Oracle® Exalogic Elastic Cloud
Administrator's Guide

Release EL X2-2, X3-2, X4-2, and X5-2
E25258-17
May 2020

Oracle Exalogic Elastic Cloud Administrator's Guide, Release EL X2-2, X3-2, X4-2, and X5-2

E25258-17

Copyright © 2012, 2020, Oracle and/or its affiliates.

Primary Author: Salvador Hernández

Contributing Authors: Shanthi Srinivasan, Ashish Thomas

Contributors: Richard Mousseau, Petr Blaha, Codanda Chinnappa, John Herendeen, Tushar Pandit, Dev Prabhu, Erich Bracht, Paul Wickstrom, Ariel Levin, Michal Bachorik, Tarun Boyella, Bharath Reddy, and Ladislav Dobias, Martin Mayhead, Lubomir Petrik, Andrew Hopkinson, Denny Yim, Richard Benkreira, Edith Avot, Homer Yau, Vaidehi Srinivasarangan, Ramakrishna Mullapudi, Michael Palmeter, Venkatesh Apsingekar, Eric Huang, Helena Krkoskova, Karen Wilson

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 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" or “commercial computer software documentation” 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 and Java 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

9 Exalogic vDC Management: Basic Tasks

10 Exalogic vDC Management: Advanced Tasks

B Installing the Cloud Management API and CLI

C Exalogic vDC Management Using IaaS CLI: Basic Tasks

D Deleting Exalogic vDC Resources Using the IaaS CLI: Example Procedures

E Customizing Guest vServer Images

List of Figures

List of Tables

Preface

This guide describes how to set up, administer and manage the Exalogic Elastic Cloud virtualized environment.

This preface contains the following sections:

Audience

This guide is intended for Oracle Exalogic customers who are interested in Exalogic machine and cloud administration.

It is assumed that the readers of this manual have knowledge of the following:

- System administration concepts
- Hardware and networking concepts
- Virtualization concepts
- API, web services, and programming concepts

Revision History

E25258-17, E25258-16 (May 2020)

- Added Appendix G's sub-page Before You Begin, to include an updated note.
- Added a command "> ovm-network.log" on page Creating a vServer Template.

E25258-15 (October 2015)

- Updated "Creating Server Templates from vServers".
- Updated Updating a vServer.
- Updated step 4 in Task 3 (optional): Place the OVS Node in Maintenance Mode
- Update the note in Creating Server Templates from vServers
- Updated the note in State of the Exalogic Machine After Running the ECU.

E25258-14 (February 2015)

- Added Specifying Managed IP Address Ranges for Networks.

- Added Viewing Networks Attached to a vServer.
- Updated step 7 in Configuring the CPU subscription Ratio and CPU Consumption Limit to retain the CPU Cap default value of 100% and added a note that the CPU Cap feature is deprecated.
- Updated "Scenario 4: Decreasing the Number of vCPUs in a Running, Oversubscribed VDC" for the CPU Cap feature.

E25258-13 (April 2014)

Updated Table 5-1 with the default partition keys for X4-2 racks.

E25258-12 (March 2014)

Updated Customizing Guest vServer Images to make it clear that `modifyjeos` does not work for LVM-based templates.

E25258-11 (March 2014)

- Added prerequisites for creating vServers in Creating vServers.
- Updated step 21 in Creating vServers, with 64000 as the required MTU for guest vServers.
- Updated Configuring a User and Connection for OVAB Deployer on Exalogic with a note about enabling multiple cloud users to access the OVAB Deployer.
- Added `nfs-utils*` to the `yum` exclusion list in Customizing Guest vServer Images.

E25258-10 (December 2013)

Rebranded the guide for X4-2.

E25258-09 (December 2013)

- Updated Accessing the Exalogic Control Browser User Interface.
- Updated Viewing Exalogic System Information.
- Added Creating a Snapshot from a Volume (EECS 2.0.6.x.x).
- Added Changing Passwords for Components on the Exalogic Machine.

E25258-08 (September 2013)

Updated Creating External EoIB Networks.

E25258-07 (September 2013)

- Updated Configuring the Exalogic Machine and Setting Up the Exalogic vDC with a pointer to the MOS document that contains the version numbers of the firmware and software included in the Exalogic Elastic Cloud Software.
- Added the topic "Default Ports Assigned by ECU" in Network Configuration Performed by the ECU.
- Updated Table 5-3 for network membership of the Exalogic Control VMs in EECS 2.0.6.
- Updated the procedure in Creating External EoIB Networks.

- Updated Figure 9-4 in Examining Cloud User's Account Information to reflect the latest Exalogic Control UI.
- Updated Creating vServer Types to include information about memory limits for vServer types.
- Updated Creating vServers with information about associating vServers with two or more EoIB networks.
- Updated Creating vServers with information about ensuring that both the gateway switches are running before creating vServers.
- Added Starting vServers.
- Added Stopping vServers.
- Added Viewing Volumes Attached to a vServer.
- Added Making an OVS Node Unavailable for vServer Placement.
- Updated Figure 10-13 in Deleting a vServer to reflect the latest Exalogic Control UI.
- Added Deploying Assemblies in the Exalogic vDC Using OVAB Deployer.
- Updated Customizing Guest vServer Images to add `initscripts*` to the yum exclude list.
- Added Mounting System.img for LVM-Based vServers.
- Added Unmounting System.img for LVM-Based vServers.
- Added Managing LVM Partitions on Guest vServers.
- Updated Creating Server Templates from vServers to reflect the Oracle VM Manager UI changes in the Oracle VM 3.2.1 release.
- Standardized the usage of the `Exalogic Systems Admin` and `Cloud Admin role` names throughout the document.

E25258-06 (March 2013)

- Updated the figure in Examining Cloud User's Account Information.
- Added a note regarding vServer names to Creating vServers.
- Added Attaching Volumes to a vServer.
- Updated the procedure in Detaching Volumes from a vServer.
- Added a cautionary note against the use of Oracle VM Manager in Creating vServers and Creating Server Templates from vServers.

E25258-05 (February 2013)

Updated How High Availability Works for Guest vServers to clarify the conditions when failed vServers are restarted on a different compute node.

E25258-04 (December 2012)

- Updated Creating vServers with information about the following:
  - Enabling and disabling high availability for vServers
  - Enabling vServers to access shares on the ZFS storage appliance
  - Associating vServers with networks

  - Assigning a static IP address
- Added Managing High Availability of vServers
- Added Configuring CPU Oversubscription
- Added Allocating Virtual IPs for an Account
- Added Deallocating Virtual IPs for an Account
- Updated the procedure to mount and unmount `System.img` in Customizing Guest vServer Images
- Updated Example Procedure: Modifying Current Disk Size
- Added Setting Up Access to the ZFS Storage Appliance for a vServer
- Updated screenshots of Exalogic Control to reflect the changes in the UI since the previous release of this document.

Documentation Accessibility

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

Access to Oracle Support

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

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.

1

Introduction to Exalogic Elastic Cloud

This chapter describes Oracle Exalogic Elastic Cloud and its terminology.
This chapter contains the following topics:

About Oracle Exalogic Elastic Cloud

Oracle Exalogic Elastic Cloud is a standard data center building block that provides a fully integrated Private Cloud platform that is ideal for a wide range of mission-critical enterprise application workloads, from middleware and custom applications to packaged applications from Oracle and hundreds of 3rd party application and tool vendors.

Exalogic is designed to fully leverage an internal InfiniBand fabric that connects all of the processing, storage, memory and external network interfaces within an Exalogic machine to form a single, large computing device. Each Exalogic machine is connected to the customer's data center networks via 10 GbE (traffic) and GbE (management) interfaces. The InfiniBand technology used by Exalogic offers significantly high bandwidth, low latency, hardware-level reliability, and security.

Oracle Exalogic Elastic Cloud offers several new features and benefits, including the following:

- Supports virtualization.
- Includes new management software components to aid in all aspects of hardware and software management for Exalogic's virtualization solution. These capabilities are included in a new software stack named Exalogic Control.
- Offers a unified interface for interacting with the Exalogic platform to configure, use, and optimize infrastructure resources.
- Allows applications and management tools to interact with the Exalogic platform via Infrastructure as a Service (IaaS) APIs that are exposed to customers.
- Manages resource supply, configuration, and utilization.

Oracle Exalogic Elastic Cloud Terminology

Table 1-1 lists a few important terms and their definitions.

Table 1-1 Important Terms and Definitions

Term	Description
Virtualized Data Center (vDC)	A collection of physical compute nodes and storage that sit on the Exalogic fabric. These physical resources are organized into a pool that can then be accessed by self-service users. It offers an access point through which to allocate and control the resources inside.
Account	A container for virtual resources in the Exalogic vDC. It includes the concept of quotas for the amount of CPU, memory, storage and networking resources that may be consumed within the context of that account (within the scope of a single vDC). **Note**: An account is created by the Cloud Admin user.
Quota	A limit for vCPU, memory, and storage resources defined while creating an account.
Account Resource Limits	The sum total of resources available to all users executing in the context of that Account.
Exalogic Systems Admin	The role for a user who is responsible for overall monitoring and management of the Exalogic machine, including its hardware components and network management.
Cloud Admin	The role for a user who configures the cloud. A Cloud Admin user creates Accounts and sets quotas. In addition, a Cloud Admin user monitors the resource consumption and Cloud User activities within the vDC.
Cloud User	The role for a user that consumes resources in the Exalogic vDC. Deploying vServers and applications is the primary responsibility of this user. A given cloud user may have access privileges to multiple Accounts within the Exalogic vDC.
Access Keys	Used for authentication of cloud user requests to a cloud account.
Key Pairs	Defines the cloud user credentials to access a vServer.
Exalogic Guest Base Template	Exalogic supports Oracle VM (OVM) server templates for the x86 processor architecture. All applications deployed on Exalogic must be deployed to vServers that are derived from a specialized server template that contains software and tools that are required for the proper functioning of vServers on Exalogic. This special server template is called the Exalogic Guest Base Template.
Server Template	An operating system image in a certain format that can be used to create a new vServer. Exalogic supports Oracle VM (OVM) Server templates for the x86 processor architecture. A server template is not just an operating system; it also contains application artifacts. In the Exalogic environment, the server template is a derivation of the Exalogic Guest Base Template. All vServers created in the Exalogic vDC are based on a server template.
Virtual Server (vServer)	An entity that provides the outward interface of a stand-alone operating system. This entity is a virtual machine with guest operating system, which consumes CPU and memory resources. A vServer can be a member of one or more vNets.

Table 1-1 (Cont.) Important Terms and Definitions

Term	Description
Virtual Network (vNet)	A networking construct that dictates which vServers may communicate with which other vServers. A vNet is created by a cloud user. The number of vNets that may be created depends on the quota allocated to an account.
Volume	A piece of storage. It consumes storage resources from an account. A volume that contains a bootable image of an operating system is called a Root Volume. Volumes have their own lifecycle and exist beyond the scope of the vServers that attach them. A volume is created by a cloud user. It can be created with an explicit command, but can also be created as a side effect of vServer creation.
Snapshot	A point-in-time image of a volume. A snapshot is created by a cloud user.

2
Understanding Exalogic Control

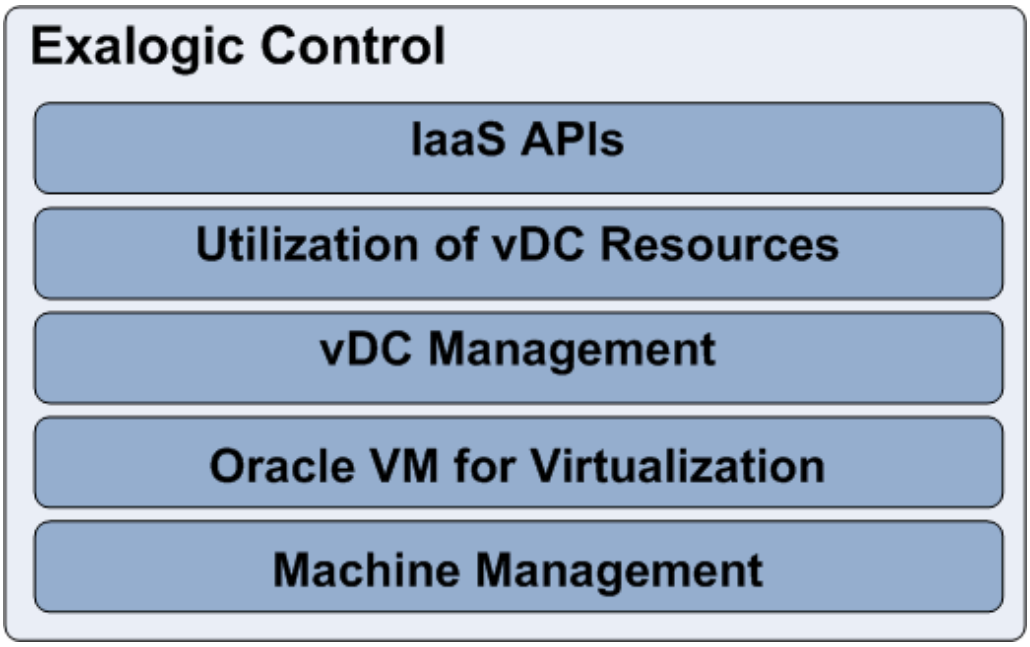
This chapter introduces Exalogic Control, which provides a comprehensive set of features and tools to interact with and manage a virtual data center on an Exalogic machine.
This chapter contains the following topics:

Overview of Exalogic Control

Exalogic Control works in conjunction with the Exalogic Elastic Cloud Software platform to deliver an extensive cloud management solution on Exalogic. Exalogic Control is a comprehensive software management stack providing onboarded capabilities for Exalogic machine and vDC management, and monitoring.

Exalogic Control's components and functions are depicted in Figure 2-1.

Figure 2-1 Exalogic Control Components and Functions



Exalogic Control offers unified interfaces for interacting with the Exalogic platform to configure, monitor, and utilize its machine and virtual data center (vDC) resources. It enables other applications and management tools to interact with the Exalogic platform via Infrastructure As a Service (IaaS) APIs.

Introduction to Exalogic Machine Management

Exalogic Control offers hardware monitoring and management capabilities specific to the well-defined Exalogic machine hardware from two important perspectives:

- Individual hardware components in the Exalogic machine
- Known relationships between these hardware components

The browser user interface (BUI) of Exalogic Control provides Exalogic-specific photorealistic views that visualize detailed diagnostic information in a manner that is specific to context and location of the hardware components. The BUI shows the Exalogic machine as an asset as opposed to a collection of discovered hardware components.

The following lists some of the Exalogic machine management features offered by Exalogic Control:

- Photorealistic visualization
- Exalogic machine rack as a top-level asset
- Exalogic fabric and multi-rack relationship
- Monitoring and alerting
- Physical fabric or network
- Fault detection and management
- Support request management with My Oracle Support
- Hardware replacement lifecycle
- Exalogic system reports

> **Note:**
>
> Exalogic machine management tasks are performed by users with the **Exalogic Systems Admin** role. For more information, see Creating the Exalogic Systems Admin User and Monitoring the Exalogic Machine.

Introduction to Exalogic vDC Management

Exalogic Control enables you to administer the Exalogic vDC and its resources. It offers the following management features specific to Exalogic:

- Management of Exalogic fabric, which constitutes the virtual data center
- Configuration and management of the vDC
- Monitoring of vDC resources
- Public network configuration (EoIB)

- Partition key (p-key) allocation and tracking
- Creation and setup of Accounts in the vDC
- Resource quota management
- Network resource allocation
- Storage resource allocation

> **Note:**
>
> Exalogic vDC management tasks are performed by users with the **Cloud Admin** role. For more information about this role, see Creating the Cloud Admin User. For procedural information, see Administering the Exalogic vDC and Setting Up the Infrastructure and Managing the Exalogic vDC Infrastructure.
>
> Each Exalogic machine contains one default vDC only.

Exalogic Cloud User Abstractions

Exalogic Control provides the Cloud User with an IaaS abstraction for provisioning application deployments to the cloud.

The following lists some of the features offered by Exalogic Control:

- Ability to provision customer applications into the Exalogic vDC
- Web Service and CLI interfaces
- Virtual machine (vServer) configuration
- Virtual machine (vServer) lifecycle and control
- Allocation and management of resources, such as private vNets, volumes, and external IP
- Dynamic private network creation
- Public network binding

> **Note:**
>
> Exalogic cloud user tasks are performed by users with the **Cloud User** role. For more information about this role, see Creating the Cloud Admin User. For procedural information, see Creating and Managing Exalogic vDC Resources and Managing Account Resources.

Exalogic Control User Interfaces

Exalogic Control provides the following management user interfaces:

- Browser User Interface (BUI) for machine management, vDC management, and cloud user tasks

- IaaS API and CLI for cloud user tasks

> **Note:**
>
> In this guide, the BUI procedures are described in Monitoring the Exalogic Machine, Exalogic vDC Management: Basic Tasks, and Exalogic vDC Management: Advanced Tasks.
>
> For information about CLI procedures, see Exalogic vDC Management Using IaaS CLI: Basic Tasks and Deleting Exalogic vDC Resources Using the IaaS CLI: Example Procedures.
>
> For information about the cloud management API, see the *Oracle Enterprise Manager Ops Center Cloud Infrastructure API and CLI Reference Guide*.

Accessing the Exalogic Control Browser User Interface

You can access the Exalogic Control browser UI at the following URL:

`https://ec_vm/emoc`

`ec_vm` is the `EoIB-external-mgmt` IP address of the vServer that hosts the Enterprise Controller component of Exalogic Control. For EECS 2.0.4.x.x and earlier releases, you can find out the `EoIB-external-mgmt` IP address from the `/opt/exalogic/ecu/config/oc_ec.json` file on the master compute node, typically cn01. For EECS 2.0.6.x.x, see `/opt/exalogic/ecu/config/elcontrol.json` on the master compute node.

3

Installing Oracle VM Server on Exalogic Compute Nodes

Oracle Linux is preinstalled on Exalogic compute nodes. To set up the Exalogic machine as a virtualized datacenter, the compute nodes should be reimaged to Oracle VM Server.

Oracle recommends strongly that reimaging the compute nodes to Oracle VM Server be performed by fully trained, qualified Oracle personnel or by formally accredited Oracle partners. For more information, contact Oracle Advanced Customer Support (http://www.oracle.com/acs).

> **Note:**
>
> For information about the version numbers of the software and firmware included in various releases of the Exalogic Elastic Cloud Software, see the My Oracle Support document 1530781.1.

4

Configuring the Exalogic Machine and Setting Up the Exalogic vDC

This chapter describes the initial configuration tasks and the state of the Exalogic machine after running the Exalogic Configuration Utility.

This chapter contains the following topics:

Important Notes Before You Begin

Oracle recommends strongly that the following tasks be performed by fully trained, qualified Oracle personnel or by formally accredited Oracle partners. For more information, contact Oracle Advanced Customer Support (http://www.oracle.com/acs).

- Verifying the system, network, and software before configuring your Exalogic machine
- Configuring your Exalogic machine
- Setting up the Virtualized Data Center (vDC) on your Exalogic machine
- Bootstrapping the Exalogic Control cloud management environment

State of the Exalogic Machine After Running the ECU

After your Exalogic machine is configured using ECU, the state of your Exalogic machine is as follows:

- Compute nodes, switches, and storage appliance configured with network interfaces
- InfiniBand partitions configured for six networks created by ECU (one EoIB external management network, and five IPoIB administration networks)
- Default Virtual Data Center (vDC) set up on Exalogic
- Exalogic Control stack running on the machine

For information about the version numbers of the software and firmware included in various releases of the Exalogic Elastic Cloud Software, see the My Oracle Support document 1530781.1.

Note:

Starting from release 2.0.6.0.0 of the Exalogic Elastic Cloud Software, you can do the following:

- Convert an Exalogic physical configuration—that is, all the compute nodes running Linux—to a hybrid configuration, where one half of the compute nodes run Oracle VM Server and serve as a virtualized data center, while the other nodes remain on Linux. While installing and configuring the Exalogic Elastic Cloud Software, you can choose the rack half (top or bottom) that should be virtual. For information about the supported hybrid configurations, see the *Oracle Exalogic Elastic Cloud Release Notes.*
- Convert a hybrid configuration to a full-virtual configuration.

These conversions require reimaging the compute nodes from Oracle Linux to Oracle VM Server. For more information and support about conversion, contact Oracle Advanced Customer Support (http://www.oracle.com/acs).

5
Understanding Exalogic Networks

This chapter describes Exalogic infrastructure fabrics and associated networks. This chapter contains the following topics:

Default Network Configuration for Oracle VM Servers

After you reimage an Exalogic compute node from Oracle Linux to Oracle VM Server, each compute node (`dom0`) has the following network configuration:

- Bonded `bond0` interface over the `eth0` interface
- Xen bridge interface (`xenbr0`) on top of `bond0` - the `xenbr0` interface holds the `eth` interface IP.
- Bonded `bond1` interface over `ib0` and `ib1` interfaces - this is the IPoIB interface for the default InfiniBand partition.

Network Configuration Performed by the ECU

Table 5-1 describes the networks set up by the Exalogic Configuration Utility (ECU) when it used to configure the Exalogic machine.

> **Note:**
>
> These are the system network partitions set by the ECU. You must not modify them.

Table 5-1 Exalogic Networks

Name of the Network	Default Partition Key (X2-2, X3-2)	Default Partition Key (X4-2)	Device and Default IP Address	Description
IPoIB-default	`Default`	`Default`	`192.168.10.1/24` `bond1` for compute nodes `ipmp1` for the storage appliance	Default InfiniBand partition.

Table 5-1 (Cont.) Exalogic Networks

Name of the Network	Default Partition Key (X2-2, X3-2)	Default Partition Key (X4-2)	Device and Default IP Address	Description
IPoIB-admin	0x8001	0x0002	192.168.20.0/24 bond2 for compute nodes ipmp2 for the storage appliance	Used for all interconnections among the different components of Exalogic Control.
IPoIB-storage	0x8002	0x0003	192.168.21.0/24 bond3 for compute nodes ipmp3 for the storage appliance	Used internally to access shares on the storage appliance. It is different from the IPoIB-vserver-shared-storage network.
IPoIB-virt-admin	0x8003	0x0004	bond4 172.16.0.0/16	Used by Exalogic Control for all virtualization management.
IPoIB-ovm-mgmt	0x8004	0x0005	bond5 192.168.23.0/24	Used for all Oracle VM management. This includes heartbeat, migration, and virtualization control.
IPoIB-vserver-shared-storage	0x8005	0x0006	bond6 for compute nodes, and ipmp4 for the storage appliance 172.17.0.0/16	Used to provide access to Sun ZFS Storage Appliance for customer or application vServers.
EoIB-external-mgmt	0x8006	0x0007	bond7 VLAN ID, Ethernet device/ connector (Ethernet port on the Sun Network QDR InfiniBand Gateway Switch), and network IP/subnet mask defined by the user	Used to provide external access to the vServer that hosts the Enterprise Controller component of Exalogic Control.

> **Note:**
>
> You can change the default network configuration of IPoIB-default (192.168.10.0/24), but you cannot change its partition key.

Default Ports Assigned by ECU

For information about the default ports of the hardware components in Exalogic, see the "Default Port Assignments" section in the *Oracle Exalogic Machine Owner's Guide*.

For information about the default ports of Enterprise Manager Ops Center components, see the "Network Port Requirements and Protocols" section in the *Oracle Enterprise Manager Ops Center Feature Reference Guide*.

Table 5-2 describes the default ports assigned to the database component of Exalogic Control and to the WebLogic Server container that hosts the Oracle VM Manager component of Exalogic Control.

Table 5-2 Default Ports Assigned by ECU

Source	Target	Protocol	Port	Application
Any	Database	TCP	1521	Database listener
Any	Oracle VM Manager	HTTP over TCP	7001	WebLogic Server listener
Any	Oracle VM Manager	HTTPS over TCP	7002	Secure WebLogic Server listener

Network Membership of Exalogic Components

Table 5-3 outlines the network participation of the components in the Exalogic machines. The table also provides information about their InfiniBand partition membership types. *N/A* indicates that the component is not part of that network.

Table 5-3 Network Membership of Exalogic Components

Component	eth-admin	IPoIB-default	IPoIB-admin	IPoIB-storage	IPoIB-virt-admin	IPoIB-ovm-mgmt	IPoIB-vserver-shared-storage	EoIB-external-mgmt
Compute nodes	Yes	Full	Both (full and limited)	Both (full and limited)	Both (full and limited)	Both (full and limited)	Both (full and limited)	N/A
ILOM on compute nodes	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Storage heads	Yes	Full	Full	Full	N/A	N/A	Full	N/A
ILOM on storage heads	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Sun Network QDR InfiniBand Gateway Switches (NM2-GW)	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Sun Datacenter InfiniBand Switch 36 (NM2-36P)	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Cisco switch	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PDUs in the Exalogic machine	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Guest VMs	N/A	N/A	N/A	N/A	Limited	N/A	Limited	N/A
Exalogic Control components (up to release 2.0.4.x.x)								
Oracle Database VM	N/A	N/A	Full	Limited	Full	Full	N/A	N/A

Table 5-3 (Cont.) Network Membership of Exalogic Components

Component	eth-admin	IPoIB-default	IPoIB-admin	IPoIB-storage	IPoIB-virt-admin	IPoIB-ovm-mgmt	IPoIB-vserver-shared-storage	EoIB-external-mgmt
Enterprise Controller VM	N/A	N/A	Full	Limited	Full	Full	Full	Full
Proxy Controller VMs	Yes	Full	Full	Limited	Full	Full	Full	N/A
Oracle VM Manager VM	N/A	N/A	Full	Limited	Full	Full	N/A	Full
Exalogic Control components (release 2.0.6.x.x)								
Exalogic Control VM	Yes	N/A	Full	Full	Full	Full	Full	Full
Proxy Controller VMs	Yes	Full	Full	Full	Full	Full	Full	N/A

Note:

For guest VMs on Exalogic connecting to Oracle Exadata Database Machine, the default InfiniBand partition is used.

6
Creating and Managing Users and Roles

This chapter discusses user and role management in Exalogic Control.
It contains the following topics:

User Profiles

Table 6-1 describes the user profiles and their primary responsibilities in the Exalogic cloud environment.

Table 6-1 Roles and Responsibilities

Role	Primary Responsibilities	Skills Required
Root user	Super user or a data center administrator that creates the Exalogic Systems Admin user.	The user must be an experienced data center administrator.
Exalogic Systems Admin	Administers and manages the Exalogic machine platform.	The user must be familiar with Exalogic machine management, Exalogic machine network, and OS management.
Cloud Admin	Sets up the cloud infrastructure and resource allocation, so that Cloud Users can deploy their applications on to authorized Accounts. The Cloud Admin user also manages the Cloud Users accessing the accounts and their authorization.	The user must be familiar with system administration, including virtualization, networking, and storage.

Table 6-1 (Cont.) Roles and Responsibilities

Role	Primary Responsibilities	Skills Required
Cloud User	Uses the resources allocated to them to create Virtual Servers and deploy applications. Cloud users are presented only with the required options in the Exalogic Control browser user interface (BUI).	The user must be familiar with hardware management, network management, virtualization, and OS management in general.

Before You Begin

When Exalogic Control is initiated and started by the Exalogic Configuration Utility (ECU), a default `root` user account is created. This `root` user must create the Exalogic Systems Admin user in Exalogic Control.

When you create a user, the user name and its associated password are imported from the local directory on the VM hosting the Enterprise Controller component of Exalogic Control. You must add a user name to this local directory before you can add it as a local user in Exalogic Control.

To create a user on the VM hosting the Enterprise Controller, do the following:

1. Run the `useradd` command, as in the following example:

   ```
   # useradd -d /home/ELAdmin -s /bin/bash -m ELAdmin
   ```

2. Run the `passwd` command to set a password for the newly created local user, as in the following example:

   ```
   # passwd ELAdmin
   ```

3. Repeat this procedure to create other local users, such as `CloudAdmin`, `User1`, and `User2`.

Creating the Exalogic Systems Admin User

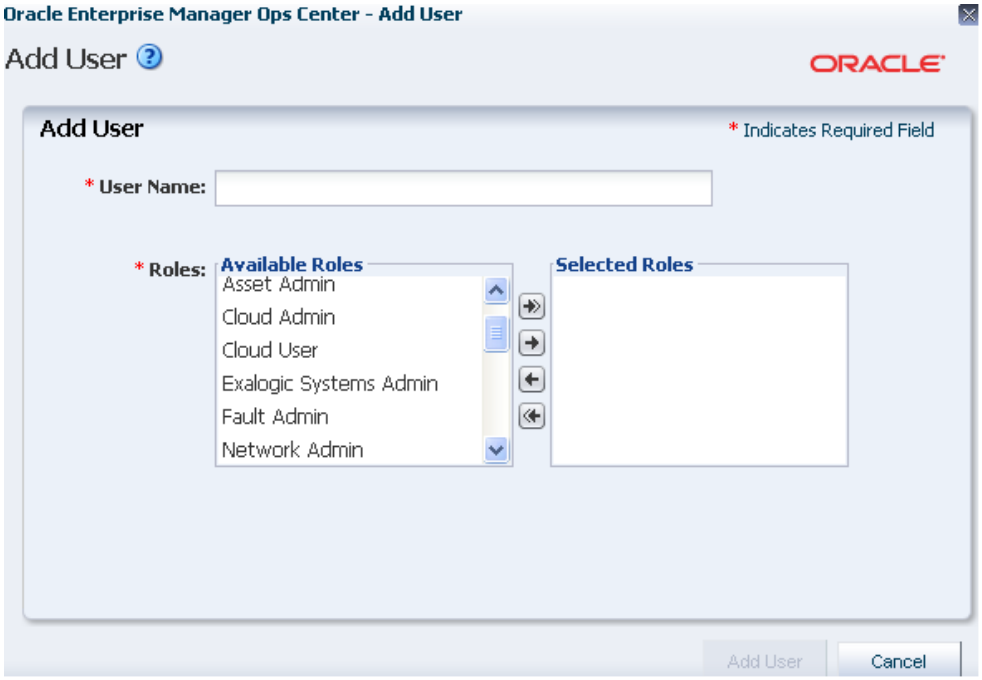
To create the Exalogic Systems Admin role in Exalogic Control, complete the following steps:

1. Ensure that the user exists as a local user on the virtual machine that hosts the Enterprise Controller component of Exalogic Control, as described in Before You Begin..
2. Access the browser UI of Exalogic Control as described in Accessing the Exalogic Control Browser User Interface, and log in as the `root` user.

   If you do not know the password for the `root` user, contact Oracle Support.
3. On the home page, click **Administration** in the navigation pane on the left.
4. Under Enterprise Controller, click **Local Users**. The Local Users page is displayed.

5. Under Users and Notification Profiles, click the **Add User** icon. Alternatively, click **Add User** on the **Operate** pane. The Add User screen is displayed, as shown in Figure 6-1.

Figure 6-1 Add User Screen



6. In the **User Name** field, enter the user name, which was added to the OS environment. For example, `ELAdmin`.
7. Select the `Exalogic Systems Admin` role, the `Role Management Admin` role, and the `User Management Admin` role from the Available Roles list, and move them to the Selected Roles list by clicking the right arrow.

> **Note:**
>
> You are adding the `User Management Admin` role to allow the Exalogic Systems Admin user to manage users.

8. Click **Add User**.

   The Exalogic Systems Admin user is created.

> **Note:**
>
> Typically, only one or two users are created with the Exalogic Systems Admin role.

9. Log out as the `root` user.

Creating the Cloud Admin User

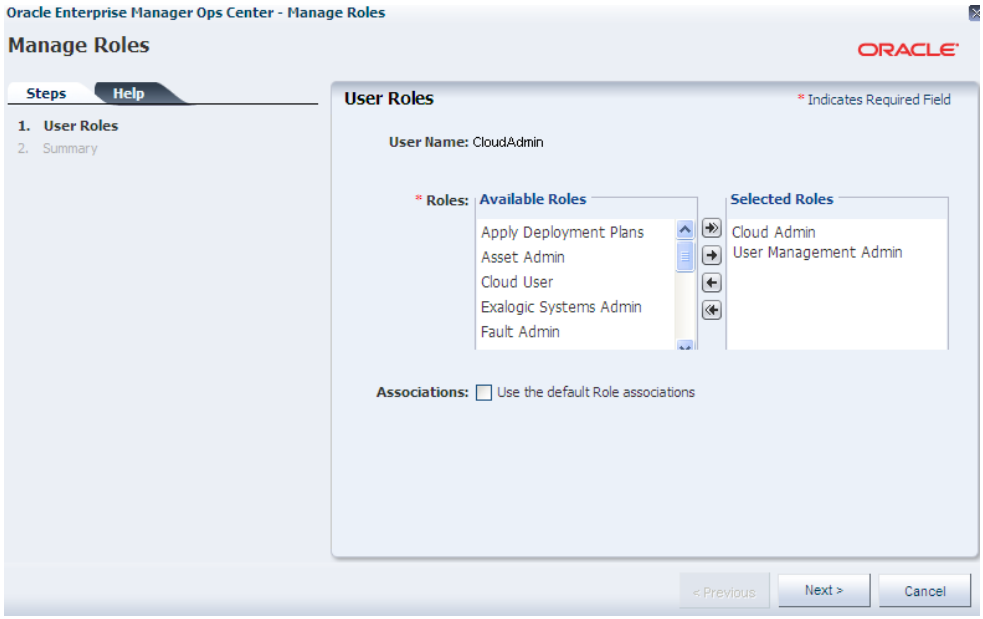
The Exalogic Systems Admin user creates the Cloud Admin user. To create the Cloud Admin user, complete the following steps:

1. Ensure that the user exists as a local user on the virtual machine that hosts the Enterprise Controller component of Exalogic Control, as described in Before You Begin..
2. Access the browser UI of Exalogic Control as described in Accessing the Exalogic Control Browser User Interface, and log in as the `ELAdmin` user.
3. On the home page, click **Administration** in the navigation pane on the left.
4. Under Enterprise Controller, click **Local Users**. The Local Users page is displayed.
5. Under Users and Notification Profiles, click the **Add User** icon. Alternatively, click **Add User** on the **Operate** pane. The Add User screen is displayed.
6. To create the Cloud Admin user, do the following:
   - In the **User Name** field, enter the user name. For example, `CloudAdmin`.
   - Select the `Cloud Admin` role and the `User Management Admin` role from the list of Available Roles, and move it to Selected Roles by clicking the right arrow.

     > **Note:**
     >
     > You are adding the `User Management Admin` role to allow the Cloud Admin user to manage users.

   - Click **Add User**. The Cloud Admin user is created. The `CloudAdmin` user is listed in the Users and Notification Profiles page.
7. Select the `CloudAdmin` user on the Users and Notification Profiles page, and click the **Manage User Roles** icon. The Manage Roles wizard is displayed, as shown in Figure 6-2.

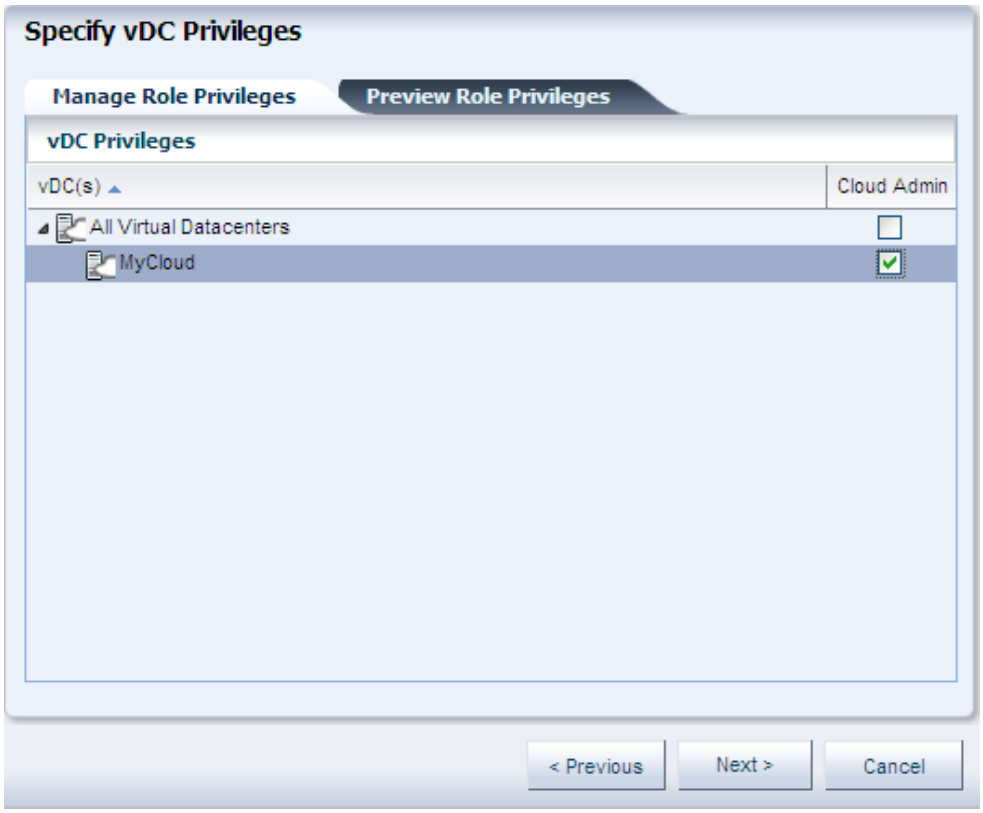
Figure 6-2 Manage Roles Wizard



By default, the **Associations** option is selected. De-select this option.

8. Click **Next**. The Specify Asset Privileges screen is displayed.
9. Click **Next**. The Specify Library Privileges screen is displayed.
10. Click **Next**. The Specify Network Privileges screen is displayed.
11. Click **Next**. The Specify Plan Management Privileges screen is displayed.
12. Click **Next**. The Specify vDC Privileges screen is displayed, as shown in Figure 6-3.

Figure 6-3 Specify vDC Privileges

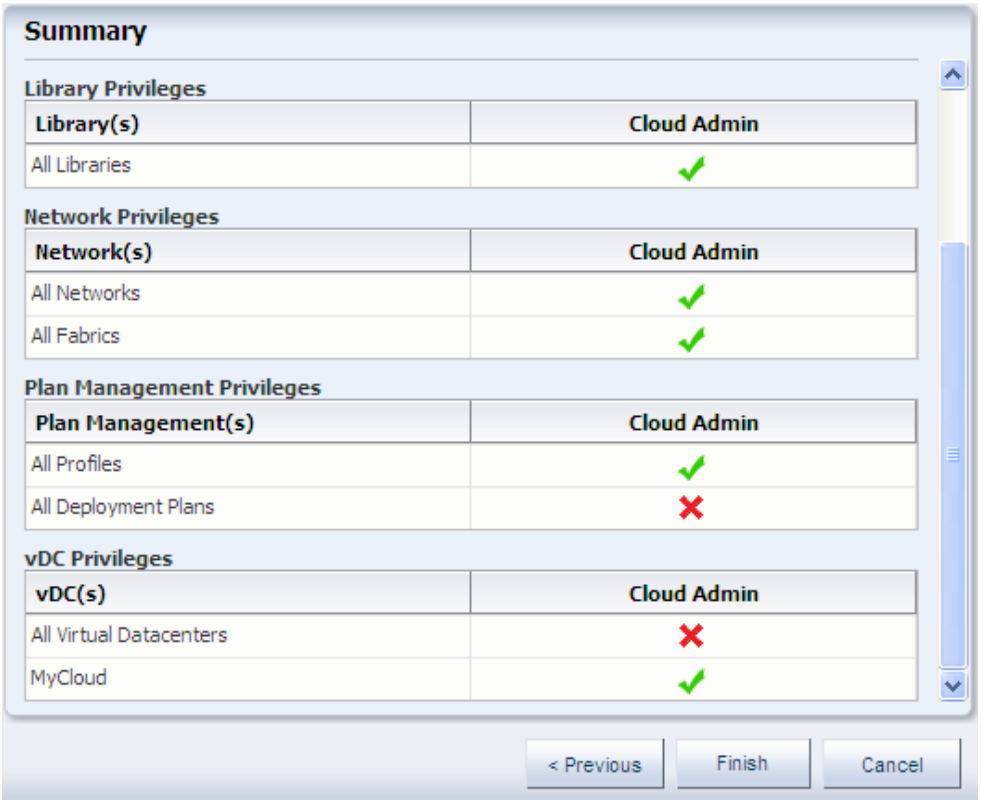


13. Expand **All Virtual Datacenters**.

    The `MyCloud` (the default Exalogic vDC) is listed. Select the **Cloud Admin** option for this vDC. Click **Next**.

    The Summary screen is displayed, as shown in Figure 6-4.

Figure 6-4 Summary



The Summary screen provides a summary of Asset Privileges, Library Privileges, Network Privileges, Report Privileges, Plan Management Privileges, and vDC Privileges.

14. Review the summary, and click **Finish**.

Creating Cloud Users

The Exalogic Systems Admin user creates Cloud Users. To create Cloud Users (`User1` and `User2`), complete the following steps:

1. Ensure that the user exists as a local user on the virtual machine that hosts the Enterprise Controller component of Exalogic Control, as described in Before You Begin..
2. Access the browser UI of Exalogic Control as described in Accessing the Exalogic Control Browser User Interface, and log in as the `ElAdmin` user.
3. On the home page, click **Administration** in the navigation pane on the left.
4. Under Enterprise Controller, click **Local Users**. The Local Users page is displayed.
5. Under Users and Notification Profiles, click the **Add User** icon. Alternatively, click **Add User** on the **Operate** pane. The Add User screen is displayed.
6. To create a Cloud User, do the following:
   - In the **User Name** field, enter the user name. For example, `User1`.

- Select the `Cloud User` role from the list of Available Roles, and move it to Selected Roles by clicking the right arrow.
- Click **Add User**. The Cloud User (`User1`) is created. The `User1` user is listed in the Users and Notification Profiles page.

7. Similarly, create `User2` with Cloud User permissions.

Adding Users from a Directory Server

You can add directory servers to Exalogic Control. Users and roles are added to Exalogic Control from the directory server. Users that are added from a directory server begin with complete privileges for each of their roles.

You must configure the remote directory server before adding it to Oracle Exalogic Control as follows:

1. Create the following user groups on the directory server:
   - `EXALOGIC_ADMIN`
   - `CLOUD_ADMIN`
   - `CLOUD_USER`
2. Add users to these groups. The users within each group are given the role corresponding to the group.

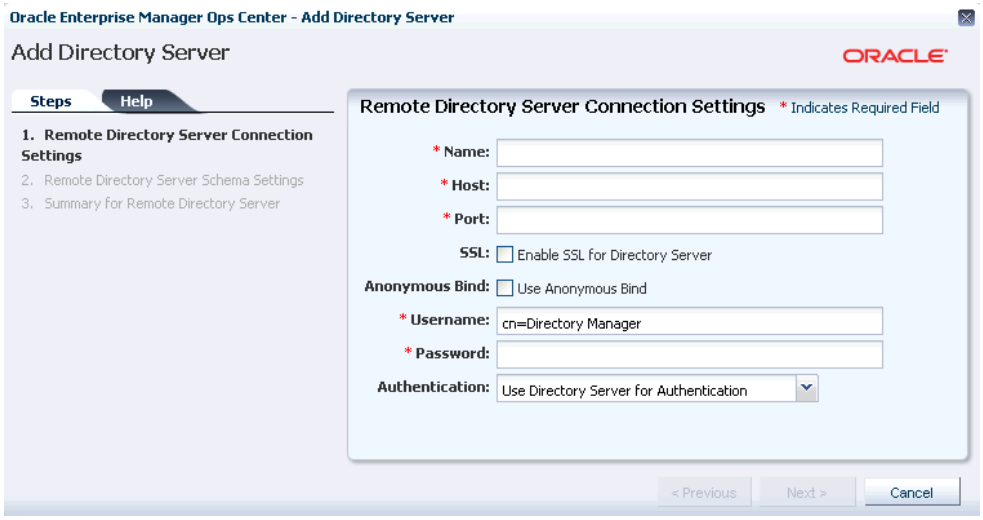
Adding a Directory Server

To add a directory server in Exalogic Control, complete the following steps:

1. Access the browser UI of Exalogic Control as described in Accessing the Exalogic Control Browser User Interface, and log in as a user with the `Exalogic Systems Admin` role.
2. In the Navigation pane, select **Administration**.
3. Select **Directory Servers**.
4. In the Actions pane, click **Add Directory Server** icon.

   The Add Directory Server wizard is displayed, as shown in Figure 6-5.

Figure 6-5 Add Directory Server Wizard



5. Enter the following connection settings:
   - **Name** - Enter the name of the directory server
   - **Hostname** - Enter the host name of the directory server
   - **Port** - Enter the port number to be used to access the directory server
   - **Use SSL** - Select this option to use SSL to connect to the directory server
   - **Username** - Enter the user name used to access the directory server
   - **Password** - Enter the password used to access the directory server
6. Click **Next**. The Remote Directory Server Schema Settings page is displayed.
7. Enter the following schema settings:
   - **Root suffix** - The root node of the directory tree for the user search
   - **User search DN** - The subnode in which to search for users
   - **User search scope** - The scope of the user search. Acceptable values are base, one, subtree, baseObject, singleLevel, wholeSubtree, or subordinateSubtree.
   - **User search filter** -An LDAP search filter which users must meet for inclusion
8. Click **Next**. The Summary page is displayed.
9. Review the summary, and click **Add Directory Server**.

Synchronizing Remote Users and Roles

You can synchronize Exalogic Control with one or all directory servers. This updates the list of users and roles to match the directory server's current information.

