OSM Configuration Guide

HP Part Number: 527273-040
Published: February 2014
Edition: J06.03 and subsequent J-series RVUs and H06.03 and subsequent H-series RVUs

Legal Notice

Contents

About This Document

This guide introduces the HP NonStop™ Open System Management (OSM) Interface, the required system management tool for HP Integrity NonStop NS-series servers and HP Integrity NonStop BladeSystems. Beginning with T0682 H02 ABI, the OSM server supports both H-series and J-series RVUs, while a separate version continues to support G-series. Likewise, this manual describes OSM for H-series and J-series; a separate version describes OSM for G-series. This manual describes OSM requirements and how to install, configure, and start OSM components and processes. Since Compaq TSM does not support H-series and J-series RVUs, this manual does not cover TSM migration issues, as the G-series version does.

Supported Release Version Updates (RVUs)

This manual supports both J06.03 and subsequent J-series RVUs and H06.03 and subsequent H-series RVUs until otherwise indicated in a replacement publication.

Intended Audience

This guide is intended for anyone who uses OSM to monitor or service NonStop BladeSystems or NonStop NS-series servers.

New and Changed Information in This Edition

- "Current Release Highlights" (page 9) section updated for new H06.28/J06.17 support.
- Clarified instructions under "Requirements for Generating and Activating a Private SSL Certificate" (page 23) and also step 7 under "Example: How To Generate a Private SSL Certificate Using OpenSSL" (page 26) to ensure that the desired Subject Alternative Names are included in the signed certificate.
- Updated information for using the NonStop Maintenance LAN DHCP DNS Configuration Wizard under "NonStop Maintenance LAN DHCP DNS Configuration Wizard" (page 70).

For a complete list of enhancements and fixes to individual OSM components, such as the OSM Service Connection or OSM Low-Level Link, see the product softdoc or online help available within each OSM application.

Recent H- and J-Series OSM Change Highlights

OSM changes for H06.27/J06.16

OSM T0682 H02 ADF added support for:

- OSM process files need to be added to the TACLCSTM exceptions in order for OSM to work properly, see "Adding OSM Process Files to TACLCSTM and CMON Exceptions" (page 14).
- OSMCONF options to disable all but selective remote notifications (dial-outs), see "Disabling Alarm Remote Notification (Dial-out) " (page 16).
- OSM certificates to use SHA1 (instead of MD5), see "Requirements for Generating and Activating a Private SSL Certificate" (page 25).
- New Get SMARTSSD Wear Status Summary guided procedure, see "OSM Guided Procedures and Service Actions" (page 61).
- Encryption and logon notes, see "Launching and Logging On" (page 68)

OSM changes for H06.26/J06.15

OSM T0682 H02 ADD added support for:

- Added the following new section: "Configuring Non-Default Users" (page 71).
- Updated note in following sections regarding the configuration of non-default users: "OSM Low-Level Link" (page 63), "NonStop Maintenance LAN DHCP DNS Configuration Wizard" (page 70), and "Down System CLIM Firmware Update Tool" (page 71).
- Updated "Configuring Secure Sockets Layer (SSL) Support" (page 22) as SSL is now enabled by default for T0682 H02 ADD (or later).
- Updated "Functional Differences" (page 68) to include the time-stamped enhancement.
- Updated "OSM Client-Based Applications" (page 38) to include new Apache OpenOffice tool.
- Updated the requirements in "System Console Requirements" (page 11).
- Updated some of the logging steps in "Logging On" (page 60).

OSM Changes for H06.25/J06.14

OSM T0682 H02 ACZ added support for:

- Support for HP Integrity NonStop NS2100 servers.
- A new guided procedure to make the replacement of CLIMs and CLIM Hard Drives more automated, see Table 2 (page 62).
- Support for "Suppressing BladeCluster Alarms" (page 52) – a new Place Local Node in Service action on the BladeCluster object can be performed to prevent all other directly-connected nodes from remotely notifying (dialing out) an alarm as soon as SNETMON is stopped or the node is halted.
- Support for "Suppressing Specific Alarms" (page 17) based on a specific problem and resource name, by adding an OSMCONF parameter.
- Support for "Specifying Alternate Collector for OSM Event Viewer" (page 16), by adding an OSMCONF parameter.
- Support for "Binding to an IP Address and Stack for OSM when Sending Indications" (page 17), by adding an OSMCONF parameter.
- Updated "Configuring Additional TCP/IP Processes for OSM Connectivity" (page 18).
- Updated "Example: How To Generate a Private SSL Certificate Using OpenSSL" (page 26)
- Updated the Subject Alternate Name (SAN) description and added an example in "Requirements for Generating and Activating a Private SSL Certificate" (page 23)
- Updated "HP Systems Insight Manager (SIM)" (page 39) and "HP Insight Control Power Management" (page 39).

OSM Changes for H06.24/J06.13

OSM T0682 H02 ACV added support for:

- Support for using IPv6 on the operations LAN, including an OSMCONF setting for "Enabling IPv6 Support" (page 32).
- Support for Core Licensing on HP Integrity NonStop BladeSystems NB54000c and NB54000c-CG . For information on related attributes and actions (including a new guided procedure), see the OSM Service Connection online help.
- Support for NonStop system consoles running Microsoft Windows Server 2008.

- The "NonStop Maintenance LAN DHCP DNS Configuration Wizard" replaces the CLIM Boot Service Configuration Wizard in OSM Console Tools.
- The "Down System CLIM Firmware Update Tool" is added to OSM Console Tools.

Related Information

Document	Location
OSM Service Connection User's Guide	Available as online help from within the OSM Service Connection; also available online at http://www.hp.com/go/nonstop-docs
NonStop System Console Installer Guide	Can be found on the current NonStop System Console Installer DVD; also available online at http://www.hp.com/go/nonstop-docs
HP SIM and SIM plug-in documentation	The best starting point for using HP SIM in the NonStop environment is *HP SIM for NonStop Manageability*, which can be found in the H- and J-series collections at http://www.hp.com/go/nonstop-docs. For information on installing HP SIM, see the *NonStop System Console Installer Guide*, which can be found on the current NonStop System Console Installer DVD or online at http://www.hp.com/go/nonstop-docs. For more general information on using HP SIM, consult the online help or the standard HP SIM documentation for the version you are using. Go to http://www.hp.com/go/insightfoundation-manuals and search on "HP SIM" and select the appropriate version.
The hardware installation manual for your NonStop NS-series server or NonStop BladeSystem.	Describes how to install and start that NonStop system for the first time. It includes information about installing server hardware, cabling system enclosures, installing and starting system consoles, installing external system devices, starting the server, and configuring the server after startup.

For information on configuring and using the other OSM applications, see the online help within each of the applications. The online help is available from the Help menu of each application. To access context-sensitive help topics (specific to the task or resource selected), click Help button or press the F1 key with a GUI element selected. Online help is also available within each OSM guided procedure.

Publishing History

Part Number	Product Version	Publication Date
520573–040	OSM T0682 H02 ADH	February 2014
520573–039	OSM T0682 H02 ADF	August 2013
520573–038	OSM T0682 H02 ADD	February 2013

HP Encourages Your Comments

HP encourages your comments concerning this document. We are committed to providing documentation that meets your needs. Send any errors found, suggestions for improvement, or compliments to:

pubs.comments@hp.com

Include the document title, part number, and any comment, error found, or suggestion for improvement you have concerning this document.

1 Introduction to OSM

The NonStop Open System Management (OSM) suite of products are the required system management tools for all NonStop NS-series servers and NonStop BladeSystems; TSM is not supported on H-series or J-series.

Primary Goals

- Provide a system management tool suite to support Integrity NonStop NS-series servers and NonStop BladeSystems.
- Replace TSM on S-series as well, providing an architecture to improve scalability and performance and overcome other limitations of TSM.
- Provide an open, standards-based interface for HP NonStop Kernel operating system hardware object access and monitoring.
- Serve as the basis for integration to other HP organizations and products such as "HP Systems Insight Manager (SIM)", "HP Insight Remote Support Advanced", NonStop Essentials products, and HP OpenView.

Major Benefits

- Smaller client, faster installation (most components reside on the server)
- Online upgrades for client and providers
- Better persistence because OSM runs as a process pair
- Faster, more accurate status and alarm updates for resource objects
- DMTF/CIM* interface to make OSM more open and adaptable (to facilitate application and provider add-ons)

  * Common Information Model (CIM) is a standards-based, data architecture model developed by the Distributed Management Task Force (DMTF).

Current Release Highlights

For H06.28/J06.17, OSM Service Connection version T0682 H02 ADH and OSM Low-Level Link version T0633 G07 ABT were released to add support for HP Integrity NonStop NS2300 servers and NS2400 series servers. Those versions, or later, are required to manage those NonStop system types.

Support for NonStop Essentials Products

OSM supports these NonStop Essentials products, which are HP SIM plug-ins:

- NonStop Cluster Essentials – an integrated cluster management solution for heterogeneous clusters, it supports clusters consisting of all NonStop servers as well as rack-mount or BladeSystem ProLiant servers running Red Hat Linux. OSM is a vital component because while NonStop Cluster Essentials allows high-level monitoring of your NonStop servers along with other HP servers in the HP SIM interface, OSM provides the system status to HP SIM and is used by the operator for more detailed monitoring and servicing of the NonStop servers as needed. For more information, see the *NonStop Cluster Essentials Installation and Quick Start Guide*.
- NonStop I/O Essentials – virtualizes the configuration and control of all CIP (Cluster I/O Protocols) tasks by providing a graphical user interface alternative to the command line

interfaces of the climcmd tool and SCF. For more information, see the *NonStop I/O Essentials Installation and Quick Start Guide*.

- NonStop Software Essentials – a software installation and management tool for NonStop servers, providing a replacement for the DSM/SCM Planner Interface and certain Host Maintenance Interface functions that is more secure, easier to use, and overcomes other shortcomings of DSM/SCM. For more information, see the *NonStop Software Essentials Installation and Quick Start Guide*.

OSM Client Interfaces

OSM contains these system management applications and tools.

