can be extracted from Oracle Key Vault during certain operations. If you want to prevent symmetric keys from being extracted, then you must set this value to false. You can set an extractable attribute value as follows:

- Set the default value for the extractable attribute of new symmetric keys in the endpoint settings. Endpoint-specific setting overrides the global endpoint settings.
- Explicitly specify the value of the extractable attribute when creating or registering a new symmetric key.
- Modify the extractable attribute of an existing symmetric key.

See Oracle Key Vault Administrator's Guide.

c. As a user who has the SYSDBA or SYSKM administrative privilege, perform a rekey operation in the primary and standby databases.

```
ADMINISTER KEY MANAGEMENT SET [ENCRYPTION] KEY
[FORCE KEYSTORE]
[USING TAG 'tag_name']
IDENTIFIED BY [EXTERNAL STORE | keystore_password]
[WITH BACKUP [USING 'backup identifier']];
```

See *Oracle Database Advanced Security Guide* for more information about rekeying a TDE master encryption key.

#### Note:

Note the following before executing script:

- You must run root.sh or root.bat script to install the latest Oracle Key Vault PKCS#11 library only once on a host machine that has multiple TDEenabled Oracle databases that use Oracle Key Vault for master encryption key management.
- Ensure that you execute the root.sh or root.bat script only after the upgrade of Oracle Key Vault endpoints for all of the TDE-enabled databases on the same host machine is complete.
- Ensure that all of the TDE-enabled Oracle databases on this host have been shutdown.

#### **Related Topics**

Oracle Key Vault Administrator's Guide



# Upgrading a Primary-Standby Oracle Key Vault Server

This upgrade includes the Oracle Key Vault server software and utilities that control the associated endpoint software

- About Upgrading a Primary-Standby Oracle Key Vault Server
   When you upgrade the Oracle Key Vault server software appliance, also upgrade the endpoint software to get access to the latest enhancements.
- Step 1: Back Up the Server Before You Upgrade
  Before you upgrade the Oracle Key Vault server, perform a one-time backup to a remote destination so that you can recover data in case the upgrade fails.
- Step 2: Perform Pre-Upgrade Tasks for the Primary-Standby Oracle Key Vault To ensure a smooth upgrade to Oracle Key Vault, you should prepare the server you are upgrading.
- Step 3: Add Disk Space to Extend the vg\_root for the Release 21.10 Upgrade
  Before upgrading to Oracle Key Vault release 21.10, you will need to extend the vg\_root to
  increase disk space.
- Step 4: Upgrade the Oracle Key Vault Primary-Standby Pair
   You can upgrade a pair of Oracle Key Vault servers in a primary-standby deployment.
- Step 5: If Necessary, Add Disk Space to Extend Swap Space
   If necessary, extend the swap space on both the primary and standby servers.
- Step 6: If Necessary, Remove Old Kernels
   Oracle recommends that for both the primary and standby servers, you clean up the older
   kernels that were left behind after the upgrade.
- Step 7: If Necessary, Remove SSH-Related DSA Keys
   For both the primary and standby servers, you should remove SSH-related DSA keys left
   behind after the upgrade, because they can cause problems with some code analysis
   tools.
- Step 8: Upgrade the Endpoint Software
  For both the primary and standby servers, as part of the upgrade, you must reenroll
  endpoints created in earlier releases of Oracle Key Vault, or update the endpoint software.
- Step 9: Back Up the Upgraded Oracle Key Vault Server
  You must perform server backup and user password tasks after completing a successful
  upgrade.

# About Upgrading a Primary-Standby Oracle Key Vault Server

When you upgrade the Oracle Key Vault server software appliance, also upgrade the endpoint software to get access to the latest enhancements.

However, the endpoint software downloaded from the previous Oracle Key Vault release will continue to function with the upgraded Oracle Key Vault server. Be aware that while the old

endpoint software will continue to work with the upgraded Oracle Key Vault server, the new endpoint functionality may not work.

You must upgrade in the order shown: first perform a full backup of Oracle Key Vault, upgrade the Oracle Key Vault primary-standby server pair, upgrade the endpoint software, and last, perform another full backup of the upgraded server. Note that upgrading requires a restart of the Oracle Key Vault server.

The Oracle Key Vault server is not available to endpoints for a limited duration during the upgrade. You can enable the persistent cache feature to enable endpoints to continue operation during the upgrade process.

Before you begin the upgrade, refer to *Oracle Key Vault Release Notes* for additional information about performing upgrades.

#### **Related Topics**

- Oracle Key Vault Release Notes
- Oracle Key Vault Administrator's Guide

## Step 1: Back Up the Server Before You Upgrade

Before you upgrade the Oracle Key Vault server, perform a one-time backup to a remote destination so that you can recover data in case the upgrade fails.



#### **Caution:**

Do not bypass this step. Back up the server before you perform the upgrade so that your data is safe and recoverable.

# Step 2: Perform Pre-Upgrade Tasks for the Primary-Standby Oracle Key Vault

To ensure a smooth upgrade to Oracle Key Vault, you should prepare the server you are upgrading.

- 1. In the server where Oracle Key Vault is installed, log in as user support, and then switch to the root user.
- Ensure that the server meets the minimum disk space requirements for an upgrade. For example, 6 GB of free space in the /usr/local/dbfw/tmp directory. See the Oracle Key Vault Readme for this release to determine the disk space requirements for the upgrade.
- 3. Ensure that you disable diagnostics and clean up disk space in /usr/local/dbfw/tmp before you upgrade by performing the following steps:
  - If the Oracle Key Vault system being upgraded is from release 21.6 or later, log in to the Oracle Key Vault management console as a user with the System Administrator role, and navigate to the **System** tab, and then click the **Diagnostics** button.

If the Diagnostics Package Files pane is displayed, then click **Clear** to disable diagnostics. Note that the **Diagnostics Package Files** pane will be displayed only if the diagnostics bundle was previously generated, and the files were not cleared.