1. Access the browser UI of Exalogic Control as described in Accessing the Exalogic Control Browser User Interface, and log in as a user with the `Exalogic Systems Admin` role.
2. In the Navigation pane, select **Administration**.
3. Click **Directory Servers**.

The list of directory servers is displayed.

4. To synchronize Exalogic Control with a single directory server, select the server and click the **Sync Remote Users and Roles** icon.

   To synchronize Exalogic Control with all the directory servers, click **Sync all remote users and roles** in the **Actions** pane.

   A confirmation window is displayed.

5. Click **OK**.

Roles and Permissions

This section lists the permissions associated with the following roles:

- Exalogic Systems Admin Permissions
- Cloud Admin Permissions
- Cloud User Permissions

Exalogic Systems Admin Permissions

Exalogic Systems Admin has the following permissions:

- READ
- WRITE
- ASSET_MGMT
- CREDENTIAL_MGMT
- DIRECTORY_SERVER_MGMT
- JOB_MGMT
- NETWORK_DOMAIN_CREATION
- NETWORK_DOMAIN_DELETION
- NETWORK_DOMAIN_MGMT
- NETWORK_DOMAIN_USAGE
- OVM_MANAGER_MGMT
- OVM_MANAGER_USAGE
- PDU_MGMT
- PDU_USAGE
- PROFILE_PLAN_MGMT
- REPORT_MGMT
- SERVER_DEPLOYMENT
- STORAGE_MGMT
- NETWORK_MGMT
- NETWORK_CREATION
- NETWORK_DELETION

- NETWORK_USAGE
- FABRIC_CREATION
- FABRIC_DELETION
- FABRIC_MGMT
- FABRIC_USAGE
- STORAGE_CREATION
- STORAGE_DELETION
- STORAGE_USAGE
- PROXY_CONTROLLER_MGMT
- USER_MGMT
- ROLE_MGMT
- SERVICE_REQUEST
- STORAGE_SERVER_USAGE
- STORAGE_SERVER_MGMT
- SERVER_USAGE
- SERVER_MGMT
- OPERATING_SYSTEM_USAGE
- OPERATING_SYSTEM_MGMT
- SWITCH_USAGE
- LINK_AGGREGATION
- UPDATE_FIRMWARE
- OPERATION_EXECUTION
- EC_REGISTRATION
- EC_HTTP_PROXY_MGMT
- EC_ENERGY_COST_MGMT

Cloud Admin Permissions

Cloud Admin has the following permissions:

- READ
- SERVER_POOL_MGMT
- SERVER_POOL_USAGE
- VIRTUALIZATION_HOST_MGMT
- VIRTUALIZATION_HOST_USAGE
- VIRTUALIZATION_GUEST_CREATION
- VIRTUALIZATION_GUEST_DELETION
- VIRTUALIZATION_GUEST_MGMT

- VIRTUALIZATION_GUEST_USAGE
- STORAGE_MGMT
- STORAGE_USAGE
- NETWORK_MGMT
- NETWORK_USAGE
- FABRIC_MGMT
- FABRIC_USAGE
- LINK_AGGREGATION
- IPMP_GROUPS
- SERVER_MGMT
- SERVER_USAGE
- OPERATING_SYSTEM_USAGE
- OPERATING_SYSTEM_MGMT
- STORAGE_SERVER_USAGE
- SWITCH_MGMT
- SWITCH_USAGE
- CLOUD_MGMT
- WRITE

Cloud User Permissions

Cloud User has the following permissions:

- READ
- VIRTUALIZATION_GUEST_MGMT
- VIRTUALIZATION_GUEST_USAGE
- STORAGE_USAGE
- NETWORK_USAGE
- FABRIC_USAGE
- SERVER_USAGE
- OPERATING_SYSTEM_USAGE
- OPERATING_SYSTEM_MGMT
- STORAGE_SERVER_MGMT
- STORAGE_SERVER_USAGE
- SWITCH_USAGE
- CLOUD_USAGE
- WRITE

7

Task Overviews and Basic Concepts

This chapter introduces some of the important tasks performed by users with the Exalogic Systems Admin, Cloud Admin, and Cloud User roles. It also describes a few basic concepts.
This chapter contains the following sections:

Cloud Admin Tasks

This section introduces the following tasks:

Account Creation

An Account entitles designated Cloud Users the authorization to use computing, network, and storage resources of the Exalogic vDC. The Account provides the required capabilities to manage these resources.

The following are the prerequisites for creating an account:

- Estimate the resource quotas to be allocated for the account
- Identify the Cloud Users to be assigned to the account

The quota for vCPU, memory, and storage resources are defined during Account creation. The Resource Quota Information display in the account wizard creation indicates how much of the corresponding vDC resources can be used. It also displays whether the vDC resources are oversubscribed or undersubscribed.

You can configure an account to be able create a maximum of 4096 private vNets in an account. You can set the limit of number of private vNets that can be created in an account. The allowable number of defined networks is a function of the server pool configuration defined in the Exalogic vDC. Within each server pool, you can create a maximum of 64 private networks. However, note that some networks are already defined for use by Exalogic Control.

During Account creation, the public networks that are available in the vDC are listed. You can set the number of public IP addresses allocated to the account from this resource. This public IP address can be used by the Cloud User to assign to the vServer, as required. You can choose what defined public networks are available to each Account.

You provide an entitlement to the virtual resources for an account. You allocate the resources from the vDC to an account. The resource allocation for all of the accounts

in a vDC can be more than the actual resources in a vDC. This oversubscription of the resources must be identified and planned for a vDC. You must configure the virtual resources for an account properly and update the resource configuration when the requirement increases. If an account does not have enough resources, then the Cloud User will get notifications that they cannot create vServers if the resources are not available.As a Cloud Admin user, you must watch the resource usage and configure resources for an account. You can create as many or few Accounts as your business requires. By doing so, you can partition the Exalogic vDC by Account, based on resource allocation.

Account Management

As a Cloud Admin user, you can update the resource configuration for an account, assign Cloud Users to an account, and delete an account.

You can assign Cloud Users to an account during account creation or separately. Cloud Users have access to only the specific Accounts to which they are added. As a Cloud Admin user, you can manage the access of the Cloud Users to all Accounts in the Exalogic vDC.

vServer Types

A vServer Type is a profile that defines the memory and virtual CPUs to be allocated to vServers creating by using that profile. A Cloud User is restricted to using these definitions to create vServers.

The following default system-defined vServer types are available in the Exalogic vDC:

- **EXTRA_LARGE**: 16 GB memory and 4 vCPUs
- **LARGE**: 8 GB memory and 2 vCPUs
- **SMALL**: 4 GB memory and 1 vCPU

As a Cloud Admin user, you can create additional vServer types and delete them. However, you cannot delete the system-defined vServer types. For information about creating vServer types, see Creating vServer Types.

When you create a vServer type, the following information is displayed in the wizard, based on the resources defined:

- The number of Oracle VM Servers in the Exalogic vDC that have sufficient physical resources to host a vServer with the selected resources
- An estimation of the number of vServers that can be hosted using the available physical resources in the vDC

Cloud User Tasks

A Cloud User with access to an account is entitled to manage and use computing, network, and storage resources in an Exalogic vDC within the limits of the account quotas.Cloud Users can create and manage the life cycle of vServers for their applications. To accomplish this, a Cloud User can manage the following virtual resources for an account:

- Virtual Network Resources
- Server Templates

- Virtual Storage Resources
- Distribution Groups
- vServers

Virtual Network Resources

Virtual networks restrict the network connectivity of a vServer. Virtual network management involves connecting and restricting the network access to vServers.

The following types of virtual networks are visible to a Cloud User:

- Public External Networks

  Defined by Cloud Admin users. Cloud Users cannot create, update, or delete this type of vNet. This type of virtual network can be shared among a number of Accounts in an Exalogic vDC. vServers that are members of public external vNets also have external communication beyond the Exalogic vDC, and they can be used to host public services. A separate IP can be allocated to this type of virtual network.

- Private vNets

  Defined by Cloud Users according to their requirements and within the limits of the account quota. A private vNet is created based on the private network from the network domain of the Exalogic vDC. Private vNets are only accessible within an account. All vServers that have membership of a private vNet in common can communicate freely through that subnet.

A Cloud User defines the public external vNet or private vNets to which a vServer is assigned. Membership of a vServer to one or more vNets can only be specified at vServer creation time. Cloud Users can also reserve a number of IP addresses from any existing virtual network. Reserved IP addresses can be used later for static allocation to vServers.

When creating vServers, a Cloud User chooses one of the following methods available to allocate IP addresses to vServer:

- Static method

  This method requires a reserved IP address from each selected virtual network to the vServer. This method can be used only when creating a single vServer at a time.

- Automatic method

  This method dynamically allocates an IP address from each selected virtual network. This method is used when creating multiple vServers at a time.

A Cloud User can release a reserved IP address that is not allocated to a vServer. IP addresses dynamically allocated to vServers are released automatically when the vServers are deleted.

A vNet has the following attributes visible to Cloud Users:

- **Name** - An identifier in the system for the vNet.
- **Description** - Descriptive text for the vNet.
- **Type** - Private vNet or public external vNet.
- **Subnet** - Defines the IP address range for a vNet.

- **Allocatable Addresses** - The maximum number of IP addresses that can be allocated to vServers from a vNet.
- **Reserved Addresses** - The number of reserved IP addresses.
- **Status** - The current status of the vNet.
- **Tags** - Available tags for a vNet. Tags can be used for better identification and classification of the vNet.

Server Templates

A Server Template is an OS image in a certain format that can be used to create a vServer. Server templates are specific to processor architecture of the server pool and virtualization type. A server template is needed for creating vServers.

Server templates are loaded into the central software library associated with the Exalogic vDC and cannot be changed later. By default, a server template is bound to a specific Account. You can register a server template for public use within any Account inside the Exalogic vDC.

You can upload a new server template to be used for creating vServers. A server template has the following attributes visible to Cloud Users:

- **Name**: An identifier in the system for the server template.
- **Description**: Descriptive text for the server template.
- **Size**: Size of the server template in GB.
- **Memory**: Memory defined in GB for the server template.
- **OS**: Type of operating system defined for the server template.
- **CPUs**: The number of CPUs defined for the server template.
- **Assembly**: The name of the assembly of the server template. This field is empty because you are uploading the server template using a template sub-type file.
- **Public**: The field that indicates if the server template is shared with other Accounts in the Exalogic vDC.
- **Tags**: Available tags for a server template. Tags can be used for better identification and classification of the server template.

Virtual Storage Resources

The following types of storage resources are visible to Cloud Users in the Exalogic vDC:

- vServer Root Disks

  Root disks are created at vServer creation time based on the server template. This is the disk in which a vServer OS operates. Root disks are available after a vServer reboot, and a root disk is deleted only when a vServer is deleted.

  A vServer root disk has the following attributes visible to Cloud Users:

  vServer, Size (GB), Status, and Created By

- Volumes

A volume is a virtual block storage device that can be attached or detached from vServers. Cloud Users can attach one or more volumes to a vServer at vServer creation time or at a later time to a stopped vServer. Storage space for volumes is limited by Account's quota.Cloud Users can create an empty volume, create a volume from a snapshot, or import a volume from an HTTP server.

Volumes can be shared at volume's creation time. If a volume is shared, the volume can be attached to multiple vServers. Volumes that are not attached to any vServer can be deleted.

A volume has the following attributes visible to Cloud Users:

Name, Description, Max Size (GB), Usage Size (GB), Attached To, Share Status, Use Status, Root Volume, R/W, Created By, Status, and Tags

- Snapshots

  A snapshot is a clone of a volume at a specific time. The snapshot captures the current state of the volume and is immutable.

  Cloud Users can create a snapshot from an existing volume. They can create a volume from a snapshot and attach those volumes to vServers at vServer creation time or later time to a stopped vServer. Deletion of a volume does not influence any snapshot that has been created previously based on that volume. Snapshots exist independently of the volume.

  A snapshot has the following attributes visible to Cloud Users:

  Name, Description, Max Size (GB), Usage Size (GB), Attached To, Share Status, Use Status, Root Volume, R/W, Created By, Status, and Tags

Distribution Groups

You can place your vServers in a distribution group to ensure that no two vServers in the distribution group run on the same Oracle VM Server. Distribution groups are bound to a specific account. vServers can be assigned to a distribution group only at vServer creation time. Cloud users can create, update, or delete their distribution groups.

For more information, see the *Oracle Enterprise Manager Ops Center Feature Reference Guide* at:

http://docs.oracle.com/cd/E27363_01/doc.121/e27511/ftr_vdc_mgmt.htm

vServers

A vServer is an entity that provides the outward interface of a standalone operating system. This is a Virtual Machine. It consumes CPU and memory resources. It can be a member of one or multiple vNets. A vServer has its own identity, local storage, interfaces, and configuration that exist for the full lifetime of the vServer.

Cloud Users can create a single or multiple vServers at a time. When creating multiple vServers, only automatic IP address assignment is possible, and a suffix is added to the vServer name for each vServer. When you create a single vServer, you can assign a static IP address. In this case, a suffix is not added to the name of the vServer.

A Cloud User should make sure the following required resources exist before creating a vServer:

- A server template

- A vServer type

  Cloud users can only select a vServer type from the existing vServer types for the account. They are visible to Cloud Users during the vServer creation process. Only Cloud Admin users can create new vServer types. For more information about vServer types, see vServer Types.

- One or more virtual networks

  For more information, see Virtual Network Resources.

Depending on their specific requirements, Cloud Users can also define in advance the following resources to be used during the vServer creation process:

- Reserved IP addresses
- Distribution groups
- Volumes
- Public key

A vServer has the following attributes visible to cloud users:

Name, Description, Created By, Creation Date, Memory Size (GB), #CPUs, OS, Status, and Tags

After creating vServers, Cloud Users can manage the life cycle of vServers. For example, they can create, start, stop, and destroy vServers.

8
Monitoring the Exalogic Machine

Exalogic Control enables you to view the Exalogic machine as an appliance. You can monitor and actively manage the Exalogic hardware and fault management lifecycle. This chapter contains the following topics:

Accessing Exalogic Control BUI

You can access the Exalogic Control browser UI at the following URL:

`http://`*`ec_vm`*

`ec_vm` is the EoIB IP address of the VM hosting the Enterprise Controller component of Exalogic Control.

The request is redirected to the following https URL:

`https://`*`ec_vm`*/emoc

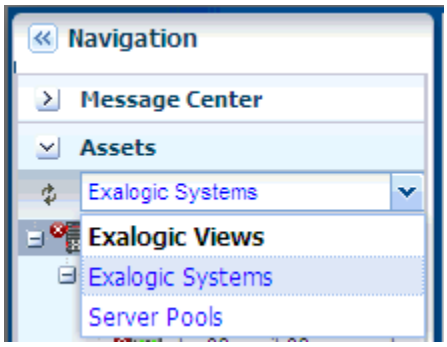
Log in as a user with the `Exalogic Systems Admin` role. For more information about this role, see Creating the Exalogic Systems Admin User.

Navigating to Exalogic Systems

After launching the Exalogic Control Browser User Interface (BUI), you can navigate to Exalogic Systems as follows:

- On the **Navigation** pane, under **Assets**, select **Exalogic Systems** from the drop-down list as follows:

Figure 8-1 Navigating to Exalogic Systems



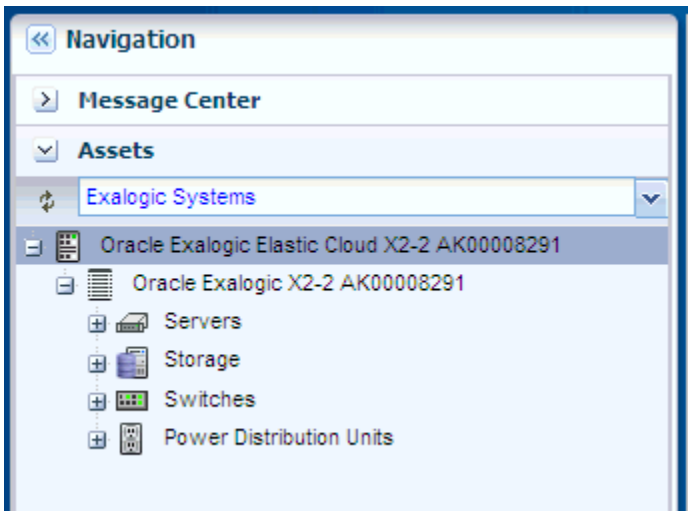
Viewing the Exalogic System

Viewing the Exalogic system details how you view the virtual Exalogic system in Exalogic Control's BUI using the four tabs on the Center pane, namely **Dashboard**, **Details**, **Controls**, and **Networks**. You can also perform relative actions by clicking the respective actions on the **Actions** pane. The actions that are allowed to be performed from the **Actions** pane are context sensitive to the selected assets on the Navigation pane. The actions are also role based, not all users will be able to perform all actions. For more information about roles, see User Profiles.

To view the Exalogic system in Exalogic Control's BUI, complete the following steps:

1. On the **Navigation** pane, under **Assets**, select **Exalogic Systems** from the drop-down list.
2. Select the Exalogic system that you want to view.

Figure 8-2 Navigating to a Specific Exalogic System



- The **Dashboard**, **Details**, **Controls**, **Networks**, and **Incidents** tabs are displayed in the Center pane.

Figure 8-3 Center Pane with Dashboard Tab Selected

3. Click each tab on the center pane to view more information:
   - **Dashboard** tab displays the summary of the Exalogic system, membership graph, and the status of the system.
   - **Details** tab displays the name of the Exalogic system, description, master subnet manager address, number of racks, compute nodes, storage nodes, switches, and PDUs present in the system.
   - **Controls** tab displays the Exalogic Control Software details such as name of the software, version number, description, name of the virtual machine, and server name.
   - **Networks** tab displays the infrastructure network table and network connectivity table.
   - **Incidents** tab displays all the incidents and alerts reported in the Exalogic System.

Viewing System Summary, Membership Graph, and Status

You can click the **Dashboard** tab on the center pane to view the following information about your Exalogic machine:

- System summary
- Membership graph
- System status

When you click the **Dashboard** tab, three sections (Summary, Membership Graph, and Status) are displayed, as shown in Figure 8-4.

Figure 8-4 Dashboard View

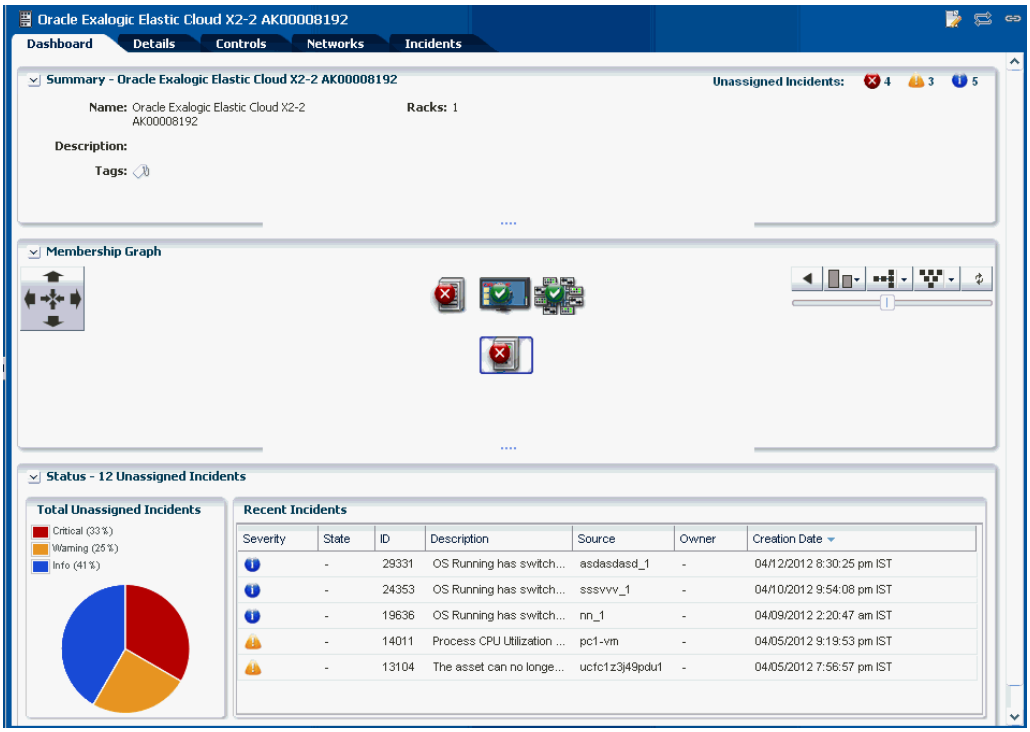


Table 8-1 Information Displayed in Dashboard View

Section	Description
Summary	The Summary section displays the name of the Exalogic system, description or name of the system identifier, number of racks that are part of the system, and also the number of unassigned incidents. The Unassigned Incidents icon in the summary pane includes incidents resulting from hardware faults. The three icons depict Critical Incidents, Warnings, and Information Incidents respectively. These incidents are from the assets that belong to all Exalogic racks.
Membership Graph	The Membership Graph pane displays the Exalogic system as a hierarchy of its components. It shows the relationship between the OVM Manager, physical InfiniBand fabric, and the hardware that is grouped in the rack. You can instantly navigate to any asset by double clicking on the asset in the membership graph. Using the controls on the top right of the graphic pane, you can change the view of the graph to either a horizontal or a vertical orientation. You can also refresh the view by clicking the Refresh icon. You can also change the graph depths or size of the images.

Table 8-1 (Cont.) Information Displayed in Dashboard View

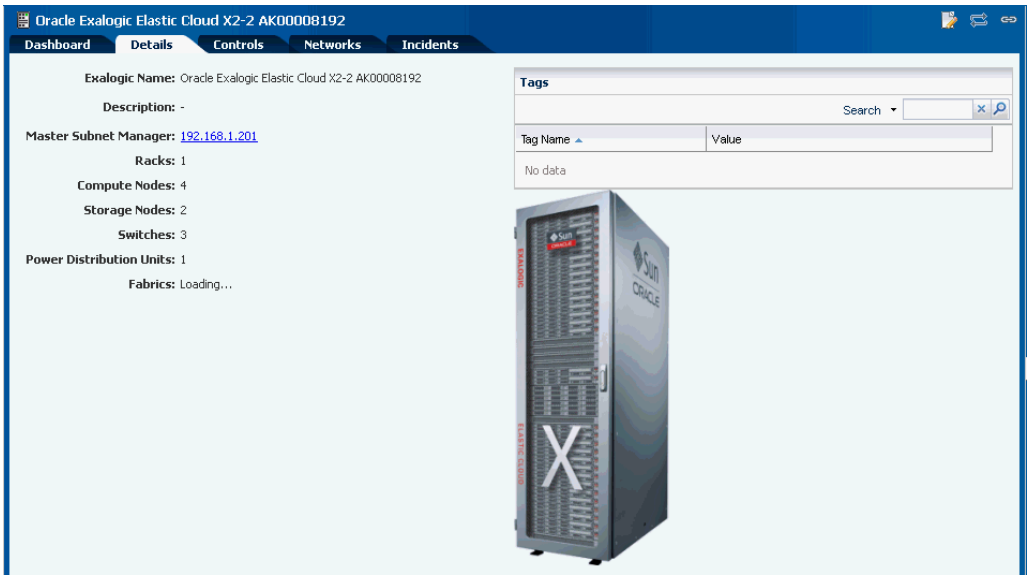
Section	Description
Status	The Status Pane displays the total unassigned incidents in chart format as well as the recent incidents encountered by the Exalogic system. In the Recent Incidents section, the following details are displayed: • Severity - displays the severity of the incident • State - displays the state of the incident • ID - displays the incident ID • Description - displays the incident description • Source - displays the source of the incident • Owner - displays the name of the owner who reported the incident • Creation Date - displays the date on which the incident was created

Viewing Exalogic System Information

You can click the **Details** tab on the center pane to view the following information about your Exalogic machine:

- Machine name
- Description
- The IP address of the IB switch on which the master subnet manager is running
- Number of racks
- Number of compute nodes
- Number of storage nodes
- Number of switches
- Number of power distribution units
- Number of fabrics

Figure 8-5 Exalogic System Information



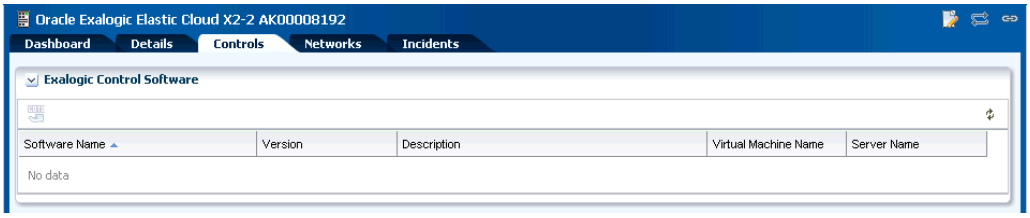
In the Tags pane, the tag names and their respective values are displayed. You can search for a particular tag using the Search feature.

Viewing Exalogic Control Information

You can click the **Controls** tab on the center pane to view the following information about Exalogic Control:

- Names and version numbers of Exalogic Control software components
- Names of virtual machines hosting Exalogic Control components
- Names of the Oracle VM Server hosting these virtual machines

Figure 8-6 Exalogic Control Information

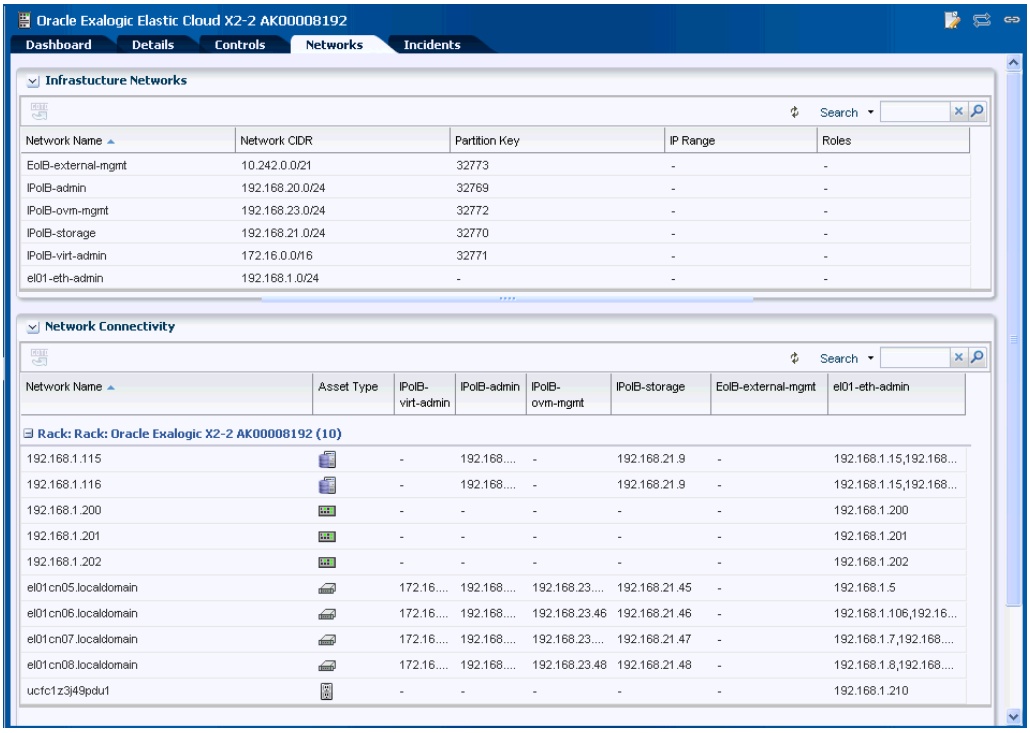


You can select any Exalogic Control component in the table and double-click to view the dashboard for each component. This table helps you identify where the Exalogic Control software components are running in your Exalogic machine. Use the **Refresh** icon on the Exalogic Control Software pane to refresh the list, when needed.

Viewing Infrastructure Networks

You can click the **Networks** tab on the center pane to view information about infrastructure networks and network connectivity.

Figure 8-7 Infrastructure Networks and Network Connectivity



The Infrastructure Networks section displays the infrastructure networks that are used in the Exalogic machine for communication between Exalogic control components, and vServers in the Exalogic vDC.

For each infrastructure network, the following information is displayed:

- **Network Name** - displays the name of the managed network.
- **Network CIDR** - displays the type of the asset.
- **Partition Key** - displays the partition of the port.
- **IP Range** - specifies the minimum and maximum boundaries of the IP addresses assigned to the network.
- **Roles** - displays the role.

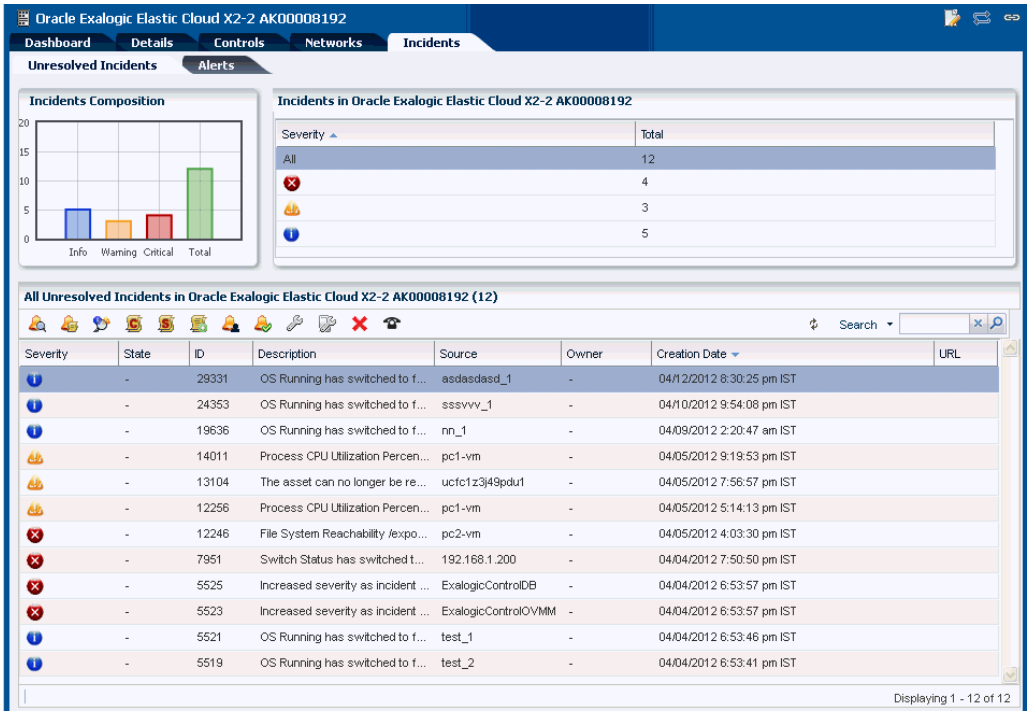
The Network Connectivity section displays the infrastructure networks with IPs assigned to the individual hardware components of Exalogic system.

- **Network Name**
- **Asset Type**

Viewing Unassigned Incidents and Alerts

You can click the **Incidents** tab on the center pane to view all unassigned incidents and alerts in your Exalogic system.

Figure 8-8 Unresolved Alerts and Incidents



In addition to viewing such alerts and incidents, you can take actions to resolve them.

Viewing the Exalogic Machine Rack

This section describes how to view the Exalogic System rack, visualization of the rack physical layout, aggregated rack components, energy data, and other rack details. As the Exalogic Systems Admin, you can drill down to an asset contained in the rack (compute node, storage node, switch, PDU) or even further.

To view the Exalogic system rack, complete the following steps:

1. On the **Navigation** pane, under **Assets**, select **Exalogic Systems**.
2. Select a rack that you want to view.

   The rack ID, description of the rack, and schematic view of assets within the rack are displayed.
3. Select one of the components of the asset in the rack and view the asset details.

For information about hardware monitoring, see the *Oracle Enterprise Manager Ops Center Feature Reference Guide*.

Viewing Photorealistic Representation of Exalogic Machine

The photorealistic view is a representation of the Exalogic physical rack, and you can see the rack layout and its components. The front and rear views of the rack are displayed in this view. All slots and the respective assets are displayed.

Each asset in the rack is represented by an image. The health status of assets, such as OK, Warning, or Critical is displayed in the form of colored lights as seen on the physical rack. The OK status is shown in green. Warning and critical statuses are shown in yellow. Hover the mouse over the slots in the rack and view information about the assets. For example, you can view slot number, asset name and description, type of asset, model number of the asset, and its health status.

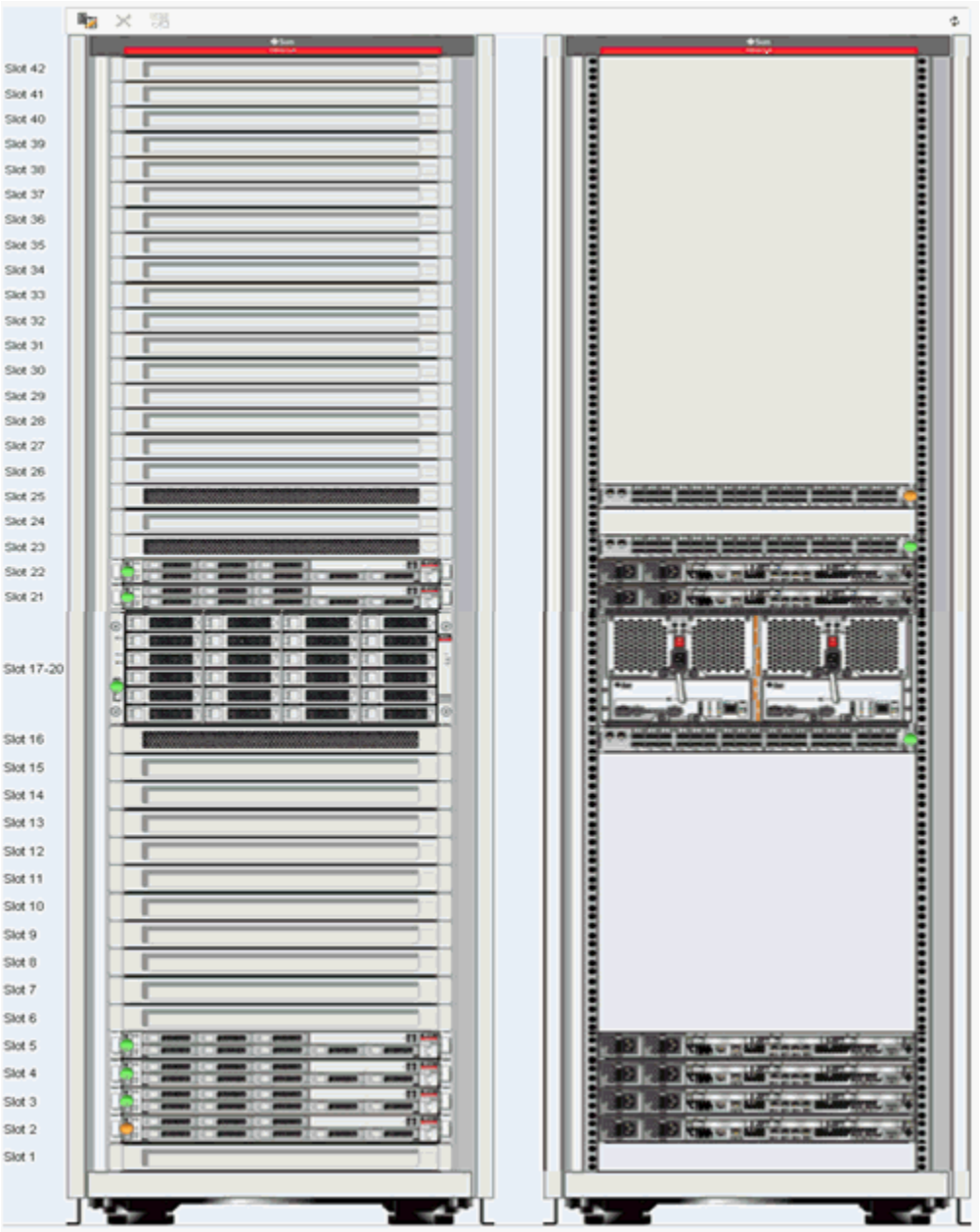
A question mark in any of the slots indicates a discrepancy from the baseline check.

To see the photorealistic view of the rack, perform the following steps:

1. On the **Navigation** pane, under **Assets**, select **Exalogic Systems**.
2. Select a rack that you want to view.
3. In the center pane, click the **Details** tab.

   A photorealistic view of the rack is displayed.

Figure 8-9 Photorealistic View of the Rack



Creating and Viewing Exalogic Reports

By using reports, you can view the Exalogic rack setup, including the asset details related to the firmware. Reports provide information about your assets, such as job history, firmware, OS updates, and problems. Reports are created in PDF and CSV formats. Reports can be exported or used to launch jobs on targeted assets.

Creating an Exalogic System Report

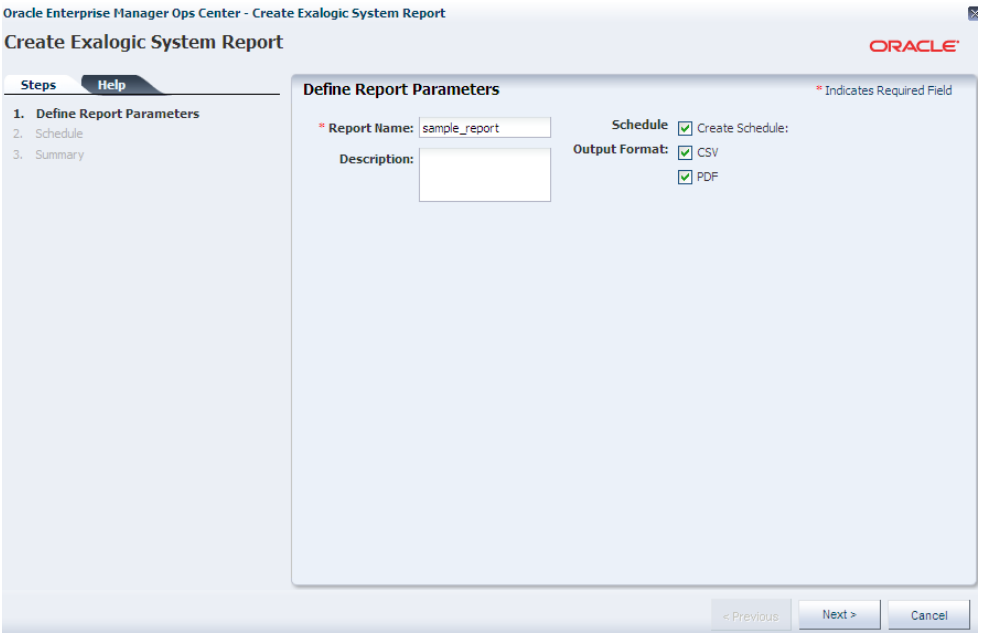
To create an Exalogic System Report in Exalogic Control, complete the following steps:

1. On the **Navigation** pane, click **Reports** > **Exalogic System Report**, as in the following:

Figure 8-10 Navigating to Exalogic System Reports

2. On the **Actions** pane, click **Create Exalogic System Report**. The Create Exalogic System Report wizard is displayed, as shown in Figure 8-11.

Figure 8-11 Create Exalogic System Report



In the **Report Name** field, enter a name. For example, enter `sample_report`.

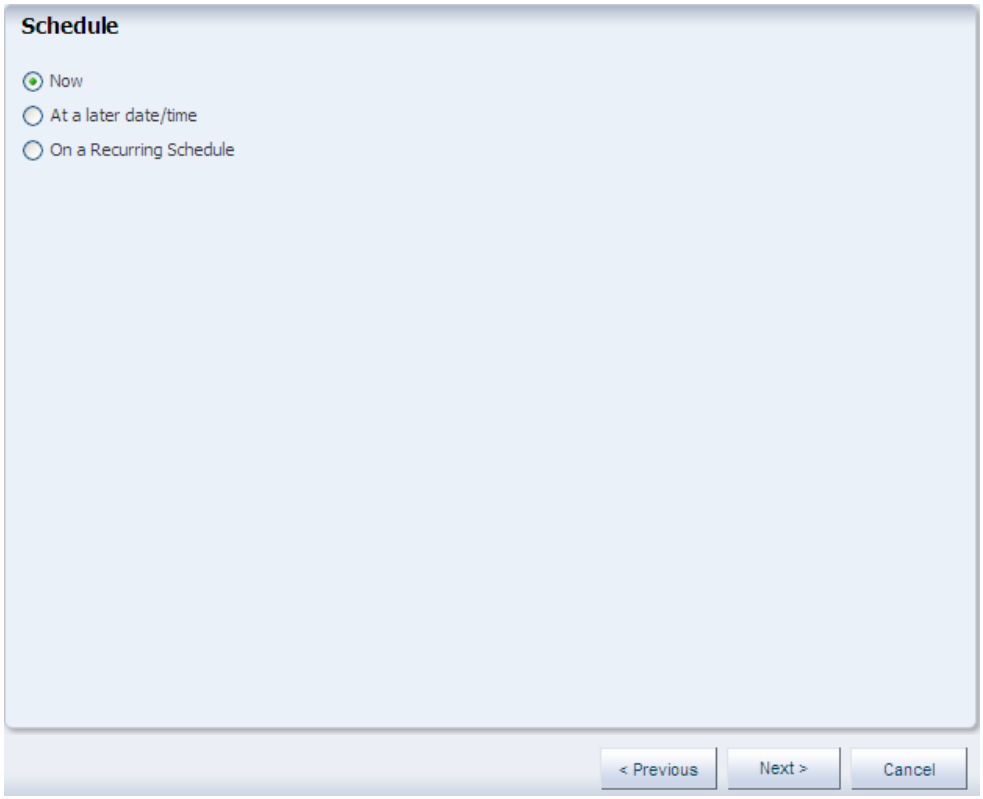
In the **Description** field, enter a short description.

Select **Create Schedule** if you want to run the report later or on a recurring schedule.

Select the output formats of the result that will be generated for the report. There is no interactive format available for this report.

3. Click **Next** to proceed. The Schedule screen is displayed, as shown in Figure 8-12.

Figure 8-12 Schedule



Set one of the following options:

- **Now** - Create the report job immediately.
- **Start Date** - Create the report job one time at a set time.
- **On a Recurring Schedule** - Create the report job routinely at a set interval. Select the Start Time, the End Time, and the Number of Hours between reports to create the intervals.

4. Click **Next**. The Summary screen is displayed.
5. Review the summary, and click **Run and Close**.

> **Note:**
>
> You can click **Save Template and Close** to save the report as a template and close the wizard. You can use the report template to generate the report later.

Viewing the Exalogic System Report

You can view existing reports. The Exalogic report contains the following sections:

- Report Parameters
- Summary Table
- System Control Software Table
- Compute Nodes Table
- Switches Table
- Storage Appliances Table
- Power Distribution Units Table
- Validation Table

Report Parameters

The Report Parameters section displays the name and model of the Exalogic system. It also displays the number of assets in the rack by their types, such as compute nodes, switches, and storage nodes in the system.

Figure 8-13 Report Parameters

Report Name: SIR01-All
Description: All Assets
Run Date: Mon Apr 09 18:49:07 EDT 2012
Report Type: Exalogic System Report

Report Parameters

Exalogic Name	Oracle Exalogic Elastic Cloud X2-2 AK00008192
Model	2.0.1.0.0
Racks	1
Compute Nodes	4
Switches	3
Storage Nodes	2

Summary Table

The Summary Table is a list of all tables in the report. It displays the number of records for each table.

Figure 8-14 Summary Table

Name of Detailed Table	Records
Virtual Datacenter Status Report	4
Rack Oracle Exalogic X2-2 AK00008192 - Compute Nodes	4
Rack Oracle Exalogic X2-2 AK00008192 - Switches	3
Rack Oracle Exalogic X2-2 AK00008192 - Storage Appliances	2
Rack Oracle Exalogic X2-2 AK00008192 - Power Distribution Units	1
Rack Oracle Exalogic X2-2 AK00008192 - Validation Table	12

System Control Software Table

The System Control Software Table lists the following:

- Exalogic Control software components
- Versions of Exalogic Control software components
- Descriptions
- Names of VMs running Exalogic Control
- Names of Oracle VM Servers hosting Exalogic Control VMs

Compute Nodes Table

The Compute Nodes Table displays the setup of the racks, such as the following:

- Type of asset
- Name of asset (compute node)
- Firmware version, such as BIOS, service processor, and HCA adapter
- Version and location of the asset in the rack

Switches Table

The Switches Table displays the name of the switch node, type of switch, firmware version, and location of the switch in the rack with the slot number where it is placed.

Storage Appliances Table

The Storage Appliances Table displays the name of the compute node, version of the service processor firmware, and the location of the appliance with the slot number where it is placed in the rack.

Power Distribution Units Table

The Power Distribution Units Table displays the PDUs and their firmware version.

Validation Table

The Validation Table displays the validation result of the rack. A baseline check is performed against the known schema for the rack. The Expected Component column in the table displays the expected component if the placed component in the slot does not match the schema when the baseline check is performed.