- OSM Service Connection – A Java-based application, with client and server delivered on a site update tape (SUT) and accessed from a system console or qualified PC through a Microsoft Internet Explorer browser session.
- OSM Guided Procedures and Service Actions – Integrated into the OSM Service Connection, they are launched by actions from within the application (rather than separately through the Start menu) and provide documentation and automation (where possible) to guide you through hardware replacements and other serviceability tasks.
- OSM Event Viewer – Also a browser-based application, the OSM Event Viewer allows you to retrieve, view, and save EMS events from event logs. It also provides event details such as cause, effect, and recovery information.
- OSM Low-Level Link – Designed primarily for down-system support, it is used to configure CLIMs and other new modules, update CLIM software and firmware, and update HSS firmware for most J-series systems.
- OSM System Inventory Tool – Installed as part of the OSM Console Tools. It allows you to create and save hardware or firmware inventory data from one or more NonStop systems running OSM.
- Terminal Emulator File Converter – Installed as part of the OSM Console Tools, this tool converts your OSM Service Connnection-related OutsideView session files to an MR-Win6530-compatible format.
- OSM Certificate Tool – Installed as part of the OSM Console Tools (but used for J-series only), this tool creates certificates necessary to establish a trust relationship between OSM and the Onboard Administrators (OAs) in the blade enclosures. For more information, see the online help available within the OSM Certificate Tool.
- NonStop Maintenance LAN DHCP DNS Configuration Wizard – Installed as part of the OSM Console Tools, it can be used to configure and manage DHCP and DNS services on your dedicated service LAN or migrate those services, as well as BOOTP services for most J-series systems between NonStop system consoles and CLIMs.

For more information on individual OSM applications, see Section 5, Getting Started With OSM Applications or the online help within each application or guided procedure.

2 Preparing for OSM

This section describes how to prepare for migration to OSM software, including:

- "System Console Requirements" (page 11)
- "Server Software Requirements" (page 11)
- "Preparing the Hardware and LAN Environment" (page 12)

System Console Requirements

NonStop system consoles used to manage NonStop NS-series servers or NonStop BladeSystems must be running Microsoft Windows Server 2003 or Windows Server 2008, as configured and shipped by HP. Those consoles will meet memory requirements for using OSM and NSC console software. For more information, see the *NonStop System Console Installer Guide*.

While it is recommended to install HP SIM and SIM plug-ins, such as Insight Remote Support Advanced, on a separate Central Management Server (CMS), installing those products on a qualified NonStop system console is supported. For more information, see *HP SIM for NonStop Manageability*, located in the NonStop Technical Library.

Java Runtime Environment (JRE) version required by OSM -- When you install OSM Console Tools from the NonStop System Console DVD, the installer will automatically download the version of JRE required for the OSM System Inventory Tool. In the event that your version of the OSM Service Connection requires a newer JRE version, you will be prompted to download and install it from the NonStop system when you attempt to establish an OSM Service Connection.

OSM Server Version	Minimum Required Java Runtime Environment Version
Before T08682 ACN	Java 6 Update 7
Starting with T08682 ACN (H06.23 & J06.12)	Java 6 Update 24
Starting with T08682 ADD	Java 6 Update 35, but not Java 7

NOTE: OSM does not support Java 7 at this time.

To use OSM software on other PC-based consoles, they must meet the following minimum requirements:

- Microsoft Windows XP Professional, Microsoft Windows Server 2003, or Microsoft Windows Server 2008 operating system
- Minimum processor for Windows XP-based console: at least 1 GB of memory
- Minimum processor for Windows Server 2003 or Windows Server 2008 console, if HP Insight Remote Support Advanced is installed on it: at least 4 GB of memory.
- Internet Explorer 6.0 or later is required for the browser-based OSM applications. The latest supported version is available, , along with all other client software needed by OSM, from the HP NonStop System Console Installer DVD.

Server Software Requirements

For both H-series and J-series RVUs, there are no prerequisites for using OSM. The OSM Service Connection Suite (T0682) and all server-based requisites are on the SUT.

Section 3, OSM Server-Based Components, describes how to configure and start OSM server processes.

Section 4, OSM and Other HP Client-Based Components, describes the OSM client-based SPRs.

Preparing the Hardware and LAN Environment

While most OSM functionality should be used only on a dedicated service LAN, some components can be used on a nondedicated operations LAN. To use OSM on a nondedicated operations LAN, see "Configuring Additional TCP/IP Processes for OSM Connectivity" (page 18).

For more information on preparing and configuring your NonStop environment, see the appropriate planning guide and hardware installation manual for your NonStop NS-series server or NonStop BladeSystem.

3 OSM Server-Based Components

This section provides information about OSM server-based components:

OSM Server-Based SPR

For both H-series and J-series RVUs, the lone OSM server-based component is the OSM Service Connection Suite (T0682). It encompasses the following OSM SPRs (that were once individual SPRs on G-series RVUs):

Table 1 OSM SPRs replaced by T0682

- T2723 (OSM Connection Library)
- T2724 (OSM Provider Interface Library)
- T2725 (OSM Configuration)
- T2726 (OSM XML API)
- T2727 (OSM CIMOM)
- T2728 (OSM Service Provider)
- T2730 (OSM Event Viewer)
- T2751 (OSM Web-Based Suite)

If you are installing OSM for the first time, use either NonStop Software Essentials or DSM/SCM for migrating to a new RVU or adding SPRs to your current RVU, as described in the appropriate H- or J-series *Software Installation and Upgrade Guide*.

Section 4, OSM and Other HP Client-Based Components, describes the OSM client-based SPRs.

Ports Used by OSM

These are the default ports used by OSM:

- 9990 – OSM web server ($ZOSM) opens this port to communicate with OSM Service Connection.
- 9991 – OSM Event Viewer web server ($ZOEV) opens this port to communicate with OSM Event Viewer client.
- 5988 – OSM CIMOM process ($ZCMOM) opens this port to communicate with OSM Service Connection, if OSM is running in non-SSL mode.
- 5989 – OSM CIMOM process ($ZCMOM) opens this port to communicate with OSM Service Connection, if OSM is running in SSL mode.

Adding OSM Process Files to TACLCSTM and CMON Exceptions

A TACLCSTM script which expects direct human interaction will interfere with certain OSM actions and activities. Some OSM processes start TACLs which are non-interactive, with the user ID of the OSM Service Connection session, or with the SUPER.SUPER ID for unattended OSM operations. The most likely issues to be noticed without previous planning occur for a shared service user id. Issues are also possible for the SUPER.SUPER user ID.

If an interactive script is part of the TACLCSTM file, you must grant exceptions to TACL sessions that the program files SEEVIEW, CIPPRVD, MDEVPRVD, and EVTL create. These program files launch TACL sessions on behalf of OSM commands or for unattended background activities.

A customized CMON exerts additional control over TACL processes. In some cases, you will also need to grant CMON exceptions for TACL processes created by SEEVIEW, CIPPRVD, MDEVPRVD, and EVTL.

OSM uses the SEEVIEW program file to launch TACL processes for some OSM actions. These actions include CLIM and Disk Enclosure firmware updates, "Set LED State" for a SAS Disk Enclosure or CLIM Attached Disk, and CLIM rediscover. If there is a problem caused by an interactive TACLCSTM, these OSM actions can appear to hang "In Progress" in the OSM user interface. If you suspect this problem arises from TACLCSTM interactions for a particular user ID, start a new OSM session with a different user ID and use the "Set LED State" or CLIM rediscover command to test your suspicions.

OSM also creates TACL processes directly from the program files CIPPRVD, MDEVPRVD, and EVTL for other activities. For example, MDEVPRVD can start a TACL as SUPER.SUPER to run a customer-supplied script as part of Power Fail shutdown. This activity occurs in the background without the possibility of human user interaction. EVTL starts a TACL to automatically configure Expand line handlers for remote systems added into a ServerNet Cluster.

These TACLCSTM and CMON issues for OSM usually begin as a consequence of improved security auditing of TACL sessions. User-initiated OSM actions are audited in the $system.zservice.ztrc* files. There is OSM auditing of user-issued OSM actions invoking TACL even when exceptions are in place for the usual TACL session auditing.

An engineer from your service provider usually logs on to tools such as the OSM Service Connection or TACL with a specific NonStop user ID in the SUPER group. Your security group might want to audit the use of this shared service user ID, or audit the use of the SUPER.SUPER ID. The TACLCSTM file for one or more user IDs might call an interactive script which verifies the identity of the particular individual working on the system.

In this example, TACLCSTM for SUPER.SERVICE calls an interactive XYGATE Access Control (XAC) script named super-service-tacl for direct human use of TACL. Grant a TACLCSTM exception for OSM as follows:

```
?tacl macro
== TACLCSTM for SUPER.SERVICE.
#push ancestor programfile
#set ancestor [#lookupprocess /ancestor/ [#processinfo /processid/]]
 #set programfile [#processinfo/programfile/ [ancestor]]
== Grant exceptions to TACL processes created for OSM actions and activities.
[#if ([#match *SEEVIEW [programfile]]) or
        ([#match *CIPPRVD [programfile]]) or
       ([#match *MDEVPRVD [programfile]]) or
       ([#match *EVTL [programfile]])
== Add any other special conditions such as a XYGATE terminal already audited.
|then|
== Skip XAC command.
|else|
       xac super-service-tacl
== Add any additional processing after XAC.
]
== Add any additional TACLCSTM code.
== Avoid redefining basic TACL behavior, interfering with OSM use of TACL.
```

```
...
#pop ancestor programfile
```

Refer to the *Guardian Programmer's Guide* for more information about CMON.

Optional OSM Configuration

It is not necessary to create a configuration file to use OSM with the default settings. However, if you want to alter any default settings or take advantage of the following OSM features, you must create and use an OSMCONF file:

For information on how an administrator for a maintenance switch or UPS changes the default SNMP access configurations for those devices, see Appendix E, Configuring SNMP Access for Monitored Service LAN Devices.

Creating and Using an OSMCONF File

OSMINI is a template file delivered as part of T0682, to assist you in creating your own (optional) customized OSMCONF file. Because the OSMCONF file is user-created and not installed by OSM, when you upgrade to a new T0682 SPR, your customized settings are not overwritten.

To create an OSMCONF file from an OSMINI template file and to put your configuration changes into effect:

1. Go to $SYSTEM.ZSERVICE and copy OSMINI to create a new file named OSMCONF.
2. Edit the OSMCONF file to customize the default settings as desired. To avoid possible problems, delete blank lines from the OSMCONF file.

3. When you start OSM server processes, configuration settings are read from the OSMCONF file if one exists in that location. If not, OSM default settings are used. To change your settings after OSM is running, select Reload Configuration Settings from the OSM Service Connection Tools menu. To complete this operation, you are instructed to restart the $ZOSM and $ZOEV processes.

If you are already using a customized OSMCONF, and an updated OSMINI template (with new settings that you want to take advantage of) is released, you can either:

- Copy those particular settings (such as the setting for "Enabling Enhanced Redundant Power Scrub") into your existing OSMCONF file, and customize as needed; or
- Use the OSMINI to create a new OSMCONF (in which case you would then have to redo any changes you made to default settings in your previous OSMCONF).

To take advantage of new functionality that is enabled by default (such as Creation of System Inventory Files), you do not have to add those settings to your OSMCONF file; OSM uses default settings unless you override them in an OSMCONF file.

