System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

IP Packet Capture

MAY 2017

MN003306A01-B

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

For...	Phone
United States Calls	**800-221-7144**
International Calls	**302-444-9800**

North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola SSC.

For...	Phone
Phone Orders	**800-422-4210** (US and Canada Orders) For help identifying an item or part number, select choice 3 from the menu.
	302-444-9842 (International Orders) Includes help for identifying an item or part number and for translation as needed.
Fax Orders	**800-622-6210** (US and Canada Orders)

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

Document History

Version	Description	Date
MN003306A01-A	Original release of the *IP Packet Capture* manual	November 2016
MN003306A01-B	This version includes the following updated and new topics: • Installing IP Packet Capture on page 59 • Applying Platform Patch on page 72 • Hypervisor Statistics State Transition Traps for UEM on page 85	May 2017

This page intentionally left blank.

Contents

This page intentionally left blank.

List of Figures

This page intentionally left blank.

List of Tables

This page intentionally left blank.

List of Processes

This page intentionally left blank.

List of Procedures

About IP Packet Capture

IP Packet Capture is an application for capturing transactions between network elements and collects performance statistics for the Virtual Management Servers (VMS) in the ASTRO® 25 system.

What Is Covered in This Manual

This manual contains the following chapters.

- IP Packet Capture Introduction on page 25 provides a description of the IP Packet Capture application, including a glossary of terms related to the operation of IP Packet Capture.
- IP Packet Capture User Interface Description on page 31 describes the Web-based user interface for IP Packet Capture and its main areas: download of packet capture files and hypervisor statistics files, configuration of packet captures and hypervisor definitions, and passphrase complexity settings.
- IP Packet Capture User Interface Operations on page 41 describes the operations that you can perform in IP Packet Capture.
- IP Packet Capture User Interface Access and Users on page 55 provides information about the clients that you can use for access, the operating system and Web browser requirements, and the configuration of user accounts with access rights for IP Packet Capture.
- IP Packet Capture Installation on page 59 describes the installation of IP Packet Capture on a Virtual Management Server (VMS).
- IP Packet Capture Configuration for SNMPv3 on page 75 provides the SNMPv3 configuration procedures to ensure secure communication between IP Packet Capture and Unified Event Manager (UEM).
- IP Packet Capture Disaster Recovery on page 79 provides recovery procedures for restoring IP Packet Capture after a failure of the VMS or the Direct Attached Storage (DAS).
- IP Packet Capture Troubleshooting on page 83 describes the traps and alarms sent by IP Packet Capture to UEM and provides guidelines for resolving issues with the application.
- IP Packet Capture Reference on page 89 contains a reference table that outlines the boot order for virtual machines hosted on a VMS and the list of Windows-based devices that can be used to connect to a VMS.
- IP Packet Capture Feature Expansion on page 93 provides the process for adding the IP Data Capture feature to your system release, including connection tables and diagrams.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

See the following documents for associated information about the radio system.

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola communications site. Also known as R56 manual. This manual may be purchased on CD *9880384V83* by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Overview and Documentation	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
ASTRO 25 vCenter Application Setup and Operations Guide	Provides a description of the VMware vCenter application used to provide VMware fault tolerance and VMware high availability for virtual machines and includes processes and procedures to support the setup and operations for the VMware vCenter application in ASTRO® 25 systems.
Authentication Services	Provides information relating to the implementation and management of the Active Directory (AD) service, Remote Authentication Dial-In User Service (RADIUS), and Domain Name Service (DNS) in ASTRO® 25 systems.
Backup and Restore Services	Provides information relating to the implementation and management of centralized backup and restore services for supported devices in ASTRO® 25 systems. This manual addresses server and client functions required for these services.
Core Security Management Server	Provides information relating to the implementation and management of Core Security Management Server (CSMS). The CSMS hosts network security software components in ASTRO® 25 systems, including client and server functions supporting RADIUS authentication for remote access. This manual also includes information about managing system-wide anti-malware, anti-virus, and anti-spyware protection along with information associated with the firewall manager user interface hosted on the CSMS.
MAC Port Lockdown	Provides information on the implementation and management of MAC Port Lockdown for standard Ethernet ports on Hewlett-Packard (HP) switches and for the internal switch of GCP 8000 Site Controllers and GPB

Table continued…

Related Information	Purpose
	8000 Reference Distribution Modules (RDMs) in ASTRO® 25 systems. Additionally, the document contains instructions for configuring supplemental Ethernet port security, including the implementation of fiber optic ports on HP switches.
Securing Protocols with SSH	Provides information on the implementation and management of the Secure Shell (SSH) protocol for secure transmission of data between devices in ASTRO® 25 systems, including configuration sequences that minimize downtime when adding this feature to a system that is already in operation.
SNMPv3	Provides information relating to the implementation and management of the SNMPv3 protocol in ASTRO® 25 systems.
System LAN Switches	Provides use of Hewlett-Packard (HP) switches in ASTRO® 25 systems, including LAN switches and backhaul switches. In addition to common procedures for installation, configuration, operation, and troubleshooting of the switches, this manual provides information for specific ASTRO® 25 system sites and features that HP switches can support.
Unified Event Manager	Covers the use of Unified Event Manager (UEM) that provides reliable fault management services for devices in ASTRO® 25 systems.
Unix Supplemental Configuration	Provides additional procedures for Solaris-based and Linux-based devices, including password management, welcome banners configuration, and general administration.
Virtual Management Server Hardware	Provides information for implementing, maintaining, and replacing common Hewlett-Packard hardware for servers in an ASTRO® 25 system.
Virtual Management Server Software	Provides procedures for implementing and managing VMware ESXi-based virtual server hosts on the common Hewlett-Packard hardware platform in ASTRO® 25 systems.

This page intentionally left blank.

Chapter 1

IP Packet Capture Introduction

The IP Packet Capture application captures transactions between network elements in an ASTRO® 25 system and collects performance data for Virtual Management Servers (VMS) in the zone where IP Packet Capture is located. The application captures network activity in the form of IP packets that pass through the designated devices and gathers statistics for the monitored servers. IP Packet Capture provides easy access to current and historical records of network traffic and server performance statistics for diagnostic purposes and timely system repair. The application ensures minimal issue investigation times.

IP Packet Capture consists of a RHEL-based server and a Web-based user interface. The server resides as a virtual machine on a VMS. IP Packet Capture is configured for automatic startup and is always on when the VMS is operating. The application does not require user interaction on a regular basis. The IP Packet Capture Web-based user interface is used to configure packet captures and hypervisor definitions, and download packet capture files and hypervisor statistics files.

IP Packet Capture assumes that switch configuration has been completed to allow specific switch ports to be monitored and a monitor port exists for IP Packet Capture to connect to. A single capture/monitor connection can be established between IP Packet Capture and a given switch. The IP Packet Capture user interface permits association of a switch name with the physical capture/monitor connection and disk space allocated to the packet capture files.

IP Packet Capture is a client of the following applications that provide network services for the virtual machines running on the VMS:

Backup and Restore (BAR)

The BAR server regularly backs up the zone-specific packet captures, hypervisor definitions, and identity data for IP Packet Capture. In a failure scenario, this data can be used to restore the IP Packet Capture virtual machine. BAR does not back up the packet capture files and hypervisor statistics files.

Centralized Event Logging

The Centralized Event Logging server uses the syslog standard to log operating system (OS) events generated by the IP Packet Capture virtual machine in the form of event messages. Events logged include operations on the Web-based user interface: login failure and success, retrieval of packet capture files and hypervisor statistics files, configuration changes, such as adding, enabling, disabling, editing, and deleting packet captures and hypervisor definitions.

Domain Controller

In L and M cores, IP Packet Capture is a client of the Domain Controller. During installation, the IP Packet Capture virtual machine is joined to the Active Directory domain to enable authentication services for the application.

McAfee

McAfee provides antivirus protection for the IP Packet Capture virtual machine.

Unified Event Manager (UEM)

IP Packet Capture reports operational states and errors to UEM for fault management. UEM displays alarms for IP Packet Capture, providing information about the severity and causes of every event.

1.1 IP Packet Capture Server Architecture

The IP Packet Capture application runs as a virtual machine that resides on a Virtual Management Server (VMS).

VMSs in the following locations support the IP Packet Capture application:

- Redundant zone cores: L2, M2, and M3
- Non-redundant zone cores: L1, M1
- K cores
- Trunking Subsystem (Tsub)

1.2 IP Packet Capture User Interface Overview

The IP Packet Capture application provides a Web-based user interface for easy access and operation. Depending on the group membership, users can access different parts of the user interface and perform operations in the following areas: packet capture files and hypervisor statistics files download, configuration of packet captures and hypervisor definitions, and passphrase complexity settings.

The IP Packet Capture user interface consists of the following components:

Login page
Provides a form for entering user credentials and accessing the application.

Capture Files Download
Displays packet capture files for a designated device from a specified period and provides the option to download the selected files in an encrypted archive. To access the files in the downloaded archive, use WinZip or 7-Zip and enter the passphrase used for packet capture file encryption.

Capture Configuration
Provides an interface for creating, editing, enabling, disabling, and deleting packet capture definitions, and removing packet capture files. A packet capture definition is a mapping of a physical capture interface to a share of the packet capture repository disk. Each packet capture definition is identified with a friendly name.

Hypervisor Statistics Download
Displays hypervisor statistics files for the host Virtual Management Server (VMS) from a specified period and allows you to download the selected files in an encrypted archive. To access the files in the downloaded archive, use WinZip or 7-Zip and enter the passphrase used for statistics file encryption.

Hypervisor Statistics Configuration
Provides an interface for creating, editing, enabling, disabling, and deleting hypervisor definitions, and removing statistics files. A hypervisor definition is a mapping of a Virtual Management Server (VMS) identified by an IP address to the hypervisor statistics files repository. This mapping allows you to collect performance data for the designated VMS. Each hypervisor definition is identified with a friendly name.

Passphrase Complexity
Provides the complexity rules for passphrases used to encrypt packet capture files and hypervisor statistics files downloaded from IP Packet Capture and to decrypt the downloaded archives. The complexity rules determine which passphrases are accepted by the application during download. The passphrase complexity rules can be modified or restored to the default settings.

1.3 IP Packet Capture Glossary

The following terms are related to installing and configuring the IP Packet Capture application in an ASTRO® 25 system and operating the IP Packet Capture user interface.

packet capture / packet capture definition

Packet captures are configuration records in IP Packet Capture. A packet capture is a mapping of a physical capture interface to a share of the packet capture repository disk. Each packet capture is identified with a friendly name. When a packet capture is enabled, the application monitors the device connected to the selected capture interface and stores packet capture files for that device on the repository disk. You can configure packet captures in the IP Packet Capture **Capture Configuration** window.

packet capture file

Packet capture files are records of traffic on the devices monitored by IP Packet Capture. The application captures the transactions between network elements in the form of IP packets that pass through the designated devices. Packet capture files are stored in the packet capture files repository. The repository disk is a component of the Virtual Management Server (VMS) that hosts the IP Packet Capture virtual machine. The repository disk is configured for file rotation, which means that as the disk fills up, the most recent packet capture files start to replace the oldest capture files. The size of the repository disk provides seven days of data retention at a minimum. When you download the selected packet capture files from the IP Packet Capture **Capture Files Download** window, the files are saved on your computer as an encrypted `.zip` archive protected with a passphrase. The same passphrase is required to decrypt the archive. To access the files in the downloaded archive, use WinZip or 7-Zip. Packet capture files provide data for diagnostic purposes and timely system repair. The packet capture file format is: `.pcap`

capture point

Capture points are network elements that are connected to IP Packet Capture for monitoring purposes, for example: core LAN switches, core backhaul switches. Network elements are connected with Ethernet cables to capture interfaces on the extender panel located on the Virtual Management Server (VMS) rack. If the network element to be monitored is a switch, the connection must use the monitor port on the switch.

capture interface

Capture interfaces are physical interfaces assigned to IP Packet Capture and located on the extender panel of the Virtual Management Server (VMS) rack. Each monitored device is connected to an available capture interface with an Ethernet cable. A single capture/monitor connection is allowed between IP Packet Capture and a monitored device. The IP Packet Capture user interface allows you to select a capture interface and enable monitoring of the designated device.

hypervisor definition

Hypervisor definitions are configuration records in IP Packet Capture. A hypervisor definition is a mapping of a Virtual Management Server (VMS) identified by an IP address to the hypervisor statistics repository. This mapping allows you to collect performance data for the designated VMS. Each hypervisor definition is identified with a friendly name. When a hypervisor definition is enabled, the application monitors the designated VMS and stores statistics for that device on the hypervisor statistics files repository disk. You can configure hypervisor definitions in the IP Packet Capture **Hypervisor Statistics Configuration** window.

hypervisor statistics

Hypervisor statistics provide performance data for the Virtual Management Servers (VMS) monitored in IP Packet Capture. The application obtains performance data for the designated servers and stores the data in the hypervisor statistics files repository. The statistics are collected every fifteen seconds. These collections are aggregated into files spanning a one hour period. The statistics files repository disk is a component of the VMS that hosts the IP Packet Capture virtual machine. The repository is configured for file rotation, which means that as the disk fills up, the most recent files start to replace the oldest files. The size of the repository provides ten days of data retention at a minimum. When you download the selected statistics files from the IP Packet Capture **Hypervisor Statistics Download** window, the statistics files are saved on your computer as an encrypted `.zip` archive protected with a passphrase. The same passphrase is required to decrypt the archive. To access the files in the downloaded archive, use WinZip or 7-Zip. Statistics provide data for diagnostic purposes and timely system repair.

monitor port

Monitor ports are configured for monitoring purposes and located on the devices that can be connected to IP Packet Capture. Monitor ports on the designated devices are connected to capture interfaces with Ethernet cables.

passphrase

Passphrases are used to encrypt and decrypt packet capture files and hypervisor statistics files. When you download packet capture files or hypervisor statistics files from IP Packet Capture, you must enter a passphrase that complies with the complexity rules configured in the application. The same passphrase is later used to decrypt the downloaded packet capture file or hypervisor statistics file. The passphrase complexity rules can be modified or restored to default settings in the IP Packet Capture **Passphrase complexity configuration** window.

1.4 Network Elements Monitored by IP Packet Capture

The packet capture feature of the IP Packet Capture application allows you to capture transactions between network elements in your ASTRO® 25 system. Depending on your system configuration, different types and numbers of devices can be connected to IP Packet Capture for IP traffic monitoring. Network elements are connected with Ethernet cables to capture interfaces on the extender panel located on the Virtual Management Server (VMS) rack. The monitored network elements are called capture points. If the network element to be monitored is a switch, the connection must use the monitor port on the switch.

Non-Redundant Cores

In non-redundant cores (K1, L1, and M1 cores), the following devices can be connected to IP Packet Capture on VMS01. In Dynamic System Resilience (DSR) configurations, the same connections are required in the backup core on VMS09.

Capture points connected to VMS01 and VMS09:

- Core LAN Switch 1
- Core Backhaul Switch 1
- ISSI/CSSI Firewall 1 (untrusted)
- Other capture points: co-located site switches

Redundant Cores

In redundant cores (K2, L2, M2, and M3), the following devices can be connected to IP Packet Capture on VMS01 and VMS02. In Dynamic System Resilience (DSR) configurations, the same connections are required in the backup core on VMS09 and VMS10.

Capture points connected to VMS01 and VMS09:

- Core LAN Switch 1
- Core Backhaul Switch 2
- Mediation LAN Switch 2
- ISSI/CSSI Firewall 2 (untrusted)

Capture points connected to VMS02 and VMS10:

- Core LAN Switch 2
- Core Backhaul Switch 1
- Mediation LAN Switch 1
- ISSI/CSSI Firewall 1 (untrusted)

NOTICE:
Capturing on the Mediation LAN Switch is possible only if the Intrusion Detection System (IDS) does not exist or a network tap is used to replicate monitor traffic to IP Packet Capture and IDS simultaneously.

In Dual Core DSR configurations, VMS09 and VMS10 are free to use for additional capture points, such as Core LAN Switch 3 and co-located site switches.

Trunking Subsystem Prime Site

At the prime site in a Trunking Subsystem (Tsub), the following devices can be connected to IP Packet Capture on VMS01.

Capture points connected to VMS01:

- Site LAN Switch 1
- Site LAN Switch 2 (non-Geo configuration)
- Site Backhaul Switch 1
- Site Backhaul Switch 2 (non-Geo configuration)

Related Links

IP Packet Capture Connections on page 103

1.5
Virtual Management Servers Monitored by IP Packet Capture

The hypervisor statistics feature of the IP Packet Capture application allows you to collect performance data for the Virtual Management Server (VMS) hosting IP Packet Capture. Hypervisor statistics configuration does not require any additional cable connections. When you install IP Packet Capture on a VMS, a default hypervisor definition is created for the VMS. This hypervisor is disabled and requires configuration. To start collecting performance statistics for the VMS, log on to the IP Packet Capture user interface and edit the hypervisor definition: enter the appropriate Global Web Services Credentials and enable the definition.

This page intentionally left blank.

Chapter 2

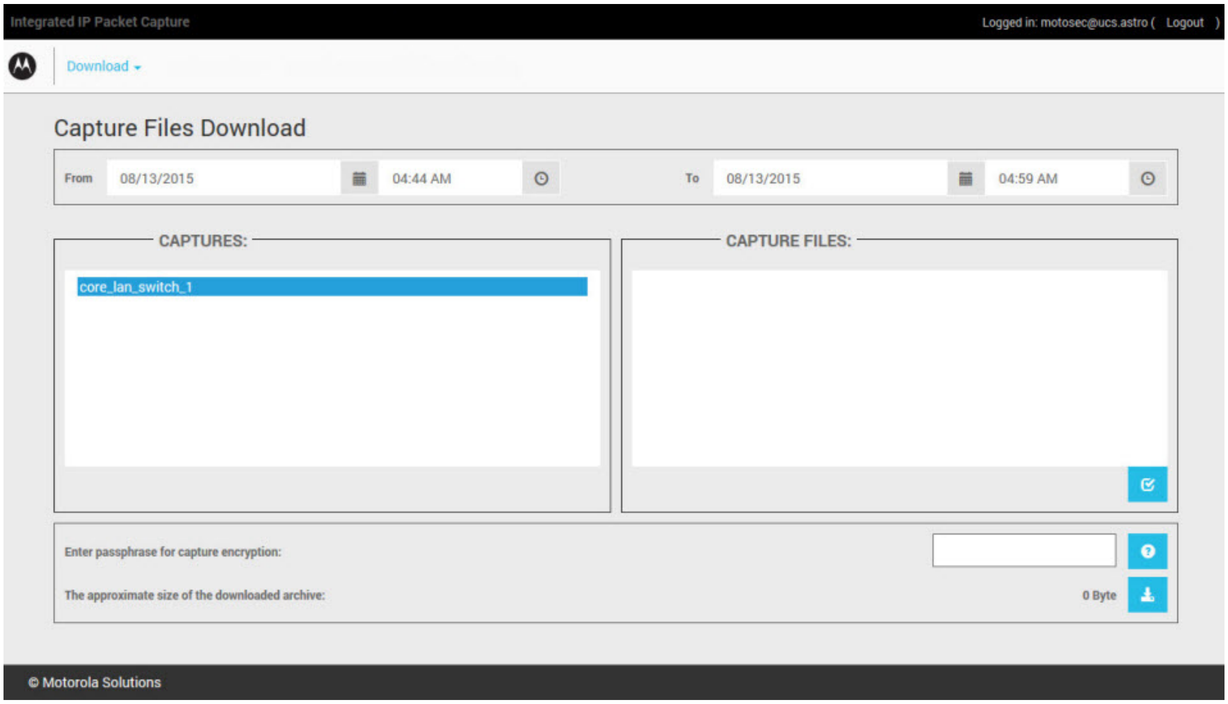
IP Packet Capture User Interface Description

This chapter describes the Web-based user interface for IP Packet Capture. Depending on the group membership of your user account, you can access the main areas and functions of IP Packet Capture: packet capture files and hypervisor statistics files download, configuration of packet captures and hypervisor definitions, and passphrase complexity settings.

2.1 Capture Files Download

Packet capture files retrieval is a feature of the IP Packet Capture application. You can select the packet capture files for a designated device from a specified period and download the files from the IP Packet Capture repository as an encrypted zipped archive protected with a passphrase. To access the files in the downloaded archive, use WinZip or 7-Zip and enter the passphrase used for packet capture file encryption. The download operation is only available to users that belong to the **confgaud** and **infradm** user groups.

Figure 1: IP Packet Capture – Capture Files Download



From 08/13/2015 04:44 AM

To 08/13/2015 04:59 AM

core_lan_switch_1

Enter passphrase for capture encryption:

The approximate size of the downloaded archive: 0 Byte

The **Capture Files Download** window contains the following fields, icons, and buttons for quick selection and download of packet capture files. Access the **Capture Files Download** window from the **Download** menu.

From
: Use this field to define the start of the period relevant for your diagnostic task. When you set the start date, the **Capture Files** area is updated with packet capture files taken in the specified period.

To

Use this field to define the end of the period relevant for your diagnostic task. When you set the end date, the **Capture Files** area is updated with packet capture files taken in the specified period.

