StorageTek Virtual Storage Manager System

VSM 7 Planning Guide

Release 7

E71318-06

April 2019

ORACLE

StorageTek Virtual Storage Manager System VSM 7 Planning Guide, Release 7

E71318-06

Contents

7 VSM 7 FC/FICON Data Path Connectivity

8 Data at Rest Encryption Feature

9 Enhanced Replication (RLINKS) Feature

10 VSM Extended Storage Feature

A Controlling Contaminants

Index

List of Figures

List of Tables

Preface

This publication is intended for Oracle or customer personnel responsible for doing site planning for Oracle's StorageTek Virtual Storage Manager System 7.

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 7 Documents

- *Safety and Compliance Guide*
- *Security Guide*
- *Licensing Information User Manual*

1 Introduction

Oracle's StorageTek Virtual Storage Manager System 7 (VSM 7) 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.

See "The VSM 7 Platform" on page 1-2.

Additionally, VSM includes the VSM Extended Storage (ExS) feature that allows the VTSS to access and utilize storage external to the VTSS, including access to the Oracle Cloud.

See "VSM Extended Storage Feature" on page 10-1.

Figure 1–1 VSM 7 VTSS

The VSM 7 Platform

The VSM 7 VTSS is packaged as a standard rack mount system built on existing Oracle server, storage, and service platforms. The servers, storage disk enclosures, and standard rack mount enclosure are delivered as a packaged system.

The Solaris 11 operating system is the foundation of the VSM 7 VTSS software environment, which also includes Solaris infrastructure components and VTSS function-specific software. The VSM 7 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 7 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 7 VTSS Functionality

The VSM 7 VTSS is a follow-on to the existing VSM 6 VTSS system, replacing the VSM 6 hardware stack with new Oracle servers, storage disk enclosures, and I/O cards. This new hardware stack provides increased performance and capacity to the VTSS.

For example, storage capacity is doubled from VSM 6, replication performance is improved with the move to all 10 Gb IP networks, and higher processor clock rates, faster internal memory, and faster I/O bus speeds provide noticeable improvements in system performance.

As a replacement for the VSM 6 VTSS, the customer view and functionality of the VSM 7 VTSS are generally equivalent, except where performance, connectivity, and serviceability have been improved.

The predominate VSM 7 VTSS platform differences from the VSM 6 VTSS are as follows:

- Increased performance and storage capacity with upgraded servers and storage disk enclosures
- 16 Gbps FC/FICON connectivity with eight ports
- 10 Gbps IP connectivity throughout the VTSS and into the customer's network environment
- Two network switches that aggregate or fan out network connections from the servers to the customer's network environment

The VSM Solution

Oracle's StorageTek Virtual Storage Manager (VSM) System 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. VTVs can be up to 32GB. When needed by the host, if the migrated VTVs are not VTSS-resident, they are then automatically recalled to the VTSS.

The VSM System includes the following subsystems:

- VTSS hardware and software.

  The VSM 7 VTSS supports emulated tape connectivity to IBM MVS hosts over FICON interfaces, Fibre Channel or FICON attachment to Real Tape Drives (RTDs), IP attachment to other (VSM 7, VSM 6, or VSM5) VTSSs and VLEs, and remote host connectivity using ECAM over IP and VTSS-to-VTSS replication.

- 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.

- 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 in the IBM MVS environment. ELS includes the Host Software Component (HSC), Storage Management Component (SMC), and HTTP Server.

- Virtual Library Extension (VLE) hardware and software.

  VLEs are IP-attached to the VSM 7 VTSS and function as a migrate and recall target for VTSS Virtual Tape Volumes (VTVs).

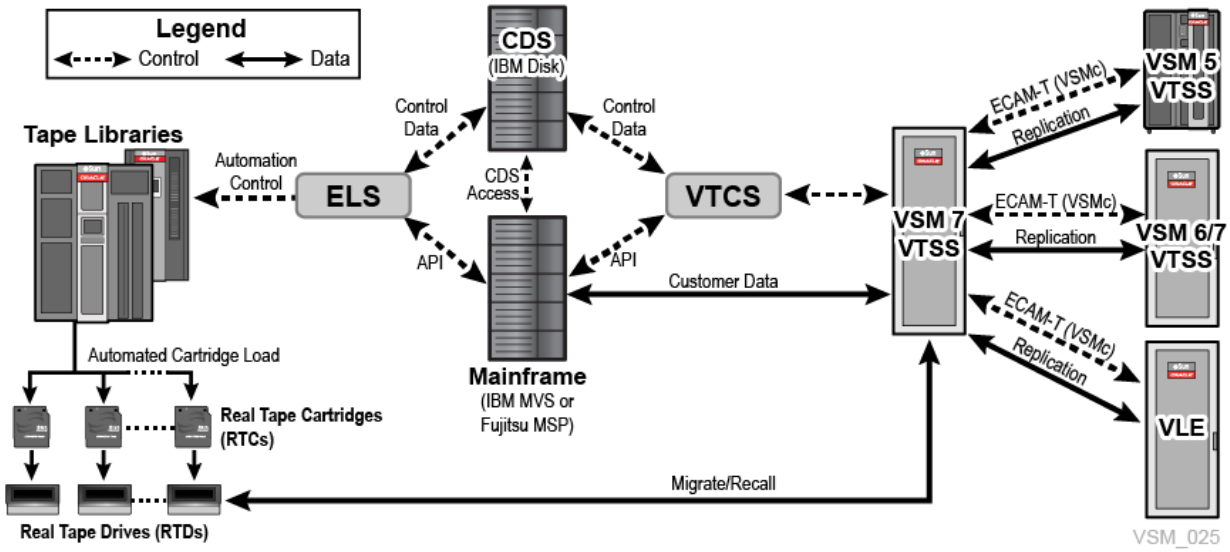
  Note: VLE supports migrate and recall to and from Oracle Cloud Storage. A VSM 7 that is connected to a properly configured VLE can use the VLE to migrate and recall VTVs to and from Oracle Cloud Storage instead of local disk. Refer to VLE publications for more information about this feature.

- Real Tape Drives (RTDs) connected to physical tape libraries.

  RTDs serve as migrate and recall targets for VTSS Virtual Tape Volumes (VTVs). RTDs are FC-attached (for OSA) or FICON-attached to the VSM 7 VTSS.

VSM subsystems are shown in Figure 1–2.

Figure 1–2 VSM 7 Context Diagram



2

VSM 7 Planning and Implementation Overview

This chapter describes the key participants and activities involved in planning for and implementing a VSM 7 system.

Planning Goals

The primary goals of the planning process are to:

- Ensure the VSM 7 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 7 system equipment, and that customer personnel are trained to assist with delivery, installation, configuration, testing, certification, and operation of the VSM 7 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 7 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 7 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 7 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 7 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 7 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 7 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 7 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 7 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 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 7 configuration. The spreadsheet also contains a sample configuration to use for reference during the planning process.

3

VSM 7 Implementation Planning

This chapter provides an overview of implementation planning activities and tasks, which are designed to ensure a VSM 7 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 7 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 7 system.
- Define a plan to migrate data from other devices and systems to the VSM 7 system.
- Define a plan to accommodate the physical layout and floor space requirements of the VSM 7 VTSS and other system devices.
- Define a plan for configuring the VSM 7 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 7 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 7 system.
2. Define plan for migrating data from other devices and systems to the VSM 7.
3. Determine default settings for the VSM 7 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 7 system software (ExLM, HSC, MVS, NCS, VTCS).
6. Define policies for configuring and managing VSM 7 system virtual entities.
7. Define plan for performance tuning, testing, and certification of the VSM 7 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 7 arrives to minimize the installation time. Ensure that the network is ready for connection to the VSM 7 as follows:

- Gigabit Ethernet protocol is required on all network switches and routers that are directly attached to the VSM 7 servers. The servers will only do speed negotiation to the 10GbE speed.
- Check that you are using the proper (customer-supplied) 10 GigE Ethernet cables. For best results, Oracle strongly recommends using CAT6A cables for any copper connections that exit the VSM 7 cabinet to the customer infrastructure.
- Two TCP/IP connections are required between a VSM 7 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 7 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 7 node that are configured on the customer network must be on separate networks.
- VSM 7 reserves and uses the following TCP ports for the identified functions:

443 – ASR (labeled CAM/ASR)

50000 - IFF/IP replication control port (labeled REP1 and REP2 on each node)

51000-55000 – IFF/IP Replication data port (labeled REP1 and REP2 on each node)

61000 - ECAM-over-IP (labeled NET0)

61300 - CLI server (labeled NET0)

63000-63999 – Enhanced Replication data port (labeled REP1 and REP2 on each node)

Satisfying MVS Host Software Requirements

Refer to the VSM 7 Release Notes for information about additional VTCS software updates that may be required for VSM 7 support.