Specifying Alternate Collector for OSM Event Viewer

In the OSM Event Viewer, $ALOG is the default name for the alternate collector when using the Save View as EMS Log action. However, if `oevprvd` is idle for 20 minutes and times out, its processes, including $ALOG, are terminated. With OSM version T0682 H02 ABZ and later, you can prevent this by specifying a different process name to be used by `oevprvd` through the `AltEventCollectorProcessName` parameter in your OSMCONF file, as follows:

```
AltEventCollectorProcessName = $alt_name
```

Where *$alt_name* is the process name that `oevprvd` will use.

This allows you to use $ALOG as your own collector process name.

Disabling Alarm Remote Notification (Dial-out)

You can disable all dial-outs using a specific `OSMCONF` flag. You can also specify alarms that should not be disabled from dialing out. By default, the alarm dial-out disabling is disabled.

NOTE: Some alarms will always be dialed out. For example, the `Denial of Service Attack` alarm will always be dialed out.

You can disable alarm dial-out by adding `disableAllDialout = YES` in the `OSMCONF` file and then run the Reload Configuration Settings or restart CIMOM.

To disable alarm dial-out, use the following flags:

Configuration Flag and Value	Description
`disableAllDialout = YES`	Disables all alarm dial-outs unless the specified alarm is indicated in the `enableDialout` or `enableDialoutPrefix` flag.
`enableDialout = <alarm description>`	Enables the dial-out of the specified alarm if `disableAllDialout = YES` and the alarm description is the same as `<alarm description>`.
`enableDialoutPrefix = <alarm description prefix>`	Enables the dial-out of an alarm with the specified prefix if `disableAllDialout = YES` and the alarm's description starts with `<alarm description prefix>`.

Example: Disabling all Alarm Dial-outs

To disable all alarm dial-outs, add the following line in the `OSMCONF` file:

```
disableAllDialout = YES
```

This will disable all alarm dial-outs except for a few alarms that are always dialed out.

Example: Disabling all Alarm Dial-outs Except a Specified Alarm

To enable the dial-out of a specified alarm (for example, `Too Many Router Port Errors`) but disable the dial-outs of all other alarms, add the following lines to the `OSMCONF` file:

```
disableAllDialout = YES
enableDialout = Too Many Router Port Errors
```

Example: Disabling all Alarm Dial-outs Except an Alarm with a Specified Prefix

To enable the dial-out of an alarm (for example, `Loss of ServerNet Fabric X for Processor 3`), with a specified prefix (for example, `Loss of ServerNet Fabric`) but disable the dial-outs of all other alarms, add the following lines to the `OSMCONF` file:

```
disableAllDialout = YES
enableDialoutPrefix = Loss of ServerNet Fabric
```

You can re-enable remote notifications (dial-outs) by removing `disableAllDialout = YES` from the `OSMCONF` file and then run Reload Configuration Settings or restart CIMOM. This will not, however, cause alarms generated prior to this point to dial-out.

Suppressing Specific Alarms

With OSM version T0682 H02 ABV and later, you can specify that a specific alarm not be created or dialed out for that system through use of the `NoAlarm` OSMCONF parameter, as follows:

```
NoAlarm = alarm_description
```

Where *alarm_description* is the exact description of the alarm as displayed in the alarm description field.

For example, if you do not want the `Loss of Running Processor` alarm to be created or dialed out, place the following setting in your OSMCONF:

```
NoAlarm = Loss of Running Processor
```

With OSM version T0682 H02 ABZ and later, the `NoAlarm` OSMCONF parameter is enhanced, allowing you to suppress alarm creation and dial out for a specific resource. By adding a specific resource name in parentheses following (separated by a space) the alarm description, you would suppress the alarm only on that resource. In the example above, the `Loss of Running Processor` alarm would be suppressed on all Logical Processors on the system. However, by adding the name of a specific resource, as shown below, you suppress that alarm only on that Logical Processor.

```
NoAlarm = Loss of Running Processor (Logical Processor 4)
```

You must specify the resource name as shown in the OSM Service Connection. In another example, to suppress the `Loss of ServerNet Fabric X` alarm on Node (1.4), the OSMCONF setting would be:

```
NoAlarm = Loss of ServerNet Fabric X (Node (1.4))
```

To make changes to your OSMCONF file take effect, see "Creating and Using an OSMCONF File" (page 15). To remove this type of suppression, simply remove the specific `NoAlarm` parameter from your OSMCONF file and repeat the process for making changes to your OSMCONF file take effect.

Binding to an IP Address and Stack for OSM when Sending Indications

You can specify a source IP address and stack for OSM to use when sending indications to HP SIM and Insight Remote Support Advanced/WEBES. This configuration flag does not affect the OSM Service Connection client. The source stack name and IP address are required, while the destination IP address and port parameters are optional and only needed if different destinations require different source IP addresses.

Edit the OSMCONF file to specify the source stack name, IP address, destination IP and port:

```
IndicationSource=source stack name>,source IP[,destination IP[,destination port]]
```

Source stack name	TCP/IP process name to use. The value of the stack entries in the OSMCONF file (see "Configuring Additional TCP/IP Processes for OSM Connectivity" (page 18)) should not be more restricted than this one.
Source IP	IP address that OSM will bind to when sending the indication. The values of the stack entries in the OSMCONF file (see "Configuring Additional TCP/IP Processes for OSM Connectivity" (page 18)) should be chosen to allow use of the desired *Source IP* entry.
Destination IP	Optional parameter used to restrict this entry to only apply to one destination.
Destination Port	Optional parameter used to restrict this entry to only apply to one port on the specified destination IP. *Destination IP* is required when *Destination Port* is specified.

Multiple source IP addresses may be specified by using multiple IndicationSource flags. If there are multiple source IP addresses specified, OSM will try to send from each of them until it has either failed with all source IP addresses or it successfully sends to the endpoint.

If there are any IndicationSource flags specified, OSM will only use the IndicationSource flags for sending indications, any stack flags specified will only be used for incoming connections.

NOTE: OSM will always attempt to send via $ZTCP0 and $ZTCP1. If there is at least one matching IndicationSource flag, the IndicationSource flag(s) will be attempted first, then $ZTCP0 and $ZTCP1.

Configuring Additional TCP/IP Processes for OSM Connectivity

OSM has two default TCP/IP processes, $ZTCP0 and $ZTCP1, which are used for OSM Service Connection and OSM Event Viewer connectivity. The physical connections (two for fault tolerance) are made through either a Gigabit 4-port ServerNet adapter (G4SA) in an IOAM or VIO enclosure or an E4SA, FESA, or GESA in an attached S-series IOMF2 CRU. OSM Low-Level Link connectivity for NS-series servers is established through the maintenance entity (ME) of the ServerNet switch board in each p-switch (using the IP address of the p-switch). This section describes how to configure (optional) additional TCP/IP processes for OSM Service Connection and OSM Event Viewer connectivity.

Edit the OSMCONF file to specify TCP/IP processes other than the default $ZTCP0 and $ZTCP1 processes for use by the OSM Service Connection, HP SIM, or Insight Remote Support Advanced:

```
stack = <TCPIP process name>
stack = <TCPIP process name 2>
```

For example:

```
stack = $ZTC00
stack = $ZTC01
```

To specify TCP/IP processes other than the default $ZTCP0 and $ZTCP1 for use by the OSM Event Viewer, add the following additional lines to OSMCONF:

```
evtstack = $ZTC00
evtstack = $ZTC01
```

The stack and evtstack entries are independent. Use of the stack entry by itself does not affect IP addresses available for the OSM Event Viewer.

Both the OSM Service Connection and the OSM Event Viewer automatically work with the IP addresses for $ZTCP0 and $ZCTP1. No additional entry is required.

NOTE: You can use the `stack` parameter with syntax `<TCPIP process name>:<specific IP address>` to control the specific server IP addresses used by the OSM Service Connection, HP SIM, or Insight Remote Support Advanced. The OSM server will not allow connections to other IP addresses. For OSM Service Connection sessions, this parameter affects both the URLs allowed for the initial connection to the OSM Server, and additional TCP/IP connections opened afterwards for realtime updates and fault tolerance.

The feature of restricting the OSM stack to specific IP addresses is available only with T0682ACV and later SPRs of T0682.

You can specify multiple specific IP addresses for a single TCP/IP process name by using more than one `stack` entry, each with an additional IP address for a single TCPIP process name. A single `stack` entry for a TCP/IP process name without any `:<specific IP address>` will cause the OSM server to permit use of any of the NSK IP addresses associated with that TCP/IP process name.

There could be many NSK Server IP addresses associated with a TCP/IP process name, especially when using IPv6. You may use an SCF command such as `SCF INFO SUBNET <TCPIP process name>.*` to see associated IP addresses.

For example, OSM Service Connection attempts to use all of the addressable IP addresses configured in SCF for TCP/IP processes $ZTC0 and $ZTC1 after configuring the following entries in the OSMCONF file:

```
stack = $ZTC0
stack = $ZTC1
```

In order to restrict OSM connections to two specific IP addresses for $ZTC0, while allowing OSM to use all addressable IP addresses for $ZTC1, use the following entries:

```
stack = $ZTC0:<IP address A>
stack = $ZTC0:<IP address B>
stack = $ZTC1
```

The additional IP address may be written in IPv4 dotted octet form or in IPv6 form with sequences of 4 hexadecimal digits separated by the : character. Do not specify IPv6 addresses unless the additional TCPIP/IP process supports IPv6 and you have enabled OSM use of IPv6. See "Enabling IPv6 Support" (page 32).

There is no point in specifying specific IP addresses in OSMCONF for the default IPv4 $ZTCP0 and $ZTCP1 TCP/IP processes, since only one address is available for each of these TCP/IP processes.

Like any changes to OSM configuration defaults, these changes are most easily enabled if you restart the affected OSM processes ($ZOSM and $ZCMOM, named $ZZKRN.#OSM-APPSRVR and $ZZKRN.#OSM-CIMOM in SCF.)

In the OSMCONF file, the `evtstack` parameter applies to the OSM Event Viewer and its server processes $ZOEV. The syntax for specifying only a specific IP address or addresses is the same as for the stack flag:

```
evtstack = <TCPIP process name>:<IP address>
```

Restart $ZOEV ($ZZKRN.#OSM-OEV in SCF) for the `evtstack` change to take effect.

Configuring OSM to Monitor Devices Not on the Dedicated Service LAN

You can configure OSM to monitor a system device (storage router, UPS, maintenance switch, Onboard Administrators, or CLIM) located outside of the dedicated service LAN ($ZTCP0/$ZTCP1) by adding additional TCP/IP stacks to your OSMCONF file as follows:

```
MaintenanceStack = $ZTC00
MaintenanceStack = $ZTC01
```

To make changes to your OSMCONF file take effect, see "Creating and Using an OSMCONF File" (page 15).