📅

Click the calendar icon or the date in the **From** and **To** fields to display a calendar application and select the appropriate date.

🕒

Click the clock icon or the time in the **From** and **To** fields to display a clock application and select the appropriate time.

Captures

This area displays the friendly names of the packet captures configured in IP Packet Capture. For example: Core_LAN_Switch_1. Each packet capture monitors the traffic on the designated device.

Capture Files

When you select a packet capture in the **Captures** area, the **Capture Files** area displays the packet capture files saved in the repository for the selected capture. The packet capture file format is: `.pcap`

☑

Click the selection icon to select all the packet capture files displayed in the **Capture Files** area.

Enter passphrase for capture encryption

Packet capture files are downloaded as an encrypted zipped archive protected with a passphrase. In this field, enter a passphrase for packet capture file encryption. You can use any passphrase that complies with the passphrase complexity rules configured in IP Packet Capture. The rules specify the minimum and maximum length of a passphrase and the minimum number of characters of each character type that a passphrase must include.

The approximate size of the downloaded archive

When you select the packet capture files for download, the application displays the approximate size of the archive in this field.

?

Click the info button to see the passphrase complexity rules currently configured in IP Packet Capture. Use this information to choose an acceptable passphrase.

⤓

Click the download button to download the selected packet capture files and save them to a selected directory on your computer.

Related Links

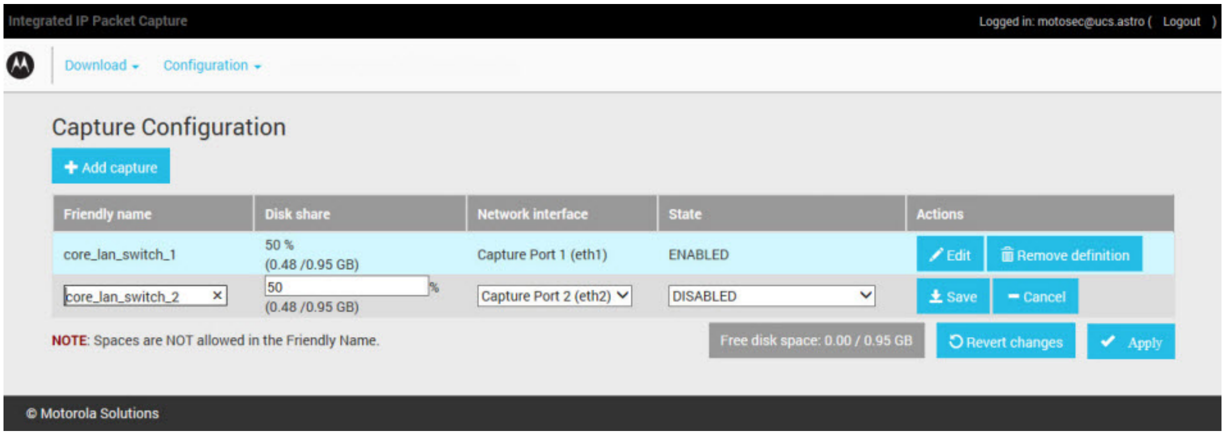
Downloading Packet Capture Files on page 43
IP Packet Capture User Interface Access on page 55

2.2 Capture Configuration

Packet capture configuration is a feature of the IP Packet Capture application. Each packet capture is associated with an available capture interface and assigned a share of the repository disk for storing packet capture files. Before you create a packet capture, ensure that an appropriate Ethernet cable connection is in place between a monitor port on the designated device and a capture interface for IP Packet Capture. Capture interfaces are located on the extender panel of the server rack holding the

Virtual Management Server (VMS) that hosts the IP Packet Capture virtual machine. Packet capture configuration is only available to users that belong to the **infradm** user group.

Figure 2: IP Packet Capture – Capture Configuration



Friendly name	Disk share	Network interface	State	Actions
core_lan_switch_1	50 % (0.48 /0.95 GB)	Capture Port 1 (eth1)	ENABLED	Edit Remove definition
core_lan_switch_2	50 % (0.48 /0.95 GB)	Capture Port 2 (eth2)	DISABLED	Save Cancel

NOTE: Spaces are NOT allowed in the Friendly Name.

The **Capture Configuration** window contains the following fields, columns, and buttons that allow you to add, remove, and edit packet captures. Access the **Capture Configuration** window from the **Download** menu.

Add capture
When you click this button, a row for a new packet capture appears in the table. The packet capture settings are ready for editing.

Friendly name
In this column, enter an easily recognizable name for a packet capture. For example: Core_LAN_Switch_1. Spaces are not allowed in friendly names for packet captures.

Disk share
In this column, enter a percentage of the repository disk space to be assigned for packet capture files from a packet capture. The total disk share configured for all packet captures defined in the application must not exceed 100%. If the total disk share is greater than 100%, the application displays a warning. Ensure that the disk share is distributed within the limit of 100% by editing other packet captures if necessary.

Network interface
This column contains a drop-down list of available capture interfaces. Select a capture interface to be used for the packet capture that you are editing.

State
In this column, select an operational state for a packet capture:

ENABLED
An enabled packet capture is active. IP Packet Capture monitors the traffic on the designated device and saves packet capture files for this device in the repository.

DISABLED
A disabled packet capture is inactive. Monitoring on the designated device is turned off.

DISABLED and DELETE FILES
Select this state to disable a packet capture and clear all packet capture files saved in the repository for this packet capture.

Actions
This column contains buttons that allow you to perform the following operations on packet captures:

Edit
Click this button to modify a packet capture.

Remove definition
Click this button to delete a packet capture and the packet capture files associated with this definition.

Save
When you finish editing a packet capture, click this button to save the changes. This option saves the new settings as pending changes, but does not affect system operation.

Cancel
Click this button to undo the changes that you have made when editing a packet capture.

Free disk space
This area shows the information about the packet capture repository disk in the following format: ***<free disk space>*** / ***<total disk space>***. The free disk space is re-calculated every time you assign a different disk share to a packet capture.

Revert changes
Click this button to undo the changes that you have made to the packet captures since the last time you clicked **Apply**.

Apply
Click this button to update the system operation with the pending changes that you have made to the packet captures.

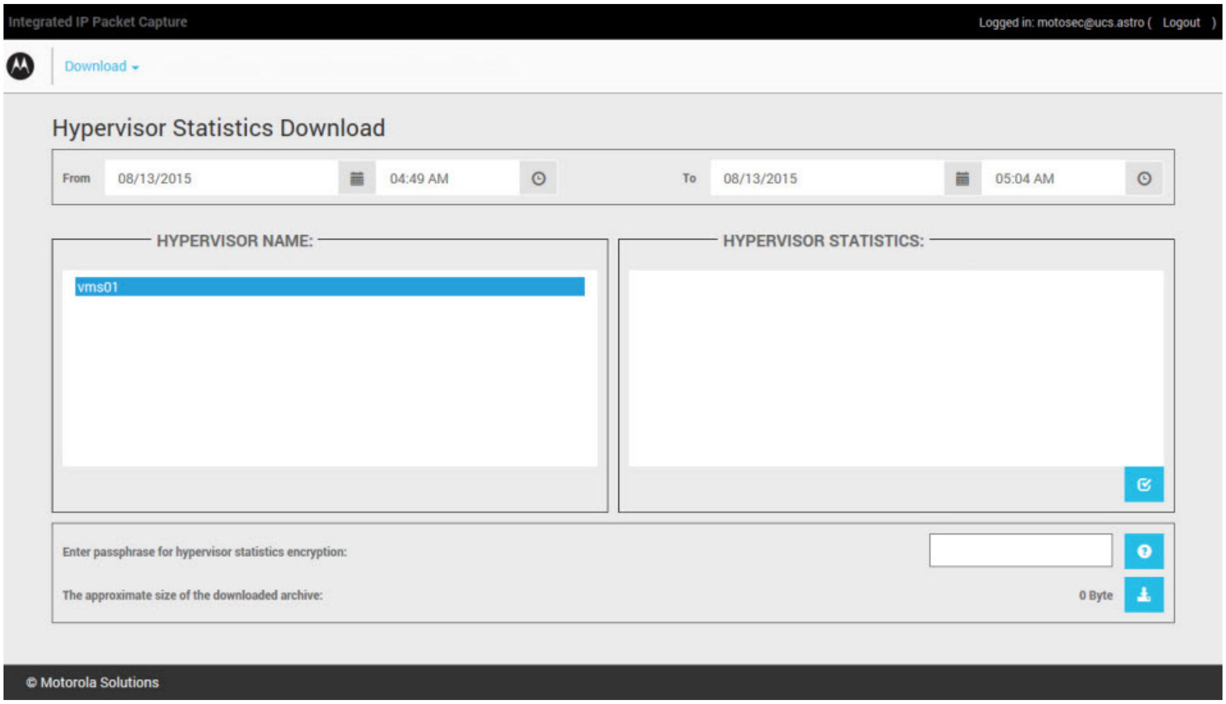
Related Links

Adding Packet Captures on page 44
Editing Packet Captures on page 45
Enabling Packet Captures on page 46
Disabling Packet Captures on page 46
Removing Packet Captures on page 47
Deleting Packet Capture Files on page 47
IP Packet Capture User Interface Access on page 55

2.3 Hypervisor Statistics Download

The hypervisor statistics feature of the IP Packet Capture application allows you to download performance data for the Virtual Management Servers (VMS) monitored by IP Packet Capture. You can select the hypervisor statistics files for a designated VMS from a specified period and download the files from the IP Packet Capture statistics repository as an encrypted zipped archive protected with a passphrase. To access the files in the downloaded archive, use WinZip or 7-Zip and enter the passphrase used for statistics encryption. The download operation is only available to users that belong to the **confgaud** and **infradm** user groups.

Figure 3: IP Packet Capture – Hypervisor Statistics Download


Integrated IP Packet Capture
Logged in: motosec@ucs.astro (Logout)
Download
Hypervisor Statistics Download
HYPERVISOR NAME:
HYPERVISOR STATISTICS:
© Motorola Solutions

From 08/13/2015 04:49 AM To 08/13/2015 05:04 AM

HYPERVISOR NAME: vms01

Enter passphrase for hypervisor statistics encryption:

The approximate size of the downloaded archive: 0 Byte

The **Hypervisor Statistics Download** window contains the following fields, icons, and buttons for quick selection and download of hypervisor statistics files. Access the **Hypervisor Statistics Download** window from the **Download** menu.

From

Use this field to define the start of the period relevant for your diagnostic task. When you set the start date, the **Hypervisor Statistics** area is updated with statistics collected in the specified period.

To

Use this field to define the end of the period relevant for your diagnostic task. When you set the end date, the **Hypervisor Statistics** area is updated with statistics collected in the specified period.

📅

Click the calendar icon or the date in the **From** and **To** fields to display a calendar application and select the appropriate date.

🕒

Click the clock icon or the time in the **From** and **To** fields to display a clock application and select the appropriate time.

Hypervisor Name

This area displays the friendly names of the hypervisor definitions configured in IP Packet Capture.

Hypervisor Statistics

When you select a VMS in the **Hypervisor Name** area, the **Hypervisor Statistics** area displays the statistics files saved in the statistics repository for the selected VMS.

☑

Click the selection icon to select all the hypervisor statistics files displayed in the **Hypervisor Statistics** area.

Enter passphrase for hypervisor statistics encryption

Hypervisor statistics files are downloaded as an encrypted zipped archive protected with a passphrase. In this field, enter a passphrase for statistics file encryption. You can use any passphrase that complies with the passphrase complexity rules configured in IP Packet Capture. The rules specify the minimum and maximum length of a passphrase and the minimum number of characters of each character type that a passphrase must include.

The approximate size of the downloaded archive

When you select the hypervisor statistics files for download, the application displays the approximate size of the archive in this field.

?

Click the info button to see the passphrase complexity rules currently configured in IP Packet Capture. Use this information to choose an acceptable passphrase.

⤓

Click the download button to download the selected statistics files and save them to a selected directory on your computer.

Related Links

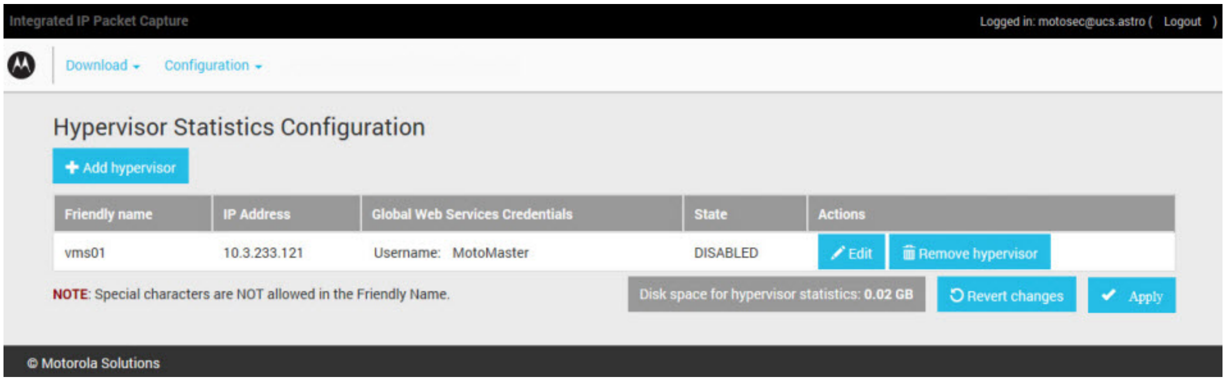
Downloading Hypervisor Statistics Files on page 48

IP Packet Capture User Interface Access on page 55

2.4 Hypervisor Statistics Configuration

The IP Packet Capture application allows you to configure hypervisor definitions for Virtual Management Servers (VMS). Hypervisor definitions are used to collect performance data for the designated VMS. Each hypervisor definition is associated with a VMS hosting IP Packet Capture and the statistics repository disk for storing statistics files. Each VMS is identified by an IP address. To configure a hypervisor definition, you must enter the credentials for a Global Web Services account with the appropriate privileges. Configuration of hypervisor definitions is only available to users that belong to the **infradm** user group.

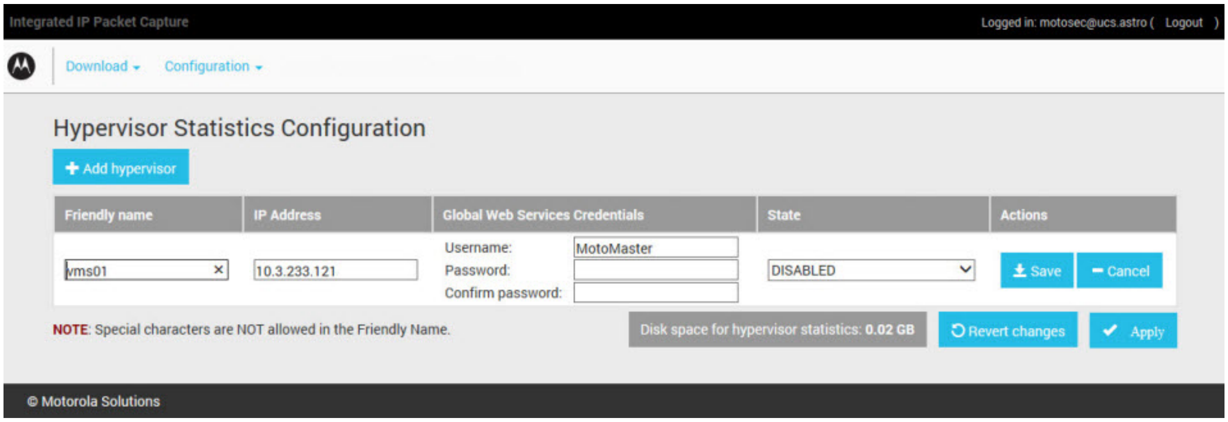
Figure 4: IP Packet Capture – Hypervisor Statistics Configuration – Viewing


Integrated IP Packet Capture
Logged in: motosec@ucs.astro (Logout)
Download ▾
Configuration ▾
Hypervisor Statistics Configuration
+ Add hypervisor
Edit
Remove hypervisor
Disk space for hypervisor statistics: 0.02 GB
Revert changes
✔ Apply
© Motorola Solutions

Friendly name	IP Address	Global Web Services Credentials	State	Actions
vms01	10.3.233.121	Username: MotoMaster	DISABLED	Edit Remove hypervisor

NOTE: Special characters are NOT allowed in the Friendly Name.

Figure 5: IP Packet Capture – Hypervisor Statistics Configuration – Editing



Hypervisor Statistics Configuration

Friendly name	IP Address	Global Web Services Credentials	State	Actions
vms01	10.3.233.121	Username: MotoMaster Password: Confirm password:	DISABLED	Save Cancel

NOTE: Special characters are NOT allowed in the Friendly Name.

Disk space for hypervisor statistics: **0.02 GB**

The **Hypervisor Statistics Configuration** window contains the following fields, columns, and buttons that allow you to add, remove, and edit hypervisor definitions. Access the **Hypervisor Statistics Configuration** window from the **Configuration** menu.

Add hypervisor

When you click this button, a row for a new hypervisor definition appears in the table. The hypervisor definition settings are ready for editing.

Friendly name

In this column, enter an easily recognizable name for a hypervisor definition. Special characters are not allowed in friendly names for hypervisor definitions.

IP Address

In this column, enter the IP address of a Virtual Management Server (VMS) for which you want to collect performance data with this hypervisor definition.

Global Web Services Credentials

In this column, enter the user name and password for a Global Web Services account that is authorized to collect and retrieve hypervisor statistics files.

State

In this column, select an operational state for a hypervisor definition:

ENABLED

An enabled hypervisor definition is active. IP Packet Capture saves statistics files for the designated VMS in the repository.

DISABLED

A disabled hypervisor definition is inactive. Monitoring on the designated VMS is turned off.

DISABLED and DELETE FILES

Select this state to disable a hypervisor definition and remove all statistics files saved in the repository for this hypervisor definition.

Actions

This column contains buttons that allow you to perform the following operations on hypervisor definitions:

Edit

Click this button to modify a hypervisor definition.

Remove hypervisor

Click this button to delete a hypervisor definition and the hypervisor statistics files associated with this definition.

Save
When you finish editing a hypervisor definition, click this button to save the changes. This option saves the new settings as pending changes, but does not affect system operation.

Cancel
Click this button to undo the changes that you have made when editing a hypervisor definition.

Disk space for hypervisor statistics
This area provides the information about the space available in the repository disk for storing hypervisor statistics files.

Revert changes
Click this button to undo the changes that you have made to the hypervisor definitions since the last time you clicked **Apply**.

Apply
Click this button to update the system operation with the pending changes that you have made to the hypervisor definitions.

Related Links

Adding Hypervisor Definitions on page 48
Editing Hypervisor Definitions on page 49
Enabling Hypervisor Definitions on page 50
Disabling Hypervisor Definitions on page 51
Removing Hypervisor Definitions on page 51
Deleting Hypervisor Statistics Files on page 52
IP Packet Capture User Interface Access on page 55

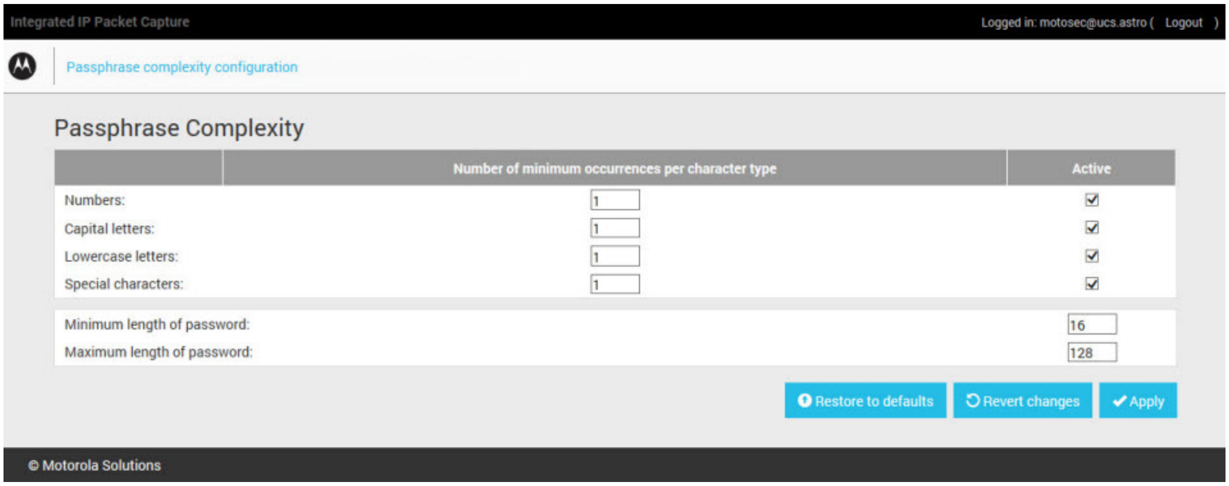
2.5 Passphrase Complexity Configuration

Packet capture files and hypervisor statistics files are downloaded in an encrypted zipped archive protected with a passphrase. When you download packet capture files and hypervisor statistics files from IP Packet Capture, you must enter a passphrase for encryption. To decrypt the downloaded archive, enter the same passphrase. Each passphrase must meet the complexity rules specified in the IP Packet Capture application. Only users that belong to the **secadm** user group can access the passphrase complexity configuration and change the complexity rules.