If the Diagnostics Package Files pane is not displayed, or if the diagnostics bundle was previously generated using the **dbfw-diagnostics-package.rb** utility, then log in to the Oracle Key Vault system and run the following commands to disable diagnostics and clean up disk space in /usr/local/dbfw/tmp:

a. SSH into the Oracle Key Vault system as user support, then switch to user root:

```
ssh support@<OKV_IP_Address>
su - root
```

b. Delete the generated diagnostics zip file and remove the package using the following commands:

```
/usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --clean /usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --remove
```

- 4. Check the boot partition size. If any of the nodes in question have a boot partition that is less than 500 MB, then you cannot upgrade that system to the new release. You can check this size as follows:
  - a. Mount the /boot partition.

```
# mount /boot
```

b. Check the Size column given by the following command:

```
# df -h /boot
```

c. Unmount the /boot partition:

```
# umount /boot
```

If the boot partition given by this command shows less than 488 MB, then you cannot upgrade to the current release. Oracle recommends that you restore a backup of the current configuration to a freshly installed system of the same release as the current system, and upgrade that to the new release instead.

- 5. If Oracle Key Vault is using the BIOS boot mode, then ensure that the disk size is not greater than 2 TB. If this is the case, then you cannot upgrade to the current release. Oracle recommends that you restore a backup of the current configuration onto a system with a disk that is less than 2 TB in size, and upgrade that to the new release instead.
- 6. If you need to increase available disk space, then remove the temporary jar files located in /usr/local/okv/ssl. *Be careful in doing so.* If you accidentally delete any files other than the jar files in /usr/local/okv/ssl, then the Oracle Key Vault server becomes nonfunctional.
- 7. Increase your disk space by extending the vg root size.

You must increase the disk space by extending vg root before you perform the upgrade.

- 8. Ensure that no full or incremental backup jobs are running. Delete all scheduled full or incremental backup jobs before the upgrade.
- **9.** Plan for downtime according to the following specifications:



Oracle Key Vault Usage	Downtime required
Wallet upload or download	NO
Java Keystore upload or download	NO
Transparent Data Encryption (TDE) direct connect	YES (NO with persistent cache)
Primary Server Upgrade in a primary-standby deployment	YES (NO with persistent cache)

#### Plan for downtimes.

- If Oracle Key Vault uses an online master encryption key, then plan for a downtime of 15 minutes during the Oracle Database endpoint software upgrades. Database endpoints can be upgraded in parallel to reduce total downtime.
- Plan for a downtime of a few hours. The persistent cache allows you to upgrade
   Oracle Key Vault servers without database downtime. The default duration of the
   persistent cache from the moment the Oracle Key Vault server becomes unavailable is
   1,440 minutes (one day).
- 11. If the Oracle Key Vault system has a syslog destination configured, ensure that the remote syslog destination is reachable from the Oracle Key Vault system, and that logs are being correctly forwarded. If the remote syslog destination is not reachable from the Oracle Key Vault system, then the upgrade process can become much slower than normal.
- 12. If Oracle Audit Vault was integrated with Oracle Key Vault in Oracle Key Vault release 21.2 or earlier, then do the following on the primary server (but not the standby) to disable and remove the Oracle Audit Vault integration:
  - a. Disable the Oracle Audit Vault integration: Log into the Oracle Key Vault management console as a System Administrator, select the **System** tab and then **Settings** from the left navigation bar. In the Monitoring and Alerts pane, select Audit Vault. In the Audit Vault integration pane that appears, disable Oracle Audit Vault. Click **Save**.
  - **b.** Perform the remaining steps in this procedure on each server where the Oracle Audit Vault integration was configured.
  - c. Log in to the Oracle Key Vault server through SSH as user support, switch user su to root and then switch user su to oracle.
  - **d.** Stop the agent by executing the following command:

```
agent_installation_directory/bin/agentctl stop
```

- e. Log in to the Oracle Audit Vault Server console as an Oracle Audit Vault administrator.
- f. Delete the corresponding agent and target.
- g. Log in to the Oracle Key Vault server through SSH as user support, then switch user su to root.
- h. Delete the installation directory for the Oracle Audit Vault agent.
- **13.** Ensure that the Oracle Key Vault server certificate has not expired, nor is close to expiry, before you begin the upgrade.
  - You can find how much time the Oracle Key Vault server certificate has before it expires by checking the **OKV Server Certificate Expiration** setting on the Configure Alerts page in the Oracle Key Vault management console.
- **14.** If you are performing an upgrade while using an HSM as a Root of Trust, then consult *Oracle Key Vault Root of Trust HSM Configuration Guide* for any additional steps that may be needed.





If you are upgrading from release 21.9.0.0.0 to release 21.10.0.0.0, Oracle recommends that you apply patch 37492574 before beginning the upgrade. This patch corrects the configuration of certain processes internal to Oracle Key Vault, and prevents upgrades to 21.10.0.0.0 from failing. Apply this patch to all systems in the Oracle Key Vault 21.9.0.0.0 deployment before beginning upgrade to 21.10.0.0.0.

- 15. Ensure that the backup of the orapwdbfwdb file matches the original file.
  - a. SSH into the Oracle Key Vault system as user support, then switch to user root:

```
ssh support@<OKV_IP_Address>
su - root
```

**b.** Verify that the backup file exists:

```
su - oracle
ls -ltr /var/lib/oracle/okv orapwd backup dir/orapwdbfwdb
```

- c. If the backup file exists, then perform the following steps:
  - Compare the original file with the backup file:

```
diff /var/lib/oracle/dbfw/dbs/orapwdbfwdb /var/lib/oracle/
okv_orapwd_backup_dir/orapwdbfwdb
```

• If there is a difference between the files, then update the backup file by copying the original file:

```
cp /var/lib/oracle/dbfw/dbs/orapwdbfwdb /var/lib/oracle/
okv orapwd backup dir/orapwdbfwdb
```

- **16.** If you are upgrading from Oracle Key Vault release 21.x to release 21.10.0.0.0, then Oracle recommends that you apply the following patches:
  - Patch 37688544, to be applied before you start the upgrade. This patch corrects any FIPS inconsistencies on the system and prevents upgrades from failing with the following error:

```
ODF-10001: Internal error: FAILED migration: okv save restore orapwd config["backup orapwd config"].
```

Apply this patch to all systems in the Oracle Key Vault deployment before you start the upgrade to 21.10.0.0.0.

 Patch 37763976, to be applied after starting the upgrade with the ruby /images/ upgrade.rb -confirm command but before resuming the upgrade with the /sbin/ reboot command.

#### **Related Topics**

Step 3: Add Disk Space to Extend the vg\_root for the Release 21.10 Upgrade
Before upgrading to Oracle Key Vault release 21.10, you will need to extend the vg\_root to
increase disk space.