Satisfying Serviceability Requirements

The VSM 7 product uses a standard Oracle service strategy common with other Oracle products. VSM 7 uses Automated Service Response (ASR) as the outgoing event notification interface to notify Oracle VSM Support that an event has occurred on the VSM 7 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 7 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 7 will be configured to allow outgoing ASR and email communication with Oracle VSM Support. To support VSM 7 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 7 installation. During this part of the install the VSM 7 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 7. Until this approval is completed by the customer, the VSM 7 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 7 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 7 to Oracle VSM Support. In this case, the customer must supply the email address where VSM 7 emails are sent.

4

VSM 7 Hardware Configuration Planning

This chapter provides an overview of configuration planning considerations.

VSM 7 Configuration Options

VSM 7 consists of a base unit and optional capacity upgrades.

VSM 7 Base Configuration

VSM 7 consists of a base unit and optional capacity upgrades. The base unit is a VSM 7 in its minimum configuration, including:

- A standard Sun Rack II cabinet, Model 1242
- Full height Sun Rack 10 KV AMP (North America or International)
- Two Oracle SPARC T7-2 servers in a specific configuration and factory preconfigured for VSM 7, including 10GbE Ethernet NICs, FC/FICON HBAs, SAS3 HBAs and TDX cards
- Two Oracle Storage Drive Enclosure DE3-24C storage disk enclosures, each with five 200GB Flash SSDs and 19 8TB SAS HDD drives, representing 150TB native capacity
- Two Oracle Switch ES1-24 10GbE Ethernet switches in a highly available top-of-rack redundant configuration for network management
- SFPs, either SR or LR, installed into T7-2 FC HBAs
- Depending on country, two VLE50HZ-POWER-Z or two VLE60HZ-POWER-Z power Power Distribution Units (PDUs)

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. They add capacity to the base unit, which has two storage disk enclosures (150TB native capacity).

A storage capacity upgrade kit is packaged as two storage disk enclosures. Up to three upgrade kits can be installed in a VSM 7 base unit, for a total of four (375TB), six (600TB), or eight (825TB) storage disk enclosures in the unit.

Capacity Upgrade for VSM 7 with Oracle DE3-24C Storage Disk Enclosures

For a VSM 7 with Oracle DE3-24C storage disk enclosures, a capacity upgrade kit has two Oracle DE3-24C storage disk enclosures, each containing 24 8TB SAS HDD drives and no Flash SSDs.

The native capacity for each possible VSM 7 configuration with Oracle DE3-24C storage disk enclosures is as follows:

- VSM 7 base unit (two storage disk enclosures total): 150TB
- VSM 7 base unit plus one capacity upgrade kit (four storage disk enclosures total): 375TB
- VSM 7 base unit plus two capacity upgrade kits (six storage disk enclosures total): 600TB
- VSM 7 base unit plus three capacity upgrade kits (eight storage disk enclosures total): 825TB

FC/FICON Upgrade

Customers may order either Long Wave or Short Wave SFPs for the FICON ports when their VSM 7 is built. This can be modified in the field with a field upgrade kit containing eight Long Wave or Short Wave SFPs:

- The VSM 7 Long Wave FC/FICON field upgrade option has eight single LW SFPs.
- The VSM 7 Short Wave FC/FICON field upgrade option has eight single SW SFPs.

Configuration Planning Overview

Designing an optimized VSM 7 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.

Key High-Level Activities

1. Define customer requirements.
2. Assess budgetary constraints.
3. Design an optimized VSM 7 system based on defined requirements and constraints.

Key Sub-Tasks

1. Refer to the VSM 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 7 system configuration.
4. Create a detailed engineering diagram of the proposed VSM 7 system configuration.

5. Present the VSM 7 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

5

VSM 7 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 7 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 7 system equipment
- A plan for the layout and location of VSM 7 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 7 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 7 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 7 system requirements.
   - Confirm floor load ratings along the transit path and at the installation location for VSM 7 VTSS cabinets.
   - Assess ceiling, hallway, and door clearances, elevator capacities, and ramp angles versus VSM 7 VTSS cabinet requirements.
3. Attend planning meetings.

Key Sub-Tasks

1. Verify site power, safety, environmental, HVAC, and data handling capabilities match VSM 7 VTSS requirements.
2. Define plan to eliminate/mitigate environmental hazards.
3. Evaluate floor load ratings along transit path and at the VSM 7 VTSS installation location.
4. Verify site door, hall and ceiling clearances, elevator capacity, and ramp angles match VSM 7 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 7 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 7 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 7 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 7 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 7 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 7 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 7 cabinets (in shipping containers, where appropriate) from the delivery dock to the data center installation location. See VSM 7 Overall Dimensions for VSM 7 cabinet-dimension details.

Elevator Lifting Capacities

Any elevators that will be used to transfer VSM 7 cabinets must have a certified load rating of at least 1102 kg (2430 lb). This provides adequate capacity to lift the heaviest fully-populated VSM 7 cabinet (roughly 803 kg (1700 lb) and a pallet jack (allow 100 kg/220 lb) and two persons (allow 200 kg/440 lb). See VSM 7 Weight for additional cabinet-weight details.

Floor-Load Ratings

Solid floors, raised floors, and ramps located along the transfer path for VSM 7 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 803 kg (1700 lb) and a rolling load of 181 kg (400 lb) 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 lb). See Floor Loading Requirements for additional floor-loading details.

When being moved from one location to another, a VSM 7 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 7 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 7 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 may 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 7 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 7 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

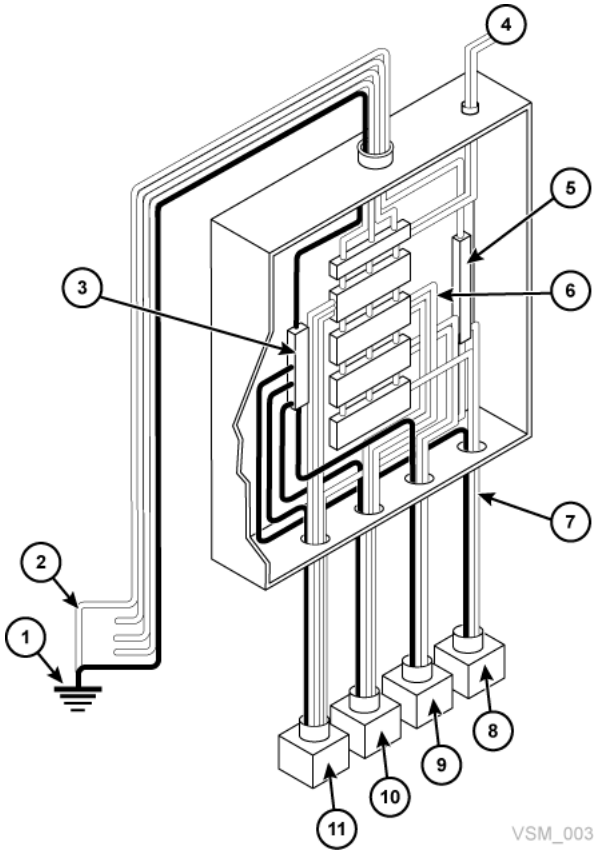
8 - 120V Single Phase

9 - 208/240V Single Phase

10 - 208/240V 3-Phase (4 wire)

11 - 208/240V 3-Phase (5 wire)

Figure 5–1 Site Electrical Power Distribution System



Equipment Grounding

For safety and ESD protection, VSM 7 system equipment must be properly grounded. VSM 7 cabinet power cables contain an insulated green/yellow grounding wire that connects the VSM 7 frame to the ground terminal at the AC source power outlet. A similar insulated green or green/yellow wire ground, of at least the same diameter as the phase wire, is required between the branch circuit panel and the power receptacle that attaches to each cabinet.

