

StorageTek Virtual Storage Manager System

VSM 6 Planning Guide

Release 6.1

E55118-03

February 2015

Copyright © 2001, 2015, Oracle and/or its affiliates. All rights reserved.

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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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

Preface	ix
Documentation Accessibility	ix
Other VSM 6 Documents.....	ix
1 Introduction	
The VSM Solution	1-2
The VSM 6 Platform	1-2
2 VSM 6 Planning and Implementation Overview	
Planning Goals	2-1
Creating Planning Teams	2-1
Planning Activities	2-2
Planning Spreadsheet	2-3
3 VSM 6 Implementation Planning	
Implementation Planning Goals	3-1
Implementation Planning Process Overview	3-1
Key High-Level Activities	3-1
Key Sub-Tasks	3-2
Key Participants	3-2
Satisfying Network Infrastructure Requirements	3-2
Satisfying MVS Host Software Requirements	3-3
Satisfying Serviceability Requirements	3-3
4 VSM 6 Hardware Configuration Planning	
VSM 6 Configuration Options	4-1
VSM 6 Base Configuration	4-1
Storage Capacity Upgrade.....	4-1
Capacity Upgrade for VSM 6 with Oracle DE2-24C Disk Shelves	4-2
Capacity Upgrade for VSM 6 with Sun J4410 Disk Shelves	4-2
FICON Upgrade	4-2
ZIL SSD Upgrade	4-2
Configuration Planning Overview	4-3
Key High-Level Activities	4-3

Key Sub-Tasks	4-3
Key Participants	4-3

5 VSM 6 Physical Site Readiness Planning

The Site Readiness Planning Process	5-1
Key High-Level Activities.....	5-1
Key Sub-Tasks.....	5-2
Key Participants.....	5-2
Site Evaluation – External Considerations	5-2
Site Evaluation – Internal Considerations	5-2
Transferring Equipment Point-to-Point	5-3
Structural Dimensions and Obstructions	5-3
Elevator Lifting Capacities.....	5-3
Floor-Load Ratings.....	5-3
Ramp Inclines	5-4
Data Center Safety	5-4
Emergency Power Control.....	5-4
Fire Prevention	5-4
Site Power Distribution Systems	5-5
Equipment Grounding	5-6
Source Power Input.....	5-6
Dual Independent Source Power Supplies.....	5-7
Transient Electrical Noise and Power Line Disturbances	5-7
Electrostatic Discharge	5-8
HVAC Requirements	5-8
Environmental Requirements and Hazards	5-8
Floor Construction Requirements	5-9
Floor Loading Requirements	5-9
Floor Loading Specifications and References	5-9
Raised-Floor Lateral Stability Ratings.....	5-9
Raised-Floor Panel Ratings.....	5-10
Raised-Floor Pedestal Ratings.....	5-10
VSM 6 Environmental Specifications	5-10
VSM 6 Base Configuration.....	5-10
VSM 6 Capacity	5-10
VSM 6 Overall Dimensions.....	5-11
VSM 6 Service Clearance.....	5-11
VSM 6 Weight.....	5-11
VSM 6 Power	5-12
VSM 6 HVAC.....	5-12

6 VSM 6 Ethernet (IP) Data Path Connectivity

VSM 6 Ethernet (IP) Port Assignments	6-1
Network Port Scenarios	6-2
Node Configuration Example	6-2
Direct, Switched, and Gateway Configuration Scenarios	6-3
VSM 6 Ethernet (IP) Connectivity Considerations	6-4

VSM 6 IP Connectivity Examples	6-6
VSM 6 IP Replication: Define the Replication Ports	6-6
VSM 6 CLI Example:	6-7
VSM 6 VLE Connectivity: Define the IPPATH	6-7
VSM 6 CLI Example:	6-7
VTCS Example:	6-7
VSM 6 CLINK Connectivity: Define the IPPATH	6-8
VSM 6 CLI Example:	6-8
VTCS Example:	6-8

7 VSM 6 FICON Data Path Connectivity

How it Works	7-1
VSM 6 FICON Port Assignments	7-1
VSM 6 RTD Connectivity Examples	7-2
VSM 6 RTD Connectivity: Direct Connection	7-2
VSM 6 CLI Example:.....	7-3
VTCS Example:.....	7-3
VSM 6 RTD Connectivity: Single Switch	7-3
VSM 6 CLI Example:.....	7-3
VTCS Example:.....	7-3
VSM 6 RTD Connectivity: Cascaded Switch	7-3
VSM 6 CLI Example:.....	7-3
VTCS Example:.....	7-3
VSM 6 RTD Connectivity: Dual RTDs	7-4
VSM 6 CLI Example:.....	7-4
VTCS Example:.....	7-4
VSM 6 RTD Connectivity: Four RTDs One Port	7-4
VSM 6 CLI Example:.....	7-4
VTCS Example:.....	7-4
VSM 6 RTD Connectivity: Dual-Path RTD	7-5
VSM 6 CLI Example 1:.....	7-5
VTCS Example 1:.....	7-5
VSM 6 CLI Example 2:.....	7-5
VTCS Example 2:.....	7-5
VSM 6 RTD Connectivity: Dual-Path Dual RTD	7-5
VSM 6 CLI Example:.....	7-6
VTCS Example:.....	7-6
VSM 6 RTD Connectivity: Multi-Path Dual RTD	7-6
VSM 6 CLI Example:.....	7-6
VTCS Example:.....	7-6

8 Data at Rest Encryption Feature

A Controlling Contaminants

Environmental Contaminants	A-1
Required Air Quality Levels	A-2

Contaminant Properties and Sources	A-2
Operator Activity	A-3
Hardware Movement	A-3
Outside Air	A-3
Stored Items	A-3
Outside Influences	A-3
Cleaning Activity	A-4
Contaminant Effects	A-4
Physical Interference.....	A-4
Corrosive Failure.....	A-4
Shorts.....	A-4
Thermal Failure	A-5
Room Conditions	A-5
Exposure Points	A-6
Filtration	A-6
Positive Pressurization and Ventilation	A-7
Cleaning Procedures and Equipment	A-8
Daily Tasks	A-8
Weekly Tasks	A-9
Quarterly Tasks	A-9
Biennial Tasks	A-10
Activity and Processes	A-10

Index

List of Figures

1-1	VSM 6 VTSS	1-1
5-1	Site Electrical Power Distribution System	5-6
5-2	NEMA L6-30P Plug and L6-30R Receptacle	5-7
5-3	Transient Electrical Grounding Plate	5-8
6-1	VSM 6 Ethernet Ports	6-1
6-2	Node Configuration Example	6-3
6-3	Example Direct, Switched, and Gateway Connection Scenarios	6-3
6-4	VSM 6 IP Replication – Define the Replication Ports	6-7
6-5	VSM 6 VLE Connectivity – Define the IPPATH	6-7
6-6	VSM 6 CLINK Connectivity – Define the IPPATH	6-8
7-1	VSM 6 FICON Port Assignments	7-2
7-2	VSM 6 RTD Connectivity – Direct Connection.....	7-2
7-3	VSM 6 RTD Connectivity – Single Switch.....	7-3
7-4	VSM 6 RTD Connectivity – Cascaded Switch.....	7-3
7-5	VSM 6 RTD Connectivity – Dual RTDs	7-4
7-6	VSM 6 RTD Connectivity – Four RTDs One Port.....	7-4
7-7	VSM 6 RTD Connectivity – Dual-Path RTD Example 1	7-5
7-8	VSM 6 RTD Connectivity – Dual-Path RTD Example 2	7-5
7-9	VSM 6 RTD Connectivity – Dual-Path Dual RTD.....	7-6
7-10	VSM 6 RTD Connectivity – Multi-Path Dual RTD.....	7-6

List of Tables

6-1	Ports Configured on Customer Network Need Separate Networks.....	6-4
6-2	Two Networks, Each with /24 Prefix Length (254 IP Addresses).....	6-4
6-3	Subnet Size Considerations	6-4
6-4	Two Networks with /28 Network Prefix (14 IP Addresses).....	6-5
6-5	/28 Networks and Ports Addresses	6-5
6-6	Sample Layout for VSM 6 Node 1 Ports and Target Network Ports.....	6-6
6-7	Sample Layout for VSM 6 Node 2 Ports and Target Network Ports.....	6-6
A-1	Dust-Spot Fractional Efficiency Percentages	A-7
A-2	Effective Cleaning Schedule	A-8

Preface

This publication is intended for Oracle or customer personnel responsible for doing site planning for Oracle's StorageTek Virtual Storage Manager System 6.

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.

Other VSM 6 Documents

- *VSM 6 Safety and Compliance Guide*
- *VSM 6 Security Guide*
- *VSM 6 Third Party Licenses and Notices*

Introduction

Oracle's StorageTek Virtual Storage Manager System 6 (VSM 6) Virtual Tape Storage Subsystem (VTSS) supports emulated tape connectivity to IBM MVS hosts and attachment to Real Tape Drives (RTDs), Virtual Library Extensions (VLEs), and other VTSSs to provide virtual tape device emulation, virtual tape cartridge images, and additional buffer capacity for the IBM MVS environment.

Figure 1-1 VSM 6 VTSS



The VSM Solution

Oracle's StorageTek Virtual Storage Manager (VSM) solution is the collection of hardware and software products that comprise a disk-based virtual tape system to provide enterprise-class storage management capabilities for the IBM mainframe environment. VSM optimizes streaming workloads and backup and recovery functions, reduces management overhead, and maximizes tape capacity utilization to reduce data protection costs in a wide range of storage environments.

VSM stores virtual tape volumes (VTVs) on a disk buffer on the VTSS and can optionally migrate them to Virtual Library Extension (VLE), Real Tape Drives (RTDs), or both. When needed by the host, if the migrated tape volumes are not VTSS-resident, they are then automatically recalled to the VTSS.

The VSM solution includes the following subsystems:

- VTSS hardware and software. The VSM 6 VTSS supports emulated tape connectivity to IBM MVS hosts over FICON interfaces, FICON attachment to Real Tape Drives (RTDs), IP attachment to other VTSSs and VLEs, and remote host connectivity using ECAM over IP and VSM 6 VTSS-to-VTSS replication.
- Enterprise Library Software (ELS). ELS is the consolidated suite of StorageTek mainframe software that enables and manages StorageTek's Automated Cartridge System (ACS) and Virtual Storage Manager (VSM) hardware. ELS includes the Host Software Component (HSC), Storage Management Component (SMC), HTTP Server, and also the Virtual Tape Control Software (VTCS). VTCS controls virtual tape creation, deletion, replication, migration and recall of virtual tape images on the VTSS and also captures reporting information from the VTSS.
- Virtual Library Extension (VLE) hardware and software. The VLE subsystem functions as a migrate and recall target for VTSS Virtual Tape Volumes (VTVs). VLEs are IP-attached to the VSM 6 VTSS.
- Real Tape Drives (RTDs) connected to physical tape libraries. RTDs serve as migrate and recall targets for VTSS Virtual Tape Volumes (VTVs). RTDs are FICON-attached to the VSM 6 VTSS.

The VSM 6 Platform

The VSM 6 platform replaces the proprietary VSM 5 platform. This platform provides increased performance and greatly expanded storage capacity compared to previous VTSS versions, and it is scalable to meet a customer's current needs while providing a path for future growth.

The VSM 6 VTSS is packaged as a standard rack mount system built on existing Sun server, storage, and service platforms. The servers, disk shelves, and standard rack mount enclosure are delivered as a packaged system.

The Solaris 11 operating system is the foundation of the VSM 6 VTSS software environment, which also includes Solaris infrastructure components and VTSS function-specific software. The VSM 6 software environment is pre-installed and preconfigured for VTSS functionality so that limited site-level configuration is required to integrate the product into the customer's managed tape environment.

VSM 6 also includes the interfaces and support required for operation within an existing VSM Tapeplex, including VTCS support, legacy VTSS support, and support for ELS, HSC/SMC, NCS, VLE, SE Tools, VAT, LCM and CDRT.

VSM 6 Planning and Implementation Overview

This chapter describes the key participants and activities involved in planning for and implementing a VSM 6 system.

Planning Goals

The primary goals of the planning process are to:

- Ensure the VSM 6 system meets the requirements of the customer, and that it is ordered, delivered, installed, configured, tested, certified, and turned over with a minimum of disruptions and problems.
- Ensure the installation site infrastructure is equipped to handle the power, data-handling, and environmental requirements of VSM 6 system equipment, and that customer personnel are trained to assist with delivery, installation, configuration, testing, certification, and operation of the VSM 6 system equipment.

Successful implementation requires regular communication and coordination between customer personnel and the Oracle account team. This ongoing collaboration helps ensure that all factors critical to the implementation are identified and addressed before equipment is delivered to the site.

Creating Planning Teams

Once a sales proposal has been accepted, the customer service manager (CSM) should confer with customer-site personnel including the network administrator, data center manager, and facilities manager to identify which individuals who should be involved with implementation planning, site readiness planning, and delivery and installation planning.

Customer and Oracle personnel who participate in these planning teams jointly own and control the various processes, activities, and deliverables of those teams.

Once the team participants have been identified, one customer team member and one Oracle team member should be selected to act as coordinators for each team. Regular meetings should be scheduled to:

- Define roles and responsibilities for all team members.
- Define required implementation activities and task completion dates.
- Identify and address issues that could impede delivery, installation, or implementation of system equipment.

Customer membership for the various planning and implementation teams should consist of:

- Persons who will determine the configuration and location of VSM 6 system equipment, including but not limited to the data center manager, one or more network administrators, the facilities manager, and the site engineer.
- Persons who will be directly involved with installation, testing, certification, and operation of VSM 6 system equipment, including but not limited to facilities personnel, system operators, and network/IT personnel.
- Persons who will be involved with delivery and dock-to-data center transit of VSM 6 system equipment, including but not limited to the dock manager, dock personnel, and facilities personnel.

Oracle membership for the various teams may include some or all of the following: the sales representative (SR), the local customer services manager (CSM), a systems engineer (SE), a system support specialist (SSS), a technical support specialist (TSS), an Oracle Advanced Customer Services (ACS) consultant, and a customer service engineer (CSE).

Planning Activities

The following activities should be completed during the time preceding delivery of VSM 6 system equipment to a customer site:

1. Define a system configuration that best addresses customer requirements.
2. Review site factors that present existing or potential safety and environmental hazards.
3. Review equipment transfer requirements and define a compliance plan as needed.
4. Review power supply and cabling requirements and evaluate compliance to requirements.
5. Review floor construction and load ratings and evaluate compliance.
6. Review data cabling requirements for the VSM 6 system configuration and evaluate compliance to requirements.
7. After completing reviews of power, environmental, flooring, and network connectivity requirements, schedule needed facilities upgrades to be completed before delivery of system equipment.
8. Create a floorplan/layout for all VSM 6 system equipment, and review it with the Professional Services consultant. A copy of the final floorplan/layout should be given to the sales representative to attach to the sales order.
9. Measure and record cable-layout distances between AC source power locations, host systems, network servers, remote support devices, and VSM 6 system hardware components.
10. Identify any special shipping requirements and reconfirm the scheduled system delivery date with the manufacturing facility.
11. Verify compliance of input power systems and power cabling in the data center.
12. Verify environmental compliance and HVAC systems readiness in the delivery, staging, and installation areas.
13. Verify floor loading compliance along the delivery path and at the data center installation location.
14. Identify which personnel will perform the VSM 6 system installation at the customer site.