Enabling Enhanced Redundant Power Scrub

For T0682 H02 ABE and later, an enhanced version of the Redundant Power Scrub test is available for legacy S-series enclosures. It provides independent battery testing and an extended load test for the bulk power supplies.

NOTE: With this new version of Redundant Power Scrub, the action can take up to 25 minutes to complete. The new battery scrub is significantly enhanced in its ability to detect weak or failed batteries. For systems with many old batteries (over 5 years old), the battery scrub might call out multiple batteries for replacement

This enhanced version of the Redundant Power Scrub must be enabled in your OSMCONF file, but not until these prerequisites are met:

- All enclosures must be updated with a new PIB-to-PIB crossover cable (see FCO 44440 for details).
- OSM T0682 H02 ABE or later is installed.

Once the prerequisites are met, add this entry into your OSMCONF file:

```
PowerScrubVersion = 3
```

The default test interval for this new version is 7 days instead of every 24 hours (as was the default for the older version). HP recommends leaving the default as 7 days unless an event requires a reduced time between scrubs.

To change the test interval for the enhanced Redundant Power Scrub test, add this entry into your OSMCONF file:

```
DailyScrubTestingInterval = n
```

To make changes to your OSMCONF file take effect, see "Creating and Using an OSMCONF File" (page 15).

Disabling Creation of System Inventory Files

For T0682H02 AAM and later, OSM has automatic system inventory file creation enabled by default. With this feature enabled, system inventory files are created whenever Periodic Incident Reports (IRs) are created, and attached to these IRs if the "Suppress Attachment files on Periodic IRs" option is deselected in the OSM Notification Director Preferences dialog box.

NOTE: A system inventory file will not be created if a Periodic IR is generated before OSM completes system discovery.

To disable automatic creation of system inventory files, you must set the following OSMCONF parameter to "OFF:"

```
INVENTORY_STATE = ON
```

The "ENABLE_INVENTORY = ON" parameter used to configure system inventory files in earlier OSM releases no longer has any effect and should be removed from your OSMCONF file. The current "INVENTORY_STATE = ON" parameter can be copied to an existing OSMCONF from the OSMINI template provided with T0682 AAM or later.

To create an OSMCONF file from the OSMINI, or to put OSM configuration file changes into effect when OSM processes are already running, see "Creating and Using an OSMCONF File".

For information on initiating Periodic incident reports and viewing attachment files, see the OSM Notification Director online help.

This automatic system inventory feature should not be confused with the standalone OSM System Inventory Tool, which can be used to create inventory files from multiple NonStop systems (see "OSM System Inventory Tool" (page 69).

Configuring Automatic Data Collection

For T0682H02 AAM and later, OSM has enhanced automatic data collection capabilities. If enabled, OSM automatically collects diagnostic data whenever a hardware failure causes a Problem Incident Report (IR) to be created.

Automatic data collection is enabled through the Enable/Disable Automation of Data Collection action, located under the system object in the OSM Service Connection. It is configured through a combination of OSMCONF file settings and Service Connection actions. To customize the OSMCONF file default settings, you can create an OSMCONF file from the OSMINI included with T0682H02 AAM or later, or copy the following settings from the OSMINI file into your existing OSMCONF file. For more information, see "Creating and Using an OSMCONF File".

ADC-related OSMCONF Parameters	Purpose/Effect	Possible Values	Default
`AdcDelayTimeInMin`	Delay time (in minutes) between the time that the initial Problem IR is received and data collection begins. The purpose is to conduct a single data collection for all related Problem IRs.	5 to 60	15
`AdcEventTimeinHrs`	Time (in hours), prior to when the Problem IR is generated, that the data collection will collect EMS events from $ZLOG and $0.	1 to 60	12
`EnableNDData`	Enables ability to send a Diagnostic Data IR to the OSM Notification Director. (Not visible in OSM ND version T0632 AAK; however, Problem IRs also provide the location of collected data files in ZZAA alarm details.)	ON/OFF	ON
`AdcFilColTimeinMin`	Specifies the time period (in minutes), after the initial Problem IR is created, that ZZAA and ZZPS files will be collected.	5 to 120	5

The following data collection configuration is done through OSM Service Connection actions, located under the System object (rather than through OSMCONF file settings, as done in early S-series releases):

- Set Data Collection Volume* – specifies a volume in which to collect diagnostic data. The default volume is $SYSTEM.
- Set Days to persist for Diagnostic Data* – specifies how long the data files remain in the collection volume before they are automatically deleted (the default is 28 days).

* There is also an OSM Service Connection action called Collect Diagnostic Data, which collects data manually at the time you perform the action. The actions used to specify data collection volume and data file persistence also apply to the diagnostic data collected by this manual action.

The current automatic data collection settings are displayed as System object attributes, under the "Data Collection Services" heading (on the Attributes tab):

- Automatic Data Collection State (Enabled or Disabled)
- Diagnostic Data Collection Volume
- Days to Persist Collected Diagnostic Data

Disabling Alarm and Attribute Suppression Persistence

With OSM version T0682 H02 ABX and later, suppression of alarms and problem attributes is persistent by default. That means alarms or attributes suppressed in the OSM Service Connection remain suppressed even after the OSM server has been stopped and restarted. Persistence is not available in OSM versions prior to T0682 H02 ABX, meaning that all suppressed values revert to unsuppressed when the current OSM server session is ended.

For more information on what suppression means, including the difference between permanent and temporary suppression, see "Suppressing Alarms" (page 52) and "Suppressing Problem Attributes" (page 51).

To disable suppression persistence in T0682 H02 ABX and later, put the following parameter into your OSMCONF file:

```
SuppressionPersistenceAcrossOSMRestart = OFF
```

To make changes to your OSMCONF file take effect, see "Creating and Using an OSMCONF File" (page 15).

Suppressing Redundant IRs from ServerNet Cluster Nodes

With OSM version T0682 AAY and later, you can suppress ServerNet Problem IRs from being propagated to other nodes connected to a ServerNet Cluster, in order to avoid redundant Problem IRs.

For each node on which you want to suppress ServerNet Problems IRs from being propagated, this line must be entered into the OSMCONF file for that node:

```
SuppressServerNetClusterAlarm = ON
```

To make changes to your OSMCONF file take effect, see "Creating and Using an OSMCONF File" (page 15).

Configuring Secure Sockets Layer (SSL) Support

Starting with T0682H02 AAM, OSM provides Secure Sockets Layer (SSL) support to provide a secure connection between OSM server software and:

- OSM Service Connection*
- OSM Event Viewer*
- HP Systems Insight Manager (HP SIM) – SSL is required for using HP SIM and SIM plug-ins such as HP Insight Remote Support Advanced with NonStop servers. For more information on configuring Insight Remote Support Advanced, see *Insight Remote Support Advanced for NonStop*, located in the Support and Services collection of NTL.

For T0682 H02 ADD (or later), SSL is now enabled for OSM by default for all NonStop systems running H-series or J-series software; you no longer have to enable the SSL support built into OSM by adding the UseSSL parameter to your OSMCONF file.

SSL encryption and authentication depend on X509 certificates to provide keys and identify the parties involved in the communication. The SSL support built into OSM relies on a "shared" SSL certificate. For maximum security, HP recommends that you generate a private SSL certificate. OpenSSL toolkits, available as shareware, can help you generate your own SSL certificate.

With T0682 H02 ACC and later, the OSM Service Connection has updated its handling of SSL server certificates relative to the CIMOM server. The dialog that relates to the default OSM certificate has been replaced by a new dialog with slightly modified certificate rules. If you use customized server certificates, you may see a new dialog after entering user credentials related to problems that the certificate may have. You will have the option to exit from OSM due to the problems or to continue with OSM despite the problems.

Configuring the Cipher Suites Used by SSL

You can control the cipher suites used by SSL for communication between OSM server processes and OSM Service Connection, OSM Event Viewer, HP SIM, and Insight Remote Support Advanced through the following parameter in your OSMCONF file:

```
CIPHERSUITES = value
```

NOTE: This parameter is valid only on a NonStop BladeSystem or when the UseSSL parameter in the OSMCONF file is set to On.

The default value is `0.4,0.10,0.5`. The value represents three different values separated by commas. (Other combinations involving multiple values may be specified in the same comma separated fashion.) The allowed values are listed below, followed by a description of each:

- `0.4` – RSA-key-exchange + RC4-128-bit encryption and MD5 (RC4-MD5)
- `0.5` – RSA-key-exchange + RC4-128-bit encryption and SHA (RC4-SHA)
- `0.10` – RSA-key-exchange + 3-DES encryption and SHA (DES-CBC3-SHA)
- `0.47*` – RSA-key-exchange + 128-bit AES encryption and SHA (AES128-SHA)
- `0.55*` – RSA-key-exchange + 256-bit AES encryption and SHA (AES256-SHA)

* These values are not currently supported on Windows XP or Windows Server 2003.

Requirements for Generating and Activating a Private SSL Certificate

The requirements for a private SSL certificate include:

- The certificate's Subject Common Name (CN) must include the DNS name or IP address configured for OSM. If you have more than one, select the most outward facing or most used address.
- A Subject Alternative Name (SAN) is required. If used, it overrides anything in the CN, so be sure to repeat the name in the CN in the SAN. The Subject Alternative Names should be specified when actually signing the certificate signing request (CSR), even if this information is already present in the CSR data fields.

  The Subject Alternative Name (SAN), `subjectAltName`, is included in a sample `config.txt` file, as shown below. You can use an ASCII text editor to create the custom configuration file `config.txt`, which is used by `openssl`.

```
[ req ]
  default_bits= 512
  default_md= sha1
  string_mask= utf8only
  distinguished_name= req_DN

[ req_DN ]
  C= Country Name
  C_min= 2
  C_max= 2
  ST= State or Province Name
  L= Locality Name
  O= Organization Name
  OU= Organization Unit Name
  CN= Common Name
  emailAddress = Email Address

[ verisign_CA ]
  keyUsage=keyCertSign
  basicConstraints= critical, CA:true , pathlen:20
  subjectKeyIdentifier= hash

[ v3_req_ext_SERVER ]
  subjectAltName = @alt_names_SERVER

[ alt_names_SERVER ]
  DNS.1    = mynsk.mydomain.com
  IP.1     = 123.1.1.23
  IP.2     = 123.1.1.24
  IP.3     = 123.1.1.25
  IP.4     = 192.168.36.11
  IP.5    = 2620:0:a05:e014:a00:111f:f001:0001
```

```
[ ca ]
  default_ca= CA_default

[ CA_default ]
  database= index.txt
  serial= serial.txt
  default_days= 365
  default_crl_days= 30
  default_md= sha1
  email_in_dn= no
  name_opt= ca_default
  cert_opt= ca_default
  copy_extensions= copy
  new_certs_dir = C:/OpenSSL-Win32/bin

[ policy_anything ]
  countryName= optional
  stateOrProvinceName= optional
  organizationName= optional
  organizationalUnitName= optional
  commonName= optional
  emailAddress= optional

[ verisign_SERVER ]
  basicConstraints= critical, CA:false
  keyUsage = keyEncipherment, dataEncipherment
  extendedKeyUsage= clientAuth,serverAuth
  subjectKeyIdentifier= hash
  authorityKeyIdentifier= keyid:always
  nsCertType= client, server
  subjectAltName = @alt_names_SERVER
```

The IP addresses for the SAN field are the IP addresses that the OSM client uses to communicate with the OSM server on the NSK server, as well as any additional IP addresses available for the OSM Event Viewer. For example, the OSM Service Connection may use any of the IP addresses available for the default TCPIP processes $ZTCP0 and $ZTCP1, and also IP addresses for the user-defined $ZTC0, $ZTC1, $ZTC4, etc. entered in OSMCONF with `stack =` entries. This fact affects the entries needed for the SAN field.