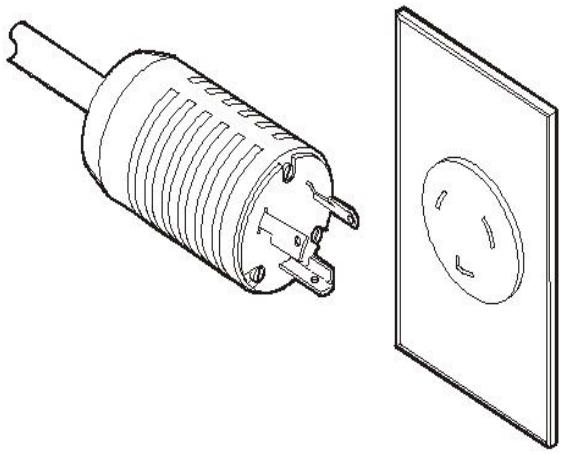
Source Power Input

Voltage and frequency ranges at the AC source power receptacle(s) that will supply power to VSM 7 system equipment must be measured and verified to meet the following specifications:

- Source Power: AC, single-phase, 3-wire
- Voltage Range: 170-240
- Frequency Range (Hz): 47-63

If you are installing the VSM 7 cabinet in the North and South America, Japan and Taiwan, ensure that the designated power sources are NEMA L6-30R receptacles, and ensure that the cabinet power cords are terminated with the required NEMA L6-30P plugs. The factory ships power cords with NEMA L6-30P plugs to North and South America, Japan and Taiwan. Shipments to EMEA and APAC will ship with IEC309 32A 3 PIN 250VAC IP44 plugs. Figure 5–2 shows a NEMA L6-30P plug and L6-30R receptacle.

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



If you are installing the VSM 7 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 7 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 7 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 7 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:

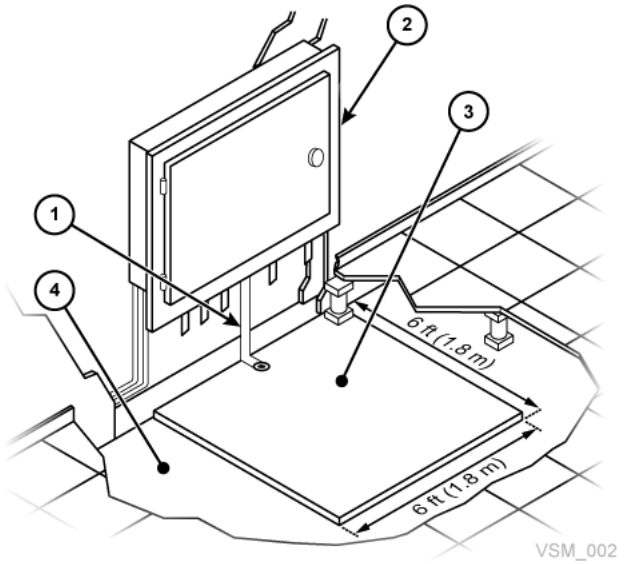
1 - Flat Braided/Strained Wire

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 7 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 7 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 7 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 lb/ft2) 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 7 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 7 system equipment.

Caution: When being moved, a VSM 7 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 7, 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 lb.ft2).

  This is the load over footprint surface area (7093.7 cm2/1099.5 in2) of an unpackaged VSM 7 cabinet, with a maximum weight of 803 kg/1700 lb (if fully loaded with 192 array disk drives).

- The maximum superimposed floor load is 485 kg/m2 (99 lb./ft2).

  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 7 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 lb horizontal force
- Seismic Risk Zone 2A: 20.2 kg / 44.6 lb horizontal force
- Seismic Risk Zone 2B: 26.9 kg / 59.4 lb horizontal force
- Seismic Risk Zone 3: 40.4 kg / 89.1 lb horizontal force

- Seismic Risk Zone 4: 53.9 kg / 118.8 lb 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 7 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 803 kg (1700 lb) and a rolling load of 181 kg (400 lb) anywhere on the panel with a maximum deflection of 2 mm (0.08 in). Perforated floor panels are not required for VSM 7 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 lb). Where floor panels are cut to provide service access, additional pedestals may be required to maintain the loading capacity of the floor panel.

VSM 7 Environmental Specifications

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

VSM 7 Base Configuration

VSM 7 consists of a base unit and optional capacity upgrades. The base unit is a VSM 7 in its minimum configuration, including:

- A standard Sun Rack II cabinet, Model 1242
- Full height Sun Rack 10 KV AMP (North America or International)
- Two Oracle SPARC T7-2 servers in a specific configuration and factory preconfigured for VSM 7, including 10GbE Ethernet NICs, FICON HBAs, SAS3 HBAs and TDX cards
- Two Oracle Storage Drive Enclosure DE3-24C storage disk enclosures, each with five 200GB Flash SSDs and 19 8TB SAS HDD drives, representing 150TB native capacity
- Two Oracle Switch ES1-24 10GbE Ethernet switches in a highly available top-of-rack redundant configuration for network management
- SFPs, either SR or LR, installed into T7-2 FC HBAs
- Depending on country, two VLE50HZ-POWER-Z or two VLE60HZ-POWER-Z power Power Distribution Units (PDUs)

VSM 7 Native Capacity

The native capacity for each possible VSM 7 configuration with Oracle DE3-24C storage disk enclosures is as follows:

- VSM 7 base unit (two disk storage enclosures total): 150TB

- VSM 7 base unit plus one capacity upgrade kit (four storage disk enclosures total): 375TB
- VSM 7 base unit plus two capacity upgrade kits (six storage disk enclosure total): 600TB
- VSM 7 base unit plus three capacity upgrade kits (eight storage disk enclosures total): 825TB

VSM 7 Overall Dimensions

SunRack II 1242 Cabinet (inches):

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

VSM 7 Service Clearance

SunRack II 1242 Cabinet (inches):

- Top: 36 inches. This is the generic Sun Rack II specification. VSM 7 does not require access through the top except for cabling.
- Front: 42
- Rear: 36

VSM 7 Weight

VSM 7 weight varies by configuration, the difference being the number of storage disk enclosures in a configuration. All weights are approximate.

Base unit (two storage disk enclosures total):

- Net weight: 827 lb/376 kg
- Shipping material: 280 lb/127 kg
- Gross weight crated: 1107 lb/503 kg

Base unit plus one capacity kit (four storage disk enclosures total):

- Net weight: 1047 lb/476 kg
- Shipping material: 280 lb/127 kg
- Gross weight crated: 1327 lb/603 kg

Base unit plus two capacity kits (six storage disk enclosures total):

- Net weight: 1267 lb/576 kg
- Shipping material: 280 lb/127 kg
- Gross weight crated: 1547 lb/703 kg

Base unit plus three capacity kits (eight storage disk enclosures total):

- Net weight: 1490 lb/676 kg
- Shipping material: 280 lb/127 kg
- Gross weight crated: 1770 lb/803 kg

VSM 7 Power

Typical power consumption in Watts (W):

- Base unit (two servers and two disk storage disk enclosures): 5404 W
- Base unit and one expansion kit (two servers and four disk storage disk enclosures): 6008 W
- Base unit and two expansion kits (two servers and six storage disk enclosures): 6584 W
- Base unit and three expansion kits (two servers and eight storage disk enclosures): 7160 W

Maximum power consumption in Watts (W):

- Base unit (two servers and two storage disk enclosures): 5727 W
- Base unit and one expansion kit (two servers and four storage disk enclosures): 6632 W
- Base unit and two expansion kits (two servers and six storage disk enclosures): 7537 W
- Base unit and three expansion kits (two servers and eight storage disk enclosures): 8442 W

VSM 7 HVAC

Typical thermal dissipation (BTU/hr):

- Base unit (two servers and two storage disk enclosures): 18440 BTU
- Base unit and one expansion kit (two servers and four storage disk enclosures): 20501 BTU
- Base unit and two expansion kits (two servers and six storage disk enclosures): 22466 BTU
- Base unit and three expansion kits (two servers and eight storage disk enclosures): 24432 BTU