15. Verify delivery dock and data center personnel and CSEs will be available to accept delivery of the system equipment, and assist in unpackaging, point-to-point transfer, and installation of system equipment.
16. Agree on firm dates and timeframes for delivery, installation, certification, and operational testing of system equipment.

Planning Spreadsheet

A VSM 6 planning spreadsheet is available to the account team from Oracle VSM Support. Use the spreadsheet to record relevant account site and contact information, and to map and record details of the VSM 6 configuration. The spreadsheet also contains a sample configuration to use for reference during the planning process.

VSM 6 Implementation Planning

This chapter provides an overview of implementation planning activities and tasks, which are designed to ensure a VSM 6 system is properly configured, tested, and certified according to customer requirements.

Implementation Planning Goals

The implementation planning process is designed to identify and schedule completion of configuration, performance tuning, and performance testing activities for a VSM 6 VTSS after it has been physically installed at a site.

A team comprised of key customer personnel (systems administrator, network administrator, data center manager, and system operator) and Oracle Professional Services personnel (technical support specialist, systems engineer, and customer service manager) works to complete these primary tasks:

- Define a plan for integrating existing devices and systems with the VSM 6 system.
- Define a plan to migrate data from other devices and systems to the VSM 6 system.
- Define a plan to accommodate the physical layout and floor space requirements of the VSM 6 VTSS and other system devices.
- Define a plan for configuring the VSM 6 system hardware (channel resources, physical disk, and so on), software (ExLM, HSC, MVS, NCS, VTCS), and virtual entities (VTDs, VTVs).
- Define a plan for completing performance tuning, performance testing, and certification of VSM 6 system hardware and software in the data center environment.
- Identify personnel training needs and scheduling appropriate knowledge-transfer training sessions.

Implementation Planning Process Overview

Planning activities, tasks, and participants include:

Key High-Level Activities

1. Select implementation planning team members, and define roles and responsibilities.
2. Schedule and attend implementation planning meetings.

3. Determine task completion priorities and scheduling.

Key Sub-Tasks

1. Define plan for integrating other devices and systems with the VSM 6 system.
2. Define plan for migrating data from other devices and systems to the VSM 6.
3. Determine default settings for the VSM 6 system.
4. Define plan for configuring and managing system hardware (channel resources, physical disk, and so on).
5. Define plan for configuring and managing VSM 6 system software (ExLM, HSC, MVS, NCS, VTCS).
6. Define policies for configuring and managing VSM 6 system virtual entities.
7. Define plan for performance tuning, testing, and certification of the VSM 6 system.
8. Assess personnel requirements for knowledge-transfer and hands-on training, and facilitate scheduling and completion of training activities.

Key Participants

- Customer: network administrator, system administrator, data center manager, system operator
- Oracle: professional services personnel (delivery consultant, systems support specialist, technical support specialist, systems engineer)

Satisfying Network Infrastructure Requirements

If possible, do any configuration of IP addresses, network switch(es) for VLANs or other setup (running cables, and so forth) before the VSM 6 arrives to minimize the installation time. Ensure that the network is ready for connection to the VSM 6 as follows:

- Gigabit Ethernet protocol is required on all network switches and routers that are directly attached to the VSM 6 servers. The servers will only do speed negotiation to the 1 Gb speed.
- Check that you are using the proper (customer-supplied) 1GigE Ethernet cables:
 - CAT5 cables and below are not acceptable for GigE transmission.
 - CAT5E cable: 90 meters is acceptable if run through a patch panel, 100 meters if straight cable.
 - CAT6 cable: 100 meters is acceptable regardless of patch panel configuration.
- Oracle recommends if a switch or router is used in the configuration, at least two switches or routers be part of the configuration at each location so that the loss of one unit will not bring down the whole configuration.
- Only one TCP/IP connection is required between a VSM 6 VTSS and another VTSS or VLE. However, for redundancy, Oracle strongly recommends that you have a total of four connections, where the VTSS connections are targets on separate servers. Each connection from a specific VTSS to a specific VLE or VTSS should be to separate interfaces.
- IP addresses must **never** be duplicated on any ports on the VSM 6 servers. For example, if you have a REP port or ASR connection of 192.168.1.1 going to Node 1,

do not make another REP port or ASR connection on Node 2 using 192.168.1.1 as the IP address.

- Ports on a VSM 6 node that are configured on the customer network must be on separate networks. See [Chapter 6, "VSM 6 Ethernet \(IP\) Data Path Connectivity"](#) for more information about this restriction.
- VSM 6 reserves and uses the following TCP ports for the identified functions:
 - 50000 - IFF/IP replication control port (labeled REP1, REP2, REP3. REP4 on each node)
 - 51000-55000 - IFF/IP replication data port (labeled REP1, REP2, REP3. REP4 on each node)
 - 61300 - CLI server (labeled NET0 or NET2)
 - 61000 - ECAM over IP (labeled NET0)
 - 63001 - Enhanced Replication control port (labeled REP1, REP2, REP3. REP4 on each node)
 - 63002-63999 - Enhanced Replication data connections (labeled REP1, REP2, REP3. REP4 on each node)
 - 443 – ASR (labeled CAM/ASR)
 - 6789 - CAM GUI - Web console (labeled CAM/ASR)
 - 8654 - CAM GUI - Web server (labeled CAM/ASR)

Satisfying MVS Host Software Requirements

See the VSM 6 Release Notes for information about VTCS software updates that may be additionally required for VSM 6 support.

Satisfying Serviceability Requirements

The VSM 6 product uses a standard Oracle service strategy common with other Oracle products. VSM 6 uses Automated Service Response (ASR) as the outgoing event notification interface to notify Oracle VSM Support that an event has occurred on the VSM 6 and the system may require service.

Additionally, in combination with ASR, an outgoing email containing details about an ASR event and a Support File Bundle containing VSM 6 log information necessary to investigate any ASR event will also be sent.

The advantages of ASR functionality are well documented in the ASR FAQ available on the My Oracle Support site in Knowledge Article Doc ID 1285574.1.

Oracle's expectation is that the VSM 6 will be configured to allow outgoing ASR and email communication with Oracle VSM Support. To support VSM 6 outgoing ASR notifications, the customer will need to supply the following information to the installing Oracle Field Engineer:

- Site information, including company name, site name and location
- Customer contact information, including name and email
- Oracle online account information, including customer Oracle CSI login name and password
- Oracle ASR setup information, including proxy host name, proxy port, proxy authentication user name and password

Some fields are not required if a proxy server is not being used or if it does not require an ID and password. If the customer will not provide the CSI email ID and password, then the customer can enter it directly during the install process.

ASR registration takes place during the CAM configuration portion of the VSM 6 installation. During this part of the install the VSM 6 will register itself on the Oracle servers as an ASR qualified product.

The customer is then required to log in to My Oracle Support (MOS) and approve the registration of the VSM 6. Until this approval is completed by the customer, the VSM 6 is not capable of auto-generating cases through MOS.

For email notification of event and log information, the customer must also supply the following information:

- Email configuration: SMTP server name, SMTP server user name, and SMTP server user password
- Email recipients

If the email server does not require a user name and password, these fields can remain blank.

In cases where outgoing communication steps are not completed at the time of installation or not allowed at all, Oracle's options for timely response to events that require support from the Oracle Service team are greatly reduced. In this scenario, the VSM 6 can send email containing event and log information directly to a designated customer internal email address. A recipient of this email can then initiate a service request directly with Oracle and forward any emails received from the VSM 6 to Oracle VSM Support. In this case, the customer must supply the email address where VSM 6 emails are sent.

VSM 6 Hardware Configuration Planning

This chapter provides an overview of configuration planning considerations.

VSM 6 Configuration Options

VSM 6 consists of a base unit and optional capacity upgrades.

VSM 6 Base Configuration

The base unit is a VSM 6 in its minimum configuration, including:

- A standard Sun Rack II cabinet, Model 1242
- Depending on country, two VLE50HZ-POWER-Z or two VLE60HZ-POWER-Z power Power Distribution Units (PDUs)
- Two Sun SPARC T4-2 servers in a specific configuration and factory preconfigured for VSM 6
- Two disk shelves, in a specific configuration depending on date of manufacture:
 - For VSM 6 units built starting in December 2013, the base unit has two Oracle Storage Drive Enclosure DE2-24C disk shelves. Each DE2-24C disk shelf has three 73GB or 200GB Flash SSDs and 21 4TB SAS HDD drives, representing 370TB approximate user capacity (configured, with 4:1 compression).
 - For VSM 6 units built before December 2013, the base unit has two Sun J4410 disk shelves, each with three 73GB Flash SSDs and 21 3TB SAS HDD drives, representing 270TB approximate user capacity (configured, with 4:1 compression).

Storage Capacity Upgrade

Storage capacity upgrades are either base capacity upgrades that are factory-built when the base unit is assembled, or field capacity upgrades that are installed in the field.

A storage capacity upgrade kit is packaged as two disk shelves. Up to three upgrade kits can be installed in a VSM 6 base unit, for a total of four, six, or eight disk shelves in the unit.

Note: The capacity upgrade must use the same disk shelf product that is used in the base configuration. You cannot mix Oracle DE2-24C and Sun J4410 disk shelves in a VSM 6.

Capacity Upgrade for VSM 6 with Oracle DE2-24C Disk Shelves

For a VSM 6 with Oracle DE2-24C disk shelves, a capacity upgrade kit has two Oracle DE2-24C disk shelves, each containing 24 4TB SAS HDD drives, representing 400TB approximate user capacity (configured, with 4:1 compression).

Total approximate user capacity (configured, with 4:1 compression) for a base unit with one, two, or three capacity upgrade kits installed is as follows:

- VSM 6 with four Oracle DE2-24C disk shelves: 800TB
- VSM 6 with six Oracle DE2-24C disk shelves: 1200TB
- VSM 6 with eight Oracle DE2-24C disk shelves: 1600TB

Capacity Upgrade for VSM 6 with Sun J4410 Disk Shelves

For a VSM 6 with Sun J4410 disk shelves, a capacity upgrade kit has two Sun J4410 disk shelves, each containing 24 3TB SAS HDD drives, representing 300TB approximate user capacity (configured, with 4:1 compression).

Total approximate user capacity (configured, with 4:1 compression) for a base unit with one, two, or three capacity upgrade kits installed is as follows:

- VSM 6 with four Sun J4410 disk shelves: 600TB
- VSM 6 with six Sun J4410 disk shelves: 900TB
- VSM 6 with eight Sun J4410 disk shelves: 1200TB

FICON Upgrade

The FICON upgrade option may include up to eight Long Wave SFPs that replace some or all of the Short Wave SFPs in the VSM 6 VTSS's FICON HBAs. There are eight SFPs total in a VSM 6 VTSS. They can be all Long Wave, all Short Wave, or mixed to balance Long and Short Wave SFPs between servers.

ZIL SSD Upgrade

The ZIL SSD upgrade adds two 200GB SSDs to the VSM 6 storage pool. These SSDs are dedicated to the ZFS intent log (ZIL) to improve synchronous write performance by speeding up specific synchronizing events.

The ZIL performance upgrade for VSM 6 systems with 4TB disk drives installed is available now. VSM 6 approximate production dates for these units are December 2013 to present. The Oracle service person can confirm the VSM 6 configuration.

The ZIL performance upgrade for VSM 6 with 3TB disk drives will be available in April 2015. VSM 6 approximate production dates for these units are November 2012 through November 2013.

This upgrade is recommended for certain VSM 6 configurations with Host workloads involving small VTVs (1MB to 2MB VTVs) and high number of simultaneous VTV mount operations. For these workloads, adding SSDs to the VSM 6 storage pool significantly improves performance.

This upgrade is only available for VSM 6 configurations with four or more disk shelves installed.

Configuration Planning Overview

Designing an optimized VSM 6 system to meet specific customer requirements requires close collaboration between Oracle personnel and key customer decision makers who are involved with selecting and implementing the system. Planning for more complex system implementations may require consultation with the Oracle Advanced Customer Services (ACS) group.

Configuration planning activities, tasks, and participants include:

Key High-Level Activities

1. Define customer requirements.
2. Assess budgetary constraints.
3. Design an optimized VSM 6 system based on defined requirements and constraints.

Key Sub-Tasks

1. See the VSM 6 Planning Spreadsheet for more detailed configuration information and a sample configuration to use for reference during the planning process. The spreadsheet is available to the account team from Oracle VSM Support.
2. Estimate capacity requirements and propose a system configuration.
3. Create a high-level conceptual diagram of the proposed VSM 6 system configuration.
4. Create a detailed engineering diagram of the proposed VSM 6 system configuration.
5. Present the VSM 6 system physical and functional configuration plans to key decision makers.

Key Participants

- Customer: network administrator, data center manager
- Oracle: account representative, systems support specialist, technical support specialist, systems engineer

VSM 6 Physical Site Readiness Planning

This chapter provides information about activities designed to ensure the site is equipped to accommodate the power, safety, environmental, HVAC, and data handling requirements of VSM 6 system equipment. Key site readiness planning considerations include, but are not limited to:

- Site surveys to evaluate and eliminate or mitigate factors which could negatively affect delivery, installation, and operation of VSM 6 system equipment
- A plan for the layout and location of VSM 6 system equipment and cabling that allows for efficient use and easy maintenance, plus adequate space and facilities for Oracle support personnel and their equipment
- Facilities construction that provides an optimum operating environment for VSM 6 system equipment and personnel, and safe flooring and protection from fire, flooding, contamination, and other potential hazards
- Scheduling of key events and task completion dates for facilities upgrades, personnel training, and delivery, implementation, installation, testing, and certification activities

Customers ultimately are responsible for ensuring that their site is physically prepared to receive and operate VSM 6 system equipment, and that the site meets the minimum specifications for equipment operation as detailed in this guide.

The Site Readiness Planning Process

Site readiness planning activities, tasks, and participants include:

Key High-Level Activities

1. Select site readiness team members, and define roles and responsibilities
2. Complete site surveys to:
 - Document existing or potential external and internal environmental hazards.
 - Assess site power, safety, environmental, HVAC, and data handling capabilities versus VSM 6 system requirements.
 - Confirm floor load ratings along the transit path and at the installation location for VSM 6 VTSS cabinets.
 - Assess ceiling, hallway, and door clearances, elevator capacities, and ramp angles versus VSM 6 VTSS cabinet requirements.
3. Attend planning meetings.

Key Sub-Tasks

1. Verify site power, safety, environmental, HVAC, and data handling capabilities match VSM 6 VTSS requirements.
2. Define plan to eliminate/mitigate environmental hazards.
3. Evaluate floor load ratings along transit path and at the VSM 6 VTSS installation location.
4. Verify site door, hall and ceiling clearances, elevator capacity, and ramp angles match VSM 6 VTSS requirements.
5. Identify required infrastructure modifications/upgrades; set work completion schedule.
6. Evaluate readiness progress, and certify site readiness.

Key Participants

- Customer: site engineer, facilities manager, data center manager, network administrator
- Oracle: technical support specialist, systems engineer

Site Evaluation – External Considerations

Several months before delivery of VSM 6 system equipment, a readiness planning team should identify and evaluate all external site factors that present existing or potential hazards, or which could adversely affect delivery, installation, or operation of the system. External factors that should be evaluated include:

- Reliability and quality of electrical power provided by the local utility, backup power generators, and uninterruptible power supplies (UPSs)
- Proximity of high-frequency electromagnetic radiation sources (for example, high-voltage power lines; television, radio, and radar transmitters)
- Proximity of natural or man-made floodplains and the resultant potential for flooding in the data center
- Potential effects of pollutants from nearby sources (for example, industrial plants)

If any existing or potential negative factors are discovered, the site readiness planning team should take appropriate steps to eliminate or mitigate those factors before VSM 6 system equipment is delivered. Oracle Global Services offers consultation services and other assistance to identify and resolve such issues. Contact your Oracle account representative for more information.