Oracle Key Vault Administrator's Guide

# Step 3: Add Disk Space to Extend the vg\_root for the Release 21.10 Upgrade

Before upgrading to Oracle Key Vault release 21.10, you will need to extend the vg\_root to increase disk space.

If you are upgrading from an earlier Oracle Key Vault release 21.x release and have already extended the vg root, then you can bypass this step.

Before you start this procedure, ensure that all endpoints have persistent cache enabled and in use.

- 1. Log in to the server for which you will perform the upgrade and switch user as root.
- 2. Ensure that the persistent cache settings for Oracle Key Vault have been set.

You will need to ensure that the persistent cache has been enabled because in a later step in this procedure, you must shut down the server. Shutting down the Oracle Key Vault server will incur downtime. To avoid any downtime, Oracle recommends that you turn on persistent cache.

3. Run the vgs command to determine the free space

vgs

The VFree column shows how much free space you have (for example, 21 GB).

4. Power off the server in order to add a new disk

```
/sbin/shutdown -h now
```

- Add a new disk to the server with a capacity of 100 GB or greater
- 6. Start the server.
- 7. Log in to the Oracle Key Vault server through SSH as user support, then switch user su to root.

```
ssh support@okv_server_IP_address
su - root
```

8. Stop the Oracle Key Vault services.

```
service tomcat stop;
service httpd stop;
service kmipus stop;
service kmip stop;
service okvogg stop;
service javafwk stop;
service monitor stop;
service controller stop;
service dbfwlistener stop;
service dbfwdb stop;
service rsyslog stop;
```



9. Run the fdisk -1 command to find if there are any available partitions on the new disk.

```
fdisk -1
```

At this stage, there should be no available partitions.

10. Run the fdisk disk device to be added command to create the new partition.

For example, to create a disk device named /dev/sdb:

```
fdisk /dev/sdb
```

In the prompts that appear, enter the following commands in sequence:

- n for new partition
- p for primary
- 1 for partition number
- Accept the default values for cylinder (press Enter twice).
- w to write and exit
- 11. Use the pvcreate <code>disk\_device\_partition</code> command to add the newly added disk to the physical volume.

For example, for a disk device named /dev/sdb1, which is the name of the disk partition that you created (based on the name used for the disk device that was added).

```
pvcreate /dev/sdb1
```

Output similar to the following appears:

```
Physical volume "/dev/sdb1" successfully created
```

**12.** Use the vgextend vg\_root disk\_device\_partition command to extend the logical volume with this disk space that you just added.

For example, for the partition /dev/sdb1, you would run:

```
vgextend vg_root /dev/sdb1
```

Output similar to the following appears:

```
Volume group "vg_root" successfully extended
```

13. Run the vgs command again to ensure that VFree shows an increase of 100 GB.

vgs

Output similar to the following appears:



#### 14. Restart the Oracle Key Vault server.

/sbin/reboot

For primary-standby deployments, ensure that the primary and standby nodes sync up before proceeding further with next steps.

#### **Related Topics**

Oracle Key Vault Administrator's Guide

## Step 4: Upgrade the Oracle Key Vault Primary-Standby Pair

You can upgrade a pair of Oracle Key Vault servers in a primary-standby deployment.

- About Upgrading an Oracle Key Vault Server Primary-Standby Pair
  In a primary-standby deployment you must upgrade both primary and standby Oracle Key
  Vault servers.
- Upgrading a Pair of Primary-Standby Oracle Key Vault Servers
   You should allocate several hours to upgrade the primary server after upgrading the standby.

### About Upgrading an Oracle Key Vault Server Primary-Standby Pair

In a primary-standby deployment you must upgrade both primary and standby Oracle Key Vault servers.

Note that persistent caching enables endpoints to continue to be operational during the upgrade process.



If you are upgrading from a system with 4 GB RAM, first add an additional 12 GB memory to the system before upgrading.

#### **Related Topics**

Oracle Key Vault Administrator's GuideAbout the Persistent Encryption Master Key Cache

### Upgrading a Pair of Primary-Standby Oracle Key Vault Servers

You should allocate several hours to upgrade the primary server after upgrading the standby.

You must perform the upgrade of standby and primary servers in one session with as little time between the standby and primary upgrade. The upgrade time is approximate and a function of the volume of data stored and managed by Oracle Key Vault. For large volumes of data, the upgrade time may be longer than several hours.

- **1.** For both primary and standby servers in the primary-standby configuration, prepare for upgrade.
  - Ensure that both the primary and standby systems have at least 16 GB memory.
  - Add disk space to extend the vg root.



- While the upgrade is in progress, do not change any settings or perform any other operations that are not part of the upgrade instructions below.
- Upgrade the Oracle Key Vault server during a planned maintenance window because
  the upgrade process requires the endpoints to be shut down during the upgrade, if no
  persistent cache has been configured. With persistent cache enabled, endpoints will
  continue to be operational during the upgrade process.
- Ensure that you have backed up the server you are upgrading so your data is safe and recoverable.

Ensure that in the time between the backup and shutting down the Oracle Key Vault servers for upgrade, that no databases perform a set or rekey operation (for example, using the ADMINISTER KEY MANAGEMENT statement), since these new keys will not be included in the backup.

Do not proceed without completing this step.

- First, upgrade the standby server while the primary server is running.
  - Log into the Oracle Key Vault management console as a user who has the System Administrator role.
  - b. Ensure that SSH access is enabled.
  - Ensure you have enough space in the destination directory for the upgrade ISO files.
  - d. Log in to the Oracle Key Vault server through SSH as user support, then switch user su to root.

```
ssh support@okv_server_IP_address
su - root
```

If the SSH connection times out while you are executing any step of the upgrade, then the operation will not complete successfully. Oracle recommends that you ensure that you use the appropriate values for the ServerAliveInterval and ServerAliveCountMax options for your SSH sessions to avoid upgrade failures.

Using the tmux command prevents network disconnections interrupting the upgrade. If the session terminates, resume as follows:

```
root# tmux a
```

 Copy the upgrade ISO file to the destination directory using Secure Copy Protocol or other secure transmission method.