Passphrases can include the following character types:

- Numbers: 0-9
- Capital letters: A-Z
- Lowercase letters: a-z
- Special characters: ` ~ ! @ # $ % ^ & * ( ) _ - + = [ ] { } ; : ' " \ | , < . > / ?

Figure 6: IP Packet Capture – Passphrase Complexity Configuration


Integrated IP Packet Capture
Logged in: motosec@ucs.astro (Logout)
Passphrase complexity configuration
Restore to defaults
Revert changes
Apply
© Motorola Solutions

Passphrase Complexity

	Number of minimum occurrences per character type	Active
Numbers:	1	☑
Capital letters:	1	☑
Lowercase letters:	1	☑
Special characters:	1	☑

Minimum length of password:	16
Maximum length of password:	128

The **Passphrase complexity configuration** window contains the following fields, columns, check boxes, and buttons for easy configuration of the passphrase complexity rules.

Number of minimum occurrences per character type

This column contains a field for each character type that can be used in a passphrase. In the field for each character type that a passphrase should include, enter the minimum number of characters to be used.

Active

This column contains a check box for each character type that can be used in a passphrase. Selecting a check box for a particular character type means that a passphrase must include characters of this type and their number must meet the specified minimum requirement.

Minimum length of password

In this field, enter the minimum number of characters to be used in a passphrase.

Maximum length of password

In this field, enter the maximum number of characters to be used in a passphrase.

Restore to defaults

Click this button to restore the default values for the passphrase complexity settings.

Revert changes

Click this button to undo the changes that you have made to the passphrase complexity settings since the last time you clicked **Apply**.

Apply

Click this button to update the system operation with your configuration changes.

Related Links

Configuring Passphrase Complexity on page 52
Restoring Default Passphrase Complexity on page 53
IP Packet Capture User Interface Access on page 55

This page intentionally left blank.

Chapter 3

IP Packet Capture User Interface Operations

This chapter describes the operations that you can perform in the IP Packet Capture user interface (UI). These operations are related to the three functions of the application: packet capture files and hypervisor statistics files download, configurations of packet captures and hypervisor definitions, and passphrase complexity settings.

- Logging on to the IP Packet Capture user interface from a Web browser
- Downloading packet capture files for a selected device from a specified monitoring period
- Downloading hypervisor statistics files for a designated Virtual Management Server (VMS) from a specified monitoring period
- Adding, editing, and deleting packet captures and hypervisor definitions
- Enabling and disabling packet captures and hypervisor definitions
- Removing packet capture files and hypervisor statistics files
- Configuring the complexity rules for passphrases used to encrypt packet capture files and hypervisor statistics files
- Restoring default values for the passphrase complexity rules

3.1

Logging On to the IP Packet Capture UI

You can access the IP Packet Capture user interface (UI) through a Web browser by establishing a connection with the application on the Virtual Management Server (VMS). Logging on to IP Packet Capture requires password-based authentication. Only one user can be logged on to an instance of IP Packet Capture at a time. After 15 minutes of inactivity, a user is logged off automatically.

Procedure:

1 On a client device, open a Web browser.

2 In the browser address field, enter the appropriate address:

If…	Then…
If you are using a DNS-capable access point,	perform one of the following actions: • For IP Packet Capture in a zone core, enter: `https://z00<X>ipcap0<Y>.zone<X>` • For IP Packet Capture at a Tsub prime site, enter: `https://z00<X>s<PPP>ipcap01.site<P>.zone<X>`
If you are using a non-DNS-capable access point,	perform one of the following actions: • For IPCAP01 (on VMS01 in a zone core), enter: 10.***<X>***.233.218 • For IPCAP01 (on VMS01 in a Tsub prime site), enter: 10.***<X+100>***.***<P>***.121 • For IPCAP02 (on VMS02), enter: 10.***<X>***.233.219

If…	Then…
	- For IPCAP03 (on VMS09), enter: 10.*<X>*.237.218 - For IPCAP04 (on VMS10), enter: 10.*<X>*.237.219

where:

<X> is the number of the zone in which the VMS is located. The possible values are: 1–7.

<Y> is the IP Packet Capture instance number associated with the VMS number. The possible values are: 1 on VMS01, 2 on VMS02, 3 on VMS09, and 4 on VMS10.

<PPP> is the 3-digit zero-padded number of the Tsub prime site. The possible values are: 001-064.

<P> is the number of the Tsub prime site. The possible values are: 1-64.

NOTICE:
The VMS number depends on the location of the server in a core or subsystem of a specific type:

- VMS01: non-redundant cores (K1, L1, and M1 cores), redundant cores (K2, L2, M2, M3), Dynamic System Resilience (DSR) primary cores, and Trunking Subsystem (Tsub) prime sites
- VMS02: redundant cores (K2, L2, M2, M3) and redundant DSR primary cores
- VMS09: DSR backup cores
- VMS10: redundant DSR backup cores

3 On the IP Packet Capture login page, enter your user name and password:

NOTICE: For an L or M core, use the credentials of a domain user registered in Active Directory (AD). For a K core, use the credentials of a local user.

- To access the **Download** menu for packet capture files and hypervisor statistics files, use an account that belongs to the **confgaud** or **infradm** user group.
- To access the **Configuration** menu for packet captures and hypervisor definitions, use an account that belongs to the **infradm** user group.
- To access the **Passphrase complexity configuration** tab, use an account that belongs to the **secadm** user group.

4 Click **Log in**.

Related Links

Logging Off the IP Packet Capture UI on page 43
Downloading Packet Capture Files on page 43
Adding Packet Captures on page 44
Editing Packet Captures on page 45
Enabling Packet Captures on page 46
Disabling Packet Captures on page 46
Removing Packet Captures on page 47
Deleting Packet Capture Files on page 47
Downloading Hypervisor Statistics Files on page 48
Adding Hypervisor Definitions on page 48
Editing Hypervisor Definitions on page 49
Enabling Hypervisor Definitions on page 50
Disabling Hypervisor Definitions on page 51
Removing Hypervisor Definitions on page 51

Deleting Hypervisor Statistics Files on page 52
Configuring Passphrase Complexity on page 52
Restoring Default Passphrase Complexity on page 53
IP Packet Capture User Interface Access on page 55
Entering the Global Web Services Credentials for the Default Hypervisor Definition on page 74

3.2 Logging Off the IP Packet Capture UI

Logging off the IP Packet Capture user interface (UI) is a one-click operation. After 15 minutes of inactivity, a user is logged off automatically.

Procedure:

In the top right corner of the **Integrated IP Packet Capture** window, click **Logout**.

The IP Packet Capture login page appears.

Related Links

Logging On to the IP Packet Capture UI on page 41

3.3 Downloading Packet Capture Files

IP Packet Capture monitors traffic on the connected capture points. The application captures transactions between network elements in the form of IP packets and saves the packets as `.pcap` capture files in the repository. You can download the packet capture files for a designated device from a specified period. The selected packet captures files are retrieved from the packet capture repository and saved to the computer that you are using to access IP Packet Capture as an encrypted zipped archive protected with a passphrase.

NOTICE: To access files in the downloaded archive, use WinZip or 7-Zip. Windows Explorer does not support encrypted archives and cannot be used to access the files.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **confgaud** or **infradm** user group.
2. From the **Download** menu, select **Capture files**.
3. In the **Capture Files Download** window, display packet capture files from the period relevant for your diagnostic task.
   a. In the **From** field, set the start of the period.
   b. In the **To** field, set the end of the period.

   The **Captures** area shows the devices monitored by IP Packet Capture. The **Capture Files** area displays the names of packet capture files saved in the repository for each device.
4. In the **Captures** area, select the packet capture for which you want to download the packet capture files.
5. In the **Capture Files** area, select the packet capture files that you want to download.
6. In the **Enter a passphrase for capture encryption** field, enter a password that is compliant with the passphrase complexity rules.

   To view the passphrase complexity rules, click the info button ?.

7. Click the **Download** button ⤓ and save the selected packet capture files to the selected directory on your computer.

Related Links

Logging On to the IP Packet Capture UI on page 41
Capture Files Download on page 31
Recovering IP Packet Capture After a Failure on page 79

3.4 Adding Packet Captures

To monitor traffic on a device, define a packet capture for that device in the IP Packet Capture application.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.
2. From the **Configuration** menu, select **Capture definition**.
3. In the **Capture Configuration** window, click **Add capture**.

   A row for the new packet capture appears in the table.

4. In the **Friendly name** column, enter an easily recognizable name for the packet capture. Do not use spaces.

   Step example: Core_LAN_Switch_1

5. In the **Disk share** column, enter a percentage of the disk space to be assigned for packet capture files from this packet capture.

   NOTICE: The total disk share configured for all the captures defined in the application must not exceed 100%. If the total disk share is greater than 100%, the application displays a warning. Ensure that the disk share is distributed within the limit of 100% by editing other captures if necessary.

   For the disk share percentages recommended for the capture connections established to the IP Packet Capture that you are configuring, see Disk Share Percentages for Capture Interfaces on page 107.

6. In the **Network interface** column, select a capture interface to be used for this packet capture.
7. To enable the packet capture, in the **State** column, select **ENABLED**.
8. In the **Actions** column, click **Save**.

   The new packet capture is saved and added to the list.

9. To update the system operation with the pending changes, click **Apply**.

Postrequisites: In the Unified Event Manager (UEM), check if the packet capture definition reports any faults. See Packet Capture State Transition Traps for UEM on page 83 and IP Packet Capture Alarm Traps for UEM on page 86.

Related Links

Logging On to the IP Packet Capture UI on page 41
Capture Configuration on page 32
Configuring IP Packet Capture to Capture from a Device on page 103

3.5 Editing Packet Captures

IP Packet Capture provides editing options for packet captures configured in the application.

By using the **Edit** option, you can make the following changes to a packet capture:

- Change the name of the packet capture.
- Assign a different percentage of the disk space for storing packet capture files from the device designated in this packet capture.
- Select a different network interface (connected to another capture point) to be used by this packet capture.
- Disable or enable the packet capture.
- Clear the packet capture files from the packet capture saved in the packet capture repository.
- Remove the packet capture.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.
2. From the **Configuration** menu, select **Capture definition**.
3. In the **Actions** column for the packet capture that you want to modify, click **Edit**.
4. To change the name of the packet capture, in the **Friendly name** column, enter a new name. Do not use spaces.
5. To change the percentage of the disk space assigned for packet capture files from this capture, in the **Disk share** column, enter a different percentage.

   NOTICE: The total disk share configured for all the captures defined in the application must not exceed 100%. If the total disk share is greater than 100%, the application displays a warning. Ensure that the disk share is distributed within the limit of 100% by editing other captures if necessary.

   For the disk share percentages recommended for the capture connections established to the IP Packet Capture that you are configuring, see Disk Share Percentages for Capture Interfaces on page 107.
6. To change the capture interface to be used by this packet capture, in the **Network interface** column, select a different capture interface.

   NOTICE: Each capture interface is connected to a network element. Selecting a different capture interface for a packet capture means that the packet capture will monitor the connected device.
7. To change the operational state of this packet capture, in the **State** column, make one of the following selections:
   - To start monitoring the traffic on the device designated in this packet capture, select **ENABLED**.
   - To stop monitoring the traffic on the device designated in this packet capture, select **DISABLED**.
   - To disable the capture and clear all the capture files saved in the repository for this packet capture, select **DISABLED and DELETE FILES**.
8. To save the changes to the packet capture configuration, in the **Actions** column, click **Save**.
9. Optional: To delete the packet capture, in the **Actions** column, click **Remove definition**.
10. To update the system operation with the pending changes, click **Apply**.

Related Links

Logging On to the IP Packet Capture UI on page 41
Capture Configuration on page 32

3.6

Enabling Packet Captures

For IP Packet Capture to start monitoring traffic on a device, enable the packet capture for that device defined in the application.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.
2. From the **Configuration** menu, select **Capture definition**.
3. In the **Actions** column for the packet capture that you want to enable, click **Edit**.
4. In the **State** column, select **ENABLED**.
5. In the **Actions** column, click **Save**.

   The changes to the packet capture configuration are saved.
6. To update the system operation with the pending changes, click **Apply**.

Related Links

Logging On to the IP Packet Capture UI on page 41
Capture Configuration on page 32

3.7

Disabling Packet Captures

For IP Packet Capture to stop monitoring traffic on a device, disable the packet capture for that device defined in the application. Disabling a packet capture is required when you want to change the configuration of a packet capture. During a restart or shutdown, the packet captures are disabled automatically.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.
2. From the **Configuration** menu, select **Capture definition**.
3. In the **Actions** column for the packet capture that you want to disable, click **Edit**.
4. In the **State** column, select **DISABLED**.
5. In the **Actions** column, click **Save**.

   The changes to the packet capture configuration are saved.
6. To update the system operation with the pending changes, click **Apply**.

Related Links

Logging On to the IP Packet Capture UI on page 41
Capture Configuration on page 32

3.8 Removing Packet Captures

The IP Packet Capture user interface allows you to remove the packet captures configured in the application. This operation removes the selected packet capture definition and the packet capture files saved for that definition.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.
2. From the **Configuration** menu, select **Capture definition**.
3. In the **Actions** column for the packet capture definition that you want to remove, click **Remove definition**.
4. When a warning appears, asking you to confirm or cancel the action, perform one of the following steps:
   - To confirm the action, click **Remove**.

     The capture definition is removed from the **Capture Configuration** window, but left as a pending change.
   - To cancel the action, click **Cancel**.

     The **Capture Configuration** window remains unmodified. The procedure ends.
5. To update the system operation with the pending changes, click **Apply**.

The packet capture definition is removed. The packet capture files associated with that definition are deleted from the packet capture files repository.

Related Links

Logging On to the IP Packet Capture UI on page 41
Capture Configuration on page 32

3.9 Deleting Packet Capture Files

To remove the packet capture files saved by IP Packet Capture for a device, change the state of the packet capture for that device to **DISABLED and DELETE FILES**.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.
2. From the **Configuration** menu, select **Capture definition**.
3. In the **Actions** column for the packet capture that you want to modify, click **Edit**.
4. In the **State** column, select **DISABLED and DELETE FILES**.
5. In the **Actions** column, click **Save**.

   The changes to the packet capture configuration are saved.
6. To update the system operation with the pending changes, click **Apply**.

Related Links

Logging On to the IP Packet Capture UI on page 41
Capture Configuration on page 32

3.10 Downloading Hypervisor Statistics Files

Hypervisor statistics are performance data collected by IP Packet Capture for the Virtual Management Server (VMS) hosting the application. You can download the hypervisor statistics files for a selected VMS from a specified period. The statistics files are retrieved from the repository and saved to the computer that you are using to access IP Packet Capture as an encrypted zipped archive protected with a passphrase.

NOTICE: To access files in the downloaded archive, use WinZip or 7-Zip. Windows Explorer does not support encrypted archives and cannot be used to access the files.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **confgaud** or **infradm** user group.
2. From the **Download** menu, select **Hypervisor statistics**.
3. In the **Hypervisor Statistics Download** window, display statistics files from the period relevant for your diagnostic task.
   a. In the **From** field, set the start of the period.
   b. In the **To** field, set the end of the period.

   The **Hypervisor Name** area shows the VMS monitored by IP Packet Capture for performance statistics. The **Hypervisor Statistics** area displays the statistics files saved in the repository for the VMS.
4. In the **Hypervisor Name** area, select the VMS for which you want to download the hypervisor statistics files.
5. In the **Hypervisor Statistics** area, select the statistics files that you want to download.
6. In the **Enter a passphrase for hypervisor statistics encryption** field, enter a password that is compliant with the passphrase complexity rules.

   To view the passphrase complexity rules, click the info button ?.
7. Click the **Download** button ⭳ and save the selected statistics files to the selected directory on your computer.

Related Links

Logging On to the IP Packet Capture UI on page 41
Hypervisor Statistics Download on page 34
Recovering IP Packet Capture After a Failure on page 79

3.11 Adding Hypervisor Definitions

To gather statistics for a Virtual Management Server (VMS), configure a hypervisor definition in the IP Packet Capture application. A hypervisor definition is a mapping of a VMS to the statistics repository that allows you to collect performance data for the server.

Prerequisites: From your system administrator, obtain the credentials for the Global Web Services account.

Procedure:

1 Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.

2 From the **Configuration** menu, select **Hypervisor statistics**.

3 In the **Hypervisor Statistics Configuration** window, click **Add hypervisor**.

A row for the new hypervisor definition appears in the table.

4 In the **Friendly name** column, enter an easily recognizable name for the hypervisor definition.

A hypervisor friendly name must be in the following format: vms***<xx>***

where ***<xx>*** is a number.

Do not use special characters.

5 In the **IP Address** column, enter the IP address of the VMS.

NOTICE: For IP addresses of the Virtual Management Servers in the zone, see the IP Plan for your system.

6 In the **Global Web Services Credentials** column, enter the user name and password for a Global Web Services account.

7 To enable the hypervisor definition, in the **State** column, select **ENABLED**.

8 In the **Actions** column, click **Save**.

The new hypervisor definition is saved and added to the list.

9 To update the system operation with the pending changes, click **Apply**.

Postrequisites: In the Unified Event Manager (UEM), check if the hypervisor definition reports any faults. See Hypervisor Statistics State Transition Traps for UEM on page 85 and IP Packet Capture Alarm Traps for UEM on page 86.

Related Links

Logging On to the IP Packet Capture UI on page 41
Hypervisor Statistics Configuration on page 36
Adding the IP Packet Capture Feature to the System on page 93

3.12 Editing Hypervisor Definitions

IP Packet Capture provides editing options for hypervisor definitions configured in the application.

By using the **Edit** option, you can make the following changes to a hypervisor definition:

- Change the name of the hypervisor definition.
- Enter a different IP address for the Virtual Management Server (VMS) monitored by the hypervisor definition.
- Provide the credentials for the Global Web Services account that is authorized to configure hypervisor definitions and retrieve hypervisor statistics files.
- Disable or enable the hypervisor definition.
- Remove the statistics saved for the VMS designated in the hypervisor definition.

- Delete the hypervisor definition.

Procedure:

1 Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.

2 From the **Configuration** menu, select **Hypervisor statistics**.

3 In the **Actions** column for the hypervisor definition that you want to modify, click **Edit**.

4 To change the name of the hypervisor definition, in the **Friendly name** column, enter a new name.

   A hypervisor friendly name must be in the following format: vms***<xx>***

   where ***<xx>*** is a number.

   Do not use special characters.

5 To change the IP address, in the **IP Address** column, enter a different IP address.

   NOTICE: For IP addresses of the Virtual Management Servers in the zone, see the IP Plan for your system.

6 To change the credentials, in the **Global Web Services Credentials** column, enter the user name and password for the Global Web Services account.

7 To change the operational state of this hypervisor definition, in the **State** column, make one of the following selections:

   - To start collecting statistics for the VMS designated in this hypervisor definition, select **ENABLED**.
   - To stop collecting statistics for the VMS designated in this hypervisor definition, select **DISABLED**.
   - To disable the hypervisor definition and remove all the statistics files saved in the repository for this hypervisor definition, select **DISABLED and DELETE FILES**.

8 To save the changes to the hypervisor definitions, in the **Actions** column, click **Save**.

9 Optional: To delete the hypervisor definition, in the **Actions** column, click **Remove hypervisor**.

10 To update the system operation with the pending changes, click **Apply**.

Related Links

Logging On to the IP Packet Capture UI on page 41
Hypervisor Statistics Configuration on page 36
Entering the Global Web Services Credentials for the Default Hypervisor Definition on page 74

3.13 Enabling Hypervisor Definitions

For IP Packet Capture to start gathering hypervisor statistics from a Virtual Management Server (VMS), enable the hypervisor definition for that VMS configured in the application.

Procedure:

1 Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.

2 From the **Configuration** menu, select **Hypervisor statistics**.

3 In the **Actions** column for the hypervisor definition that you want to enable, click **Edit**.

4 In the **State** column, select **ENABLED**.

5. In the **Actions** column, click **Save**.

   The changes to the hypervisor definition are saved.

6. To update the system operation with the pending changes, click **Apply**.

Related Links

Logging On to the IP Packet Capture UI on page 41
Hypervisor Statistics Configuration on page 36
Entering the Global Web Services Credentials for the Default Hypervisor Definition on page 74

3.14 Disabling Hypervisor Definitions

For IP Packet Capture to stop gathering statistics for a Virtual Management Server (VMS), disable the hypervisor definition for that VMS configured in the application. Disabling a hypervisor definition is required when you want to change the configuration of a hypervisor definition. During a restart or shutdown, the hypervisor definitions are disabled automatically.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.
2. From the **Configuration** menu, select **Hypervisor statistics**.
3. In the **Actions** column for the hypervisor definition that you want to disable, click **Edit**.
4. In the **State** column, select **DISABLED**.
5. In the **Actions** column, click **Save**.

   The changes to the hypervisor definition are saved.