Site Evaluation – Internal Considerations

Several months before delivery of VSM 6 system equipment, a readiness planning team should identify and evaluate all internal site factors that present existing or potential hazards, or which could adversely affect delivery, installation, or operation of the system. Internal factors that should be evaluated include:

- Structural dimensions, elevator capacities, floor-load ratings, ramp inclines, and other considerations when transferring equipment point-to-point between the delivery dock, staging area, and data center installation site
- Site power system(s) design and capacity

- VSM 6 system equipment power system design and capacity
- Data center safety system design features and capabilities
- Data center environmental (HVAC) design features and capabilities
- Potential effects of corrosive materials, electrical interference, or excessive vibration from sources near to system equipment.

If any existing or potential negative factors are discovered, the site readiness planning team should take appropriate steps to eliminate or mitigate those factors before VSM 6 system equipment is delivered. Oracle Global Services offers consultation services and other assistance to identify and resolve such issues. Contact your Oracle account representative for more information.

Transferring Equipment Point-to-Point

Site conditions must be verified to ensure all VSM 6 system equipment can be safely transported between the delivery dock, staging area, and data center without encountering dimensional restrictions, obstructions, or safety hazards, or exceeding rated capacities of lifting and loading equipment, flooring, or other infrastructure. Conditions that must be verified are described below.

Structural Dimensions and Obstructions

Dimensions of elevators, doors, hallways, and so on must be sufficient to allow unimpeded transit of VSM 6 cabinets (in shipping containers, where appropriate) from the delivery dock to the data center installation location. See [VSM 6 Overall Dimensions](#) for VSM 6 cabinet-dimension details.

Elevator Lifting Capacities

Any elevators that will be used to transfer VSM 6 cabinets must have a certified load rating of at least 1050 kg (2312 lbs.). This provides adequate capacity to lift the heaviest fully-populated VSM 6 cabinet (roughly 751 kg (1652 lbs.)) and a pallet jack (allow 100 kg/220 lbs.) and two persons (allow 200 kg/440 lbs.). See [VSM 6 Weight](#) for additional cabinet-weight details.

Floor-Load Ratings

Solid floors, raised floors, and ramps located along the transfer path for VSM 6 cabinets must be able to withstand concentrated and rolling loads generated by the weight of a populated cabinet, the pallet jack used to lift the cabinet, and personnel who are moving the cabinet from point to point.

Raised floor panels located along a transfer path must be able to resist a concentrated load of 751 kg (1652 lbs.) and a rolling load of 181 kg (400 lbs.) anywhere on the panel, with a maximum deflection of 2 mm (0.08 in.). Raised floor pedestals must be able to resist an axial load of 2268 kg (5000 lbs.). See [Floor Loading Requirements](#) for additional floor-loading details.

When being moved from one location to another, a VSM 6 cabinet generates roughly twice the floor load as in a static state. Using 19 mm (0.75 in.) plywood along a transfer path reduces the rolling load produced by a cabinet.

Ramp Inclines

To prevent VSM 6 cabinets from tipping on ramps while being moved from point to point, the site engineer or facilities manager must verify the incline angle of all ramps in the transfer path. Inclines cannot exceed 10 degrees (176 mm/m; 2.12 in./ft.).

Data Center Safety

Safety must be a primary consideration in planning installation of VSM 6 system equipment, and is reflected in such choices as where equipment will be located, the rating and capability of electrical, HVAC, and fire-prevention systems that support the operating environment, and the level of personnel training. Requirements of local authorities and insurance carriers will drive decisions about what constitutes appropriate safety levels in a given environment.

Occupancy levels, property values, business interruption potential, and fire-protection system operating and maintenance costs should also be evaluated. The *Standard for the Protection of Electronic Computer / Data Processing Equipment (NFPA 75)*, the *National Electrical Code (NFPA 70)*, and local and national codes and regulations can be referenced to address these issues.

Emergency Power Control

The data center should be equipped with readily-accessible emergency power-off switches to allow immediate disconnection of electrical power from VSM 6 system equipment. One switch should be installed near each principal exit door so the power-off system can be quickly activated in an emergency. Consult local and national codes to determine requirements for power disconnection systems.

Fire Prevention

The following fire-prevention guidelines should be considered in the construction, maintenance, and use of a data center:

- Store gases and other explosives away from the data center environment.
- Ensure data center walls, floors, and ceilings are fireproof and waterproof.
- Install smoke alarms and fire suppression systems as required by local or national codes, and perform all scheduled maintenance on the systems.

Note: Halon 1301 is the extinguishing agent most commonly used for data center fire suppression systems. The agent is stored as a liquid and is discharged as a colorless, odorless, electrically nonconductive vapor. It can be safely discharged in occupied areas without harm to personnel. Additionally, it leaves no residue, and has not been found to cause damage to computer storage media.

- Install only shatterproof windows, in code-compliant walls and doors.
- Install carbon dioxide fire extinguishers for electrical fires and pressurized water extinguishers for ordinary combustible materials.
- Provide flame-suppressant trash containers, and train personnel to discard combustible waste only into approved containers.
- Observe good housekeeping practices to prevent potential fire hazards.

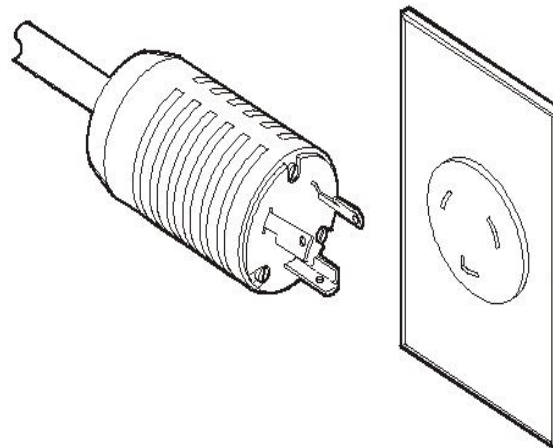
Site Power Distribution Systems

A properly installed power distribution system is required to ensure safe operation of VSM 6 system equipment. Power should be supplied from feeders separate from those used for lighting, air conditioning, and other electrical systems.

A typical input power configuration, shown in [Figure 5-1](#), is either a five-wire high-voltage or a four-wire low-voltage type, with three-phase service coming from a service entrance or separately derived source, and with overcurrent protection and suitable grounding. A three-phase, five-wire distribution system provides the greatest configuration flexibility, since it allows power to be provided to both three-phase and single-phase equipment.

In [Figure 5-1](#):

- 1 - Service entrance ground or suitable building ground
- 2 - Only valid at service entrance or separately derived system (transformer)
- 3 - Ground Terminal Bar (bound to enclosure) Same size as neutral
- 4 - Remotely Operated Power Service Disconnect
- 5 - Neutral Bus
- 6 - Circuit Breakers of Appropriate Size
- 7 - Branch Circuits
- 8 - 120V Single Phase
- 9 - 208/240V Single Phase
- 10 - 208/240V 3-Phase (4 wire)
- 11 - 208/240V 3-Phase (5 wire)

Figure 5–2 NEMA L6-30P Plug and L6-30R Receptacle

If you are installing the VSM 6 cabinet outside of North and South America, Japan and Taiwan, ensure that designated source-power receptacles meet all applicable local and national electrical code requirements. Then attach the required connectors to the three-wire ends of the cabinet power cords.

Dual Independent Source Power Supplies

VSM 6 cabinets have a redundant power distribution architecture designed to prevent disruption of system operations from single-source power failures. Four 30 Amp power plugs are required. To ensure continuous operation, all power cables must be connected to separate, independent power sources that are unlikely to fail simultaneously (for example, one to local utility power, the others to an uninterruptible power supply (UPS) system). Connecting multiple power cables to the same power source will not enable this redundant power capability.

Transient Electrical Noise and Power Line Disturbances

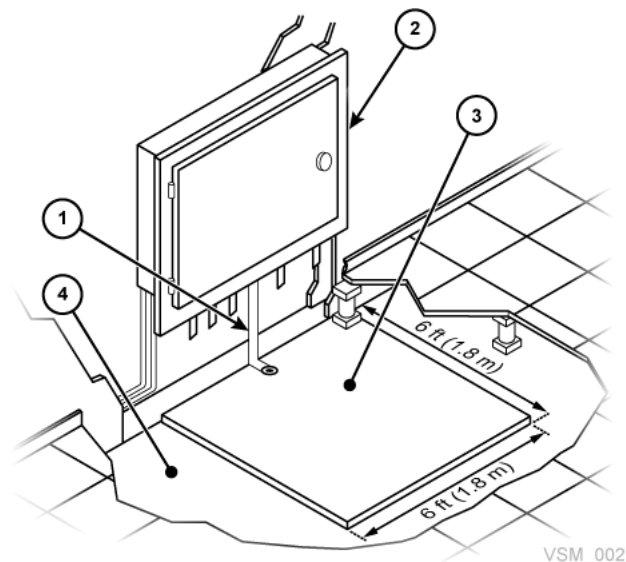
Reliable AC source power free from interference or disturbance is required for optimum performance of VSM 6 system equipment. Most utility companies provide power that can properly operate system equipment. However, equipment errors or failures can be caused when outside (radiated or conducted) transient electrical noise signals are superimposed on power provided to equipment.

Additionally, while VSM 6 system equipment is designed to withstand most common types of power line disturbances with little or no effect on operations, extreme power disturbances such as lightning strikes can cause equipment power failures or errors if steps are not taken to mitigate such disturbances.

To mitigate the effects of outside electrical noise signals and power disturbances, data center source power panels should be equipped with a transient grounding plate similar to that shown in [Figure 5–3](#).

In [Figure 5–3](#):

- 1 - Flat Braided/Strained Wire
- 2 - Power Panel
- 3 - Plate
- 4 - Concrete Floor

Figure 5-3 Transient Electrical Grounding Plate

Electrostatic Discharge

Electrostatic discharge (ESD) static electricity is caused by movement of people, furniture, and equipment. ESD can damage circuit card components, alter information on magnetic media, and cause other equipment problems. The following steps are recommended to minimize ESD potential in the data center:

- Provide a conductive path from raised floors to ground.
- Use floor panels with nonconducting cores.
- Maintain humidity levels within recommended control parameters.
- Use grounded anti-static work mats and wrist straps to work on equipment.

HVAC Requirements

Cooling and air-handling systems must have sufficient capacity to remove heat generated by equipment and data center personnel. Raised-floor areas should have positive underfloor air pressure to facilitate airflow. If conditions change within a data center (for example, when new equipment is added or existing equipment is rearranged), airflow checks should be done to verify sufficient airflow.

Environmental Requirements and Hazards

VSM 6 system components are sensitive to corrosion, vibration, and electrical interference in enclosed environments such as data centers. Because of this sensitivity, equipment should not be located near areas where hazardous or corrosive materials are manufactured, used, or stored, or in areas with above-average electrical interference or vibration levels.

For best performance, equipment should be operated at nominal environmental conditions. If VSM 6 system equipment must be located in or near adverse environments, additional environmental controls should be considered to mitigate those factors before installation of the equipment.

Floor Construction Requirements

VSM 6 system equipment is designed for use on either raised or solid floors. Carpeted surfaces are not recommended since these retain dust and contribute to the buildup of potentially damaging electrostatic charges. A raised floor is preferable to a solid floor since it permits power and data cables to be located safely away from floor traffic and other potential floor-level hazards.

Floor Loading Requirements

Flooring with an overall (superimposed) load rating of 490 kg/m² (100 lbs./ft.²) is recommended. If floors do not meet this rating, a site engineer or facilities manager must consult the floor manufacturer or a structural engineer to calculate actual loads and determine if the weight of a particular VSM 6 system configuration can be safely supported.

WARNING: Exceeding recommended raised-floor loads can cause a floor collapse, which could result in severe injury or death, equipment damage, and infrastructure damage. It is advisable to have a structural engineer perform a floor-load analysis before beginning installation of VSM 6 system equipment.

Caution: When being moved, a VSM 6 cabinet creates almost twice the floor load as when static. To reduce floor load and stress, and the potential for damage or injury when moving a VSM 6, consider using 19 mm/0.75 in. plywood on the floor along the path where the cabinet will be moved.

Floor Loading Specifications and References

- The basic floor load is 730 kg/m² (149 lbs./ft.²).
This is the load over footprint surface area (7093.7 cm²/1099.5 in²) of an unpackaged VSM 6 cabinet, with a maximum weight of 620 kg/1365 lbs (if fully loaded with 192 array disk drives).
- The maximum superimposed floor load is 485 kg/m² (99 lbs./ft.²).
This assumes minimum Z+Z axis dimension of 185.3 cm/73.0 in. (cabinet depth 77.1 cm/30.4 in. + front service clearance of 54.1 cm/21.3 in. + rear service clearance of 54.1 cm/21.3 in.), minimum X+X axis dimension of 104.9 cm/41.2 in. (cabinet width 92.1 cm/36.3 in. + left clearance of 6.4 cm/2.5 in. + right clearance of 6.4 cm/2.5 in.).

Raised-Floor Lateral Stability Ratings

In areas of high earthquake activity, the lateral stability of raised floors must be considered. Raised floors where VSM 6 system equipment is installed must be able to resist the following horizontal force levels applied at the top of the pedestal:

- Seismic Risk Zone 1: 13.5 kg / 29.7 lbs horizontal force
- Seismic Risk Zone 2A: 20.2 kg / 44.6 lbs horizontal force
- Seismic Risk Zone 2B: 26.9 kg / 59.4 lbs horizontal force
- Seismic Risk Zone 3: 40.4 kg / 89.1 lbs horizontal force

- Seismic Risk Zone 4: 53.9 kg / 118.8 lbs horizontal force

Note: Horizontal forces are based on the 1991 Uniform Building Code (UBC) Sections 2336 and 2337, and assume minimum operating clearances for multiple VSM 6 cabinets. Installations in areas not covered by the UBC should be engineered to meet seismic code provisions of the local jurisdiction.

Raised-Floor Panel Ratings

Raised floor panels must be able to resist a concentrated load of 620 kg (1365 lbs.) and a rolling load of 181 kg (400 lbs.) anywhere on the panel with a maximum deflection of 2 mm (0.08 in.). Perforated floor panels are not required for VSM 6 system equipment, but if used must follow the same ratings.

Raised-Floor Pedestal Ratings

Raised floor pedestals must be able to resist an axial load of 2268 kg (5000 lbs.). Where floor panels are cut to provide service access, additional pedestals may be required to maintain the loading capacity of the floor panel.

VSM 6 Environmental Specifications

Note: Statistics for power and cooling data are approximate due to variations in data rates and the number of operations occurring.

VSM 6 Base Configuration

VSM 6 consists of a base unit and optional capacity upgrades. The base unit is a VSM 6 in its minimum configuration, including:

- A standard Sun Rack II cabinet, Model 1242
- Depending on country, two VLE50HZ-POWER-Z or two VLE60HZ-POWER-Z power Power Distribution Units (PDUs)
- Two Sun SPARC T4-2 servers in a specific configuration and factory preconfigured for VSM 6
- Two disk shelves, in a specific configuration depending on date of manufacture:
 - For VSM 6 units built starting in December 2013, the base unit has two Oracle DE2-24C disk shelves, each with three 73GB or 200GB Flash SSDs and 21 4TB SAS HDD drives, representing 370TB approximate user capacity (configured, with 4:1 compression).
 - For VSM 6 units built before December 2013, the base unit has two Sun J4410 disk shelves, each with three 73GB Flash SSDs and 21 3TB SAS HDD drives, representing 270TB approximate user capacity (configured, with 4:1 compression).