Maximum thermal dissipation (BTU/hr):

- Base unit (two servers and two storage disk enclosures): 19542 BTU
- Base unit and one expansion kit (two servers and four storage disk enclosures): 22630 BTU
- Base unit and two expansion kits (two servers and six storage disk enclosures): 25718 BTU
- Base unit and three expansion kits (two servers and eight storage disk enclosures): 28806 BTU

6

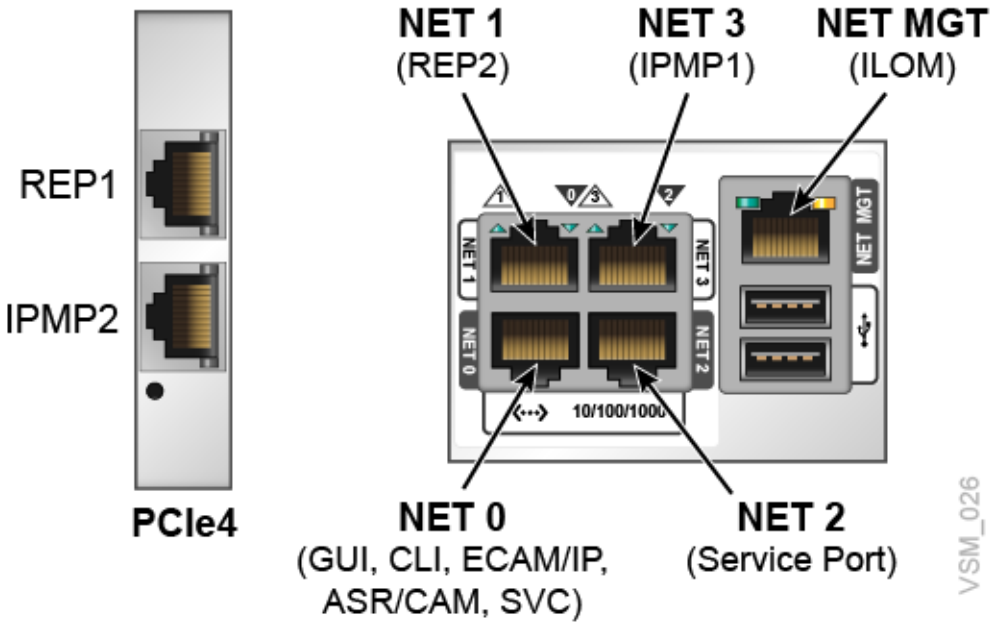
VSM 7 Ethernet (IP) Data Path Connectivity

Unlike VSM 6, customer networks are not connected directly to the VSM 7 server nodes. Instead, the customer network uplinks connect to the two ES1-24 switches, which in turn connect to the Ethernet ports on the two VSM 7 server nodes.

VSM 7 Ethernet (IP) Port Assignments

Figure 6–1 shows the IP Ethernet ports on each VSM 7 node.

Figure 6–1 VSM 7 Ethernet Ports



The network ports (NET0, NET1, NET2) are connected to various networks through the two ES1-24 switches:

- Port 0 (NET0) is for user interface connections (CLI, GUI, ECAM over IP).
- Port 1 (NET1) connects to the Oracle Switch ES1-24 10GbE Ethernet switches
- Port 2 (NET2) is a dedicated maintenance port reserved for direct connection by Services. Port 1 on each switch is dedicated to field maintenance for Port 2 (NET2); Switch 1 goes to Node 1 and Switch 2 goes to Node 2.

Port 3 (NET3) is not connected to the network switches. It is connected directly to NET3 on the other server node.

The Twinville HBA ports PCIe4 are connected to their respective networks through the ES1-24 switches:

- Port 4 is used for replication over IP (RoIP).
- Port 5 is used for IPMP connections

Network Switch Port Assignments

The two Oracle ES1-24 network switches are mounted at the top of the rack to aggregate or fan out network connections from the servers to the customer's network environment.

Specifically, the switches provide:

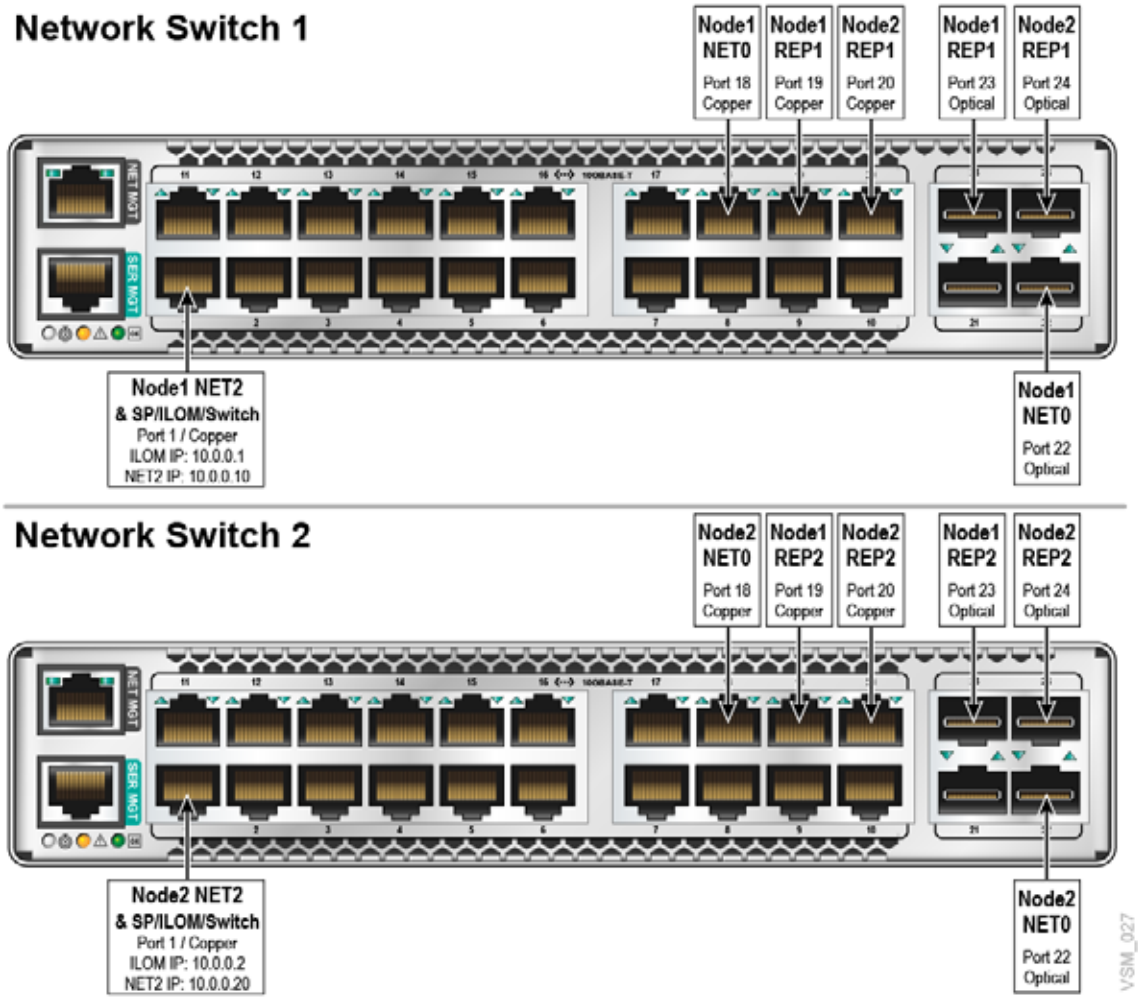
- Redundant connections for all network connections except the ILOM ports.
- Aggregation and fan-out of the four RoIP connections from the two VTSS servers to four copper or four optical RoIP connections that may be connected to the customer's network environment.
- Aggregation of the ILOM and Service port connections from the servers to a pair of single, redundant ports, one on each switch.
- Aggregation of the ECAM, VSM GUI, ASR/CAM networks from the two servers to a pair of single, redundant ports, one on each switch.

Figure 6–2 shows the port assignments from the servers to the two ES1-24 Ethernet switches.

A port connection must use all copper or all optical but not both on a single switch (for example, NET0, REP1, REP2).