6. To update the system operation with the pending changes, click **Apply**.

Related Links

Logging On to the IP Packet Capture UI on page 41
Hypervisor Statistics Configuration on page 36

3.15 Removing Hypervisor Definitions

The IP Packet Capture user interface allows you to remove the hypervisor definitions configured in the application. This operation removes the selected hypervisor definition and the hypervisor statistics files saved for that definition.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.
2. From the **Configuration** menu, select **Hypervisor statistics**.
3. In the **Actions** column for the hypervisor definition that you want to remove, click **Remove hypervisor**.
4. When a warning appears, asking you to confirm or cancel the action, perform one of the following steps:
   - To confirm the action, click **Remove**.

The hypervisor definition is removed from the **Hypervisor Statistics** window, but left as a pending change.

- To cancel the action, click **Cancel**.

  The **Hypervisor Statistics** window remains unmodified. The procedure ends.

5. To update the system operation with the pending changes, click **Apply**.

The hypervisor definition is removed. The hypervisor statistics files associated with that definition are deleted from the statistics repository.

Related Links

Logging On to the IP Packet Capture UI on page 41
Hypervisor Statistics Configuration on page 36

3.16
Deleting Hypervisor Statistics Files

To remove the statistics saved by IP Packet Capture for a Virtual Management Server (VMS), change the state of the hypervisor definition for that VMS to **DISABLED and DELETE FILES**.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.
2. From the **Configuration** menu, select **Hypervisor statistics**.
3. In the **Actions** column for the hypervisor definition that you want to modify, click **Edit**.
4. In the **State** column, select **DISABLED and DELETE FILES**.
5. In the **Actions** column, click **Save**.

   The changes to the hypervisor definition are saved.

6. To update the system operation with the pending changes, click **Apply**.

Related Links

Logging On to the IP Packet Capture UI on page 41
Hypervisor Statistics Configuration on page 36

3.17
Configuring Passphrase Complexity

When you download packet capture files and hypervisor statistics files from IP Packet Capture, you must enter a passphrase for encryption. The passphrase must comply with the passphrase complexity rules configured in the IP Packet Capture application.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **secadm** user group.

   The **Passphrase complexity configuration** window appears.

2. For each character type, specify the minimum number of characters that a passphrase must include:

   a. In the **Numbers** field, enter the minimum number of numbers.

   b. In the **Capital letters** field, enter the minimum number of capital letters.

c In the **Lowercase letters** field, enter the minimum number of lowercase letters.

d In the **Special characters** field, enter the minimum number of special characters.

The following special characters are allowed: ` ~ ! @ # $ % ^ & * ( ) _ - + = [ ] { } ; : ' " \ | , < . > / ?

3 In the **Active** column, select the box for each character type that a passphrase must include.

4 In the field for **Minimum length of password**, enter the minimum number of characters to be used in a passphrase.

5 In the field for **Maximum length of password**, enter the maximum number of characters to be used in a passphrase.

6 To update the system operation with the pending changes, click **Apply**.

7 Optional: To restore the default settings for passphrase complexity, click **Restore to defaults**.

Related Links

Logging On to the IP Packet Capture UI on page 41
Passphrase Complexity Configuration on page 38

3.18 Restoring Default Passphrase Complexity

You can restore the passphrase complexity rules from custom settings to default settings at any time.

Procedure:

1 Log on to the IP Packet Capture user interface using an account that belongs to the **secadm** user group.

The **Passphrase complexity configuration** window appears.

2 Click **Restore to defaults**.

The default values of the passphrase complexity settings are restored.

3 To update the system operation with the pending changes, click **Apply**.

Related Links

Logging On to the IP Packet Capture UI on page 41
Passphrase Complexity Configuration on page 38

This page intentionally left blank.

Chapter 4

IP Packet Capture User Interface Access and Users

This chapter provides information about creating, modifying, and deleting user accounts that you can use to access IP Packet Capture. In L and M cores, authentication requires the use of domain user accounts registered in Active Directory. In K cores, local user authentication is used.

4.1 IP Packet Capture User Interface Access

To establish a connection to the IP Packet Capture user interface, you need a client with a Web browser and a user account with the appropriate access rights. Depending on the type of core used in your system (K, L, or M core), different types of clients and user accounts are available.

Access by Devices

In L core and M core systems, you can access IP Packet Capture from the following devices:

- Network Management (NM) Client
- Service computer/laptop

NOTICE:
IP Packet Capture located at a Trunking Subsystem (Tsub) prime site: When there is no connectivity to the zone core, you can only access the IP Packet Capture user interface from the following devices and locations:

- From a service laptop within the Tsub prime site
- From an NM Client at an NM/Dispatch subsite

In K core systems, you can access IP Packet Capture from the following devices, listed in the order of preference:

1. Service computer or customer owned laptop
2. Unified Event Manager (UEM) PC client
3. Configuration Manager
4. Console PC not being used for dispatch

To establish a connection to IP Packet Capture, the client must have the following software installed:

- Microsoft Windows 7 (with Windows 7 Service Pack 1) or Windows 10
- Web browser

NOTICE:
If you are using Internet Explorer, ensure that the version is Internet Explorer 11 or greater with Transport Layer Security (TLS) 1.2 enabled.

If you are using Firefox, logins may fail. If updating Firefox does not solve this problem, use an alternate browser.

Access by User Type

Depending on the type of zone core used in your system, use the following types of user accounts to access IP Packet Capture.

Domain user registered in Active Directory (AD)
In L core and M core systems, access IP Packet Capture with the credentials of an Active Directory user.

Local user
In K core systems, access IP Packet Capture with the credentials of a local user.

Access by Group Membership

Access to the three main areas of IP Packet Capture is restricted to users that belong to a group with the appropriate privileges.

confgaud
This group membership provides access to the **Download** menu for packet capture files and hypervisor statistics files.

infradm
This group membership provides access to the **Download** and **Configuration** menus for packet captures and hypervisor definitions.

secadm
This group membership provides access to the **Passphrase complexity rules** menu.

NOTICE: After system installation, change the default passwords for the default local user accounts.

Related Links

Capture Files Download on page 31
Capture Configuration on page 32
Hypervisor Statistics Download on page 34
Hypervisor Statistics Configuration on page 36
Passphrase Complexity Configuration on page 38
Logging On to the IP Packet Capture UI on page 41
Active Directory Users on page 56
Local Users on page 57

4.2 Active Directory Users

In L and M cores, accessing the IP Packet Capture user interface requires Active Directory user authentication. Depending on their group membership, Active Directory user accounts provide access to different functions of IP Packet Capture: packet capture files and hypervisor statistics files download, configuration of packet captures and hypervisor definitions, and passphrase complexity settings. To access IP Packet Capture, use an existing account or create an account with the appropriate group membership.

See the *Authentication Services* manual for information about the configuration of user accounts in Active Directory. The “Active Directory Server Operation” chapter provides guidelines for the following operations:

- Creating Active Directory user accounts
- Adding user accounts to an Active Directory domain
- Enabling, disabling, and resetting user accounts in Active Directory
- Modifying user account attributes for accessing Unix-based devices, such as IP Packet Capture
- Assigning group membership to a user account

Access by Group Membership

Access to the three main areas of IP Packet Capture is restricted to users that belong to a group with the appropriate privileges.

confgaud
This group membership provides access to the **Download** menu for packet capture files and hypervisor statistics files.

infradm
This group membership provides access to the **Download** and **Configuration** menus for packet captures and hypervisor definitions.

secadm
This group membership provides access to the **Passphrase complexity rules** menu.

NOTICE: After system installation, change the default passwords for the default local user accounts.

Related Links

IP Packet Capture User Interface Access on page 55

4.3

Local Users

In K cores, accessing the IP Packet Capture user interface requires local user authentication. To start using IP Packet Capture, use one of the default local user accounts with the appropriate group membership.

The following default user accounts with the rights to access the IP Packet Capture UI are available in K core systems:

ipcapusr
Belongs to the **confgaud** user group. This group membership provides access to the **Download** menu for packet capture files and hypervisor statistics files.

infrusr
Belongs to the **infradm** user group. This group membership provides access to the **Download** and **Configuration** menus for packet captures and hypervisor definitions.

secusr
Belongs to the **secadm** user group. This group membership provides access to the **Passphrase complexity rules** menu.

NOTICE: After system installation, change the default passwords for the default local user accounts.

Related Links

Changing Passwords for Local Users on page 57
IP Packet Capture User Interface Access on page 55

4.3.1

Changing Passwords for Local Users

Perform this procedure to change the password on a default local user account in a K core system. Default local user accounts are: ipcapusr, infrausr, and secusr.

NOTICE: After system installation, change the default passwords for the default local user accounts.

Prerequisites:

Review the restrictions on user names for Linux-based virtual machines. See “User/Group Name Restrictions” in the *Authentication Services* manual.

Procedure:

1. Log on to the IP Packet Capture virtual machine as root.
2. At the prompt, enter: `passwd` ***`<default local user>`***
3. Enter the new password.
4. Enter the new password again.

Related Links

Logging On to the IP Packet Capture Virtual Machine on page 58
Local Users on page 57

4.3.2 Logging On to the IP Packet Capture Virtual Machine

The IP Packet Capture virtual machine resides on the Virtual Management Server (VMS) with the ESXi operating system. You can log on to the common Unix administration menu of the IP Packet Capture virtual machine on the VMS by using the VMware vSphere Client.

Prerequisites: Obtain the following information:

- IP address of the VMS hosting the IP Packet Capture virtual machine
- Password for the root user account

Procedure:

1. From a Windows-based device, launch the **VMware vSphere Client**.
2. Log on to the VMS hosting the IP Packet Capture virtual machine with local administrator root account credentials.

   The **vSphere Client Inventory** window appears.
3. On the pane on the left, right-click the IP Packet Capture virtual machine and click **Open Console**.
4. In the **Console** tab, log on to the IP Packet Capture virtual machine with the appropriate user account credentials.

Related Links

Changing Passwords for Local Users on page 57

Chapter 5

IP Packet Capture Installation

This chapter details the installation process for the IP Packet Capture application on a Virtual Management Server (VMS) in an ASTRO® 25 system zone core.

For information on installing the Virtual Management Server (VMS) hardware and software, see the *Virtual Management Server Hardware* and *Virtual Management Server Software* manuals.

For information on making the physical capture/monitor connections, see IP Packet Capture Connections on page 103.

5.1

Installing IP Packet Capture

Install the IP Packet Capture application in every zone on the following Virtual Management Servers (VMS) if present: VMS01, VMS02, VMS09, and VMS10. The VMS must be an HP DL380 Gen9 server or later version.

NOTICE:
The VMS number depends on the location of the server in a core or subsystem of a specific type:

- VMS01: non-redundant cores (K1, L1, and M1 cores), redundant cores (K2, L2, M2, M3), Dynamic System Resilience (DSR) primary cores, and Trunking Subsystem (Tsub) prime sites
- VMS02: redundant cores (K2, L2, M2, M3) and redundant DSR primary cores
- VMS09: DSR backup cores
- VMS10: redundant DSR backup cores

Prerequisites:
Before installing a virtual machine on a VMS host, satisfy all appropriate requirements and review all appropriate installation considerations.

For more information, see the *Virtual Management Server Hardware* and *Virtual Management Server Software* manuals.

Obtain the *Unix Supplemental Configuration* manual.

Process:

1. Log on to the VMS host on which you want to install IP Packet Capture.

   See Logging On to the VMS Host of the IP Packet Capture Virtual Machine on page 60.
2. Import the IP Packet Capture virtual machine.

   See Importing the Virtual Machine on page 61.
3. **Only for systems with vCenter installed:** Configure VMware vCenter for the IP Packet Capture virtual machine.

   See Configuring the vCenter for the Newly Deployed VM on page 63.
4. Move the IP Packet Capture virtual machine to the correct place in the startup and shutdown order.

   See Setting the Virtual Machine Startup and Shutdown Order on page 64.
5. Configure the security settings for the IP Packet Capture virtual machine.

See Applying Supplemental Configuration to Virtual Machines on page 65.

6 Add a third virtual hard disk to the IP Packet Capture virtual machine.

See Adding a Third Virtual Hard Disk to IP Packet Capture on page 67.

7 Connect and power on the IP Packet Capture virtual machine.

See Connecting and Powering On the IP Packet Capture Virtual Machine on page 68.

8 Configure the time zone on the IP Packet Capture virtual machine.

See Configuring the Time Zone on Linux Servers on page 69.

9 Set the identity for the IP Packet Capture virtual machine.

See Setting the Identity for the IP Packet Capture Virtual Machine on page 70.

10 **L and M cores only:** Join the IP Packet Capture virtual machine to an Active Directory domain.

See Joining a Virtual Machine to the Domain on page 72.

11 Apply the platform patch to the IP Packet Capture virtual machine.

See Applying Platform Patch on page 72.

12 If applicable, perform Linux OS patching on the IP Packet Capture virtual machine.

Installation procedures for the MOTOPATCH are available at: https://sites.google.com/a/motorolasolutions.com/sus-motopatch/

If you cannot open the link, this means that MOTOPATCH for RHEL 7 is not available yet. Go to step 13.

IMPORTANT:
The Linux MOTOPATCH CD must be applied after all applications are installed.

Patches must be installed on a regular basis and for each fresh installation.

13 Perform supplemental configuration procedures on the IP Packet Capture virtual machine, as required by your organization. See the *Unix Supplemental Configuration* manual.

14 Change the root password for the IP Packet Capture virtual machine.

See “Changing Root Account Passwords for Linux-Based Devices” in the *Unix Supplemental Configuration* manual.

15 Enter the Global Web Services Credentials for the default hypervisor definition and enable the definition.

See Entering the Global Web Services Credentials for the Default Hypervisor Definition on page 74.

Related Links

Recovering IP Packet Capture After a Failure on page 79
Adding the IP Packet Capture Feature to the System on page 93

5.1.1 Logging On to the VMS Host of the IP Packet Capture Virtual Machine

The IP Packet Capture virtual machine is installed on a Virtual Management Server (VMS) with the ESXi operating system. You can log on to the VMS from the VMware vSphere Client.

Prerequisites: Obtain the following information:

- IP address of the VMS hosting the IP Packet Capture virtual machine.
- Password for the root user account

Procedure:

1. From a Windows-based device, launch the **VMware vSphere Client**.
2. Log on to the VMS as the root user:
   a. In the **IP address / Name** field, enter the IP address of the VMS.
   b. In the **User name** field, enter: `root`
   c. In the **Password** field, enter the password for the root user account.

   The **vSphere Client Inventory** window appears.

Related Links

Installing IP Packet Capture on page 59

5.1.2
Importing the Virtual Machine

Importing a virtual machine may take approximately an hour, depending on network traffic and disk usage.

Prerequisites: Obtain the following media and information:

- *IP Packet Capture DVD*
- IP address of the ESXi-based server (Virtual Management Server host)
- ESXi-based server root account password
- Hostname for the device that you are importing
- Zone network for the virtual machine

Procedure:

1. From a Windows-based device, launch the VMware vSphere Client.

   A desktop shortcut was created during installation.

   A dialog box appears prompting for an IP address, user name, and password.
2. Log on to the server by entering the IP address of the ESXi server, `root` in the user name field, and the appropriate password in the password field.
3. In the **vSphere Client Inventory** window, perform one of the following actions:
   - If you are installing from the DVD, insert the media listed in the prerequisites in the DVD drive of the device where the vSphere Client resides.
   - If you are not installing from the DVD, determine the location of the following file: ***<IP_Packet_Capture>***`.ovf`
4. Select **File** → **Deploy OVF Template**.
5. In the **Deploy OVF Template – Source** window, click **Browse**.

   A window displays file directories.
6. Perform the following actions:
   a. Navigate to the file location.
   b. Select the file:

      <IP_Packet_Capture>`.ovf`
   c. Open the file.

- **d** Click **Next**.

7 In the **Deploy OVF Template – OVF Template Details** window, click **Next**.

8 In the **Deploy OVF Template – Name and Location** window, perform the following actions:

- **a** In the **Name** field, enter the appropriate host name.
  - For IP Packet Capture in a zone core, enter: `z00`***<X>***`ipcap0`***<Y>***`.zone`***<X>***
  - For IP Packet Capture at a Tsub prime site, enter: `z00`***<X>***`s`***<PPP>***`ipcap01.site`***<P>***`.zone`***<X>***

  where:

  <X> is the number of the zone in which the VMS is located. The possible values are: 1–7.

  <Y> is the IP Packet Capture instance number associated with the VMS number. The possible values are: 1 on VMS01, 2 on VMS02, 3 on VMS09, and 4 on VMS10.

  <PPP> is the 3-digit zero-padded number of the Tsub prime site in which the IP Packet Capture virtual machine is located. The possible values are: 001-064.

  <P> is the number of the Tsub prime site. The possible values are: 1-64.
- **b** Click **Next**.

9 Optional: If the **Resource Pool** window appears, click on the IP address of the server. Click **Next**.

10 If the **Deploy OVF Template – Storage** window appears, perform the following actions:

- **a** Select a datastore to install the virtual machine upon.
  - For IP Packet Ca***<X>***pture in an L or M core, outside a Trunking Subsystem (Tsub), select: **z00das*<YY>*_datastore1**
  - For IP Packet Capture in a K core, select: **z00*<X>*vms01_datastore1**
  - For IP Packet Capture at a Trunking Subsystem (Tsub) prime site, select: **z00*<X>*s*<PPP>*vms01_datastore1**

  where:

  <X> is the zone number. The possible values are: 1-7.

  <YY> is the instance of the Direct Attached Storage (DAS).

  <PPP> is the 3-digit zero-padded number of the prime site in which the IP Packet Capture virtual machine is located. The possible values are: 001-064.
- **b** Click **Next**.

11 In the **Deploy OVF Template – Disk Format** window, perform one of the following actions:

- If the **Thick Provision Eager Zeroed** format is an available option, select it.
- If that option is not available, select **Thick Provision**.

12 Click **Next**.

13 In the **Deploy OVF Template – Network Mapping** window, select the appropriate **Destination Network** for each **Network Source**.

- For **znm0**, select **znm0**.
- For **cap1**, select **cap1**.
- For **cap2**, select **cap2**.
- For **cap3**, select **cap3**.
- For **cap4**, select **cap4**.

14 Click **Next**.

15 In the **Deploy OVF Template – Ready to Complete** window, verify the deployment settings. Click **Finish**.

> **NOTICE:** Ensure that the **Power on after deployment** check box is cleared. Modifications done after deployment require the virtual machine to be powered off.

The import starts.

16 When the process is completed successfully, verify that the left pane of the **vSphere Client** main window displays the application virtual machine name. You may need to expand the list in the left pane to locate the virtual machine name.

17 In the **Deployment Completed Successful** window, click **Close**.

18 Optional: If you used the DVD, remove it from the DVD drive.

Related Links

Installing IP Packet Capture on page 59

5.1.3

Configuring the vCenter for the Newly Deployed VM

For newly deployed virtual machines to run properly in an existing vCenter environment, you must override the default HA cluster settings and modify the restart priority for the new VMs. After a host failure, the VMs are restarted in the relative order determined by their restart priority.

When and where to use:

- This procedure applies only to systems where vCenter is installed.
- Run this procedure only if a VM OVF was deployed after the vCenter was originally configured.

Procedure:

1 Launch the Internet Explorer from a Windows-based device, such as the Network Management (NM) Client, or a service computer or laptop.

- Connect to: `https://`***`<vCenterIP>`***`/vsphere-client`
- Ignore or accept any warnings about the connection security or self-signed certificates.

2 In the dialog box, perform the following actions:

a Type in the user name `administrator@z00`***`<Z>`***`vcs`***`<H>`***`.zone`***`<Z>`***

where ***<Z>*** is the zone number and ***<H>*** is the vCenter instance number

b Type in the administrator user password.

c Click **Login**.

The vSphere Web Client homepage appears.

3 In the left pane, click **Hosts and Clusters**.

4 Expand the tree and right-click the **Zone*<X>*** HA cluster

where ***<X>*** is the zone number.

5 Select **Settings**.

6 In the **Settings** window, click **VM Overrides**.

7 Click **Add**.

8 Click the **+** button.

9 Select the check box for the VM you are configuring. Click **OK**.

10 Depending on the VM you are configuring, perform the following actions:

- For the vCenter VM, change the **VM Restart Priority** to **Medium**.
- For the VMs that are monitored under Fault Tolerance, change the **VM Restart Priority** to **High**.
- For the VMs that are not monitored under Fault Tolerance/HA, change the **VM Restart Priority** to **Disabled**.

11 Click **OK**.

12 **Perform the following actions only if you are recovering the VM after a failure and the VM is not monitored under Fault Tolerance:**

a In the **Settings** window, click **VM/Host Groups**.

b Select the group for the Virtual Management Server (VMS) on which the VM resides and click **Edit**.

c Click **Add**.

d Select the check box next to the VM and click **OK**.

For information about the locations of virtual machines on the VMS and their configurations with regard to vCenter, see "Virtual Machine Locations for vCenter Configs" in the *ASTRO 25 vCenter Application Setup and Operations Guide*.

e Click **OK**.