Figure 8-15 Validation Table

Rack: Oracle Exalogic X2-2 AK00008192 - Validation Table

Location	Type	Name	Validation Result	Expected Component
Slot 25	Switch	192.168.1.200	OK	
Slot 23	Switch	192.168.1.202	OK	
Slot 22	Storage	192.168.1.116	OK	
Slot 21	Storage	192.168.1.115	OK	
Slot 17	DiskShelf	192.168.1.15	OK	
Slot 16	Switch	192.168.1.201	OK	
Slot 5	Server	el01cn08.localdomain	OK	
Slot 4	Server	el01cn07.localdomain	OK	
Slot 3	Server	el01cn06.localdomain	OK	
Slot 2	Server	el01cn05.localdomain	OK	
-	PDU	ucfc1z3j49pdu1	OK	
-	-	-	MISSING	PDU, Oracle Rack Power Distribution Unit

9
Exalogic vDC Management: Basic Tasks

This chapter discusses how to perform basic tasks related to Exalogic Virtual Data Center (vDC) management using the browser user interface (BUI) of Exalogic Control. This chapter contains the following topics:

- Administering the Exalogic vDC and Setting Up the Infrastructure (tasks performed by a `Cloud Admin` user)
- Creating and Managing Exalogic vDC Resources (tasks performed by a `Cloud User`)

Administering the Exalogic vDC and Setting Up the Infrastructure

This section contains the following topics:

- Logging In as Cloud Admin User
- Examining the Default vDC
- Creating vServer Types
- Creating External EoIB Networks
- Specifying Managed IP Address Ranges for Networks
- Establishing Cloud Accounts
- Examining the vDC
- Verifying the vDC
- Logging Out of Exalogic Control

Logging In as Cloud Admin User

Log in to the Exalogic Control console as the `Cloud Admin` user. For more information about this user role, see Creating the Cloud Admin User.

Examining the Default vDC

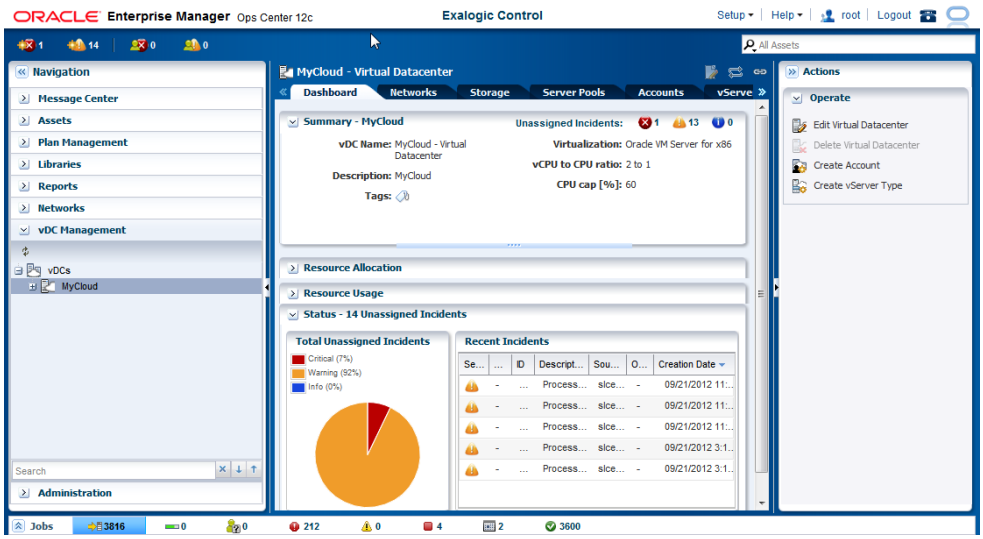
Examine the default Virtual Data Center (vDC) in your Exalogic machine by doing the following:

1. Log in to the Exalogic Control console as the `Cloud Admin` user.
2. In the navigation pane on the left, click **vDC Management**. Under vDCs, click the name of the default vDC in your Exalogic machine. The vDC dashboard is displayed.

> **Note:**
>
> An Exalogic machine has one default vDC only.

3. View the vDC dashboard, which is shown in Figure 9-1.

Figure 9-1 vDC Dashboard



4. Examine the networks in the default vDC by clicking the **Networks** tab. You can view the network configuration and network allocation by clicking **Network Configuration** and **Network Allocation** tabs, respectively.

   The Network Configuration page shows the network infrastructure, public external networks, and application-internal (private) networks in the vDC. The Network Allocation page shows the allocation of public IP addresses and virtual networks (vNets) in the vDC.

5. View the storage information by clicking **Storage** on the top navigation bar. You can view information about storage infrastructure in the vDC.

6. Examine the Oracle VM Server pools in the vDC by clicking **Server Pools** on the top navigation bar.

> **Note:**
>
> The server pools are configured in the Exalogic machine by Exalogic Control, by default.

7. Examine the default vServer types by clicking **vServer Types** on the top navigation bar. For information about creating new vServer types, see Creating vServer Types.

8. Examine incidents in the vDC by clicking the **Incidents** tab in the top navigation bar. In this tab, you can view both incidents and alerts for the entire vDC.

9. Examine any current or historical jobs by clicking the **Jobs** tab on the top navigation bar.

Creating vServer Types

Certain default, system-defined vServer types are available in the Exalogic vDC, as described in vServer Types..

Users with the `Cloud Admin` role can create additional vServer types, as follows:

1. Log in to the Exalogic Control BUI as the `Cloud Admin` user.
2. In the navigation pane on the left, click **vDC Management**. Under vDCs, click the name of your vDC. The vDC dashboard is displayed.
3. In **Actions** pane on the right, click **Create vServer Type**.

   The Create vServer Type wizard starts.
4. Enter the name, description, and tags for the new vServer type, as necessary. For example, enter `SUPER_LARGE` in the **Name** field.
5. Click **Next**.

   The Configure vServer Type screen is displayed.
6. Specify the memory and number of vCPUs in the **Memory Size (GB)** and **Number of vCPUs** fields.

   The maximum memory that you can assign to a vServer Type is the memory size of the largest compute node on the Exalogic machine, minus a small amount that is reserved for system use.

   For example, on a machine that contains *only* X2-2 nodes, the Create vServer Type wizard shows 95 GB as the maximum selectable memory, but the maximum memory that you should assign is *91 GB*. Similarly, on a machine that contains X3-2 nodes, the wizard shows 255 GB as the maximum, but you can create vServer types with memory size up to *246 GB*.

   > **Note:**
   >
   > When a vServer is created or restarted, if none of the nodes can meet the resource requirements of the vServer, the creation or restart will fail.
7. After specifying the memory size and number of vCPUs, click **Next**.

   The Summary screen is displayed.
8. Review the summary, and click **Finish**.
9. Verify the newly created vServer type by clicking the **vServer Types** tab on the top navigation pane. The newly created vServer type is listed under vServer Types.

Creating External EoIB Networks

As the `Exalogic Systems Admin`, you can create external EoIB networks to isolate public traffic for different Cloud Accounts in the Exalogic vDC.

Before creating an external EoIB network using Exalogic Control, collect the following information from your network administrator:

- IP addresses for the new network you are creating
- VLAN ID for the EoIB fabric for which you want to create a network

The following example procedure describes how to create an external EoIB network in Exalogic Control:

1. Log in to Oracle Exalogic Control BUI as the `ELAdmin` user.
2. In the navigation pane on the left, click **Networks**. Select the `default` domain on the navigation pane.
3. Click **Define Network** on the **Actions** pane.

   The Define Network wizard starts.
4. Enter the following information:
   - In the **Network IP (CIDR Format)** field, enter an IP address for the network in the Classless Inter-Domain Routing (CIDR) format. For example, enter `206.13.1.48/25`.

     > **Note:**
     >
     > A CIDR address includes the standard 32-bit IP address, and it indicates how many bits are used for the network prefix. For example, in the CIDR address `206.13.1.48/25`, the `/25` value indicates that the first 25 bits are used to identify the unique network. The remaining bits are available to identify the specific host.
     >
     > Ensure that the network you specify in the **Network IP (CIDR Format)** field is not used by another EoIB network. Do not attempt to create more than one EoIB network using the same VLAN ID.

   - In the **Gateway** field, enter the corresponding gateway address. For example, **206.13.1.100**.
   - Do not modify the default **MTU** value, which is `1500`.
   - In the **Network Name** field, enter a name. For example, `public_eoib1`.

   Click **Next**.

   The Assign Fabric screen is displayed.
5. Select the fabric named **Exalogic EoIB Fab...**.

   In the **VLAN ID** field, enter the VLAN ID for the fabric. Use the VLAN ID provided by your network administrator. If the default VLAN ID for the EoIB fabric is untagged, enter `-1`.

   Click **Next**.

   The Specify Managed Address Ranges screen is displayed.
6. Based on the IP address and subnet you specified in the step 4, specify the range of IP addresses that may be used by vServers.

   Click **+** to specify an address range and any exclusions. Define the IP address that your network administrator has provided to you. For example, enter `206.13.01.125` in the **From IP Address** field.

> **Note:**
>
> You can change the ranges even after the network is created.

After specifying the range and exclusions, click **Next**.

The Specify Static Routes screen is displayed. Do not enter or change any values.

Click **Next**.

The Specify Network Services screen is displayed.

7. If you want to access vServers associated with this network from outside the Exalogic rack using their host names, do the following:
   a. In the **DNS Domain Name** field, enter the domain name of the DNS server.
   b. In the **DNS Servers** field, enter a DNS server. If you want to add multiple DNS servers, click the plus (+) button.

> **Note:**
>
> Do not enter or change any other values.

Click **Next**.

The Summary screen is displayed.

8. Review the summary, and click **Finish**.

   After the network is created, the new external EoIB network, such as `public_eoib1`, is listed under **Networks** in the navigation pane. Verify the network by clicking its name.

Specifying Managed IP Address Ranges for Networks

To specify the IP addresses that Exalogic Control must manage for a given network, complete the following steps:

1. Log in to the Exalogic Control BUI a user with the `Exalogic Systems Admin` role.
2. In the **Networks** accordion, select the required network under the **default** domain.
3. In the **Actions** pane, click **Edit Managed IP Ranges**.

   The Edit Managed IP Address Ranges dialog box is displayed.
4. Add or remove IP addresses ranges, as required:
   - To add an IP address range, click **+** in the toolbar, and specify a range.
     - Make sure that the new IP address range is within the network. For example, if the IP address of the network is 192.168.168.0 and the netmask is 255.255.248.0, the new IP address range must be within the range 192.168.168.1–192.168.175.254.
     - If any of the IP addresses in the range is in use already, they must be excluded from the range of addresses managed by Exalogic Control.

Examples include IP addresses on `IPoIB-default` that are allocated to Exalogic hardware and software components during ECU, and EoIB IP addresses that are in use outside the Exalogic rack in the customer's data center.

To do this, click **+** in the toolbar, add the IP addresses that you want to exclude, and select the check box in the **Exclude Managed IP Range** column.

- To remove an IP address range, select the range to be removed, and click **X** in the toolbar.

5. Click **Update**.

Establishing Cloud Accounts

This section contains the following topics:

- Creating Accounts
- Adding Users to an Account
- Assigning Networks to an Account

Creating Accounts

To create an account, complete the following steps:

1. Log in to the Exalogic Control BUI as a user with the `Cloud Admin` role.
2. In the navigation pane on the left, expand **vDC Management**.
3. Under vDCs, select the name of the default vDC in your Exalogic machine and click **Accounts**.

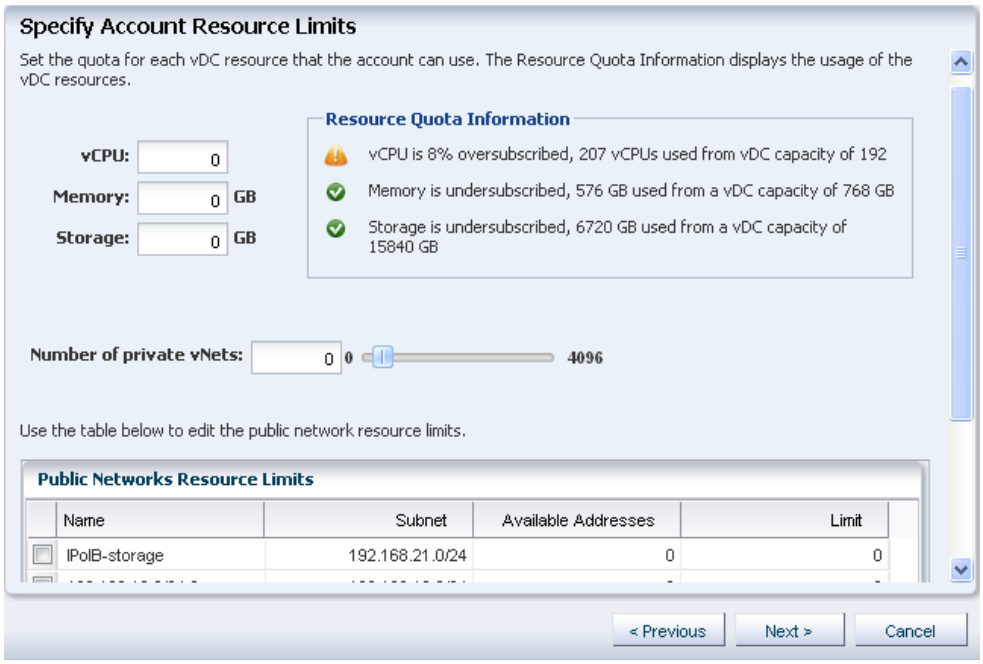
   The Accounts page is displayed.
4. Click the **+** button in the toolbar.

   The Create Account wizard starts.
5. Enter a name and description for the new account.
6. Click **Next**.

   The Specify Account Resource Limits screen is displayed.

> **Note:**
>
> Account resource limits represent the sum total of resources available to all users executing in the context of that account.

Figure 9-2 Specify Account Resource Limits



7. Enter appropriate values in the following fields:

   - **vCPU**: Enter an integer value. For example, enter `20`.
   - **Memory**: Enter a value in GB. For example, `100` GB.
   - **Storage**: Enter the storage size in GB. For example, enter `2000` GB.
   - **Number of private vNets**: Enter a numeric value from 0 to 4096 to specify the number of private vNets that the account can use. For example, enter `15`.

   > **Tip:**
   >
   > The Resource Quota Information section on the screen displays the available resources.

   - Under Public Networks Resource Limits, the public networks available in the vDC are listed.

     From the list, select the Public Networks that must be accessible by users of this account. In the **Limit** column, specify the limit that defines the number of IP addresses to be allocated from the available addresses. If you do not specify the limit, you cannot create vServers later.

> **Note:**
>
> - If guest vServers must be connected to an Exadata machine, you must assign the IPoIB-default network.
> - If guest vServers must have access to shares on the ZFS storage appliance, you must assign the IPoIB-vserver-shared-storage network.

8. Click **Next**.

   The Assign Users screen is displayed.

   A list of users with the Cloud User role is displayed. Select the Cloud Users that should be assigned to the account. For example, assign `User1`.

   > **Note:**
   >
   > You can add Cloud Users to the account even after the account creation, as described in Adding Users to an Account.

9. Click **Next**. The Summary screen is displayed.
10. Review the summary, and click **Finish** to create the account.

    The new accounts is listed under Accounts in the navigation pane on the left.

Adding Users to an Account

You can add Cloud Users to the account and give them the privileges to use the resources allocated to an account. You can add the Cloud Users while you create an account or after creating an account.

To add Cloud Users after creating the account, complete the following steps:

1. Log in to Exalogic Control as the `Cloud Admin` user.
2. In the navigation pane on the left, click **vDC Management**. Under vDCs, click the name of the default vDC in your Exalogic machine. Click **Accounts**. Alternatively, click the **Accounts** tab on the top navigation bar.

   The Accounts page is displayed.
3. Select the account, such as `Dept1`.
4. Click **Add Users** on the **Actions** pane.

   The Add Users wizard is displayed. The screen lists the available Cloud Users and already assigned Cloud Users to the account are displayed.
5. Select the users that should be assigned to the account and move them to the Assigned Users.Click **Next** to view the summary.
6. View the summary, and click **Finish** to add the user to the account.

Assigning Networks to an Account

As the `Cloud Admin` user, you can assign networks (for example, an external EoIB network) to an account, by doing the following:

1. Log in to Exalogic Control as the `Cloud Admin` user.
2. In the navigation pane on the left, click **vDC Management**. Under vDCs, click the name of the default vDC in your Exalogic machine. Select the account listed under **Accounts** in your default vDC.
3. Right-click and choose **Update Account**.

   The Update Account wizard is displayed.
4. On the Specify Account Details screen, click **Next**.

   The Specify Account Resource Limits screen is displayed.
5. On this screen, select the check box corresponding to the required network (say, an external EoIB network) from the list in the Public Networks Resource Limits section.

   In the **Limit** field, specify the number of IP addresses to be allocated from the available addresses.

   > **Note:**
   >
   > - If guest vServers must be connected to an Exadata machine, you must assign the IPoIB-default network.
   > - If guest vServers must have access to shares on the ZFS storage appliance, you must assign the IPoIB-vserver-shared-storage network.
   > - If a network does not have enough IP addresses to meet the requirements of the account, a user with the `Exalogic Systems Admin` role must first add IP address ranges to the network, as described in Specifying Managed IP Address Ranges for Networks.

   Click **Next**.

   The Summary screen is displayed.
6. Review the summary, and verify that it includes assigned networks under **Newly assigned Public networks**.
7. Click **Finish**.

Examining the vDC

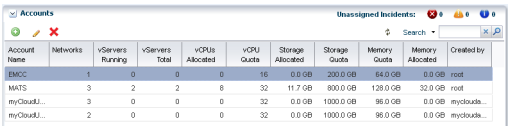
After performing the above Cloud Administration tasks, examine the Virtual Data Center (vDC) in your Exalogic machine as follows:

1. Log in to Exalogic Control as the `Cloud Admin` user.

2. In the navigation pane on the left, click **vDC Management**. Under vDCs, click the name of the default vDC in your Exalogic machine. The vDC dashboard is displayed.
3. Examine the accounts in the vDC by selecting the **Accounts** tab. You can view the newly created accounts.

   Starting from release 2.0.6.0.0 of the Exalogic Elastic Cloud Software, the Exalogic Control browser user interface displays a consolidated view of the resources—vCPUs, storage, and memory—allocated to each account, as shown in Figure 9-3.

Figure 9-3 View of Resources Allocated to Accounts



4. Examine the networks in the default vDC by clicking the **Networks** tab. You can view the network configuration and network allocation by clicking **Network Configuration** and **Network Allocation** tabs, respectively.

   The Network Configuration page shows the network infrastructure, public external networks, and application internal networks in the vDC. The Network Allocation page shows the allocation of public IP addresses and virtual networks (vNets) in the vDC.

Verifying the vDC

After Cloud Users have performed their actions, the `Cloud Admin` user can verify and monitor the new private vNets and the storage availability in the vDC. The `Cloud Admin` user can also verify the CPU, memory, and storage allocation and usage metrics.

1. Log in to Exalogic Control as the `Cloud Admin` user.
2. In the navigation pane on the left, click **vDC Management**. Under vDCs, click the name of the default vDC in your Exalogic machine.

   The Dashboard tab is displayed. The Resource Allocation section of the Dashboard tab presents graphical views of the CPU, memory, and storage resources allocated to the accounts in the vDC. The Resource Usage section shows the usage of the CPU, memory, and storage resources.
3. Examine the private vNets in the vDC by clicking the **Networks** tab on the top navigation pane. You can view all private vNets, under Application Internal Networks.
4. Examine the storage usage and availability in the vDC by clicking the **Storage** tab on the top navigation pane. You can view information about vServers' root disks, block storage, and storage allocation.

Logging Out of Exalogic Control

Log out of Exalogic Control after completing the above tasks. The `Logout` link is in the right hand top corner of the Exalogic Control BUI.

Creating and Managing Exalogic vDC Resources

This section contains the following topics:

Logging In As a Cloud User

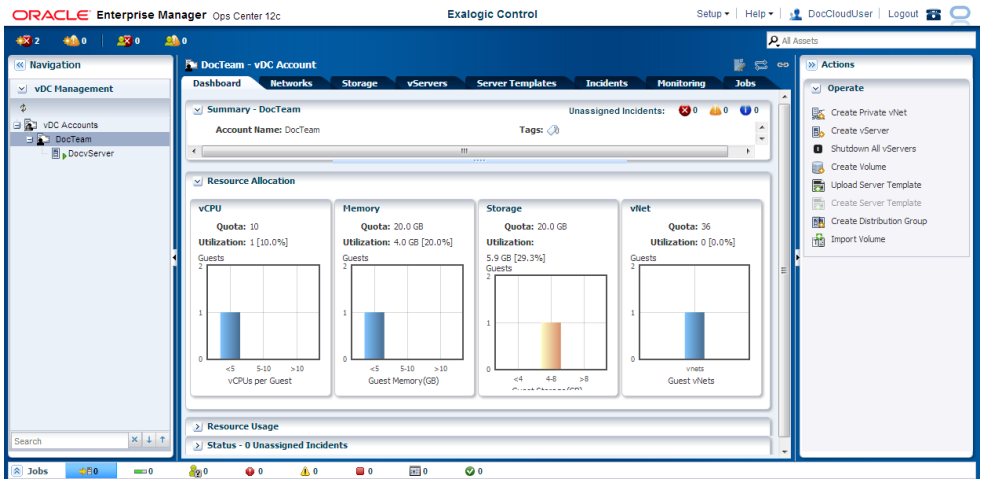
Log in to the Exalogic Control console as a Cloud User, such as `User1`, that you created in Creating the Cloud Admin User.

Examining Cloud User's Account Information

After logging in, examine your vDC account as follows:

1. Log in to the Exalogic Control console as a Cloud User.
2. In the navigation pane on the left, click **vDC Management**. Under vDC Accounts, click the name of your account, such as `Dept1`. The vDC Account dashboard is displayed.
3. View the vDC dashboard, which is shown in Figure 9-4.

Figure 9-4 vDC Account Dashboard



4. Examine the networks in your vDC account by clicking the **Networks** tab. You can view the private vNets in your Account and their resource quota and limits.
5. View the storage information by clicking **Storage** on the top navigation bar. You can view information about storage resources and quotas in your account, vServer root disks, volumes, and Snapshots.
6. Examine vServers and Distribution Groups in your account by clicking **vServers** on the top navigation bar.
7. Click **Server Templates** on the top navigation bar to examine the Server Templates available in your account.
8. Examine incidents in the account by clicking the **Incidents** tab on the top navigation bar. You can view incidents in your account and alerts.
9. Examine any current or historical jobs by clicking the **Jobs** tab on the top navigation bar.

Uploading and Registering a Server Template

Server Templates contain the configuration of an individual vServer with its virtual disk. Templates can be of the format `.tgz`, `.tar` or other file types.

You can use HTTP, HTTPS, or FTP protocols to upload Server Templates from any network, including the external EoIB network, that is available to the VM hosting the Enterprise Controller component of Exalogic Control.

You can upload a Server Template to Exalogic Control as follows:

1. Log in to the Exalogic Control as a Cloud User.
2. In the navigation pane on the left, click **vDC Management**.

   Under vDC Accounts, click the name of your account, such as `Dept1`.

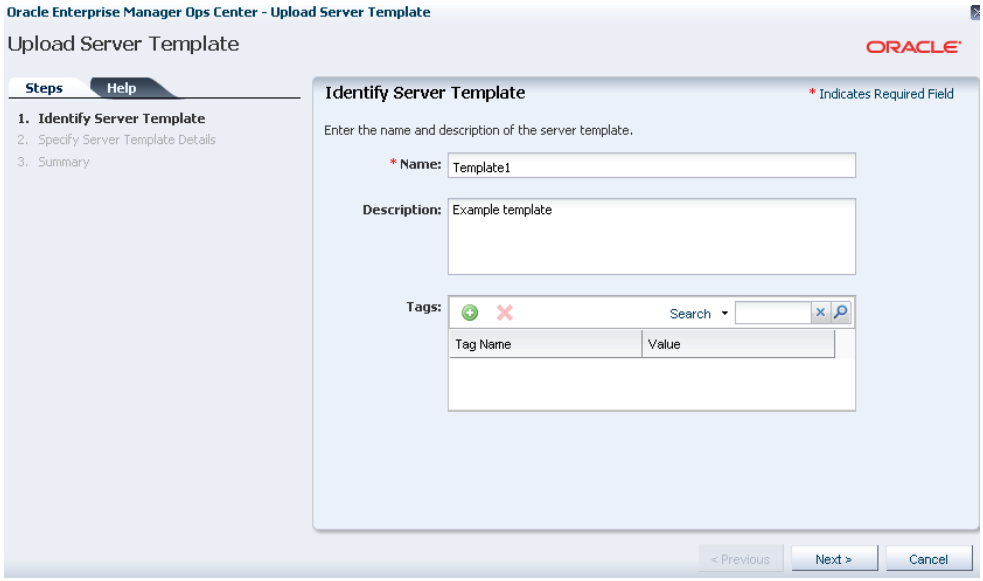
   The vDC Account dashboard is displayed.
3. Click **Server Templates** on the top navigation bar.

   The Server Templates available in your account are listed.

4. Under Server Templates, click the **Upload Server Template** icon. Alternatively, click **Upload Server Template** under **Operate** on the **Actions** pane.

   The Upload Server Template wizard is displayed, as shown in Figure 9-5.

Figure 9-5 Identify Server Template



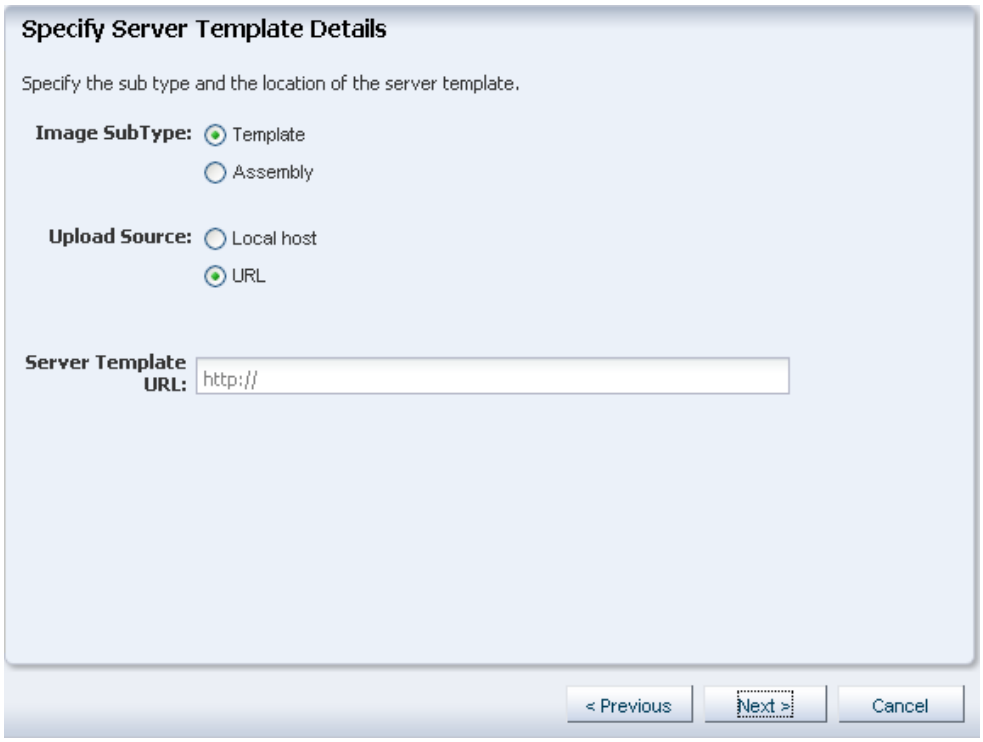
5. On the Identify Server Template screen, enter a name and description for the Server Template to be uploaded.

   You can add tags for later identification and search.

6. Click **Next**.

   The Specify Server Template Details screen is displayed, as shown in Figure 9-6.

Figure 9-6 Specify Server Template Details



7. Select the **Image SubType** option, and select **Template**.
8. Select the **Upload Source**.

   You can upload a Server Template stored on your local machine, or you can specify the URL of the location.

   To specify a URL, enter the URL in the **Server Template URL** field.

   Click **Next**.
9. Review the summary, and click **Upload** to upload the Server Template.

   The newly uploaded Server Template is listed under Server Template in the navigation pane on the left.
10. Click **Server Templates** on the top navigation bar.

    You should see the newly uploaded Server Template listed.

Making a Server Template Public

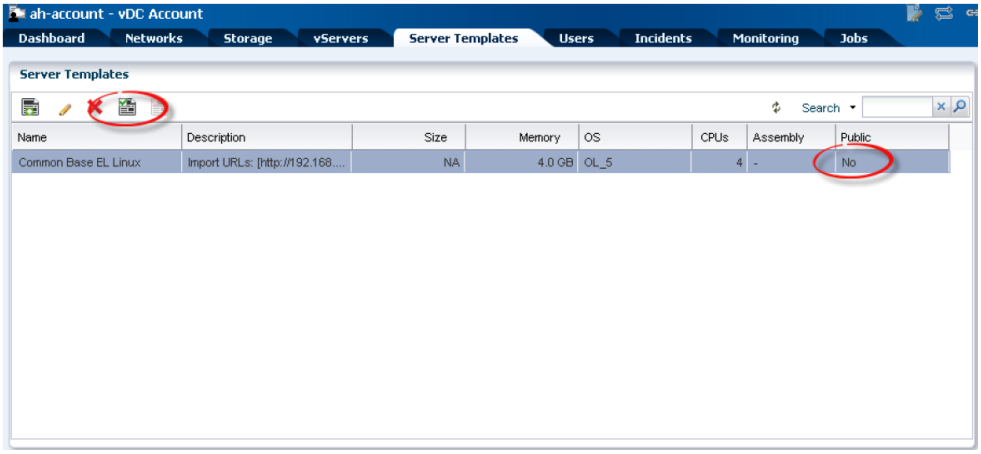
To make a server template available to all accounts in the vDC, you must make the template public. Private server templates are available to only the Cloud Users assigned to the account in which the server template was created.

After uploading a server template, complete the following steps to make it public:

1. Log in to the Exalogic Control as a Cloud User.
2. Select **vDC Management** from the Navigation pane on the left side of the page.
3. Expand **MyCloud** under **vDCs**.
4. Expand **Accounts** and select your account.

5. Click the **Server Templates** tab.
6. Click the server template you uploaded earlier, and select the **Register Server Template** icon, as highlighted in Figure 9-7.

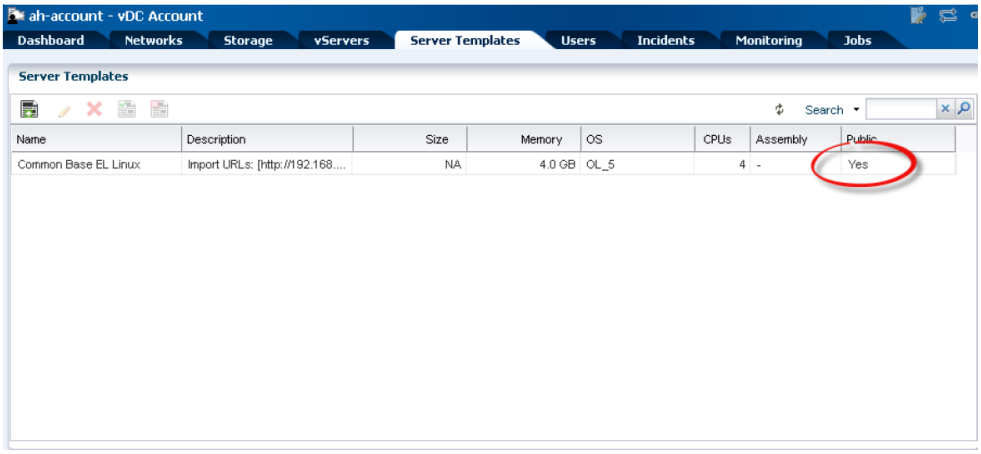
Figure 9-7 Registering a Server Template



7. Click **OK** in the confirmation screen that is displayed.

   The server template's public field will now read **Yes**, as shown in Figure 9-8.

Figure 9-8 Server Template Public Field



> **Note:**
>
> To make a public template private, select the template in the list, click the **Unregister Server Template** icon in the toolbar just above the list of templates, and follow the on-screen instructions.

Creating Private vNets

A private vNet is an IPoIB network within the Exalogic fabric that enables secure vServer-vServer communication.

You can create a private vNet in Exalogic Control as follows:

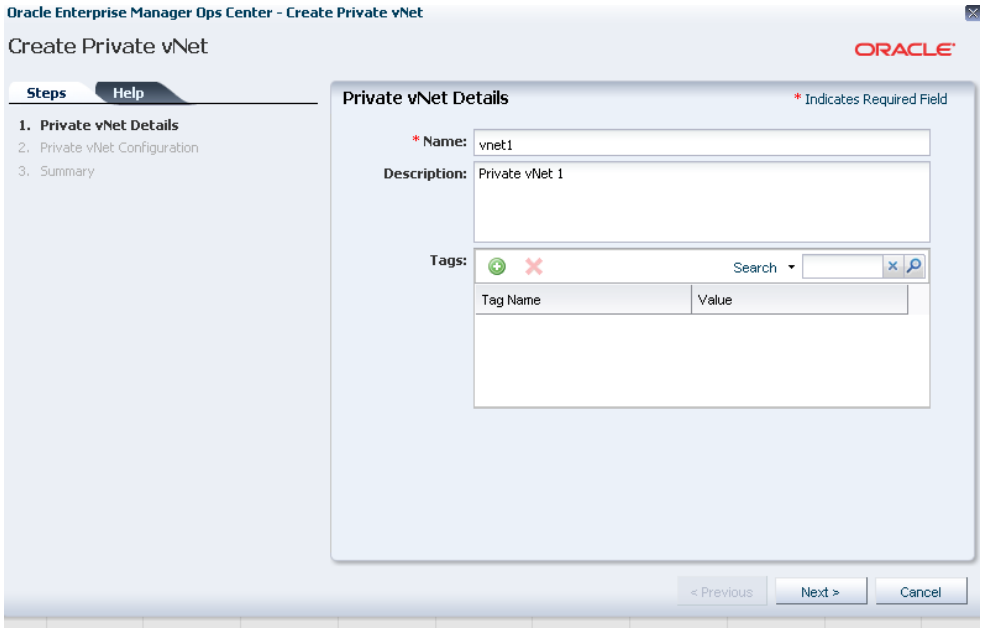
1. Log in to the Exalogic Control as a Cloud User.
2. In the navigation pane on the left, click **vDC Management**.

   Under vDC Accounts, click the name of your Account, such as `Dept1`.

   The vDC Account dashboard is displayed.
3. Click **Create Private vNet** on the Actions pane.

   The Create Private vNet wizard is displayed, as shown in Figure 9-9.

Figure 9-9 Create Private vNet Wizard



4. In the **Name** field, enter a name for the private vNet.

   For example, `vnet1`. Note that the Name field accepts a-z, A-Z, 0-9, and - characters only.
5. In the **Description** field, you can enter a description for the private vNet.
6. Click **Next**. The Private vNet Configuration screen is displayed.
7. In the **Number Of Elements** field, enter the maximum number of vServers that can be part of this vNet. Use the slide bar to set the value.

   The values entered are rounded up to the next value of 2, 6, 14, 30, 62, 126, 254, 510, 1022, 2046, 4094, and 8190. For example, enter `20`.

> **Note:**
>
> The slider on this screen gives a set of limited values only. If you enter a value not on the list, the summary displays the next highest number in the list. A private vNet uses n high order bits of the IP address range. With CIDR of 29, three bits are used, which means 8 IP addresses in the range. The highest and lowest values are reserved. Therefore, 6 IP addresses are available to the private vNet.

8. Click **Next**.

   The Summary screen is displayed.

9. Review the summary, and click **Finish** to create the private vNet.

   After a private vNet is created, you can click the **Networks** tab on the top navigation bar to verify that `vnet1` is listed in the Private vNets section.

   This private vNet can now be used by new vServers created by Cloud Users in this Account.

Creating Distribution Groups

Create a Distribution Group in Exalogic Control as follows:

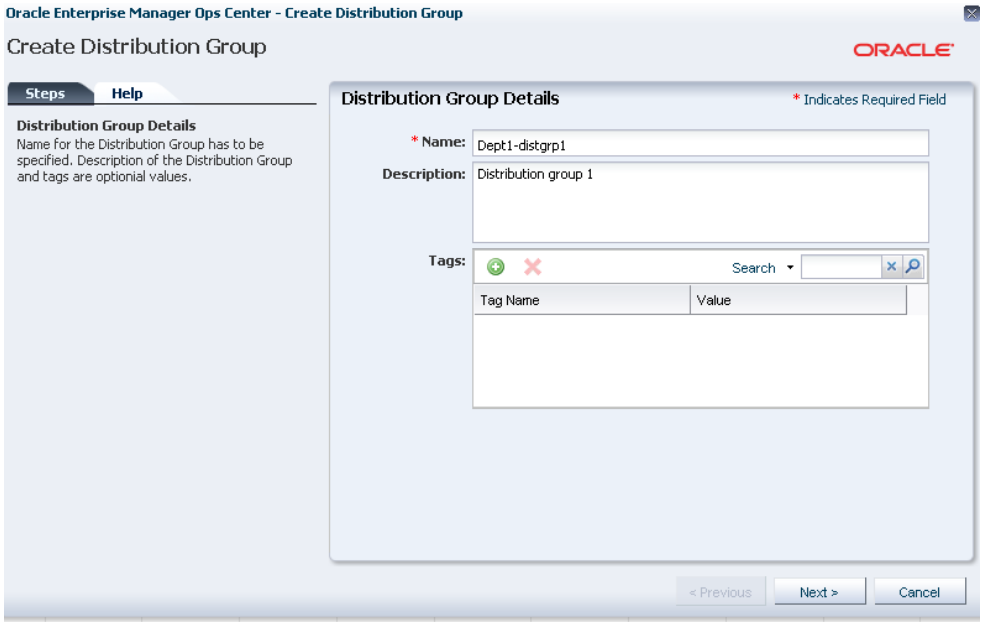
1. Log in to the Exalogic Control as a Cloud User.
2. In the navigation pane on the left, click **vDC Management**.

   Under vDC Accounts, click the name of your account, such as `Dept1`. The vDC Account dashboard is displayed.

3. Click **Create Distribution Group** on the **Actions** pane (under **Operate** on the right).

   The Create Distribution Group wizard is displayed, as shown in Figure 9-10.

Figure 9-10 Create Distribution Group Wizard



4. In the **Name** field, enter a name for the Distribution Group.

   For example, `Dept1-distgrp1`. Note that the **Name** field accepts a-z, A-Z, 0-9, and - characters only.

5. Click **Next**.

   The Distribution Group Configuration screen is displayed.

6. In the **Number of Elements** field, enter a number that defines the number of Oracle VM Servers on which the vServers can be placed.

   The size of the distribution group is limited by the actual number of Oracle VM Servers available in the server pools of the vDC. In the Exalogic vDC, the server pool is configured by Exalogic Control, by default.

7. Click **Next**.

   The Summary screen is displayed.

8. Review the summary, and click **Finish** to create the Distribution Group.

> **Note:**
>
> You cannot specify a distribution group for a set of vServers after vServer creation. For information about associating a vServer with a distribution group while creating the vServer, see step 17 in Creating vServers.

Creating Volumes

Volumes are disk images stored as virtual disks in the Oracle VM Manager repository.

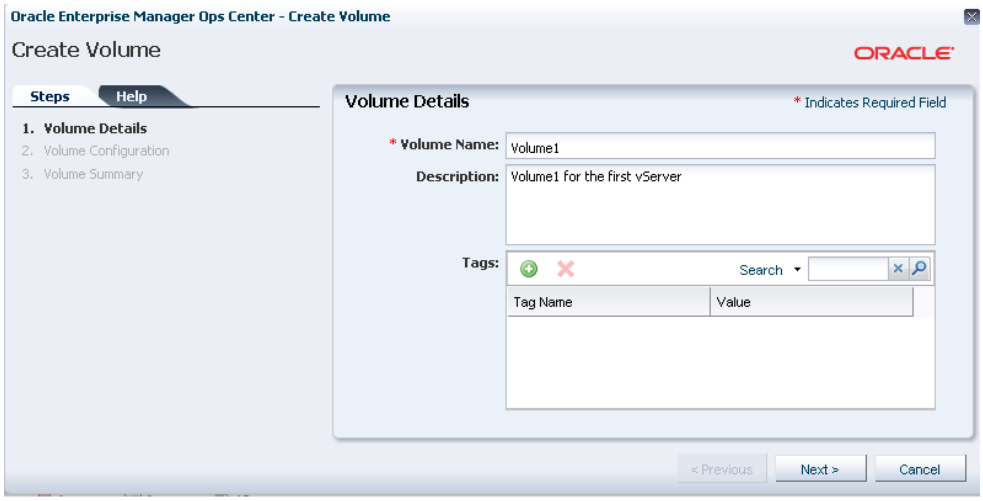
To create a volume, complete the following steps:

1. Log in to the Exalogic Control as a Cloud User.
2. In the navigation pane on the left, click **vDC Management**.

   Under vDC Accounts, click the name of your account, such as `Dept1`. The vDC Account dashboard is displayed.
3. Click **Storage** on the top navigation bar.
4. Click the **Volumes** tab.
5. Under Volumes, click the **+** icon.

   The Create Volume wizard is displayed, as shown in Figure 9-11.

Figure 9-11 Volume Details



6. In the **Volume Name** field, enter a name for the volume. For example, `Volume1`.
7. In the **Description** field, enter a short description.
8. Click **Next**.

   The Volume Configuration screen is displayed.
9. Select the **Shared** option if you wish to attach the volume to multiple vServers in the account.

   If you do not select the **Shared** option, a volume is created for one vServer to use.

> **Note:**
>
> Use shared volumes, with caution. In general, if you are going to mount one partition between multiple vServers, you should allow only one vServer to have read/write access, and use read-only for other vServers.

10. Define the size of the volume in GB.
11. Click **Next**.

    The Volume Summary screen is displayed.
12. Review the summary, and click **Finish** to create the volume in your account.

13. Repeat this procedure to create additional volumes (`Volume2`, `Volume3`, and `Volume4`).

> **Note:**
>
> After creating a volume, you must partition the volume using `fdisk` and create a file system using `mkfs` on the first vServer to which the volume is attached. On the vServer, the volume appears as a disk (`/dev/hdX` or `/dev/xvdX`). After the volume is partitioned and file system created, you must mount it using the `/etc/fstab` file on the vServer to make the filesystem accessible.
>
> For information about attaching a volume to a vServer, see Creating vServers.

Importing Volumes

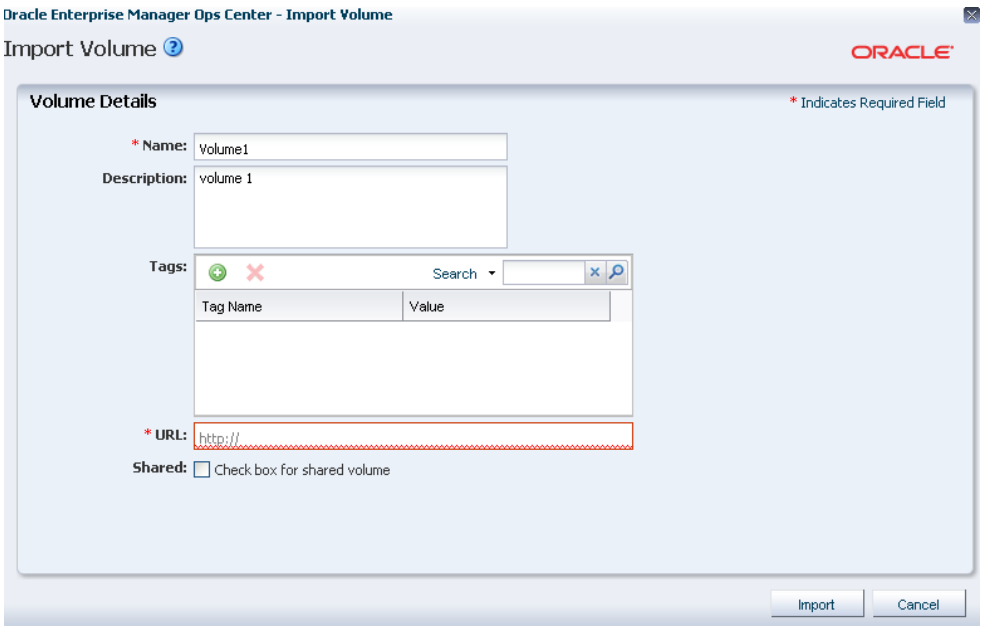
If you want to import a volume from an external URL instead of creating a volume, complete the following steps:

1. Log in to the Exalogic Control as a Cloud User.
2. In the navigation pane on the left, click **vDC Management**.

   Under vDC Accounts, click the name of your account, such as `Dept1`. The vDC Account dashboard is displayed.
3. Click **Import Volume** on the Actions pane (under Operate on the right).

   The Import Volume screen is displayed, as shown in Figure 9-12.

Figure 9-12 Import Volume



4. In the **Name** field, enter a name for the volume. For example, `Volume1`.
5. In the **Description** field, enter a short description.
6. In the **URL** field (mandatory), enter the URL from which the volume is to be imported.
7. Optional: Select the **Shared** option, which enables a volume to be used by multiple vServers in the account.
8. Click **Import** to import the volume into your account.

Creating vServers

Before you begin creating vServers, ensure that the following prerequisites are fulfilled:

- Ensure that a vDC account has been created and users assigned to it as described in Establishing Cloud Accounts.
- Ensure that the vDC account has the required network resources:
  - The required networks must be assigned to the account.
  - There must be sufficient unused IP addresses from the limit that was specified while assigning the networks to the account.

  If the network-related prerequisites are not fulfilled, the `Cloud Admin` user must update the account, as described in Assigning Networks to an Account.
- If you want to use a custom vServer Type, ensure that it has been created as described in Creating vServer Types.
- If you want to use a custom vServer template, ensure that the template has been uploaded to Exalogic Control as described in Uploading and Registering a Server Template.
- Ensure that the required private vNets have been created as described in Creating Private vNets.