Note that the upgrade ISO file is **not** the installation ISO file that you downloaded from eDelivery. You can download the Oracle Key Vault upgrade software from the My Oracle Support website at <a href="https://support.oracle.com/portal/">https://support.oracle.com/portal/</a>.

```
root# scp remote_host:remote_path/okv-upgrade-disc-
new_software_release.iso /var/lib/oracle
```

#### In this specification:

- remote host is the IP address of the computer containing the ISO upgrade file.
- remote\_path is the directory of the ISO upgrade file. Do not copy this file to any location other than the /var/lib/oracle directory.
- f. Make the upgrade accessible by using the mount command:



root# /bin/mount -o loop,ro /var/lib/oracle/okv-upgrade-discnew software release.iso /images

g. Clear the cache using the clean all command:

root# yum -c /images/upgrade.repo clean all

h. Apply the upgrade with the upgrade.rb command:

root# ruby /images/upgrade.rb --confirm

If the system is successfully upgraded, then the command will display the following message:

Reboot now to continue the upgrade process.

If you see an error message, then check the log file <code>/var/log/messages</code> for additional information.

#### Note:

If the upgrade of the Oracle Key Vault system fails with the following message:

Failed to apply update: The Oracle Key Vault upgrade has detected issues with FIPS mode. Please consult the Oracle Key Vault upgrade documentation or contact Oracle Support

Apply patch 37688544 to correct the FIPS inconsistencies, and attempt the upgrade again.

- i. Apply patch 37763976, following the instructions in the patch readme.
- j. Restart the Oracle Key Vault server by running the reboot command:

# reboot

On the first restart of the computer after the upgrade, the system will apply the necessary changes. This can take a few hours. Do not shut down the system during this time.

The upgrade is completed when the screen with heading: Oracle Key Vault Server new\_software\_release appears. The revision should reflect the upgraded release.

- 4. Ensure that the upgraded standby Oracle Key Vault server is restarted and running.
- 5. Upgrade the primary Oracle Key Vault server following same steps that you followed for the standby server in Step 3.

After both the standby and primary Oracle Key Vault servers are upgraded, the two servers will automatically synchronize.

- Log in to the Oracle Key Vault management console as a user with the System Administrator role.
- 7. Select the **System** tab, and then **Status**.
- 8. Verify that the **Version** field displays the new software version.
- 9. If your site uses the Commercial National Security Algorithm (CNSA) suite, then re-install these algorithms onto the primary and standby servers.



#### **Related Topics**

Oracle Key Vault Administrator's Guide

## Step 5: If Necessary, Add Disk Space to Extend Swap Space

If necessary, extend the swap space on both the primary and standby servers.

Oracle Key Vault release 21.10 requires a hard disk size greater than or equal to 1 TB in size with approximately 64 GB of swap space. If your system does not meet this requirement, follow these instructions to extend the swap space. You can check how much swap space you have by running the <code>swapon -s</code> command. By default, Oracle Key Vault releases earlier than release 18.1 were installed with approximately 4 GB of swap space. After you complete the upgrade to release 18.1 or later, Oracle recommends that you increase the swap space allocation for the server on which you upgraded Oracle Key Vault. A new Oracle Key Vault installation is automatically configured with sufficient swap space. However, if you upgraded from a previous release, and your system does not have the desired amount of swap space configured, then you must manually add disk space to extend the swap space, particularly if the intention is to convert the upgraded server into the first node of a multi-master cluster.

- 1. Log in to the server in which you upgraded Oracle Key Vault and connect as root.
- 2. Check the current amount of swap space.

```
[root@my okv server support] # swapon -s
```

Output similar to the following appears. This example shows that the system has 4 GB of swap space.

```
Filename Type Size Used Priority /dev/dm-0 partition 4194300 3368 -1
```

There **must** be 64 GB of swap space if the disk is greater than 1 TB in size.

3. Run the vgs command to determine how much free space is available.

vgs

The VFree column shows how much free space you have (for example, 21 GB).

Power off the server in order to add a new disk.

```
/sbin/shutdown -h now
```

- 5. Add a new disk to the server of a size that will bring the VFree value to over 64 GB.
- 6. Start the server.
- 7. Log in to the Oracle Key Vault server through SSH as user support, then switch user su to root.

```
ssh support@okv_server_IP_address
su - root
```



8. Run the fdisk -1 command to find if there are any available partitions on the new disk.

fdisk -l

At this stage, there should be no available partitions.

9. Run the fdisk disk device to be added command to create the new partition.

For example, to create a disk device named /dev/sdc:

fdisk /dev/sdc

In the prompts that appear, enter the following commands in sequence:

- n for new partition
- p for primary (for primary partition)
- 1 for partition number
- Accept the default values for cylinder (press Enter twice).
- w to write and exit
- **10.** Use the pvcreate <code>disk\_device\_partition</code> command to add the newly added disk to the physical volume.

For example, for a disk device named /dev/sdc1, which is the name of the disk partition that you created (based on the name used for the disk device that was added).

```
pvcreate /dev/sdc1
```

Output similar to the following appears:

```
Physical volume "/dev/sdc1" successfully created
```

**11.** Use the vgextend vg\_root disk\_device\_partition command to extend the logical volume with this disk space that you just added.

For example, for the partition /dev/sdc1, you would run:

```
vgextend vg_root /dev/sdc1
```

Output similar to the following appears:

```
Volume group "vg_root" successfully extended
```

12. Run the vgs command again to ensure that VFree shows an increase of 64 GB.

vgs

13. Disable swapping.

[root@my okv server support]# swapoff -v /dev/vg root/lv swap



**14.** To extend the swap space, run the lyresize command.

```
[root@my okv server support]# lvresize -L +60G /dev/vg root/lv swap
```

#### Output similar to the following appears:

```
Size of logical volume vg_root/lv_swap changed from 4.00 GiB (128 extents) to 64.00 GiB (2048 extents) Logical volume lv swap successfully resized.
```

15. Format the newly added swap space.

```
[root@my okv server support] # mkswap /dev/vg root/lv swap
```

#### Output similar to the following appears:

```
mkswap: /\text{dev/vg}\_\text{root/lv}\_\text{swap}: warning: don't erase bootbits sectors on whole disk. Use -f to force. Setting up swapspace version 1, size = 67108860 KiB no label, UUID=fea7fc72-0fea-43a3-8e5d-e29955d46891
```

**16.** Enable swapping again.

```
[root@my okv server support]# swapon -v /dev/vg root/lv swap
```

17. Verify the amount of swap space that is available.

```
[root@my okv server support]# swapon -s
```

#### Output similar to the following appears:

```
Filename Type Size Used Priority /dev/dm-0 partition 67108860 0 -1
```

18. Restart the Oracle Key Vault server.

```
/sbin/reboot
```

For primary-standby deployments, ensure that the primary and standby nodes sync up before proceeding further with next steps.