VSM 6 Capacity

Total approximate user capacity (configured, with 4:1 compression) is as follows:

Oracle DE2-24C Disk Shelves:

- VSM 6 with two Oracle DE2-24C disk shelves: 370TB
- VSM 6 with four Oracle DE2-24C disk shelves: 800TB
- VSM 6 with six Oracle DE2-24C disk shelves: 1200TB
- VSM 6 with eight Oracle DE2-24C disk shelves: 1600TB

Sun J4410 Disk Shelves:

- VSM 6 with two Sun J4410 disk shelves: 270TB
- VSM 6 with four Sun J4410 disk shelves: 600TB
- VSM 6 with six Sun J4410 disk shelves: 900TB
- VSM 6 with eight Sun J4410 disk shelves: 1200TB

VSM 6 Overall Dimensions

SunRack II 1242 Cabinet (inches):

- Height: 78.7
- Width: 23.6
- Depth: 47.2

VSM 6 Service Clearance

SunRack II 1242 Cabinet (inches):

- Top: 36 inches. This is the generic Sun Rack II specification. VSM 6 does not require access through the top except for cabling.
- Front: 42
- Rear: 36

VSM 6 Weight

In Pounds: (Base 712 pounds, Max 1372 pounds)

- Servers: [80 pounds] times [two servers] equal [160 pounds]
- Cabinet: 332 pounds
- Disk shelves: [110 pounds] times [two disk shelves] equal [220 pounds]
- [Max eight disk shelves] equal [880 pounds]
- Total max weight: 1372 pounds
- Shipping material: 280 pounds
- [Total max weight] plus [shipping material] equal [1652 pounds]

In Kilograms: (Base: 323.64 kilograms, Max 623.64 kilograms)

- Servers: [36.36 kilograms] times [two servers] equal [72.73 kilograms]
- Cabinet: 150.91 kilograms
- Disk shelves: [50 kilograms] times [two disk shelves] equal [100 kilograms]
- [Max eight disk shelves] equal [400 kilograms]
- Total max weight: 623.64 kilograms

- Shipping material: 127.27 kilograms
- [Total max weight] plus [shipping material] equal [750.91 kilograms]

VSM 6 Power

Base Watts 2834, Max Watts 5852

- Servers: [914 (peak) 590 (idle)] times [two servers] equal [1828 (peak) 1180 (idle)]
- Each disk shelf: 503 (peak) 201 (Idle)
- Eight disk shelves: 4024 (peak) 1608 (Idle)
- Minimum total power (with two disk shelves): 2834 (peak) 1582 (Idle)
- Maximum total power (with eight disk shelves): 5852 (peak) 2788 (Idle)

VSM 6 HVAC

Base Watts 2834, Max Watts 5852

- Servers: [914 (peak) 590 (idle)] times [two servers] equal [1828 (peak) 1180 (idle)]
- Each disk shelf: 503 (peak) 201 (Idle)
- Eight disk shelves: 4024 (peak) 1608 (Idle)
- Minimum total power (with two disk shelves): 2834 (peak) 1582 (Idle)
- Maximum total power (with eight disk shelves): 5852 (peak) 2788 (Idle)

x3.414 BTUs/Watt: Base BTUs 9670, Max BTUs 19968

- Servers: [3119 (peak) 2013 (idle)] times [two servers] equal [6238 (peak) 4026 (idle)]
- Each disk shelf: 1716 (peak) 686 (Idle)
- Eight disk shelves: 13730 (peak) 5487 (Idle)
- Minimum total power (with two disk shelves): 9670 (peak) 5398 (Idle)
- Maximum total power (with eight disk shelves): 19968 (peak) 9513(Idle)

VSM 6 Ethernet (IP) Data Path Connectivity

VSM 6 supports direct and multi-port director switch attachment between VSM 6 and VLE appliances, and CLINKs to other VSM 6 or VSM 5 VTSSs.

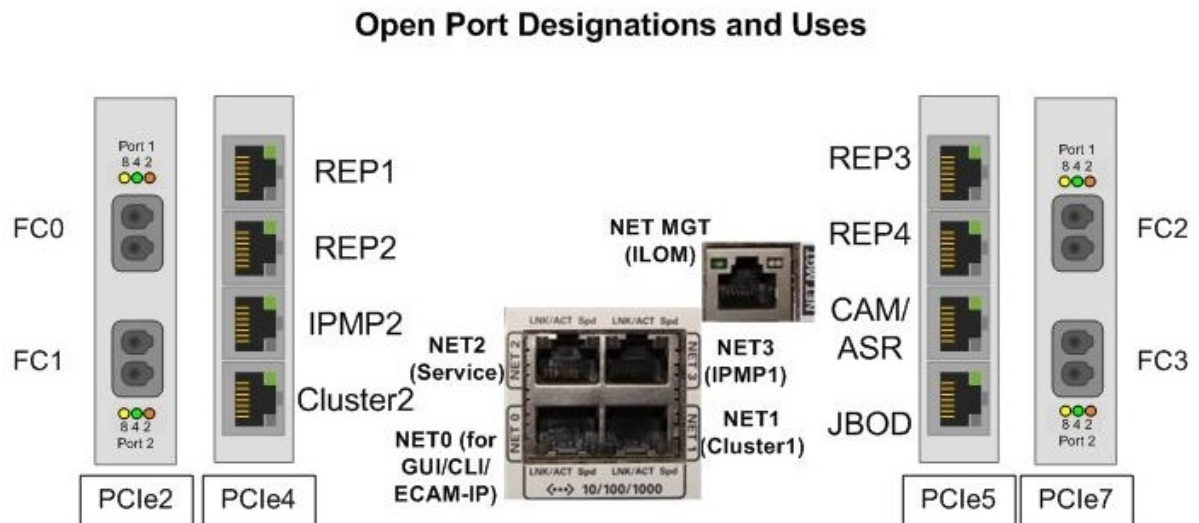
VLE traffic and CLINK traffic are not segregated by the VSM 6. Any RoIP port with connectivity will be used for either.

To define these connections, you need to define the RoIP ports that VSM 6 uses to replicate out and the ippaths to the targets.

VSM 6 Ethernet (IP) Port Assignments

As shown in [Figure 6–1](#), there are 12 Ethernet ports on each VSM 6 node. These port assignments assume Solaris 11.1 or higher is installed on the VSM 6 server nodes.

Figure 6–1 VSM 6 Ethernet Ports



- Port 0 (NET0) is for user interface connections (CLI, GUI, ECAM over IP).
- Port 1 (NET1), port 3 (NET3), port 6 (IPM2), and port 7 (Cluster2) are connected between nodes for cluster support.
- Port 2 (NET2) is a dedicated maintenance port reserved for direct connection by Services personnel.

- Ports 4, 5, 8, and 9 (REP1, REP2, REP3, and REP4) are available for connection to the customer-defined network for IP replication use.
- Port 10 (ASR) is available for Outbound ASR.
- Port 11 (JBOD) connects the server(s) to the first disk shelf above them in the stack.

Network Port Scenarios

Common network port scenarios include:

- Scenario 1: Connect the VSM 5 IFF port and a VSM 6 replication port in the data center.

Direct connections are made point-to-point with a network cable between interfaces, and the interface connections are on the same network. Only one connection is possible in this scenario. No gateway is required. Static routing is not required.

- Scenario 2: Connect a VSM 5 IFF port and a VLE port to a VSM 6 replication port in the data center.

Connections are between interfaces through a switch, and the interface connections are on the same network. From one to many connections are possible. No gateway is required. Static routing is not required.

- Scenario 3: Connect a VSM 6 replication port to a VSM 6 replication port in a remote data center, or set up ASR connection to a remote support site.

Connections between interfaces are through a gateway, and the interface connections are on different networks. From one to many connections are possible. A gateway is required. Static routing may be required if the customer cannot segregate and there is more than one route to the target.

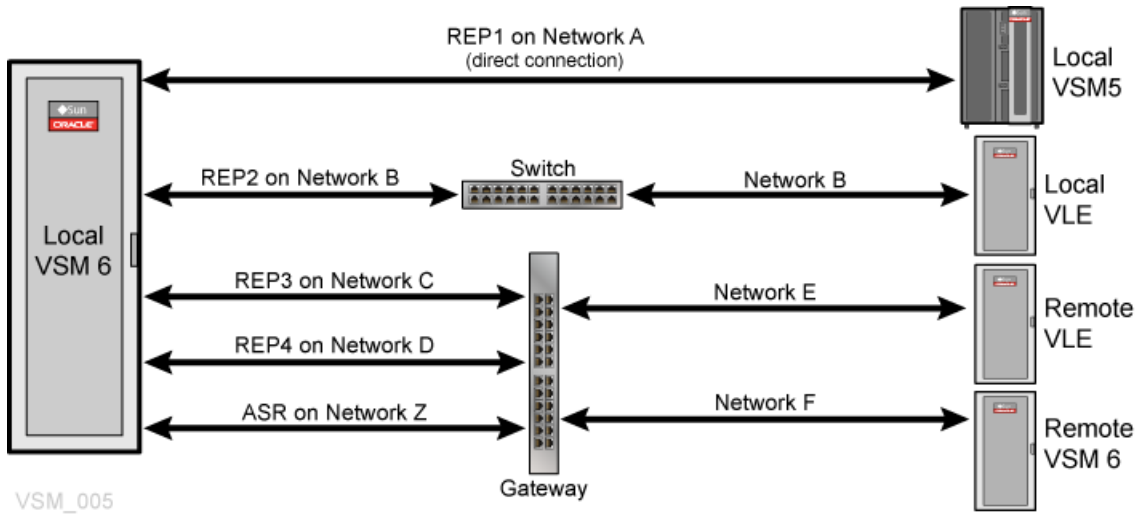
A VSM 6 node is configurable in an environment such that one, two, or all three scenarios are implemented.

Node Configuration Example

The example node configuration shown in [Figure 6–2](#) covers all three scenarios:

- The first replication port (network A) is connected directly to a local VSM 5 IFF port.
- The second replication port (network B) is connected to a local VLE port through a switch.
- The third replication port (network C) targets a remote VLE port on a different network.
- The fourth replication port (network D) targets replication ports on a remote VSM 6 port on a different network.
- ASR traffic (network Z) is sent to Oracle.

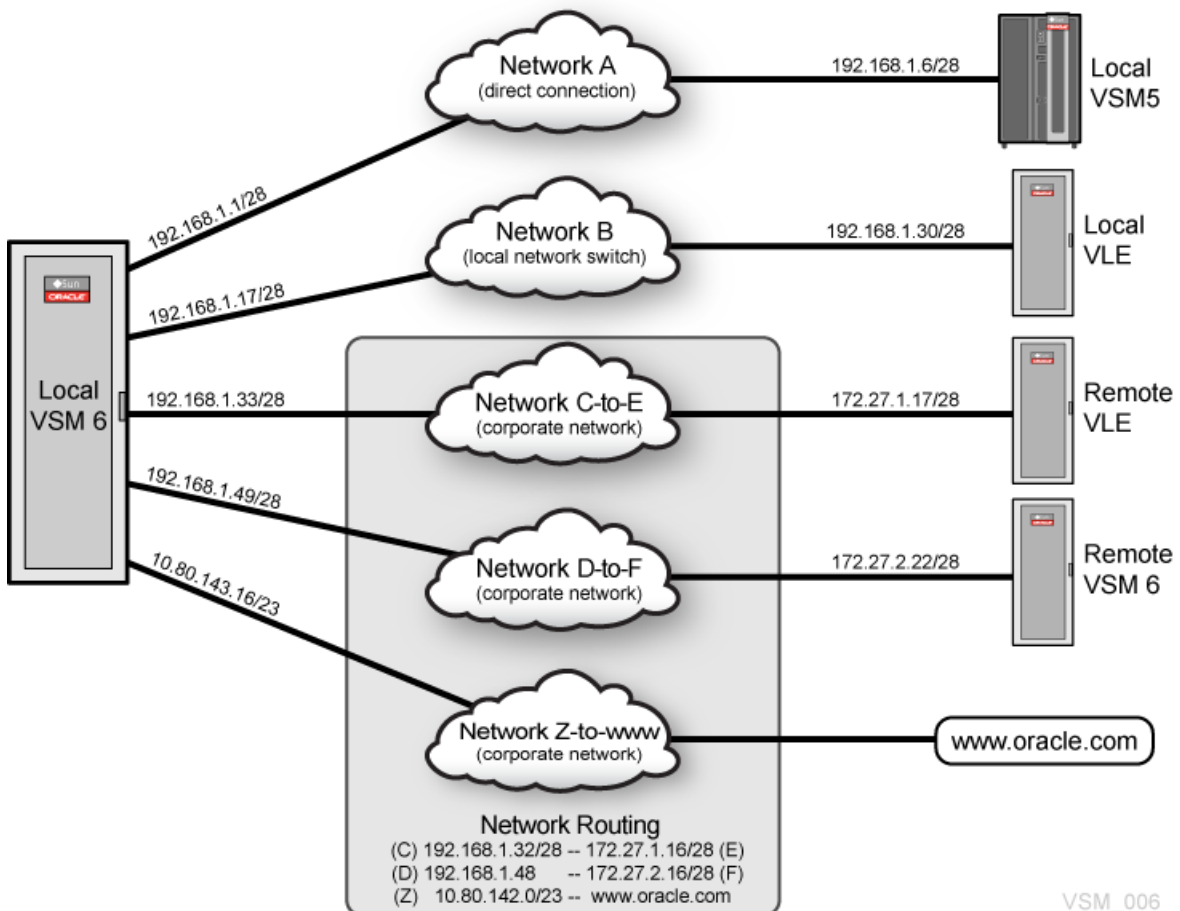
Figure 6-2 Node Configuration Example



Direct, Switched, and Gateway Configuration Scenarios

Figure 6-3 shows a network with a direct connection, a network with a switch connection, and three networks with connections through a gateway.

Figure 6-3 Example Direct, Switched, and Gateway Connection Scenarios



VSM 6 Ethernet (IP) Connectivity Considerations

As shown in [Table 6–1](#), replication and ASR ports on a VSM 6 node that are configured on the customer network must be on unique separate networks.

Table 6–1 Ports Configured on Customer Network Need Separate Networks

Location	Device	Link	Function	Customer Network	Separate Network
PCIE4	nxge0	net4	Replication	YES	YES
PCIE4	nxge1	net5	Replication	YES	YES
PCIE5	nxge4	net8	Replication	YES	YES
PCIE5	nxge5	net9	Replication	YES	YES
PCIE5	nxge6	net10	Automated Service Requests	YES	YES

[Table 6–2](#) shows two networks, each with 254 IP addresses. If two or more ports have IP addresses within the range, then the ports are on the same subnet.

Table 6–2 Two Networks, Each with /24 Prefix Length (254 IP Addresses)

Network	Netmask	Prefix Length	IP Address Range	Broadcast IP Address
192.168.1.0	255.255.255.0	/24	192.168.1.1 - 192.168.1.254	192.168.1.255
192.168.2.0	255.255.255.0	/24	192.168.2.1 - 192.168.2.254	192.168.2.255

In this example:

- Ports with addresses of 192.168.1.10/24 and 192.168.1.25/24 are on the same network.
- Ports with addresses of 192.168.1.10/24 and 192.168.2.25/24 are not on the same network.