To create a vServer, do the following:

> **Note:**
>
> Use only Exalogic Control for creating vServers. Unless explicitly documented, do not use Oracle VM Manager to create vServers. Creating, cloning, deleting, or modifying vServers by using Oracle VM Manager will result in unsupported configurations.

1. Log in to the Exalogic Control as a user with the `Cloud User` role.
2. In the navigation pane on the left, click **vDC Management**.

   Under vDC Accounts, click the name of your account, such as `Dept1`.

   The vDC Account dashboard is displayed.
3. Click **vServers** on the top navigation bar.

> **Note:**
>
> To be able to create vServers, both the Sun Network QDR InfiniBand Gateway switches must be running. So before proceeding, check—with your Exalogic Systems Administrator—whether both the gateway switches are running.

4. Under vServers, click the **+** icon.

   The Create vServer wizard starts.

5. In the **vServer Name** field, enter a name for the vServer to be created. For example, `vserver1`.

> **Note:**
>
> The name of a vServer need not be unique. To identify the Universally Unique Identifier (UUID) of a vServer, see the **Domain Name** field in the **Dashboard** tab of the vServer.

6. In the **Description** field, enter a brief description.
7. In the **Number of vServers** field, enter the number of vServers to be created. For example, `1`.
8. If you want to enable high availability for the vServer, leave the **High Availability Support** check box selected; otherwise, deselect it.

   For more information about how vServer high availability works, see Managing High Availability of vServers.

9. Click **Next**.

   The Server Template Selection screen is displayed.

10. Select one of the available Server Templates that you uploaded in Uploading and Registering a Server Template.
11. Click **Next**.

    The vServer Type Selection screen is displayed.

12. Select a vServer Type and click **Next**.

    The Attach Volumes screen is displayed.

13. Attach additional volumes, if required, to the vServer by selecting an available volume and clicking the right arrow. For example, attach `Volume1`.
14. Click **Next**.

    The vNet Selection screen is displayed.

15. If you want to associate the vServer with one or more networks available for the account, select from the available networks.

    After selecting the required networks, click **Next**.

> **Note:**
>
> - The networks to which you want to associate the vServer must be assigned (by a `Cloud Admin` user) to the account and the required IP addresses must be provisioned, as described in Assigning Networks to an Account.
> - If the vServer must have access to shares on the ZFS storage appliance, you must select the `IPoIB-vserver-shared-storage` network and also (later) perform the procedure described in Setting Up Access to the ZFS Storage Appliance for a vServer.
> - If you associate the vServer with two or more EoIB networks, then, for enabling access to the vServer from outside the machine through all the EoIB interfaces, you must configure advanced routing on the vServer, by using (for example) iproute2 or dynamic routing.

The Assign IP Address screen is displayed because you are creating a single vServer. If you chose to create multiple vServers by specifying the number of vServers, the IP address assignment is skipped. All IP addresses are allocated automatically.

16. Select an IP address allocation method: **static IP**, or **automatic**. If you select **static IP**, select the required IP address in the **IP Address** field. If you select **automatic**, you do not need to enter an IP address; it is selected from IP addresses available for the network.

> **Note:**
>
> If you select the static IP address option, ensure that you have allocated IP addresses for the network. For more information, see Allocating Virtual IPs for an Account

After assigning an IP address, click **Next**.

The Distribution Group Selection screen is displayed.

17. If necessary, select one of the available distribution groups in which the new vServer should be placed. Note that you cannot assign a vServer to a distribution group *after* creating the vServer.

    Click **Next**.

    The vServer Access screen is displayed.

18. If required, set up access for the vServer by specifying the path to the public key file. Alternatively, enter the public key in the **Public Key** field.

19. Click **Next**.

    The Summary screen is displayed.

20. Review the summary screen, and click **Finish** to create the vServer (`vserver1`).

> **Note:**
>
> If a Create-vServer job is taking a long time, wait till the job either fails or is completed. *Do not* stop the job. If the job fails, *do not* run it again. Attempting to stop a job or run it again can corrupt the system, making it difficult to diagnose and recover.

21. Set the MTU to 64000 for each InfiniBand interface:
    a. Log in to the vServer using SSH as the `root` user.
    b. Verify the current MTU for `bond2` by running the `ifconfig` command.

> **Note:**
>
> The steps in this procedure use `bond2` as an example. This procedure should be repeated for all the InfiniBand interfaces.

```
# ifconfig bond2
bond2     Link encap:InfiniBand  HWaddr
80:58:08:CA:FE:80:00:00:00:00:00:00:00:00:00:00:00:00:00:00
inet addr:192.168.1.12  Bcast:192.168.1.255  Mask:255.255.255.0
UP BROADCAST RUNNING MASTER MULTICAST  MTU:1500  Metric:1
RX packets:9 errors:0 dropped:0 overruns:0 frame:0
TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:504 (504.0 b)  TX bytes:420 (420.0 b)
```

    c. Append the line `MTU=64000` to the `ifcfg` file corresponding to the `bond2` interface:

```
# echo MTU=64000 >> /etc/sysconfig/network-scripts/ifcfg-bond2
```

    d. Verify whether the `MTU=64000` line was added to the `ifcfg-bond2` file:

```
# cat /etc/sysconfig/network-scripts/ifcfg-bond2 | grep MTU
MTU=64000
```

    e. Find the slave interfaces for `bond2`:

```
# cd /etc/sysconfig/network-scripts
# grep "MASTER=bond2" ifcfg-* | awk -F":" '{print $1}'
ifcfg-ib0.8009
ifcfg-ib1.8009
```

    f. Set the mode to `connected` for both the slave interfaces of the `bond2` interface:

```
# echo connected > /sys/class/net/ib0.8009/mode
# echo connected > /sys/class/net/ib1.8009/mode
```

    g. Perform steps 21.b through 21.f for the other InfiniBand interfaces.
    h. Stop and start the vServer as described in Stopping vServers and Starting vServers.
    i. After the vServer starts, log in again to the vServer using SSH as the `root` user.

j. Run the `ifconfig` command for each InfiniBand interface, and verify that the output of the command displays `MTU:64000`, as shown in the following example for `bond2` and its slave interfaces:

```
# ifconfig bond2 | grep MTU
UP BROADCAST RUNNING MASTER MULTICAST  MTU:64000  Metric:1

# ifconfig ib0.8009 | grep MTU
UP BROADCAST RUNNING SLAVE MULTICAST  MTU:64000  Metric:1

# ifconfig ib1.8009 | grep MTU
UP BROADCAST RUNNING SLAVE MULTICAST  MTU:64000  Metric:1
```

Stopping vServers

To stop a vServer, do the following:

> **Note:**
>
> Do not use the `xm destroy` command or Oracle VM Manager to stop a vServer. Use only Exalogic Control.

1. Log in to the Exalogic Control as a Cloud User.
2. From the navigation pane on the left, click **vDC Management**.
3. Under vDCs, expand your cloud such as `MyCloud`.
4. Expand **Accounts**.
5. Expand the name of your account, such as `Dept1`. All the vServers in the account are displayed.
6. Select the **vServer** you wish to stop. The dashboard of the vServer is displayed.
7. From the actions pane on the right, click **Stop vServer**. Wait till the job succeeds in the jobs pane.

Starting vServers

To start a vServer, do the following:

> **Note:**
>
> Do not use the `xm create` command or Oracle VM Manager to start a vServer. Use only Exalogic Control.

1. Log in to the Exalogic Control as a Cloud User.
2. From the navigation pane on the left, click **vDC Management**.
3. Expand your cloud, such as `MyCloud`.
4. Expand **Accounts**.

5. Expand the name of your account, such as `Dept1`.

   All the vServers in the account are displayed.

6. Select the **vServer** you wish to start.

   The dashboard of the vServer is displayed.

7. From the actions pane on the right, click **Start vServer**. Wait till the job succeeds in the jobs pane.

Managing High Availability of vServers

This section describes how high availability (HA) for guest vServers works and can be managed in a vDC running on Exalogic. In this context, HA is the ability to automatically restart vServers that may be affected by an unexpected outage such as a vServer crash or a compute node failure. This feature is available starting from release 2.0.4.0.0 of the Exalogic Elastic Cloud Software.

> **Note:**
>
> Currently, high availability for Exalogic Control VMs is not supported. For information about restoring failed Exalogic Control VMs, contact Oracle Support.

This section contains the following topics:

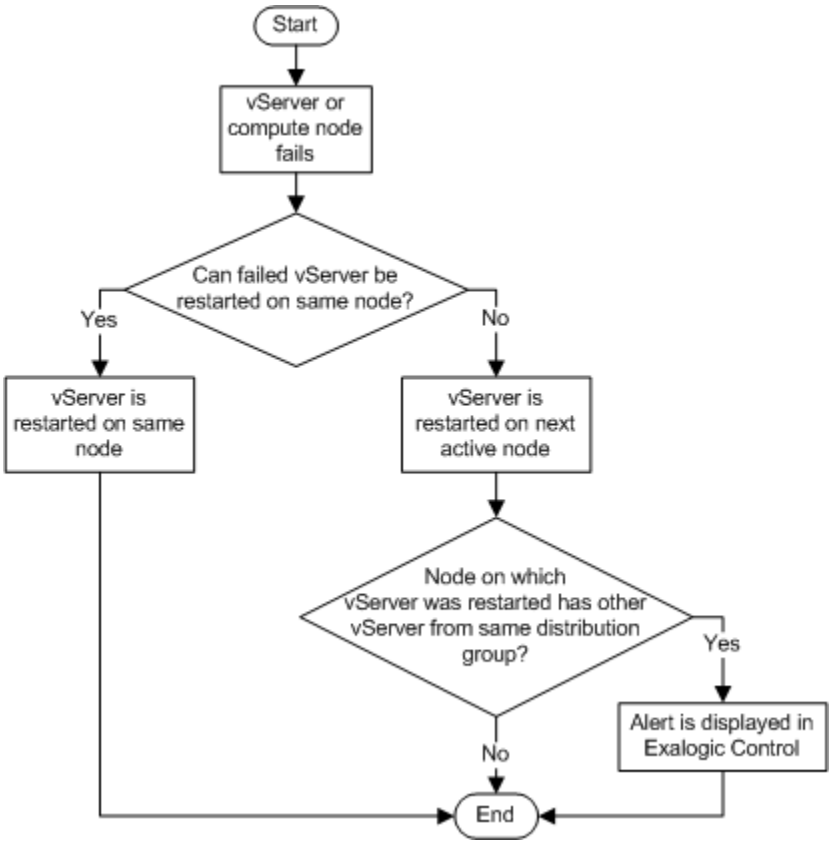
- How High Availability Works for Guest vServers
- Enabling and Disabling High Availability for Guest vServers

How High Availability Works for Guest vServers

Figure 9-13 is a flowchart depicting how the vServer HA feature works.

> **Note:**
>
> You must ensure that there are sufficient CPU and memory resources on compute nodes in the vDC for a successful migration of the vServers affected by an unexpected outage. If none of the compute nodes has sufficient resources, the failed vServer is not migrated.

Figure 9-13 Guest vServer High-Availability Process



Description of the HA Flow for Guest vServers

1. If an HA-enabled vServer crashes, the failed vServer is restarted automatically on the same compute node.

   However, if the compute node on which the vServer was originally running has failed or does not have enough resources, the vServer is started on the next active compute node in the same server pool. Note that, if there are no active compute nodes in the server pool, the failed vServer is not started.

2. If the compute node on which a failed vServer is restarted already hosts any vServer that belongs to the same distribution group as that of the restarted vServer, an alert is displayed for the account to which the distribution group belongs in the Incidents tab of Exalogic Control.

   To resolve this distribution-group violation, the `Cloud User` should stop the vServer and then start it again as described in Stopping vServers and Starting vServers. The vServer is then restarted on a compute node that does not host any vServer from the same distribution group. If such a compute node is not available, the vServer is not started.

Enabling and Disabling High Availability for Guest vServers

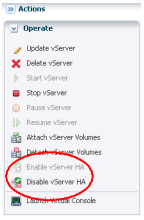
HA for guest vServers is enabled by default when the vServers are created. If the vServers fail, they are automatically restarted on the same compute node, or migrated

to a different compute node if the original node is down, as described in How High Availability Works for Guest vServers.

If required, the `Cloud User` can, while creating vServers, disable HA, as described in Creating vServers.

Migration of vServers to a different compute node (if the original node is down) can be disabled and re-enabled by `Cloud Users` by using the **Disable vServer HA** and **Enable vServer HA** actions in Exalogic Control, as shown in Figure 9-14.

- **Figure 9-14 Enabling and Disabling HA for Guest vServers**



> **Note:**
>
> The state of the **Enable vServer HA** or **Disable vServer HA** items in the Actions pane indicates whether HA is currently enabled for a vServer. If **Enable vServer HA** is clickable, then HA is currently disabled for the vServer. If **Disable vServer HA** is clickable, then HA is currently enabled for the vServer. In addition, in the vServers tab of any account, you can view the HA state of a vServer by clicking the **Status** icon corresponding to the vServer.

Viewing Networks Attached to a vServer

To view all the networks of a vServer, do the following:

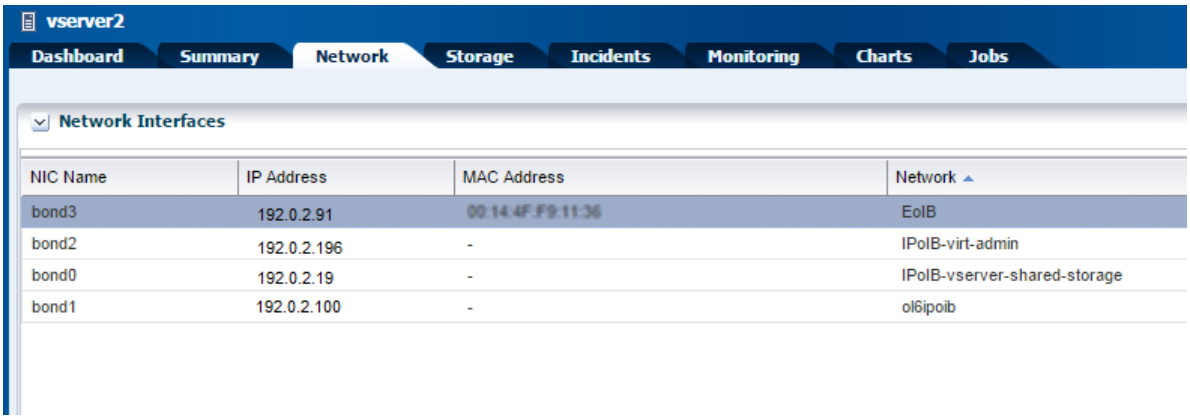
1. In the navigation pane on the left, click **vDC Management**.
2. Under vDC Accounts, expand the name of your account, such as `Dept1`.

   All the vServers in the account are displayed.
3. Select the **vServer** (for example, `vserver2`) for which you wish to view attached networks.

   The `vserver2` dashboard is displayed.
4. Click the **Network** tab.

   The list of networks of vServer is displayed.

Figure 9-15 vServer Networks



Viewing Volumes Attached to a vServer

To view the volumes attached to a vServer, do the following:

1. In the navigation pane on the left, click **vDC Management**.
2. Under vDC Accounts, expand the name of your account, such as `Dept1`.

   All the vServers in the account are displayed.
3. Select the **vServer** (for example, `vserver2`) for which you wish to view attached volumes.

   The `vserver2` dashboard is displayed.
4. Click the **Storage** tab.
5. Click the **Volumes** tab.

   The list of volumes attached to the vServer is displayed.

Attaching Volumes to a vServer

You can attach a volume to a vServer as follows:

1. Log in to the Exalogic Control as a Cloud User.
2. In the navigation pane on the left, click **vDC Management**.
3. Under vDC Accounts, expand the name of your account, such as `Dept1`. All the vServers in the account are displayed.
4. Select the **vServer** (for example, `vserver2`) to which you wish to attach a volume. The `vserver2` dashboard is displayed.
5. From the actions pane on the right, click **Stop vServer**. Wait till the job succeeds in the jobs pane.
6. From the actions pane on the right, click **Attach vServer Volumes**. The Attach vServer Volumes wizard is displayed.
7. Select the volume you wish to attach to `vserver2`.
8. Click the right arrow icon.
9. Click **Next**. The confirmation screen is displayed.

10. Click **Finish**. Wait till the job succeeds in the jobs pane.
11. From the actions pane on the right, click the **Start vServer** button to restart the vServer.

Detaching Volumes from a vServer

You can detach a volume from a vServer as follows:

1. Log in to the Exalogic Control as a Cloud User.
2. In the navigation pane on the left, click **vDC Management**.
3. Under vDC Accounts, expand the name of your account, such as `Dept1`. All the vServers in the account are displayed.
4. Select the **vServer** (for example, `vserver2`) from which you wish to detach a volume. The `vserver2` dashboard is displayed.
5. From the actions pane on the right, click **Stop vServer**. Wait till the job succeeds in the jobs pane.
6. From the actions pane on the right, click **Detach vServer Volumes**. The Detach vServer Volumes wizard is displayed.
7. Select the volume you wish to detach from `vserver2`.
8. Click the right arrow icon.
9. Click **Next**. The confirmation screen is displayed.
10. Click **Finish**. Wait till the job succeeds in the jobs pane.
11. From the actions pane on the right, click the **Start vServer** button to restart the vServer.

Creating a Snapshot from a Volume

This section describes how to create a snapshot from a volume attached to a vServer. It contains the following topics:

- Creating a Snapshot from a Volume (EECS 2.0.4.x.x or Earlier)
- Creating a Snapshot from a Volume (EECS 2.0.6.x.x)

Creating a Snapshot from a Volume (EECS 2.0.4.x.x or Earlier)

In EECS release 2.0.4.x.x (or earlier), you can create a snapshot from a volume attached to a vServer, as follows:

1. Log in to the Exalogic Control as a Cloud User.
2. From the navigation pane on the left, click **vDC Management**. Under vDC Accounts, click the name of your account, such as `Dept1`.

   The vDC Account dashboard is displayed.
3. Click **vServers** on the top navigation bar.
4. Under vServers, select a running vServer and click the **Stop vServer** icon (red icon) to stop the vServer.

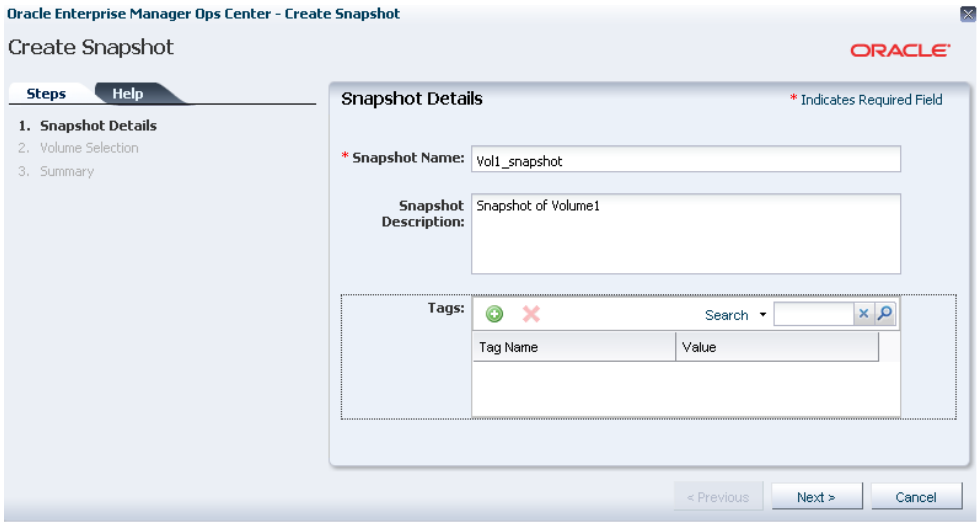
5. From the navigation pane on the left, click **vDC Management**. Under vDC Accounts, click the name of your account, such as `Dept1`.

   The vDC Account dashboard is displayed.

6. Click **Create Snapshot** on the **Actions** pane (under **Operate** on the right).

   The Create Snapshot wizard is displayed, as shown in Figure 9-16.

Figure 9-16 Snapshot Details



7. In the **Snapshot Name** field, enter a name. For example, enter `Vol1_snapshot`.
8. In the **Snapshot Description** field, enter a brief description.
9. Click **Next**.

   The Volume Selection screen is displayed.

10. Select the volume for which you want to take a snapshot. For example, select `Volume1`.

    Note that the time taken to create a snapshot can vary depending on the size of the volume.

11. Click **Next**.

    The Summary screen is displayed.

12. Review the summary, and click **Finish** to create a snapshot.
13. From the navigation pane on the left, click **vDC Management**. Under vDC Accounts, click the name of your account, such as `Dept1`.

    The vDC Account dashboard is displayed.

14. Click **vServers** on the top navigation bar.
15. Under vServers, select the previously stopped vServer and click the **Start vServer** icon (green arrow) to restart the vServer.

Creating a Snapshot from a Volume (EECS 2.0.6.x.x)

In EECS 2.0.6.x.x, you can create a snapshot from a volume attached to a vServer, as follows:

1. Log in to the Exalogic Control as a Cloud User.
2. From the navigation pane on the left, click **vDC Management**.
3. Under vDC Accounts, click the name of your account, such as `Dept1`.

   The vDC Account dashboard is displayed.
4. Click **vServers** on the top navigation bar.
5. Under vServers, select a running vServer and click the **Stop vServer** icon (red icon) to stop the vServer.
6. From the navigation pane on the left, click **vDC Management**. Under vDC Accounts, click the name of your account, such as `Dept1`.

   The vDC Account dashboard is displayed.
7. Click **Storage** on the top navigation bar.
8. Click the **Volumes** subtab.
9. Select the volume for which you want to take a snapshot. For example, select `Volume1`.

   Note that the time taken to create a snapshot can vary depending on the size of the volume.
10. Click the **Launch Create Snapshot Wizard** button.

    The Create Snapshot wizard appears.
11. In the **Snapshot Name** field, enter a name. For example, enter `Vol1_snapshot`.
12. In the **Snapshot Description** field, enter a brief description.
13. Click **Create**.

    The snapshot is created.
14. From the navigation pane on the left, click **vDC Management**. Under vDC Accounts, click the name of your account, such as `Dept1`.

    The vDC Account dashboard is displayed.
15. Click **vServers** on the top navigation bar.
16. Under vServers, select the previously stopped vServer and click the **Start vServer** icon (green arrow) to restart the vServer.

Creating a Volume from a Snapshot

To create a volume from a snapshot, complete the following steps:

1. Log in to the Exalogic Control as a Cloud User.
2. In the navigation pane on the left, click **vDC Management**. Under vDC Accounts, click the name of your account, such as `Dept1`. The vDC Account dashboard is displayed.
3. Click **Storage** on the top navigation bar.
4. Click the **Snapshots** tab.
5. Click the **Create Volume from a Snapshot** icon (this icon is below the Snapshots section title). The Create Volume from a Snapshot wizard is displayed.
6. In the **Volume Name** field, enter a name for the volume.

7. In the **Volume Description** field, enter a brief description.
8. Click **Next**. The Snapshot Selection screen is displayed.
9. Select a snapshot for which you want to create a volume. For example, select `Vol1_snapshot`.

   Note that the time taken to create a volume can vary depending on the size of the snapshot.
10. Click **Next**. The Summary screen is displayed.
11. Review the summary, and click **Finish** to create a volume.

Logging Out of Exalogic Control

After completing the above tasks, log out of Exalogic Control. The `Logout` link is in the right hand top corner of the Exalogic Control BUI.

10

Exalogic vDC Management: Advanced Tasks

This chapter discusses how to perform advanced tasks related to Exalogic Virtual Data Center (vDC) management using the browser user interface (BUI) of Exalogic Control. You can perform these tasks after completing the management tasks described in Exalogic vDC Management: Basic Tasks.
This chapter contains the following sections:

- Managing the Exalogic vDC Infrastructure
- Managing Account Resources

Managing the Exalogic vDC Infrastructure

This section describes how to complete the following tasks:

- Logging In as Cloud Admin User
- Updating an Account
- Deleting an Account
- Removing a Cloud User from an Account
- Configuring CPU Oversubscription
- Making an OVS Node Unavailable for vServer Placement
- Changing Passwords for Components on the Exalogic Machine

Before you can perform these tasks, you must have completed the Cloud Admin tasks, as described in Administering the Exalogic vDC and Setting Up the Infrastructure.

Logging In as Cloud Admin User

Log in to the Exalogic Control console as the `CloudAdmin` user.

For more information about creating this user role, see Creating the Cloud Admin User.

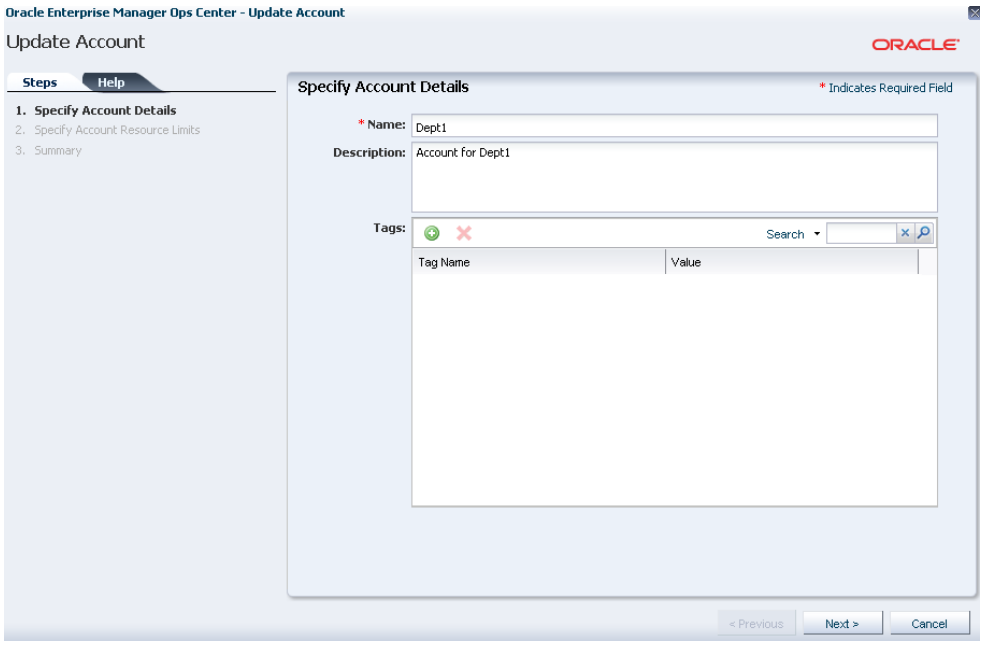
Updating an Account

To update an account, complete the following steps:

1. Log in to the Exalogic Control console as the `CloudAdmin` user.
2. In the navigation pane on the left, click **vDC Management**. Under vDCs, click the name of the default Exalogic vDC (`MyCloud`).
3. Expand **Accounts** under **MyCloud**. The accounts in the vDC are listed.
4. To update an account (for example, `Dept1`), select `Dept1` listed under **Accounts** in the navigation pane on the left.

5. Click **Update Account** on the **Actions** pane. The Update Account wizard is displayed, as shown in Figure 10-1.

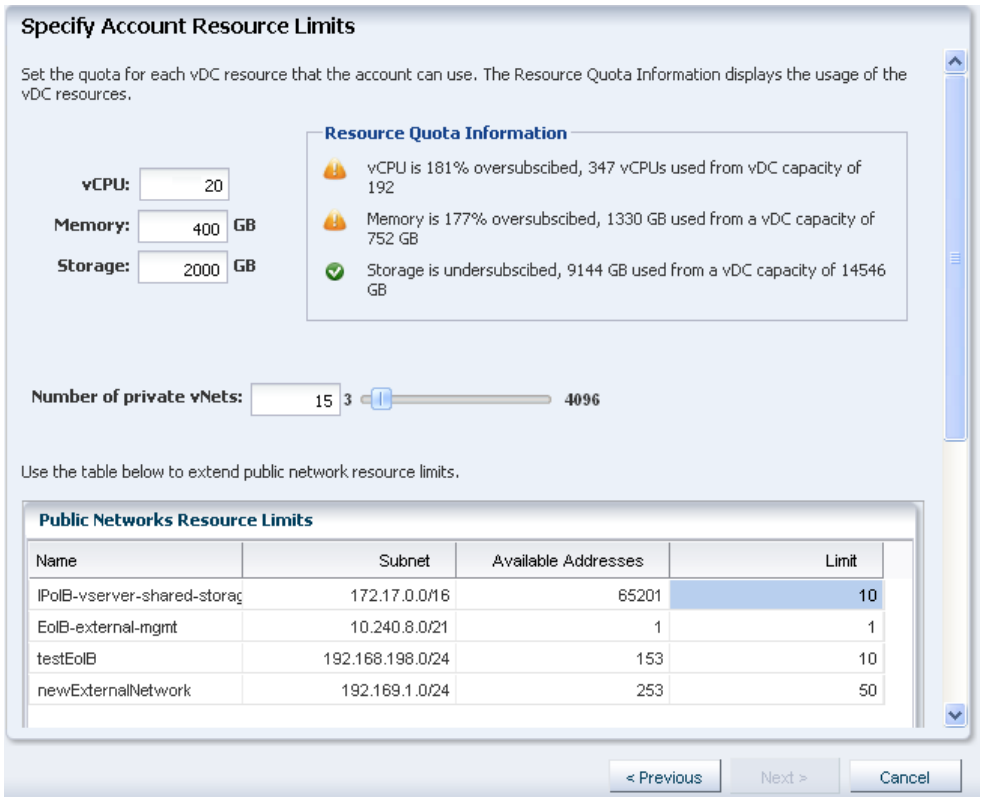
Figure 10-1 Specify Account Details



6. Click **Next**.

   The Specify Account Resource Limits screen is displayed, as shown in Figure 10-2.

Figure 10-2 Specify Account Resource Limits



In this screen, you can update resource limits in `Dept1`. For example, change the Memory limit from `100` GB to `400` GB.

7. After updating the values, click **Next**.

   The Summary screen is displayed.

8. Review the summary, and click **Finish**.

Deleting an Account

To delete an account, complete the following steps:

1. Log in to the Exalogic Control console as the `CloudAdmin` user.
2. In the navigation pane on the left, click **vDC Management**. Under vDCs, click the name of the default Exalogic vDC (`MyCloud`).
3. Expand **Accounts** under **MyCloud**. The accounts in the Exalogic vDC are listed.
4. To delete an account (for example, `Dept1`), select `Dept1` listed under **Accounts** in the navigation pane on the left.

> **Note:**
>
> Deleting an account removes all resources in the account, such as Server Templates, volumes, vServers, and private vNets. When you try to delete an account that has running vServers, the following message is displayed:
>
> `You cannot delete this account because there are virtual servers in running state. Shut down all the virtual servers to delete the account.`

5. Click **Delete Account** on the **Actions** pane. The Delete Account screen is displayed, as shown in Figure 10-3.

Figure 10-3 Delete Account

6. To delete the `Dept1` account, click **Delete**.

Removing a Cloud User from an Account

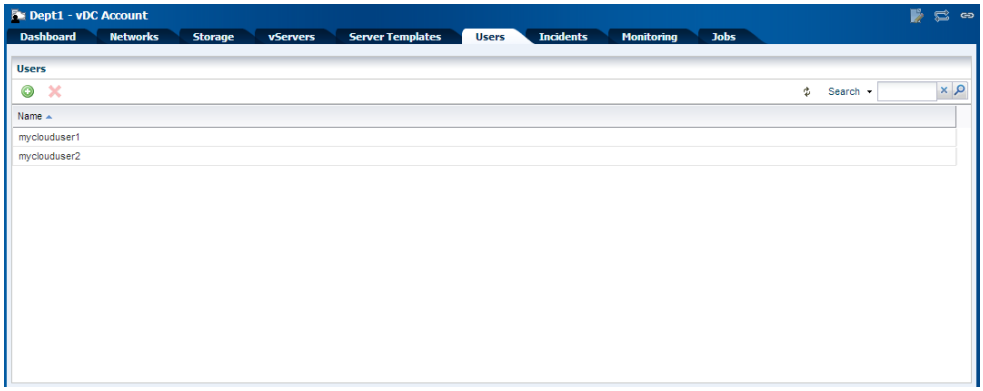
An Account needs at least one Cloud User. You cannot remove a Cloud User from an account, which has a single Cloud User associated.

To remove a Cloud User from an account with multiple Cloud Users, complete the following steps:

1. Log in to the Exalogic Control console as the `CloudAdmin` user.
2. In the navigation pane on the left, click **vDC Management**. Under vDCs, click the name of the default Exalogic vDC (`MyCloud`).
3. Expand **Accounts** under **MyCloud**. The accounts in the Exalogic vDC are listed.
4. To remove a Cloud User from an account (for example, `mycloduser1` assigned to `Dept1`), select `Dept1` listed under **Accounts** in the navigation pane on the left. The `Dept1` account dashboard is displayed.

5. In the `Dept1` dashboard, click the **Users** tab. A list of the Cloud Users assigned to the `Dept1` Account is displayed as shown in Figure 10-4.

Figure 10-4 List of Cloud Users Assigned to an Account



6. Select a Cloud User (for example, `mycloduser1`), and click the **X** icon (**Launch Delete User Wizard**). The Remove User from Account screen is displayed.
7. Click **Remove** to remove the user (`mycloduser1`).

Configuring CPU Oversubscription

This section contains the following topics:

- Overview of CPU Oversubscription
- Configuring the CPU subscription Ratio and CPU Consumption Limit
- Example Scenarios for CPU Oversubscription

Overview of CPU Oversubscription

In an Exalogic vDC, the underlying CPU hardware resources of the machine are allocated to the vServers in the form of vCPUs. By default, each vCPU consumes one CPU hardware thread.

For example, each Sun Fire X4170 M2 compute node on an Exalogic X2-2 machine consists of two 6-core sockets—that is, 12 cores per compute node. Each core supports two hardware threads. So a single X2-2 compute node can support 24 vCPUs—one vCPU per hardware thread—in the default configuration.

To improve hardware utilization and to facilitate denser consolidation of applications, starting with the Exalogic Elastic Cloud Software release 2.0.4.0.0, the Exalogic vDC can be configured to support more vCPUs than the available CPU threads—that is, the CPU resources can be oversubscribed.

- `Cloud Admin` users can enable CPU oversubscription by increasing the vCPU-to-physical-CPU-threads ratio. For example, in a vDC that is based on a standard Exalogic X2-2 machine, when the vCPU-to-physical-CPU-threads ratio is increased from the default 1:1 to 2:1, the number of vCPUs available on each Sun Fire X4170 M2 compute node on an Exalogic X2-2 machine increases from 24 to 48. Table 10-1 shows the number of vCPUs available in the vDC at various vCPU-to-physical-CPU-threads ratios.

Table 10-1 Number of vCPUs at Different vCPU-to-Physical-CPU-threads Ratios

vCPU-to-Physical-CPU-threads Ratio	X2-2 Full	X2-2 1/2	X2-2 1/4	X2-2 1/8
1:1 – CPU oversubscription not enabled	720	384	192	96
2:1	1440	768	384	192
3:1	2160	1152	576	288

Configuring the CPU subscription Ratio and CPU Consumption Limit

To enable CPU oversubscription, run the following steps:

1. Log in to Exalogic control as the `Cloud Admin`.
2. From the navigation pane on the left, select **vDC Management**.
3. Expand **vDCs** and select the vDC you want to modify.
4. From the actions pane on the right, select **Edit Virtual Datacenter**.

   The Edit Virtual Datacenter wizard is displayed.
5. You can use the initial screens of the Edit Virtual Datacenter wizard to change the name, description, and tags of the vDC. If you do not want to change any of these settings, click **Next** till the Specify vCPU Sizing screen is displayed.
6. In the **vCPU to Physical CPU Threads Ratio** field, enter the maximum number of virtual CPUs that can share each physical CPU thread. Decimal values can be entered.

   For example, if the **vCPU to Physical CPU Threads Ratio** field is set to 2, each virtual CPU will receive at least 50% of the cycles of a physical CPU thread.

   > **Note:**
   >
   > As the CPU oversubscription ratio increases, performance may be affected, but the utilization of CPU resources improves. The CPU oversubscription ratio that you might want to use is at most 3:1. At extremely high ratios, the risk of instability of the system increases.
   >
   > For racks hosting production vServers, CPU oversubscription must be 1:1 to avoid performance issues.
7. Do not modify the **CPU Cap** from its default value of 100%.

   > **Note:**
   >
   > CPU Cap feature is deprecated.
8. Click **Next**.

   The Edit Volume Storage screen is displayed. If required, select more storage resources to allocate to the vDC from the list; otherwise proceed to the next step.
9. Click **Next**.

The Summary screen is displayed.

10. Review the updated settings of the vDC and click **Finish**.

Example Scenarios for CPU Oversubscription

This section describes the following example scenarios:

- Scenario 1: Increasing the Number of vCPUs in a New VDC
- Scenario 2: Increasing the Number of vCPUs in a Running, Fully Subscribed VDC
- Scenario 3: Increasing the Number of vCPUs in a Running, Oversubscribed VDC
- Scenario 4: Decreasing the Number of vCPUs in a Running, Oversubscribed VDC

Scenario 1: Increasing the Number of vCPUs in a New VDC

- An Exalogic X2-2 full rack is set up as a virtual datacenter.
- At the default vCPU-to-physical-CPU-threads ratio of 1:1, 720 vCPUs (24 x 30) are available in the vDC.
- The `Cloud Admin` determines that more than 720 vCPUs are required to support the workloads planned for the vDC.

In this scenario, the `Cloud Admin` can increase the number of vCPUs available in the vDC, by enabling CPU oversubscription. For example, the `Cloud Admin` can increase the number of vCPUs available in the vDC to 1440 (**2** x 24 x 30), by increasing the vCPU-to-physical-CPU ratio to **2**:1, as described in Configuring CPU Oversubscription.

Scenario 2: Increasing the Number of vCPUs in a Running, Fully Subscribed VDC

- An Exalogic X2-2 full rack is set up as a virtual datacenter.
- At the default vCPU-to-physical-CPU-threads ratio of 1:1, 720 vCPUs (24 x 30) are available in the vDC.
- The vCPU quotas of the accounts in the vDC are fully allocated to the vServers created by the cloud users assigned to the accounts.
- The memory and storage quotas of the accounts in the vDCs are not yet fully allocated to vServers.
- `Cloud Users` want to create more vServers, but cannot do so because the vCPU quota is fully allocated.

In this scenario, the `Cloud Admin` can allow `Cloud Users` to create more vServers, by enabling CPU oversubscription. For example, the `Cloud Admin` can increase the number of vCPUs available in the vDC to 1440 (**2** x 24 x 30), by increasing the vCPU-to-physical-CPU ratio to **2**:1, as described in Configuring CPU Oversubscription. Then, the `Cloud Admin` can increase the vCPU quota of the accounts in the vDC to enable creation of additional vServers.

Scenario 3: Increasing the Number of vCPUs in a Running, Oversubscribed VDC

- An Exalogic X2-2 full rack is set up as a virtual datacenter.

- CPU oversubscription has been enabled and the oversubscription ratio is currently at **2**:1—that is, 1440 vCPUs (**2** x 24 x 30) are available in the vDC.
- The vCPU quotas of the accounts in the vDC are fully allocated to the vServers created by the cloud users assigned to the accounts.
- The memory and storage quotas of the accounts in the vDCs are not yet fully allocated to vServers.
- `Cloud Users` want to create more vServers, but cannot do so because the vCPU quota is fully allocated.

In this scenario, the `Cloud Admin` can allow `Cloud Users` to create more vServers, by increasing the CPU oversubscription ratio further. For example, the `Cloud Admin` can increase the number of vCPUs available in the vDC to 2160 (**3** x 24 x 30), by increasing the vCPU-to-physical-CPU ratio to **3**:1, as described in Configuring CPU Oversubscription. Then, the `Cloud Admin` can increase the vCPU quota of the accounts in the vDC to enable creation of additional vServers.

Scenario 4: Decreasing the Number of vCPUs in a Running, Oversubscribed VDC

- An Exalogic X2-2 full rack is set up as a virtual datacenter.
- CPU oversubscription has been enabled and the ratio is currently at **3**:1—that is, 2160 vCPUs (**3** x 24 x 30) are available in the vDC.
- Only 1000 of the available 2160 vCPUs are being used by vServers.
- The `Cloud Admin` decides that an oversubscription ratio of 2:1 would suffice for this vDC.

In this scenario, the `Cloud Admin` can decrease the number of vCPUs available in the vDC to 1440 (**2** x 24 x 30), by decreasing the vCPU-to-physical-CPU ratio to **2**:1.

> **Note:**
>
> In any of the CPU oversubscription scenarios described earlier, to ensure that application performance across the vDC remains predictable, the `Cloud Admin` must keep the CPU Cap at 100% and not recommend to change. Note that the CPU Cap feature is deprecated.

Making an OVS Node Unavailable for vServer Placement

In certain situations, you may want to make an OVS node unavailable for vServer placement. For example, when you want to perform maintenance on a compute node.

To make an OVS node unavailable for vServer placement, you must perform the following tasks:

Task 1: Identify and Tag the OVS Node with vserver_placement.ignore_node=true

Task 2: Migrate the vServers on the Tagged OVS Node to Other Available OVS Nodes

Task 3 (optional): Place the OVS Node in Maintenance Mode

Task 1: Identify and Tag the OVS Node with vserver_placement.ignore_node=true

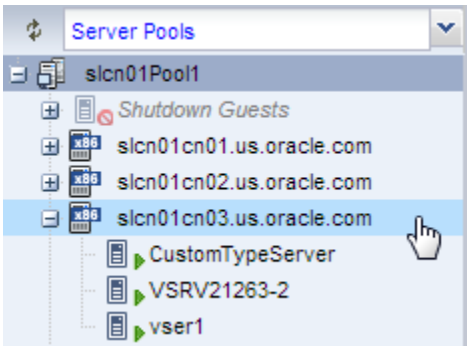
1. Identify the OVS node that you want to make unavailable for vServer placement.
2. Tag the OVS node with `vserver_placement.ignore_node=true` by doing the following:
   a. Log in to Exalogic Control as the `ELAdmin` user.
   b. From the navigation pane on the left, click **Assets**.
   c. Under **Assets**, from the drop-down list, select **Server Pools**, as shown in the following screenshot:

Figure 10-5 Exalogic Views List

A list of the OVS nodes is displayed.

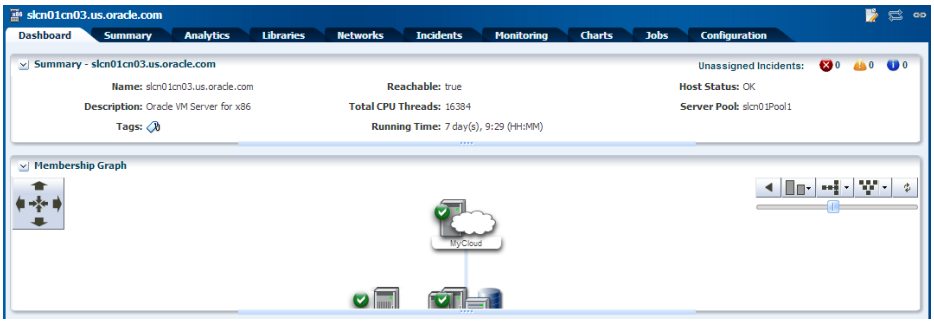
   d. Select the OVS node you identified in step 1, as shown in the following screenshot:

Figure 10-6 Select the OVS Node



The OVS node dashboard is displayed as shown in the following screenshot:

Figure 10-7 OVS Node Dashboard



e. Click the **Summary** tab.

f. From the Actions pane on the right, click **Edit Tags**.

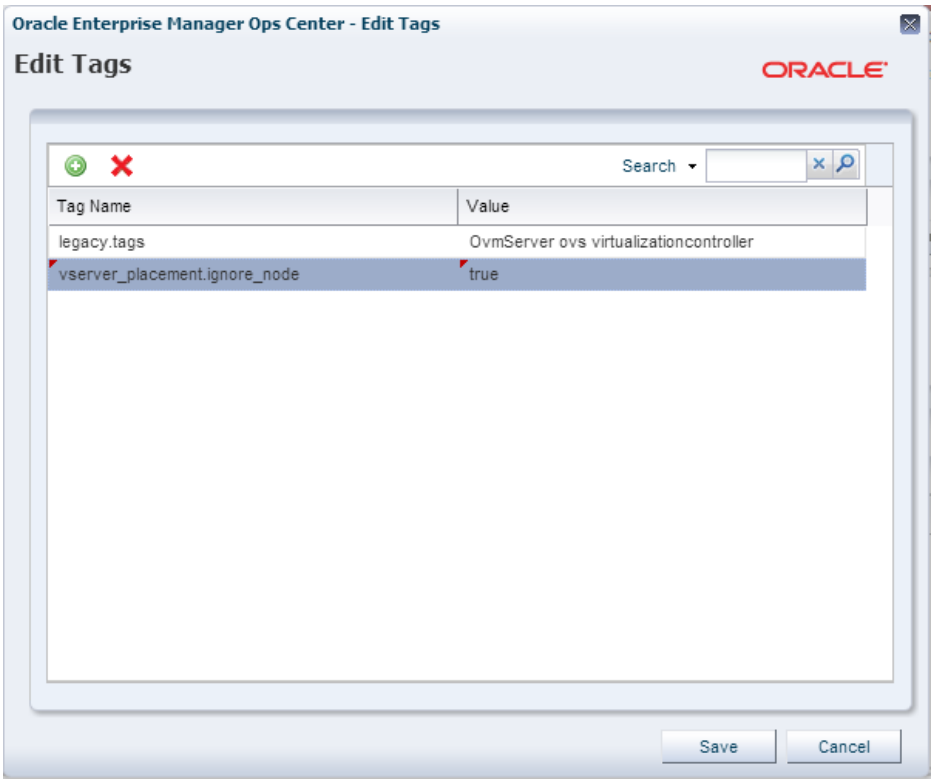
The Edit Tags dialog box is displayed.

g. Click the plus (+) button.

h. Enter `vserver_placement.ignore_node` as the Tag Name.

i. Enter `true` as the Value. The following screenshot shows the Edit Tags dialog box after adding the `vserver_placement.ignore_node=true` tag:

Figure 10-8 Edit Tags Dialog Box



j. Click the Save button. Once the job is complete, the tag should be visible in the **Summary** tab under the Tags table. Any new vServers that you create will

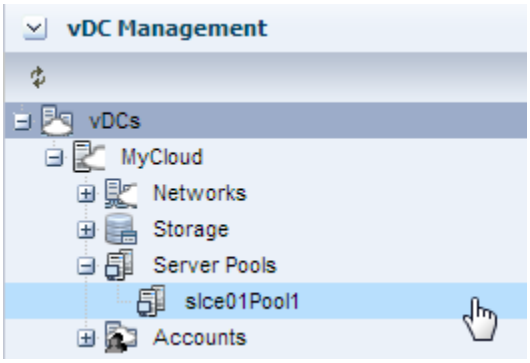
be placed on nodes other than ones tagged with `vserver_placement.ignore_node=true`.