## Step 6: If Necessary, Remove Old Kernels

Oracle recommends that for both the primary and standby servers, you clean up the older kernels that were left behind after the upgrade.

While the older kernel is not in use, it may be marked as an issue by some code analysis tools.

- 1. Log in to the Oracle Key Vault server as the support user.
- 2. Switch to the root user.

```
su - root
```



- 3. Mount /boot if it was not mounted on the system.
  - a. Check if the /boot is mounted. The following command should display /boot information if it was mounted.

```
df -h /boot;
```

**b.** Mount it if /boot is not mounted.

```
/bin/mount /boot;
```

For EFI-based systems, you may need to mount /boot/efi if it is not already mounted.

```
/bin/mount /boot/efi
```

- 4. Check the installed kernels and the running kernel.
  - a. Search for any kernels that are installed.

```
rpm -q kernel-uek | sort;
```

The following example output shows that two kernels are installed:

```
kernel-uek-4.1.12-103.9.4.el6uek.x86_64
kernel-uek-4.1.12-112.16.7.el6uek.x86_64
```

b. Check the latest kernel.

```
uname -r;
```

The following output shows an example of a kernel version that was installed at the time:

```
4.1.12-112.16.7.el6uek.x86 64
```

This example assumes that 4.1.12-112.16.7.el6uek.x86\_64 is the latest version, but newer versions may be available by now. Based on this output, you will need to remove the kernel-uek-4.1.12-103.9.4.el6uek.x86\_64 kernel. You should remove all kernels that are older than the latest kernel.

5. Remove the older kernel and its associated RPMs.

For example, to remove the kernel-uek-4.1.12-103.9.4.el6uek.x86 64 kernel:

```
yum --disablerepo=* remove `rpm -qa | grep 4.1.12-103.9.4.el6uek`;
```

#### Output similar to the following appears:



- **6.** Enter y to accept the deletion output.
- 7. Repeat these steps starting with Step 4 for all kernels that are older than the latest kernel.

## Step 7: If Necessary, Remove SSH-Related DSA Keys

For both the primary and standby servers, you should remove SSH-related DSA keys left behind after the upgrade, because they can cause problems with some code analysis tools.

- 1. Log in to the Oracle Key Vault management console as a user with the System Administrator role.
- 2. Enable SSH.

Log in to the Oracle Key Vault management console as a user who has the System Administrator role. Select the **System** tab, then **Settings**. In the Network Details area, click **SSH Access**. Select **IP address(es)** and then enter only the IP addresses that you need, or select **All**. Click **Save**.

Login to the Oracle Key Vault support account using SSH.

```
ssh support@OracleKeyVault serverIPaddress
```

Switch to the root user.

```
su - root
```

5. Change directory to /etc/ssh.

```
cd /etc/ssh
```

Rename the following keys.

```
mv ssh_host_dsa_key.pub ssh_host_dsa_key.pub.retire
mv ssh_host_dsa_key ssh_host_dsa_key.retire
```

Disable SSH access.

Log in to the Oracle Key Vault management console as a user who has the System Administrator role. Select the **System** tab, then **Settings**. In the Network Details area, click **SSH Access**. Select **Disabled**. Click **Save**.

## Step 8: Upgrade the Endpoint Software

For both the primary and standby servers, as part of the upgrade, you must reenroll endpoints created in earlier releases of Oracle Key Vault, or update the endpoint software.

If you are upgrading from an earlier release to the latest release of Oracle Key Vault, then you must reenroll the endpoint instead of upgrading the endpoint software. Reenrolling the endpoint automatically updates the endpoint software.

Before an endpoint that uses online TDE master encryption key management by Oracle Key Vault can take advantage of the ability to control the extraction of objects from Oracle Key Vault during cryptographic operations, it must be upgraded to Oracle Key Vault release 21.10.

- Ensure that you have completely upgraded both the primary and standby servers that are configured Oracle Key Vault. If you are upgrading the endpoint software for an Oracle database configured for online TDE master encryption key management, then shut down the database.
- 2. Download the endpoint software (okvclient.jar) for your platform from the Oracle Key Vault server as follows:
  - a. Go to the Oracle Key Vault management console login screen.
  - b. Click the Endpoint Enrollment and Software Download link.
  - c. In the **Download Endpoint Software Only** section, select the appropriate platform from the drop-down list.
  - d. Click the **Download** button.
- 3. Identify the path to your existing endpoint installation that you are about to upgrade (for example, /etc/ORACLE/KEYSTORES/okv (where /etc/ORACLE/KEYSTORES is WALLET\_ROOT of your database, or the softlink in \$ORACLE\_BASE/okv/\$ORACLE\_SID points to).
- 4. Install the endpoint software by executing the following command:

```
java -jar okvclient.jar -d existing endpoint directory path
```

#### For example:

```
java -jar okvclient.jar -d /etc/ORACLE/KEYSTORES/okv
java -jar okvclient.jar -d c:\etc\ORACLE\KEYSTORES\okv
```

Install the updated PKCS#11 library file.

This step is needed only for online TDE master encryption key management by Oracle Key Vault. If an endpoint uses online TDE master encryption key management by Oracle Key Vault, then you must upgrade the PKCS#11 library while upgrading the endpoint software.

On UNIX/Linux platforms: Run root.sh from the bin directory of endpoint installation directory to copy the latest liborapkes.so file for Oracle Database endpoints.

```
$ sudo /etc/ORACLE/KEYSTORES/okv/bin/root.sh
```

#### Or

```
$ su - root
# /etc/ORACLE/KEYSTORES/okv/bin/root.sh
```



• On Windows platforms: Run root.bat from the bin directory of endpoint installation directory to copy the latest liborapkes.dll file for Oracle Database endpoints. You will be prompted for the version of the database in use.

```
bin\root.bat
```

Update the SDK software.

If you have already deployed the SDK software, Oracle recommends that you redeploy the SDK software in the same location after you complete the upgrade to Oracle Key Vault release 21.10. This enables you to have access to the new SDK APIs that were introduced since the Oracle Key Vault version that you are upgrading from.