Increasing the prefix length changes the netmask so that the 192.168.1.0 network is divisible into more networks or subnets. For example, as shown in [Table 6–3](#), if the prefix length is changed to /28, the number of hosts per subnet is reduced from 254 down to 14.

Note: You should plan ahead for future expansion needs during your initial configuration process. Reducing the prefix at a later time will affect adjacent networks and consequently will require network reconfiguration on all affected ports to ensure that IP addresses are valid and ports remain on separate networks.

Table 6–3 Subnet Size Considerations

Prefix	Netmask	Host IP Addresses per Subnet	Subnet Size Considerations
/24	255.255.255.0	254	Up to 254 total replication, VLE, and VSM5 ports in the subnet
/25	255.255.255.128	126	Up to 126 total replication, VLE, and VSM5 ports in the subnet
/26	255.255.255.192	62	Up to 62 total replication, VLE, and VSM5 ports in the subnet

Table 6–3 (Cont.) Subnet Size Considerations

Prefix	Netmask	Host IP Addresses per Subnet	Subnet Size Considerations
/27	255.255.255.224	30	Up to 30 total replication, VLE, and VSM5 ports in the subnet
/28	255.255.255.240	14	Up to 14 total replication, VLE, and VSM5 ports in the subnet
/29	255.255.255.248	6	Up to six total replication, VLE, and VSM5 ports in the subnet
/30	255.255.255.252	2	Maximum of one replication, VLE, or VSM5 port per VSM 6 node (two nodes total) in the subnet

As shown in Table 6–4, when the network prefix length is changed to /28, ports with addresses of 192.168.1.10/24 and 192.168.1.25/24 are no longer on the same network.

Table 6–4 Two Networks with /28 Network Prefix (14 IP Addresses)

Network	Netmask	Prefix Length	IP Address Range	Broadcast IP Address
192.168.1.0	255.255.255.240	/28	192.168.1.1 - 192.168.1.14	192.168.1.15
192.168.1.16	255.255.255.240	/28	192.168.1.17 - 192.168.1.30	192.168.1.31

WARNING: Infrastructure at the customer site must support any network configured on VSM 6 server nodes. Just configuring the ports and plugging them into a customer's network infrastructure is no guarantee that traffic will route properly.

Table 6–5 shows /28 networks to accommodate up to 14 network ports (a mix of VSM 6, VSM 5, and VLE ports) on a given network. The ASR port is on the customer's broader /23 network with a route to Oracle.

Note: Both VSM 6 nodes are configured separately and independently. Replication and ASR ports for nodes may or may not be on the same subnets. For example, the REP1 port on Node1 and the REP1 port on Node 2 may or may not be on the same subnet.

Table 6–5 /28 Networks and Ports Addresses

Port	Network	Netmask	Length	IP Address Range	Broadcast Address
REP1	192.168.1.0	255.255.255.240	/28	192.168.1.1 - 192.168.1.14	192.168.1.15
REP2	192.168.1.16	255.255.255.240	/28	192.168.1.17 - 192.168.1.30	192.168.1.31
REP3	192.168.1.32	255.255.255.240	/28	192.168.1.33 - 192.168.1.46	192.168.1.47
REP4	192.168.1.48	255.255.255.240	/28	192.168.1.49 - 192.168.1.62	192.168.1.63
ASR	10.80.142.0	255.255.254.0	/23	10.80.142.1 - 10.80.143.254	10.80.143.255

Table 6–6 shows a sample layout between local VSM 6 ports and various target network ports using IP addresses provided by the customer.

Table 6–6 Sample Layout for VSM 6 Node 1 Ports and Target Network Ports

Port (Node 1)	IP Address	Scenario	Gateway	Target Port	Target Address
VSM6-REP1	192.168.1.1/28	1 (Net A)	N/A	Local-VSM5	192.168.1.6/28
VSM6-REP2	192.168.1.17/28	2 (Net B)	N/A	Local-VLE	192.168.1.30/28
VSM6-REP3	192.168.1.33/28	3 (Net C)	192.168.1.46	Remote-VLE	172.27.1.17/28
VSM6-REP4	192.168.1.49/28	3 (Net D)	192.168.1.62	Remote-VSM 6	172.27.2.22/28
VSM6-ASR	10.80.143.16/23	3 (Net Z)	10.80.143.254	Oracle-Support	Oracle-Support

Table 6–7 shows Node 2 with ports on the same subnets as those on Node 1.

Note: If traffic to the remote-VLE and the remote-VSM can route from both VSM6-REP3 or VSM6-Rep4, then static routing may be necessary. Consequently, a gateway is required.

Table 6–7 Sample Layout for VSM 6 Node 2 Ports and Target Network Ports

Port (Node 2)	IP Address	Scenario	Gateway	Target Port	Target Address
VSM6-REP1	192.168.1.2/28	1 (Net A)	N/A	Local-VSM5	192.168.1.7/28
VSM6-REP2	192.168.1.18/28	2 (Net B)	N/A	Local-VLE	192.168.1.30/28
VSM6-REP3	192.168.1.34/28	3 (Net C)	192.168.1.46	Remote-VLE	172.27.1.17/28
VSM6-REP4	192.168.1.50/28	3 (Net D)	192.168.1.62	Remote-VSM 6	172.27.2.22/28
VSM6-ASR	10.80.143.17/23	3 (Net Z)	10.80.143.254	Oracle-Support	Oracle-Support

VSM 6 IP Connectivity Examples

The following examples illustrate IP connectivity between VSM 6 and a VLE or VTSS:

- [VSM 6 IP Replication: Define the Replication Ports](#)
- [VSM 6 VLE Connectivity: Define the IPPATH](#)
- [VSM 6 CLINK Connectivity: Define the IPPATH](#)

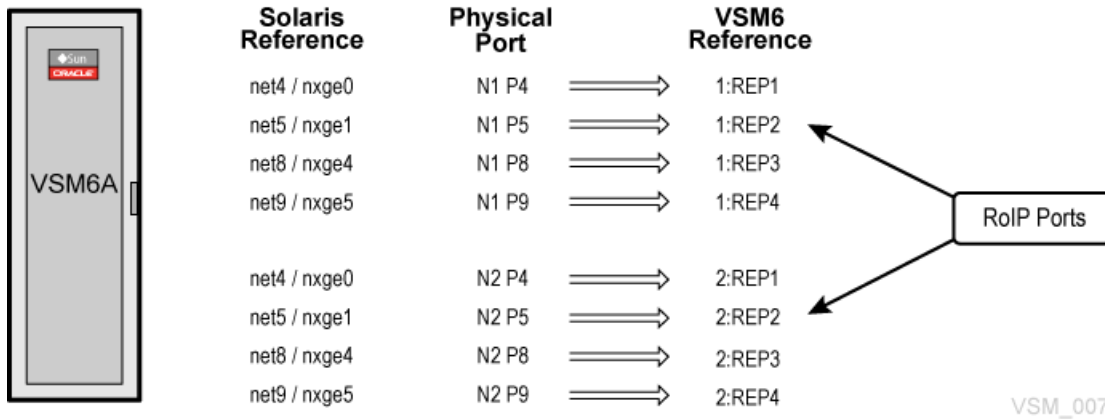
Each example includes:

- Connections between devices
- CLI commands that define the connections to the VSM 6
- VTCS commands that define the VSM 6 connections to the VTCS configuration

VSM 6 IP Replication: Define the Replication Ports

- Each port defined as an RoIP is just a route out from the VSM 6.
- The number of RoIP routes defined does not relate to the IPPATHs defined for the vRTD/CLINKs.
- Multiple RoIP ports provide bandwidth and resilience.

Figure 6-4 VSM 6 IP Replication – Define the Replication Ports



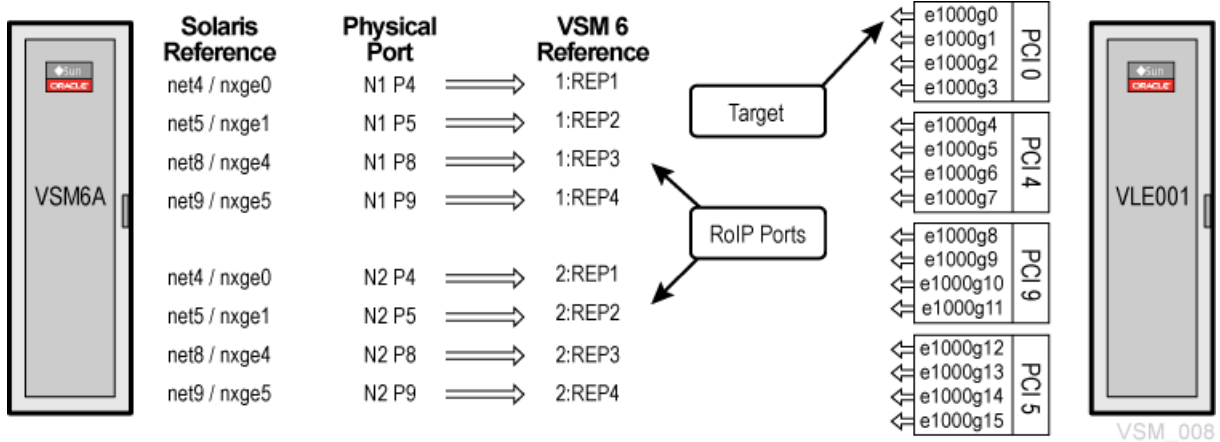
VSM 6 CLI Example:

```
vsmadmin: update ipport -name 1:REP1 -ip 35.107.24.1/24
vsmadmin: update ipport -name 2:REP2 -ip 35.107.25.2/24
```

VSM 6 VLE Connectivity: Define the IPPATH

- VTCS uses the VLE name of the target defined on the IPPATH command used in the VSM 6 CLI. Each IPPATH is just a route out of the VSM 6 to the VSM target.
- vRTDs are defined to VTCS as IP devices with IPIF ids.
- The IPIF id is not used to reference the definition but must be present to meet VTCS syntax rules. Each IPIF id must be unique and with valid syntax for each VSM 6 defined in VTCS.
- VTCS allows 16 IPIF ids total, so each VSM 6 can have a maximum combined total of 16 IP vRTDs/CLINKS in any combination.

Figure 6-5 VSM 6 VLE Connectivity – Define the IPPATH



VSM 6 CLI Example:

```
vsmadmin: add ippath -target vle -name V6VRTD00 -ip 35.107.22.10
```

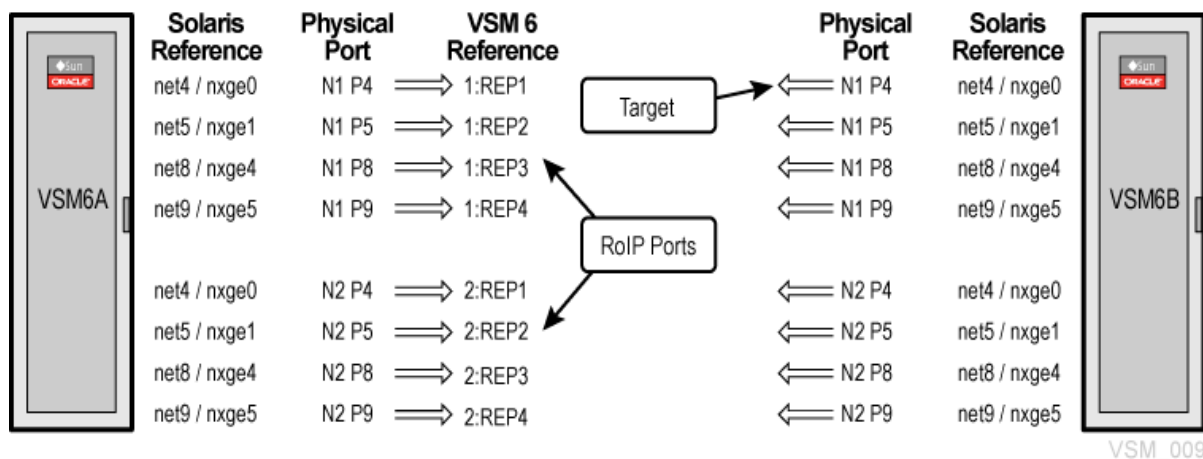
VTCS Example:

```
RTD NAME=V6VRTD00 STORMNGR=VLE001 IPIF=0A:0
```

VSM 6 CLINK Connectivity: Define the IPPATH

- VTCS and VSM 6 use the VSM partner on the CLINK definitions and the VTSS target name on the IPPATH command to link the CLINKs. Each IPPATH is just a route out of the VSM 6 to the VSM target.
- VTCS sees all VSM 6 CLINKs as IP devices.
- CLINKs are defined to VTCS as IP devices with IPIF ids.
- The IPIF id is not used to reference the definition but must be present to meet VTCS syntax rules. Each IPIF id must be unique for each VSM 6 defined in VTCS.
- VTCS allows 16 IPIF ids total, so each VSM 6 can have a maximum combined total of 16 IP vRTDs/CLINKS in any combination.
- VTCS can have multiple CLINKs defined even for a single IPPATH. Best practice is to define as many CLINKs to VTCS as possible.

Figure 6–6 VSM 6 CLINK Connectivity – Define the IPPATH



VSM 6 CLI Example:

```
vsmadmin: add ippath -target vtss -name VSM6B -ip 35.107.23.10
```

VTCS Example:

```
CLINK IPIF=0A:2 PARTNER=VSM6B
CLINK IPIF=0I:0 PARTNER=VSM6B
```

VSM 6 FICON Data Path Connectivity

FICON ports connect the two VSM 6 nodes to the ELS host software and VTCS interface software on the MVS host systems, and to Real Tape Drives (RTDs) in the tapeplex. Attachment may be direct or through a switch.

There are four FICON ports per VSM 6 node, a total of eight for the VTSS. Each port supports IBM Control Unit (CU) and IBM Channel Mode (CH) images concurrently, so that when connected through a switch each port may attach to both hosts and RTDs. Sharing a HOST port with an RTD connection does not reduce logical pathing.

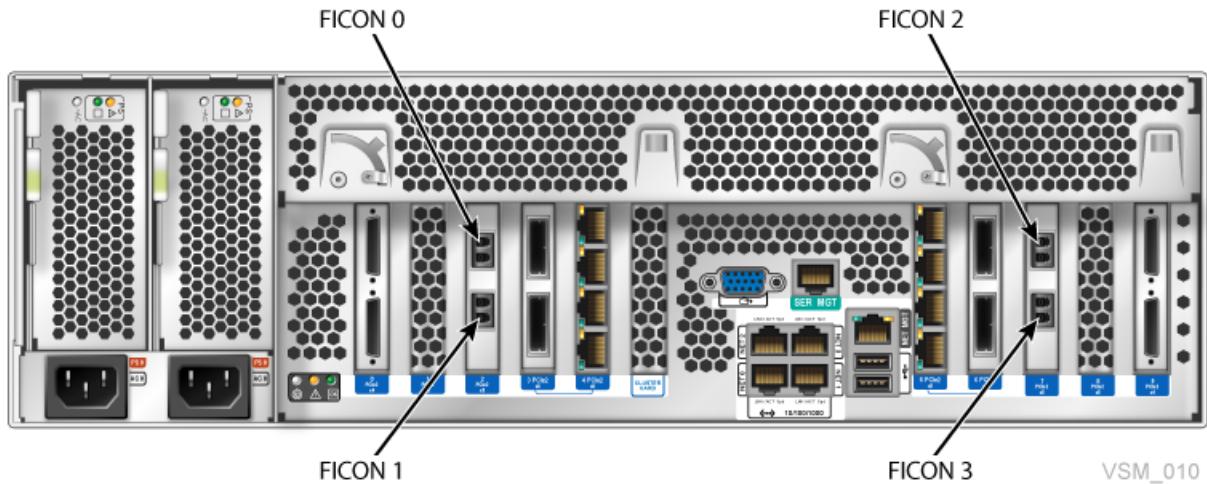
How it Works

- The link between the VSM 6 and VTCS is the RTD NAME.
- The link between VTCS and the RTD is the FICON cable to the relevant DEVNO in the relevant drive bay.
- VSM 6 CLI commands define the connections to the VSM 6.
- VTCS commands define the connections to the VTCS configuration.
- VTCS uses the RTD name defined on the FICONPATH command used in the VSM 6 CLI.
- Multiple FICONPATHs can route to the SAME RTD.
- Physical RTDs are defined to VTCS as FICON devices with CHANIF ids.
- The CHANIF id is not used to reference the device but must be present to meet VTCS syntax rules. Each CHANIF id must be unique and with valid syntax for each VSM 6 defined in VTCS.
- VTCS allows 32 unique CHANIF ids. Each VSM 6 can have a maximum of 32 physical RTDs defined.