> **Note:**
>
> To make the OVS node available for placement again, either delete the tag or set the value of the `vserver_placement.ignore_node` tag to false.

Task 2: Migrate the vServers on the Tagged OVS Node to Other Available OVS Nodes

1. Identify the vServers running on the tagged OVS node by doing the following:
   a. Log in to Exalogic Control as a user with the `Cloud Admin` role.
   b. From the navigation pane on the left, click **vDC Management**.
   c. Expand **vDCs**.
   d. Expand **MyCloud**.
   e. Expand **Server Pools**.
   f. Click your server pool as shown in the following screenshot:

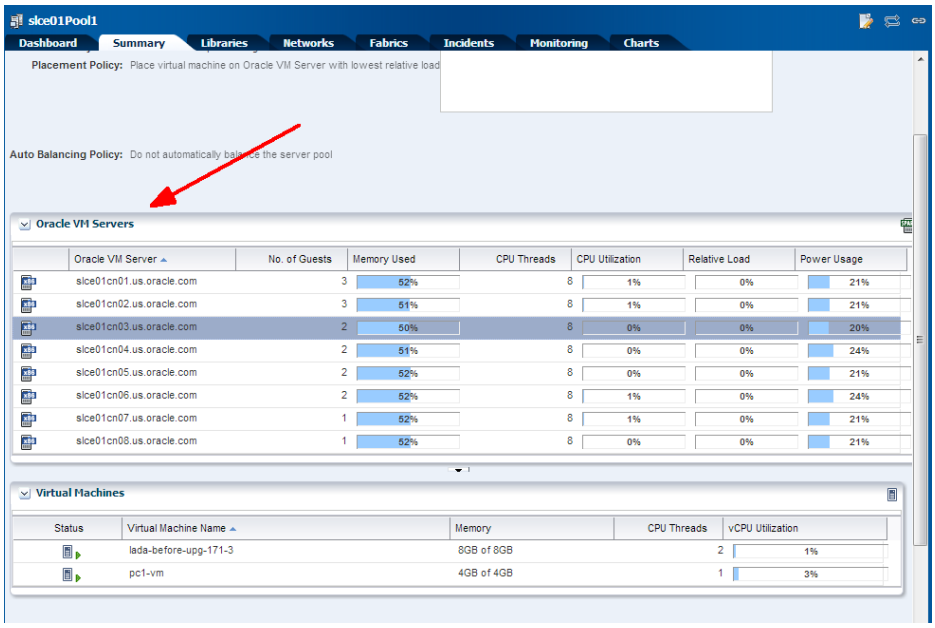
Figure 10-9 Server Pools



The server pool dashboard is displayed.

   g. Click the **Summary** tab.
   h. Scroll down to the Oracle VM Servers section as shown in the following screenshot:

Figure 10-10 List of Oracle VM Servers



i. Select the OVS node you tagged in Task 1: Identify and Tag the OVS Node with vserver_placement.ignore_node=true.

j. Under the Virtual Machines section, note the vServers hosted on the node.

2. Stop the vServers you identified in the previous step by following the steps described in Stopping vServers.

3. Start the vServers you stopped in the previous step by following the steps described in Starting vServers.

> **Note:**
>
> If a HA-enabled vServer fails, while selecting a node for restarting the failed vServer, Exalogic Control considers all of the available nodes, including those that are tagged with `vserver_placement.ignore_node=true`. To make an OVS node unavailable to HA-enabled vServers as well, you must perform Task 3 (optional): Place the OVS Node in Maintenance Mode.

Task 3 (optional): Place the OVS Node in Maintenance Mode

To make an OVS node unavailable to all vServers, including HA-enabled vServers, do the following:

1. Migrate all vServers off the OVS node as described in Task 2: Migrate the vServers on the Tagged OVS Node to Other Available OVS Nodes.

2. Log in to Exalogic Control as the Exalogic Systems Admin user.

3. From the navigation pane on the left, click **Assets**.

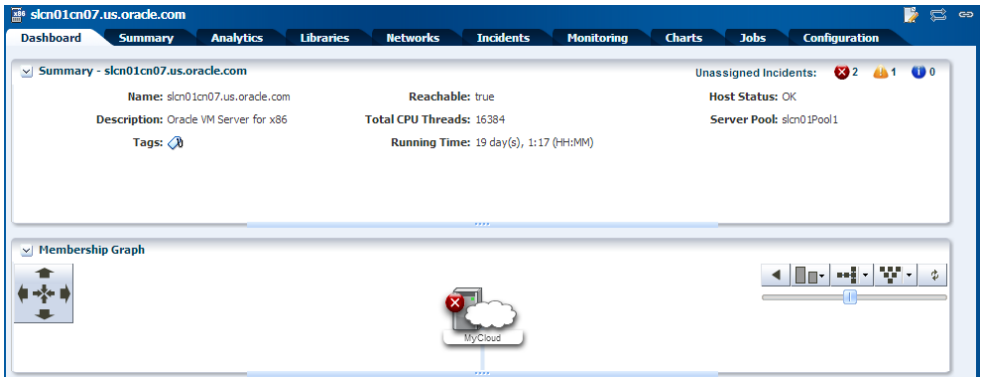
4. Under **Assets**, from the drop-down list, select **Exalogic Systems** and expand **Servers**.

A list of the OVS nodes is displayed.

5. Select the OVS node you want to make unavailable.

   The OVS node dashboard is displayed as shown in the following screenshot:

Figure 10-11 OVS Node Dashboard



6. From the actions pane on the right, click **Place in Maintenance Mode**.

> **Note:**
>
> Before you place an OVS node in maintenance mode, ensure that there are no vServers running on the OVS node. All vServers running on the OVS node must be migrated as described in step 1.

A confirmation box is displayed.

7. Click **Yes**.

Changing Passwords for Components on the Exalogic Machine

See MOS document 1594316.1 at:

`https://support.oracle.com/epmos/faces/DocumentDisplay?id=1594316.1`

Managing Account Resources

This section describes the following topics:

- Logging In as a Cloud User
- Updating a Server Template
- Deleting a Server Template
- Updating a vServer
- Deleting a vServer
- Updating a Private vNet
- Deleting a Private vNet

- Allocating Virtual IPs for an Account
- Deallocating Virtual IPs for an Account
- Updating a Distribution Group
- Deleting a Distribution Group
- Updating a Volume
- Deleting a Volume
- Updating a Snapshot
- Deleting a Snapshot

Before you can complete these tasks, you must have completed the Cloud User tasks, as described in Creating and Managing Exalogic vDC Resources.

Logging In as a Cloud User

Log in to the Exalogic Control console as a `Cloud User` that you created in Creating the Cloud Admin User.

Updating a Server Template

To update the server template that you previously uploaded in your Account, complete the following steps:

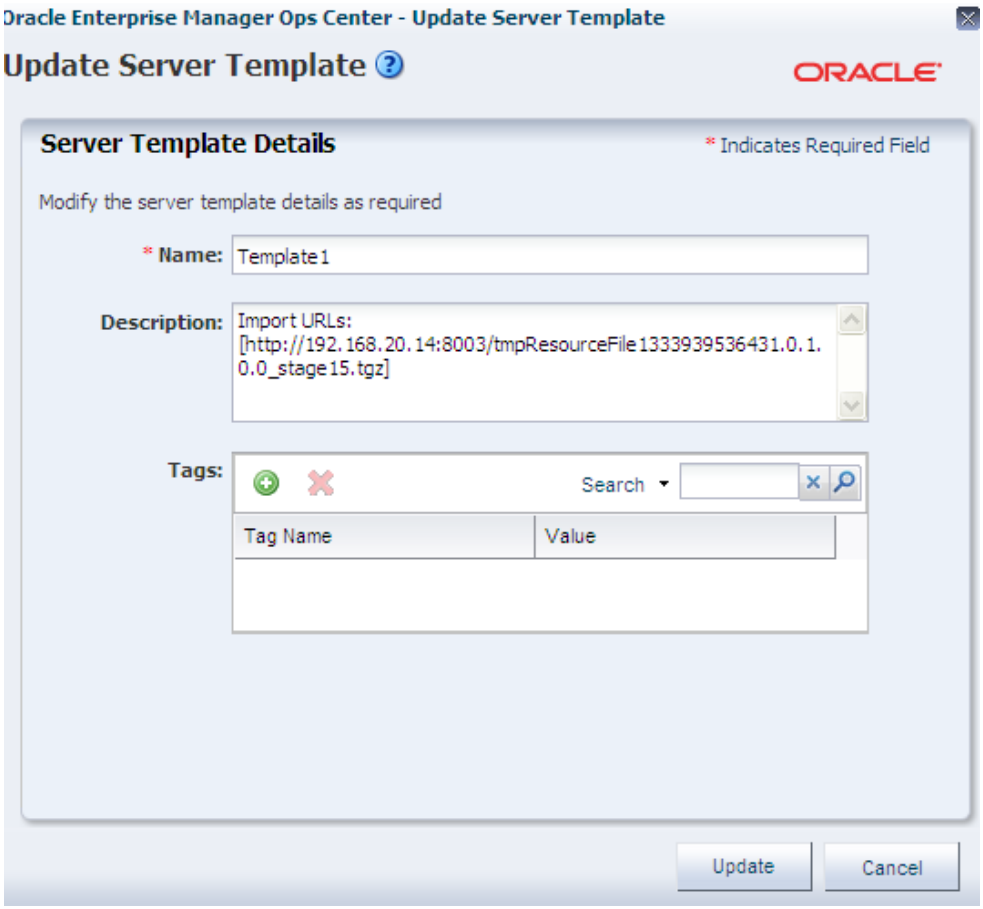
1. Log in to the Exalogic Control console as a `Cloud User`.
2. In the navigation pane on the left, click **vDC Accounts**. Under vDC Accounts, click the name of your Account (example: `Dept1`).

   The `Dept1` Account dashboard is displayed.
3. Click the **Server Templates** tab.

   A list of Server Templates available in your Account is displayed.
4. Select the Server Template (for example, `Template1`) that you previously uploaded to your Account.
5. Click the pencil icon to update the template.

   The Update Server Template screen is displayed, as shown in Figure 10-12.

Figure 10-12 Update Server Template



6. Modify the template details, as necessary.
7. Click **Update**.

Deleting a Server Template

To delete the Server Template that you previously uploaded in your Account, complete the following steps:

1. Log in to the Exalogic Control console as a `Cloud User`.
2. In the navigation pane on the left, click **vDC Accounts**. Under vDC Accounts, click the name of your Account (`Dept1`). The `Dept1` Account dashboard is displayed.
3. Click the **Server Templates** tab. The list of Server Templates available in your Account is displayed.
4. Select the Server Template (for example, `Template1`) that you previously uploaded to your Account.
5. Click the **X** icon to delete the template. A confirmation message is displayed.
6. Click **OK** to confirm.

Updating a vServer

To update a vServer, complete the following steps:

1. Log in to the Exalogic Control console as a `Cloud User`.
2. In the navigation pane on the left, click **vDC Accounts**. Under vDC Accounts, click the name of your Account (`Dept1`). The `Dept1` Account dashboard is displayed.
3. Click the **vServers** tab. vServers created and running in your Account are listed.
4. Select the vServer (for example, `vserverl`) that you previously created in your Account.
5. Click the pencil icon to update the vServer. The Update vServer wizard is displayed.
6. Modify vServer details, as necessary and click **Next**.
7. Modify vServer attributes, the number of vCPUs and memory size of the vServer.

> **Note:**
>
> You can update the vCPU and memory size only when the vServer is in shutdown or shutdown/detached status.

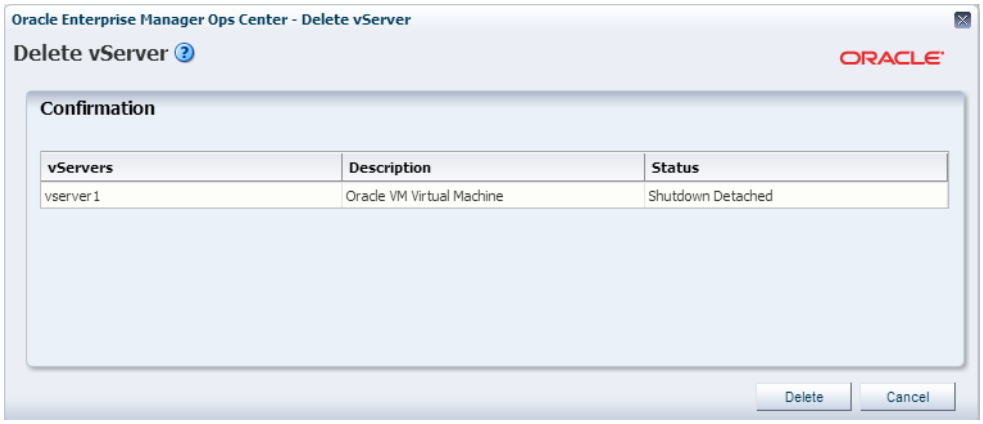
8. Click **Update** to finish.

Deleting a vServer

To delete a vServer, complete the following steps:

1. Log in to the Exalogic Control console as a `Cloud User`.
2. In the navigation pane on the left, click **vDC Accounts**. Under vDC Accounts, click the name of your Account (`Dept1`). The `Dept1` Account dashboard is displayed.
3. Click the **vServers** tab. vServers running or stopped in your Account are listed.
4. If the vServer (for example, `vserver1`) is running, click the **Stop vServer** icon (red icon) to stop the vServer. Wait till the job succeeds in the Jobs pane.
5. Select `vserver1`, and click the **X** icon. The Delete vServer screen is displayed, as shown in Figure 10-13.

Figure 10-13 Delete vServer Screen



This screen also displays the name of the vServer, its description and status.

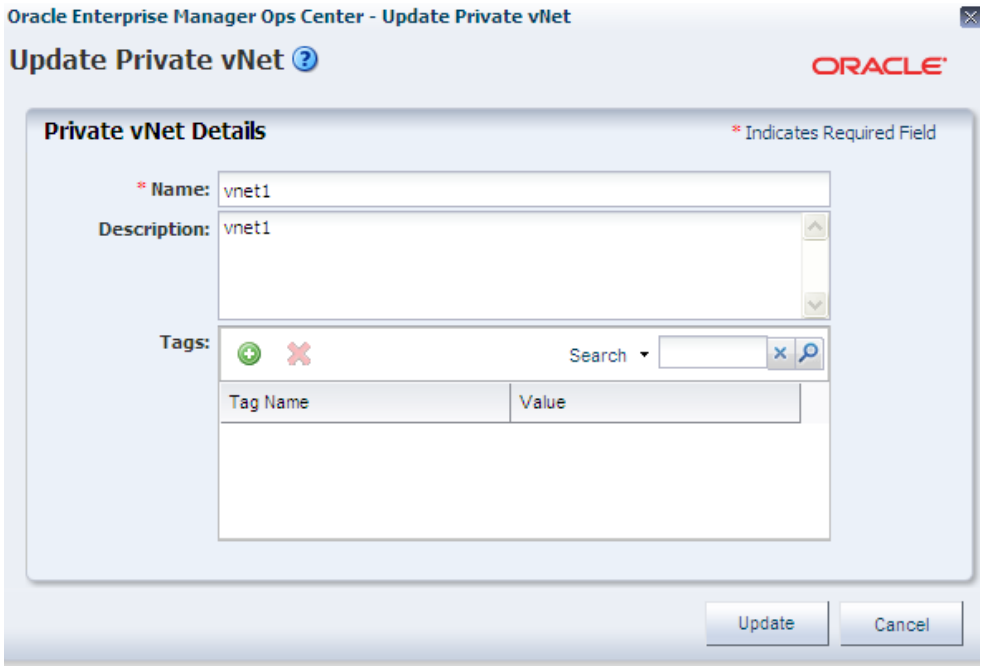
6. Click **Delete** to confirm.

Updating a Private vNet

To update a private vNet that you previously created in your Account, complete the following steps:

1. Log in to the Exalogic Control console as a `Cloud User`.
2. In the navigation pane on the left, click **vDC Accounts**. Under vDC Accounts, click the name of your Account (`Dept1`). The `Dept1` Account dashboard is displayed.
3. Click the **Networks** tab. In the Private vNets section, the list of private vNets available in your Account is displayed.
4. Select the private vNet (for example, `vnet1`) that you previously created in your Account.
5. Click the pencil icon to update the private vNet. The Update Private vNet screen is displayed, as shown in Figure 10-14.

Figure 10-14 Update Private vNet



6. Modify private vNet details, as necessary.
7. Click **Update** to finish.

Deleting a Private vNet

To delete a private vNet, do the following:

> **Note:**
>
> With this procedure, you can delete a vNet even if it is associated with vServers. So before attempting to delete a private vNet, make sure that the vNet not associated with any vServer.

1. Log in to the Exalogic Control console as a `Cloud User`.
2. In the navigation pane on the left, click **vDC Accounts**. Under vDC Accounts, click the name of your Account (`Dept1`).

   The `Dept1` Account dashboard is displayed.
3. Click the **Networks** tab.

   In the Private vNets section, the list of private vNets available in your Account is displayed.
4. Select the private vNet (for example, `vnet1`) that you want to delete.
5. Ensure that the private vNet (`vnet1`) is not associated with any vServer.
6. Click the **X** icon to delete the private vNet.

   A confirmation screen is displayed.

7. Click **Delete**.

Allocating Virtual IPs for an Account

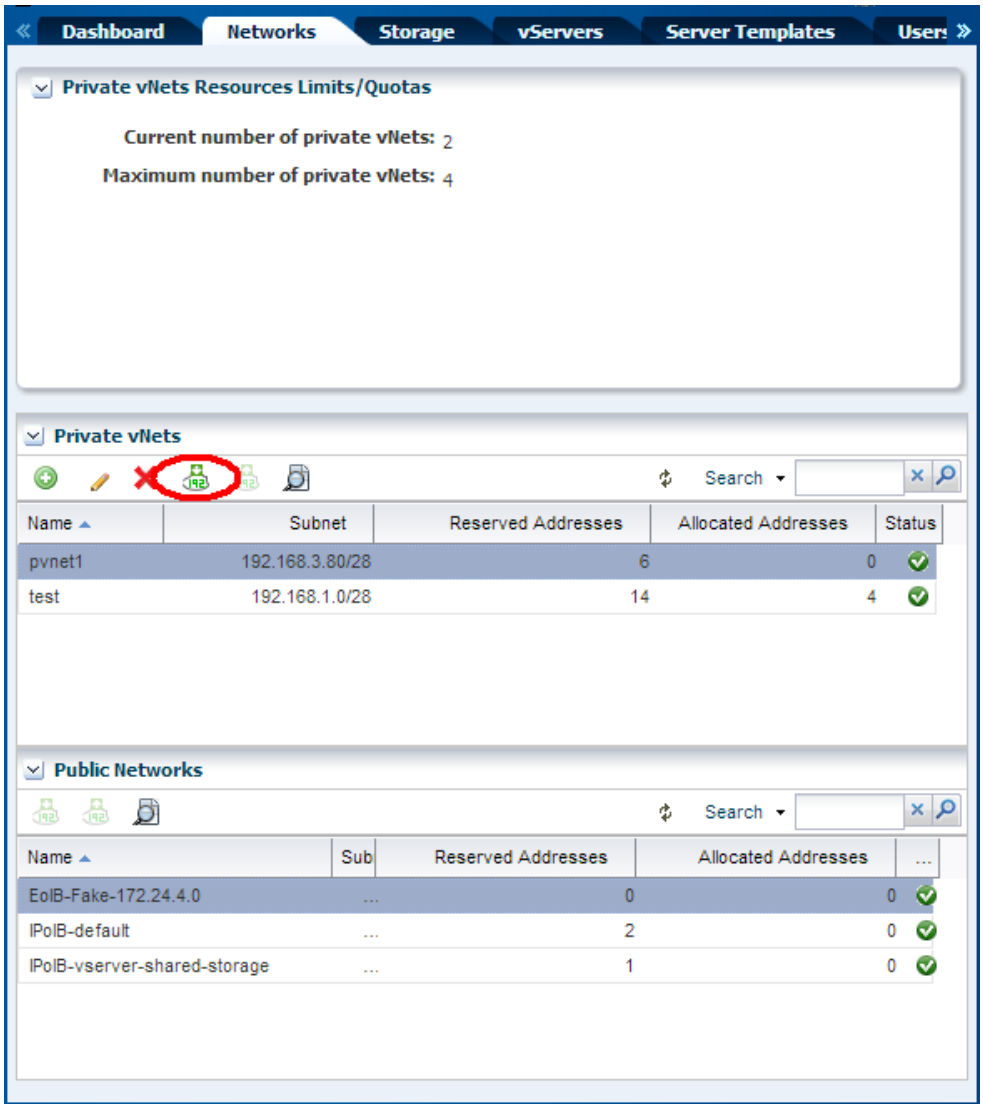
Before creating vServers with a static IP address, you must allocate IP addresses for your account as follows:

1. Log in to the Exalogic Control console as a `Cloud User`.
2. From the navigation pane on the left, click **vDC Accounts**.
3. Under **vDC Accounts**, click the name of your account.

   The Account dashboard for your account is displayed.
4. Click the **Networks** tab.

   The private vNets and public networks available to your account are displayed.
5. Select the network for which you want to allocate IP addresses.
6. Click the **Launch Allocate vIP Wizard** button as shown in Figure 10-15.

Figure 10-15 Launch Allocate vIP Wizard Button



The Allocate vIP Addresses Wizard is displayed.

7. In the **Number of vIPs** field, enter the number of IP addresses you want to reserve for static assignments to vServers.

   The IP addresses that you have allocated are displayed.

8. Click the **Allocate vIP** button.

9. Click **OK**.

   The IP addresses are now available while creating a vServer with a static IP address as described in step 16 of Creating vServers.

> **Note:**
>
> You can click the **View Allocated IP Addresses** button to see IP addresses that you can allocate when creating vServers with static IP addresses.

Deallocating Virtual IPs for an Account

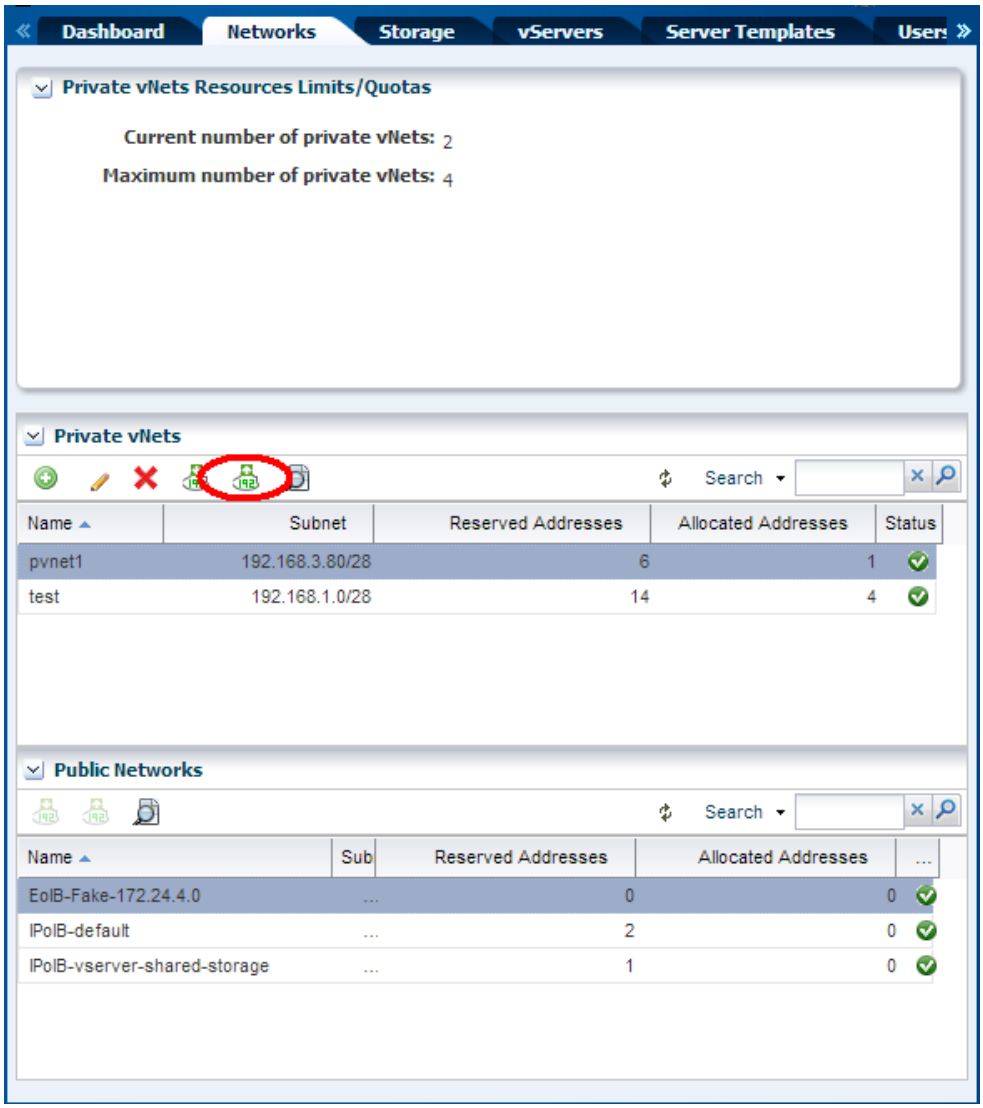
IP addresses that are no longer necessary for use as static IP addresses for an account can be deallocated as follows:

1. Log in to the Exalogic Control console as a `Cloud User`.
2. From the navigation pane on the left, click **vDC Accounts**.
3. Under **vDC Accounts**, click the name of your account.

   The Account dashboard for your account is displayed.
4. Click the **Networks** tab.

   The private vNets and public networks available to your account are displayed.
5. Select the network for which you want to deallocate IP addresses.
6. Click the **Launch Deallocate vIP Wizard** button as shown in Figure 10-16

Figure 10-16 Launch Deallocate vIP Wizard Button



The Deallocate vIP Addresses Wizard is displayed.

7. Select the IP addresses that you want to deallocate.

   You can use the `Ctrl` key to select multiple IP addresses.

8. Click the **Deallocate vIP** button.

   The IP addresses that you have deallocated are displayed.

9. Click **OK**.

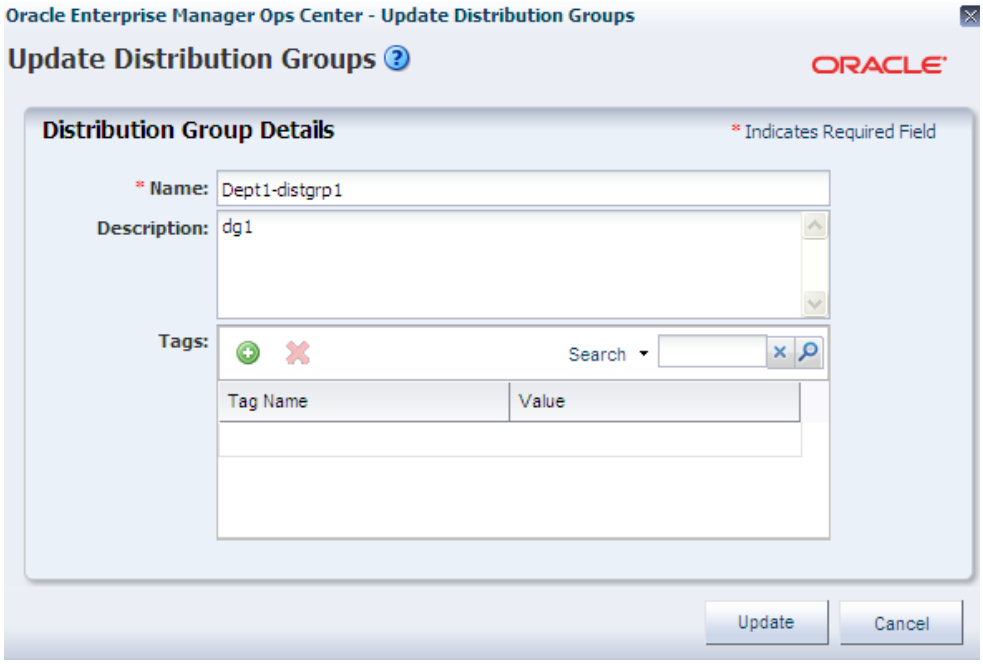
   The IP addresses that you deallocated are now unavailable for static allocation to vServers.

Updating a Distribution Group

To update a Distribution Group that you previously created in your Account, complete the following steps:

1. Log in to the Exalogic Control console as a `Cloud User`.
2. In the navigation pane on the left, click **vDC Accounts**. Under vDC Accounts, click the name of your Account (`Dept1`). The `Dept1` Account dashboard is displayed.
3. Click the **vServers** tab. Distribution Groups available in your Account are listed.
4. Ensure that the Distribution Group (`Dept1-distrgrp11`) is not associated with any running vServers.
5. Select the Distribution Group (for example, `Dept1-distgrp1`) that you previously created in your Account.
6. Click the pencil icon to update the Distribution Group. The Update Distribution Groups screen is displayed, as shown in Figure 10-17.

Figure 10-17 Update Distribution Groups



7. Modify Distribution Group details, as necessary.
8. Click **Update** to finish.

Deleting a Distribution Group

To update a Distribution Group that you previously created in your Account, complete the following steps:

1. Log in to the Exalogic Control console as a `Cloud User`.
2. In the navigation pane on the left, click **vDC Accounts**. Under vDC Accounts, click the name of your Account (`Dept1`). The `Dept1` Account dashboard is displayed.
3. Click the **vServers** tab. Distribution Groups available in your Account are listed.
4. Select the Distribution Group (for example, `Dept1-distgrp1`) that you previously created in your Account.

5. Click the **X** icon to delete the Distribution Group.

> **Note:**
>
> You can delete a Distribution Group only if it does not have assigned vServers.

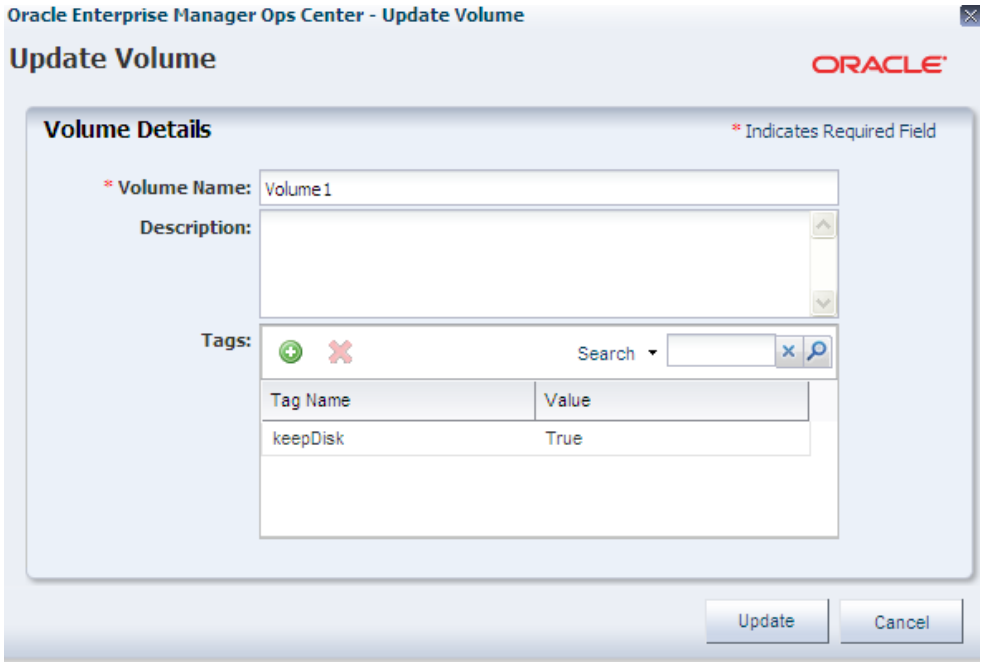
6. If the Distribution Group does not have assigned vServers, click **Delete** to confirm.

Updating a Volume

To update a volume that you previously created in your Account, complete the following steps:

1. Log in to the Exalogic Control console as a `Cloud User`.
2. In the navigation pane on the left, click **vDC Accounts**. Under vDC Accounts, click the name of your Account (`Dept1`). The `Dept1` Account dashboard is displayed.
3. Click the **Storage** tab.
4. Click the **Volumes** tab. Volumes in your Account are listed.
5. Select the volume (for example, `Volume1`) that you previously created in your Account.
6. Click the pencil icon to update the volume. The Update Volume screen is displayed, as shown in Figure 10-18.

Figure 10-18 Update Volume



7. Modify volume details, as necessary.
8. Click **Update** to finish.

Deleting a Volume

To delete a volume that you previously created in your Account, complete the following steps:

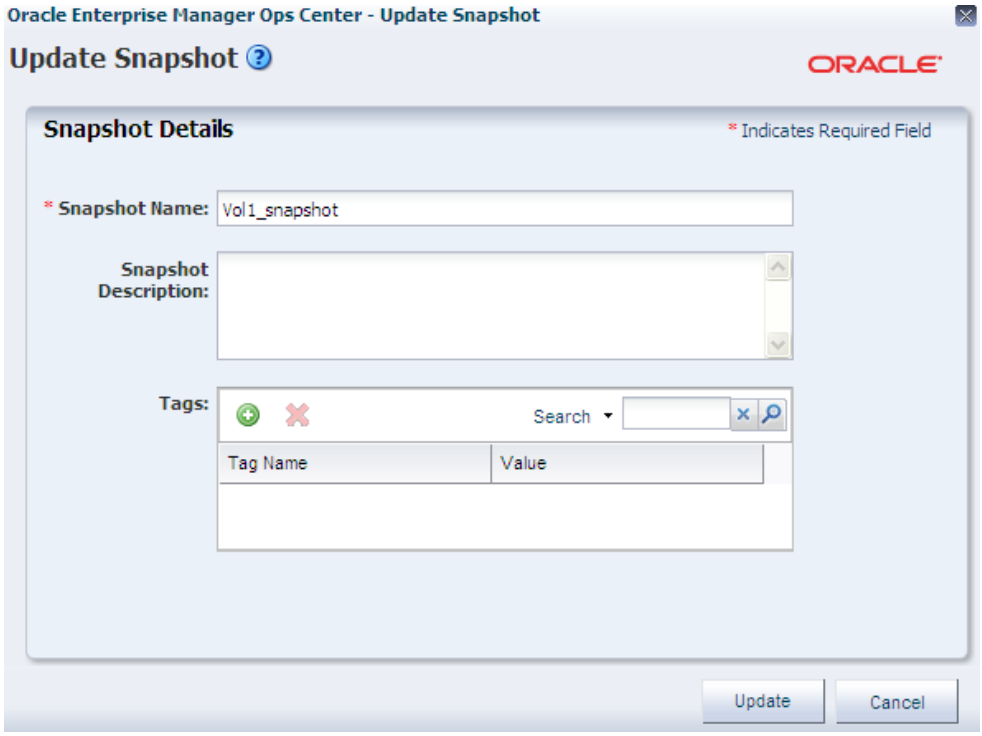
1. Log in to the Exalogic Control console as a `Cloud User`.
2. In the navigation pane on the left, click **vDC Accounts**. Under vDC Accounts, click the name of your Account (`Dept1`). The `Dept1` Account dashboard is displayed.
3. Click the **Storage** tab.
4. Click the **Volumes** tab. Volumes in your Account are listed.
5. Ensure that the Volume (`Volume1`) is not attached to any vServer.
6. Select the volume (for example, `Volume1`) that you previously created in your Account.
7. Click the **X** icon to delete the volume. The Update Volume screen is displayed.
8. Click **Delete** to finish.

Updating a Snapshot

To update a volume Snapshot that you previously created in your Account, complete the following steps:

1. Log in to the Exalogic Control console as a `Cloud User`.
2. In the navigation pane on the left, click **vDC Accounts**. Under vDC Accounts, click the name of your Account (`Dept1`). The `Dept1` Account dashboard is displayed.
3. Click the **Storage** tab.
4. Click the **Snapshots** tab. Snapshots in your Account are listed.
5. Select the Snapshot (for example, `Vol1_snapshot`) that you previously created in your Account.
6. Click the pencil icon to update the Snapshot. The Update Snapshot screen is displayed, as shown in Figure 10-19.

Figure 10-19 Update Snapshot



7. Modify Snapshot details, as necessary.
8. Click **Update** to finish.

Deleting a Snapshot

To delete a volume Snapshot that you previously created in your Account, complete the following steps:

1. Log in to the Exalogic Control console as a `Cloud User`.
2. In the navigation pane on the left, click **vDC Accounts**. Under vDC Accounts, click the name of your Account (`Dept1`). The `Dept1` Account dashboard is displayed.
3. Click the **Storage** tab.
4. Click the **Snapshots** tab. Snapshots in your Account are listed.
5. Select the Snapshot (for example, `Vol1_snapshot`) that you previously created in your Account.
6. Click the **X** icon to delete the Snapshot. A confirmation screen is displayed.
7. Click **Delete** to confirm.

11

Deploying Assemblies in the Exalogic vDC Using OVAB Deployer

This chapter describes how to deploy *assemblies*, created by using Oracle Virtual Assembly Builder (OVAB) Studio, in an Exalogic virtualized data center (vDC). This chapter contains the following sections:

- Introduction to Oracle Virtual Assembly Builder (OVAB) Deployer
- Deploying Assemblies in an Exalogic vDC Using the OVAB Deployer

> **Note:**
>
> For information about creating assemblies by using OVAB Studio, see "Operations Related to Creating an Assembly" in the *Oracle Virtual Assembly Builder User's Guide*.

Introduction to Oracle Virtual Assembly Builder (OVAB) Deployer

This section contains the following topics:

- OVAB Deployer on Exalogic
- Differences Between the Generally Available OVAB Release and OVAB Deployer 11.1.1.6.2

Oracle Virtual Assembly Builder (OVAB) is a tool that enables you to create a blueprint of a reference, multitier application topology, and then deploy that topology in Oracle VM and virtualized Exalogic environments. Using OVAB, you can examine a reference topology and capture the configuration of the individual Oracle software components in the topology, as *appliances*. You can then group the appliances into an *assembly*, which serves as a blueprint for the entire multitier application topology. You can deploy multiple instances of the OVAB-generated assemblies rapidly on virtualized systems, by using OVAB Deployer, which is an application running within an Oracle WebLogic Server container.

For information about creating assemblies by using OVAB Studio, see "Operations Related to Creating an Assembly" in the *Oracle Virtual Assembly Builder User's Guide*.

OVAB Deployer on Exalogic

When you upgrade the Exalogic Elastic Cloud Software (EECS) on an Exalogic machine to v2.0.6.0.0 or when you install EECS 2.0.6.0.0, OVAB Deployer 11.1.1.6.2 is installed in the Exalogic Control VM. You can use OVAB Deployer to deploy

instances of OVAB-generated assemblies in the Exalogic vDC, as described in Deploying Assemblies in an Exalogic vDC Using the OVAB Deployer.

> **Note:**
>
> For the differences between the generally available OVAB release and OVAB Deployer 11.1.1.6.2, see Differences Between the Generally Available OVAB Release and OVAB Deployer 11.1.1.6.2.

Differences Between the Generally Available OVAB Release and OVAB Deployer 11.1.1.6.2

Table 11-1 describes the differences between release 11.1.1.6.2 of OVAB Deployer and the generally available release.

Table 11-1 Differences Between the Generally Available OVAB Release and OVAB Deployer 11.1.1.6.2

Feature	Generally Available OVAB Release	OVAB 11.1.1.6.2
Creating deployment targets	Multiple targets can be created.	A single pre-configured target, which is the same Exalogic system in which the OVAB Deployer is installed. The operation for adding targets is disabled.
Updating deployment targets	All the properties of targets can be updated	Only the operation time-out value (that is, the `exalogic.vmOperationTimeout` property) can be changed, by using the CLI.
Adding users to targets	Users belonging to the `Cloud Admins` group can grant permission to users in the `Application Admins` group, to use a target.	Users belonging to the `Cloud Admins` group can use a configured target; however, they must supply their own credential information to the virtualization system.
Guest base images that can be used for creating assemblies by using OVAB Studio	Any generic Oracle VM image	Only the Exalogic guest base image
Deployment interfaces	Command-line interface and API	Command-line interface, web console (for the tasks described in Using the OVAB Deployer Web Console), and API

Table 11-1 (Cont.) Differences Between the Generally Available OVAB Release and OVAB Deployer 11.1.1.6.2

Feature	Generally Available OVAB Release	OVAB 11.1.1.6.2
IP-address assignment for appliances	The IP addresses can be DHCP-assigned or static. So in the deployment plan, the `network.eth<network>-usedhcp` property can be set to `true` or `false`, depending on the requirement.	IP-address assignment is similar to DHCP, except that the addresses are from a set of addresses that are pre-allocated in Exalogic Control, as described in Allocating Virtual IPs for an Account. To use this feature, set the `network.eth<network>-usedhcp` property in the deployment plan to `true`. If static IP addresses are required, set `network.eth<network>-usedhcp` to `false`, and specify IP addresses from the set of pre-allocated addresses.
Network creation/ binding	The required networks must exist and must be preconfigured. The OVAB metadata defines bindings to the existing networks.	Based on the assembly metadata, private vNets are constructed dynamically on the InfiniBand fabric.
Anti-affinity behavior	See the *Oracle Virtual Assembly Builder User's Guide*.	If the `anti-affinity-min-servers` property is set to a value other than 0, anti-affinity is enabled for the appliance; otherwise, anti-affinity is disabled. When anti-affinity is enabled, the instances of the appliance are placed on separate nodes, up to the number of nodes available. • If the number of instances is equal to, or less than, the number of nodes, each instance is placed on a separate node. • When the number of instances exceeds the number of nodes, a placement failure occurs for the additional instances.

Deploying Assemblies in an Exalogic vDC Using the OVAB Deployer

This section contains the following topics:

Configuring a User and Connection for OVAB Deployer on Exalogic

When OVAB Deployer is installed in the Exalogic Controller vServer in an Exalogic vDC, a single target (named `exalogic`) is preconfigured. In addition, a default security realm is created in the Oracle WebLogic Server that hosts the OVAB Deployer application. The required OVAB-specific user groups—`Application Admins` and `Cloud Admins`—are preconfigured in the default security realm.

Before using OVAB Deployer on Exalogic, complete the following steps:

1. In the Exalogic vDC, identify the following:
   - A `Cloud User` that you want to use to access the OVAB Deployer.

     > **Note:**
     >
     > If you want more than one `Cloud User` to be able to access the OVAB Deployer, you must repeat the procedure described in this section separately for each such user.

   - The UUID of an account to which the selected user is assigned.

     This account that will be used for deploying assemblies, and the resulting vServers will be displayed in the Exalogic Control BUI under this account.

   To find out the UUID of an account in the Exalogic vDC, do the following:

   a. Log in to the Exalogic Control browser user interface (BUI) as a `Cloud Admin` user.

      The URL for the Exalogic Control BUI is:

      `https://`*`ec-vm`*`/emoc`

      In this URL, `ec-vm` is the IP address of the Exalogic Control VM on the `EoIB-external-mgmt` network on the Exalogic machine.

   b. In the navigation pane on the left, expand vDC Management, expand the name of the vDC (say, `MyCloud`), and select **Accounts**.

      The available accounts are listed in the main pane.

   c. Hover the mouse pointer over the name of the account for which you want to find the UUID.

      The resulting display box shows the details of the account, including its UUID (example: `ACC-bbc4ea03-70c5-4fe8-8148-8e770e1b2ec2`).

   If you want to use a new `Cloud User` and a new account, create the required user and account as described in Creating and Managing Users and Roles, and assign the user to the account, as described in Establishing Cloud Accounts.

2. Create a user in the Oracle WebLogic Server that hosts the OVAB Deployer on Exalogic:

   a. Log in to the Oracle WebLogic Server Administration Console as the `weblogic` user with the administration password. If you do not know the password for the `weblogic` user, contact Oracle Support.

The URL for the Oracle WebLogic Server Administration Console is:

```
http://ec-vm:9001/console/login/LoginForm.jsp
```

In this URL, `ec-vm` is the IP address of the Exalogic Control VM on the `EoIB-external-mgmt` network on the Exalogic machine.

b. Create a user, as described in "Create users" in the *Oracle WebLogic Server Administration Console Online Help*.

c. Assign the new user to the `Application Admins` group, as described in "Add users to groups" in the *Oracle WebLogic Server Administration Console Online Help*.