- a. Go to the Oracle Key Vault management console login screen.
- b. Click the Endpoint Enrollment and Software Download link.
- c. In the Download Software Development Kit section, select the appropriate language and platform for your site.
- d. Click the **Download** button to get the SDK zip file.
- e. Identify the existing location where SDK software was already deployed.
- f. Navigate to the directory in which you saved the SDK zip file.
- g. Unzip the SDK zip file.

For example, on Linux, to unzip the Java SDK zip file, use the following command:

```
unzip -o okv_jsdk.zip -d existing_endpoint_sdk_directory_path
```

For the C SDK zip file, use this command:

```
unzip -o okv csdk.zip -d existing endpoint sdk directory path
```

- h. Do not exit this page.
- 7. If you had deployed the RESTful services utility in the previous release, then re-deploy the latest okvrestclipackage.zip file.

The latest <code>okvrestclipackage.zip</code> file enables you to have access to the new RESTful services utility commands that were introduced since the Oracle Key Vault version that you are upgrading from.

You can use wget or curl to download okvrestclipackage.zip.

```
wget --no-check-certificate https://Oracle_Key_Vault_IP_address:5695/
okvrestclipackage.zip
```

```
curl -0 -k https://Oracle_Key_Vault_IP_address:5695/okvrestservices.jar
```

- 8. Start the Oracle databases if the upgrade of Oracle Key Vault endpoints for all of the TDE-enabled databases on this host machine is complete.
  - At this stage, the endpoint will be fully upgraded.
- 9. If your site requires that you restrict TDE master encryption keys from leaving Oracle Key Vault and if you are using an Oracle Real Application Clusters (Oracle RAC) environment, then perform the following steps on each Oracle RAC node:
  - a. Perform the endpoint upgrade on each Oracle RAC node.



**b.** Set the extractable attribute value for symmetric keys.

By default, the extractable attribute value is true, which means that the key material of symmetric keys can be extracted from Oracle Key Vault during certain operations. If you want to prevent symmetric keys from being extracted, then you must set this value to false. You can set an extractable attribute value as follows:

- Set the default value for the extractable attribute of new symmetric keys in the endpoint settings. Endpoint-specific setting overrides the global endpoint settings.
- Explicitly specify the value of the extractable attribute when creating or registering a new symmetric key.
- Modify the extractable attribute of an existing symmetric key.

See Oracle Key Vault Administrator's Guide.

c. As a user who has the SYSDBA or SYSKM administrative privilege, perform a rekey operation in the Oracle RAC node. Use the following syntax:

```
ADMINISTER KEY MANAGEMENT SET [ENCRYPTION] KEY
[FORCE KEYSTORE]
[USING TAG 'tag_name']
IDENTIFIED BY [EXTERNAL STORE | keystore_password]
[WITH BACKUP [USING 'backup identifier']];
```

See *Oracle Database Advanced Security Guide* for more information about rekeying a TDE master encryption key.

- 10. If your site requires that you restrict TDE master encryption keys from leaving Oracle Key Vault and if you are using an Oracle Data Guard environment, then do the following on the primary and standby databases:
  - a. Perform the endpoint upgrade on the primary and standby databases.
  - **b.** Set the extractable attribute value for symmetric keys.

By default, the extractable attribute value is true, which means that the key material of symmetric keys can be extracted from Oracle Key Vault during certain operations. If you want to prevent symmetric keys from being extracted, then you must set this value to false. You can set an extractable attribute value as follows:

- Set the default value for the extractable attribute of new symmetric keys in the endpoint settings. Endpoint-specific setting overrides the global endpoint settings.
- Explicitly specify the value of the extractable attribute when creating or registering a new symmetric key.
- Modify the extractable attribute of an existing symmetric key.

See Oracle Key Vault Administrator's Guide.

c. As a user who has the SYSDBA or SYSKM administrative privilege, perform a rekey operation in the primary and standby databases.

```
ADMINISTER KEY MANAGEMENT SET [ENCRYPTION] KEY
[FORCE KEYSTORE]
[USING TAG 'tag_name']
IDENTIFIED BY [EXTERNAL STORE | keystore_password]
[WITH BACKUP [USING 'backup identifier']];
```



See *Oracle Database Advanced Security Guide* for more information about rekeying a TDE master encryption key.

#### Note:

Note the following before executing script:

- You must run root.sh or root.bat script to install the latest Oracle Key Vault PKCS#11 library only once on a host machine that has multiple TDEenabled Oracle databases that use Oracle Key Vault for master encryption key management.
- Ensure that you execute the root.sh or root.bat script only after the upgrade of Oracle Key Vault endpoints for all of the TDE-enabled databases on the same host machine is complete.
- Ensure that all of the TDE-enabled Oracle databases on this host have been shutdown.

#### **Related Topics**

Oracle Key Vault Administrator's Guide

## Step 9: Back Up the Upgraded Oracle Key Vault Server

You must perform server backup and user password tasks after completing a successful upgrade.

- 1. Take a full backup of the upgraded Oracle Key Vault Server Database to a new remote destination. Avoid using the old backup destination for the new backups.
- 2. Schedule a new periodic incremental backup to the new destination defined in the preceding step.
- 3. Change the Oracle Key Vault administrative passwords.

Password hashing has been upgraded to a more secure standard than in earlier releases. This change affects the operating system passwords, support and root. You must change Oracle Key Vault administrative passwords after the upgrade to take advantage of the more secure hash.



9

# Getting Started Using Oracle Key Vault After the Installation or Upgrade

After you complete the installation or upgrade, you can log in to the Oracle Key Vault management console and begin to use Oracle Key Vault functionality.

- Logging In to the Oracle Key Vault Management Console
   To use Oracle Key Vault, you can log in to the Oracle Key Vault management console.
- Overview of the Oracle Key Vault Management Console

  The Oracle Key Vault management console provides a graphical user interface for Oracle Key Vault users.
- Performing Actions and Searches
   The Oracle Key Vault management console enables you to perform standard actions and search operations, as well as get help information.

## Logging In to the Oracle Key Vault Management Console

To use Oracle Key Vault, you can log in to the Oracle Key Vault management console.

- Open a web browser.
- 2. Connect using an HTTPS connection and the IP address of Oracle Key Vault.

For example, to log in to a server whose IP address is 192.0.2.254, enter:

https://192.0.2.254

- 3. After the login screen appears, enter your user name and password.
- 4. Click Login.