VSM 6 FICON Port Assignments

As shown in [Figure 7-1](#), the FICON ports are numbered 0 to 3 beginning from the left top port when looking at the back of the server node.

Figure 7-1 VSM 6 FICON Port Assignments



VSM 6 RTD Connectivity Examples

The following examples illustrate FICON connectivity between VSM 6 and RTDs:

- VSM 6 RTD Connectivity: Direct Connection
- VSM 6 RTD Connectivity: Single Switch
- VSM 6 RTD Connectivity: Cascaded Switch
- VSM 6 RTD Connectivity: Dual RTDs
- VSM 6 RTD Connectivity: Four RTDs One Port
- VSM 6 RTD Connectivity: Dual-Path RTD
- VSM 6 RTD Connectivity: Dual-Path Dual RTD
- VSM 6 RTD Connectivity: Multi-Path Dual RTD

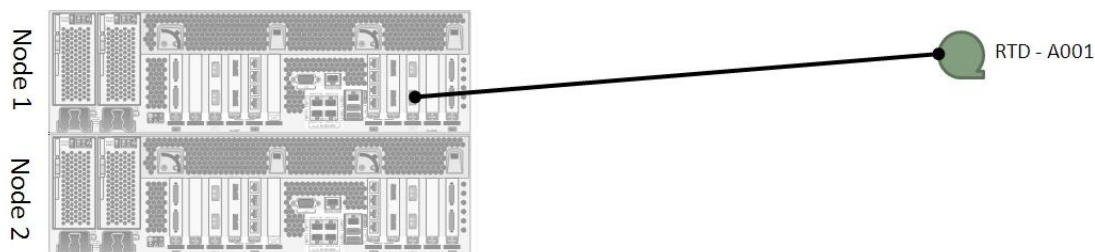
Each example includes:

- Connections between devices
- CLI commands that define the connections to the VSM 6
- VTCS commands that define the VSM 6 connections to the VTCS configuration

VSM 6 RTD Connectivity: Direct Connection

Figure 7-2 shows a direct connection between a VSM 6 FICON port and an RTD.

Figure 7-2 VSM 6 RTD Connectivity – Direct Connection



VSM 6 CLI Example:

```
vsmadmin: add ficonpath -name RTDA001 -node 1 -port 3
```

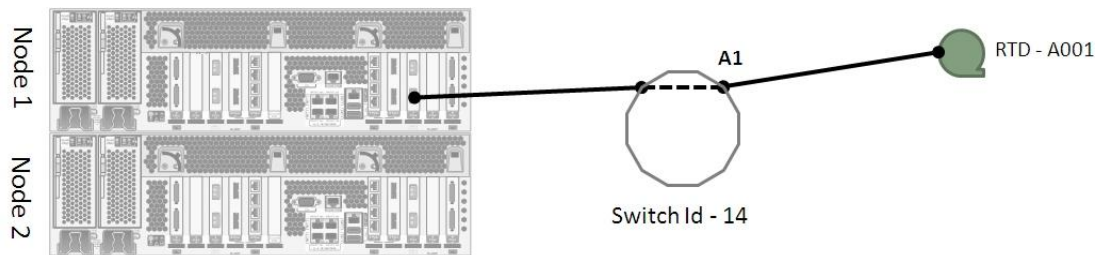
VTCS Example:

```
RTD NAME=RTDA001 DEVNO=A001 CHANIF=0A:0
```

VSM 6 RTD Connectivity: Single Switch

Figure 7–3 shows a connection through a single switch between a VSM 6 FICON port and an RTD:

Figure 7–3 VSM 6 RTD Connectivity – Single Switch



VSM 6 CLI Example:

```
vsmadmin: add ficonpath -name RTDA001 -node 1 -port 3 -area A1
```

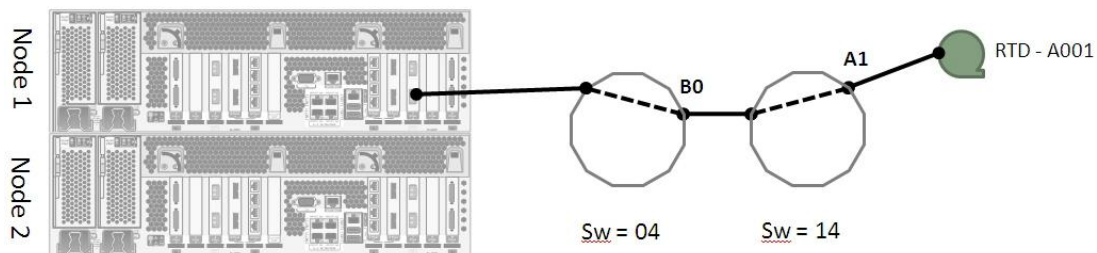
VTCS Example:

```
RTD NAME=RTDA001 DEVNO=A001 CHANIF=0A:0
```

VSM 6 RTD Connectivity: Cascaded Switch

Figure 7–4 shows a connection through cascaded switches between a VSM 6 FICON port and an RTD.

Figure 7–4 VSM 6 RTD Connectivity – Cascaded Switch



VSM 6 CLI Example:

```
vsmadmin: add ficonpath -name RTDA001 -node 1 -port 3 -domain 14 -area A1
```

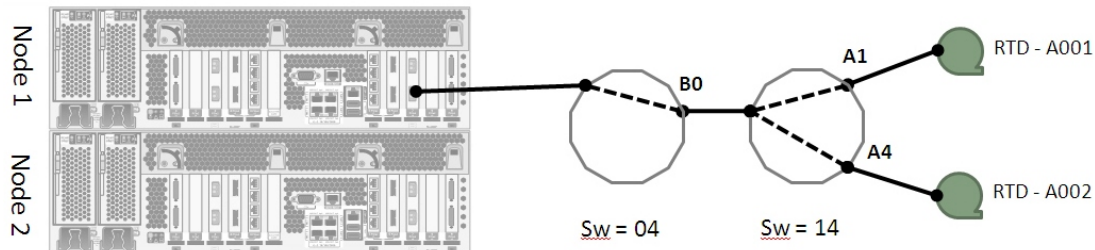
VTCS Example:

```
RTD NAME=RTDA001 DEVNO=A001 CHANIF=0A:0
```

VSM 6 RTD Connectivity: Dual RTDs

Figure 7-5 shows a connection through cascaded switches between a VSM 6 FICON port and two RTDs.

Figure 7-5 VSM 6 RTD Connectivity – Dual RTDs



VSM 6 CLI Example:

```
vsmadmin: add ficonpath -name RTDA001 -node 1 -port 3 -domain 14 -area A1
vsmadmin: add ficonpath -name RTDA002 -node 1 -port 3 -domain 14 -area A4
```

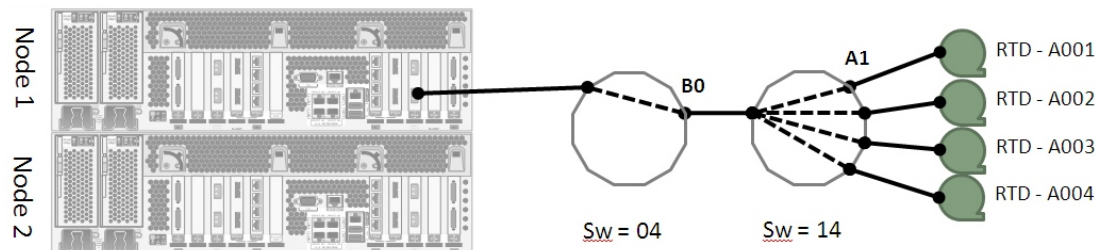
VTCS Example:

```
RTD NAME=RTDA001 DEVNO=A001 CHANIF=0A:0
RTD NAME=RTDA002 DEVNO=A002 CHANIF=0C:0
```

VSM 6 RTD Connectivity: Four RTDs One Port

Figure 7-6 shows a connection through cascaded switches between a VSM 6 FICON port and four RTDs. This is the maximum number of RTDs you can connect to a single VSM 6 FICON port, and there are eight ports total, so 32 RTDs maximum per VSM 6.

Figure 7-6 VSM 6 RTD Connectivity – Four RTDs One Port



VSM 6 CLI Example:

```
vsmadmin: add ficonpath -name RTDA001 -node 1 -port 3 -domain 14 -area A1
vsmadmin: add ficonpath -name RTDA002 -node 1 -port 3 -domain 14 -area A2
vsmadmin: add ficonpath -name RTDA003 -node 1 -port 3 -domain 14 -area A3
vsmadmin: add ficonpath -name RTDA004 -node 1 -port 3 -domain 14 -area A4
```

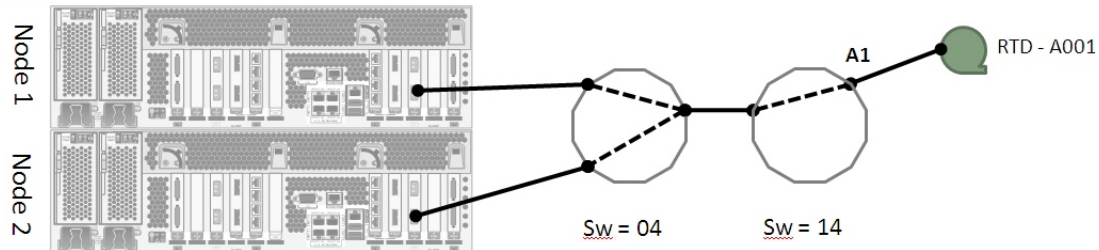
VTCS Example:

```
RTD NAME=RTDA001 DEVNO=A001 CHANIF=0A:0
RTD NAME=RTDA002 DEVNO=A002 CHANIF=0K:0
RTD NAME=RTDA003 DEVNO=A003 CHANIF=1M:0
RTD NAME=RTDA004 DEVNO=A004 CHANIF=00:0
```


VSM 6 RTD Connectivity: Dual-Path RTD

Figure 7-7 and Figure 7-8 show two FICON paths to the same RTD. The connections are between two VSM 6 FICON ports located on separate VSM 6 nodes, through cascaded switches, to a single RTD. There is a single definition for the RTD in VTCS, and the VTSS resolves access down either path.

Figure 7-7 VSM 6 RTD Connectivity – Dual-Path RTD Example 1



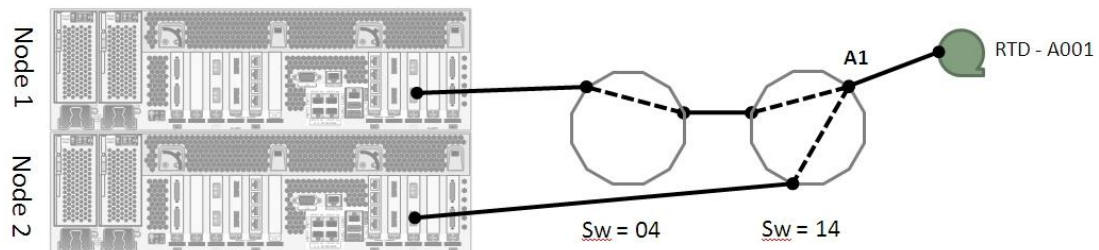
VSM 6 CLI Example 1:

```
vsmadmin: add ficonpath -name RTDA001 -node 1 -port 3 -domain 14 -area A1
vsmadmin: add ficonpath -name RTDA001 -node 2 -port 3 -domain 14 -area A1
```

VTCS Example 1:

```
RTD NAME=RTDA001 DEVNO=A001 CHANIF=0A:0
```

Figure 7-8 VSM 6 RTD Connectivity – Dual-Path RTD Example 2



VSM 6 CLI Example 2:

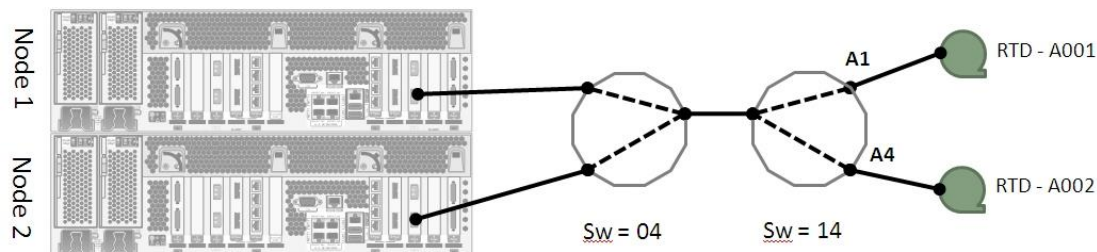
```
vsmadmin: add ficonpath -name RTDA001 -node 1 -port 3 -domain 14 -area A1
vsmadmin: add ficonpath -name RTDA001 -node 2 -port 3 -area A1
```

VTCS Example 2:

```
RTD NAME=RTDA001 DEVNO=A001 CHANIF=0A:0
```

VSM 6 RTD Connectivity: Dual-Path Dual RTD

Figure 7-9 shows two FICON paths to two different RTDs. The connections are between two VSM 6 FICON ports located on separate VSM 6 nodes, through cascaded switches, to two RTDs.

Figure 7–9 VSM 6 RTD Connectivity – Dual-Path Dual RTD**VSM 6 CLI Example:**

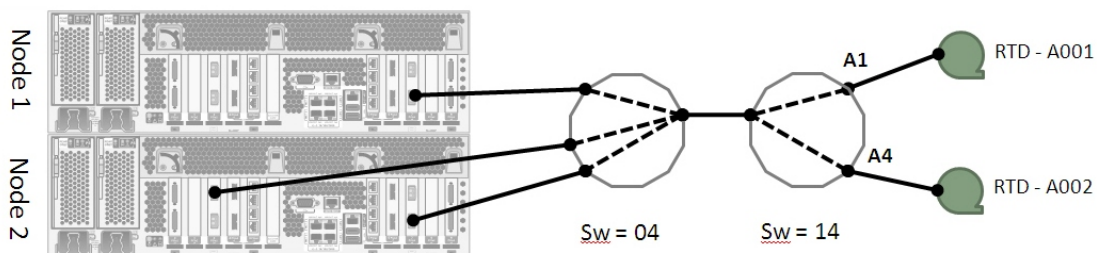
```
vsmadmin: add ficonpath -name RTDA001 -node 1 -port 3 -domain 14 -area A1
vsmadmin: add ficonpath -name RTDA001 -node 2 -port 3 -domain 14 -area A1
vsmadmin: add ficonpath -name RTDA002 -node 1 -port 3 -domain 14 -area A4
vsmadmin: add ficonpath -name RTDA002 -node 2 -port 3 -domain 14 -area A4
```

VTCS Example:

```
RTD NAME=RTDA001 DEVNO=A001 CHANIF=0A:0
RTD NAME=RTDA002 DEVNO=A002 CHANIF=0C:0
```

VSM 6 RTD Connectivity: Multi-Path Dual RTD

Figure 7–10 shows multiple FICON paths to two different RTDs. The connections are between three VSM 6 FICON ports located on two separate VSM 6 nodes, through cascaded switches, to two separate RTDs. In this example, there are six FICON paths defined on the VSM 6 and two RTDs defined to VTCS.