The *Oracle WebLogic Server Administration Console Online Help* is available at:

http://docs.oracle.com/cd/E23943_01/apirefs.1111/e13952/core/index.html

3. Create a connection from an OVAB Studio installation to OVAB Deployer running on Exalogic:

```
$ abctl createDeployerConnection -name connection_name -url http://ec-vm:9001 -username wls_user
```

- `wls_user` is the user that you created in step 2.
- `connection_name` is the name of the connection that you are creating.
- `ec-vm` is the IP address of the Exalogic Control VM on the `EoIB-external-mgmt` network on the Exalogic machine.

A prompt to enter the password is displayed. Enter the password that you defined while creating the user in step 2.

4. From the OVAB Studio installation, add the user (that you created in step 2) to the preconfigured target named `exalogic`:

```
$ abctl addTargetUser -connectionName connection_name -user wls_user
 -target exalogic -properties exalogic.user=cloud_user
 exalogic.pwd=cloud_user_password exalogic.tenancy=account_UUID
```

- `connection_name` is the connection that you defined in step 3.
- `wls_user` is the user that you created in step 2.
- `cloud_user` is the user that you identified (or created) in step 1.
- `cloud_user_pasword` is the password for the user you identified (or created) in step 1.
- `account_UUID` is the UUID of the account to which the specified `Cloud User` is assigned, as identified in step 1.

5. Verify the configuration by running the following command:

```
$ abctl describeTargets -connectionName connection_name
```

This command displays the name, type, and status of the `exalogic` target. It also displays information about the available networks, volumes, and memory.

Accessing the OVAB Deployer Interfaces

OVAB Deployer provides a web console and a command-line interface (CLI) for deploying assemblies on Exalogic.

> **Note:**
>
> You can also use OVAB Studio and OVAB web-service APIs for the deployer operations. For more information, see the following documentation:
>
> - OVAB web-service APIs: See "API Reference: Deployer Operations" in the *Oracle Virtual Assembly Builder Developer's Guide*.
> - OVAB Studio: See the *Oracle Virtual Assembly Builder User's Guide*.

Accessing the OVAB Deployer Web Console

To access the web console for OVAB Deployer on Exalogic, do the following:

1. Ensure that a user and connection have been configured for OVAB Deployer as described in Configuring a User and Connection for OVAB Deployer on Exalogic.
2. Go to the following URL:

   `http://ec-vm:9001/ovab/login.jsp`

   In this URL, `ec-vm` is the IP address of the Exalogic Control VM on the `EoIB-external-mgmt` network on the Exalogic machine.

   The login page is displayed.
3. Specify the user name and password that you defined earlier, as described in step 2 of Configuring a User and Connection for OVAB Deployer on Exalogic.

On the resulting page, you can perform the assembly deployment operations. For more information, see Using the OVAB Deployer Web Console.

Using OVAB Deployer-Related `abctl` CLI Commands

To run OVAB Deployer-related `abctl` CLI commands, you must use the OVAB Studio installation from which you defined a connection to OVAB Deployer on Exalogic as described in step 3 of Configuring a User and Connection for OVAB Deployer on Exalogic.

The `abctl` commands that are available for OVAB Deployer on Exalogic are the same as the commands that are available in a deployer-only installation of the generally available OVAB Deployer release, except for the differences noted in Differences Between the Generally Available OVAB Release and OVAB Deployer 11.1.1.6.2.

For more information about the OVAB Deployer-related `abctl` commands, see "Command Line Reference" in the *Oracle Virtual Assembly Builder User's Guide*.

You can also view help for individual commands directly at the console, by running the following command:

```
./abctl help -command command
```

Assembly Deployment Workflow

Table 11-2 provides an overview of the typical workflow for deploying an assembly in an Exalogic vDC by using the OVAB Deployer, and contains pointers to the sections describing the procedures for performing the tasks in the workflow by using the OVAB Deployer web console. The table also lists the `abctl` CLI commands that you can use to perform the deployment tasks. For more information about the CLI commands, see the *Oracle Virtual Assembly Builder User's Guide*.

Note that, before deploying an assembly, you must create a deployment plan. For more information, see "Operations Related to Deployment" in the *Oracle Virtual Assembly Builder User's Guide*.

Table 11-2 Assembly Deployment Workflow

Workflow Sequence	Task	Procedure Using the Web Console	CLI Command/s
1	Upload the assembly archive to the OVAB Deployer on Exalogic.	Uploading an Assembly Archive	`uploadAssemblyArchive`
2	Register the assembly with the Exalogic target.	Registering an Assembly Archive	`registerAssemblyArchive`
3	Create an assembly instance.	Create an Assembly Instance	`createAssemblyInstance`
4	Deploy the assembly instance.	Deploying an Assembly Instance	`deployAssemblyInstance`

5	Start, stop, restart, or redeploy the assembly instance.	Starting, Stopping, Restarting, and Redeploying Assembly Instances	`startAssemblyInstance`
			`stopAssemblyInstance`
			`restartAssemblyInstance`
			`redeployAssemblyInstance`

6	Scale appliances.	Scaling an Appliance	`scale`

Using the OVAB Deployer Web Console

This section describes the procedures to perform various assembly lifecycle-related tasks by using the OVAB Deployer web console.

This section contains the following subsections:

- Viewing a List of Uploaded Assembly Archives
- Uploading an Assembly Archive
- Downloading an Assembly Archive
- Deleting an Assembly Archive
- Registering an Assembly Archive
- Unregistering an Assembly Archive
- Create an Assembly Instance

Viewing a List of Uploaded Assembly Archives

To view a list of assembly archives that are currently uploaded to the OVAB Deployer, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Archives** tab.

Uploading an Assembly Archive

To upload an assembly archive to OVAB Deployer, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Archives** tab.
3. Click the **Upload** button on the toolbar.
4. On the resulting page, specify a name and description for the archive, and the location, on the local host, of the archive file.
5. Click **Upload**.

Downloading an Assembly Archive

To download an assembly archive from OVAB Deployer, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Archives** tab.
3. Select the assembly archive that you want to download.
4. Click the **Download** button on the toolbar.
5. In the resulting dialog box, specify the location, on the local host, to which the assembly archive should be downloaded.

Deleting an Assembly Archive

To delete an assembly archive from OVAB Deployer, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Archives** tab.
3. Select the assembly archive that you want to delete.
4. Click the **Delete** button on the toolbar.

Registering an Assembly Archive

To register an assembly archive to the Exalogic target, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Registrations** tab.
3. Click the **Register** button on the toolbar.
4. On the resulting page, do the following:
   a. In the **Assembly** field, select the assembly for which you want to register.
   b. In the **Version** field, select the assembly version number.
   c. In the **Plan** field, specify the location of the deployment plan.
   d. Click **Register**.

Unregistering an Assembly Archive

To unregister an assembly archive, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Registrations** tab.
3. Select the assembly archive that you want to unregister.
4. Click the **Unregister** button on the toolbar.

Create an Assembly Instance

To create an assembly instance, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Deployments** tab.
3. Click the **Create** button on the toolbar.
4. On the resulting page, do the following:
   a. In the **Assembly** field, select the assembly for which you want to create an instance.

b. In the **Version** field, select the assembly version number.

c. In the **Plan** field, specify the location of the deployment plan.

d. Click **Create**.

Viewing a List of Assembly Instances

To view a list of assembly instances, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Deployments** tab.

Deleting an Assembly Instance

To delete an assembly instance, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Deployments** tab.
3. Select the assembly instance that you want to delete.
4. Click the **Delete** button on the toolbar.

Deploying an Assembly Instance

To deploy an instance of an assembly, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Deployments** tab.
3. Select the assembly for which you want to create an assembly instance.
4. Click the **Deploy** button on the toolbar.

Undeploying an Assembly Instance

To undeploy an assembly instance, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Deployments** tab.
3. Select the assembly instance that you want to undeploy.
4. Click the **Undeploy** button on the toolbar.

Starting, Stopping, Restarting, and Redeploying Assembly Instances

To start, stop, restart, or redeploy an assembly instance, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Deployments** tab.

3. Select the assembly instance that you want to start, stop, restart, or redeploy.
4. Click the appropriate button on the toolbar.

Viewing the Status of Deployment Requests

To view the status of deployment requests, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Requests** tab.

Deleting a Completed Deployment Request

To delete a deployment request that has been completed, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Requests** tab.
3. Select the request that you want to delete.
4. Click the **Delete** button on the toolbar.

Viewing a List of Appliances

To view a list of appliances, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Appliances** tab.

Deleting a Failed Appliance

To delete an appliance that is in the `failed` state, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Appliances** tab.
3. Select the appliance that you want to delete.
4. Click the **Delete** button on the toolbar.

Scaling an Appliance

To scale an appliance, do the following:

1. Log in to the OVAB Deployer web console, as described in Accessing the OVAB Deployer Interfaces.
2. Click the **Appliances** tab.
3. Select the appliance that you want to scale.
4. Click the **Scale** button on the toolbar.
5. On the resulting page, specify the scaling parameters.

A

Exploring the Exalogic Control BUI

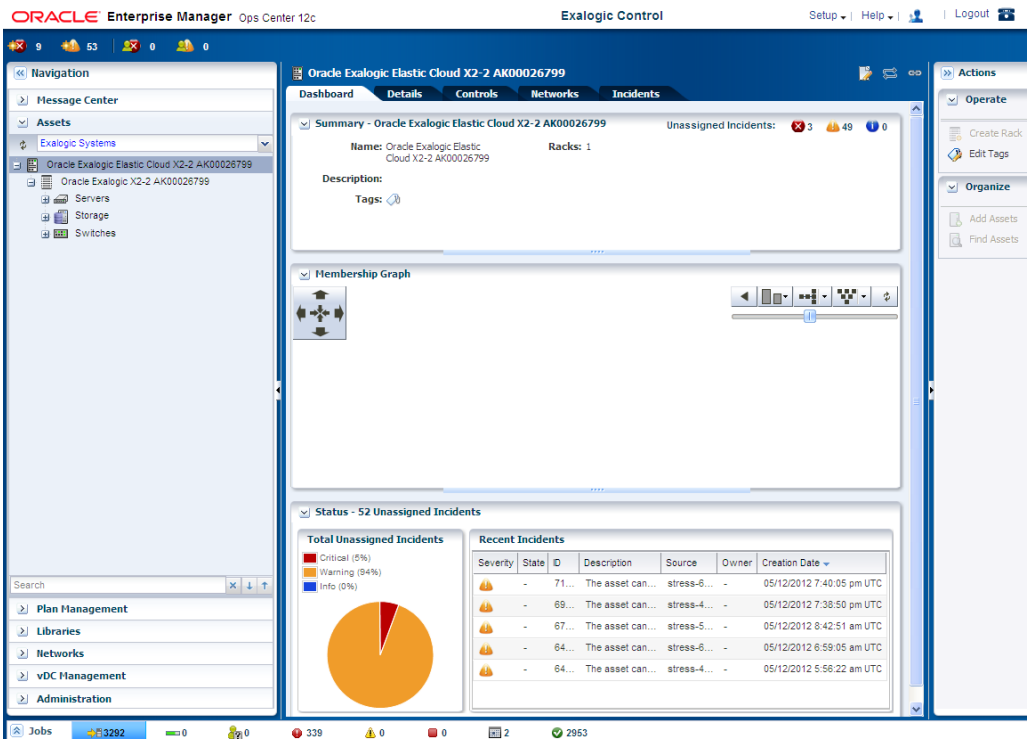
This appendix introduces the Exalogic Control Browser User Interface (BUI). This appendix contains the following sections:

Overview

The user interface has a rich set of features that enable you to observe and control your data center's assets. These features present the range of information from a high-level overview of your data center to the low-level details of a specific asset. You can view the information in the center pane according to your selections made in the **Navigation** pane and in the **Actions** pane.

Hover your mouse over the incident icons at the left-side corner of the user interface to know more about the incidents.

Figure A-1 User Interface of Exalogic Control BUI



Exalogic Control BUI comprises five panes:

- Masthead – This pane displays the global functions and information about the Exalogic Control BUI instance.
- Navigation pane – This pane consists of several drawers that displays assets and objects that are managed by Exalogic Control.
- Actions pane – This pane displays the actions that can be run on the object currently selected in the Navigation pane. The actions of the Actions pane are enabled or disabled based on the state of the object, as well as your role in managing the object.

  Only actions that can be directly applied to the object are displayed in Actions pane.
- Jobs pane – This pane displays the number of jobs in Exalogic Control's BUI, categorized by the status of respective jobs.
- Center pane – This pane displays detailed information of the object that is currently selected in the Navigation pane.

Status of Your Session

Exalogic Control displays the following icons in the title bar. To view information about the status of your session, click the icons displayed in the title bar.

Figure A-2 Icons in the Title Bar

- Setup – Sets UI preferences for the current user or for specific roles.
- Help – Opens the documentation hierarchy for Exalogic Control BUI.
- Your Account – Shows the roles and privileges for the current user.
- Logout – Logs you out of the application.
- Status of Internet Connection – Indicates whether Exalogic Control is connected to the Internet.
- Status of Knowledge Base Service – Indicates whether Exalogic Control BUI is connected to Knowledge Base Service to obtain the latest operating system updates from My Oracle Support.
- Status of My Oracle Support Services – Indicates whether Exalogic Control BUI is connected to My Oracle Support. You must enter valid My Oracle Support (MOS) credentials to be connected.

  For more information about creating and verifying MOS credentials, go to the My Oracle Support portal at the following Web Site:

  `https://support.oracle.com`

Navigation Pane

The Navigation pane contains the following sections:

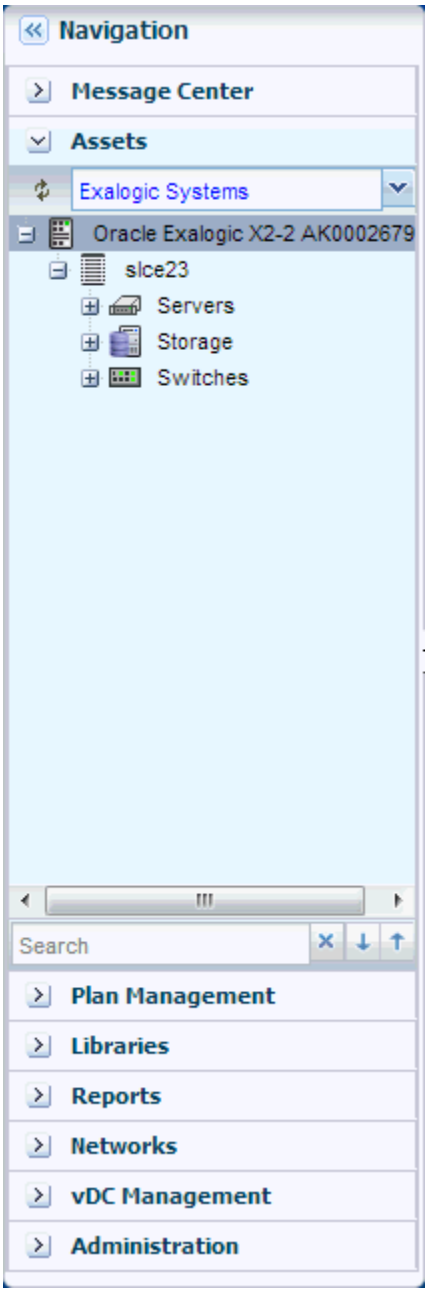
- Message Center: This section displays, and manages incidents, generates notifications, displays service requests, and the warranty information of an asset.
- Assets: This section lists all the assets of Exalogic Control BUI. Assets display standard views, user defined groups, and resource management views. Assets display Server pools which are not assets, but different groupings of managed assets. In the case of server pools, Assets also governs the guest placements and migrations, as well as networking and storage for server pool members.
- Plan Management: This section displays Deployment Plans and Profiles that are used to install, provision, and update servers in Exalogic Control BUI. It also displays Monitoring Policies, Operational Plans, Incidents Knowledge Base, and the credentials that are used in Exalogic Control BUI.
- Networks: Networks can be private or public. The Networks section display all of the networks that are discovered, declared, and created in Exalogic Control BUI. It also displays discovered fabrics.
- Libraries: Software libraries stores images, operating system updates components (policies and profiles). Storage libraries list different NAS storages that are known to Exalogic Control BUI.
- Reports: This section lists the various types of reports that you can create, such as Operating System Reports, Incident Reports, Firmware Reports, and Additional Reports.

- vDC Management: This section stores and manages a set of physical resources, and makes them available as virtual resources to virtual data center accounts.
- Administration: This section performs administrative functions, such as user administration, logs, and the status of service, including the version and upgrades available for the Agent Controller.

  Only the Administrator of Exalogic Control BUI can access the Administration drawer. The administrator can change any configuration for the Enterprise Controller, Proxy Controllers, LDAP directories, users, and so on.

Click the right-arrow next to the section title to open the section and see its available resources and options. You can open only one section at a time.

Figure A-3 Assets Drawer of Navigation Pane



When a new asset is discovered, or when a job or a task is completed, the information changes in Exalogic Control BUI, and the user interface refreshes automatically. When you do not see a new asset in the Assets pane, click the Refresh symbol in the Asset section of the Navigation pane to get the latest lists of assets. Similarly, click the Refresh symbol in the Jobs pane to view the latest list of jobs.

The Assets section of the Navigation pane lists all the asset that are managed by Exalogic Control BUI, grouped by its type and the required criteria. Even in the smallest data center, Exalogic Control BUI can display the list of managed assets. You can choose one of the following views in these categories to see the lists of assets.

- Standard Views – Use the All Assets view to display all managed assets of every type. To filter the view to display one type of asset, use one of the other standard views: Operating Systems, Chassis, and Servers. Click the plus symbol to display the subordinate or individual assets.
- Resource Management Views – Use Resource Management View to filter the assets in the form of Server Pools, Storage, and Racks.
- User Defined Groups – Use the User Defined Group to filter the assets according to user definitions. When you create a group, this customized list becomes the new default view. A list shows a hierarchy of assets.

Each asset and its status is represented by an icon. These icons help you distinguish one type of asset from another type. Appendix F in *Oracle Enterprise Manager Ops Center Feature Reference Guide* shows the product icons and badges.

A quick scan of the asset hierarchy displays the list of servers that are running Oracle Linux. The scan also provides information on the unconfigured assets.

In an Asset hierarchy, an incident associated with an asset is notified by a badge that appears next to the asset icon. Badges show the current status of each asset like running, shutdown, locked, and suspended. When the incident is of a high priority in the membership group, the badge appears next to the parent asset in the asset hierarchy. The system removes the badge after the incident is acknowledged, marked repaired, or closed.

> **Note:**
>
> The badges are disabled by default. To display the badges in the Navigation pane, click Setup, My Preferences, then click User Interface Preferences. Click the check box to make the badges visible in the user interface.

Along with the assets, the Navigation pane shows all other elements that are managed by Exalogic Control BUI, such as plans and profiles, networks, libraries of images and data, reports, and administrative functions. Click the right arrow on the title bar to view the hierarchy of these items.

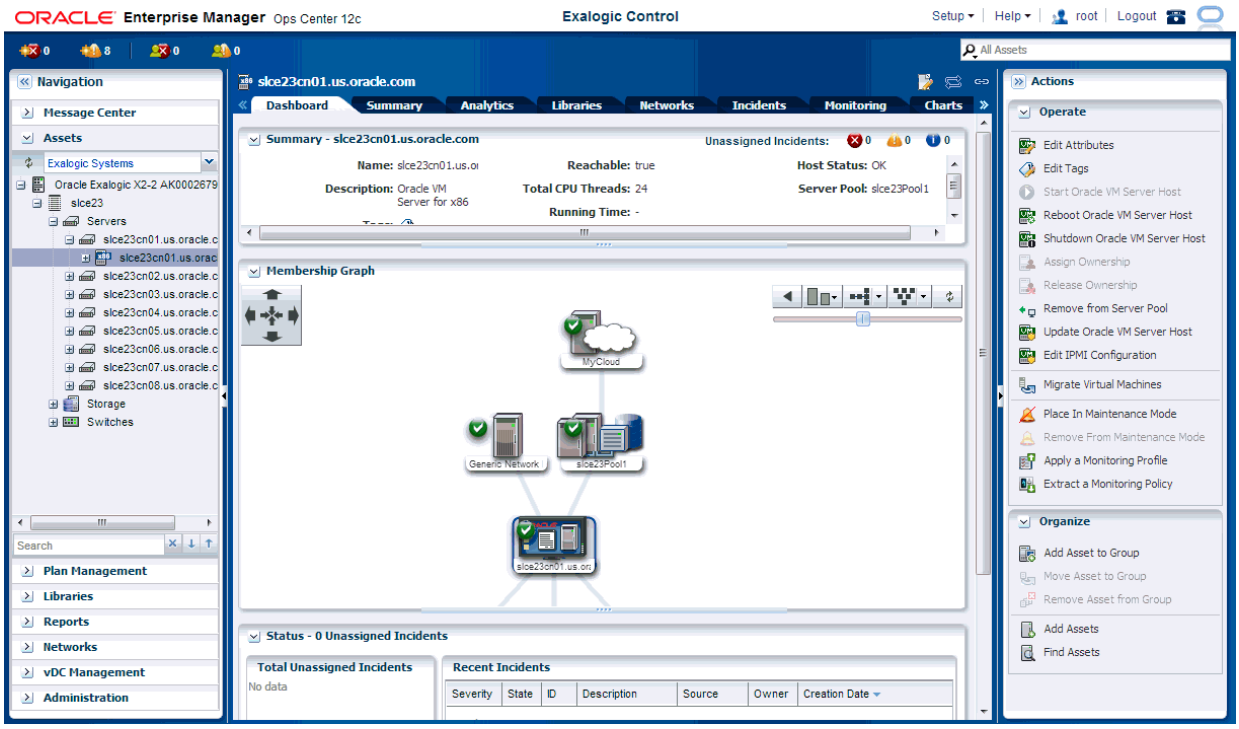
The center pane displays information according to your selection in the Navigation pane.

For example, when you select the Server node of Assets section in the Navigation pane, the center pane displays the information about the Managed Members, and Unmanaged Members. Under the Server node, when you select a server, the center pane displays information about the Server's Hardware, Incidents, Service Requests, Rules, Jobs, Configurations, and Summary details. When you select the Operating

System in the Asset section of Navigation pane, the center pane displays the Analytics, Incidents, Terminal, Storage, Jobs, Configuration, and the Summary of the Operating System.

Similarly, when you select All Assets node in the Assets section, the Action pane displays options to create, find, and add assets. When you select Server in the Assets section, the Actions pane displays the related actions to Execute Operation, Edit Tags, Refresh and so on. Further selection of the operating system in the Assets section of Navigation pane displays operations related to the operating system like Creating New Boot Environment, Executing Operation, Attach New Network, Edit Tags, Edit Attributes, and so on.

Figure A-4 Details of Asset Displayed in the Center Pane

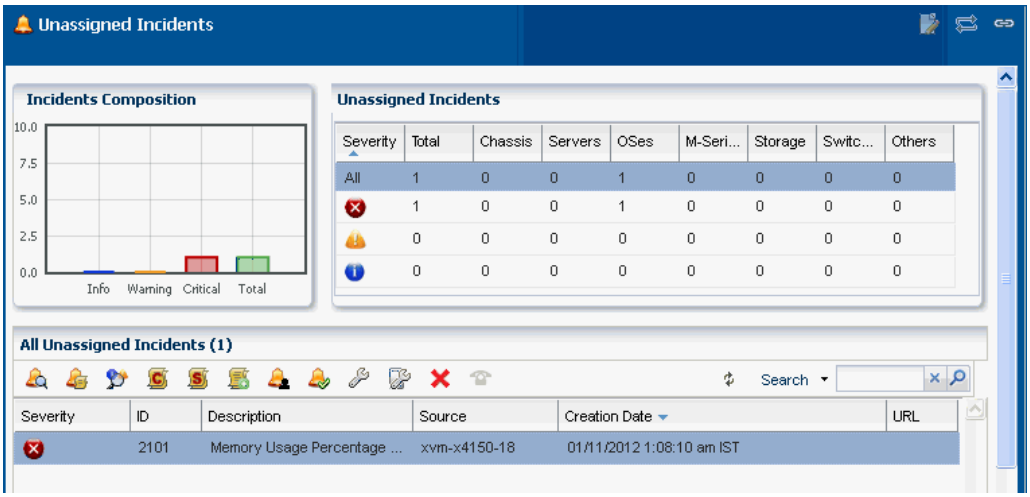


Message Center

The Message Center displays and manages incidents, sends notifications, displays service requests, and displays warranty information for assets.

You can view details about the unassigned incidents in the Unassigned Incidents queue in the Message Center. The Message Center displays the composition of incidents, the severity level for different types of assets along with the severity status icon, and all unassigned incidents along with Severity, Incident ID, Incident Description, Incident Source, Incident Creation Date, and URL. Hover your mouse on an unassigned incident to view details such as Duration, Assigned Date, Suggested Actions, Owner, Source and so on.

Figure A-5 Unassigned Incidents in Message Center



You can view incidents that are assigned to you in the My Incidents queue of the Message Center. A bar chart in the Incidents composition section displays the number of new incidents by severity. The page also displays a table that categorizes the incidents by severity and type of asset. You can select an incident at All My Incidents section to perform the following operations.

- View Alerts – View the alerts that comprise an incident.
- View Annotations – View all comments and notes that are created by alerts and any operation related to the incident. You can also view any suggested actions associated to the type of incident.

  You can edit or delete the annotations that you have created. An administrator has the privileges to edit or delete any annotation.
- View Possible Impacts and Causes – View the possible causes and impacts of an incident.
- View Comments – You can view all comments associated with the selected incident. You can also add a comment to an incident. Only the Exalogic Control BUI administrator and owner of the comment can edit and delete a comment.

  When you add comments, you cannot add an associated Operational Plan. To include the comment or suggested action on any incident with the same type and severity, click the check box **Save this annotation in Incident Knowledge Base to associate the annotation with all incidents of this type and severity**.
- View Suggested Actions – You can view all suggested actions in the Incident Knowledge Base, that are related to the incidents; as well as any suggested actions entered specifically for the incident through Add Annotation. To include the suggested action in the Incident Knowledge Base, click the check box **Save this annotation in the Incident Knowledge Base to associate the annotation with all incidents of this type and severity**.
- Assign Incidents – You can assign one or more incidents to a user. The table enables multiple selection of incidents to be assigned to the user.
- Add Annotation to Incidents – You can add a comment or a suggested action to one or more incidents. When you add a suggested action, you can add an

associated Operational Plan to the suggested action and you can save and execute it.

- Acknowledge Incident – Acknowledging incident changes the state of one or more incidents to 'Acknowledged'. It indicates that you are currently investigating the incidents. This action automatically moves the selected incidents to the "My Incidents" category.
- Take Action on Incidents – Indicates that you can take appropriate action on one or more incidents of the same type, with the same attribute.
- Mark Incidents as Repaired – It moves the state of one or more incidents to "Marked as Being repaired". This state indicates that the source of the incident is being repaired. Other users should not run any operational plan, or take any other actions on the source of the incident.
- Close Incidents – While an incident remains open, the continued monitoring of the asset generates alerts. When you close an incident, if further issues occur, they will create a new incident.
- Open Service Requests – Opens a service request for the incident. You must connect to My Oracle Support to open a service request.

Similarly, you can view the incidents that are assigned to others by clicking Incidents Assigned to Others.

Message Center lets you delete a selected notification or delete all notifications.

Below the title bar, a set of icons summarizes the Incident status. The icons are Unassigned Critical Incident, Unassigned Warning Incident, All Relayed Incident, My Critical Incident, and My Warning Incident. The number next to each icon indicates the count of incidents for the particular status. Hold or hover the mouse cursor over the icon to view information that identifies the most recent incident. These icons keep you updated of the incident status while you perform other operations.

To view more information about the incidents, click these incident icons. They redirect you to the corresponding category in the Message Center. For example, clicking the Unassigned Warning Incident icon below the title bar redirects you to Message Center and displays detailed information about those number of Warning Unassigned Incidents in the center pane. Similarly, when you click Unassigned Critical Incident, it redirects you to Message Center and displays detail about the Critical Unassigned Incidents. Double-click the selected incident to view details such as Summary, Membership Graph, Status, Compliance Reports and so on. For more information about Incidents, see *Oracle Enterprise Manager Ops Center Feature Reference Guide*.

Figure A-6 Incidents Count in the Masthead

Center Pane

Any selection in the Navigation pane changes the display in the center pane. Allow time for the information to finish loading in the Membership Graph, depending on the complexity of your selection. The center pane is where you do most of the work.

To increase the size of the center pane, close the Navigation pane. Click the left double-arrow in the title bar of the Navigation pane, to collapse the pane. To select another asset, expand the Navigation pane again by clicking on the right double-arrow

For most types of assets, the center pane shows a dashboard of standard information about the selected asset, a Membership Graph that shows its relationships, and a status summary that includes information about the unassigned incidents. Use the scroll bars to view all the information. For some types of assets, you need to click the right double-arrow button to view all the tabs.

You can edit, and refresh the details of an asset that are displayed in the center pane. Click Edit icon to edit the summary details of the selected asset in the Summary tab of the center pane. Commit the changes by clicking the Save icon or Cancel to ignore any change. A pop-up message displays information about the successful commit in the application.

The center pane also has icons that perform an action on the selected item, depending on the drawer selected in the Navigation pane. These icons are View Alerts, Close Incidents, Open Service Requests, Add User, Manage User Roles and so on.

Click Refresh to reload the latest information in the center pane.

Some types of assets have additional sections such as Services, Status, Compliance Reports, and File Systems. You can collapse these sections to hide the display and to prevent the information from refreshing. Click the down-arrow in the corner of the section to hide the section. Click the resulting right-arrow to reveal the section.

Tabs

Some of the drawers of the Navigation pane display their details in the form of tabs in center pane. With your setting preference, you can set up any tabs in an object to be the default tab. Dashboard or Summary can be the default tab for those selected drawers.

In case of assets selected as a drawer, the Dashboard tab displays a high-level overview of the asset. Every group and managed asset has a dashboard tab that provides a Summary, a Membership Graph, and the Monitoring status. The Dashboard tab displays additional information, depending on the type of asset selected in the drawer.

Dashboard enables you to customize your display preference by changing the position and height, or by collapsing or expanding any panel of the dashboard. The set preference is saved and used at the time of your next login.The same display preference is applied to other dashboards of the same type for other assets. For example, when you move the Status panel to the top for a dashboard of the selected server, at your next login, you find the Status panel at the same new location. When you select another server, you find the Status panel at the same new location of the dashboard.

When you select a group of assets, the Summary tab provides information about all members of a group, and charts to identify the most active and least active members. To know more about the asset, click one of the tabs. Click the right double-arrow button to view the remaining tabs when there are too many tabs to fit into the center pane. Hold or hover the mouse over the value in the table to see its definition.

Charts are included in the Dashboard, Summary, and the Charts tab. Charts give access to the data collected by Exalogic Control BUI for all the assets all the time. Hover the mouse over a portion of the chart to view the value it represents. On the

Dashboard, you can hide the legend for a chart and the chart itself. Hide the legend when you want to see more details in the chart. Hide the entire chart to focus on another part of the center pane. Click the down-arrow button to hide and click the right-arrow button to show.

The Charts tab, displays a variety of charts. Right-click one of the charts to display a submenu of the following actions to customize the chart:

- Select to pick a point on the line and display its values.
- Zoom to concentrate on a portion of the chart.
- Move to change the location of the chart.
- 100% to restore the chart to its original scale.
- Select All
- Property to display a table of all the values in the chart. You can control the scope of the chart by increasing or decreasing the time period of the data collection.

You can export your chart data in one of the following formats:

- CSV
- XML

Select one of the following timeframes to export your chart data.

- Current View
- 6 months

The display of the tabs change in the center pane depending on the type of asset selected in the Navigation pane. For example, the display of tabs change in center pane when a hardware asset or an operating system is selected. Center pane displays some common tabs such as Dashboard, Monitoring, Jobs, and so on. On the selection of an asset in the Navigation pane, the center pane displays information about incidents in Incidents tab. You can view the alerts, incidents composition, and the unresolved incidents for the selected asset.

Administering Enterprise Controller displays its information in various tabs like Summary, Configuration, Storage Libraries, Proxy Controller, and Logs.

You can select a template to view the template details or create a deployment plan from the templates tab in Plan Management. Existing Deployment Plans tab helps you in viewing a collection of profiles and plans that enables using the software to perform the tasks needed to maintain, monitor, and manage the infrastructure of your data center.

Exalogic Control uses libraries to store and manage cached data, images, packages, and metadata. It displays all its information through Summary, Usage, Disks, Incidents, and Monitoring tabs.

The Networks tab shows the network domains that are created. The Dashboard tab shows details about the network type, MTU, IP Range, Bandwidth, status of unassigned incidents, and recent incidents. The Network Details tab shows information about the Network IP, Netmask, Network Type, Network Name, and various other information about the network domain. Other tabs of Managed Network that provide more information about the network domain are IP Address Allocator, Network Services, Network Connections, Incidents, and Monitoring.

Membership Graph

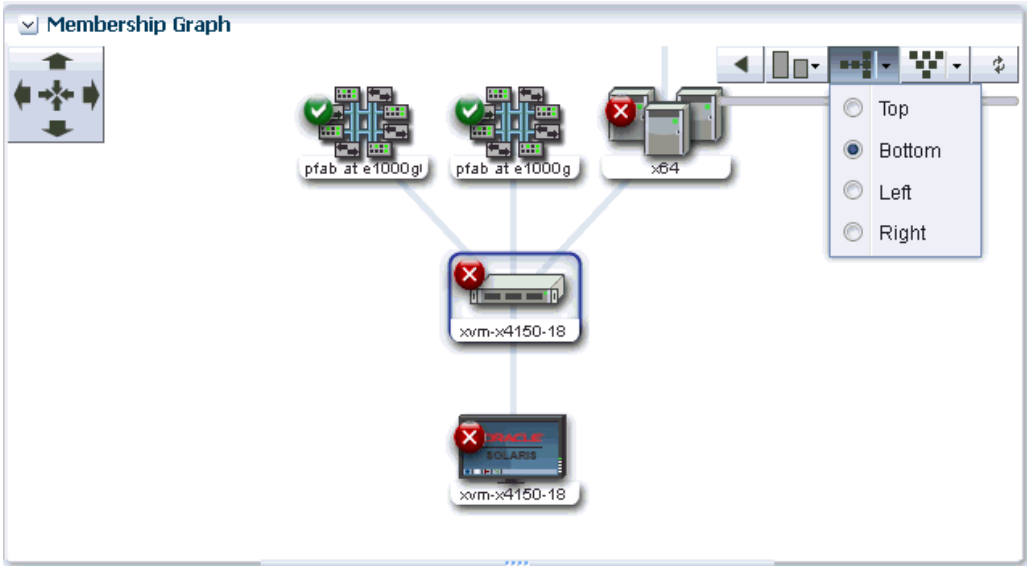
The Dashboard tab is the default display of the center pane, and the Membership Graph is a part of the Dashboard tab. The Membership Graph shows the relationships between the assets that are selected. Depending on what you select in the Navigation pane and on your data center's organization, the Membership Graph can have a single object or multiple objects. To control the view, you can use these options:

- Use the scroll bar for moving the display and bringing the assets in large graphs into view.
- Use view controls to move the Membership Graph left and right, and up and down. These view controls are two sets of arrows: four inward arrows and four outward arrows. Click one of the outward arrows to move the Membership Graph. Click one of the inward arrows to center the graph in the center pane.
- Use the orientation controls to change the orientation of the graph. The hierarchy can be presented from the top down or from the bottom up. If the hierarchy is flat and wide, a more convenient display might be to change to a horizontal display so that the top is now on the left or right. Click the left arrow to restore the display.
- Drill into the graph. When you choose assets or a group at the top of a hierarchy, the Membership Graph consolidates the display of the assets so that the graph is not unwieldy. Click in the graph to show the actual members.

Hover your mouse on the desired icon in the Membership Graph to view details about the type of asset like name, description, type, and tags. Double-click the icon in the Membership Graph to reach that asset in the Navigation pane and also view its detailed description in the Dashboard tab of center pane.

For an incident, the warning and critical icons appear next to the asset. These icons also appear as a badge on the asset and the asset group in the Navigation pane.

Figure A-7 Membership Graph



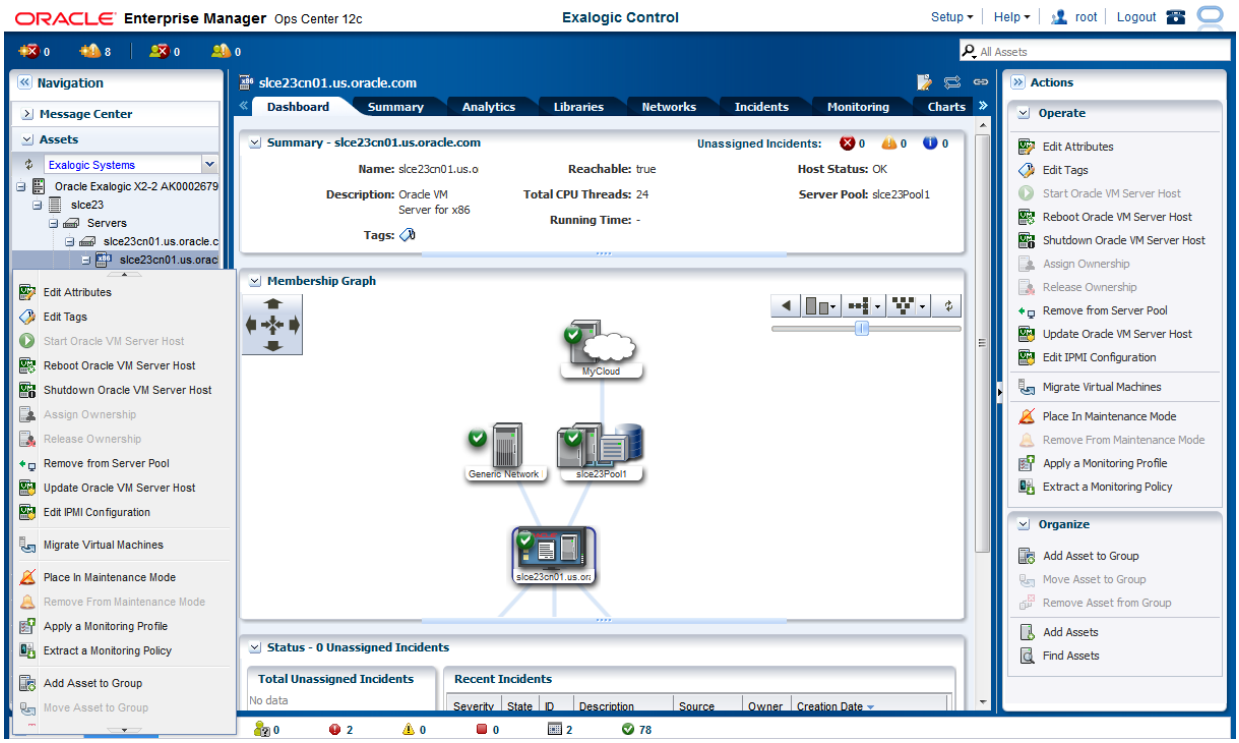
Click the **Refresh** icon at the top on the right side to refresh the Membership Graph.

See the section Establishing Your Account Preferences for more information about setting the default display preferences for Membership Graph.

Actions Pane

The Actions pane is used to start jobs based on the current selection in the Navigation pane. Your selections in the Navigation pane or center pane change the display of operations in the Actions pane. Depending on the selection of asset in the Navigation pane, the set of available actions change in the Actions pane. Right-click an asset in the Navigation pane to view the list of available action icons.

Figure A-8 Available Actions Icons for an Asset

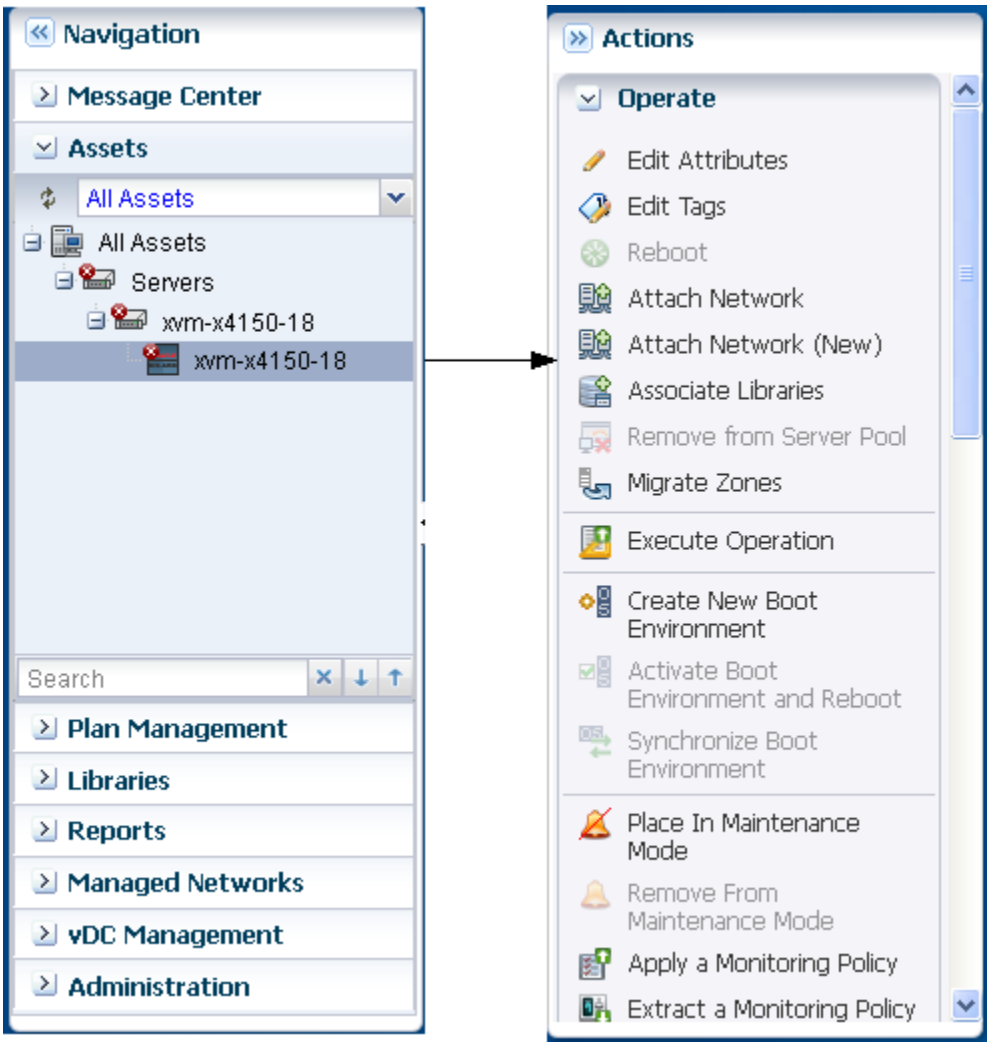


The Actions pane is further subdivided into four sections – Operate, Organize, Deploy, and Update. An action is available only when:

- it is relevant to the currently selected asset. For example, the Update OS action is only displayed if one or more operating systems is selected.
- you have the necessary role to take the action.

At any time, when you are not running commands, then you can increase the size of the center pane by hiding the Actions pane. In the Action pane's title bar, click the right double-arrow to collapse the pane. The icons for the available actions are displayed without text. Hover your mouse over the available action icons in the collapsed state to view the action names. To select another action, click its icon or expand the pane by clicking on the left double-arrow button to be able to select the names of the actions.