### Overview of the Oracle Key Vault Management Console

The Oracle Key Vault management console provides a graphical user interface for Oracle Key Vault users.

The Oracle Key Vault management console is a browser-based console that connects to the server using the https secure communication channel. It provides the graphical user interface for Oracle Key Vault, where users can perform tasks such as the following:

- Setting up and managing the cluster
- Creating and managing users, endpoints, and their respective groups
- Creating and managing virtual wallets and security objects
- Setting system settings, like network and other services
- Setting up primary-standby
- Performing backups

## Performing Actions and Searches

The Oracle Key Vault management console enables you to perform standard actions and search operations, as well as get help information.

Many of the tab and menu pages contain an **Actions** menu or **Search** bars that allow you to search and perform actions on lists and the results of searches. The **Help** selection of the **Actions** list provides detailed help for using these features.

#### Actions Menus

The actions available from an **Actions** drop-down menu can vary but typically include a set of standard menu items.

Search Bars

Along with **Actions** menus, many tabs in the Oracle Key Vault management console contain search bars.

#### **Actions Menus**

The actions available from an **Actions** drop-down menu can vary but typically include a set of standard menu items.

These items are as follows:

- Select Columns: Select which column should be displayed.
- Filter: Filter by column or row and a user-defined expression.
- Rows Per Page: Choose how many rows you want to view.
- Format: Choose formatting such as Sort, Control Break, Highlight, Compute, Aggregate, Chart, and Group By.
- Save Report: Save reports.
- Reset: Reset the report settings, removing any customizations.
- Help: Get information about these actions.
- Download: Download the result set in CSV or HTML.

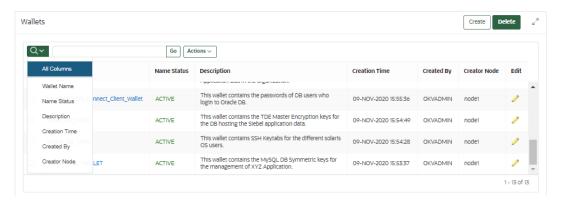
#### Search Bars

Along with **Actions** menus, many tabs in the Oracle Key Vault management console contain search bars.

This demonstration searches for wallets, but the process is the same for other searches, except that the column headings are different. Wildcard characters are not supported, but the search does match any letter or phrase that you enter. You can use the **Filter** menu item under **Actions** to further fine-tune the search.

 Enter a name or other identifier in the search field or (optionally) place your cursor on the magnifying icon in the Search bar to select one of the table headings (in this case, All Columns, Wallet Name, Name Status, Description, Creation Time, Created By, and Creator Node) and then enter a search term.





#### 2. Click Go.

A new wallet list appears, displaying the wallets that meet the search criteria. A filter icon (a funnel) indicates that a search has been performed and displays the search criteria.

3. You can select or deselect the filter icon to disable search and view the entire list.





## Hyper-V Installation on Windows

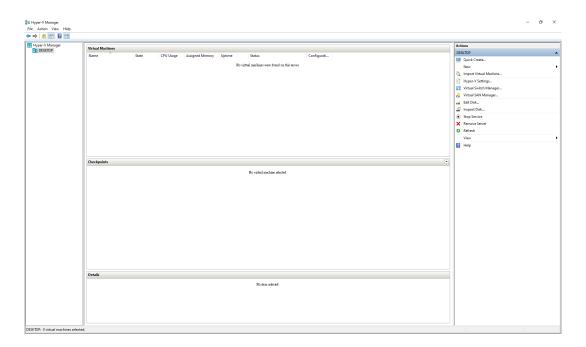
Hyper-V Installation
You can install Oracle Key Vault on Hyper-V using the provided information.

## Hyper-V Installation

You can install Oracle Key Vault on Hyper-V using the provided information.

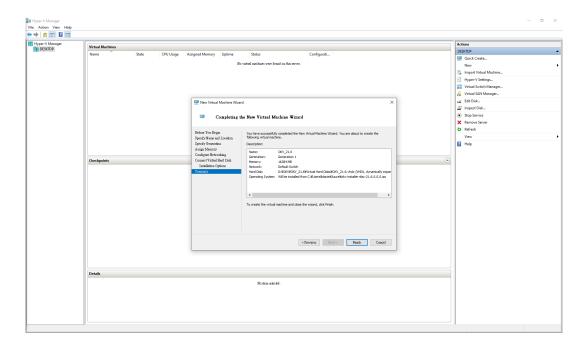
To install Oracle Key Vault on Hyper-V.

1. Open the Hyper-V Manager.



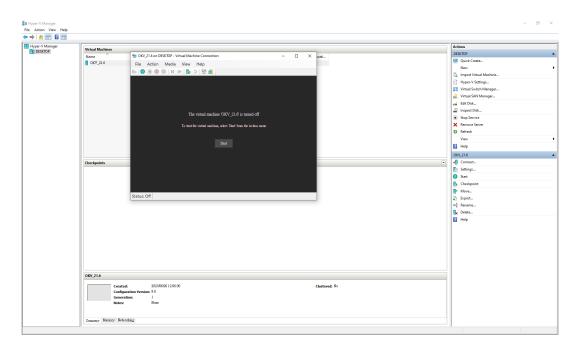
2. Select **DESKTOP**. The **New Virtual Machine Wizard** displays.

Follow the **New Virtual Machine Wizard** to complete the steps to create a new virtual machine.



#### 3. Click Finish.

The Oracle Key Vault Virtual Machine desktop window appears.



- **4.** Go to **Actions** window pane.
- 5. Select **Start** to start the virtual machine.
- 6. Select the required options from the displayed window. See, Installing Oracle Key Vault to complete the Oracle Key Vault installation and post-installation.





For an Oracle Key Vault server on a Hyper-V, dual nic (in the Oracle Key Vault network configuration) is not supported.

#### **Related Topics**

Installing Oracle Key Vault
You must download the Oracle Key Vault application software, and then you can perform the installation.



B

## Tablespace Encryption for Oracle Key Vault

Tablespace Encryption for Oracle Key Vault Upgraded from 12.2.0.3.0 or Before
You can refer to this topic for the tablespace encryption for Oracle Key Vault upgraded
from 12.2.0.3.0 or before.