The restart priority setting for the newly deployed virtual machine is configured.

Related Links

Installing IP Packet Capture on page 59

5.1.4

Setting the Virtual Machine Startup and Shutdown Order

In an ASTRO® 25 system, virtual machines hosted on a Virtual Management Server (VMS) are configured to boot automatically with the system in a prescribed order. When you install a virtual machine on a VMS, change the VMS settings to ensure that the new virtual machine boots in the correct order with respect to the other virtual machines hosted on the VMS.

Procedure:

1 From a Windows-based device, launch the VMware vSphere Client.

A desktop shortcut was created during installation.

2 Log on to the server as a user with root privileges.

3 On the upper left side of the **vSphere Client Inventory** window, select the ESXi server.

4 On the right side of the window, select the **Configuration** tab.

The window displays information about the configuration of the ESXi server.

5 In the **Software** section, select **Virtual Machine Startup/Shutdown**.

6 On the right side of the main window, select **Properties**.

7 In the **System Settings** area, select **Allow virtual machines to start and stop automatically with the system**.

8 In the **Default Startup Delay** area, select **Continue immediately if the VMware Tools start**.

9 In the **Default Shutdown Delay** area, from the **Shutdown Action** drop-down list, select **Guest Shutdown**.

10 Put the virtual machines hosted on the ESXi server in the correct boot order:

  a In the **Startup Order** area, from the **Automatic Startup** list, select a virtual machine.

  b By using the **Move Up** and **Move Down** buttons, move the virtual machine to the correct ordered slot.

  NOTICE:
  Zone Core Virtual Machine Boot Order on page 89 outlines the boot order for the virtual machines that can reside on an ESXi-based Zone Core Virtual Management Server (VMS).

  To determine the correct ordered slot for each virtual machine hosted on the ESXi server that you are configuring, see the boot order table.

  c Repeat step 10 a and step 10 b until the boot order for the virtual machines is correct.

11 Click **OK**.

The **Properties** window closes.

Related Links

Installing IP Packet Capture on page 59

5.1.5

Applying Supplemental Configuration to Virtual Machines

Virtual machines hosted on the ESXi-based Virtual Management Server (VMS) require supplemental configuration to improve their security settings. You apply the supplemental configuration by running a script stored on the *VMware vSphere Configuration Media* disc.

Prerequisites:

- Obtain the *VMware vSphere Configuration Media* disc.
- Install VMware PowerCLI on the Windows-based device. See "Installing VMware PowerCLI" in the *Virtual Management Server Software* manual.

When and where to use: To perform this procedure, use a Windows-based device, such as the Network Management (NM) Client, Dispatch Console, or service computer/laptop.

Procedure:

1 Insert the *VMware vSphere Configuration Media* disc into the optical drive of the Windows-based device.

2 Open the PowerShell command prompt as administrator, using the actions that apply to the Windows operating system version present on the device.

If…	Then…
For Windows 7 or Windows Server 2008,	perform the following actions: a From **Start**, in the **Search programs and files** field, enter: `Command Prompt` b Right-click **Command Prompt** and select **Run as administrator**. c If the **User Account Control** window appears, click **Continue** or **Yes**, depending on the prompt you see. d If you are not logged on with an administrative account, enter the domain admin credentials. e At the command prompt, enter: `powershell`

If…	Then…
For Windows 10 or Windows Server 2012,	perform the following actions: **a** From **Start**, click **Search**. **b** In the search field, type in `powershell` **c** Right-click **Windows PowerShell**, and select **Run as administrator**. • If the **User Account Control** window appears, click **Yes**. • If you are not logged on with an administrative account, enter the domain admin credentials.

3 At the PowerShell prompt, enter the drive letter of the optical drive that contains the *VMware vSphere Configuration Media* disc followed by a colon.

Step example: `E:`

The directory is changed to the root directory of the *VMware vSphere Configuration Media* disc.

4 At the PowerShell prompt, enter: `cd common\bin`

The directory is changed to the `common\bin` directory of the *VMware vSphere Configuration Media* disc.

5 At the PowerShell prompt, enter: `.\Configure-VMHardening.ps1`

6 At the ESXi host IP prompt, enter the IP address of the ESXi host.

7 At the user name prompt, enter the ESXi host user name for an administrative account.

8 At the password prompt, enter the ESXi host password for an administrative account.

9 At the PowerShell, prompt, enter the name of the virtual machine for which you want to update the configuration.

NOTICE: Ensure that the name matches the name of the virtual machine as it appears in the left pane of the vSphere Client inventory view when connected to the ESXi host.

- For a zone core IP Packet Capture virtual machine, the name is: `z00`***<X>***`ipcap0`***<Y>***`.zone`***<X>***
- For a Tsub prime site IP Packet Capture virtual machine, the name is: `z00`***<X>***`s`***<PPP>***`ipcap01.site`***<P>***`.zone`***<X>***

where:

<X> is the number of the zone in which the VMS is located. The possible values are: 1–7.

<Y> is the IP Packet Capture instance number associated with the VMS number. The possible values are: 1 on VMS01, 2 on VMS02, 3 on VMS09, and 4 on VMS10.

<PPP> is the 3-digit zero-padded number of the prime site in which the IP Packet Capture virtual machine is located. The possible values are: 001-064.

<P> is the number of the Tsub prime site. The possible values are: 1-64.

The virtual machines supplemental configuration is applied.

10 Verify that there are no messages stating `[FAILED]` in the output of the script.

11 At the PowerShell prompt, enter: `exit`

12 At the Windows command prompt, enter: `exit`

Related Links

Installing IP Packet Capture on page 59

Devices for Connecting to the VMS on page 90

5.1.6 Adding a Third Virtual Hard Disk to IP Packet Capture

The IP Packet Capture virtual machine is imported and installed on two virtual hard disks. In L cores and M cores, the two virtual hard disks are stored on the Direct Attached Storage (DAS). In K cores and at Trunking Subsystem (Tsub) prime sites, the disks are stored on the Virtual Management Server (VMS). The installation process involves the creation of a third virtual hard disk on the VMS. This disk is used as a packet capture and hypervisor statistics file repository and is non-redundant.

Add a third virtual hard disk to the IP Packet Capture virtual machine by using a properly configured Windows-based device and a script available on the *VMware vSphere Configuration Media* DVD.

Prerequisites:
Obtain the *VMware vSphere Configuration Media* DVD.

Ensure that the following procedures have been performed on the Windows-based device:

- “Installing VMware PowerCLI”
- “Installing .NET Framework”
- “Installing Windows Management Framework”

For the procedures, see the *Virtual Management Server Software* manual.

Procedure:

1. Insert the *VMware vSphere Configuration Media* DVD into the optical drive of the Windows-based device.
2. Open the **Start** menu. Navigate to the **Command Prompt**.
3. Right-click the **Command Prompt** and select **Run as administrator**.
4. In the **Command Prompt** window, enter: `powershell`
5. At the PowerShell prompt, enter the drive letter of the optical drive that contains the *VMware vSphere Configuration Media* DVD followed by a colon.

   Step example: `E:`
   The directory is changed to the root directory of the *VMware vSphere Configuration Media* DVD.

6. At the PowerShell prompt, enter: `cd astro\bin`

   The directory is changed to the `astro\bin` directory of the *VMware vSphere Configuration Media* DVD.

7. At the PowerShell prompt, enter: `.\Create-ASTROIpcapLoggingDisk.ps1`
8. At the system location prompt, enter the number corresponding to the system location that this IP Packet Capture is being installed in.
   - For K core, enter: `1`
   - For L or M core, enter: `2`
   - For Trunking Subsystem (Tsub) prime site, enter: `6`
9. **IP Packet Capture located in a zone core:** At the VMS host instance number prompt, enter the number corresponding to the VMS number:
   - `1` for VMS01
   - `2` for VMS02
   - `9` for VMS09

- `10` for VMS10

NOTICE:
The VMS number depends on the location of the server in a core or subsystem of a specific type:

- VMS01: non-redundant cores (K1, L1, and M1 cores), redundant cores (K2, L2, M2, M3), Dynamic System Resilience (DSR) primary cores, and Trunking Subsystem (Tsub) prime sites
- VMS02: redundant cores (K2, L2, M2, M3) and redundant DSR primary cores
- VMS09: DSR backup cores
- VMS10: redundant DSR backup cores

10 **IP Packet Capture located in a zone core:** At the Dynamic System Resilience (DSR) prompt, perform one of the following actions:

- If the system is configured for DSR, enter: `y`
- Otherwise, enter: `n`

11 **IP Packet Capture located in a zone core with DSR:** At the core type prompt, enter the number corresponding to the core type that this IP Packet Capture is being installed in:

- For the primary DSR core, enter: `1`
- For the secondary DSR core, enter: `2`

12 At the zone ID prompt, enter the number corresponding to the zone number that this IP Packet Capture is being installed in.

13 **IP Packet Capture located at a Tsub prime site:** At the Tsub prime site number prompt, enter the number of the prime site.

The possible values are 1-64.

14 At the Virtual Management Server (VMS) login prompt, enter the root user password.

The system verifies if the VMS datastore exits, checks the available space on the datastore, and displays a list of virtual machines installed on the VMS.

15 When the system prompts you to select the IP Packet Capture virtual machine, enter the number corresponding to the IP Packet Capture VM.

16 When the system prompts you to create the new hard disk, select: `Y`.

A third virtual hard disk is created and added to IP Packet Capture.

17 At the exit prompt, verify that there are no messages in the output script stating that the operation failed and press ENTER.

18 At the PowerShell prompt, enter: `exit`

19 At the Windows command prompt, enter: `exit`

Related Links

Installing IP Packet Capture on page 59
Devices for Connecting to the VMS on page 90

5.1.7
Connecting and Powering On the IP Packet Capture Virtual Machine

At this point in the installation, connect and power on the IP Packet Capture virtual machine.

Prerequisites: From the system administrator, obtain the name of the appropriate zone network for IP Packet Capture that you are setting up as a virtual machine.

Procedure:

1. In the **VMware vSphere Client**, in the navigation pane on the left, right-click the IP Packet Capture virtual machine.
2. From the pop-up menu, select **Edit Settings**.
3. For each network adapter in the **Hardware** column, perform the following actions:
   a. Select a network adapter.
   b. In the **Device Status** area, select the **Connect at power on** check box.
   c. From the **Network label** drop-down list, select the correct zone network connection.
      - For **Network Adapter 1**, select **znm0**.
      - For **Network Adapter 2**, select **cap1**.
      - For **Network Adapter 3**, select **cap2**.
      - For **Network Adapter 4**, select **cap3**.
      - For **Network Adapter 5**, select **cap4**
   d. Click **OK**.
4. In the navigation pane, right-click the IP Packet Capture virtual machine.
5. From the pop-up menu, select **Power** → **Power On**.

Related Links

Installing IP Packet Capture on page 59

5.1.8

Configuring the Time Zone on Linux Servers

As a part of the installation, ensure that the virtual machine is set to the correct time zone.

Procedure:

1. From a Windows-based device, launch the VMware vSphere Client.

   A desktop shortcut was created during installation.
2. Log on to the ESXi server hosting the virtual machine as root by entering the IP address of the server and the root credentials.
3. In the **vSphere Client Inventory** window, verify that the virtual machine is powered on. If the virtual machine is powered off, power it on by right-clicking the virtual machine in the navigation pane and selecting **Power** → **Power On**.
4. From the navigation pane on the left, select the virtual machine. Click the **Console** tab for this virtual machine.
5. Wait until a prompt to log on console appears.
6. Click in the **Console** window and log on to the virtual machine as root.
7. At the prompt, enter: `admin_menu`
8. In the main administration menu, enter the number for the **OS Administration** option.
9. In the **OS Administration** menu, enter the corresponding number for **Manage Platform Configuration**.

10 In the **Manage Platform Configuration** menu, enter the corresponding number for **Set Time Zone**.

A menu displays numbered options to the change time zone.

11 The **Set Time Zone** option starts by prompting you for the region of the world.

You can choose to specify the time zone using the **Posix TZ format**. Continue responding to the prompts until you see a message regarding `/usr/bin/tzselect`. Ignore the message.

12 Press `q` to quit the menu.

Related Links

Installing IP Packet Capture on page 59

5.1.9 Setting the Identity for the IP Packet Capture Virtual Machine

At this point in the installation, configure the identity parameters of the IP Packet Capture virtual machine. The identity configuration allows other network elements to locate the IP Packet Capture virtual machine in the system. The identity parameters include the system ID, zone core type, zone ID, application ID, and optionally, a list of Centralized Logging Servers.

Procedure:

1 From a Windows-based device, launch the **VMware vSphere Client**.

A desktop shortcut was created during installation.

2 At the login prompt, perform the following actions:

a In the **IP address** field, type the IP address of the ESXi server.

b In the **User name** field, type: `root`

c In the **Password** field, type the appropriate password.

d Click **Login**.

3 In the **vSphere Client Inventory** window, on the navigation pane on the left, click the IP Packet Capture virtual machine.

4 In the navigation pane on the right, click the **Console** tab.

5 Click in the IP Packet Capture console and log on to the virtual machine as the root user.

6 At the command prompt, enter: `admin_menu`

7 In the **Main Menu**, enter the number corresponding to the **OS Administration** option.

8 In the **OS Administration** menu, enter the number corresponding to the **Manage Platform Configuration** option.

9 In the **Manage Platform Configuration** menu, enter the number corresponding to the **Set Identity** option.

10 At the location type prompt, enter the number corresponding to the location (zone core or Trunking Subsystem prime site) in which the IP Packet Capture virtual machine is located.

11 **IP Packet Capture at a Tsub prime site:** At the Tsub ID prompt, enter the number corresponding to the Prime Site in which the IP Packet Capture virtual machine is located.

12 At the Dynamic System Resilience (DSR) prompt, perform one of the following actions:

- If the system is configured for DSR, enter: `y`
- Otherwise, enter: `n`

13 **IP Packet Capture in a DSR system:** At the core type prompt, enter the number corresponding to the core type that this IP Packet Capture is being installed in.

14 At the zone ID prompt, enter the number corresponding to the zone number that this IP Packet Capture is being installed in.

- For K core, enter: `1`
- For L or M core, enter the zone number in the range of 1-7.

15 At the application ID prompt, enter the application ID that should be used for this IP Packet Capture installation:

- `1` on VMS01
- `2` on VMS02
- `3` on VMS09
- `4` on VMS10

NOTICE:
The VMS number depends on the location of the server in a core or subsystem of a specific type:

- VMS01: non-redundant cores (K1, L1, and M1 cores), redundant cores (K2, L2, M2, M3), Dynamic System Resilience (DSR) primary cores, and Trunking Subsystem (Tsub) prime sites
- VMS02: redundant cores (K2, L2, M2, M3) and redundant DSR primary cores
- VMS09: DSR backup cores
- VMS10: redundant DSR backup cores

16 At the system ID prompt, enter the system ID.

The system ID is a four-character-long hexadecimal number. It is a unique system identifier provided by Motorola Solutions.

Step example: 2CB5

17 **IP Packet Capture located in a zone core:** At the K core prompt, perform one of the following actions:

a If this IP Packet Capture is being installed in a K core, enter: `y`

b Otherwise, enter: `n`

18 At the syslog prompt, perform one of the following actions:

- If Centralized Syslog Servers are part of the system configuration, enter their IP addresses or hostnames. Separate multiple entries with a colon.
- Otherwise, press Enter.

19 At the confirmation prompt, verify if the input is correct and enter: `y`

The identity for the IP Packet Capture is applied. The virtual machine is restarted.

Related Links

Installing IP Packet Capture on page 59

5.1.10

Joining a Virtual Machine to the Domain

If the virtual machine is located in an L core or M core system, join the virtual machine to the Active Directory domain to enable authentication services.

Prerequisites:
Set the identity of the application.

Ensure that the application time is within 5 minutes of the time of the domain controller to avoid a failure.

When and where to use: This procedure is not applicable for a Unified Event Manager (UEM) in a K core system.

Procedure:

1. From a Windows-based device, launch the VMware vSphere Client.

   A desktop shortcut was created during installation.
2. Log on to the ESXi server hosting the Linux-based virtual machine as `root`.
3. In the **vSphere Client Inventory** window, from the navigation pane on the left, select the virtual machine and click the **Console** tab.
4. Click in the **Console** window and log on to the virtual machine as `root`.
5. At the prompt, enter: `admin_menu`
6. In the **Main Menu** menu, enter the corresponding number for **Services Administration**.
7. In the **Services Administration** menu, enter the corresponding number for **Manage AAA Client Configuration**.
8. In the **Manage AAA Client Configuration** menu, enter the number corresponding to **Join Domain**.

   The list of Active Directory domains appears.
9. Enter the number corresponding to the domain that you want to join.
10. At the domain account prompt, enter the name of the domain account used to join applications to the domain.
11. At the domain password prompt, enter the password of the domain account entered in the previous step.

    The application is joined to the domain.
12. In the **Manage AAA Client Configuration** menu, enter: `q`

    The command-line prompt for that application appears.
13. Enter: `exit`

    You are logged out of the application.

Related Links

Installing IP Packet Capture on page 59

5.1.11

Applying Platform Patch

You must update the virtual machine by applying the platform patch.

Procedure:

1. From a Windows-based device, launch the VMware vSphere Client.
2. Log on to the ESXi server.
3. Verify whether the following path appears on the toolbar: **Home** → **Inventory** → **Inventory**.
4. In the left pane, navigate to the virtual machine that you want to update.
5. In the right pane, click the **Console** tab.
6. Connect the virtual machine to the local DVD drive or ISO:

If…	Then…
If you have the DVD,	perform the following actions: **a** Insert the DVD in the drive of the Windows-based device. **b** In the VMware vSphere Client, click the disc icon on the toolbar and select **CD/DVD drive 1** → **Connect to** ***`<drive letter:>`*** where ***`<drive letter>`*** represents the drive with the DVD.
If you have the ISO,	perform the following actions: **a** Upload the ISO image to the Windows-based device. **b** In the VMware vSphere Client, click the disc icon on the toolbar and select **CD/DVD drive 1** → **Connect to ISO image on local disk**.

7. Navigate to the location of the patch ISO and select it. Click **Open**.
8. Click anywhere in the **Console** tab and log on to the virtual machine as the root user.
9. Enter: `systemctl start autofs`

   If messages appear about the autofs service already running, ignore them.
10. Enter: `ls /media/cdrom0/`

    If the drive contains the updater script, the update directory appears.
11. If the update directory does not appear, enter: `ls /media/cdrom1/`
12. Enter one of the following commands:
    - If the updater script is on cdrom0, enter: `/media/cdrom0/update/updater`
    - If the updater script is on cdrom1, enter: `/media/cdrom1/update/updater`
13. Change the directory to root by entering: `cd /`
14. Enter: `admin_menu`
15. Select **OS Administration** → **Eject CD/DVD** → **Eject All**.
16. Remove the DVD or ISO:
    - **a** Disengage the cursor from the console by pressing left CTRL + ALT.
    - **b** In the VMware vSphere Client, click the disc icon on the top toolbar and disconnect the DVD or ISO from the virtual machine.
    - **c** If prompted, confirm the operation.
17. Click anywhere in the **Console** tab.
18. Press ENTER.
19. Enter: `q`
20. Enter: `exit`

5.1.12

Entering the Global Web Services Credentials for the Default Hypervisor Definition

When you install IP Packet Capture, a default hypervisor definition is created for the Virtual Management Server (VMS) that hosts the application. This hypervisor definition is disabled and requires configuration. Log on to the IP Packet Capture user interface and edit the default hypervisor definition by entering the Global Web Services Credentials for an appropriate user account.

Prerequisites: From your system administrator, obtain the credentials for the Global Web Services account.

Procedure:

1. Log on to the IP Packet Capture user interface using an account that belongs to the **infradm** user group.
2. From the **Configuration** menu, select **Hypervisor statistics**.
3. In the **Actions** column for the default hypervisor definition, click **Edit**.
4. In the **Global Web Services Credentials** column, enter the user name and password for a Global Web Services account.
5. In the **Actions** column, click **Save**.

   The changes to the hypervisor definition are saved.

6. To update the system operation with the pending changes, click **Apply**.

Postrequisites: Enable the hypervisor definition. See Enabling Hypervisor Definitions on page 50.

Related Links

Installing IP Packet Capture on page 59
Editing Hypervisor Definitions on page 49
Logging On to the IP Packet Capture UI on page 41

Chapter 6

IP Packet Capture Configuration for SNMPv3

IP Packet Capture reports operational states and faults to the Unified Event Manager (UEM). UEM displays alarms and events for IP Packet Capture, such as errors related to packet captures or hypervisor definitions. The SNMPv3 protocol is used for secure communication between IP Packet Capture and UEM.

Related Links

Packet Capture State Transition Traps for UEM on page 83
Hypervisor Statistics State Transition Traps for UEM on page 85
IP Packet Capture Alarm Traps for UEM on page 86

6.1 Configuring USM User Security for IP Packet Capture

By using the SNMP Configuration Utility, you can configure the security levels and passphrases for user accounts in the User-based Security Model (USM) for SNMPv3. The USM contains a list of users and their attributes, including SNMPv3 support for authentication with or without encryption. You can access the SNMP Configuration Utility from the main administration menu of the IP Packet Capture virtual machine.