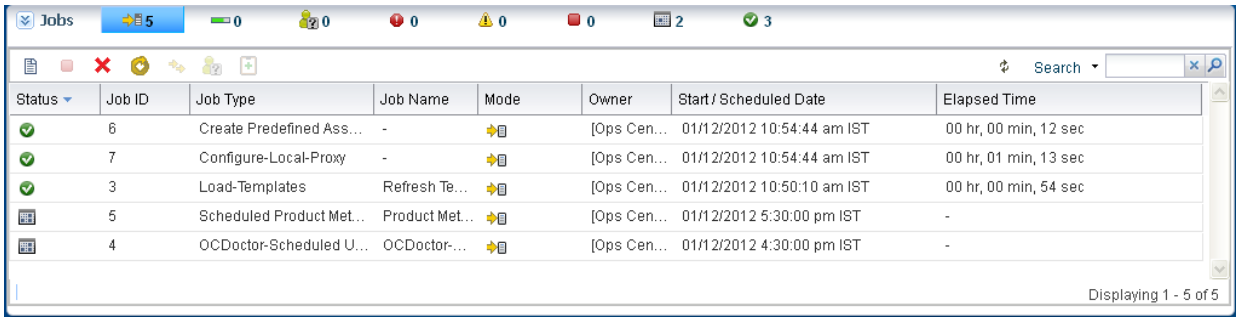
Figure A-9 Actions for an Asset



Jobs Pane

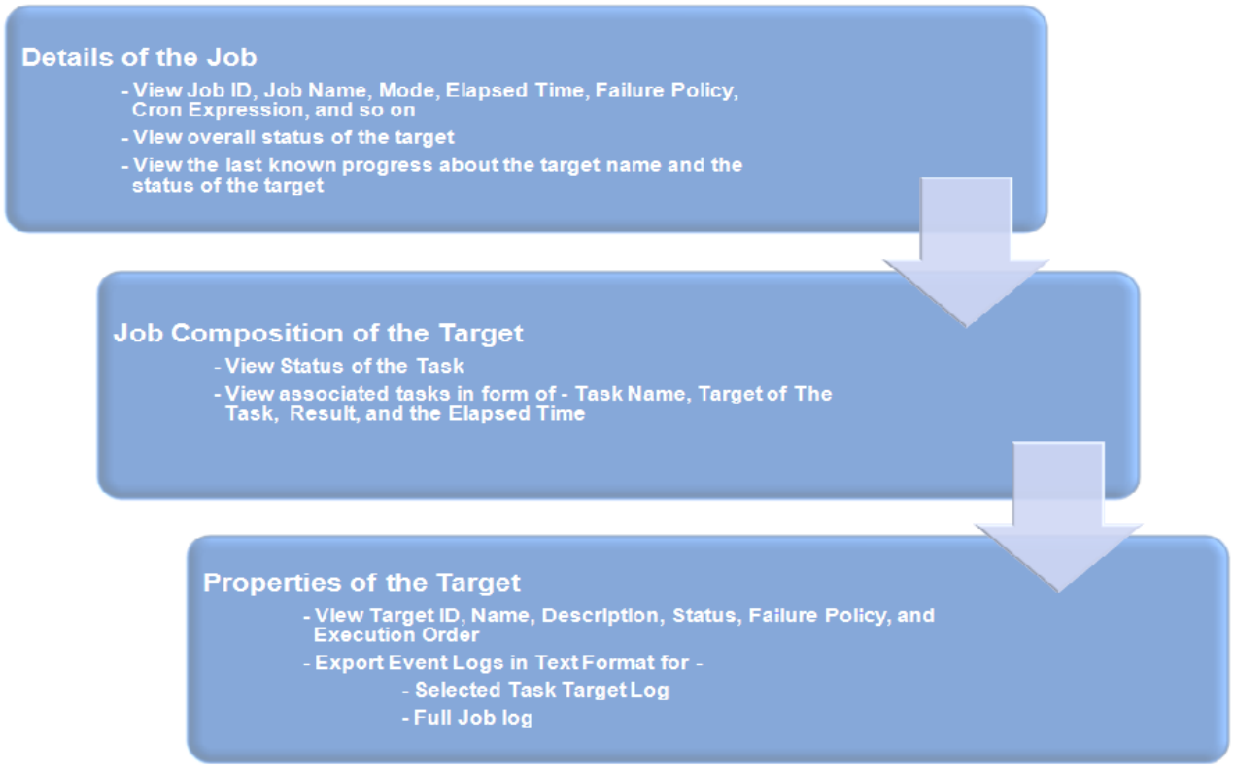
Every action creates a job. The Jobs pane at the bottom of the user interface displays a count of all jobs according to the status of each job. To see the status type, hover the mouse over the Job icon. Some jobs have many steps. To view the progress of a job, select a job, and then click the View Job Details icon.

Figure A-10 Jobs Pane



To view more information about a job, double-click a job. Click the right-arrow of Job Details to view a summarized information about Job ID, Job Name, Job Type, Mode, Failure Policy, Job Owner, and so on. You can view the Target Overall Status, Last Known Progress, and the Target Name. Double-click the target to view all the associated tasks for that job. It displays Task Name, Target of The Task, Result, and the Elapsed Time. The status of the task is displayed as an icon. Double-click the task to view the task properties, and the event logs. Exalogic Control BUI lets you export the logs of a job or a selected task target log in text format. Click the Refresh symbol at a desired point of time to refresh the user interface.

Figure A-11 Reviewing a Job



At any point, you can stop a running job, delete a job, copy a job, answer questions for a job that needs user input, or debug a job using the OCDoctor.

Some actions creates the job immediately but, in many cases, you must provide more information to specify the job. These actions start a wizard to guide you through creating a job. The last page of the wizard displays a summary of your specifications before you submit a job.

Exalogic Control BUI displays all types of jobs together. You can filter the jobs in various categories and view them. You can view the Jobs In Progress, Jobs awaiting for User Input, Failed Jobs, Partially Successful Jobs, Stopped Jobs, Scheduled Jobs, and the Successful Jobs.

The job details also includes the job Status, Job ID, Job Type, Job Name, Mode, Owner, Elapsed Time, and Start/Scheduled Date. Exalogic Control BUI also provides a search facility for jobs on these details. The search functionality lets you view result as per your search criteria. You can click the Refresh icon, to view the latest information for jobs.

The Jobs pane, when collapsed, displays the Status Icons, the Count for All Jobs, Jobs In Progress, Jobs Waiting For User Input, Jobs failed, Jobs Partially Successful, Jobs Stopped, Jobs Scheduled, and Jobs Successful.

Searching in Exalogic Control BUI

Exalogic Control BUI provides various search options, such as the following:

- In the global search field, in the upper-right corner of the user interface, you can search for any Network, Storage Library, or Asset.
- In the Navigation pane, you can search for specific assets. It highlights the first result in the asset tree for your selection, and the Dashboard tab of the center pane displays information about the searched asset. Use the up and down arrows to view the next matching asset.
- In the Navigation pane, select All Assets and click Managed Assets tab to search all assets or filter by assets type. You can further search for an asset.
- In the Jobs pane, you can search for specific jobs. Use the search function to filter the category of information you want to view.

Establishing Your Account Preferences

Exalogic Control BUI enables you to customize the user interface according to your preferences.

You can select any drawer of the Navigation pane to be displayed as the default view upon every log in. When you select assets from the Navigation pane, then you can also select the sub-option for assets to be displayed as the default view on start up. Your personal preferences overrides the preferences that were previously set for your role.

Apart from the default view preferences, you can use the Display preferences to display any specific drawer from the Navigation pane. By default, the Assets and Administration drawers cannot be hidden. When you select Assets for display, then you can also choose a default tab to display.

You can set values for Session Timeout, Console Session Timeout, Connectivity Check Interval, Table Refresh Frequency, and Job Status Popup Duration for Time Intervals.

You can also select the default display preferences for Membership Graph. You can set the display preferences for the orientation, icon size, and level of depth for the assets in Membership Graph.

The User Preferences Summary displays a summarized history of the preferences that you have selected in My Preferences. You can view your set preferences for the start page, display, time intervals, asset default tab, and Membership Graph.

B

Installing the Cloud Management API and CLI

This appendix describes how to install and configure Cloud Management API and CLI interfaces in the Exalogic Elastic Cloud environment.
It contains the following topics:

Prerequisites

The following are the prerequisites for installing Cloud Management API and CLI:

- Installation of Java Runtime Environment (JRE) or Java Development Kit (JDK) version 1.6 or higher, necessary for the platform on which the Cloud Management API and the CLI will be installed
- Access to the VM that hosts the Enterprise Controller component of Exalogic Control

Installation

This section contains the following topics:

Installing Cloud Management API

The Cloud Web Service is automatically installed in the VM that hosts the Enterprise Controller component of Exalogic Control during the Exalogic Control installation. You do not need to install the API separately on the VM that hosts the Enterprise Controller.

Installing Java Client API

The Java Client API is delivered as a separate package with Oracle Enterprise Manager Ops Center. You can install the Java Client API as a standalone package on a different machine with connection to the VM that hosts the Enterprise Controller component of Exalogic Control.

If you are installing this client API on a machine running Oracle Solaris, you must install the **ORCL-sysman-iaas-api.pkg** package. If you are installing this client API on

a machine running Oracle Linux, you must install the **orcl-sysman-iaas-api.rpm** package.

You must copy these packages from the VM that hosts the Enterprise Controller component of Exalogic Control (`/var/opt/orcl/orcl-sysman-oes-template-config/dvd/Linux_i686/Product/components/packages/` or `/var/opt/orcl/orcl-sysman-oes-template-config/dvd/SunOS_i386/Product/components/packages/`) to the remote machine on which you are installing the Java Client API.

You can install the Java client API on the remote machine as follows:

1. Log in to the remote machine as the `root` user.
2. Move to the directory in which you copied the Java Client API package from the VM hosting the Enterprise Controller.
3. Install the package as follows:

   On Solaris: `#pkgadd -d ORCLsysman-iaas-api`

   On Linux: `#rpm -i orcl-sysman-iaas-api*.rpm`

> **Note:**
>
> The files from the API jar package are stored in the `/opt/oracle/iaas/iaas-java-api` directory. Before using the API jar file, set the `JAVA_HOME` environment variable and ensure that it is included your `PATH` environment variable.

Installing Cloud Management CLI

The Cloud Management CLI is delivered as a separate package with Oracle Enterprise Manager Ops Center. You can install this package as a standalone package on a different machine with connection to the VM that hosts the Enterprise Controller component of Exalogic Control.

If you are installing the CLI on a machine running Oracle Solaris, you must install the **ORCL-sysman-iaas-cli.pkg** package. If you are installing this CLI on a machine running Oracle Linux, you must install the **orcl-sysman-iaas-cli.rpm** package.

You must copy these packages from the VM that hosts the Enterprise Controller component of Exalogic Control (`/var/opt/orcl/orcl-sysman-oes-template-config/dvd/Linux_i686/Product/components/packages/` or `/var/opt/orcl/orcl-sysman-oes-template-config/dvd/SunOS_i386/Product/components/packages/`) to the remote machine on which you are installing the IaaS CLI client.

You can install the CLI client on the remote machine as follows:

1. Log in to the remote machine as the `root` user.
2. Move to the directory in which you copied the IaaS CLI packages from the VM that hosts the Enterprise Controller component of Exalogic Control.
3. Install the package as follows:

   On Solaris: `#pkgadd -d ORCLsysman-iaas-cli`

   On Linux: `#rpm -i orcl-sysman-iaas-cli*.rpm`

> **Note:**
>
> The files from the package are stored in the `/opt/oracle/iaas/cli` directory. The user running the CLI commands must have permissions to access this directory.

4. Run the following commands:

   ```
   #cd /opt/oracle/iaas/cli/bin
   ```

   ```
   #export IAAS_HOME=/opt/oracle/iaas/cli
   ```

   ```
   #export JAVA_HOME=<location_of_Java>
   ```

5. As a Cloud Admin user or Cloud User, set the base URL to the location of Enterprise Controller, as follows:

   ```
   ./akm-describe-accounts --base-url https://<EC_URL>/--user root --
   password-file ~/root.pwd.file
   ```

   `EC_URL` is the location of Enterprise Controller. You can set the variable `IAAS_BASE_URL` to avoid typing the location when running additional commands.

   ```
   #export IAAS_BASE_URL=https://<EC_URL>/
   ```

C

Exalogic vDC Management Using IaaS CLI: Basic Tasks

This appendix describes how to perform basic tasks related to Exalogic Virtual Data Center (vDC) management using the Infrastructure As A Service (IaaS) command-line interface. It discusses how to create and use vDC resources. For information on deleting such resources, see Deleting Exalogic vDC Resources Using the IaaS CLI: Example Procedures.

> **Note:**
>
> This appendix describes some of the important tasks only. For information about all the IaaS commands, see the *Oracle Enterprise Manager Ops Center API and CLI Reference Guide*.

This appendix contains the following topics:

Overview

IaaS CLI offers the same functions and features as Cloud Management API or Java Client API. In a typical scenario, the CLI is installed on a machine outside of the Exalogic machine. This remote machine must have network access to Exalogic Control.

In this guide, the Cloud Admin user's tasks use the Browser User Interface (BUI) method, and Cloud User tasks use CLI as well as BUI.

Prerequisites

Complete the following prerequisites for using the IaaS CLI on a remote machine:

- Install the IaaS CLI client package on the remote machine, as described in Installing the Cloud Management API and CLI.
- Ensure that the remote machine, on which the CLI client is installed, can access the Exalogic Control network.
- Ensure that the IaaS user is added to Exalogic Control locally or via LDAP.

Setting Up and Administering Exalogic vDC

As the Cloud Admin user, use the Browser User Interface (BUI) of Exalogic Control to set up and administer the vDC on Exalogic, as described in Administering the Exalogic vDC and Setting Up the Infrastructure.

Creating and Managing vDC Resources

This section contains the following topics:

Overview of CLI Commands

Cloud Management CLI commands one of the following prefixes:

- `akm`

  Commands used for tasks related to access key management.

- `iaas`

  Commands used for the full set of supported cloud management tasks.

All IaaS calls are asynchronous. Each CLI command has some common options. Depending on the command prefix, the options can vary. The following table lists these options and their descriptions.

Option	Description	Required
--base-url <base_url>	Base URL of the Oracle Enterprise Manager Ops Center vServer. `https://<ochost>`	Yes
--user	User name of the cloud user.	Yes for `akm` commands only
--password-file|-p <pw_file>	Path to the file storing the password of the cloud user.	Yes for `akm` commands only
--access-key-file|-a <access_key_file>	Path to the file storing the access key.	Yes for `iaas` commands only
--help|-h	Explains the command usage and its arguments.	No
--header|-H	Adds a header row to the output.	No
--sep <separator>	Specifies a column separator character. The default separator is TAB.	No
--xml	Displays the output in XML format. The default output is in tabular format.	No
--verbose|-v	Starts the command in verbose mode.	No
--debug|-D	Starts the command in debug mode.	No

Getting Started

Before you can use the vDC infrastructure as an Iaas user, you must create an access key, which is used for authenticating cloud web service requests for an account.

User management is provided by a central service within Exalogic Control. The central entry point for cloud API or CLI requests is the cloud web service. The cloud web service handles the authentication and authorization of the calling user, and it manages access keys.

An access key consists of an ID, a private key, a public key, and an authentication target account. The private key is used on the client side to sign HTTP requests. The cloud web service uses the public key to verify incoming HTTP requests and to authenticate the calling user. After creation, the private key is provided to the user. The Cloud User is responsible for limiting access to the private key.

Run the following commands to get started:

1. View Accounts' information for a cloud user by using the **akm-describe-accounts** command, as in the following example:

   ```
   ./akm-describe-accounts --base-url https://<localhost>/ --user
   testuser --password-file ~/pwd.file
   ```

   This command displays the user name of the specified cloud user along with the account ID, the name, and the description of each account available for that cloud user.

2. Create an access key by using the **akm-create-access-key** command, as in the following example:

   ```
   ./akm-create-access-key --base-url https://<localhost>/ --user User1
   --password-file ~/pwd.file --account ACC-4b83b85e-592c-45a1-
   ba71-3bd0774fbd0e --access-key-file ~/ak.file
   ```

   This command creates an access key and returns an access key identifier, such as `AK_32`.

   > **Note:**
   >
   > You can obtain the account ID from the output of the **akm-describe-accounts** command.

3. View information about an access key by using the **akm-describe-access-keys** command, as in the following example:

   ```
   akm-describe-access-keys --base-url https://<localhost>/ --user User1
   --password-file ~/pwd.file
   ```

Describing vDC Capabilities

You can describe the vDC capabilities for an account by using the iaas-describe-vdc-capabilities command, as in the following example:

```
./iaas-describe-vdc-capabilities --base-url https://<localhost>/ -a
ak.file -H
```

This command displays information about the following:

- Virtualization type, such as OVM
- Virtualization version, such as OVM 3.0.2
- Processor architecture
- Distribution group support

Example Procedure: Importing Server Templates

To import a Server Template, complete the following steps:

1. Ensure that the Server Template is on a network that is available to the VM hosting the Enterprise Controller.
2. Register a Server Template from URL by using the **iaas-create-server-template-from-url** command, as in the following example:

   ```
   ./iaas-create-server-template-from-url --base-url https://<localhost>/
   --access-key-file ak.file --name myST --url http://
   <host_name_of_ZFS_appliance>/common/images/OVM.tar.gz
   ```

   Upon success, this command returns the Server Template ID and loads the Server Template in an account. For example, `TMPL-aaaaaaa8-bbb4-ccc4-ddd4-eeeeeeeeee03`.

3. View information about the newly registered Server Template by using the **iaas-describe-server-templates** command, as in the following example:

   ```
   ./iaas-describe-server-templates --base-url https://<localhost>/ --
   access-key-file ak.file -H
   ```

   Upon success, this command returns a list of the Server Templates available in the account corresponding to the access key file. Each of the Server Templates listed contains the ID, name, description, status, size, and image type. The output also indicates whether the Server Template is public or read-only.

4. Create a tag on the newly registered Server Template by using the **iaas-create-tags** command, as in the following example:

   ```
   ./iaas-create-tags --base-url https://<localhost>/ -a ak.file --id
   TMPL-aaaaaaa8-bbb4-ccc4-ddd4-eeeeeeeeee03 --tags myTag=myTagValue
   ```

   This command adds or overwrites tags to the specified resource (Server Template, in this example). The command does not return any value.

   > **Note:**
   >
   > A tag is a key/value pair that can be attached to a resource. The key and the value are strings. All entities in Enterprise Manager Ops Center are managed resources that can be tagged in a resource using their tag names or tag values. Tags are used to bind user-specific information to entities.

5. View information about the Server Template that has an associated tag. Run the **iaas-describe-tags** command, as in the following example:

   ```
   ./iaas-describe-tags --base-url https://<localhost>/ -a ak.file --ids
   TMPL-aaaaaaa8-bbb4-ccc4-ddd4-eeeeeeeeee03
   ```

   This command returns the name and value of the tag associated with the specified Server Template.

Example Procedure: Creating Key Pairs for an Account

Complete the following tasks:

1. Create a key pair for an account, and store the private key in a specified key file by using the **iaas-create-key-pair** command, as in the following example:

   ```
   ./iaas-create-key-pair --base-url https://<localhost>/ -a ak.file --
   key-name myKeyPair --key-file myKeyFile
   ```

   This command returns the ID of the key pair. For example, `dx a9:60:cb:88:4a:42:2d:c5:d4:f1:23:63:64:54:d9:0a:e0:c5:a5:9e`.

2. View information about key pairs in an account by using the **iaas-describe-key-pairs** command, as in the following example:

   ```
   ./iaas-describe-key-pairs --base-url https://<localhost>/ -a ak.file
   ```

   This command returns the list of existing key pairs and their attributes. If no key pairs are found, the response is empty.

Example Procedure: Creating Private Virtual Networks

Complete the following tasks:

1. Create a private virtual network (vNet) for the account by using the **iaas-create-vnet** command, as in the following example:

   ```
   ./iaas-create-vnet --base-url https://<localhost>/ --access-key-file
   ak.file --name vnet1
   ```

   Upon success, this command returns an ID of the newly created vNet. For example, `VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad`.

2. View information about the newly created private vNet by using the **iaas-describe-vnets** command, as in the following example:

   ```
   ./iaas-describe-vnets --base-url https://<localhost>/ -a ak.file --ids
   VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad
   ```

   This command returns information about the specified private vNet. The output includes the name, ID, status, and IP address.

3. Create a tag on the newly created vNet by using the **iaas-create-tags** command, as in the following example:

   ```
   ./iaas-create-tags --base-url https://<localhost>/ -a ak.file --id
   VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad --tags myTag=myTagValue
   ```

   This command adds or overwrites tags to the specified resource (vNet, in this example). The command does not return any value.

   > **Note:**
   >
   > A tag is a key/value pair that can be attached to a resource. The key and the value are strings. All entities in Enterprise Manager Ops Center are managed resources that can be tagged in a resource using their tag names or tag values. Tags are used to bind user-specific information to entities.

4. View information about the newly created vNet with its associated tag. Run the **iaas-describe-tags** command, as in the following example:

   ```
   ./iaas-describe-tags --base-url https://<localhost>/ -a ak.file --ids
   VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad
   ```

   This command returns the name and value of the newly created tag associated with the vNet.

Example Procedure: Allocating IP Addresses for vServers

You must allocate a set of IP addresses from the private virtual network (vNet) for vServers to be created later.

Complete the following tasks:

1. Allocate a set of IP addresses from the private vNet by using the **iaas-allocate-ip-addresses** command, as in the following example:

```
./iaas-allocate-ip-addresses --base-url https://<localhost>/ -a
ak.file --vnet VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad --num 2
```

This command allocates two IP addresses from the private vNet `VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad`. For example, `192.168.0.2` and `192.168.0.3`. You can assign one of these IP addresses when creating a vServer at a later time.

2. View information about the newly allocated IP addresses by using the **iaas-describe-ip-addresses** command, as in the following example:

```
./iaas-describe-ip-addresses --base-url https://<localhost>/ -a
ak.file --filters VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad
```

This command returns the IP addresses allocated from the specified vNet.

Example Procedure: Creating Distribution Groups

Distribution groups are necessary for anti-affinity scaling in an Oracle VM Server pool.

Complete the following tasks:

1. Create a distribution group by using the **iaas-create-distribution-group** command, as in the following example:

```
./iaas-create-distribution-group --base-url https://<localhost>/ -a
ak.file --name Dept1-distgrp1
```

This command returns the ID of the distribution group. For example, `DG-068ae84c-d0fc-406d-aa37-0be4f88d411c`.

2. View information about the newly created distribution group by using the **iaas-describe-distribution-groups** command, as in the following example:

```
./iaas-describe-distribution-groups --base-url https://<localhost>/ -a
~/ak.file --ids DG-068ae84c-d0fc-406d-aa37-0be4f88d411c -H
```

This command returns the attributes of the specified distribution group, which is empty at this time.

Example Procedure: Creating Volumes

Complete the following tasks:

1. Create a volume by using the **iaas-create-volume** command, as in the following example:

```
./iaas-create-volume --base-url https://<localhost>/ --access-key-file
ak.file --name Volume1 --size 16
```

This command creates a Volume named `Volume1` of size `16` GB. It returns the ID of the newly created volume. For example, `VOL-f23a8ba1-ec55-4159-bbdf-de220d18a1c4`.

2. View information about the newly created volume by using the **iaas-describe-volumes** command, as in the following example:

```
./iaas-describe-volumes --base-url https://<localhost>/ -a ak.file --
ids VOL-f23a8ba1-ec55-4159-bbdf-de220d18a1c4
```

This command returns the ID of the specified volume, its name, status, and size.

> **Note:**
>
> After creating a volume, you must partition the volume using `fdisk` and create a file system using `mkfs` on the first vServer that is created with the volume. On the vServer, the volume appears as a disk (`/dev/hdX` or `/dev/xvdX`). After the volume is partitioned and file system created, you must mount it using the `/etc/fstab` file on the vServer to make the file system accessible.

Example Procedure: Importing Volumes

If you wish to import a volume from an existing URL instead of creating a new volume, complete the following tasks:

1. Import a volume by using the **iaas-import-volume** command, as in the following example:

   ```
   ./iaas-import-volume --base-url https://<localhost>/ -a ak.file --name
   Volume2 --url http://ovm.oracle.com/volume-image/volume.img
   ```

   This command returns the ID of the volume that was imported as `Volume2`. For example, `VOL-e9afec8c-dbe2-4e03-8561-15716650b81e`.

2. View information about `Volume2` by using the **iaas-describe-volumes** command, as in the following example:

   ```
   ./iaas-describe-volumes --base-url https://<localhost>/ -a ak.file --
   ids VOL-e9afec8c-dbe2-4e03-8561-15716650b81e
   ```

   This command returns the ID of the specified volume, its name, status, and size.

Example Procedure: Creating vServers

You can create vServers using one of the following commands:

- `iaas-run-vservers`

  This command enables you to create and start multiple vServers at once. For more information, see Example Procedure: Creating Multiple vServers.

- `iaas-run-vserver`

  This command enables you to create and start a single vServer. For more information, see Example Procedure: Creating a Single vServer.

When you create multiple vServers, only automatic IP address assignment is possible, and a suffix is added to the vServer name for each vServer. When you create a single vServer, you can assign a static IP address. In this case, a suffix is not added to the name of the vServer.

Example Procedure: Creating Multiple vServers

1. Create two vServers by using the **iaas-run-vservers** command, as in the following example:

   ```
   ./iaas-run-vservers --base-url https://<localhost>/ -a ~/ak.file --
   vnets VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad --key-name myKeyPair
   ```

```
--name myvserver --num 2 --server-template-id TMPL-aaaaaaa8-bbb4-ccc4-
ddd4-eeeeeeeeee03 --dist-group DG-068ae84c-d0fc-406d-aa37-0be4f88d411c
--vserver-type 457
```

In this example, you are creating two vServers with the following attributes:

- Name: `myvserver`
- Private vNet to be associated with: `VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad`

> **Note:**
>
> In this example, the vServers are associated with a single private vNet. However, you can associate a vServer with multiple vNets.

- Server Template to be used: `TMPL-aaaaaaa8-bbb4-ccc4-ddd4-eeeeeeeeee03`
- Distribution group to be associated with: `DG-068ae84c-d0fc-406d-aa37-0be4f88d411c`

This command creates the specified vServers and returns their ID. For example, `VSRV-d6800889-f59b-4798-a57d-3f9f31b0cf1c` and `VSRV-d6500889-f59b-4567-a65g-3f9f31b0se1d`. The vServers are created and started. The IP addresses are assigned to the vServers automatically.

2. View information about the newly created vServer `vserver1` by using the **iaas-describe-vservers** command, as in the following example:

   ```
   ./iaas-describe-vservers --base-url https://<localhost>/ -a ak.file --
   ids VSRV-d6800889-f59b-4798-a57d-3f9f31b0cf1c VSRV-d6500889-f59b-4567-
   a65g-3f9f31b0se1d
   ```

   Alternatively, you can view information about all vServers by using the **iaas-describe-vservers** command, as in the following example:

   ```
   ./iaas-describe-vservers --base-url https://<localhost>/ -a ak.file
   ```

3. Create a tag on the newly created vServers by using the **iaas-create-tags** command, as in the following example:

   ```
   ./iaas-create-tags --base-url https://<localhost>/ -a ak.file --id
   VSRV-d6800889-f59b-4798-a57d-3f9f31b0cf1c VSRV-d6500889-f59b-4567-
   a65g-3f9f31b0se1d --tags myTag=myTagValue
   ```

   This command adds or overwrites tags to the specified resource (vServer, in this example). The command does not return any value.

   > **Note:**
   >
   > A tag is a key/value pair that can be attached to a resource. The key and the value are strings. All entities in Enterprise Manager Ops Center are managed resources that can be tagged in a resource using their tag names or tag values. Tags are used to bind user-specific information to entities.

4. View information about the newly created vServers with their associated tag. Run the **iaas-describe-tags** command, as in the following example:

   ```
   ./iaas-describe-tags --base-url https://<localhost>/ -a ak.file --ids
   VSRV-d6800889-f59b-4798-a57d-3f9f31b0cf1c VSRV-d6500889-f59b-4567-
   a65g-3f9f31b0se1d
   ```

   This command returns the name and value of the newly created tag associated with the vServers.

Example Procedure: Creating a Single vServer

To create a single vServer, complete the following steps:

1. Create a vServer by using the **iaas-run-vserver** command, as in the following example:

   ```
   ./iaas-run-vserver --base-url https://<localhost>/ -a ~/ak.file --
   vnets VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad --key-name myKeyPair
   --name vserver1 --server-template-id TMPL-aaaaaaa8-bbb4-ccc4-ddd4-
   eeeeeeeeee03 --dist-group DG-068ae84c-d0fc-406d-aa37-0be4f88d411c --
   ip-addresses 192.168.0.2 --vserver-type 457
   ```

   In this example, you are creating a vServer with the following attributes:

   - Name: `vserver1`
   - Private vNet to be associated with: `VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad`

     > **Note:**
     >
     > In this example, the vServer is associated with a single private vNet. However, you can associate a vServer with multiple vNets.

   - Server Template to be used: `TMPL-aaaaaaa8-bbb4-ccc4-ddd4-eeeeeeeeee03`
   - Distribution group to be associated with: `DG-068ae84c-d0fc-406d-aa37-0be4f88d411c`
   - IP address to use: `192.168.0.2`

   This command creates the specified vServer and returns its ID. For example, `VSRV-0fb57293-347c-4717-96ef-6dd23154596f`. The vServer is created and started.

2. View information about the newly created vServer `vserver1` by using the **iaas-describe-vservers** command, as in the following example:

   ```
   ./iaas-describe-vservers --base-url https://<localhost>/ -a ak.file --
   ids VSRV-0fb57293-347c-4717-96ef-6dd23154596f
   ```

3. Create a tag on the newly created vServer by using the **iaas-create-tags** command, as in the following example:

   ```
   ./iaas-create-tags --base-url https://<localhost>/ -a ak.file --id
   VSRV-0fb57293-347c-4717-96ef-6dd23154596f --tags myTag=myTagValue
   ```

   This command adds or overwrites tags to the specified resource (vServer, in this example). The command does not return any value.

> **Note:**
>
> A tag is a key/value pair that can be attached to a resource. The key and the value are strings. All entities in Enterprise Manager Ops Center are managed resources that can be tagged in a resource using their tag names or tag values. Tags are used to bind user-specific information to entities.

4. View information about the newly created vServer with its associated tag. Run the **iaas-describe-tags** command, as in the following example:

   ```
   ./iaas-describe-tags --base-url https://<localhost>/ -a ak.file --ids
   VSRV-0fb57293-347c-4717-96ef-6dd23154596f
   ```

   This command returns the name and value of the newly created tag associated with the vServer.

Example Procedure: Stopping a vServer

To stop a running vServer, run the **iaas-stop-vservers** command, as in the following example:

```
./iaas-stop-vservers --base-url https://<localhost>/ -a ak.file --vserver-
ids VSRV-0fb57293-347c-4717-96ef-6dd23154596f
```

This command stops the specified vServer. It does not return any value.

Example Procedure: Attaching Volume to vServer

To attach a volume to a vServer, complete the following steps:

1. Ensure that the vServer is stopped.
2. Attach a volume to the vServer by using the **iaas-attach-volumes-to-vserver** command, as in the following example:

   ```
   ./iaas-attach-volumes-to-vserver --base-url https://<localhost>/ -a ~/
   ak.file -vserver-id VSRV-0fb57293-347c-4717-96ef-6dd23154596f --
   volume-ids VOL-f23a8ba1-ec55-4159-bbdf-de220d18a1c4
   ```

   This command attaches the specified volume to the specified vServer. It does not return any value. To verify that a vServer is stopped, check the status of the vserver using the `iaas-describe-vservers` command.
3. After attaching the volume to the vServer, start the vServer by using the **iaas-start-vservers** command, as in the following example:

   ```
   ./iaas-start-vservers --base-url https://<localhost>/ -a ak.file --
   vserver-ids VSRV-0fb57293-347c-4717-96ef-6dd23154596f
   ```

   This command starts the specified vServer. It does not return any value.

Example Procedure: Detaching Volume from vServer

If you wish to detach a volume from a vServer, complete the following steps:

1. Ensure that the vServer is stopped.

2. Detach a volume from the vServer by using the **iaas-detach-volumes-from-vserver** command, as in the following example:

   ```
   ./iaas-detach-volumes-from-vserver --base-url https://<localhost>/ -a
   ~/ak.file -vserver-id VSRV-0fb57293-347c-4717-96ef-6dd23154596f --
   volume-ids VOL-f23a8ba1-ec55-4159-bbdf-de220d18a1c4
   ```

   This command detaches the specified volume from the specified vServer. It does not return any value.

3. After detaching the volume from the vServer, start the vServer by using the **iaas-start-vservers** command, as in the following example:

   ```
   ./iaas-start-vservers --base-url https://<localhost>/ -a ak.file --
   vserver-ids VSRV-0fb57293-347c-4717-96ef-6dd23154596f
   ```

   This command starts the specified vServer. It does not return any value.

Example Procedure: Creating Snapshot from Volume

To create a Snapshot from a volume, complete the following steps:

1. Before creating a Snapshot from a volume, verify that the volume is not attached to any vServers. If the volume is attached to a vServer, you must stop the vServer by using the **iaas-stop-vservers** command, as in the following example:

   ```
   ./iaas-stop-vservers --base-url https://<localhost>/ -a ak.file --
   vserver-ids VSRV-0fb57293-347c-4717-96ef-6dd23154596f
   ```

   This command stops the specified vServer. It does not return any value.

2. Create a Snapshot from a volume by using the **iaas-create-snapshot** command, as in the following example:

   ```
   ./iaas-create-snapshot --base-url https://<localhost>/ -a ak.file --
   volume-id VOL-f23a8ba1-ec55-4159-bbdf-de220d18a1c4 --name mySnapshot
   ```

   This command creates a Snapshot from the specified volume. It returns the Snapshot ID. For example, `SNAP-7a717e39-fe67-4573-a93d-889b3446176b`.

3. View information about the newly created Snapshot `mySnapshot` by using the **iaas-describe-snapshots** command, as in the following example:

   ```
   ./iaas-describe-snapshots --base-url https://<localhost>/ -a ak.file -
   H
   ```

   This command returns a list of all Snapshots in the account.

4. After creating a Snapshot, start the vServer by using the **iaas-start-vservers** command, as in the following example:

   ```
   ./iaas-start-vservers --base-url https://<localhost>/ -a ak.file --
   vserver-ids VSRV-0fb57293-347c-4717-96ef-6dd23154596f
   ```

   This command starts the specified vServer. It does not return any value.

Example Procedure: Creating Volume from Snapshot

To create a volume from Snapshot, complete the following tasks:

1. Create a volume by using the **iaas-create-volume** command, as in the following example:

```
./iaas-create-volume --base-url https://<localhost>/ --access-key-file
ak.file --name Volume2 --snapshot-id SNAP-7a717e39-fe67-4573-
a93d-889b3446176b
```

This command creates a volume named Volume2 from the specified Snapshot. It returns the Volume ID. For example, `VOL-g23a8ba1-ec55-4159-bbdf-de220d18a1b7`.

2. View information about the newly created volume by using the **iaas-describe-volumes** command, as in the following example:

```
./iaas-describe-volumes --base-url https://<localhost>/ -a ak.file --
ids VOL-g23a8ba1-ec55-4159-bbdf-de220d18a1b7
```

This command returns the ID of the specified volume, its name, status, and size.

D

Deleting Exalogic vDC Resources Using the IaaS CLI: Example Procedures

This appendix provides example procedures for deleting vDC resources using the IaaS command-line interface (CLI). For an overview of the Iaas CLI, see Overview of CLI Commands. For information about CLI commands that are not described here, see the *Oracle Enterprise Manager Ops Center API and CLI Reference Guide*. This appendix contains the following sections:

Before You Begin

Before performing the tasks described in this appendix, you must have created vDC resources, as described in Exalogic vDC Management Using IaaS CLI: Basic Tasks.

Example Procedure: Deleting a Server Template

To delete a Server Template, complete the following steps:

1. Run the following command:

   ```
   ./iaas-delete-server-template --base-url https://<localhost>/ --
   access-key-file ak.file --server-template-id TMPL-aaaaaaa8-bbb4-ccc4-
   ddd4-eeeeeeeeee03
   ```

   The command deletes the specified Server Template. The command does not return any value; only the command prompt is returned.

2. Verify the deletion of the Server Template by running the **iaas-describe-server-templates** command, as in the following example:

   ```
   ./iaas-describe-server-templates --base-url https://<localhost>/ --
   access-key-file ak.file --ids TMPL-aaaaaaa8-bbb4-ccc4-ddd4-
   eeeeeeeeee03
   ```

Verify that the deleted Server Template is not listed in the output of this command.

Example Procedure: Deleting Tags

To delete a tag from a specified resource (for example, private vNet), complete the following steps:

1. Run the following command:

   ```
   ./iaas-delete-tags --base-url https://<localhost>/ -a ak.file --id
   VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad --tags myTag
   ```

   The command deletes the specified tag from the specified resource. The command does not return any value; only the command prompt is returned.

2. Verify the deletion by running the **iaas-describe-tags** command, as in the following example:

   ```
   ./iaas-describe-tags --base-url https://<localhost>/ -a ak.file --ids
   VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad
   ```

   This command should not return the tag that was initially associated with the specified private vNet.

Example Procedure: Terminating vServers

To stop and delete one or more vServers, complete the following steps:

1. Run the following command:

   ```
   ./iaas-terminate-vservers --base-url https://<localhost>/ -a ~/ak.file
   --vserver-ids VSRV-d6800889-f59b-4798-a57d-3f9f31b0cf1c VSRV-d6500889-
   f59b-4567-a65g-3f9f31b0se1d --force
   ```

   The command stops and deletes the specified vServers.

2. Verify the deletion by running the **iaas-describe-vservers** command, as in the following example:

   ```
   ./iaas-describe-vservers --base-url https://<localhost>/ -a ak.file --
   ids VSRV-d6800889-f59b-4798-a57d-3f9f31b0cf1c VSRV-d6500889-f59b-4567-
   a65g-3f9f31b0se1d
   ```

   This command should return empty output, as the specified vServers are deleted.

Example Procedure: Deleting a Private vNet

Before deleting a private vNet, ensure that it is not associated with any running vServers.

To delete a private vNet, complete the following steps:

1. Run the following command:

   ```
   ./iaas-delete-vnet --base-url https://<localhost>/ -a ak.file --vnet
   VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad
   ```

   The command deletes the specified private vNet. The command does not return any value.

2. Verify the deletion by running the **iaas-describe-vnets** command, as in the following example:

   ```
   ./iaas-describe-vnets --base-url https://<localhost>/ -a ak.file --ids
   VNET-350c9c3f-0ee5-41be-917e-ebbaed0fa4ad
   ```

   This command should return empty output, as the specified private vNet is deleted.

Example Procedure: Deleting a Distribution Group

Before deleting a distribution group, ensure that it does not have any running vServers.

To delete a distribution group, complete the following steps:

1. Run the following command:

   ```
   ./iaas-delete-distribution-group --base-url https://<localhost>/ --
   access-key-file ak.file --distribution-group-id DG-068ae84c-d0fc-406d-
   aa37-0be4f88d411c
   ```

   The command deletes the specified distribution group. The command does not return any value; only the command prompt is displayed.

2. Verify the deletion by running the **iaas-describe-distribution-groups** command, as in the following example:

   ```
   ./iaas-describe-distribution-groups --base-url https://<localhost>/ -a
   ~/ak.file --ids DG-068ae84c-d0fc-406d-aa37-0be4f88d411c -H
   ```

   This command should return empty output, as the specified distribution group is deleted.

Example Procedure: Deleting a Volume

Before deleting a volume, ensure that it is not attached to any running vServers.

To delete a volume, complete the following steps:

1. Run the following command:

   ```
   ./iaas-delete-volume --base-url https://<localhost>/ -a ak.file --
   volume-id VOL-f23a8ba1-ec55-4159-bbdf-de220d18a1c4
   ```

   The command deletes the specified volume. The command does not return any value; only the command prompt is displayed.

2. Verify the deletion by running the **iaas-describe-volumes** command, as in the following example:

   ```
   ./iaas-describe-volumes --base-url https://<localhost>/ -a ak.file --
   ids VOL-f23a8ba1-ec55-4159-bbdf-de220d18a1c4
   ```

   This command should return empty output, as the specified volume is deleted.

Example Procedure: Deleting a Snapshot

To delete a Snapshot, complete the following steps:

1. Run the following command:

   ```
   ./iaas-delete-snapshot --base-url https://<localhost>/ -a ak.file --
   snapshot-id SNAP-7a717e39-fe67-4573-a93d-889b3446176b
   ```

   The command deletes the specified Snapshot. The command does not return any value; only the command prompt is displayed.

2. Verify the deletion by running the **iaas-describe-snapshots** command, as in the following example:

   ```
   ./iaas-describe-snapshots --base-url https://<localhost>/ -a ak.file
   --ids SNAP-7a717e39-fe67-4573-a93d-889b3446176b
   ```

   In the output, you should not see the Snapshot `SNAP-7a717e39-fe67-4573-a93d-889b3446176b`, which is deleted.

Example Procedure: Deleting a Key Pair

To delete a key pair, complete the following steps:

1. Run the following command:

   ```
   ./iaas-delete-key-pair --base-url https://<localhost>/ --access-key-
   file ak.file --key-name myKeyPair
   ```

   The command deletes the specified key pair. The command does not return any value; only the command prompt is displayed.

2. Verify the deletion by running the **iaas-describe-key-pairs** command, as in the following example:

   ```
   ./iaas-describe-key-pairs --base-url https://<localhost>/ -a ak.file
   ```

   This command returns the list of all key pairs in your Account. In the output, you should not see the key pair that you deleted.

Example Procedure: Deleting an Access Key

To delete an access key, complete the following steps:

1. Run the following command:

   ```
   ./akm-delete-access-key --base-url https://<localhost>/ --user User1
   --password-file ~/pwd.file AK_32
   ```

   The command deletes the specified access key. The command does not return any value; only the command prompt is displayed.

2. Verify the deletion by running the **iaas-describe-access-keys** command, as in the following example:

   ```
   ./akm-describe-access-keys --base-url https://<localhost>/ --user
   User1 --password-file ~/pwd.file
   ```

   This command returns the list of all access keys in your Account. In the output, you should not see the access key that you deleted.

E

Customizing Guest vServer Images

This appendix describes how to customize guest vServer images based on your specific requirements. The tasks described in this appendix are optional.
It contains the following sections:

Important Notes Before You Begin

Read the following notes before you start modifying Exalogic VM images:

- *Do not* modify any of the Exalogic Control VM images. If you wish to modify them, contact Oracle Support.
- *Do not* modify templates that are already imported and registered in the Oracle VM (OVM) repository. If you wish to modify a Exalogic guest base template, you should start with the `tgz` file.

  Alternatively, copy artifacts from the Exalogic OVM repository to a host outside Exalogic, as follows:

  > **Note:**
  >
  > This procedure uses example names. You should use the appropriate template names and paths.

  1. Identify the `vm.cfg` file corresponding to the template being modified. For example, run the following command:

     ```
     grep Exalogic_Base_Template /OVS/Repositories/*/Templates/*/vm.cfg
     ```

     The example output is as follows:

     ```
     /OVS/Repositories/0004fb0000030000986539c7d4fe8a92/Templates/
     0004fb00001400000f5e855e6e5dbb32/vm.cfg:OVM_simple_name =
     'Exalogic_Base_Template'
     ```

  2. Find the disks corresponding to the `vm.cfg` file as follows:

```
grep disk /OVS/Repositories/0004fb0000030000986539c7d4fe8a92/
Templates/0004fb00001400000f5e855e6e5dbb32/vm.cfg
```

The example output is as follows:

```
disk = ['file:/OVS/Repositories/0004fb0000030000986539c7d4fe8a92/
VirtualDisks/4d84c59e-fbb3-4c3b-92c7-
fe7bd591ae38.img,hda,w','file:/OVS/Repositories/
0004fb0000030000986539c7d4fe8a92/VirtualDisks/b0ed1dee-7323-420d-
b7f2-364d1ec70194.img,hdb,w']
```

3. Copy all of these artifacts to a host outside Exalogic.
4. Edit the `vm.cfg` file, as necessary.
5. Edit the template using `modifyjeos` or manually.
6. Create a tar file after making all modifications.

- To modify a VM image, you can use the `modifyjeos` command, which is included in one of the RPMs packaged with the VM image. Alternatively, you can modify the VM image manually.

> **Note:**
>
> `modifyjeos` does not work for LVM-based templates.

When using `modifyjeos` to customize a VM image, ensure that the VM is not running. In addition, back up the `vm.cfg` and `System.img` files before running `modifyjeos`.

To locate the configuration file for a VM (`vm.cfg`), complete the following steps:

1. Determine the ID of the VM as follows:

   a. Log in to Exalogic Control web interface.

   b. Under **Assets** in the navigation pane on the left, select your Exalogic machine (for example, `Oracle Exalogic X2-2AK00026800`), and expand **Servers**. Under **Servers**, identify the VM whose ID you want to collect. See the **Virtual Machine Display Name**, which is different from the **Virtual Machine Name**.

   c. After determining the VM, click the **Summary** tab on the Center pane. This pane displays both **Virtual Machine Name** and **Virtual Machine Display Name**. An example Virtual Machine Name is `0004fb000006000021e3117abee1b9df`.
2. Use SSH to connect to any of the compute nodes in the server pool `exelpool1` that hosts the VM.
3. After logging in, move to the following directory:

   ```
   # cd /OVS/Repositories/*/VirtualMachines/<ID>
   ```

   For example,

   ```
   # cd /OVS/Repositories/*/VirtualMachines/
   0004fb0000060000dcda55f345cc8ec3
   ```

This directory contains a single file named `vm.cfg` that contains the configuration information for the VM.

Adding RPMs

This section describes how to add RPMs to an existing Exalogic VM image. It contains the following topics:

- Adding RPMs Using modifyjeos
- Adding RPMs Manually

Adding RPMs Using modifyjeos

> **Note:**
>
> `modifyjeos` does not work for LVM-based templates. For such templates, use the manual method described in Adding RPMs Manually.

To add RPMs using `modifyjeos`, complete the following steps:

1. Add the names of the new RPMs in a list file, such as `addrpms.lst`. In this file, you should list each new RPM in a separate line.
2. Ensure that all of the new RPMs are in a single directory, such as `rpms`.
3. Run the following command to add the new RPMs:

   ```
   # modifyjeos -f System.img -a <path_to_addrpms.lst> -m <path_to_rpms> -
   nogpg
   ```

   In this command, `<path_to_addrpms.lst>` is the path to the location of the `addrpms.lst` file, and `<path_to_rpms>` is the path to the directory that contains the RPMs. The `-nogpg` option eliminates signature check on the RPMs.

Adding RPMs Manually

To add an RPM manually, complete the following steps:

1. Ensure that the VM is not running.
2. Mount the `System.img` file, as described in Mounting System.img.
3. Run the following command to install the RPM on the mounted image:

   ```
   # chroot <path_to_mounted_System.img> /bin/bash -c 'rpm -i
   <path_to_rpm>'
   ```

   In this command, `<path_to_mounted_System.img>` is the path to the mount location, and `<path_to_rpm>` is the path to the RPM file. Ensure the RPM file is in the mount directory of `System.img`.
4. Unmount the `System.img` file, as described in Unmounting System.img.