# Tablespace Encryption for Oracle Key Vault Upgraded from 12.2.0.3.0 or Before

You can refer to this topic for the tablespace encryption for Oracle Key Vault upgraded from 12.2.0.3.0 or before.

The fresh installations of Oracle Key Vault 12.2.0.4.0 and higher encrypt the tablespaces using AES256 encryption.

If you have an installation of Oracle Key Vault that is upgraded from a fresh installation of Oracle Key Vault version prior to 12.2.0.4.0, the Oracle Key Vault tablespace continues to use AES128 encryption and the auditing tablespace remains unencrypted.

Use the following steps to encrypt the tablespaces of an Oracle Key Vault that is upgraded from a fresh installation of Oracle Key Vault version prior to 12.2.0.4.0 using AES256.

#### Note:

For the multi-master cluster deployment, you need to run below steps on every node. For the primary-standby deployment, you need to run the steps on the primary node only. The standby conversion takes place automatically.

- Perform a full backup of Oracle Key Vault to a remote destination. Ensure that the backup is successful.
- 2. Log in to the Oracle Key Vault server through SSH as user support, then switch user su to root.

```
ssh support@okv_server_IP_address
su - root
```

Switch user to oracle user.

```
su - oracle
```

4. Use sqlplus to connect to the Database as the SYSDBA user.

```
sqlplus / as SYSDBA
```



5. Run the query to verify that the tablespace KEYVAULT\_SPACE is encrypted using AES128 and the tablespace KEYVAULT AUDIT TBS is not encrypted.

```
SQL> select a.name, b.encryptionalg, b.status
    from v$tablespace a, v$encrypted_tablespaces b
where a.ts# = b.ts#;
```

NAME	ENCRYPT	STATUS
AVSPACE	AES256	NORMAL
KEYVAULT_SPACE	AES128	NORMAL

Ensure that the auxiliary space (tablespace SYSAUX) is at least the same size as the largest data file of this tablespace.

This size requirement is because Oracle Database performs the conversion one file at a time. For example, if the largest data file of the tablespace is 32 GB, then ensure that you have 32 GB of auxiliary space.

To find the space a data file uses, run the below query.

```
select a.name, a.bytes, a.blocks, a.block size, a.create bytes, b.name
from v$datafile a, v$tablespace b where a.TS# = b.TS#
SQL> /
NAME
   BYTES BLOCKS BLOCK SIZE CREATE BYTES NAME
-----
/var/lib/oracle/oradata/dbfwdb/system01.dbf
1614807040 197120 8192
                                    0 SYSTEM
/var/lib/oracle/oradata/dbfwdb/keyvault tbs
 33554432 4096 8192 33554432 KEYVAULT SPACE
/var/lib/oracle/oradata/dbfwdb/sysaux01.dbf
2715811840
           331520 8192
                                    0 SYSAUX
/var/lib/oracle/oradata/dbfwdb/undotbs01.dbf
2202009600 268800 8192 0 UNDOTBS1
/var/lib/oracle/oradata/DBFWDB/datafile/o1 mf avspace ln88t6vp .dbf
209715200 25600 8192 104857600 AVSPACE
/var/lib/oracle/oradata/dbfwdb/users01.dbf
  5242880 640 8192 0 USERS
/var/lib/oracle/oradata/dbfwdb/keyvault audit tbs
 33554432 4096 8192 33554432 KEYVAULT AUDIT TBS
```

Ensure that the size of tablespace SYSAUX is larger than size of tablespaces KEYVAULT\_SPACE and KEYVAULT\_AUDIT\_TBS.

.

7. Re-encrypt online tablespace KEYVAULT SPACE using AES256.

```
SQL> ALTER TABLESPACE KEYVAULT_SPACE ENCRYPTION ONLINE USING 'AES256' REKEY;
Tablespace altered.
```

8. Encrypt online tablespace KEYVAULT AUDIT TBS using AES256.

```
SQL> ALTER TABLESPACE KEYVAULT_AUDIT_TBS ENCRYPTION ONLINE USING 'AES256'
ENCRYPT;
Tablespace altered.
```

9. Verify that Oracle Key Vault tablespaces are now encrypted using AES256.

KEYVAULT\_AUDIT\_TBS AES256 NORMAL

NORMAL



# Index

A	L
Actions menu, 9-2	logging in to management console, 9-1
D	M
deployment options, 1-2 disk space adding for release 21.4 for primary-standby, 8-6 adding for release 21.5 for standalone deployment, 6-6 disk space, adding for release 21.4, 6-11, 7-9, 8-11 DSA keys, removing after upgrade, 6-15, 7-13, 8-15 dual NIC network mode	management console logging in to, 9-1 overview of, 9-1 multi-master clusters checking upgrade success, 7-9 preparation for pre-upgrade, 7-3 upgrade, about, 7-1 upgrading each node, 7-6
about, <i>4-2</i>	network port requirements, 2-3
E	0
endpoint database requirements, 2-5 endpoint platforms, supported, 2-5	Oracle Key Vault management console overview of, 9-1
	Р
nstallation and configuration downloading appliance software, 4-1 endpoint database requirements, 2-5 endpoint platform, supported, 2-5 installing appliance software procedure, 4-2 network port requirements, 2-3 post-installation tasks, 4-6 system requirements, 2-1 nstallation and upgrade about, 1-1 privileges, 1-2 nstalling appliance software, 4-2	post-installation tasks, 4-6  S  search bars, 9-2 searches how to perform searches in Oracle Key Vault management console, 9-2 system requirements, 2-1  U
K	upgrading backing up
kernels, removing after upgrade, 6-13, 7-12, 8-13	Oracle Key Vault server, 6-19, 8-19 backing up upgraded Oracle Key Vault server, 6-19, 8-19 endpoint software, 6-15, 8-16



upgrading (continued)	upgrading (continued)
endpoint software for multi-master clusters,	removing old kernels, 6-13, 7-12, 8-13
7-14	upgrading multi-master cluster nodes
Oracle Key Vault pair	about, <b>7-1</b>
procedure, 8-8	checking upgrade success, 7-9
Oracle Key Vault primary-server pair	pre-upgrading preparation, 7-3
about, 8-8	upgrading each node, 7-6
Oracle Key Vault standalone	upgrading primary-server
about, <i>6-8</i>	about, <i>8-1</i>
procedure, 6-8	upgrading standalone
removing DSA keys, 6-15, 7-13, 8-15	about, <b>6-1</b>