Prerequisites: For L and M core systems, obtain Active Directory account credentials. For information about setting up Active Directory users so that they can perform specific administration menu procedures, see “Appendix B” in the *Authentication Services* manual and contact your Active Directory administrator.

Procedure:

1. Log on to the IP Packet Capture server:
   - For L and M core systems, log on with your Active Directory account credentials.
   - For K core systems, log on with local administrator root account credentials.
2. At the user prompt, enter: `admin_menu`
3. In the main IP Packet Capture administration menu, select **OS Administration**.
4. In the **OS Administration** menu, select **Security Provisioning**.
5. In the **Security Provisioning** menu, select **Manage SNMP Passphrases**.
6. In the **Manage SNMP Passphrases** menu, select **Configure SNMPv3 Agent**.

   The SNMP Configuration Utility appears.
7. At the MotoAdmin authentication passphrase prompt, enter the MotoAdmin authentication passphrase.
8. At the MotoAdmin Privacy passphrase prompt, enter the MotoAdmin Privacy passphrase.
9. In the **SNMP Administration** menu, select the type of user account to configure:

If…	Then…
If you want to modify credentials for an INFORM user account,	select **Modify SNMP Inform Configuration**. The system displays the currently active INFORM user account (MotoInformA or MotoInformB) and indicates the security level of that user account.
If you want to modify credentials for any other user account,	select **Modify SNMP User Configuration**. The system displays a list of user accounts currently available for configuration if you are logged on as MotoAdmin, including MotoMaster. The list shows the security levels of the user accounts listed.

10 From the **Select User to Modify** menu, select a user:

If…	Then…
If you select the MotoAdmin user, which always has a security level of AuthPriv, so only its passphrases can be changed,	change the passphrases. See Modifying User Passphrases for IP Packet Capture on page 76.
If you select a user with a security level of noAuthNoPriv, which means that no passphrases are configured for that user,	set the security level. See Setting User Security Levels for IP Packet Capture on page 77.
If you select a user other than MotoAdmin with a security level of AuthPriv, or you select a user with a security level of AuthNoPriv,	in the **Select Modification** menu, perform one of the following actions: • Change the passphrases. See Modifying User Passphrases for IP Packet Capture on page 76. • Change the security level. See Modifying User Security Levels for IP Packet Capture on page 77.

11 Enter: `q`

Repeat the sequence until the **Common Credentials User Interface** closes.

6.2 Modifying User Passphrases for IP Packet Capture

The SNMP Configuration Utility provides the option to modify the authentication and privacy passphrases for users with the AuthPriv and AuthNoPriv security levels. You can access the SNMP Configuration Utility from the main administration menu of the IP Packet Capture virtual machine.

Prerequisites: Perform Configuring USM User Security for IP Packet Capture on page 75.

Procedure:

1 After selecting a user account from the **Select User to Modify** menu, perform one of the following actions:

If…	Then…
If the selected user account	perform the following actions:

If…	Then…
has the AuthPriv security level,	**a** From the **Select Modification** menu, select **Update Passphrases**. **NOTICE:** The change of passphrases is the only modification available for the MotoAdmin user account. For the MotoAdmin user account, the **Select Modification** menu does not appear. **b** Enter the current authentication and privacy passphrases for the selected user account. **c** Enter and confirm the new authentication passphrase. **d** Enter and confirm the new privacy passphrase.
If the selected user account has the AuthNoPriv security level,	perform the following actions: **a** From the **Select Modification** menu, select **Update Passphrases**. **b** Enter the current authentication passphrase for the selected user account. **c** Enter and confirm the new authentication passphrase.

The passphrases are updated and the **Select User to Modify** menu appears.

6.3 Setting User Security Levels for IP Packet Capture

The SNMP Configuration Utility provides the option to set user security levels for users with the NoAuthNoPriv security level. You can access the SNMP Configuration Utility from the main administration menu of the IP Packet Capture virtual machine.

Prerequisites: Perform Configuring USM User Security for IP Packet Capture on page 75.

Procedure:

1. After selecting a user to modify, from the **Enter New Security Level** menu, select the option for the new security level of the user.
2. At the prompts for the new passphrases, enter the appropriate passphrases.
3. At the prompts for the MotoAdmin passphrases, enter the appropriate passphrases.

   The security level of the selected user is updated and the **Select User to Modify** menu appears.

6.4 Modifying User Security Levels for IP Packet Capture

The SNMP Configuration Utility provides the option to modify user security levels for users other than MotoAdmin with the AuthPriv security level and users with the AuthNoPriv security level. You can access the SNMP Configuration Utility from the main administration menu of the IP Packet Capture virtual machine.

Prerequisites: Perform Configuring USM User Security for IP Packet Capture on page 75.

Procedure:

1. After selecting a user account to modify, from the **Select Modification** menu, select **Change Security Level**.

   The **Enter New Security Level** menu appears, displaying the name and current security level of the selected user account, and a list of allowed security levels for that user account.

2. From the **Enter New Security Level** menu, select the desired security level.

   Depending on the security level selected, prompts for new passphrases may appear, followed by prompts for MotoAdmin passphrases.

3. At each prompt, enter the appropriate passphrase.

   The security level of the selected user is updated and the **Select User to Modify** menu appears.

Chapter 7

IP Packet Capture Disaster Recovery

This chapter provides disaster recovery procedures for IP Packet Capture.

7.1 Recovering IP Packet Capture After a Failure

The IP Packet Capture application can become unavailable due to a failure of the Virtual Management Server (VMS), the VMS local disk, or the Direct Attached Storage (DAS). To recover the application, replace the failed component and re-install the IP Packet Capture virtual machine or restore the IP Packet Capture repository.

IP Packet Capture is a Backup and Restore (BAR) client, which means that the BAR server regularly backs up the configuration and identity data for IP Packet Capture. If IP Packet Capture becomes unavailable due to a failure of the VMS or DAS, the backup data is used to restore the IP Packet Capture configuration.

IMPORTANT: BAR does not back up the packet capture and hypervisor statistics file repositories.

Process:

1. Replace the component the failure of which caused the loss of IP Packet Capture:
   - Virtual Management Server (VMS)
   - VMS local disk
   - Direct Attached Storage (DAS)

   See the *Virtual Management Server Hardware* and *Virtual Management Server Software* manuals.
2. Perform one of the following actions:
   - If the DAS has been replaced, delete the IP Packet Capture third virtual disk image from the VMS local disk.

     See Deleting the IP Packet Capture Third Virtual Disk on page 80.
   - If the VMS or VMS local disk has been replaced, delete the IP Packet Capture virtual machine.

     See Deleting a Virtual Machine on page 81.
3. Install IP Packet Capture.

   See Installing IP Packet Capture on page 59.
4. If the centralized Backup and Restore (BAR) service is implemented in the system, perform the following to register the BAR client on the IP Packet Capture virtual machine to the BAR server:

   a Perform the necessary key provisioning steps if the system is set to secure and the keys on the BAR server have been rotated.

   See “Performing the Secure Transfer of the SSH Client Key to Linux-Based Backup Clients” in the *Securing Protocols with SSH* manual.

   b Verify that you can successfully register the BAR client on the IP Packet Capture virtual machine to the BAR server, if it is available.

See “Registering and Enabling Linux BAR Clients” in the *Backup and Restore Services* manual.

c Restore configurations that were backed up by the Backup Client on the IP Packet Capture virtual machine you are replacing.

See the following procedures in the *Backup and Restore Services* manual:

- “Executing a BAR Client Data Restore”
- “Completing a Data Restore on a Linux BAR Client”

5 Verify that IP Packet Capture has been recovered by performing the following actions:

a Verify that packet capture definitions match expectations.

b Verify that the defined packet captures are collecting files.

c Verify that the passphrase complexity configuration matches expectations.

d Verify that the packet capture files can be downloaded.

See Downloading Packet Capture Files on page 43.

e Verify that the hypervisor definitions match expectations.

f Verify that the configured hypervisor definitions are collecting statistics.

g Verify that the hypervisor statistics files can be downloaded.

See Downloading Hypervisor Statistics Files on page 48

7.1.1 Deleting the IP Packet Capture Third Virtual Disk

A failure-related replacement of the Direct Attached Storage (DAS) requires a removal of the IP Packet Capture third virtual disk image from the Virtual Management Server (VMS) local disk.

The third virtual disk was created on the VMS local disk during the installation of IP Packet Capture and remains on the VMS when the DAS has failed.

⚠ **CAUTION:** Perform this procedure only when recovering the IP Packet Capture virtual machine lost due to a failure of the DAS.

Prerequisites: Obtain the following information:

- IP address of the VMS hosting the IP Packet Capture virtual machine
- Password for the root user account

Procedure:

1 From a Windows-based device, launch the **VMware vSphere Client**.

2 Log on to the appropriate VMS as the root user.

The **vSphere Client Inventory** window appears.

3 In the navigation pane on the left, select the VMS and click **Configuration** → **Storage**.

4 In the **Datastores** view, identify the VMS datastore: **z00*<X>*vms*<YY>*_datastore1**

where:

<X> is the number of the zone in which the VMS is located. The possible values are: 1–7.

<YY> is the VMS number. The possible values are: 01, 02, 09, and 10.

NOTICE:
The VMS number depends on the location of the server in a core or subsystem of a specific type:

- VMS01: non-redundant cores (K1, L1, and M1 cores), redundant cores (K2, L2, M2, M3), Dynamic System Resilience (DSR) primary cores, and Trunking Subsystem (Tsub) prime sites
- VMS02: redundant cores (K2, L2, M2, M3) and redundant DSR primary cores
- VMS09: DSR backup cores
- VMS10: redundant DSR backup cores

5 Right-click the VMS datastore and select **Browse Datastore**.

6 In the **Datastore Browser** window, identify the IP Packet Capture folder.

The name of the folder is the same as the name entered for the IP Packet Capture virtual machine during installation:

- For IP Packet Capture in a zone core, the name is: `z00`***<X>***`ipcap0`***<Y>***`.zone`***<X>***
- For IP Packet Capture at a Tsub prime site, the name is: z00***<X>***s***<PPP>***ipcap01.site***<P>***.zone***<X>***

where:

<X> is the number of the zone in which the VMS is located. The possible values are: 1–7.
<Y> is the IP Packet Capture instance number associated with the VMS number. The possible values are: 1 on VMS01, 2 on VMS02, 3 on VMS09, and 4 on VMS10.
<PPP> is the 3-digit zero-padded number of the prime site in which the IP Packet Capture virtual machine is located. The possible values are: 001-064.
<P> is the number of the Tsub prime site. The possible values are: 1-64.

7 Delete the IP Packet Capture folder and its content:

a Right-click the folder and select **Delete from Disk**.

b In the **Confirm Delete** window, click **Yes**.

8 Close the **Datastore Browser** window.

9 In the **Datastores** view, click **Refresh** to refresh the view of the datastore content.

Related Links

Recovering IP Packet Capture After a Failure on page 79

7.1.2
Deleting a Virtual Machine

This procedure describes how to delete a virtual machine hosted on a Virtual Management Server (VMS).

CAUTION: Deleting a virtual machine can disrupt the system operation and cause irreversible data loss. Perform this procedure only in specific situations for a specific purpose; for example, in disaster recovery scenarios as a part of the prescribed recovery process.

Procedure:

1 Launch the **VMware vSphere Client** from the Windows-based device where it resides (a desktop shortcut was created during installation).

2 Log on to the server as `root`.

3 On the left-side of the main window, expand the list of virtual machines.

4. On the left-side of the main window, right-click the virtual machine and select **Power** → **Power Off**.

   The virtual machine powers off.

5. Right-click the virtual machine again and select **Delete from Disk**.

   A confirmation dialog box appears.

6. Click **Yes**.

   The confirmation dialog box closes and the virtual machine is deleted from the virtual server.

Related Links

Recovering IP Packet Capture After a Failure on page 79

Chapter 8

IP Packet Capture Troubleshooting

This chapter provides troubleshooting information for IP Packet Capture. If an error occurs during IP Packet Capture operation, the application sends an error message to the Unified Event Manager (UEM) application. Follow the information about UEM traps and alarms for IP Packet Capture to solve any issues with the application.

Related Links

Packet Capture State Transition Traps for UEM on page 83
Hypervisor Statistics State Transition Traps for UEM on page 85
IP Packet Capture Alarm Traps for UEM on page 86

8.1
Packet Capture State Transition Traps for UEM

IP Packet Capture reports operational states and faults to the Unified Event Manager (UEM) application. UEM displays states for IP Packet Capture categorized by severity: clear, warning, major, and critical. The security level of a state is indicated by the appropriate color and message. In the **Alarms** window in UEM, the states for packet captures are marked as **IP Packet Capture Service** in the **EntityName** field.

UEM can display the following states for the packet capture feature of the IP Packet Capture application, listed in the order from the least to the most severe:

ENABLED, NORMAL

Severity: clear

Message: ENABLED, NORMAL – Online captures – ***<captures list>***

where:

<captures list> can include: capture-eth1, capture-eth2, capture-eth3, capture-eth4

Example: ENABLED, NORMAL – Online captures – capture-eth1, capture-eth2

Description: This event indicates normal operation and appears when the system has been started correctly.

ENABLED, USER REQUESTED

Severity: clear

Message: ENABLED, USER REQUESTED – Online captures – ***<captures list>***

where:

<captures list> can include: capture-eth1, capture-eth2, capture-eth3, capture-eth4

Example: ENABLED, USER REQUESTED – Online captures – capture-eth1, capture-eth2

Description: This event indicates normal operation and appears when a user has enabled all the defined packet captures after one or all the captures were disabled.

DISABLED, USER REQUESTED

Severity: major

Message: DISABLED, USER REQUESTED

Description: A user has disabled all the defined packet captures.

Solution: Enable the disabled packet capture definitions.

DISABLED, NORMAL

Severity: major

Message: DISABLED, NORMAL

Description: This alarm indicates that all the defined packet captures are disabled during a restart or shutdown.

Solution: Wait for the restart to complete or power on the IP Packet Capture virtual machine.

MAJOR MALFUNCTION, SOFTWARE ERROR

Severity: major

Message: MAJOR MALFUNCTION, SOFTWARE ERROR – Several critical services down – ***<captures list>***

where:

<captures list> can include: capture-eth1, capture-eth2, capture-eth3, capture-eth4

Example: MAJOR MALFUNCTION, SOFTWARE ERROR – Several critical services down – capture-eth1

Description: One of the defined packet captures is disabled. The service (for example: capture-eth1) responsible for running this packet capture is down.

Solution:

1. Disable and then enable the packet capture definition.
2. If that does not work, power off and power on the IP Packet Capture virtual machine.
3. If that does not work, contact Motorola Solutions.

CRITICAL MALFUNCTION, SOFTWARE ERROR

Severity: critical

CRITICAL MALFUNCTION, SOFTWARE ERROR – All critical services down – ***<captures list>***

where:

<captures list> can include: capture-eth1, capture-eth2, capture-eth3, capture-eth4

Example: CRITICAL MALFUNCTION, SOFTWARE ERROR – All critical services down – capture-eth1

Description: All the defined packet captures are disabled. The services (capture-eth1, capture-eth2, capture-eth3, capture-eth4) responsible for running the packet captures are down.

Solution:

1. Disable and then enable each packet capture definition.
2. If that does not work, power off and power on the IP Packet Capture virtual machine.
3. If that does not work, contact Motorola Solutions.

Related Links

Adding Packet Captures on page 44

8.2 Hypervisor Statistics State Transition Traps for UEM

IP Packet Capture reports operational states and faults to the Unified Event Manager (UEM) application. UEM displays states for Hypervisor Statistics categorized by severity: clear, warning, major, and critical. The security level of a state is indicated by the appropriate color and message. In the **Alarms** window in UEM, the states for hypervisor statistics are marked as **Hypervisor Statistics Capture Service** in the **EntityName** field.

UEM can display the following states for hypervisor statistics collected by IP Packet Capture, listed in the order from the least to the most severe:

ENABLED, NORMAL

Severity: clear

Message: ENABLED, NORMAL – Online hypervisors – ***<hypervisors list>***

where:

<hypervisors list> can include: vmstat-vms01, vmstat-vms02, vmstat-vms09, vmstat-vms10

Example: ENABLED, NORMAL – Online hypervisors – vmstat-vms01

Description: This event indicates normal operation and appears when the system has been started correctly.

ENABLED, USER REQUESTED

Severity: clear

Message: ENABLED, USER REQUESTED – Online hypervisors – ***<hypervisors list>***

where:

<hypervisors list> can include: vmstat-vms01, vmstat-vms02, vmstat-vms09, vmstat-vms10

Example: ENABLED, USER REQUESTED – Online hypervisors – vmstat-vms01

Description: This event indicates normal operation and appears when a user has enabled all the hypervisor definitions after one or all the hypervisor definitions were disabled.

DISABLED, USER REQUESTED

Severity: major

Message: DISABLED, USER REQUESTED

Description: A user has disabled all the hypervisor definitions.

Solution: Enable the disabled hypervisor definitions.

DISABLED, NORMAL

Severity: major

Message: DISABLED, NORMAL

Description: This alarm indicates that all the hypervisor definitions are disabled during a restart or shutdown.

Solution: Wait for the restart to complete or power on the IP Packet Capture virtual machine.

MAJOR MALFUNCTION, SOFTWARE ERROR

Severity: major

Message: MAJOR MALFUNCTION, SOFTWARE ERROR – Several critical services down – ***<hypervisors list>***

where:

<hypervisors list> can include: vmstat-vms01, vmstat-vms02, vmstat-vms09, vmstat-vms10

Example: MAJOR MALFUNCTION, SOFTWARE ERROR – Several critical services down – vmstat-vms01

Description: One of the hypervisor definitions is disabled. The service (for example: vmstat-vms01) responsible for running this hypervisor definition is down.

Solution:

1. Recover SSH connections from IP Packet Capture to the Virtual Management Server (VMS).

   See "Updating Known Hosts List on an IP Packet Capture for Connections to a VMS" in the *Securing Protocols with SSH*.
2. Disable and then enable the hypervisor definition.
3. If that does not work, power off and power on the IP Packet Capture virtual machine.
4. If that does not work, contact Motorola Solutions.

CRITICAL MALFUNCTION, SOFTWARE ERROR

Severity: critical

CRITICAL MALFUNCTION, SOFTWARE ERROR – All critical services down – ***<hypervisors list>***

where:

<hypervisors list> can include: vmstat-vms01, vmstat-vms02, vmstat-vms09, vmstat-vms10

Example: CRITICAL MALFUNCTION, SOFTWARE ERROR – All critical services down – vmstat-vms01

Description: All the defined hypervisor definitions are disabled. The services (for example: vmstat-vms01) responsible for running the hypervisor definitions are down.

Solution:

1. Recover SSH connections from IP Packet Capture to the Virtual Management Server (VMS).

   See "Updating Known Hosts List on an IP Packet Capture for Connections to a VMS" in the *Securing Protocols with SSH*.
2. Disable and then enable each hypervisor definition.
3. If that does not work, power off and power on the IP Packet Capture virtual machine.
4. If that does not work, contact Motorola Solutions.

Related Links

Adding Hypervisor Definitions on page 48

8.3 IP Packet Capture Alarm Traps for UEM

Unified Event Manager (UEM) can display the following alarms for the non-critical services that are a part of the IP Packet Capture application. If one or more of these services fails, the operation of IP Packet Capture can become unstable and the user interface can become temporary unavailable.

One or more non-critical services are down

Severity: warning

Message: One or more non-critical services are down. – ***<list of services>***

where:

<services list> can include: ipcap-tomcat, ipcap-monitor, ipcap-rotator

Example: One or more non-critical services are down. – ipcap-rotator

Description: This alarm indicates that one of the non-critical services has suddenly stopped:

ipcap-tomcat
The Web server is down. The IP Packet Capture user interface cannot be accessed through a Web browser.

ipcap-monitor
The configuration changes monitor is down. Changes to the packet capture definitions and hypervisor definitions made by users are not saved.

ipcap-rotator
The files rotation in the `/var/capture` and `/var/stats` partitions is down. The partitions can fill up.

Solution:

1 Power off and power on the IP Packet Capture virtual machine.

2 If that does not work, contact Motorola Solutions.

Related Links

Adding Packet Captures on page 44
Adding Hypervisor Definitions on page 48

This page intentionally left blank.

Chapter 9

IP Packet Capture Reference

This chapter contains reference information for IP Packet Capture installation. The chapter provides the boot order for the virtual machines hosted on a Virtual Management Server (VMS) and the list of Windows-based devices that can be used to connect to a VMS.

9.1 Zone Core Virtual Machine Boot Order

NOTICE:
Up to two instances of the GMC can be on the server.

If UNCDS is present, three instances of the UNCDS are on the server.