Any IP addresses available for OSM server or OSM Event Viewer use which are not listed in the SAN field of a customer-supplied SSL certificate will cause security warning dialogs for the OSM Service Connection or OSM Event Viewer clients. The warnings may vary depending on the specific client type and the specific LAN used by the client workstation. The certificate SAN field, `subjectAltName`, must include both numerical IP addresses and any corresponding DNS names to be used for OSM Service Connection sessions or Event Viewer sessions. Note in the sample config.txt file that you must use a different syntax for DNS names (DNS.1, DNS.2, etc.) than the syntax used for IP addresses (IP.1, IP.2, etc.)

The OSM Service Connection uses background NSK IP addresses for fault tolerance, not just the IP address or DNS name visible in the original URL for the web browser session. All IP addresses for $ZTCP0 and $ZTCP1, as well as those allowed by `stack` entries in the OSMCONF file, are tried in the background of the user session. On the Service LAN, the OSM Service Connection uses connections on both the $ZTCP0 and $ZTCP1 TCP/IP stacks, even though only one IP address is included in the original URL address of the web browser session. When using other LANs, the $ZTCP0 and $ZTCP1 IP addresses will probably be inaccessible, but multiple other IP addresses allowed by OSMCONF `stack` parameter entries may be accessible. The certificate SAN field, `subjectAltName`, must include the totality of all IP addresses which could be used on any LAN, because only one SSL certificate is available for the different LANs which will be used for the OSM Service Connection.

The OSM Event Viewer uses only the IP address specified in the original URL of the web browser session. It uses the same SSL certificate as the OSM Service Connection.

The total number of IP addresses visible with `SCF INFO SUBNET <TCPIP process name>.*` could be larger than the number of IP addresses a Certificate Authority allows in the SAN field. To restrict the IP addresses used by the OSM Service Connection, you must use the following specialized syntax for the OSMCONF `stack` parameter:

```
stack = <TCPIP process name>:<IP address>
```

A similar syntax holds for the `evtstack` parameter, which affects the OSM Event Viewer. See "Configuring Additional TCP/IP Processes for OSM Connectivity" (page 18).

NOTE: If the OSM Service Connection or OSM Event Viewer client uses an IP address for the NonStop server which is not listed in the SAN field of the signed SSL certificate (for example, not listed in the `verisign_SERVER` and `alt_names_SERVER` section of the `config.txt` example above), you will see a security warning in the web browser session for the OSM tool.

- Wildcards are allowed in DNS names only.
- RSA key lengths can be up to 2048 bits.
- Although MD5 hashing is supported, SHA1 is recommended as much more secure.

  Starting with T0682 H02 ADF, HP has signed new versions of the default self-signed OSM certificate files `SERVCERT` and `CACERT` by using the SHA1 digest algorithm instead of the MD5 algorithm. These new certificates provide more secure fingerprints, while avoiding compatibility problems when connecting to the OSM Service Connection or OSM Event Viewer from a PC with an older Microsoft operating system. You can notice changes in the detailed Internet Explorer warning when using the OSM Event Viewer, since these are new certificates. A warning is expected from OSM Event Viewer sessions, since modern versions of Internet Explorer do not trust self-signed certificates.

  When signing your private SSL certificates for OSM, security standards for your servers can prescribe use of an even stronger SHA2 digest algorithm such as SHA256. Note that Microsoft Internet Explorer versions before IE7 are not compatible with SHA2 algorithms. Windows XP and Windows Server 2003 require updates to support SHA2. Windows XP Service Pack 3 should be sufficient, but Windows Server 2003 can require a special update from Microsoft. Be prepared to retire older PCs or to update software.

  For more information on Windows XP and Windows Server 2003 certificate support, refer to:

  http://support.microsoft.com/kb/968730

For an example of one method for generating a private certificate, see "Example: How To Generate a Private SSL Certificate Using OpenSSL".

Once acquired, the certificate must be placed on the server for use. Three files and five settings in OSMCONF must be configured. OSM needs to know the certificate used for SSL and also the Certificate Authority (CA) certificate that signed the server's certificate. Additionally, the server's private key file is needed to encrypt the communications. The requirements for these files are:

- The server certificate and the CA certificate must be in binary DER format.
- The server key file must also be in binary DER format, but must also be in PKCS#8 format.
- The server certificate, the CA certificate, and the server key file must be binary code 0 files. Be sure to FTP in binary mode.
- The server key file must be encrypted with a password.

Configuring OSM for SSL support requires adding the following settings to your OSMCONF:

- `UseSSL = On`
- `SERVCERT = <server certificate filename>`

- `CACERTS = <CA certificate filename>`
- `SERVKEY = <server private key filename>`
- `SERVKEYPASS = <key password>`

On the PC side, the certificate will be trusted by default if:

- The certificate is not self-signed.
- The certificate is valid (and not expired).
- The certificate is signed by a trusted CA.
- If the certificate has a SAN, the server's address matches one of the entries in the SAN.
- If the certificate does not have a SAN, the server's address matches the Subject CN.

If any of these are not the case, there will be a warning dialog. In OSM Service Connection, a warning dialog (sometimes two) will be displayed detailing the issues with the certificate. The user will have the option to exit at this point or to continue on with OSM despite these issues. Also, the user will have the option to trust this certificate or this CA in the future and automatically skip past the warning dialog. In OSM Event Viewer, the behavior is dependent on Internet Explorer and IE's security settings. A variety of different warnings are possible depending on the version of IE and how tightly security is set on the browser.

IE's certificate list can be reached by opening IE, and selecting Tools > Internet Options > Content tab, and clicking the **Certificates** button.

Java's certificate list can be reached by selecting Start > Control Panel > Java > Security tab, and clicking the **Certificates** button.

Example: How To Generate a Private SSL Certificate Using OpenSSL

This section describes just one of the possible methods for generating a private certificate. You can use alternative methods as long as you meet the "Requirements for Generating and Activating a Private SSL Certificate". This example includes creating a CA, adding it to the trusted list, and securing one server with a certificate. See "Requirements for Generating and Activating a Private SSL Certificate" for an example of the `config.txt` file.

1. Obtain a copy of OpenSSL. These instructions are designed for Win32 OpenSSL 1.0.0g 18 Jan 2012:).

   http://www.slproweb.com/products/Win32OpenSSL.html

2. Create the `index.txt` file and leave it empty. Create the `serial.txt` file and include the following one line text in it:

   ```
   01
   ```

3. Create the internal root CA. It will ask about the identity of the certificate. List your organization. Then assign a password to the key when asked, to be used later during the signing process.

   ```
   openssl req -out ca.cer.pem -new -newkey rsa:2048 -keyout ca.key.pem -x509
   -days 365 -config config.txt -extensions verisign_CA
   ```

   The `verisign_CA` section in the `config.txt` file contains certificate extensions to be added when a certificate is issued.

4. Convert the PEM format certificate to DER format.

   ```
   openssl x509 -inform PEM -outform DER -in ca.cer.pem -out ca.cer
   ```

5. Create the certificate signing request (CSR) for the server. It will ask about the identity of the server. Be sure to list your organization, but list the DNS name of the server in the CN field. Assign a password to the key to be used later in OSMCONF.

   ```
   openssl req -out server.csr -new -newkey rsa:2048 -keyout server.key.pem
   -config config.txt -reqexts v3_req_ext_SERVER
   ```

The `v3_req_ext_SERVER` section in the `config.txt` file specifies the Subject Alternative Name (SAN) to be added when a certificate is issued.

6. Convert the key to PKCS#8 DER format.

   ```
   openssl pkcs8 -topk8 -outform DER -in server.key.pem -out server.key
   ```

7. Sign the new CSR with the CA key.

   ```
   openssl ca -days 365 -policy policy_anything -keyfile ca.key.pem -cert ca.cer.pem
   -in server.csr -out server.cer.pem -config config.txt -extensions verisign_SERVER
   ```

   The `verisign_SERVER` section in the `config.txt` file contains the contents of multi-valued extensions to be added when a certificate is issued.

   Before issuing this command, check that the subjectAltName section occurs in the section specified by the –extensions flag of this command. In the example configuration file config.txt, the verisign_SERVER section includes a `subjectAltName` reference which in turn includes the `alt_names_SERVER` section with the desired IP addresses and DNS names.

   If the Subject Alternative Names extensions are not included when signing the CSR, the SAN entries will generally be dropped from the signed certificate. This omission will cause warnings when you later use the OSM Service Connection.

   If you engage an external Certificate Authority to sign the CSR, consult with the vendor or vendor's documentation to make certain that the desired Subject Alternative Names are included in the signed certificate.

8. Convert the signed certificate to DER format.

   ```
   openssl x509 -inform PEM -outform DER -in server.cer.pem -out server.cer
   ```

9. FTP the files to the NonStop server. Be sure to select binary transfer mode.

   ```
   cd $SYSTEM.OSMCERTS
   put server.cer OSMCERTS.SERVCERT
   put server.key OSMCERTS.SERVKEY
   put ca.cer OSMCERTS.CACERT
   ```

10. Using TACL, add these lines to `OSMCONF`:

    ```
    UseSSL = On
    SERVCERT = $SYSTEM.OSMCERTS.SERVCERT
    CACERTS = $SYSTEM.OSMCERTS.CACERT
    SERVKEY = $SYSTEM.OSMCERTS.SERVKEY
    SERVKEYPASS = password
    ```

11. Restart the OSM CIMOM ($ZCMOM) and Event Viewer ($ZOEV) processes in SCF.
12. On the PC, import `ca.cer` into the IE list of Trusted Root Certification Authorities.

Configuring Event Viewer Security Timeout

With OSM version T0682 H02 ABP and later, the OSM Event Viewer has a new security feature whereby an event viewer session left idle for more than 20 minutes expires, requiring you to log on again before you can access that session again. After being idle for 24 hours, that event viewer session is deleted, meaning that session cannot be accessed again. Idle refers to the period of time since the user last clickable action in either the OSM Event Viewer main window or the EMS Events Returned window. Both the 20 minute and 24-hour default values are configurable and can be changed by inserting the following parameters into your OSMCONF file.