Removing RPMs

This section describes how to remove RPMs from an existing Exalogic VM image. It contains the following topics:

- Removing RPMs Using modifyjeos
- Removing RPMs Manually

> **Note:**
>
> Exercise caution when removing RPMs from an existing Exalogic VM image. The Exalogic VM image contains application artifacts and critical files in addition to the operating system.

RPMs That Must Not be Modified or Removed

Do not modify or delete the following RPMs outside of an Exalogic release, a patch set update (PSU), or a patch:

- compat-dapl
- compat-dapl-devel
- dapl
- dapl-debuginfo
- dapl-devel
- dapl-devel-static
- dapl-utils
- ib-bonding
- ib-bonding-debuginfo
- ibacm
- ibsim
- ibsim-debuginfo
- ibutils
- infiniband-diags
- infiniband-diags-guest
- initscripts
- kernel
- kernel-devel
- kernel-ib
- kernel-ib-devel
- kernel-uek

- kernel-uek-devel
- kernel-uek-firmware
- kernel-uek-headers
- kmod-ovmapi-uek
- libibcm
- libibcm-debuginfo
- libibcm-devel
- libibmad
- libibmad-debuginfo
- libibmad-devel
- libibmad-static
- libibumad
- libibumad-debuginfo
- libibumad-devel
- libibumad-static
- libibverbs
- libibverbs-debuginfo
- libibverbs-devel
- libibverbs-devel-static
- libibverbs-utils
- libmlx4
- libmlx4-debuginfo
- libmlx4-devel
- libovmapi
- librdmacm
- librdmacm-debuginfo
- librdmacm-devel
- librdmacm-utils
- libsdp
- libsdp-debuginfo
- libsdp-devel
- mpi-selector
- mpitests_openmpi_gcc
- mstflint
- nfs-utils
- ofed-docs
- ofed-scripts

- openmpi_gcc
- opensm
- opensm-debuginfo
- opensm-devel
- opensm-libs
- opensm-static
- ovm-template-config
- ovm-template-config-authentication
- ovm-template-config-datetime
- ovm-template-config-firewall
- ovm-template-config-network
- ovm-template-config-ovmm
- ovm-template-config-selinux
- ovmd
- perftest
- qperf
- qperf-debuginfo
- rds-tools
- sdpnetstat
- srptools
- xenstoreprovider

Key RPMs That Are Necessary for vServers to Work

Do not delete the following RPMs, which are necessary for vServers to function in the Exalogic environment. However, you can update these RPMs to latest versions (through yum update, for example) outside of Exalogic releases, PSUs, and patches, to address security or other issues. The following RPMs depend on other RPMs on the system. So exercise caution when removing any RPMs for minimizing or hardening the system.

- compat-db
- glibc
- glibc-common
- glibc-devel
- expect
- glibc-headers
- keepalived
- libaio-devel
- nscd

- pexpect
- python-simplejson
- sysstat

Yum Exclusion List

Use the following exclusion list in `/etc/yum.conf` for updating the vServer. This exclusion list includes all the RPMs listed in RPMs That Must Not be Modified or Removed.

```
exclude=compat-dapl* dapl* ib-bonding* ibacm* ibsim* ibutils* infiniband-diags*
initscripts* kernel* kmod-ovmapi-uek* libibcm* libibmad* libibumad* libibverbs*
libmlx4* libovmapi* librdmacm* libsdp* mpi-selector* mpitests_openmpi_gcc*
mstflint* nfs-utils* ofed* openmpi_gcc* opensm* ovm-template-config* ovmd*
perftest* qperf* rds-tools* sdpnetstat* srptools* xenstoreprovider*
```

Removing RPMs Using modifyjeos

> **Note:**
>
> `modifyjeos` does not work for LVM-based templates. For such templates, use the manual method described in Removing RPMs Manually.

To remove RPMs by using `modifyjeos`, complete the following steps:

1. Add the names of the RPMs (the ones you want to remove) in a list file, such as `removerpms.lst`. In this file, you must list each RPM in a separate line. Do not add the `.rpm` extension to the names of the RPMs.
2. Run the following command to remove the RPMs:

   ```
   # modifyjeos -f System.img -e <path_to_removerpms.lst>
   ```

   In this command, `<path_to_removerpms.lst>` is the path to the location of the `removerpms.lst` file.

Removing RPMs Manually

To remove an RPM manually, complete the following steps:

1. Ensure that the VM is not running.
2. Mount the `System.img` file, as described in Mounting System.img.
3. Run the following command to remove the RPM from the mounted image:

   ```
   # chroot <path_to_mounted_System.img> /bin/bash -c 'rpm -e <rpmname>'
   ```

   In this command, `<path_to_mounted_System.img>` is the path to the mount location, and `<rpmname>` is the name of the RPM that you want to remove.
4. Unmount the `System.img` file, as described in Unmounting System.img.

Adding Disks

This section describes how to add a disk to an existing Exalogic VM image. It contains the following topics:

- Example Procedure: Adding a 10 GB Disk Using modifyjeos
- Example Procedure: Adding a 10 GB Disk Manually

Example Procedure: Adding a 10 GB Disk Using modifyjeos

To add a 10 GB disk, such as `ExtraDisk.img`, to an Exalogic VM image using `modifyjeos`, complete the following steps:

> **Note:**
>
> This procedure applies to guest vServers created by using version 2.0.4.x.x (or earlier) of the Exalogic Guest Base Template. For guest vServers creating using v2.0.6.x.x of the Exalogic Guest Base Template, you can manage disks by using LVM commands, as described in Managing LVM Partitions on Guest vServers.

1. Run the following command to add a 10 GB disk:

   ```
   # modifyjeos -f System.img -P ExtraDisk.img 10240 <mount_location>
   ```

   In this command, `<mount_location>` is the path to the location at which you want to mount the new disk (`ExtraDisk.img`) on `System.img`.

2. Ensure that the `vm.cfg` file for the VM references the new disk as follows:

   ```
   disk = ['file:<Path_to_System.img>,hda,w',
           'file:<Path_to_ExtraDisk.img>,hdb,w']
   ```

   In this command, `<path_to_System.img>` is the path to the mount location, and `<path_to_ExtraDisk.img>` is the path to `ExtraDisk.img` mounted on `System.img`.

Example Procedure: Adding a 10 GB Disk Manually

To manually add a 10 GB disk, such as `ExtraDisk.img`, to an Exalogic VM image, complete the following steps:

> **Note:**
>
> This procedure applies to guest vServers created by using version 2.0.4.x.x (or earlier) of the Exalogic Guest Base Template. For guest vServers creating using v2.0.6.x.x of the Exalogic Guest Base Template, you can manage disks by using LVM commands, as described in Managing LVM Partitions on Guest vServers.

1. Ensure that the VM is not running.
2. Create a blank disk as follows:

   ```
   # dd if=/dev/zero of=ExtraDisk.img bs=1M count=10240
   ```

   This example uses a 10 GB disk. You can create a disk of your desired size.
3. Edit the vm.cfg file to include the new disk:

   ```
   # vi vm.cfg
   ...
   disk = ['file:<Path_to_System.img>,hda,w',
           'file:<Path_to_ExtraDisk.img>,hdb,w']...
   ```

   In this command, `<path_to_System.img>` is the path to the mount location, and `<path_to_ExtraDisk.img>` is the path to `ExtraDisk.img` mounted on `System.img`.
4. Start the VM.
5. Find the device with the new disk by running the following command:

   ```
   # cat /proc/partitions
   ```

   This example procedure uses the `/dev/xvdb` device.
6. Make the disk `ext3` as follows:

   ```
   # mkfs.ext3 /dev/xvdb
   ```
7. Edit the `/etc/fstab` file to add the mount point for the disk:

   ```
   /dev/xvdb     /<mount_point>     ext3     defaults     1 2
   ```
8. Mount the disk either by restarting the VM or by running the following command:

   ```
   # mount -t ext3 /dev/xvdb <mount_point>
   ```

Example Procedure: Modifying Current Disk Size

This section describes how to modify the current disk size using `modifyjeos`. In the following example, the default disk size (4 GB) is modified to 10 GB:

```
# modifyjeos -f System.img -I 10240
```

> **Note:**
>
> This procedure applies to guest vServers created by using version 2.0.4.x.x (or earlier) of the Exalogic Guest Base Template. For guest vServers creating using v2.0.6.x.x of the Exalogic Guest Base Template, you can manage disks by using LVM commands, as described in Managing LVM Partitions on Guest vServers.

Modifying Swap

This section describes how to modify the swap size (in MB). It contains the following topics:

- Example Procedure: Modifying Swap Size Using modifyjeos

- Example Procedure: Adding Swap Manually

Example Procedure: Modifying Swap Size Using modifyjeos

You can modify the current swap size using `modifyjeos`. In the following example, the default swap size (512 MB) is modified to 1 GB:

> **Note:**
>
> This procedure applies to guest vServers created by using version 2.0.4.x.x (or earlier) of the Exalogic Guest Base Template. For guest vServers creating using v2.0.6.x.x of the Exalogic Guest Base Template, you can manage disks by using LVM commands, as described in Managing LVM Partitions on Guest vServers.

```
# modifyjeos -f System.img -S 1024
```

When you start the VM after modifying the swap size, it may start without any active swap. To fix this problem, complete the following steps:

1. Verify the label by running the following command:

   ```
   # cat /etc/fstab
   ```

2. Look for a line starting with `LABEL=SWAP` and make sure that it is `LABEL=SWAP-VM`. If not, change it by editing the `/etc/fstab` file.
3. Reboot the VM. The swap should become active.

Example Procedure: Adding Swap Manually

To add swap manually (for example, 1 GB), complete the following steps:

> **Note:**
>
> This procedure applies to guest vServers created by using version 2.0.4.x.x (or earlier) of the Exalogic Guest Base Template. For guest vServers creating using v2.0.6.x.x of the Exalogic Guest Base Template, you can manage disks by using LVM commands, as described in Managing LVM Partitions on Guest vServers.

1. Create a swap file as follows:

   ```
   # dd if=/dev/zero of=<path_to_swap_file> bs=1M count=1024
   ```

   This example uses a 1 GB swap. You can create a swap file of your desired size.
2. Run the following commands:

   ```
   # mkswap <path_to_swap_file>
   ```

   ```
   # swapon <path_to_swap_file>
   ```

3. Add an entry to the `/etc/fstab` file to persist the swap file in the case of reboots:

```
<path_to_swap_file>     swap     swap     defaults     0 0
```

Mounting and Unmounting System.img

This section describes how to mount and unmount `System.img` for Logical Volume Manager (LVM) vServers and non-LVM vServers

Mounting System.img

This section describes how to mount `System.img` for LVM-based vServers and non-LVM vServers.

Mounting System.img for Non-LVM vServers

You can mount `System.img` and directly modify the mounted files. To mount `System.img`, do the following:

> **Note:**
>
> This procedure applies to guest vServers created by using version 2.0.4.x.x (or earlier) of the Exalogic Guest Base Template. For guest vServers creating using v2.0.6.x.x of the Exalogic Guest Base Template, you can manage disks by using LVM commands, as described in Mounting System.img for LVM-Based vServers.

1. Create a script, say `MountSystemImg.sh`, containing the following code:

```
#!/bin/sh
# Export for later, i.e. during unmount
export LOOP=`losetup -f`
export SYSTEMIMG=/mount/point
# Create temporary mount directory
mkdir -p $SYSTEMIMG
# Create a loop for the system image
losetup $LOOP System.img
kpartx -a $LOOP
mount /dev/mapper/`basename $LOOP`p2 $SYSTEMIMG
#Change directory to the mounted image
cd $SYSTEMIMG
```

2. Run `MountSystemImg.sh` from the directory containing the `System.img` file.

Mounting System.img for LVM-Based vServers

You can mount `System.img` and directly modify the mounted files. To mount `System.img`, do the following:

1. Ensure LVM is installed on the mount host.
2. Create a script, say `MountSystemImg.sh`, containing the following code:

```
#!/bin/sh

export LOOP=`losetup -f`
```

```
losetup $LOOP path_to_system.img
kpartx -a $LOOP
lvm pvscan
lvm vgchange -ay
mount /dev/mapper/VolGroup00-LogVol00 mount_location
```

This example uses the default template disk name `VolGroup00`. *`mount_location`* is the path to the location at which you want to mount the image.

3. If you are mounting the image on an Oracle VM Server node, there may be a name conflict with `VolGroup00`. You must temporarily rename the host by adding the following command to the MountSystemImg.sh script, in the line after `#!/bin/sh`:

   ```
   lvm vgrename VolGroup00 VolGroupTmp1
   ```

4. Run `MountSystemImg.sh` from the directory containing the `System.img` file.

Unmounting System.img

This section describes how to unmount Exalogic VM images for LVM-based vServers and non-LVM vServers.

Unmounting System.img for Non-LVM vServers

To unmount `System.img` for non-LVM vServers, do the following:

> **Note:**
>
> This procedure applies to guest vServers created by using version 2.0.4.x.x (or earlier) of the Exalogic Guest Base Template. For guest vServers creating using v2.0.6.x.x of the Exalogic Guest Base Template, you can manage disks by using LVM commands, as described in Unmounting System.img for LVM-Based vServers.

1. Create a script, say `UnmountSystemImg.sh`, containing the following code:

   ```
   #!/bin/sh
   # Assuming $LOOP and $SYSTEMIMG exist from a previous run of MountSystemImg.sh
   umount $SYSTEMIMG
   kpartx -d $LOOP
   losetup -d $LOOP
   ```

2. Run `UnmountSystemImg.sh` from the directory containing the `System.img` file.

Unmounting System.img for LVM-Based vServers

To unmount `System.img` for LVM-based vServers, do the following:

1. Create a script, say `UnmountSystemImg.sh`, containing the following code:

   ```
   #!/bin/sh

   # Assuming $LOOP exists from a previous run of MountSystemImg.sh
   umount /mount/point
   lvm vgchange -an
   ```

```
kpartx -d $LOOP
losetup -d $LOOP
```

2. If you renamed the template disk in step 3 of Mounting System.img for LVM-Based vServers, add the following command to the UnmountSystemImg.sh script, in the line after `#!/bin/sh`:

   ```
   lvm vgrename VolGroupTmp1 VolGroup00
   ```

3. Run `UnmountSystemImg.sh` from the directory containing the `System.img` file.

F

Managing LVM Partitions on Guest vServers

The local disks on guest vServers that you create by using the EECS 2.0.6.x.x Guest Base Template use Logical Volume Manager (LVM)-based partitioning, which gives the administrator more flexibility in allocating disk space to applications and users. This appendix provides a few example procedures for managing the LVM-based partitions on guest vServers.
This appendix contains the following sections:

- Increasing the Size of the Root Partition
- Creating a /tmp Partition
- Increasing the Swap Space

For more information about using LVM to manage partitions, go to:

`http://www.howtoforge.com/linux_lvm`

Increasing the Size of the Root Partition

This section describes how to increase the size of the default logical volume `VolGroup00-LogVol00` mounted at the root "`/`" directory of a guest vServer.

> **Note:**
>
> The procedure described here is relevant to vServers created by using the EECS 2.0.6.x.x Guest Base Template. *Do not* use this procedure to modify the disks of vServers creating using a Guest Base Template that is earlier than EECS version 2.0.6.0.0.

1. Create a volume (say, 100 GB), as described in Creating Volumes.
2. Attach the volume to the vServer, for which you want to modify the size of the root partition, as described in Attaching Volumes to a vServer.
3. Log in, as the `root` user, to the vServer.
4. Examine the current partitioning by running the following commands:

   ```
   # df -h
   ```

   The following is an example of the output of this command:

   ```
   Filesystem                      Size  Used Avail Use% Mounted on
   /dev/mapper/VolGroup00-LogVol00  5.1G  3.3G  1.6G  68% /
   /dev/xvda1                       99M   23M   71M  25% /boot
   tmpfs                           4.0G     0  4.0G   0% /dev/shm
   ```

5. Examine the available physical volumes on the vServer by running the following command:

```
# cat /proc/partitions
major minor  #blocks  name

 202        0    6145024 xvda
 202        1     104391 xvda1
 202        2    6040440 xvda2
 253        0    5505024 dm-0
 253        1     524288 dm-1
 202       16  104857600 xvdb
```

`/dev/xvdb` is the newly attached volume.

6. Run the `fdisk` command, as shown in the following example:

> **Note:**
>
> The user input required at various stages while running the `fdisk` command is indicated by **`bold`** text.

```
# fdisk /dev/xvdb
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF
disklabel
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previous
content won't be recoverable.

The number of cylinders for this disk is set to 13054.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
(e.g., DOS FDISK, OS/2 FDISK)
Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)
Command (m for help): p

Disk /dev/xvdb: 107.3 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

    Device Boot      Start         End      Blocks   Id  System

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-13054, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-13054, default 13054):
Using default value 13054

Command (m for help): t
Selected partition 1
Hex code (type L to list codes): 8e
```

```
Changed system type of partition 1 to 8e (Linux LVM)

Command (m for help): p

Disk /dev/xvdb: 107.3 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/xvdb1               1       13054   104856223+  8e  Linux LVM

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

7. Create a physical volume:

```
# pvcreate /dev/xvdb1
  Writing physical volume data to disk "/dev/xvdb1"
  Physical volume "/dev/xvdb1" successfully created
```

8. Extend the volume group `VolGroup00` with the physical volume `/dev/xvdb1`:

```
# vgextend VolGroup00 /dev/xvdb1
  Volume group "VolGroup00" successfully extended
```

9. Extend the logical volume `LogVol00`:

```
# lvextend -l +100%FREE /dev/VolGroup00/LogVol00
  Extending logical volume LogVol00 to 105.22 GB
  Logical volume LogVol00 successfully resized
```

10. Resize the file system:

```
# resize2fs /dev/VolGroup00/LogVol00
resize2fs 1.39 (29-May-2006)
Filesystem at /dev/VolGroup00/LogVol00 is mounted on /; on-line resizing required
Performing an on-line resize of /dev/VolGroup00/LogVol00 to 27582464 (4k) blocks.
The filesystem on /dev/VolGroup00/LogVol00 is now 27582464 blocks long.
```

11. Check whether the root partition of the guest vServer has the updated size, by running the `df -h` command as shown in the following example:

```
# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
                      102G  3.3G   94G   4% /
/dev/xvda1             99M   23M   71M  25% /boot
tmpfs                 4.0G     0  4.0G   0% /dev/shm
```

Creating a /tmp Partition

This section describes how to creating a `/tmp` partition on a guest vServer by using a logical volume.

> **Note:**
>
> The procedure described here is relevant to vServers created by using the EECS 2.0.6.x.x Guest Base Template. *Do not* use this procedure to modify the disks of vServers creating using a Guest Base Template that is earlier than EECS version 2.0.6.0.0.

1. Create a volume, as described in Creating Volumes.
2. Attach the volume to the vServer for which you want to modify the `/tmp` size, as described in Attaching Volumes to a vServer.
3. Log in, as the `root` user, to the vServer for which you want to modify the `/tmp` size, and verify whether the volume is attached.

```
# cat /proc/partitions
major minor  #blocks  name
202        0    6145024 xvda
202        1     104391 xvda1
202        2    6040440 xvda2
253        0    5505024 dm-0
253        1     524288 dm-1
202       16    16777216 xvdb
```

   The output should contain a line similar to the last line (`xvdb` in this example), which is the partition corresponding to the volume that you attached.

4. Format the partition as an LVM-type partition.

> **Note:**
>
> The user input required at various stages in this step is indicated by **`bold`** text.

```
# fdisk /dev/xvdb
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF
disklabel
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previouscontent won't
be recoverable.
Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): n
Command action
e   extended
p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-522, default 1): Press Enter
Last cylinder or +size or +sizeM or +sizeK (1-522, default 522): Press Enter
Using default value 522

Command (m for help): t
Hex code (type L to list codes): 8e
Changed system type of partition 2 to 8e (Linux LVM)
```

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

5. Show the current physical volumes on the disk:

```
# pvdisplay
--- Physical volume ---
PV Name               /dev/xvda2
VG Name               VolGroup00
PV Size               5.76 GB / not usable 10.87 MB
Allocatable           yes (but full)
PE Size (KByte)       32768
Total PE              184
Free PE               0
Allocated PE          184
PV UUID               SaMlQo-Ct55-8IhX-ZEaf-rT4X-gISK-XEwdvc
```

6. Create a physical volume using the new partition:

```
# pvcreate /dev/xvdb1
  Writing physical volume data to disk "/dev/xvdb1"
  Physical volume "/dev/xvdb1" successfully created
```

7. Verify the new physical volume:

```
# pvdisplay
--- Physical volume ---
PV Name               /dev/xvdb1
VG Name
PV Size               15.99 GB / not usable 2.74 MB
Allocatable           yes (but full)
PE Size (KByte)       4096
Total PE              4094
Free PE               0
Allocated PE          4094
PV UUID               o2HIse-1gsv-lzdk-YEC1-rXKq-4Fkg-8RN2rL

--- Physical volume ---
PV Name               /dev/xvda2
VG Name               VolGroup00
PV Size               5.76 GB / not usable 10.87 MB
Allocatable           yes (but full)
PE Size (KByte)       32768
Total PE              184
Free PE               0
Allocated PE          184
PV UUID               SaMlQo-Ct55-8IhX-ZEaf-rT4X-gISK-XEwdvc
```

8. Create a volume group for the new physical volume:

```
# vgcreate myVolGroup /dev/xvdb1
```

9. Activate the new volume group:

```
# vgchange -a y myVolGroup
```

10. Create a logical volume:

```
# lvcreate -l 4094 myVolGroup -n myVolGroup-LogVol00
```

11. Change the type of the new logical volume to `ext3`:

```
# mkfs.ext3 /dev/myVolGroup/myVolGroup-LogVol00
```

12. Mount the logical volume to `/tmp`:

```
# mount /dev/myVolGroup/myVolGroup-LogVol00  /tmp/
```

13. Verify whether `/tmp` has the modified space.

```
# df -h
Filesystem                                    Size  Used Avail Use% Mounted on
/dev/mapper/VolGroup00-LogVol00               5.1G  3.3G  1.6G  68% /
/dev/xvda1                                     99M   23M   71M  25% /boot
tmpfs                                         2.0G     0  2.0G   0% /dev/shm
/dev/mapper/myVolGroup-myVolGroup-LogVol00     16G  173M   15G   2% /tmp
```

Increasing the Swap Space

This section describes how to increase the swap space on a guest vServer by using LVM commands.

> **Note:**
>
> The procedure described here is relevant to vServers created by using the EECS 2.0.6.x.x Guest Base Template. *Do not* use this procedure to modify the disks of vServers creating using a Guest Base Template that is earlier than EECS version 2.0.6.0.0.

1. Create a volume as described in Creating Volumes.
2. Attach the volume to the vServer for which you want to modify the swap space, as described in Attaching Volumes to a vServer.
3. Log in, as the `root` user, to the vServer for which you want to modify the swap space, and verify whether the volume is attached.
4. Format the partition as an LVM-type partition.

```
# fdisk /dev/xvdc
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF
disklabel
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previouscontent won't
be recoverable.
Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): n
Command action
e   extended
p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-261, default 1): Press Enter
Last cylinder or +size or +sizeM or +sizeK (1-261, default 261): Press Enter
Using default value 261

Command (m for help): t
Hex code (type L to list codes): 8e
Changed system type of partition 2 to 8e (Linux LVM)
```

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource
busy.
The kernel still uses the old table.
The new table will be used at the next reboot.
Syncing disks.
```

5. Create a physical volume for the partition:

```
# pvcreate /dev/xvdc1
```

6. Add the newly formatted disk to the existing volume group:

```
# vgextend myVolGroup /dev/xvdc1
```

7. Create a logical volume:

```
# lvcreate -l 511 myVolGroup -n myVolGroup-LogVol01
```

8. Format the logical volume for swap use:

```
# mkswap /dev/myVolGroup/myVolGroup-LogVol01
```

9. Enable swap:

```
# swapon /dev/myVolGroup/myVolGroup-LogVol01
```

10. Verify the updated swap space by either using the `top` command, or by examining the `/proc/swaps` file as shown in the following example:

```
]# cat /proc/swaps
Filename Type Size Used Priority
/dev/mapper/VolGroup00-LogVol01 partition 524280 0 -1
/dev/mapper/myVolGroup-myVolGroup--LogVol01 partition 2093048 0 -2
```

G

Creating Server Templates from vServers

This appendix describes how to create a server template from an existing vServer using Exalogic Control, Oracle VM Manager (OVMM), and Oracle Linux commands. This appendix contains the following sections:

Before You Begin

Note:

- Do not use this procedure if you are running Exalogic Elastic Cloud Software 2.0.6.4.x. The recommended and supported way to create a template from a vServer on EECS 2.0.6.4.x is by using EKIT, as described in the following MOS document: Exalogic Kinetic Infrastructure Tools (EKIT): Set of scripts that provide common reusable command line infrastructure actions for Exalogic virtual platforms
- EKIT is also highly recommended and supported for EECS 2.0.6.3.x and earlier releases.
- If you are familiar with Oracle Exalogic Control, Oracle VM Manager, and Oracle Linux system administration, you may perform the following procedure for EECS 2.0.6.3.x and earlier releases.
- Before you try to create a server template from a running vServer, ensure that you have customized the vServer to the desired configuration by adding or removing RPM packages, attaching and configuring storage volumes, modifying swap space, configuring Linux Volume Manager, and so on.

  For information about adding disks, increasing disk size, or modifying swap space on an existing vServer, see Customizing Guest vServer Images.

Creating a vServer Template

To create a vServer template from an existing vServer (for example, `pwtest`), do the following:

1. Stop the vServer as described in Stopping vServers.
2. Log in to the OVMM web interface as the `root` user and do the following:

> **Note:**
>
> - In this procedure, you use OVMM to clone and start a vServer. Unless explicitly documented (as in this appendix), do not use OVMM to create a vServer or perform any lifecycle operations on a vServer. Use only Exalogic Control to manage vServers.
> - The steps in this procedure are based on the OVMM web interface of Oracle VM release 3.2, which is included in Exalogic Elastic Cloud Software 2.0.6.x.x. If you are at Exalogic Elastic Cloud Software 2.0.4.x.x (or a lower release), the corresponding Oracle VM release would be 3.0.3, and the OVMM web interface may be different from that described here.

a. Select the **Servers and VMs** tab.

b. Expand **Server Pools** in the navigation pane on the left, and select the server pool displayed there.

c. In the tool bar of the main display pane, change the **Perspective** to **Virtual Machines**.

   A list of all the VMs is displayed.

d. Look for the vServer that you stopped in step 1. The status of the VM would be **Stopped**.

e. Right-click on the VM, and from the resulting context menu, select **Clone or Move**.

   The Clone or Move Virtual Machine wizard starts.

f. Leave the **Create a clone of this VM** option selected, and click **Next**.

g. On the next screen, do the following:

   i. Leave the **Clone to a Virtual Machine** option selected.

   ii. Leave the **Clone Count** value at 1.

   iii. Enter a name for the clone (for example, `pw-test2`), and enter a description.

   iv. Click **OK**.

   Wait for the OVMM job to finish. The job may take a few minutes, depending on the size of the virtual disks in the VM being cloned.

   OVMM assigns the new vServer (`pw-test2`) to one of the available servers in the pool.

h. Select the new VM, right-click, and select **Start**.

i. Expand the row corresponding to the new VM by double-clicking in the first column.

   In the resulting pane, look for the **ID** (for example, `0004fb000006000030c6ec27dd5a2327`). This is the UUID of the VM. Note the UUID for later use.

> **Note:**
>
> In this procedure, this ID is referenced as `VM_CLONE_UUID`.

3. After the clone VM (`pw-test2`) starts, log in as `root` to the Oracle VM Server node that hosts the VM (`slce02cn02` in this example).

   View a list of the VMs running on the node, by running the following command:

   ```
   [root@slce02cn02 ~]#xm list
   ```

   This command displays output, as in the following example:

   ```
   Name                                        ID  Mem  VCPUs    State   Time(s)
   0004fb00000600009c75583293d01d04            1   4096   2       -b---- 139169.3
   0004fb000006000030c6ec27dd5a2327            24  4096   1       -b----    36.8
   Domain-0                                    0   2002   24       r----- 115451.5
   ```

   Log in to the VM (`pw-test2`) by using the `xm console <ID>` command, where `<ID>` is the ID of the VM, which has `<VM_CLONE_UUID>` as its name. For example, run the `xm console 24` command on `slce02cn02`. This command displays output, as in the following example:

   ```
   Oracle Linux Server release 5.6
   Kernel 2.6.32-200.21.2.el5uek on an x86_64

   pw-test login: root
   Password:
   Last login: Thu May 24 12:35:35 on ttyS0
   [root@pw-test ~]#
   ```

   > **Note:**
   >
   > In the output, note that the hostname is the same as the original VM (`pw-test`). It is not the name of the clone (`pw-test2`). Further, the network interfaces initialized by `/etc/sysconfig/network-scripts/ifcfg-bond*` are also the same as the original VM. The next step unconfigures the VM, so it can be used to create a template that causes Exalogic Control to configure hostname and network scripts when a vServer is created with the template.

4. Unconfigure the clone VM (`pw-test2`), and stop the VM as follows:

   a. Edit and `/etc/sysconfig/ovmd` file and change the `INITIAL_CONFIG=no` parameter to `INITIAL_CONFIG=yes`. Save the file after making this change.

   b. Remove DNS information by running the following commands:

      ```
      cd /etc

      sed -i '/.*/d' resolv.conf
      ```

   c. Remove SSH information by running the following commands:

      ```
      rm -f /root/.ssh/*

      rm -f /etc/ssh/ssh_host*
      ```

d. Clean up the `/etc/sysconfig/network` file by running the following commands:

```
cd /etc/sysconfig

sed -i '/^GATEWAY/d' network
```

e. Clean up the `hosts` files by running the following commands:

```
cd /etc

sed -i '/localhost/!d' hosts

cd /etc/sysconfig/networking/profiles/default

sed -i '/localhost/!d' hosts
```

f. Remove network scripts by running the following commands:

```
cd /etc/sysconfig/network-scripts

rm -f ifcfg-*eth*

rm -f ifcfg-ib*

rm -f ifcfg-bond*
```

g. Remove log files, including the ones that contain information you do not want to propagate to new vServers, by running the following commands:

```
cd /var/log

rm -f messages*

rm -f ovm-template-config.log

rm -f ovm-network.log

rm -f boot.log*

rm -f cron*

rm -f maillog*

rm -f messages*

rm -f rpmpkgs*

rm -f secure*

rm -f spooler*

rm -f yum.log*
```

h. Remove kernel messages by running the following commands:

```
cd /var/log

rm -f dmesg

dmesg -c

> ovm-network.log
```

i. Edit the `/etc/modprobe.conf` file and remove the following lines (and other lines starting with `alias bond`):

```
options bonding max_bonds=11
alias bond0 bonding
alias bond1 bonding
```

Save the file after making these changes.

j. Edit the `/etc/sysconfig/hwconf` file and modify the `driver: mlx4_en` entry to `driver: mlx4_core`. Save the file after making changes.

k. Remove the Exalogic configuration file by running the following command:

```
rm -f /etc/exalogic.conf
```

l. Remove bash history by running the following commands:

```
rm -f /root/.bash_history
```

```
history -c
```

Do this in the end to avoid recording the cleanup commands.

> **Note:**
>
> Before proceeding, consider the following points:
>
> - Any storage volume that is attached to the base VM (`pw-test`) is cloned to the clone VM (`pw-test2`), including all the contents of the volume. This also applies to the template you are creating in the next step and to the vServers created from the template. Be sure to delete any unwanted files, or drop the storage volume before proceeding with template creation.
> - When creating a vServer, Exalogic Control resizes any attached storage volumes smaller than the storage size in the Server Type to the specified storage size. For example, if you have an attached volume of size 2 GB and you select a Server Type with storage size of 4 GB, the new attached volume will have the size 4 GB. There is no change to the file systems on the volume.

5. Package the template for upload into Exalogic Control as follows:

a. Log in to any Oracle VM Server node, such as `slce02cn01`, as the `root` user.

b. Create a workspace on the Sun ZFS Storage Appliance, which is included in your Exalogic machine.

The following example uses a directory in the `/export/common/images` share:

```
[root@slce02cn01 ~]# mkdir -p /u01/common/images
[root@slce02cn01 ~]# mount -t nfs slce02sn01:/export/common/images /u01/
common/images
[root@slce02cn01 ~]# mkdir /u01/common/images/pw-template
```

c. Change directory to the Oracle VM Server (OVS) repository for the VM clone and verify that you are in the correct directory:

```
[root@slce02cn01 ~]# cd /OVS/Repositories/*/VirtualMachines/<VM_CLONE_UUID>
[root@slce02cn02 0004fb000006000030c6ec27dd5a2327]# grep simple_name
vm.cfgOVM_simple_name = 'pw-test2'
```

d. Copy the configuration file to the Sun ZFS Storage Appliance workspace:

```
[root@slce02cn01 0004fb000006000030c6ec27dd5a2327]# cp vm.cfg /u01/common/
images/pw-template
```

e. Display the disk(s) used by the cloned VM:

```
[root@slce02cn01 0004fb000006000030c6ec27dd5a2327]# grep disk vm.cfg
disk = ['file:/OVS/Repositories/0004fb0000030000169d06eb2fdfcc6f/
VirtualDisks/0004fb00001200004e5b424a5f5965bf.img,hda,w', 'file:/OVS/
Repositories/0004fb0000030000169d06eb2fdfcc6f/VirtualDisks/
0004fb00001200008d2bc3496683e1c4.img,xvdb,w']
```

f. Copy the disk(s) to the Sun ZFS Storage Appliance workspace using the file name(s) displayed above:

```
[root@slce02cn01 0004fb000006000030c6ec27dd5a2327]# cp /OVS/Repositories/
0004fb0000030000169d06eb2fdfcc6f/VirtualDisks/
0004fb00001200004e5b424a5f5965bf.img /u01/common/images/pw-template/
[root@slce02cn01 0004fb000006000030c6ec27dd5a2327]# cp /OVS/Repositories/
0004fb0000030000169d06eb2fdfcc6f/VirtualDisks/
0004fb00001200008d2bc3496683e1c4.img /u01/common/images/pw-template/
```

g. Create a compressed tar file with template configuration and disk(s) as follows:

```
[root@slce02cn01 0004fb000006000030c6ec27dd5a2327]# cd /u01/common/images/pw-
template
[root@slce02cn01 pw-template]# tar zcvf pw-template.tgz *
0004fb00001200004e5b424a5f5965bf.img 0004fb00001200008d2bc3496683e1c4.img
vm.cfg
```

The resulting file is a server template ready for upload into Exalogic Control.

h. Delete the VM clone, which you no longer need. In OVMM, right-click on the VM clone, and select **Delete**. In the Delete Confirmation screen, select the virtual disk(s) used by the VM, and click **OK**.

6. If the HTTP protocol is not enabled on the Sun ZFS Storage Appliance with access to the workspace, complete the following steps:

a. Use SSH to log in to the storage node (for example, `slce02sn01`) and enable the HTTP service, as in the following example:

```
slce02sn01:> configuration services http
slce02sn01:configuration services http> enable
slce02sn01:configuration services http> show
Properties:
                <status> = online
                require_login = false
                protocols = http/https
                listen_port = 80
                https_port = 443
```

b. Verify that the workspace with the template package is accessible by HTTP.

```
slce02sn01:configuration services http> cd /
slce02sn01:> shares
slce02sn01:shares> select common
slce02sn01:shares common> get sharedav
                     sharedav = off
slce02sn01:shares common> set sharedav=ro
                     sharedav = ro (uncommitted)slce02sn01:shares common>
commit
slce02sn01:shares common> select images
slce02sn01:shares common/images> get sharedav
                     sharedav = off
slce02sn01:shares common/images> set sharedav=ro
                     sharedav = ro (uncommitted)
slce02sn01:shares common/images> commit
```

If the `sharedav` property is already set to `rw` or `ro`, you do not need to change it.

c. Log out of the Sun ZFS Storage Appliance:

```
slce02sn01: shares common/images> exit
Connection to slce02sn01 closed.
```

7. Using Exalogic Control, upload the new server template to an account as follows:

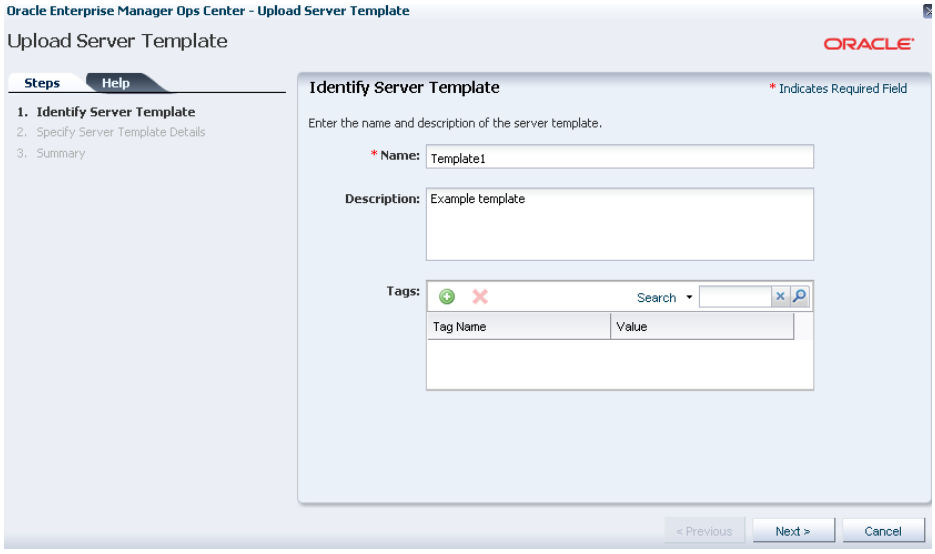
a. Log in to the Exalogic Control web interface as a `Cloud Admin` or `Cloud User`.

b. In the navigation pane on the left, click **vDC Management**. Under vDC Accounts, click the name of your Account. The vDC Account dashboard is displayed.

c. Click **Server Templates** on the top navigation bar. The server templates available in your Account are listed.

d. Under Server Templates, click the **Upload Server Template** icon. Alternatively, click **Upload Server Template** under **Operate** on the **Actions** pane. The Upload Server Template wizard is displayed, as shown in Figure G-1.

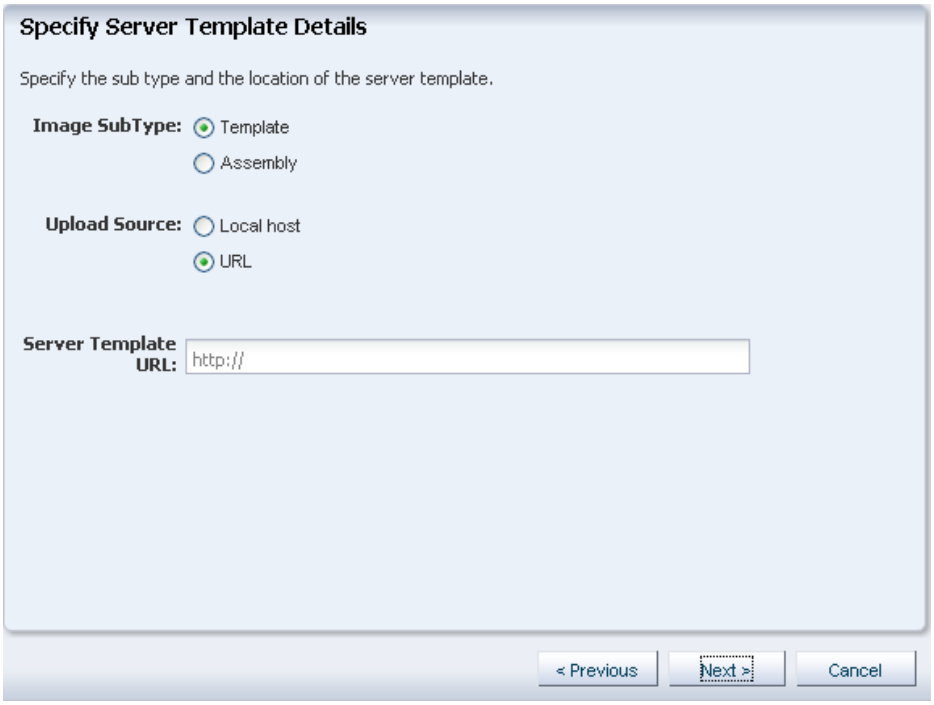
Figure G-1 Identify Server Template



e. On the Identify Server Template screen, enter a name and description for the server template to be uploaded. For example, enter `Template1` in the **Name** field. In the **Description** field, enter a brief description.You can add tags for later identification and search.

f. Click **Next**. The Specify Server Template Details screen is displayed, as shown in Figure G-2.

Figure G-2 Specify Server Template Details



g. Select the **Image SubType** option, and select **Template**.

h. Select **URL** as the **Upload Source**. To specify a URL, enter the HTTP URL for the template package created in Step 6, in the **Server Template URL** field.

   If you used the same workspace as this document, the URL will be:

   ```
   http://<zfssa-host>/shares/export/common/images/<workspace>/
   <template>.tgz
   ```

   Click **Next**.

i. Review the summary, and click **Upload** to upload the server template.

j. Click **Server Templates** on the top navigation bar. You should see the newly uploaded server template listed. You can start creating vServers based on this server template.

H

Setting Up Access to the ZFS Storage Appliance for a vServer

This section describes how to set up access to the ZFS Storage Appliance for a vServer.
The procedure to enable vServers to access ZFS shares involves the following steps:

1. Identifying the IP Address of the vServer
2. Identifying the ipmp4 Address of the Storage Appliance
3. Creating and Configuring a Share on the ZFS Storage appliance
4. Mounting the Share in the File System of the vServer

Identifying the IP Address of the vServer

To configure a vServer for accessing the storage appliance, you must know the IP address of the vServer in the `IPoIB-vserver-shared-storage` network.

> **Note:**
>
> For a vServer to be able to access ZFS shares, the `IPoIB-vserver-shared-storage` network should have been assigned to the vServer as described in step 15 of Creating vServers.

1. Log in to Exalogic Control as a `Cloud User`.
2. From the navigation pane on the left, select **vDC Management.**
3. Under vDC Accounts, expand the name of your account, and select the vServer for which you want to configure access to the storage appliance.

   The vServer dashboard is displayed.
4. Select the **Network** tab, and note the IP address of the vServer for the `IPoIB-vserver-shared-storage` network.

Identifying the ipmp4 Address of the Storage Appliance

To mount a ZFS share on the vServer, you must identify the IP address of the storage appliance on the `IPoIB-vserver-shared-storage` network, also known as the ipmp4 address.

1. SSH to the ZFS Storage Appliance as `root`.
2. Run the following command:

   ```
   storage_node> configuration net interfaces show
   ```

3. From the output of the command, note the ipmp4 address.

```
slce23sn01:> configuration net interfaces show
Interfaces:

INTERFACE   STATE    CLASS LINKS       ADDRS                LABEL
igb0        up       ip    igb0        10.244.64.60/21      igb0
igb1        offline  ip    igb1        10.244.64.61/21      igb1
ipmp1       up       ipmp  pffff_ibp1  192.168.10.15/24     ipmp1
                           pffff_ibp0
ipmp2       up       ipmp  p8001_ibp0  192.168.20.9/24      IB_IF_8001
                           p8001_ibp1
ipmp3       up       ipmp  p8002_ibp0  192.168.21.9/24      IB_IF_8002
                           p8002_ibp1
ipmp4       up       ipmp  p8005_ibp0  172.17.0.9/16        IB_IF_8005
                           p8005_ibp1
p8001_ibp0  up       ip    p8001_ibp0  0.0.0.0/8            ibp0.8001
p8001_ibp1  up       ip    p8001_ibp1  0.0.0.0/8            ibp1.8001
p8002_ibp0  up       ip    p8002_ibp0  0.0.0.0/8            ibp0.8002
p8002_ibp1  up       ip    p8002_ibp1  0.0.0.0/8            ibp1.8002
p8005_ibp0  up       ip    p8005_ibp0  0.0.0.0/8            ibp0.8005
p8005_ibp1  up       ip    p8005_ibp1  0.0.0.0/8            ibp1.8005
pffff_ibp0  up       ip    pffff_ibp0  0.0.0.0/8            ibp0
pffff_ibp1  up       ip    pffff_ibp1  0.0.0.0/8            ibp1
```

   In the example output, the ipmp4 address is `172.17.0.9`.

Creating and Configuring a Share on the ZFS Storage appliance

Create a share as described in the "Creating Custom Shares" section of the *Exalogic Elastic Cloud Machine Owner's Guide*.

Mounting the Share in the File System of the vServer

Perform the following steps to mount the share you created in the file system of the vServer:

1. Log in to the ZFS Storage Appliance as `root`.
2. Select the **Shares** tab, and locate the share you created.
3. Click the **edit entry** icon.

   The details of the share are displayed.
4. Click the **Protocols** tab.
5. Click the plus (+) button next to NFS Exceptions, and specify the following:
   - **Type**: Network
   - **Entity**: `ip_address_of_vserver`/32 (in CIDR format)
   - **Access mode**: Read/write
   - **Charset**: default
   - **Root Access**: Selected
6. Click the **Apply** button near the upper right corner.

7. SSH to any compute node on the Exalogic machine.
8. SSH to the vServer by using the IP address that you noted in the Identifying the IP Address of the vServer section.
9. Create a directory that will serve as the mount point for the ZFS share:

   ```
   mkdir mount_point_directory
   ```

   Example:

   ```
   mkdir /root/test1
   ```

10. Mount the share on the vServer:

    ```
    # mount ipmp4_address_of_storage_appliance:/share_directory mount_point_directory
    ```

    Example:

    ```
    # mount 172.17.0.9:/export/testshare /root/test1
    ```

Index

H