Figure 7–10 VSM 6 RTD Connectivity – Multi-Path Dual RTD**VSM 6 CLI Example:**

```
vsmadmin: add ficonpath -name RTDA001 -node 1 -port 3 -domain 14 -area A1
vsmadmin: add ficonpath -name RTDA001 -node 2 -port 0 -domain 14 -area A1
vsmadmin: add ficonpath -name RTDA001 -node 2 -port 3 -domain 14 -area A1
vsmadmin: add ficonpath -name RTDA002 -node 1 -port 3 -domain 14 -area A4
vsmadmin: add ficonpath -name RTDA002 -node 2 -port 0 -domain 14 -area A4
vsmadmin: add ficonpath -name RTDA002 -node 2 -port 3 -domain 14 -area A4
```

VTCS Example:

```
RTD NAME=RTDA001 DEVNO=A001 CHANIF=0A:0
RTD NAME=RTDA002 DEVNO=A002 CHANIF=0C:0
```

Data at Rest Encryption Feature

VSM 6.1 and higher supports a feature for encrypting data at rest on the disk shelf disk drives. Solaris 11.1 ZFS performs the actual encryption when the feature is enabled. Solaris ZFS is FIPS 140-2 certified.

The service person enables the encryption feature by running a utility from a command shell on node 1 of the VSM 6 system. The feature utility can only be run while the VSM 6 application is shut down.

For a new installation with no customer data, it only takes a few minutes to enable or disable encryption.

For an existing VSM 6 that already has customer data present, the encryption feature can be enabled only if the current utilization of the disk shelf arrays is less than 45 per cent of total physical capacity.

Conversion of existing data (either from un-encrypted to encrypted or from encrypted to un-encrypted) takes approximately 105 minutes per TB of physical data.

Once VTV data encryption at rest has been enabled, the fact that data is encrypted before being written to disk and decrypted as it is read is largely transparent to the rest of the system. Throughput performance is reduced by less than five per cent.

When the encryption feature is enabled, the encryption authorization key is stored at a fixed location in the mirrored server's rpool disk drives, and a backup copy is created on a USB storage device. The USB storage device is required to be available when this feature is being enabled.

Only one USB storage device must be plugged into a VSM 6 node 1 USB port when the encryption authorization key is created. If multiple USB storage devices are discovered, the key creation will fail.

If the encryption authorization key is lost from the mirrored server's rpool disks, a script is provided to restore the key from the USB storage device used to back up the key when it was created or changed.

The VSM6 application will fail to start if the customer data file systems cannot be mounted due to the encryption authorization key not being present.

The ZFS-supported encryption algorithm used is AES-256-CCM. The authorization key is a 256-bit file, generated by the `pktool(1)` utility program, invoked by the encryption feature utility.

Capacity upgrades to an encryption-enabled VSM 6 will simply increase the storage size of the disk shelves arrays storage, maintaining the encryption setting that exists at upgrade time.

Software upgrades to the VSM 6 will preserve the encryption authorization key(s) stored on the mirrored server's rpool disk drives.

The VSM 6 CLI and Service GUI will indicate if the encryption feature is enabled.

The Service GUI allows the service person to change the encryption authorization key. Changing the key does not invalidate access to any VTV data stored before the change. Changing the key simply obsoletes the prior encryption authorization key and generates a new key that is required to validate access to the encrypted VTV file systems. Changing the key, like at creation time, requires a single USB storage device to be discovered, as the backup location for a key stored in the mirrored servers rpool disk drives.

The encryption authorization key is stored on the mirrored rpool disk drives on both servers. The key will be located in the `/lib/svc/method/application/vsm/.vsm_` keystore directory. The file name format of the key will be `_yyymmddhhmmssnnn.key`. Prior generations of keys will be maintained in the same directory. Whenever a key is created, or changed, all generations of the keys in this directory are backed up to the USB storage device.

Controlling Contaminants

- Environmental Contaminants
- Required Air Quality Levels
- Contaminant Properties and Sources
- Contaminant Effects
- Room Conditions
- Exposure Points
- Filtration
- Positive Pressurization and Ventilation
- Cleaning Procedures and Equipment
- Activity and Processes

Environmental Contaminants

Control over contaminant levels in a computer room is extremely important because tape libraries, tape drives, and tape media are subject to damage from airborne particulates. Most particles smaller than ten microns are not visible to the naked eye under most conditions, but these particles can be the most damaging. As a result, the operating environment must adhere to the following requirements:

- ISO 14644-1 Class 8 Environment.
- The total mass of airborne particulates must be less than or equal to 200 micrograms per cubic meter.
- Severity level G1 per ANSI/ISA 71.04-1985.

Oracle currently requires the ISO 14644-1 standard approved in 1999, but will require any updated standards for ISO 14644-1 as they are approved by the ISO governing body. The ISO 14644-1 standard primarily focuses on the quantity and size of particulates and the proper measurement methodology, but does not address the overall mass of the particulates. As a result, the requirement for total mass limitations is also necessary as a computer room or data center could meet the ISO 14644-1 specification, but still damage equipment because of the specific type of particulates in the room. In addition, the ANSI/ISA 71.04-1985 specification addresses gaseous contaminations as some airborne chemicals are more hazardous. All three requirements are consistent with the requirements set by other major tape storage vendors.

Required Air Quality Levels

Particles, gasses and other contaminants may impact the sustained operations of computer hardware. Effects can range from intermittent interference to actual component failures. The computer room must be designed to achieve a high level of cleanliness. Airborne dusts, gasses and vapors must be maintained within defined limits to help minimize their potential impact on the hardware.

Airborne particulate levels must be maintained within the limits of *ISO 14644-1 Class 8 Environment*. This standard defines air quality classes for clean zones based on airborne particulate concentrations. This standard has an order of magnitude less particles than standard air in an office environment. Particles ten microns or smaller are harmful to most data processing hardware because they tend to exist in large numbers, and can easily circumvent many sensitive components' internal air filtration systems. When computer hardware is exposed to these submicron particles in great numbers they endanger system reliability by posing a threat to moving parts, sensitive contacts and component corrosion.

Excessive concentrations of certain gasses can also accelerate corrosion and cause failure in electronic components. Gaseous contaminants are a particular concern in a computer room both because of the sensitivity of the hardware, and because a proper computer room environment is almost entirely recirculating. Any contaminant threat in the room is compounded by the cyclical nature of the airflow patterns. Levels of exposure that might not be concerning in a well ventilated site repeatedly attack the hardware in a room with recirculating air. The isolation that prevents exposure of the computer room environment to outside influences can also multiply any detrimental influences left unaddressed in the room.

Gasses that are particularly dangerous to electronic components include chlorine compounds, ammonia and its derivatives, oxides of sulfur and petrol hydrocarbons. In the absence of appropriate hardware exposure limits, health exposure limits must be used.

While the following sections will describe some best practices for maintaining an ISO 14644-1 Class 8 Environment in detail, there are some basic precautions that must be adhered to:

- Do not allow food or drink into the area.
- Cardboard, wood, or packing materials must not be stored in the data center clean area.
- Identify a separate area for unpacking new equipment from crates and boxes.
- Do not allow construction or drilling in the data center without first isolating sensitive equipment and any air targeted specifically for the equipment. Construction generates a high level of particulates that exceed ISO 14644-1 Class 8 criteria in a localized area. Dry wall and gypsum are especially damaging to storage equipment.

Contaminant Properties and Sources

Contaminants in the room can take many forms, and can come from numerous sources. Any mechanical process in the room can produce dangerous contaminants or agitate settled contaminants. A particle must meet two basic criteria to be considered a contaminant:

- It must have the physical properties that could potentially cause damage to the hardware.

- It must be able to migrate to areas where it can cause the physical damage.

The only differences between a potential contaminant and an actual contaminant are time and location. Particulate matter is most likely to migrate to areas where it can do damage if it is airborne. For this reason, airborne particulate concentration is a useful measurement in determining the quality of the computer room environment.

Depending on local conditions, particles as big as 1,000 microns can become airborne, but their active life is very short, and they are arrested by most filtration devices.

Submicron particulates are much more dangerous to sensitive computer hardware because they remain airborne much longer and are more apt to bypass filters.

Operator Activity

Human movement within the computer space is probably the single greatest source of contamination in an otherwise clean computer room. Normal movement can dislodge tissue fragments, such as dander or hair, or fabric fibers from clothing. The opening and closing of drawers or hardware panels or any metal-on-metal activity can produce metal filings. Simply walking across the floor can agitate settled contamination making it airborne and potentially dangerous.

Hardware Movement

Hardware installation or reconfiguration involves a great deal of subfloor activity, and settled contaminants can very easily be disturbed, forcing them to become airborne in the supply air stream to the room's hardware. This is particularly dangerous if the subfloor deck is unsealed. Unsealed concrete sheds fine dust particles into the airstream, and is susceptible to efflorescence -- mineral salts brought to the surface of the deck through evaporation or hydrostatic pressure.

Outside Air

Inadequately filtered air from outside the controlled environment can introduce innumerable contaminants. Post-filtration contamination in duct work can be dislodged by air flow, and introduced into the hardware environment. This is particularly important in a downward-flow air conditioning system in which the sub-floor void is used as a supply air duct. If the structural deck is contaminated, or if the concrete slab is not sealed, fine particulate matter (such as concrete dust or efflorescence) can be carried directly to the room's hardware.

Stored Items

Storage and handling of unused hardware or supplies can also be a source of contamination. Corrugated cardboard boxes or wooden skids shed fibers when moved or handled. Stored items are not only contamination sources; their handling in the computer room controlled areas can agitate settled contamination already in the room.

Outside Influences

A negatively pressurized environment can allow contaminants from adjoining office areas or the exterior of the building to infiltrate the computer room environment through gaps in the doors or penetrations in the walls. Ammonia and phosphates are often associated with agricultural processes, and numerous chemical agents can be produced in manufacturing areas. If such industries are present near the data center facility, chemical filtration may be necessary. Potential impact from automobile emissions, dusts from local quarries or masonry fabrication facilities or sea mists should also be assessed if relevant.

Cleaning Activity

Inappropriate cleaning practices can also degrade the environment. Many chemicals used in normal or “office” cleaning applications can damage sensitive computer equipment. Potentially hazardous chemicals outlined in the "[Cleaning Procedures and Equipment](#)" section should be avoided. Out-gassing from these products or direct contact with hardware components can cause failure. Certain biocide treatments used in building air handlers are also inappropriate for use in computer rooms either because they contain chemicals, that can degrade components, or because they are not designed to be used in the airstream of a re-circulating air system. The use of push mops or inadequately filtered vacuums can also stimulate contamination.

It is essential that steps be taken to prevent air contaminants, such as metal particles, atmospheric dust, solvent vapors, corrosive gasses, soot, airborne fibers or salts from entering or being generated within the computer room environment. In the absence of hardware exposure limits, use applicable human exposure limits from OSHA, NIOSH or the ACGIH.

Contaminant Effects

Destructive interactions between airborne particulate and electronic instrumentation can occur in numerous ways. The means of interference depends on the time and location of the critical incident, the physical properties of the contaminant and the environment in which the component is placed.

Physical Interference

Hard particles with a tensile strength at least 10% greater than that of the component material can remove material from the surface of the component by grinding action or embedding. Soft particles will not damage the surface of the component, but can collect in patches that can interfere with proper functioning. If these particles are tacky they can collect other particulate matter. Even very small particles can have an impact if they collect on a tacky surface, or agglomerate as the result of electrostatic charge build-up.

Corrosive Failure

Corrosive failure or contact intermittence due to the intrinsic composition of the particles or due to absorption of water vapor and gaseous contaminants by the particles can also cause failures. The chemical composition of the contaminant can be very important. Salts, for instance, can grow by absorbing water vapor from the air (nucleating). If a mineral salts deposit exists in a sensitive location, and the environment is sufficiently moist, it can grow to a size where it can physically interfere with a mechanism, or can cause damage by forming salt solutions.

Shorts

Conductive pathways can arise through the accumulation of particles on circuit boards or other components. Many types of particulate are not inherently conductive, but can absorb significant quantities of water in high-moisture environments. Problems caused by electrically conductive particles can range from intermittent malfunctioning to actual damage to components and operational failures.

Thermal Failure

Premature clogging of filtered devices will cause a restriction in air flow that could induce internal overheating and head crashes. Heavy layers of accumulated dust on hardware components can also form an insulative layer that can lead to heat-related failures.

Room Conditions

All surfaces within the controlled zone of the data center should be maintained at a high level of cleanliness. All surfaces should be periodically cleaned by trained professionals on a regular basis, as outlined in the "[Cleaning Procedures and Equipment](#)" section. Particular attention should be paid to the areas beneath the hardware, and the access floor grid. Contaminants near the air intakes of the hardware can more easily be transferred to areas where they can do damage. Particulate accumulations on the access floor grid can be forced airborne when floor tiles are lifted to gain access to the sub-floor.

The subfloor void in a downward-flow air conditioning system acts as the supply air plenum. This area is pressurized by the air conditioners, and the conditioned air is then introduced into the hardware spaces through perforated floor panels. Thus, all air traveling from the air conditioners to the hardware must first pass through the subfloor void. Inappropriate conditions in the supply air plenum can have a dramatic effect on conditions in the hardware areas.

The subfloor void in a data center is often viewed solely as a convenient place to run cables and pipes. It is important to remember that this is also a duct, and that conditions below the false floor must be maintained at a high level of cleanliness. Contaminant sources can include degrading building materials, operator activity or infiltration from outside the controlled zone. Often particulate deposits are formed where cables or other subfloor items form air dams that allow particulate to settle and accumulate. When these items are moved, the particulate is re-introduced into the supply airstream, where it can be carried directly to hardware.

Damaged or inappropriately protected building materials are often sources of subfloor contamination. Unprotected concrete, masonry block, plaster or gypsum wall-board will deteriorate over time, shedding fine particulate into the air. Corrosion on post-filtration air conditioner surfaces or subfloor items can also be a concern. The subfloor void must be completely and appropriately decontaminated on a regular basis to address these contaminants. Use only vacuums equipped with High Efficiency Particulate Air (HEPA) filtration in any decontamination procedure. Inadequately filtered vacuums will not arrest fine particles, passing them through the unit at high speeds, and forcing them airborne.

Unsealed concrete, masonry or other similar materials are subject to continued degradation. The sealants and hardeners normally used during construction are often designed to protect the deck against heavy traffic, or to prepare the deck for the application of flooring materials, and are not meant for the interior surfaces of a supply air plenum. While regular decontaminations will help address loose particulate, the surfaces will still be subject to deterioration over time, or as subfloor activity causes wear. Ideally all of the subfloor surfaces will be appropriately sealed at the time of construction. If this is not the case, special precautions will be necessary to address the surfaces in an on-line room.