Customer networks must be connected to the ES1-24 switches and may not be connected directly to the VSM 7 server ports.

Figure 6–2 ES1-24 Switch 1 and 2



Customer Network Integration

The ES1-24 switches in the VSM 7 rack represent a major change from VSM 6, where customer network connections were plugged directly into the servers. Now, with VSM 7, the customer network is instead plugged into the switches, and the switches in turn are plugged into the servers.

To access NET0 interfaces, the customer connects to either port 18 (if copper/RJ45) or port 22 (if optical) on both Switch-1 (Node 1 interfaces) and Switch-2 (Node 2 interfaces).

- For Net0 traffic on Node 1, an uplink is connected from the customer infrastructure to port 18 (if copper/RJ45) or port 22 (if optic) to switch 1
- For Net0 traffic on Node 2, an uplink is connected from the customer infrastructure to port 18 (if copper/RJ45) or port 22 (if optic) to switch 2

Replication traffic warrants two 10Gb uplinks for REP*x* traffic (20Gb total). REP1 traffic goes through Switch 1 and REP2 traffic goes through Switch 2. To provide adequate bandwidth to nodes, uplinks on switches for REP*x* traffic are assumed to

be on the same subnet and configured in port-channel from the customer infrastructure.

- For REP1 traffic to both Node 1 and Node 2, uplinks are connected from the customer infrastructure to ports 19 and 20 (if copper/RJ45) or ports 23 and 24 (if optic) to switch 1.
- For REP2 traffic to both Node 1 and Node 2, uplinks are connected from the customer infrastructure to ports 19 and 20 (if copper/RJ45) or ports 23 and 24 (if optic) to switch 2.

7

VSM 7 FC/FICON Data Path Connectivity

FC and FICON ports connect the two VSM 7 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 FC/FICON ports per VSM 7 node, a total of eight for the VTSS. For FICON, 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.

For FC, two FC ports on each node are dedicated for host connections and two ports are dedicated for RTD connections.

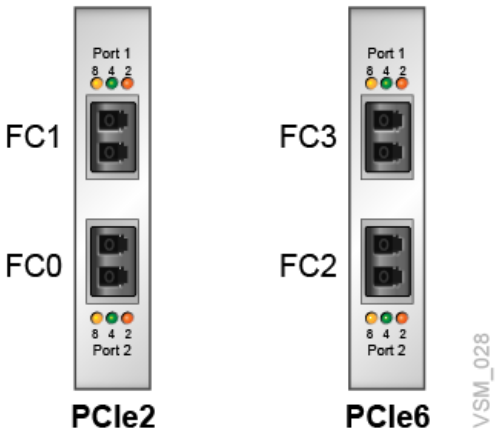
How it Works

- The link between the VSM 7 and VTCS is the RTD NAME.
- The link between VTCS and the RTD is the FC/FICON cable to the relevant DEVNO in the relevant drive bay.
- VSM 7 CLI commands define the connections to the VSM 7.
- VTCS commands define the connections to the VTCS configuration.
- VTCS uses the RTD name defined on the FCPPATH or FICONPATH command used in the VSM 7 CLI.
- Multiple FCPPATHs/FICONPATHs can route to the SAME RTD.
- Physical RTDs are defined to VTCS as FC or 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 7 defined in VTCS.
- VTCS allows 32 unique CHANIF ids. Each VSM 7 can have a maximum of 32 physical RTDs defined.

VSM 7 FC/FICON Port Assignments

As shown in Figure 7–1, the FC/FICON ports are numbered 0 to 3. When looking at the back of the server node, the left (PCIe2) top port is 1, the left (PCIe2) bottom port is 0, the right (PCIe6) top port is 3, and the right (PCIe6) bottom port is 2.

Figure 7–1 FC/FICON Ports



VSM 7 RTD Connectivity Examples

The following examples illustrate FC/FICON connectivity between VSM 7 and RTDs:

- VSM 7 RTD Connectivity: Direct Connection
- VSM 7 RTD Connectivity: Single Switch
- VSM 7 RTD Connectivity: Cascaded Switch
- VSM 7 RTD Connectivity: Dual RTDs
- VSM 7 RTD Connectivity: Four RTDs One Port
- VSM 7 RTD Connectivity: Dual-Path RTD
- VSM 7 RTD Connectivity: Dual-Path Dual RTD
- VSM 7 RTD Connectivity: Multi-Path Dual RTD

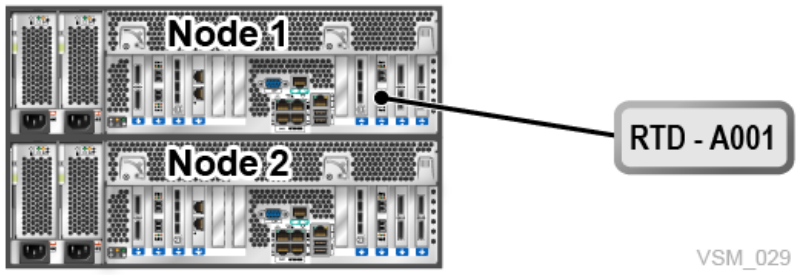
Each example includes:

- Connections between devices
- CLI commands that define the connections to the VSM 7
- VTCS commands that define the VSM 7 connections to the VTCS configuration

VSM 7 RTD Connectivity: Direct Connection

Figure 7–2 shows a direct connection between a VSM 7 FC or FICON port and an RTD.

Figure 7–2 VSM 7 RTD Connectivity – Direct Connection



VSM 7 CLI Example for FICON:

```
vsmadmin: add ficonpath -name RTDA001 -node 1 -port 2
```

VSM 7 CLI Example for FC:

```
vsmadmin: add fcppath -name RTDA001 -node 1 -port 2 -wwpn 500104F509793640
```

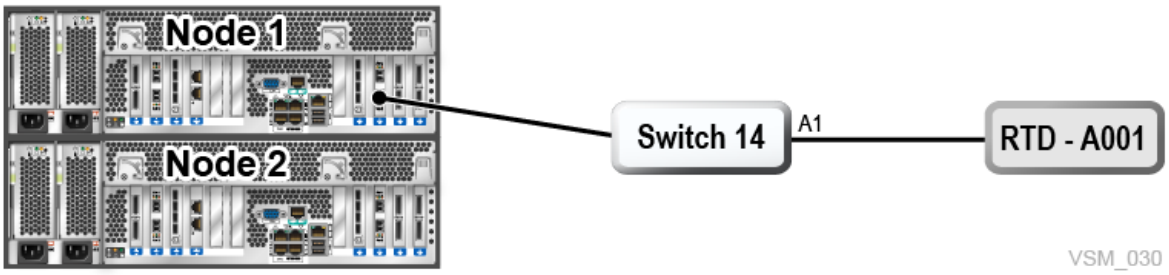
VTCS Example:

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

VSM 7 RTD Connectivity: Single Switch

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

Figure 7–3 VSM 7 RTD Connectivity – Single Switch



VSM 7 CLI Example for FICON:

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

VSM 7 CLI Example for FC:

```
vsmadmin: add fcppath -name RTDA001 -node 1 -port 2 -wwpn 500104F509793640
```

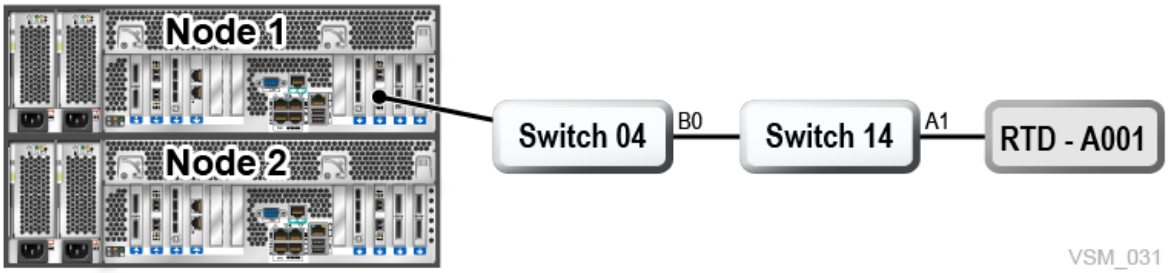
VTCS Example:

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

VSM 7 RTD Connectivity: Cascaded Switch

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

Figure 7–4 VSM 7 RTD Connectivity – Cascaded Switch



VSM 7 CLI Example for FICON:

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

VSM 7 CLI Example for FC:

```
vsmadmin: add fcppath -name RTDA001 -node 1 -port 2 -wwpn 500104F509793640
```

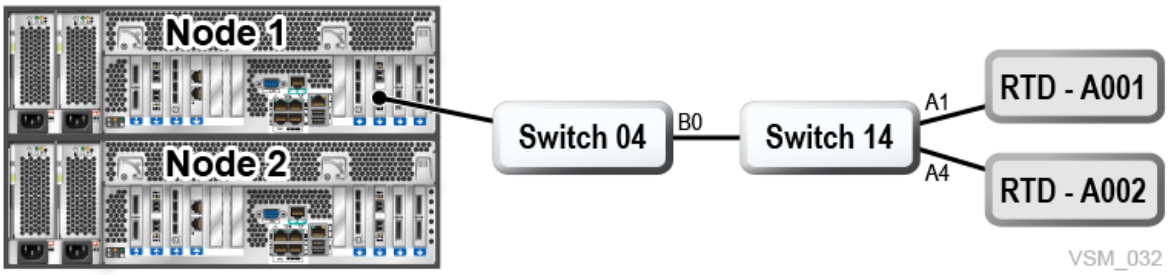
VTCS Example:

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

VSM 7 RTD Connectivity: Dual RTDs

Figure 7–5 shows a connection through cascaded switches between a VSM 7 FC or FICON port and two RTDs.

Figure 7–5 VSM 7 RTD Connectivity – Dual RTDs



VSM 7 CLI Example for FICON:

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

VSM 7 CLI Example for FC:

```
vsmadmin: add fcppath -name RTDA001 -node 1 -port 2 -wwpn 500104F509793640
vsmadmin: add fcppath -name RTDA002 -node 1 -port 2 -wwpn 500104F509793641
```

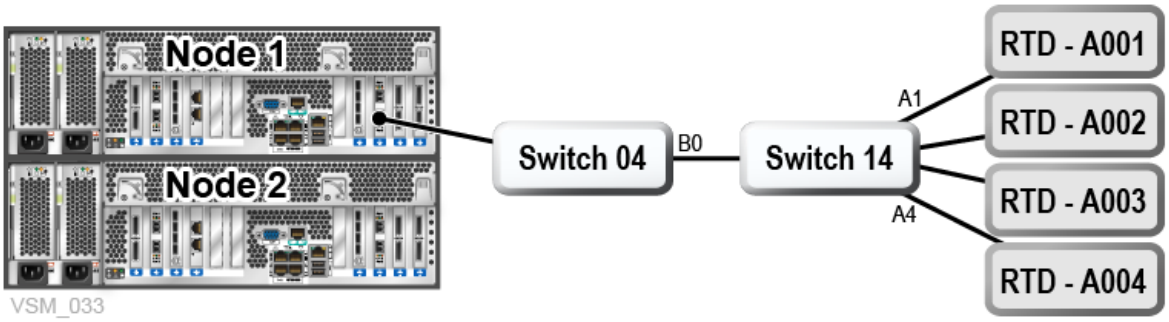
VTCS Example:

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

VSM 7 RTD Connectivity: Four RTDs One Port

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

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



VSM 7 CLI Example for FICON:

```
vsmadmin: add ficonpath -name RTDA001 -node 1 -port 2 -domain 14 -area A1
vsmadmin: add ficonpath -name RTDA002 -node 1 -port 2 -domain 14 -area A2
vsmadmin: add ficonpath -name RTDA003 -node 1 -port 2 -domain 14 -area A3
vsmadmin: add ficonpath -name RTDA004 -node 1 -port 2 -domain 14 -area A4
```

VSM 7 CLI Example for FC:

```
vsmadmin: add fcppath -name RTDA001 -node 1 -port 2 -wwpn 500104F509793640
vsmadmin: add fcppath -name RTDA002 -node 1 -port 2 -wwpn 500104F509793641
vsmadmin: add fcppath -name RTDA003 -node 1 -port 2 -wwpn 500104F509793642
vsmadmin: add fcppath -name RTDA004 -node 1 -port 2 -wwpn 500104F509793643
```

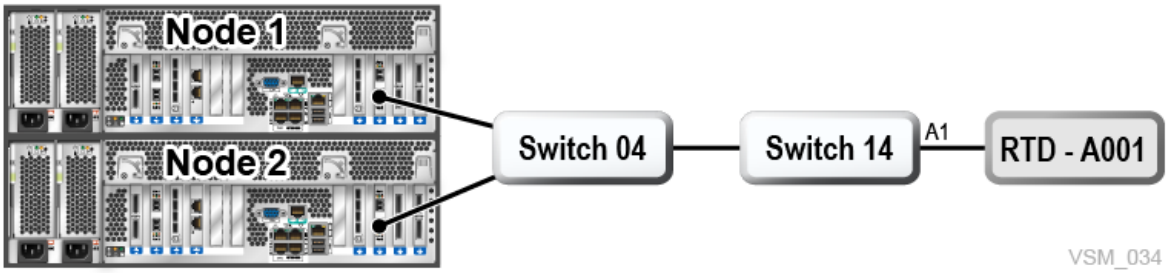
VTCS Example:

```
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=0O:0
```

VSM 7 RTD Connectivity: Dual-Path RTD

Figure 7–7 and Figure 7–8 show two FC or FICON paths to the same RTD. The connections are between two VSM 7 FC or FICON ports located on separate VSM 7 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 7 RTD Connectivity – Dual-Path RTD Example 1



VSM 7 CLI Example 1 for FICON:

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

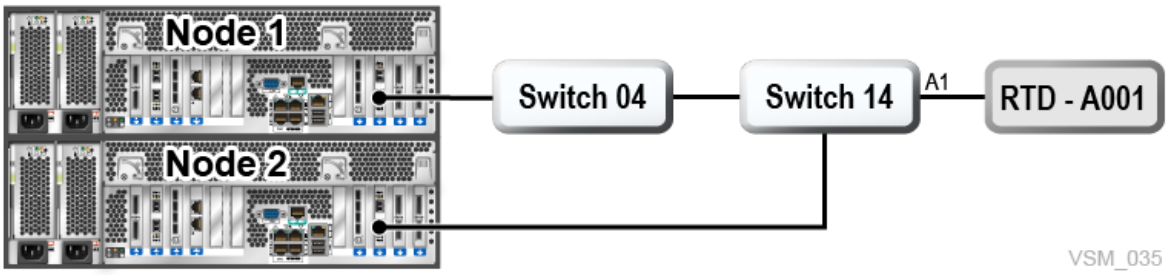
VSM 7 CLI Example 1 for FC:

```
vsmadmin: add fcppath -name RTDA001 -node 1 -port 2 -wwpn 500104F509793640
vsmadmin: add fcppath -name RTDA001 -node 2 -port 2 -wwpn 500104F509793640
```

VTCS Example 1:

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

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



VSM 7 CLI Example 2 for FICON:

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

VSM 7 CLI Example 2 for FC:

```
vsmadmin: add fcppath -name RTDA001 -node 1 -port 2 -wwpn 500104F509793640
vsmadmin: add fcppath -name RTDA001 -node 2 -port 2 -wwpn 500104F509793640
```

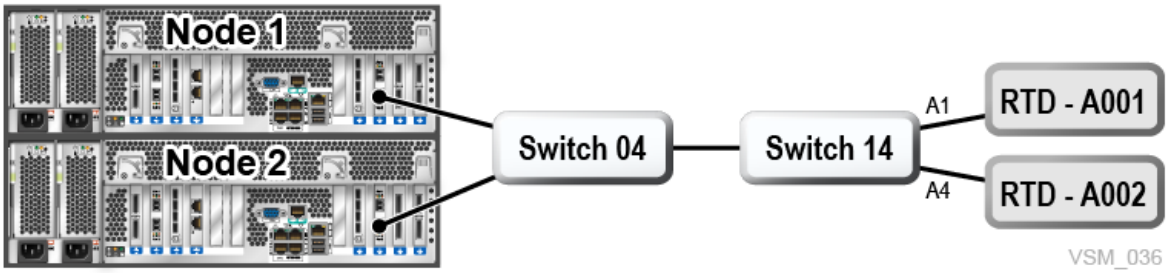
VTCS Example 2:

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

VSM 7 RTD Connectivity: Dual-Path Dual RTD

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

Figure 7–9 VSM 7 RTD Connectivity – Dual-Path Dual RTD



VSM 7 CLI Example for FICON:

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

VSM 7 CLI Example for FC:

```
vsmadmin: add fcppath -name RTDA001 -node 1 -port 2 -wwpn 500104F509793640
vsmadmin: add fcppath -name RTDA001 -node 2 -port 2 -wwpn 500104F509793640
vsmadmin: add fcppath -name RTDA002 -node 1 -port 2 -wwpn 500104F509793641
vsmadmin: add fcppath -name RTDA002 -node 2 -port 2 -wwpn 500104F509793641
```

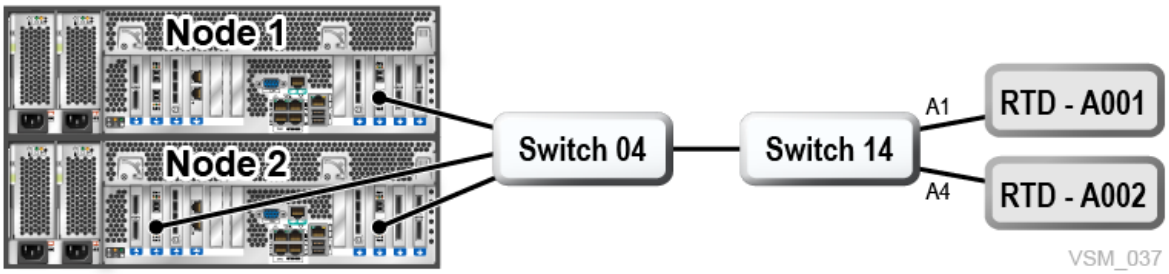
VTCS Example:

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

VSM 7 RTD Connectivity: Multi-Path Dual RTD

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

Figure 7–10 VSM 7 RTD Connectivity – Multi-Path Dual RTD



VSM 7 CLI Example for FICON:

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

```
vsmadmin: add ficonpath -name RTDA002 -node 2 -port 2 -domain 14 -area A4
```

VSM 7 CLI Example for FC:

```
vsmadmin: add fcppath -name RTDA001 -node 1 -port 2 -wwpn 500104F509793640
vsmadmin: add fcppath -name RTDA001 -node 2 -port 1 -wwpn 500104F509793640
vsmadmin: add fcppath -name RTDA001 -node 2 -port 2 -wwpn 500104F509793640
vsmadmin: add fcppath -name RTDA002 -node 1 -port 2 -wwpn 500104F509793641
vsmadmin: add fcppath -name RTDA002 -node 2 -port 1 -wwpn 500104F509793641
vsmadmin: add fcppath -name RTDA002 -node 2 -port 2 -wwpn 500104F509793641
```

VTCS Example:

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

8

Data at Rest Encryption Feature

VSM 7 supports a feature for encrypting data at rest on the storage disk enclosure drives. Solaris 11.3 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 7 system. The feature utility can only be run while the VSM 7 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 7 that already has customer data present, the encryption feature can be enabled only if the current utilization of the storage disk enclosure 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 7 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 VSM 7 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 7 will simply increase the storage size of the storage disk enclosure arrays, maintaining the encryption setting that exists at upgrade time.

Software upgrades to the VSM 7 will preserve the encryption authorization key(s) stored on the mirrored server's rpool disk drives.

The VSM 7 CLI will indicate if the encryption feature is enabled and 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.

9

Enhanced Replication (RLINKS) Feature

VSM 7 supports an Enhanced Replication feature that extends the replication capabilities of the VSM 7 product. With Enhanced Replication, synchronous replication begins replicating data to the target VTSS upon first host write to the VTV and provides host acknowledgment to the rewind unload operation once all data has been successfully replicated to the target VTSS.

A new replication facility, RLINKs, is used for Enhanced Replication. An RLINK is composed of all IP paths defined to the target VTSS. There is only one RLINK between the primary and target VTSS. With RLINKs, the number of replications is limited only to the number of virtual tape devices (VTDs) supported within the VTSS.

Note: RLINK functionality cannot be used concurrently with synchronous CLINK replication.

Enhanced Replication is initially available for use between clustered VSM 7 or VSM 6 VTSSs, where each VTSS can be both a primary and a target for bi-directional synchronous VTV-level replication. Subsequent releases provide support for three-target synchronous replication and file-level synchronous replication.

10

VSM Extended Storage Feature

The VSM Extended Storage feature (ExS) is a VTCS software enhancement that allows the VTSS to access and utilize storage external to the VTSS.

With this feature, a VSM 6 or VSM 7 system can migrate and recall VTVs to storage targets “extended” beyond the typical Oracle StorageTek targets (for example, tape libraries, tape drives, and Virtual Library Extension).

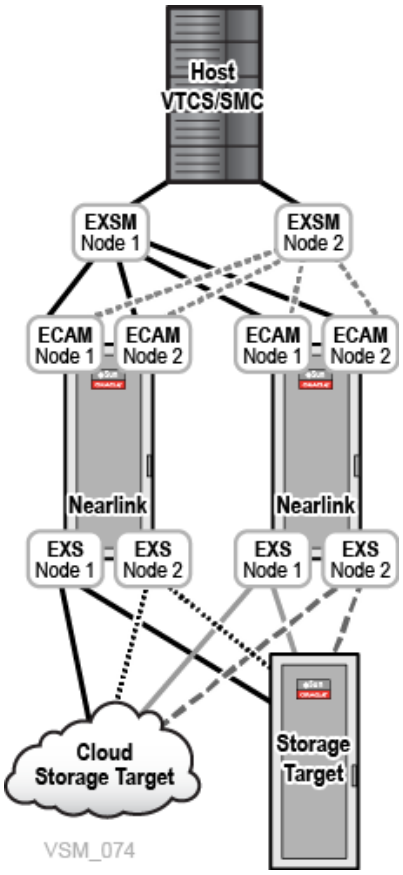
ExS is included in the base VSM 6 or VSM 7 microcode and is configured by Oracle Services personnel as part of the VSM configuration.

ExS supports targets that utilize the OpenStack Swift (object storage) protocol and those that support network attached storage (NAS). These include:

- Oracle Object Storage Classic (OCC)
- Oracle Archive Storage Classic (OCC)
- Any private cloud that supports the OpenStack Swift protocol
- Oracle ZS5-2 or ZS5-4 configured as a Swift target
- Oracle ZS5-2 or ZS5-4 configured as an NSF target

The following figure illustrates a VSM 7 environment using VSM Extended Storage for cloud attach:

Figure 10–1 VTSS Extended Storage cloud Attach



As shown in Figure 10–1, ExS software is distributed across multiple VSM nodes, and communicates as follows:

- VTCS or oVTCS resides on the customer network and communicates with all Extended Storage Manager (EXSM) instances using the UUI protocol to NET0 on all VTSS nodes.
- All EXSM instances communicate with all ECAM/IP instances on all VTSS nodes through NET0.
- All EXS instances communicate with all Extended Storage targets through the VTSS REP ports.

ExS software is maintained as part of the VTSS code. ExS reconfiguration requires a disruptive outage of the VTSS in order to initiate changes.

Oracle Cloud Options

VSM 7 Extended Storage supports three Oracle Cloud options:

- Oracle Cloud Object Storage Classic
- Oracle Cloud Archive Storage Classic
- Encryption within Oracle Cloud

For each option, the Oracle CSE must retrieve the customer's Oracle Cloud account information to create and configure your initial connection between VSM Extended Storage and Oracle Cloud. Account information includes the following:

- Account Name
- User Name
- User Password
- Authentication URL

For information about how to get started with the Oracle Cloud:

http://docs.oracle.com/cloud/latest/trial_paid_subscriptions/CSGSG/toc.htm

For more information about the Oracle Cloud subscription:

http://docs.oracle.com/en/cloud/iaas/storage-cloud/index.html

For up-to-date Cloud information:

http://docs.oracle.com/cloud/latest/

Oracle Storage Cloud Service – Object Storage

Storing data in the Oracle Cloud is much like storing data in a VLE local disk pool. The following steps outline what is needed to configure VSM Extended Storage for storing a virtual tape volume (VTV) in Oracle Cloud.