`EvtMgr_Session_Expiration_Time = nn`

nn is the number in minutes before an idle event viewer session expires and requires logon to access that session again. The minimum possible value is 1 minute. It can be set to any value, such as 1440 for one day or 524160 for one year (the upper limit being the maximum value that a 32-bit field can take: 2^32); however, it must be set to a lower value than the `EvtMgr_Session_Deletion_Time` parameter, or the idle session will be deleted without an opportunity to log on again.

`EvtMgr_Session_Deletion_Time = nn`

nn is the number in minutes before an idle event viewer session is deleted and cannot be accessed again. This parameter has the same value options as the `EvtMgr_Session_Expiration_Time` parameter. However, as noted above, it must be set higher than the expiration parameter in order to have the ability to log on again to an expired session before it is deleted permanently.

NOTE: In the absence of either of these parameters in an OSMCONF file for OSM version T0682 H02 ABP and later, the default value for that particular parameter (session expiration and/or session deletion) will be in effect.

To make changes to your OSMCONF file take effect, see "Creating and Using an OSMCONF File" (page 15).

Configuring OSM in a Network Address Translation (NAT) Environment

Network Address Translation (NAT) is a technology that allows small networks to contain internal-only addresses that need only be unique inside of a sub-network, and translate them to externalized addresses that are unique for a larger network, usually the public Internet. With T0682 H02 ABR and later, OSM can be configured to be compatible in an NAT environment.

While NAT automatically translates addresses back and forth in some situations, the nature of OSM connectivity is such that it knows only the private (internal) network addresses and requires that OSM be provided with the external addresses. This is done through the OSMCONF file, as described in "Specifying Externalized OSM Addresses for NAT".

Specifying Externalized OSM Addresses for NAT

To connect to a NonStop server in an NAT environment, the OSM Service Connection must be provided with its external addresses. These external addresses must be specified in your OSMCONF file as follows:

```
url = <protocol>://<first IP address or DNS name>:<port>
url = <protocol>://<second IP address or DNS name>:<port>
<etc.>
```

Rules:

- The URL must contain either a valid IP address or fully-qualified DNS name for the server.
- The only valid protocols are "http" and "https" and it must be in synch with the "UseSSL" OSMCONF setting. If the UseSSL parameter is set to "On," then the protocol setting must be "https."
- A port number must be specified; the default port of 80 for "http" is almost certainly incorrect. The ports are normally 5988 for http and 5989 for https, but may vary depending on your NAT configuration.
- Each address must be confined within a 79 character limit.

To make changes to your OSMCONF file take effect, see "Creating and Using an OSMCONF File" (page 15).

NOTE: The initial addresses are ordinarily provided by querying SCF for addresses corresponding to the stacks specified either by the default setting ($ZTC0 and $ZTC1) or the stacks specified in OSMCONF via the "stack" setting. For more information, see "Configuring Additional TCP/IP Processes for OSM Connectivity").

Known Issue: When using a NAT environment, there is an issue with external links provided within the OSM Service Connection. The Tools menu option (on the OSM menu bar) to launch the OSM Event Viewer will fail, as will OSM Service Connection actions to launch web-based management applications such as iLOs, Onboard Administrators, and web interfaces for Maintenance Switch, UPS, Alarm Panel, and Fibre Channel Router objects.

Workaround: Launched independently of the OSM Service Connection, the OSM Event Viewer is already compatible with NAT and no additional configuration is necessary. The workaround for accessing the web-based management applications is also to launch them directly from an Internet browser and not through the OSM Service Connection.

Configuring Insight Remote Support Advanced

"HP Insight Remote Support Advanced" (page 39) replaces the OSM Notification Director in both modem-based and HP ISEE remote support solutions. For information on migrating to Insight Remote Support Advanced, refer to the instructions in *Insight Remote Support Advanced for NonStop*, located in the Support and Services collection of NTL

As part of the migration process described in that document (after disabling the OSM ND), you will be directed to add the following parameter to your OSMCONF file (for each NonStop system to be monitored by Insight Remote Support Advanced) to enable remote notification (dial-out) to Insight Remote Support Advanced/WEBES:

```
IR_Alert = YES
```

Additionally, the following parameter must be added to each NonStop system to be monitored by Insight Remote Support Advanced (not necessary needed for NonStop BladeSystems, as SSL is enabled by default):

```
UseSSL = ON
```

NOTE:

With OSM version T0682 H02 ADD (or later), you do not need to add the `UseSSL` parameter.

NOTE: This assumes you are using OSM version T0682 H02 ACC or later, which eliminates the need for additional OSMCONF parameters required in earlier versions and also supports fault tolerant console configurations for NonStop NS-series and NonStop BladeSystems, allowing Insight Remote Support Advanced to monitor a system from more than one console without getting duplicate remote notifications (dial-outs).

After editing your OSMCONF file, you must restart the following OSM server processes (if running on the NonStop system) for the changes to take effect:

- $ZCMOM ($ZZKRN.#OSM-CIMOM)
- $ZOSM ($ZZKRN.#OSM-APPSRVR)
- $ZOEV ($ZZKRN.#OSM-OEV)

Configuring OSM Power Fail Support

With T0682 H02 ACC (and later), OSM enhances power fail support by providing two new OSMCONF settings to allow for execution of an automated system application shutdown script. The SHUTDOWN_SCRIPT_NAME and SHUTDOWN_SCRIPT_TIME parameters specify the name and location of the script to be run and when it will be executed during the power fail detection and monitoring sequence. For information on how to configure your NonStop system to take advantage of OSM power fail support, see the planning guide for that type of NonStop NS-series or NonStop BladeSystem.

When power fail support is properly configured and OSM detects an AC power failure, it triggers and counts down a ride-through period after which – if the power has not yet been restored – OSM initiates a controlled shutdown of I/O operations and processors. If the script name and time parameters have been added to your OSMCONF, the specified script is triggered by the SHUTDOWN_SCRIPT_TIME, which provides time for the script to run before the end of the configured ride-through time (as described below).

```
SHUTDOWN_SCRIPT_NAME = name
```

name is a fully qualified location/name of the application shutdown script to be executed. The file type should be file code 101 (an editable text file). The location/name must be fully

qualified because if not specified, OSM will only look in the default subvolume of $system.zservice, which is not recommended for the placement of such script files.

Example: `SHUTDOWN_SCRIPT_NAME = $SYSTEM.SYS00.SYSHTDWN`

`SHUTDOWN_SCRIPT_TIME = nn`

nn is the time, in seconds, that the script is to be executed before the end of the configured ride-through period. For example, if the ride-through time is set to 60 seconds and the specified SHUTDOWN_SCRIPT_TIME is 25 seconds, then the shutdown script executes 35 seconds after the ride-through time begins. The value of the SHUTDOWN_SCRIPT_TIME cannot exceed the configured ride-through time minus 5 seconds (if the ride-through time is 60 seconds, the SHUTDOWN_SCRIPT_TIME can be no greater than 55 seconds).

The goal in specifying a SHUTDOWN_SCRIPT_TIME is to wait as long as possible before executing the shutdown script – in the hope that AC power is restored and the shutdown avoided – while allowing enough time for the script to complete the application shutdown steps before ride-through ends and the shutdown of I/O operations and processors begins.

To make changes to your OSMCONF file take effect, see "Creating and Using an OSMCONF File" (page 15).

The Verify Power Fail Configuration action, located on the System object in the OSM Service Connection, now checks the validity of these two variables in addition to verifying that OSM power failure support has been properly configured and is in place for the system. The check will return an error if OSM cannot find the script file in the specified location, the file does not have the file code of 101, or the specified time is not at least 5 seconds less than the configured ride-through time.

Configuring OSM Process File Security Levels

With version T0682 H02 ACE and later, OSM sets the default process file security to `NCNC`, and gives you the option to change the security levels for OSM persistent processes using either of the following methods:

- "Editing the ADDTOSCF File" (page 30)
- "Aborting, Altering, and Starting OSM Process Files" (page 31)

Editing the ADDTOSCF File

One way to can change the default security levels for OSM persistent process is by editing the ADDTOSCF file. Within the file, locate the STARTUPMSG (startup message) line for the OSM-CIMOM, OSM-APPSRVR, and OSM-OEV processes and change the security levels (the default is "`security NCNC`") as desired. The following is an example of an ADDTOSCF file showing the default settings:

```
== Add $ZCMOM process to SCF database and issue start command
@ ABORT PROCESS $ZZKRN.#OSM-CIMOM
@ DELAY 1
@ DELETE PROCESS $ZZKRN.#OSM-CIMOM
@ ADD PROCESS $ZZKRN.#OSM-CIMOM,      &
    AUTORESTART 5,                    &
    CPU FIRSTOF [listProcessors],     &
    DEFAULTVOL $SYSTEM.ZSERVICE,      &
    HIGHPIN ON,                       &
    HOMETERM $ZHOME,                  &
    NAME $ZCMOM,                      &
    PRIORITY 150,                     &
    PROGRAM $SYSTEM.SYSTEM.CIMOM,     &
    OUTFILE $ZHOME,                   &
    STARTUPMSG "cpu-list cpu-list, security NCNC", &
    STARTMODE APPLICATION

@ START PROCESS $ZZKRN.#OSM-CIMOM
```

```
== Add $ZOSM process to SCF database and issue start command
@ ABORT PROCESS $ZZKRN.#OSM-APPSRVR
@ DELAY 1
@ DELETE PROCESS $ZZKRN.#OSM-APPSRVR

@ ADD PROCESS $ZZKRN.#OSM-APPSRVR,  &
    AUTORESTART 10,                 &
    CPU FIRSTOF [listProcessors],   &
    DEFAULTVOL $SYSTEM.ZSERVICE,    &
    HIGHPIN ON,                     &
    HOMETERM $ZHOME,                &
    NAME $ZOSM,                     &
    PRIORITY 150,                   &
    PROGRAM $SYSTEM.SYSTEM.APPSRVR, &
    OUTFILE $ZHOME,                 &

    STARTUPMSG "cpu-list cpu-list, security NCNC", &
    STARTMODE APPLICATION

@ START PROCESS $ZZKRN.#OSM-APPSRVR

== Add $ZOEV process to SCF database and issue start command
@ ABORT PROCESS $ZZKRN.#OSM-OEV
@ DELAY 1
@ DELETE PROCESS $ZZKRN.#OSM-OEV
@ ADD PROCESS $ZZKRN.#OSM-OEV,     &
    AUTORESTART 10,                &
    CPU FIRSTOF [listProcessors],  &
    DEFAULTVOL $SYSTEM.ZSERVICE,   &
    HIGHPIN ON,                    &
    HOMETERM $ZHOME,               &
    NAME $ZOEV,                    &
    PRIORITY 150,                  &
    PROGRAM $SYSTEM.SYSTEM.EVTMGR, &
    OUTFILE $ZHOME,                &
    STARTUPMSG "cpu-list cpu-list, security NCNC", &
    STARTMODE APPLICATION

@ START PROCESS $ZZKRN.#OSM-OEV
```

Use the following command to make changes to the ADDTOSCF file take effect:

```
obey addtoscf
```

NOTE: You should save a copy of your ADDTOSCF before installing a new OSM SPR, as your existing ADDTOSCF is overwritten at that time and security settings would revert to default values if ADDTOSCF is obeyed again after installing the new OSM SPR.