It is extremely important that only appropriate materials and methodology are used in the encapsulation process. Inappropriate sealants or procedures can actually degrade the conditions they are meant to improve, impacting hardware operations and

reliability. The following precautions should be taken when encapsulating the supply air plenum in an on-line room:

- Manually apply the encapsulant. Spray applications are totally inappropriate in an on-line data center. The spraying process forces the sealant airborne in the supply airstream, and is more likely to encapsulate cables to the deck.
- Use a pigmented encapsulant. The pigmentation makes the encapsulant visible in application, ensuring complete coverage, and helps in identifying areas that are damaged or exposed over time.
- It must have a high flexibility and low porosity to effectively cover the irregular textures of the subject area, and to minimize moisture migration and water damage.
- The encapsulant must not out-gas any harmful contaminants. Many encapsulants commonly used in industry are highly ammoniated or contain other chemicals that can be harmful to hardware. It is very unlikely that this out-gassing could cause immediate, catastrophic failure, but these chemicals will often contribute to corrosion of contacts, heads or other components.

Effectively encapsulating a subfloor deck in an on-line computer room is a very sensitive and difficult task, but it can be conducted safely if appropriate procedures and materials are used. Avoid using the ceiling void as an open supply or return for the building air system. This area is typically very dirty and difficult to clean. Often the structural surfaces are coated with fibrous fire-proofing, and the ceiling tiles and insulation are also subject to shedding. Even before filtration, this is an unnecessary exposure that can adversely affect environmental conditions in the room. It is also important that the ceiling void does not become pressurized, as this will force dirty air into the computer room. Columns or cable chases with penetrations in both the subfloor and ceiling void can lead to ceiling void pressurization.

Exposure Points

All potential exposure points in the data center should be addressed to minimize potential influences from outside the controlled zone. Positive pressurization of the computer rooms will help limit contaminant infiltration, but it is also important to minimize any breaches in the room perimeter. To ensure the environment is maintained correctly, the following should be considered:

- All doors should fit snugly in their frames.
- Use gaskets and sweeps to address any gaps.
- Automatic doors should be avoided in areas where they can be accidentally triggered. An alternate means of control would be to remotely locate a door trigger so that personnel pushing carts can open the doors easily. In highly sensitive areas, or where the data center is exposed to undesirable conditions, it may be advisable to design and install personnel traps. Double sets of doors with a buffer between can help limit direct exposure to outside conditions.
- Seal all penetrations between the data center and adjacent areas.
- Avoid sharing a computer room ceiling or subfloor plenum with loosely controlled adjacent areas.

Filtration

Filtration is an effective means of addressing airborne particulate in a controlled environment. It is important that all air handlers serving the data center are

adequately filtered to ensure appropriate conditions are maintained within the room. In-room process cooling is the recommended method of controlling the room environment. The in-room process coolers re-circulate room air. Air from the hardware areas is passed through the units where it is filtered and cooled, and then introduced into the subfloor plenum. The plenum is pressurized, and the conditioned air is forced into the room, through perforated tiles, which then travels back to the air conditioner for reconditioning. The airflow patterns and design associated with a typical computer room air handler have a much higher rate of air change than typical comfort cooling air conditioners so air is filtered much more often than in an office environment. Proper filtration can capture a great deal of particulates. The filters installed in the in-room, re-circulating air conditioners should have a minimum efficiency of 40% (Atmospheric Dust-Spot Efficiency, ASHRAE Standard 52.1). Low-grade pre-filters should be installed to help prolong the life of the more expensive primary filters.

Any air being introduced into the computer room controlled zone, for ventilation or positive pressurization, should first pass through high efficiency filtration. Ideally, air from sources outside the building should be filtered using High Efficiency Particulate Air (HEPA) filtration rated at 99.97% efficiency (DOP Efficiency MILSTD-282) or greater. The expensive high efficiency filters should be protected by multiple layers of pre-filters that are changed on a more frequent basis. Low-grade pre-filters, 20% ASHRAE atmospheric dust-spot efficiency, should be the primary line of defense. The next filter bank should consist of pleated or bag type filters with efficiencies between 60% and 80% ASHRAE atmospheric dust-spot efficiency. Table A-1 shows fractional efficiency percentage for three filtration types.

Table A-1 Dust-Spot Fractional Efficiency Percentages

ASHRAE 52-76 Dust-Spot Efficiency Percentage	3.0 micron	1.0 micron	0.3 micron
25-30	80	20	<5
60-65	93	50	20
80-85	99	90	50
90	>99	92	60
DOP 95	--	>99	95

Low efficiency filters are almost totally ineffective at removing sub-micron particulates from the air. It is also important that the filters used are properly sized for the air handlers. Gaps around the filter panels can allow air to bypass the filter as it passes through the air conditioner. Any gaps or openings should be filled using appropriate materials, such as stainless steel panels or custom filter assemblies.

Positive Pressurization and Ventilation

A designed introduction of air from outside the computer room system will be necessary to accommodate positive pressurization and ventilation requirements. The data center should be designed to achieve positive pressurization in relation to more loosely controlled surrounding areas. Positive pressurization of the more sensitive areas is an effective means of controlling contaminant infiltration through any minor breaches in the room perimeter. Positive pressure systems are designed to apply outward air forces to doorways and other access points within the data processing center to minimize contaminant infiltration of the computer room. Only a minimal amount of air should be introduced into the controlled environment. In data centers with multiple rooms, the most sensitive areas should be the most highly pressurized. It is, however, extremely important that the air being used to positively pressurize the

room does not adversely affect the environmental conditions in the room. It is essential that any air introduction from outside the computer room is adequately filtered and conditioned to ensure that it is within acceptable parameters. These parameters can be looser than the goal conditions for the room since the air introduction should be minimal. A precise determination of acceptable limits should be based on the amount of air being introduced and the potential impact on the environment of the data center.

Because a closed-loop, re-circulating air conditioning system is used in most data centers, it will be necessary to introduce a minimal amount of air to meet the ventilation requirements of the room occupants. Data center areas normally have a very low human population density; thus the air required for ventilation will be minimal. In most cases, the air needed to achieve positive pressurization will likely exceed that needed to accommodate the room occupants. Normally, outside air quantities of less than 5% make-up air should be sufficient (ASHRAE Handbook: Applications, Chapter 17). A volume of 15 CFM outside air per occupant or workstation should sufficiently accommodate the ventilation needs of the room.

Cleaning Procedures and Equipment

Even a perfectly designed data center requires continued maintenance. Data centers containing design flaws or compromises may require extensive efforts to maintain conditions within desired limits. Hardware performance is an important factor contributing to the need for a high level of cleanliness in the data center.

Operator awareness is another consideration. Maintaining a fairly high level of cleanliness will raise the level of occupant awareness about special requirements and restrictions while in the data center. Occupants or visitors to the data center will hold the controlled environment in high regard and are more likely to act appropriately.

Any environment that is maintained to a fairly high level of cleanliness and is kept in a neat and well organized fashion will also command respect from the room's inhabitants and visitors. When potential clients visit the room they will interpret the overall appearance of the room as a reflection of an overall commitment to excellence and quality. An effective cleaning schedule must consist of specially designed short-term and long-term actions, as summarized in [Table A-2](#).

Table A-2 Effective Cleaning Schedule

Frequency	Task
Daily Actions	Rubbish removal
Weekly Actions	Access floor maintenance (vacuum and damp mop)
Quarterly Actions	Hardware decontamination
	Room surface decontamination
Biennial Actions	Subfloor void decontamination
	Air conditioner decontamination (as necessary)

Daily Tasks

This statement of work focuses on the removal of each day's discarded trash and rubbish from the room. In addition, daily floor vacuuming may be required in Print Rooms or rooms with a considerable amount of operator activity.

Weekly Tasks

This statement of work focuses on the maintenance of the access floor system. During the week, the access floor becomes soiled with dust accumulations and blemishes. The entire access floor should be vacuumed and damp mopped. All vacuums used in the data center, for any purpose, should be equipped with High Efficiency Particulate Air (HEPA) filtration. Inadequately filtered equipment cannot arrest smaller particles, but rather simply agitates them, degrading the environment they were meant to improve. It is also important that mop-heads and dust wipes are of appropriate non-shedding designs.

Cleaning solutions used within the data center must not pose a threat to the hardware. Solutions that could potentially damage hardware include products that are:

- Ammoniated
- Chlorine-based
- Phosphate-based
- Bleach enriched
- Petro-chemical based
- Floor strippers or re-conditioners.

It is also important that the recommended concentrations are used, as even an appropriate agent in an inappropriate concentration can be potentially damaging. The solution should be maintained in good condition throughout the project, and excessive applications should be avoided.

Quarterly Tasks

The quarterly statement of work involves a much more detailed and comprehensive decontamination schedule and should only be conducted by experienced computer room contamination-control professionals. These actions should be performed three to four times per year, based on the levels of activity and contamination present. All room surfaces should be completely decontaminated including cupboards, ledges, racks, shelves and support equipment. High ledges and light fixtures and generally accessible areas should be treated or vacuumed as appropriate. Vertical surfaces including windows, glass partitions, and doors should be completely treated. Special dust cloths that are impregnated with a particle absorbent material are to be used in the surface decontamination process. Do not use generic dust rags or fabric cloths to perform these activities. Do not use any chemicals, waxes or solvents during these activities.

Settled contamination should be removed from all exterior hardware surfaces including horizontal and vertical surfaces. The unit's air inlet and outlet grilles should be treated as well. Do not wipe the unit's control surfaces as these areas can be decontaminated by the use of lightly compressed air. Special care should also be taken when cleaning keyboards and life-safety controls. Use specially treated dust wipes to treat all hardware surfaces. Monitors should be treated with optical cleansers and static-free cloths. Do not use Electro-Static Discharge (ESD) dissipative chemicals on the computer hardware, since these agents are caustic and harmful to most sensitive hardware. The computer hardware is sufficiently designed to permit electrostatic dissipation thus no further treatments are required. After all of the hardware and room surfaces have been completely decontaminated, the access floor should be HEPA vacuumed and damp mopped as detailed in the Weekly Actions.

Biennial Tasks

The subfloor void should be decontaminated every 18 months to 24 months based on the conditions of the plenum surfaces and the degree of contaminant accumulation. Over the course of the year, the subfloor void undergoes a considerable amount of activity that creates new contamination accumulations. Although the weekly above floor cleaning activities will greatly reduce the subfloor dust accumulations, a certain amount of surface dirt will migrate into the subfloor void. It is important to maintain the subfloor to a high degree of cleanliness since this area acts as the hardware's supply air plenum. It is best to perform the subfloor decontamination treatment in a short time frame to reduce cross contamination. The personnel performing this operation should be fully trained to assess cable connectivity and priority. Each exposed area of the subfloor void should be individually inspected and assessed for possible cable handling and movement. All twist-in and plug-in connections should be checked and fully engaged before cable movement. All subfloor activities must be conducted with proper consideration for air distribution and floor loading. In an effort to maintain access floor integrity and proper psychrometric conditions, the number of floor tiles removed from the floor system should be carefully managed. In most cases, each work crew should have no more than 24 square feet (six tiles) of open access flooring at any one time. The access floor's supporting grid system should also be completely decontaminated, first by vacuuming the loose debris and then by damp-sponging the accumulated residue. Rubber gaskets, if present, as the metal framework that makes up the grid system should be removed from the grid work and cleaned with a damp sponge as well. Any unusual conditions, such as damaged floor suspension, floor tiles, cables and surfaces, within the floor void should be noted and reported.

Activity and Processes

Isolation of the data center is an integral factor in maintaining appropriate conditions. All unnecessary activity should be avoided in the data center, and access should be limited to necessary personnel only. Periodic activity, such as tours, should be limited, and traffic should be restricted to away from the hardware to avoid accidental contact. All personnel working in the room, including temporary employees and janitorial personnel, should be trained in the most basic sensitivities of the hardware to avoid unnecessary exposure. The controlled areas of the data center should be completely isolated from contaminant producing activities. Ideally, print rooms, check sorting rooms, command centers or other areas with high levels of mechanical or human activity should have no direct exposure to the data center. Paths to and from these areas should not necessitate traffic through the main data center areas.

Index

B

Base Configuration, 4-1, 5-10
Biennial Tasks, A-10

C

Capacity, 5-10
Cleaning Activity, A-4
CLINK Connectivity, 6-8
Configuration Planning, 4-1
Configuration Planning Overview, 4-3
Contaminant Effects, A-4
Contaminant Properties and Sources, A-2
Controlling Contaminants, A-1
Corrosive Failure, A-4
Creating Planning Teams, 2-1

D

Data at rest encryption, 8-1
Data Center Safety, 5-4
Define the ippath, 6-7
Define the Replication Ports, 6-6
Dimensions, 5-11
Dual Independent Source Power Supplies, 5-7

E

Electrical Noise, 5-7
Elevator Lifting Capacities, 5-3
Emergency Power Control, 5-4
Encryption, 8-1
Environmental Contaminants, A-1
Environmental Requirements and Hazards, 5-8
Environmental Specifications, 5-10
Ethernet Port Assignments, 6-1
Exposure Points, A-6

F

FICON Port Assignments, 7-1
FICON Upgrade, 4-2
Filtration, A-6
Fire Prevention Guidelines, 5-4
Floor Construction Requirements, 5-9
Floor Loading Requirements, 5-9

Floor Loading Specifications and References, 5-9
Floor-Load Ratings, 5-3

G

Grounding
 B-Series Equipment, 5-6

H

HVAC, 5-12
HVAC Requirements, 5-8

I

Implementation Planning, 3-1
Implementation Planning Goals, 3-1
Implementation Planning Process Overview, 3-1
Input Power Requirements, 5-6
IP Connectivity Examples, 6-6

L

Long Wave SFPs, 4-2

M

MVS Host Software Requirements, 3-3

N

Network Infrastructure Requirements, 3-2

O

Operator Activity, A-3
Outside Air, A-3
Outside Influences, A-3

P

Physical Site Readiness Planning, 5-1
Planning Activities, 2-2
Planning and Implementation Overview, 2-1
Planning Goals, 2-1
Planning Spreadsheet, 2-3
Planning Teams, 2-1

Power, 5-12
Power Distribution Systems, 5-5
Product Introduction, 1-1
Product Overview, 1-1

R

Raised-Floor Lateral Stability Ratings, 5-9
Raised-Floor Panel Ratings, 5-10
Raised-Floor Pedestal Ratings, 5-10
Ramp Inclines, 5-3
Replication Ports, Define, 6-6
Room Conditions, A-5
RTD Connectivity Examples, 7-2

S

Service Clearance, 5-11
Serviceability Requirements, 3-3
SFPs, 4-2
Short Wave SFPs, 4-2
Shorts, A-4
Site Power Distribution Systems, 5-5
Site Readiness Planning, 5-1
Site Readiness Planning Process, 5-1
Static Electricity, 5-8
Storage Capacity Upgrade, 4-1
Stored Items, A-3
Structural Dimensions and Obstructions, 5-3

T

The VSM Solution, 1-2
Thermal Failure, A-5
Transferring Equipment Point-to-Point, 5-3

V

VLE Connectivity, 6-7
VSM 6 Base Configuration, 4-1
VSM 6 Base Unit, 4-1, 5-10
VSM 6 Platform, 1-2
VSM 6 Product Overview, 1-1
VSM Solution, 1-2

W

Weight, 5-11

Z

ZIL SSD Upgrade, 4-2