MVC ranges are determined by the customer. They are used to configure VTCS host software and provided to the Oracle support team for configuration of the VSM Extended Storage feature.

If the VSM ExS will store VTV data in the Oracle Cloud, you must define and configure the vMVC pool range for VSM ExS Oracle Cloud Storage.

The performance of VSM ExS to cloud data transfer performance is subject to IP bandwidth and delay as well as Oracle Cloud performance capabilities.

Oracle Storage Cloud Service – Archive Storage

Storing data in the Oracle Cloud is much like storing data locally, though there are some exceptions regarding a recall of data stored in the Cloud Archive.

The steps for setting up the VLE for using the Oracle Storage Cloud Service – Archive Storage is similar to the steps for Oracle Cloud.

MVC ranges are determined by the customer. They are used to configure VTCS host software and given to the Oracle support team for configuration of VSM Extended Storage. The customer must provide up to two vMVC ranges when using Cloud Archive:

- A vMVC range for VSM ExS Storage Cloud
- A vMVC range for VSM ExS Cloud Archive Storage

When creating vMVCs on the ExS, the Oracle support person selects an 'archive' flag for vMVCs that will use Cloud Archive. This is what triggers the 'archive' functionality within the Oracle Cloud. Once VMVC definitions are configured, VTV Migrate, Recall, and Copy operations are possible for both vMVC ranges, however there are exceptions for the Cloud Archive range of vMVCs.

Migrate

VTV migrate operations perform the same for VTVs migrated to VLE local disk pool or VTVs migrated to the Oracle Cloud Service. Once a VTV is migrated to Oracle Cloud Object Storage, it automatically moves to Oracle Cloud Archive Storage.

Restore and Recall

Once a migrated VTV is moved to Oracle Cloud Archive Storage, you must manually restore the VTV before it can be recalled by ExS. This involves moving the VTV from Oracle Cloud Archive Storage back to Oracle Cloud Object Storage.

Use a `RESTORE_VTV` request to manually restore a VTV from Oracle Cloud Archive Storage. Use a `Route` command to issue this request for the appropriate ExS storage manager.

Use and of the following methods to process the `RESTORE_VTV` request:

- Issue the SMC `Route` command from an MVS console.

  ```
  F ELS73SMC, ROUTE DVTGRD13 RESTORE_VTV VOLUME=5B1307 VTV=CV1234
  ```

- Issue the SMC `Route` command from the `SMCUUUI` utility. Include the `Route` command in the `UUIIN` data set. Refer to the *ELS command, Control Statement, and Utility Reference* for more information.
- Issue the SMC `Route` command from the VSM GUI.

  ```
  ROUTE DVTGRD13 RESTORE_VTV VOLUME=5B1307 VTV=CV1234
  ```

Displaying Progress

Issue a `QUERY_RESTORE` request to display progress for the VTVs that are in the restore process. For example:

```
ROUTE DVTGRD13 QUERY_RESTORE VOLUME=5B1307 VTV=CV1234
```

Progress is displayed. For example:

```
Restore initiated via SMCUUI Interface:
```

- `Archived`
- `In Progress`
- `Complete - Restored`
- `Complete - Not Archive`

Once a `Complete` response is received, the VTV can be recalled normally.

> **Note:** Once a VTV is restored, it will remain in Oracle Storage Cloud Service – Object Storage for 24 hours; then it will return to Archive state. Oracle service level agreement (SLA) to restore a VTV is 4 hours. Multiple `RESTORE_VTV` commands can be initiated at the same time.

Oracle Cloud Encryption

Encryption, if VTV data is stored in the Oracle Cloud, is offered for both Archive and non-Archive Cloud offerings.

Encryption is controlled at the vMVC boundary, that is, if a vMVC is created with the Encryption flag set, all of the VTVs in that vMVC will be encrypted. Migrate and recall

operations for encrypted VTVs behave exactly the same for each of the respective Clouds (Archive and non-archive) as described above. The only behavior difference is a performance decrease of 10% for encrypted VTVs. The steps for setting up the VSM Extended Storage for Oracle Cloud Encryption are very similar to steps above for Oracle Cloud and Oracle Cloud Archive.

MVC ranges are determined by the customer. They are used to configure VTCS host software and given to the Oracle support team for configuration of VSM Extended Storage. The customer must provide up to two vMVC ranges when using Cloud with Encryption:

- A vMVC range for VSM ExS Storage Cloud
- A vMVC range for VSM ExS Cloud Archive Storage (with or without Encryption)

When creating vMVCs on ExS, an Oracle support person sets an encryption flag for any vMVCs that will contain encrypted VTVs. Other than the performance there is no difference in the way VTV data is stored (Migrate) and retrieved (Recall) from an ExS or host perspective.

Visit the Oracle Cloud website for information pertaining to the Encryption feature as it is handled within the Oracle Cloud.

Configuring VTCS or oVTCS for Extended Storage

VTCS and oVTCS applications recognize the ExS system as a Storage Manager, similar to a standard VLE system. Therefore, configuration is the same as for VLE 1.5.3 Cloud storage.

Refer to the VLE publication *Configuring Host Software for VLE Guide* for more information.

Updating ELS PARMLIB

To define the Extended Storage Manager name and define RTDs in VTCS or oVTCS:

1. Define the Extended Storage Manager name.

   Use the VTCS `CONFIg TAPEPlex STORMNGR` statement to define the Extended Storage Manager name.

   For example:

   ```
   TAPEPLEX THISPLEX(tapeplex_name) STORMNGR(exs_name)
   ```

   Refer to the your Oracle StorageTek Enterprise Library Software (ELS) publications for more information about these commands.

2. Define RTD(s) to the ExS STORMNGR.

   Use the VTCS `CONFIg RTDpath` statement to define the path to the ExS STORMNGR, using only the `STORMNGR` and `IPIF` parameters.

   ```
   RTD NAME=EXSRTDxx STORMNGR=exs_name IPIF=nn:nn
   ```

   Refer to the your Oracle StorageTek Enterprise Library Software (ELS) publications for more information about these commands.

Updating SMC PARMLIB

To define the ExS STORMNGR and SERVER in SMC:

1. Define and enable the ExS STORMNGR.

   Use the SMC STORMNGR command to define and enable the ExS storage manager to SMC.

   ```
   STORMNGR NAME(exs_name) ENABLE
   ```

   The ENAble keyword enables the specified ExS Storage Manager. This is the default when a new ExS Storage Manager is added.

   Refer to the your Oracle StorageTek Enterprise Library Software (ELS) publications for more information about these commands.

2. Define the ExS SERVER.

   Use the SMC SERVer command to define a named path for the ExS Storage Manager.

   For example:

   ```
   SERVER NAME(server_name) STORMNGR(exs_name)
   IP(vtssnet0ipaddress) PORT(60000)
   ```

   Before a SERVer is defined, the ExS Storage Manager that it references must be defined using a STORMNGR command. The ExS Storage Manager name associated with a SERVer cannot be changed.

   Refer to the your Oracle StorageTek Enterprise Library Software (ELS) publications for more information about these commands.

Defining POOLPARM MVCs and VOLPARM VOLSERs

To define MVC pools:

1. Code POOLPARM or VOLPARM statements to define the MVC pools.

   ```
   POOLPARM NAME(LEPOOL1) TYPE(MVC)
   VOLPARM VOLSER(A00000-A00099)
   ```

2. Use the SET VOLPARM command to validate the POOLPARM or VOLPARM statements without loading them.

   ```
   SET VOLPARM APPLY(NO)
   ```

3. Use the SET VOLPARM command to load the POOLPARM or VOLPARM statements.

   ```
   SET VOLPARM APPLY(YES)
   ```

Refer to the your Oracle StorageTek Enterprise Library Software (ELS) publications for more information about these commands.

A

Controlling Contaminants

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

P

R

S

T

V

W