An alternative method for changing process file security levels is by "Aborting, Altering, and Starting OSM Process Files" (page 31).

Aborting, Altering, and Starting OSM Process Files

Instead of "Editing the ADDTOSCF File" (page 30), you can also change the default security levels for an individual OSM persistent process by aborting the process, altering the startup message, and then starting that process as described below (using the CIMOM process as an example):

1. Because altering a startup message overwrites the existing message, perform the following command so you can note the contents of the current startup message. When altering the startup message, you will need to re-enter any parts of the existing message that you want to preserve, such as any BackupCpu or cpu-list entries).

   ```
   SCF info process $zzkrn.#osm-cimom, detail
   ```

2. Abort the process:

```
SCF abort process $zzkrn.#osm-cimom
```

3. Use the following command to alter and overwrite the startup message (STARTUPMSG) for the process, re-creating any entries from the current file that you wish to preserve, while specifying the desired security levels for the process using the *rwep* (Read, Write, Execute, Purge) format illustrated below:

   ```
   SCF alter process $zzkrn.#osm-cimom, startupmessage "BackupCpu | cpu-list cpu-list,
   security rwep"
   ```

4. Start the process:

   ```
   SCF start process $zzkrn.#osm-cimom
   ```

5. Use the following command again to the confirm the changed security settings:

   ```
   SCF info process $zzkrn.#osm-cimom, detail
   ```

Repeat steps 1–5 for the APPSRVR ($zzkrn.#osm-appsrvr) and EVTMGR ($zzkrn.#osm-oev) processes, as desired.

Flagging Up-rev CLIM and SAS Disk Enclosure Firmware as a Problem Attribute

With T0682 H02 ACJ and later, you can configure OSM to flag Up-rev firmware on CLIM and SAS Disk Enclosure components as a problem attribute that is propagated up to parent objects in the OSM Service Connection. To do so, add the following parameter to your OSMCONF file:

```
ShowCLIMUpRevFirmare = YES
```

NOTE: The default value is "No," in which case a Compare State attribute value of "Up-rev" would not cause a problem flag to be created and propagated up to parent objects in the OSM Service Connection.

To make changes to your OSMCONF file take effect, see "Creating and Using an OSMCONF File" (page 15).

Disabling Access Control List Functionality

With OSM version T0682 H02 ACJ and later, the Access Control List feature is enabled by default. To disable the feature, put the following parameter into your OSMCONF file:

```
ACL_Enabled = OFF
```

To make changes to your OSMCONF file take effect, see "Creating and Using an OSMCONF File" (page 15).

Enabling IPv6 Support

With T0682 H02 ACV and later, OSM supports IPv6 addresses (in addition to IPv4 addresses) for communication, outside of maintenance LAN, between OSM Service Connection and OSM server, and between OSM Event Viewer client and OSM Event Viewer server. To configure and enable the use IPv6 addresses for OSM:

- Specify a TCP6SAM or CIPSAM process as a "stack" parameter in your OSMCONF file (for more information, see "Configuring Additional TCP/IP Processes for OSM Connectivity" (page 18)).

  NOTE: IPv4 addresses are in dotted format (16.107.201.230), while IPv6 addresses are in hexadecimal format (2001:0db8:85a3:0000:0000:8a2e:0370:7334).

- Add or alter the following parameter in your OSMCONF file:

  ```
  Allow_IPv6 = ON
  ```

  NOTE: The default setting for IPv6 is disabled in the absence of this parameter, or if set to "OFF."

To make changes to your OSMCONF file take effect, see "Creating and Using an OSMCONF File" (page 15).

OSM Upgrade Considerations

To help ensure accurate alarm reporting in OSM, when upgrading to a new OSM servers SPR (or falling back to a previous version), you should purge the IAREPO file from $SYSTEM.ZSERVICE.

Starting OSM Persistent Processes

Once you have installed all required server-based OSM and requisite SPRs from the SUT (using DSM/SCM) and completed any configuration changes (see "Optional OSM Configuration" (page 15) and "OSM Upgrade Considerations" (page 33)), use this TACL command to invoke the OSM Configuration script and start the OSM persistent processes (other than $ZTCP0 and $ZTCP1):

```
RUN $SYSTEM.ZOSM.ADDTOSCF
```

This table lists and describes the OSM persistent processes:

Process Name	Description	Symbolic Name	File Name
$ZCMOM	Main OSM server process (Common Information Model Object Manager)	$ZZKRN.#OSM-CIMOM	$SYSTEM.SYS*nn*.CIMOM
$ZOSM	Applet Server process – uploads client files to the Service Connection	$ZZKRN.#OSM-APPSRVR	$SYSTEM.SYS*nn*.APPSRVR
$ZOEV	Event Viewer Manager process – server for Event Viewer requests	$ZZKRN.#OSM-OEV	$SYSTEM.SYS*nn*.EVTMGR
$ZSPE	SP Event Distributor process – writes SP events to $ZLOG	$ZZKRN.#SP-EVENT	$SYSTEM.SYS*nn*.ZSPE
$ZLOG	EMS Collector for service events	$ZZKRN.#ZLOG	$SYSTEM.SYS*nn*.EMSACOLL
$ZOLHI	EMS Routing Distributor – used by ServerNet Cluster Automatic Line Handler Configuration to send events to $ZOLH	$ZZKRN.#OSM-CONFLH-RD	$SYSTEM.ZOSMLH.INITRD
$ZTCP0$ZTCP1	TCP/IP processes – required by the Service Connection, Notification Director, and Event Viewer for HTTP over TCP/IP communication	$ZZKRN.# ZTCP0$ZZKRN.# ZTCP1	$SYSTEM.ZOSM.CTCPIP0 $SYSTEM.ZOSM.CTCPIP1
$ZTMUX	OSM now starts the SNMPTMUX process as $ZTMUX, a standard persistent process used by OSM providers to convert SNMP traps to EMS events.	$ZZKRN.#OSM-SNMPTMUX	$SYSTEM.SYSnn.SNMPTMUX

Other OSM Server Processes

This section describes the other OSM and OSM-related (*) server processes that are started by the OSM persistent processes described in the preceding section. For each of these processes, the process name is dynamically assigned.

$SYSTEM.SYSnn.APPRVD

Launched by $ZOSM, Applet Providers are responsible for serving client files.

The maximum number that can run simultaneously is eight.

$SYSTEM.SYSnn.EMSDIST*

EMS Event Distributor used for Auto Reallocate. Monitors medium error events generated by disk driver and starts the automatic sector reallocation process ($ZARS)

Process name: $ZRD9

SCF process: $ZZKRN.#ROUTING-DIST

* Not delivered as part of OSM, but rather an existing process used by OSM.

$SYSTEM.SYSnn.EVNTPRVD

Launched by $ZCMOM, the Event Listener Provider is responsible for retrieving SP and EMS events.

The maximum number that can run simultaneously is one.

$SYSTEM.SYSnn.FDIST*

Launched by the EVNTPRVD process, the Fast EMS Event Distributor process is responsible for retrieving EMS events from $ZLOG and $0.

The maximum number that can run simultaneously one.

* Not delivered as part of OSM, but rather an existing process used by OSM.

$SYSTEM.SYSnn.IAPRVD

Launched by $ZCMOM, the Incident Analysis Provider is responsible for state propagation and generation of incident reports (IRs)

The maximum number that can run simultaneously is one.

$SYSTEM.SYSnn.INDPRVD

Launched by $ZCMOM, the Object Indication Provider sends object indications to WBEM clients (such as HP SIM).

Process names are dynamically assigned.

The maximum number that can run simultaneously is one.

$SYSTEM.SYSnn.MDEVPRVD

Launched by $ZCMOM, the Monitored Maintenance Devices Provider is responsible for monitoring the modular I/O UPS, Ethernet maintenance switches, and storage routers. When a UPS is configured, the MDEVPRVD process starts an SNMPTMUX process.

Process names are dynamically assigned.

The maximum number that can run simultaneously is one.

NOTE: If OSM Power-Fail support is configured, a second, non-persistent, MDEVPRVD process might exist during an actual power fail event.

$SYSTEM.SYSnn.OEVPRVD

Launched by $ZOEV, the Open Event Viewer Providers are responsible for retrieving EMS events.

The maximum number that can run simultaneously is eight.

$SYSTEM.SYSnn.RALPRVD and $SYSTEM.SYSnn.RALPRVNP

Launched by $ZCMOM, these Resource Access Layer Providers are responsible for:

- Interacting with SP and subsystems such as Storage, SLSA, etc., to gather attributes and states for system resources
- Executing all actions on OSM objects
- Triggering Incident Analysis to generate and clear alarms

RALPRVD is used for initial discovery, initial incident analysis, event processing and all action execution that require a super-group user.

RALPRVNP is used for action executions that do not require super-group permission.

The maximum number that can run simultaneously is 48:

- Maximum of eight RALPRVD processes for event processing
- Maximum of eight RALPRVD processes for refresh or reanalyze action processing
- Maximum of eight RALPRVD processes for short-term super-group action processing (Start/Stop disk, etc.)
- Maximum of eight RALPRVD processes for long-term super-group action processing (Firmware Update, Validate Checksum, etc.)
- Maximum of eight RALPRVNP processes for short-term non-super-group action processing (Responsive Test, etc.)
- Maximum of eight RALPRVNP processes for long-term non-super-group action processing (None at this time)

$SYSTEM.SYSnn.SECPRVD

Launched by: $ZCMOM, the Security Providers are responsible for user authentication.

The maximum number that can be running simultaneously is eight.

$SYSTEM.SYSnn.SPDIST2

Launched by the EVNTPRVD process, the SP Event Distributor process is responsible for retrieving SP events from $YMIOP.

The maximum number that can run simultaneously is one.

$SYSTEM.SYSnn.TACLPRVD

Launched by $ZCMOM, the TACL Providers are responsible for performing embedded TACL actions (Reload Processor).

The maximum number that can run simultaneously is eight.

$SYSTEM.ZTCPIP.FTPSERV

FTP server, required by OSM Notification Director to retrieve alarm attachment files.