Table 1: Zone Core Virtual Machine Boot Order

Order		Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Automatic Startup						
	1	ZC	Enabled	Use Default	Use Default	Use Default
	2	Transcoder	Enabled	Use Default	Use Default	Use Default
	3	ISGW	Enabled	Use Default	Use Default	Use Default
	4	PDG-Conv	Enabled	Use Default	Use Default	Use Default
	5	PDG-HPD	Enabled	Use Default	Use Default	Use Default
	6	PDG-IV&D	Enabled	Use Default	Use Default	Use Default
	7	License Manager	Enabled	Use Default	Use Default	Use Default
	8	ATR	Enabled	Use Default	Use Default	Use Default
	9	DC-System	Enabled	Use Default	Use Default	Use Default
	10	DC-Zone	Enabled	Use Default	Use Default	Use Default
	11	IPCAP	Enabled	Use Default	Use Default	Use Default
Any Order		AuC	Enabled	Use Default	Use Default	Use Default
		BAR	Enabled	Use Default	Use Default	Use Default
		CSMS	Enabled	Use Default	Use Default	Use Default
		InfoVista	Enabled	Use Default	Use Default	Use Default
		FMS – Fortinet	Enabled	Use Default	Use Default	Use Default
		GDG	Enabled	Use Default	Use Default	Use Default
		GMC	Enabled	Use Default	Use Default	Use Default
		NM Client	Enabled	Use Default	Use Default	Use Default
		UCS	Enabled	Use Default	Use Default	Use Default
		SSS	Enabled	Use Default	Use Default	Use Default

Table continued…

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
	Syslog	Enabled	Use Default	Use Default	Use Default
	UEM	Enabled	Use Default	Use Default	Use Default
	UNC	Enabled	Use Default	Use Default	Use Default
	UNCDS	Enabled	Use Default	Use Default	Use Default
	vCenter App	Enabled	Use Default	Use Default	Use Default
	ZDS	Enabled	Use Default	Use Default	Use Default
	ZSS	Enabled	Use Default	Use Default	Use Default
Manual Startup	DESU Waypoint	Disabled	Use Default	Use Default	Use Default

Related Links

Setting the Virtual Machine Startup and Shutdown Order on page 64

9.2

Devices for Connecting to the VMS

In the ASTRO® 25 system, you can connect to the Virtual Management Server (VMS) with a properly configured Windows-based device. A connection to the VMS allows you to view the server configuration, run configuration scripts on the server, and make other changes to the server settings.

L and M cores

The following Windows-based devices can be used to connect to the VMS in L and M cores:

- NM Clients
- MCC 7100 or MCC 7500 consoles
- Service computers/laptops

K cores

The following Windows-based devices can be used to connect to the VMS in K cores:

- K core Clients
- MCC 7100 or MCC 7500 consoles
- Service computers/laptops
- NM Clients (via the firewall)

Configuration Requirements

Before connecting to the VMS, ensure that the following procedures have been performed on the Windows-based device:

- “Installing VMware PowerCLI”
- “Installing .NET Framework”
- “Installing Windows Management Framework”

For the procedures, see the *Virtual Management Server Software* manual.

Related Links

Applying Supplemental Configuration to Virtual Machines on page 65

Adding a Third Virtual Hard Disk to IP Packet Capture on page 67

This page intentionally left blank.

Appendix A

IP Packet Capture Feature Expansion

This appendix provides the process for adding the IP Data Capture feature to your system release, including connection tables and diagrams.

A.1

Adding the IP Packet Capture Feature to the System

To add the IP Packet Capture feature to the system, perform the expansion procedure on the correct Virtual Management Server or Servers (VMS).

- In non-redundant systems (K1, L1, and M1 cores), perform the expansion on VMS01.
- In redundant systems (K2, L2, M2, and M3 cores) without Dynamic System Resilience (DSR), perform the expansion on VMS01 and VMS02.
- In M1 cores with DSR, perform the expansion on VM01 and VMS09.
- In M3 cores with DSR, perform the expansion on VMS01, VMS02, VMS09, and VMS10.
- At Trunking Subsystem (Tsub) prime sites, perform the expansion on VMS01.

For each VMS, the expansion consists of the following tasks:

- Installing or replacing the extender panel on the VMS rack and connecting the back of the extender panel to the VMS.
- Installing the IP Packet Capture virtual machine on the VMS. The installation includes configuration of hypervisor statistics for the VMS hosting the IP Packet Capture virtual machine.
- Configuring additional features for IP Packet Capture: Backup and Restore (BAR) services, SNMPv3, Unified Event Manager (UEM) monitoring, McAfee antivirus protection, and SSH.
- Establishing Ethernet cable connections between IP Packet Capture and capture points (such as core LAN switches) and adding packet capture definitions for these connections in the IP Packet Capture user interface.

Prerequisites: Disconnect the existing Data Collection Devices (DCD) present in the zone core. IP Packet Capture is a replacement for the DCD. You can redeploy the DCD elsewhere and any DCD at the sites can remain, but the DCD in the zone core must be disconnected.

Process:

1. Check if the required version of the extender panel is installed on the VMS rack.

   The previous version of the panel only has the Backup and Restore NAS Connection Port. For the new version of the panel with additional ports for IP Packet Capture, see Figure 16: Extender Panel on page 106.

2. If the new version of the extender panel is not present, perform the following actions:

   a Prepare the necessary parts for installation and connections.

   Kit T8303 contains the required parts. The kit is included in System Upgrades and certain other expansion orders.

   b Mount the new extender panel on the VMS rack:

   - If the rack has no extender panel, install the new extender panel in an available one rack-unit (1U) space on the rack.

- If the previous version of the panel is installed on the rack, remove the existing panel and install the new extender panel in its place.

c Connect the back side of the extender panel to the VMS according to the information provided in HP DL380 Gen9 Physical Ports and Connections on page 94.

3 If the MAC Port Lockdown feature is used in the system, disable MAC Port Lockdown.

See the *MAC Port Lockdown* manual.

4 Install IP Packet Capture on the correct servers.

See Installing IP Packet Capture on page 59.

5 If the centralized Backup and Restore (BAR) service is implemented in the system, perform the following to register the BAR client on the IP Packet Capture virtual machine to the BAR server:

a Perform the necessary key provisioning steps if the system is set to secure and the keys on the BAR server have been rotated.

See “Performing the Secure Transfer of the SSH Client Key to Linux-Based Backup Clients” in the *Securing Protocols with SSH* manual.

b Verify that you can successfully register the BAR client on the IP Packet Capture virtual machine to the BAR server, if it is available.

See “Registering and Enabling Linux BAR Clients” in the *Backup and Restore Services* manual.

6 If required by the needs of your organization, configure the security levels and passphrases used for secure communication between the IP Packet Capture virtual machine and UEM.

See Configuring USM User Security for IP Packet Capture on page 75.

7 Discover each new IP Packet Capture virtual machine in UEM.

See “Discovering Network Elements” in the *Unified Event Manager* manual.

8 On each IP Packet Capture virtual machine, install the McAfee Agent and the McAfee VirusScan Enterprise (VSE).

See “Deploying the McAfee Client Software to Anti-Malware Clients in RNI” in the *Core Security Management Server* manual.

9 Connect Ethernet cables to the physical monitor ports and the capture interfaces, and configure packet capture definitions for the established connections.

See Configuring IP Packet Capture to Capture from a Device on page 103.

10 If the MAC Port Lockdown feature is used in the system, enable MAC Port Lockdown.

See the *MAC Port Lockdown* manual.

11 **For IP Packet Capture in a Trunking Subsystem (Tsub):** Add the IP Packet Capture sites to the Dynamic Trusted Sites Group Policy on the Domain Controller.

See Adding Sites to the Dynamic Trusted Sites Group Policy on page 106.

A.1.1 HP DL380 Gen9 Physical Ports and Connections

Physical network adapter ports correspond to virtual network adapters. Validate physical and virtual networking before installing virtual machines. The network adapters are configured using the VMware vSphere Client application. See “Virtual Management Server Installation and Configuration” in the *Virtual Management Server Software* manual.

Figure 7: HP DL380 Gen9 Front View with Description

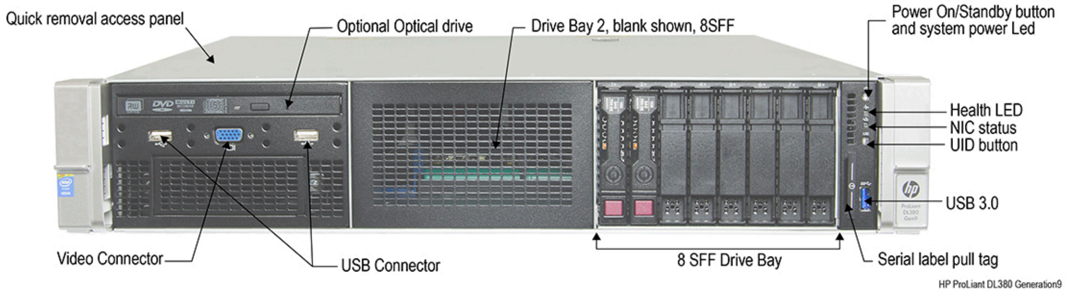

Quick removal access panel
Optional Optical drive
Drive Bay 2, blank shown, 8SFF
Power On/Standby button and system power Led
Health LED
NIC status
UID button
USB 3.0
Video Connector
USB Connector
8 SFF Drive Bay
Serial label pull tag
HP ProLiant DL380 Generation9

Figure 8: HP DL380 Gen9 Rear View with Description

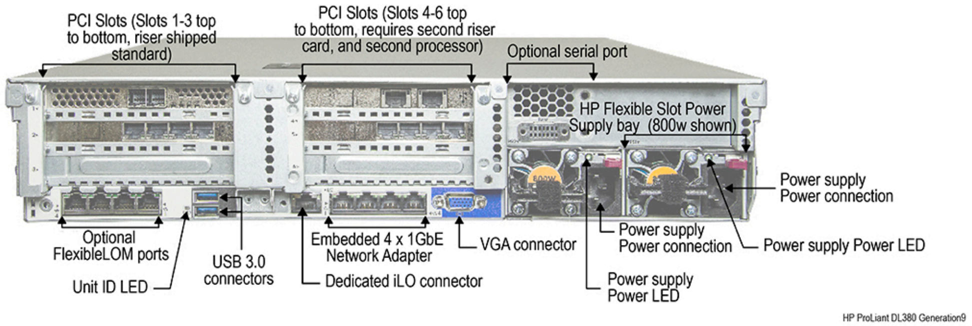
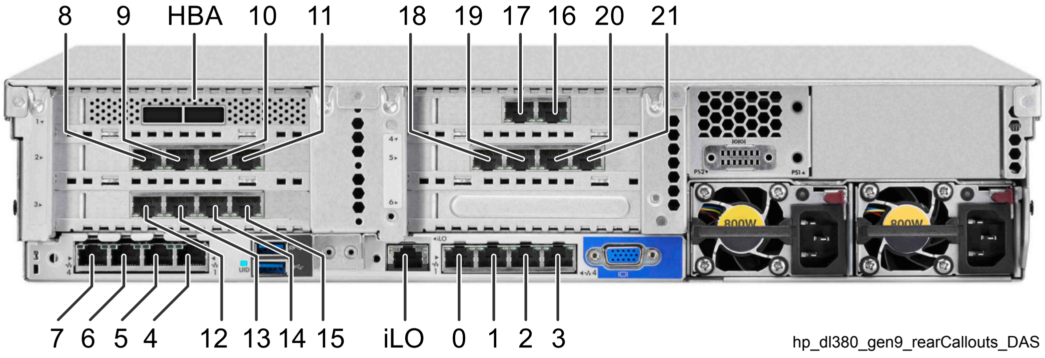

PCI Slots (Slots 1-3 top to bottom, riser shipped standard)
PCI Slots (Slots 4-6 top to bottom, requires second riser card, and second processor)
Optional serial port
HP Flexible Slot Power Supply bay (800w shown)
Power supply Power connection
Power supply Power connection
Power supply Power LED
Power supply Power LED
VGA connector
Embedded 4 x 1GbE Network Adapter
Dedicated iLO connector
USB 3.0 connectors
Optional FlexibleLOM ports
Unit ID LED
HP ProLiant DL380 Generation9

Table 2: HP DL380 Gen9 Cable Connections

HP DL380 Port	To
Flexible LOM Port	Core LAN Switch, or Crossover cable to other VMS (optional)
Embedded 1GbE RJ-45	Network Adapter
Serial Port	Terminal server
iLO Connector	Remote access/service (Ethernet)
Video Connector	Video monitor – if used
USB Connector 1	Not used
USB Connector 2	Not used
USB Connector 3	Not used
USB Connector 4	Not used
Power Supply 1 Port	AC power source
Power Supply 2 Port	AC power source

Figure 9: HP DL380 Gen9 NIC Ports with HBA Connectors for L and M Core VMS (except Transcoder and ISGW)

The following figure is an example. It describes the system with DAS implementation. The number of available ports and slots may vary depending on your system configuration.



©2015 Hewlett-Packard Development Company, L.P. Reproduced with permission.

Table 3: HP DL380 Gen9 NIC Port Cable Connections for L and M Core VMS (except Transcoder and ISGW)

The connections provided in this table apply to the following Virtual Management Servers: VMS01, VMS02, VMS03, VMS09, and VMS10 in system configurations with DAS.

- Non-redundant cores (L1 and M1) include VMS01.
- Non-redundant M1 DSR cores include VMS01 and VMS09.
- Redundant cores (L2, M2, and M3) without DSR include VMS01 and VMS02.
- Redundant M3 DSR cores include VMS01, VMS02, VMS09, and VMS10.
- Redundant M3 High Capacity UNC cores include VMS03.

HP DL380 NIC Port	VMS Number or System Configuration	Connects to	Port Usage
NIC 0	Redundant and non-redundant cores	Core LAN Switch 1	Network Management
NIC 1	Redundant and non-redundant cores	Core LAN Switch 1	Network Management
NIC 2	VMS01, VMS02, VMS09, and VMS10 in redundant and non-redundant cores	Core LAN Switch 1	Intersystem Audio/ Control
	VMS03	Unused	Unused
NIC 3	VMS01, VMS02, VMS09, and VMS10 in redundant and non-redundant cores	Core LAN Switch 1	Control
	VMS03	Unused	Unused

Table continued…

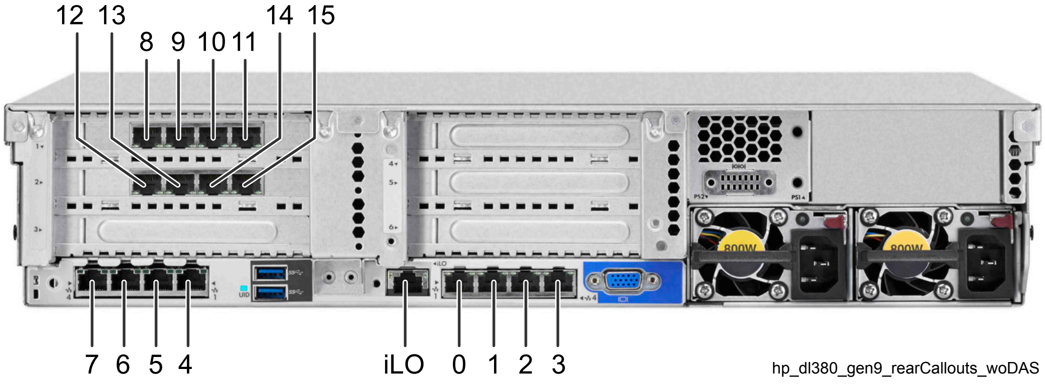
HP DL380 NIC Port	VMS Number or System Configuration	Connects to	Port Usage
NIC 4	Redundant and non-redundant cores	Core LAN Switch 1	Transcoding
NIC 5	VMS01, VMS02, VMS09, and VMS10 in redundant and non-redundant cores	Core LAN Switch 1	Data
	VMS03	Unused	Unused
NIC 6	Redundant cores	Core LAN Switch 2	Network Management
	Non-redundant cores	Unused	Unused
NIC 7	Redundant cores	Core LAN Switch 2	Network Management
	Non-redundant cores	Unused	Unused
NIC 8	Redundant cores	Core LAN Switch 2	Transcoding
	Non-redundant cores	Core LAN Switch 1	Control
NIC 9	VMS01, VMS02, VMS09, and VMS10 in redundant cores	Core LAN Switch 2	Data
	VMS03 and non-redundant cores	Unused	Unused
NIC 10	VMS01 and VMS09 in redundant and non-redundant cores	Back side of the Backup and Restore NAS Connection Port on the Rack Extender Panel	Network Attached Storage
	VMS02, VMS03, and VMS10	Unused	Unused
NIC 11	VMS01, VMS02, VMS09, and VMS10 in redundant and non-redundant cores	CDEM	Conventional Data Encryption
	VMS03	Unused	Unused
NIC 12	VMS01, VMS02, VMS09, and VMS10 in redundant cores	Core LAN Switch 2	Intersystem Audio/Control
	VMS03 and non-redundant cores	Unused	Unused
NIC 13	VMS01, VMS02, VMS09, and VMS10 in redundant cores	Core LAN Switch 2	Control
	VMS01 and VMS09 in non-redundant cores	Core LAN Switch 1	Control
	VMS03	Unused	Unused
NIC 14	VMS01 and VMS02	Core LAN Switch 1	Firmware Download
NIC 15	Redundant and non-redundant cores	Unused	Unused
NIC 16	VMS01, VMS02, VMS09, and VMS10 in redundant cores	Peer VMS	vMotion
	Non-redundant cores	Unused	Unused

Table continued…

HP DL380 NIC Port	VMS Number or System Configuration	Connects to	Port Usage
NIC 17	VMS01, VMS02, VMS09, and VMS10 in redundant cores	Peer VMS	Fault Tolerance
	Non-redundant cores	Unused	Unused
NIC 18	VMS01 and VMS09	Back side of capture interface 1 on the Rack Extender Panel	IP Capture
	VMS02 and VMS10	Back side of capture interface 5 on the Rack Extender Panel	IP Capture
NIC 19	VMS01 and VMS09	Back side of capture interface 2 on the Rack Extender Panel	IP Capture
	VMS02 and VMS10	Back side of capture interface 6 on the Rack Extender Panel	IP Capture
NIC 20	VMS01 and VMS09	Back side of capture interface 3 on the Rack Extender Panel	IP Capture
	VMS02 and VMS10	Back side of capture interface 7 on the Rack Extender Panel	IP Capture
NIC 21	VMS01 and VMS09	Back side of capture interface 4 on the Rack Extender Panel	IP Capture
	VMS02 and VMS10	Back side of capture interface 8 on the Rack Extender Panel	IP Capture
iLO	Redundant and non-redundant cores	Core LAN Switch 1	Integrated Light Out Management

Figure 10: HP DL380 Gen9 NIC Ports for L and M Core VMS for Transcoder and ISGW

The following figure is an example. It describes the system without DAS implementation. The number of available ports and slots may vary depending on your system configuration.



©2015 Hewlett-Packard Development Company, L.P. Reproduced with permission.

Table 4: HP DL380 Gen9 NIC Port Cable Connections for L and M Core VMS for Transcoder and ISGW

The connections provided in this table apply to the following Virtual Management Servers hosting Transcoders and ISGW: VMS07, VMS08, VMS15, and VMS16.

- Redundant cores (L2, M2, M3, and M3 DSR) include all four servers.
- Non-redundant cores (L1, M1, and M1 DSR backup) include VMS07 and VMS16 only.

HP DL380 NIC Port	VMS Number or System Configuration	Connects to	Port Usage
NIC 0	Redundant and non-redundant cores	Core LAN Switch 1	Network Management
NIC 1	Redundant and non-redundant cores	Unused	Unused
NIC 2	Redundant and non-redundant cores	Core LAN Switch 1	Intersystem Audio/ Control
NIC 3	Redundant and non-redundant cores	Core LAN Switch 1	Control
NIC 4	Redundant and non-redundant cores	Core LAN Switch 1	Control
NIC 5	Redundant and non-redundant cores	Unused	Unused
NIC 6	Redundant cores	Core LAN Switch 2	Network Management
	Non-redundant cores	Unused	Unused
NIC 7	Redundant and non-redundant cores	Unused	Unused
NIC 8	Redundant cores	Core LAN Switch 2	Control

Table continued…

HP DL380 NIC Port	VMS Number or System Configuration	Connects to	Port Usage
	Non-redundant cores	Core LAN Switch 1	Control
NIC 9	Redundant and non-redundant cores	Unused	Unused
NIC 10	Redundant and non-redundant cores	Unused	Unused
NIC 11	Redundant and non-redundant cores	Unused	Unused
NIC 12	Redundant cores	Core LAN Switch 2	Intersystem Audio/ Control
	Non-redundant cores	Unused	Unused
NIC 13	Redundant cores	Core LAN Switch 2	Control
	Non-redundant cores	Core LAN Switch 1	Control
NIC 14	Redundant and non-redundant cores	Unused	Unused
NIC 15	Redundant and non-redundant cores	Unused	Unused
iLO	Redundant and non-redundant cores	Core LAN Switch 1	Integrated Lights Out Management

Figure 11: HP DL380 Gen9 NIC Ports for K Core and Other Configurations VMS

The following figure is an example. The number of available ports and slots may vary depending on your system configuration.

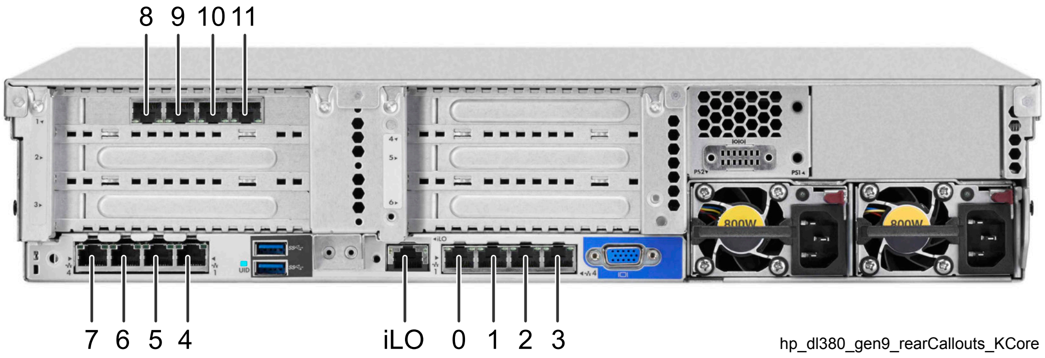


Table 5: HP DL380 Gen9 NIC Port Cable Connections for K Core and Other Configurations VMS

The connections provided in this table apply to Virtual Management Servers in system configurations without DAS.

HP DL380 NIC Port	VMS Number or System Configuration	To	Port Usage
NIC 0	K1 and K2 cores	Core LAN Switch 1	Network Management
	Other configurations	Core LAN Switch 1	Network Management
NIC 1	K1 and K2 cores	Core LAN Switch 1	Network Management
NIC 2	K1 and K2 cores	Back side of capture interface 1 on the Rack Extender Panel	IP Capture
NIC 3	K1 and K2 cores	Back side of capture interface 2 on the Rack Extender Panel	IP Capture
NIC 4	K1 and K2 cores	Back side of capture interface 3 on the Rack Extender Panel	IP Capture
NIC 5	K1 and K2 cores	Core LAN Switch 1	Data
NIC 6	K2 cores	Core LAN Switch 2	Network Management
	K1 cores	Unused	Unused
NIC 7	K2 cores	Core LAN Switch 2	Network Management
	K1 cores	Unused	Unused
NIC 8	K1 and K2 cores	Back side of capture interface 4 on the Rack Extender Panel	IP Capture
NIC 9	K2 cores	Core LAN Switch 2	Data
	K1 cores	Unused	Unused
NIC 10	K1 and K2 cores	Unused	Unused
NIC 11	K1 and K2 cores	CDEM	Conventional Data Encryption
iLO	K1 and K2 cores	Core LAN Switch 1	Integrated Lights Out Management

Figure 12: HP DL380 Gen9 NIC Ports for Trunking Subsystem Prime Site VMS

The following figure is an example. It describes the system without DAS implementation. The number of available ports and slots may vary depending on your system configuration.

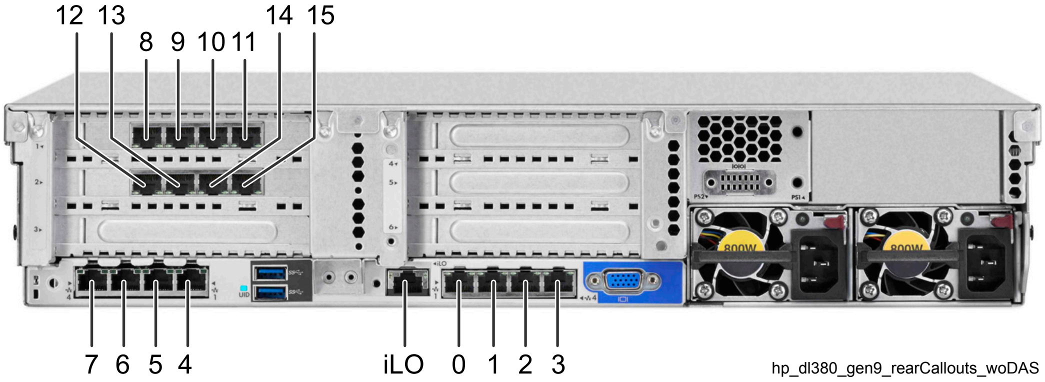


Table 6: HP DL380 Gen9 NIC Port Cable Connections for Trunking Subsystem Prime Site VMS

The connections provided in this table apply to the Virtual Management Server at the prime site in a Trunking Subsystem (Tsub).

HP DL380 NIC Port	VMS Number or System Configuration	To	Port Usage
NIC 0	VMS01	Site LAN Switch 1	Network Management
NIC 1	VMS01	Site LAN Switch 1	Control
NIC 2	VMS01	Back side of the Backup and Restore NAS Connection Port on the Rack Extender Panel	Network Attached Storage
NIC 3	VMS01	Site LAN Switch 1	Transcoding
NIC 4	VMS01	Site LAN Switch 2*	Control
NIC 5	VMS01	Site LAN Switch 2*	Transcoding
NIC 6	VMS01	Site LAN Switch 2*	Network Management
NIC 7	VMS01	Unused	Unused
NIC 8	VMS01	Back side of capture interface 1 on the Rack Extender Panel	IP Capture
NIC 9	VMS01	Back side of capture interface 2 on the Rack Extender Panel	IP Capture
NIC 10	VMS01	Back side of capture interface 3 on the Rack Extender Panel	IP Capture
NIC 11	VMS01	Back side of capture interface 4 on the Rack Extender Panel	IP Capture
NIC 12	VMS01	Unused	Unused

Table continued…

HP DL380 NIC Port	VMS Number or System Configuration	To	Port Usage
NIC 13	VMS01	Unused	Unused
NIC 14	VMS01	Unused	Unused
NIC 15	VMS01	Unused	Unused
iLO	VMS01	Site LAN Switch 1	Integrated Lights Out Management

* LAN Switch 2 connections apply to non-geographically redundant prime sites only.

Related Links

Adding the IP Packet Capture Feature to the System on page 93

A.1.2
Configuring IP Packet Capture to Capture from a Device

For IP Packet Capture to monitor traffic on a device, such as Core LAN Switch 1, connect a monitor port on the device to an interface on the extender panel of the server rack with the Virtual Management Server (VMS) hosting the IP Packet Capture virtual machine. Next, configure a packet capture definition for the interface on the extender panel to which you connected the device.

Prerequisites: Study the connection diagrams for IP Packet Capture to see the possible connections. See IP Packet Capture Connections on page 103.

Procedure:

1. Identify the monitor port on a device from which you want to take packet captures.

   For more information about switch ports and connections, see the *System LAN Switches* manual.
2. Identify an available interface on the extender panel on the VMS rack.
3. Connect an Ethernet cable between the identified monitor port and the identified interface.
4. In the IP Packet Capture user interface, configure a packet capture definition for the identified interface. See Adding Packet Captures on page 44.

Related Links

Adding the IP Packet Capture Feature to the System on page 93

A.1.3
IP Packet Capture Connections

See the following diagrams to learn about establishing connections between IP Packet Capture and capture points. The IP Packet Capture virtual machine runs on the Virtual Management Server (VMS). Ports 18-21 on the VMS are assigned to IP Packet Capture. These capture interfaces are connected to the interfaces on the extender panel on the VMS rack. Connect the capture points to the appropriate interfaces on the extender panel. Capture connections are established during staging of new systems or during upgrades of existing systems. Motorola Solutions field personnel or the system owner can change the cabling to connect other devices to enable situation-specific investigation.

Figure 13: IP Packet Capture Connections for Non-Redundant Cores

The following connections apply to non-redundant cores: K cores, L1, and M1 cores. In Dynamic System Resilience (DSR) configurations, the same connections are required in the backup core.

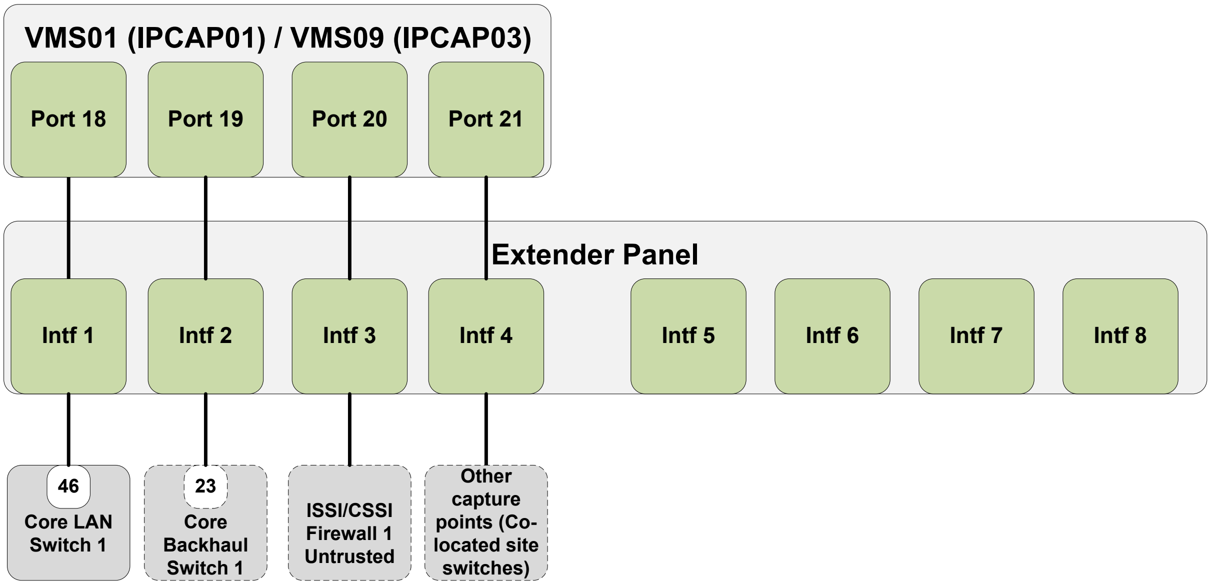


Figure 14: IP Packet Capture Connections for Redundant Cores

The following connections apply to redundant cores: L2, M2, and M3 cores. In Dynamic System Resilience (DSR) configurations, the same connections are required in the backup core.

NOTICE:
Capturing on the Mediation LAN Switch is possible only if the Intrusion Detection System (IDS) does not exist or a network tap is used to replicate monitor traffic to IP Packet Capture and IDS simultaneously.

In Dual Core DSR configurations, VMS09 and VMS10 are free to use for additional capture points, such as Core LAN Switch 3 and co-located site switches.

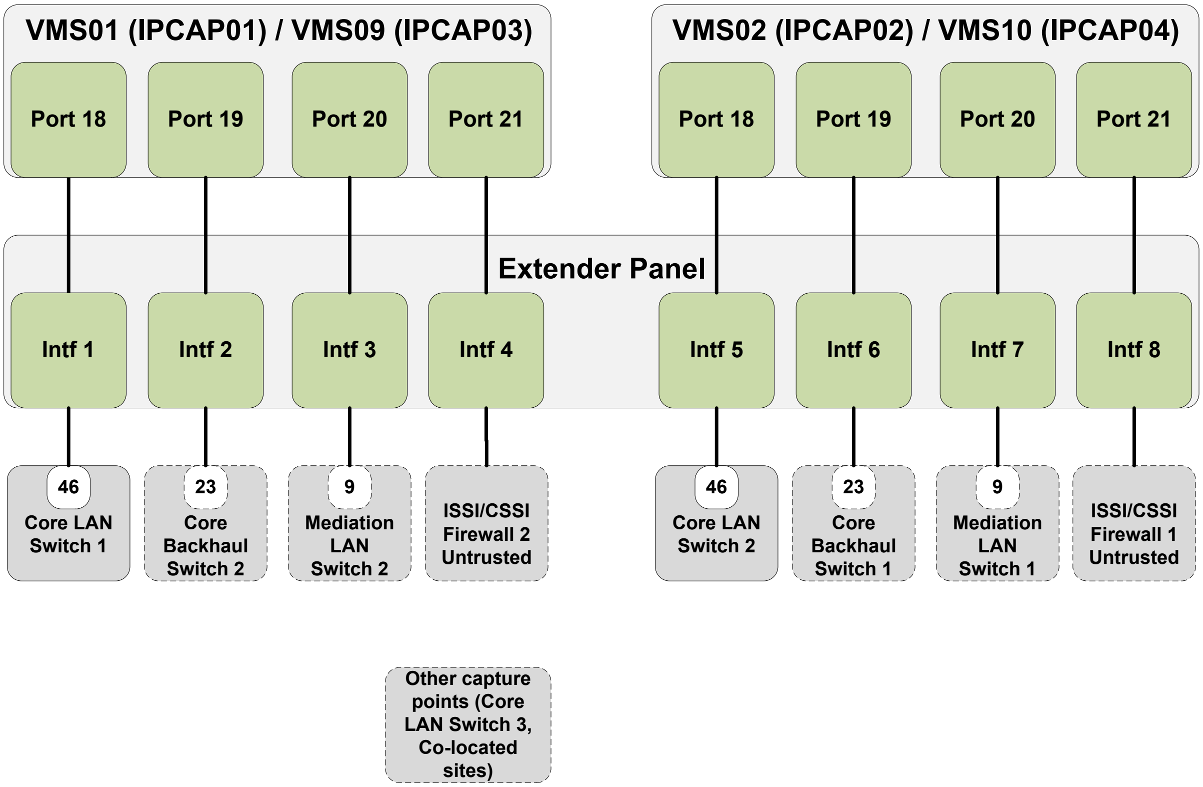


Figure 15: IP Packet Capture Connections for Trunking Subsystem Prime Sites

The following connections apply to Trunking Subsystem (Tsub) prime sites.

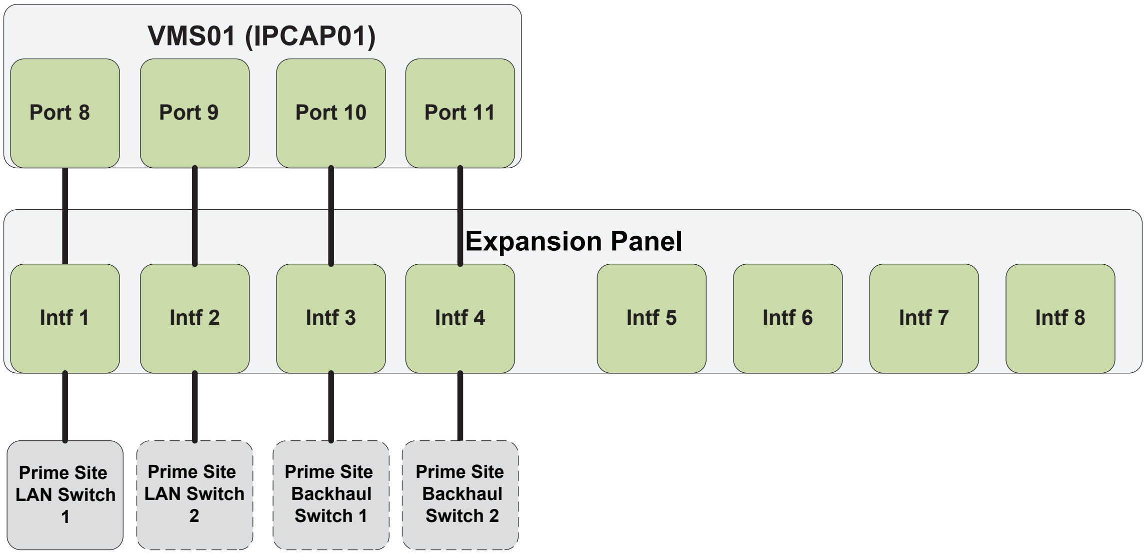
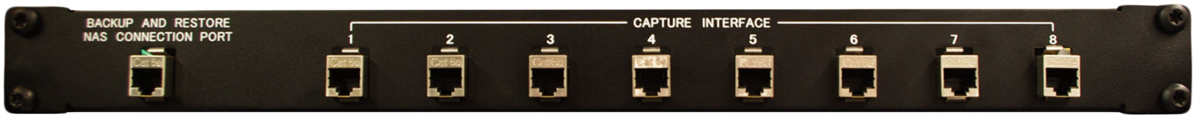


Figure 16: Extender Panel

The following diagram shows the extender panel on the VMS rack. The extender panel includes capture interfaces 1-8 for connecting devices to IP Packet Capture. An additional port provides a connection to the Network Attached Storage (NAS) connected to the Backup and Restore (BAR) server.



Related Links

Network Elements Monitored by IP Packet Capture on page 28
Adding the IP Packet Capture Feature to the System on page 93
Configuring IP Packet Capture to Capture from a Device on page 103

A.1.4

Adding Sites to the Dynamic Trusted Sites Group Policy

To complete the installation of IP Packet Capture in a Trunking Subsystem (Tsub), you have to add the addresses of the IP Packet Capture user interface to the Dynamic Trusted Sites Group Policy on the Domain Controller.

Procedure:

1. Log on to the Domain Controller using your Active Directory account that is a member of the Domain Admins group.
2. From the administrator's desktop, open PowerShell:
   - a. From **Start**, click **Search**.
   - b. In the search field, type in `powershell`
   - c. Click **Windows PowerShell**.
3. At the prompt, enter:
   ```
   cd "C:\Program Files\Motorola\AstroDC\common\scripts"
   ```
4. Add the following IP Packet Capture addresses to the dynamic trusted sites group policy:
   - a. At the prompt, enter:
     ```
     addTrustedSite.ps1 -Hostname *://z00<X>s<PPP>ipcap01.site<P>.zone<X>
     ```
   - b. At the prompt, enter:
     ```
     addTrustedSite.ps1 -Hostname *://10.<X+100>.<P>.121
     ```

   where:

   <X> is the number of the zone in which the VMS is located. The possible values are: 1–7.

   <PPP> is the 3-digit zero-padded number of the prime site in which the IP Packet Capture virtual machine is located. The possible values are: 001-064.

   <P> is the number of the Tsub prime site. The possible values are: 1-64.

Related Links

Adding the IP Packet Capture Feature to the System on page 93

A.2 Disk Share Percentages for Capture Interfaces

The following disk share percentages are recommended for the packet capture definitions that you add or edit in the IP Packet Capture application. The recommended percentages depend on the type of the zone core where IP Packet Capture is located and the number and type of devices connected to the capture interfaces for IP packet monitoring.

Identify the table appropriate for the IP Packet Capture instance that you are configuring and the zone core where the application is located. In the table, identify the row that lists the devices connected to this IP Packet Capture. Configure packet capture definitions for the monitored devices using the recommended percentages.

NOTICE: The percentages provided in the tables are not valid for IPCAP03 on VMS09 or IPCAP04 on VMS10 in Dynamic System Resilience (DSR) systems with a dual core master site. These IP Packet Capture instances may not have any monitored connections.

Table 7: Disk Share Percentage for IPCAP01 in Non-Redundant Cores

Interfaces/Switches Monitored	Core LAN Switch 1 (%)	Core Backhaul Switch 1 (%)	ISSI/CSSI (%)
Core LAN Switch 1	100	n/a	n/a
Core LAN Switch 1, Core Backhaul Switch 1	60	40	n/a
Core LAN Switch 1, Core Backhaul Switch 1, ISSI/CSSI	50	30	20

Table 8: Disk Share Percentage for IPCAP01 or IPCAP03 in Redundant Cores

Interfaces/Switches Monitored	Core LAN Switch 1 (%)	Core Backhaul Switch 2 (%)	Mediation LAN Switch 2 (%)	ISSI/ CSSI (%)
Core LAN Switch 1	100	n/a	n/a	n/a
Core LAN Switch 1, Core Backhaul Switch 2	70	30	n/a	n/a
Core LAN Switch 1, Core Backhaul Switch 2, Mediation LAN Switch 2	60	20	20	n/a
Core LAN Switch 1, Core Backhaul Switch 2, Mediation LAN Switch 2, ISSI/CSSI	50	15	15	20

Table 9: Disk Share Percentage for IPCAP02 or IPCAP04 in Redundant Cores

Interfaces/Switches Monitored	Core LAN Switch 2 (%)	Core Backhaul Switch 1 (%)	Mediation LAN Switch 1 (%)	ISSI/ CSSI (%)
Core LAN Switch 2	100	n/a	n/a	n/a
Core LAN Switch 2, Core Backhaul Switch 1	20	80	n/a	n/a
Core LAN Switch 2, Core Backhaul Switch 1, Mediation LAN Switch 1	20	40	40	n/a
Core LAN Switch 2, Core Backhaul Switch 1, Mediation LAN Switch 1, ISSI/CSSI	10	35	35	20

Table 10: Disk Share Percentage for IPCAP01 at a Trunking Subsystem Prime Site

Interfaces/Switches Monitored	Site LAN Switch 1 (%)	Site LAN Switch 2 (%)	Site Backhaul Switch 1 (%)	Site Backhaul Switch 2 (%)
Site LAN Switch 1, Site LAN Switch 2, Site Backhaul Switch 1, Site Backhaul Switch 2	25	25	25	25
Site LAN Switch 1, Site LAN Switch 2	50	50	n/a	n/a

Related Links

Adding Packet Captures on page 44
Editing Packet Captures on page 45