Process names are dynamically assigned.

OSM Server Files

This section lists and describes OSM server files. It is organized by the directory in which the files reside.

$SYSTEM.ZOSM

File Name	Description
ADDTCPIP	Script to configure $ZTCP0/1 into the persistence manager using INIT0/1.
ADDTOSCF	Script to configure OSM persistent processes into the persistence manager.
ALTERIP	Script to restart $ZTCP0/1 using CTCPIP0/1.
CTCPIP0/1	Script to configure $ZTCP0/1.
INIT0/1	Script to bring up $ZTCP0/1 with the factory default IP address (set by ADDTCPIP).
LOGALTIP	Trace log generated by ALTERIP
LOGSCF	Trace log generated by ADDTOSCF.
LOGTCP0/1	Trace log generated by INIT0/1 and CTCPIP0/1.
LOGTCPIP	Trace log generated by ADDTCPIP.

$SYSTEM.SYS*nn*

File Name	Description
APPFLMAP	Text file used by APPRVD to map client file names to NSK files.
CIMREPO	CIM repository (Enscribe database) file, contains DMTF CIM class information for all the classes used by CIMOM and OSM Service Connection client.
RAREPO	Enscribe database file used by RALPRVD, contains repair actions in XML format.

$SYSTEM.ZSERVICE

File Name	Description
ADCREPO	Enscribe database file. Contains configuration information for Automatic Data Collection (ADC).
IAREPO	Enscribe database file that contains alarm history. Created and maintained by IAPRVD.
MDREPO	Enscribe database file. Contains configuration information related to the MSIO UPS and maintenance switches.
OSMINI	Default configuration file delivered with OSM on the SUT; used as a template for "Creating and Using an OSMCONF File".
PCREPO	Enscribe database file. Contains Rack name, Offset, Locator String Info. Created and maintained by RALPRVD/MDEVPRVD.
SUPPREPO	Enscribe database file that contains remote notification (dial-out) configuration information. Created and maintained by IAPRVD.
SYSH*nnnn*	Software Configuration IR text file.
ZZAA*nnnn*	Alarm Attachment (text) file for each alarm. Created by IAPRVD.
ZZDD*nnnn*	OSM Data Diagnostic Collection text files. Created by Datacoll.
ZZPS*nnnn*	Dump file of the processor scan string. Created by processor IA (part of RALPRVD).
ZZSN*nnnn*	"Disabling Creation of System Inventory Files " whenever a Periodic incident report is initiated. Must be enabled in your OSMCONF file and configured in the OSM ND.

ZTRC	File containing pointer to the current ZTRC*n* file. Created and maintained by CIMOM.
ZTRC*n*	Text files containing user trace logs (1-5). Created and maintained by CIMOM. Maximum size: 0.25 MB.
ZZSK*nnnn*	$ZLOG alternate key file.
ZZSV*nnnn*	$ZLOG data files.

4 OSM and Other HP Client-Based Components

OSM Client-Based Applications

OSM client-based components are installed on new system console shipments and also delivered by an OSM installer on the HP NonStop System Console (NSC) Installer DVD. The NSC DVD also delivers all other client software required for managing and servicing all NonStop systems. (Unlike OSM server, which has one version for G-series and another for H- and J-series, the client-based software is the same for all three RVU threads.) Installation instructions are included in the *NonStop System Console Installer Guide*.

The OSM Master installer installs (or upgrades) the following components onto your NonStop system console:

- OSM Low-Level Link (T0633) – used mostly for down-system support.
- OSM Console Tools (T0634) – which installs:
  - With version T0634 ABD and later, Apache OpenOffice has been added to the OSM Console Tools. It provides a method to view spreadsheets, documents, and presentations on the system console. For example, the `.csv` (or comma delimited) files created by OSM, such as hardware inventories created by the OSM System Inventory Tool and the Access Control List reports and saved Multi-Resource Views created in the OSM Service Connection.
  - Start menu shortcuts and default home pages for the OSM Service Connection and OSM Event Viewer (the two browser-based OSM applications that reside on the server and are not installed on the system console). While not necessary for using these applications, the home pages display bookmarks for easy access to your NonStop systems.
  - With version T0634 AAL and later, the "OSM System Inventory Tool".
  - With version T0634 AAN and later, a "Terminal Emulator File Converter" to convert OSM Service Connection-related OutsideView session files to MR-Win6530 format. For more information on the conversion tool, see the *NonStop System Console Installer Guide* and the online help available within the conversion tool.
  - With version T0634 AAQ and later, the "OSM Certificate Tool", which is used for NonStop BladeSystems only, to facilitate communication between OSM and the Onboard Administrators (OAs) in the blade enclosures. It is used to create and upload certificates so that OSM can invoke the OA web interface, logon to an OA, and make SOAP calls without having to provide a username and password each time.
  - With version T0634 ABB and later, the "NonStop Maintenance LAN DHCP DNS Configuration Wizard", which replaces the CLIM Boot Service Configuration Wizard. It is used to configure the DHCP, DNS, FTP, TFTP, and BOOTP servers as needed.
  - With version T0634 ABB and later, the "Down System CLIM Firmware Update Tool", which can be used for updating firmware/BIOS for all CLIM components during planned system down time.

NOTE: The OSM Notification Director is no longer supported for remote notification (dial-out) services. Remote notifications are now provided by "HP Insight Remote Support Advanced" (page 39). The equivalent of remote connection (dial-in) is now provided by Remote Desktop, as described in the *NonStop System Console Installer Guide*.

Other HP Client-Based Tools

HP Systems Insight Manager (SIM)

HP Systems Insight Manager (SIM), which provides infrastructure management for all HP servers and storage, now supports the NonStop platform via a Web-Based Enterprise Management (WBEM) provided by OSM. HP SIM is capable of discovering NonStop systems, displaying and forwarding alarms generated by OSM, and collecting system and device data. It is required for HP SIM plug-in products, such as "HP Insight Remote Support Advanced" (page 39), "HP Insight Control Power Management" (page 39), and NonStop Essentials products (see "Support for NonStop Essentials Products" (page 9)).

As of H06.25 and J06.14, NonStop system consoles shipped with new system orders will have HP SIM and the NonStop Software Essentials product pre-installed. NonStop Software Essentials replaces the DSM/SCM Planner Interface, which is not supported on 64-bit system consoles (including NSCs running Windows Server 2008).

Other sources of information regarding HP SIM include:

- Installing the HP SIM client – the NonStop System Console Installer kit includes a separate HP Insight Control for NonStop DVD from which you can install HP SIM and various plug-in products. For hardware and software requirements and installation information, see the *NonStop System Console Installer Guide* and *HP SIM for NonStop Manageability* (located in the NonStop Service Information collection of NTL).
- Configuration – After HP SIM and requisite OSM versions are installed, you must enable secure sockets layer (SSL) in OSM (see "Configuring Secure Sockets Layer (SSL) Support" (page 22).

HP Insight Remote Support Advanced

HP Insight Remote Support Advanced is now the remote support solution of choice for NonStop NS-series systems and NonStop BladeSystems, replacing the OSM Notification Director (both modem-based and in conjunction with ISEE). As a plug-in to "HP Systems Insight Manager (SIM)", Insight Remote Support Advanced enhances HP SIM with intelligent event diagnosis and automatic, secure submission of hardware event notifications to HP support, including acknowledgment and status.

For more information on installing and using Insight Remote Support Advanced in the NonStop environment, see *Insight Remote Support Advanced for NonStop*, located in the Support and Service collection of NTL. When directed to by the migration procedure, you will be asked to add parameters to your OSMCONF file, as described in "Configuring Insight Remote Support Advanced" (page 29).

HP Insight Control Power Management

Insight Control Power Management is an "HP Systems Insight Manager (SIM)" plug-in that provides the ability to visualize the layout of servers and devices in racks and data center floors, summarizing temperature and power consumption. It provides the capability to monitor and manage power capacity and utilization for blades and c-class enclosures and power delivery devices for data centers. It also lets the user monitor inlet air temperature and 24-hour peak temperature for blades and c-class enclosures. For HP Integrity NonStop BladeSystems, Insight Control Power Management provides both power and thermal monitoring. It can also provide alerts on potential errors, lack of redundancy and configuration anomalies. And, for NonStop BladeSystems NB56000c and NB56000c-cg, as well as NonStop BladeSystems NB54000c and NB54000c-cg running J06.14 or later and OSM server SPR T0682ACZ or later, you can enable the Power Regulator feature to provide centralized control of server power consumption. For more information, see *HP SIM for NonStop Manageability* (located in the NonStop Service Information collection of NTL).

OSM has been enhanced to allow a NonStop system to be powered down gracefully from Insight Control Power Management. OSM also allows Insight Control Power Management to display CPU utilization data for NonStop systems as it does for other platforms.

The Insight Control Power Management installer is included on the HP Insight Control for NonStop DVD that ships along with the NonStop System Console Installer DVD. For information on installing Insight Control Power Management, see the *NonStop System Console Installer Guide*.

For information on using Insight Control Power Management, see the *HP Insight Control Power Management User Guide* for the version you are using.

comForte MR-Win6530

At H06.10, comForte MR-Win6530 replaced OutsideView 7.3c as the terminal emulator shipped on NonStop system consoles. It is used by the OSM Low-Level Link for startup event stream (CNSL) and startup TACL (CLCI) windows and by the OSM Service Connection for TACL and FTP sessions. OSM Console Tools, version T0634 AAN and later, provides a "Terminal Emulator File Converter" to convert OSM Service Connection-related OutsideView session files to MR-Win6530 format. For information on installing MR-Win6530 and OSM Console Tools, and launching the conversion tool, see the *NonStop System Console Installer Guide*.

At H06.11, MR-Win6530 (T0819 AAB) was updated to take advantage of Secure Shell Server (SSH), a new product for H06.11. SSH provides secure communication between MR-Win6530 and the NonStop server, so it can be used for OSM Service Connection-related emulator sessions. The following procedures describe how to start TACL and SecureFTP sessions using SSH.

Starting SSH TACL Sessions with MR-Win6530

1. Make sure the SSH-ZPTY, SSH-ZTCP0, SSH-ZTCP1 processes are running.
2. Start MR-Win6530.
3. Create a new profile by selecting File > New Profile > 6530 Terminal, then click **OK**.
4. Select Options > Communications > SSH (Secure Shell), then click **Configure**.
5. Configure Host, User ID, and optional Password; leave the port at default 22, then click **OK**. The host ip address can be found for the $ztcp0 or $ztcp1 process with the command:

   ```
   scf; info subnet $ztcp*.#*
   ```

6. In the Options dialog box click **Apply**, then **OK**.
7. Select **File**, then **Connect**.
8. The following message should display at startup, indicating an SSH session, followed by the regular TACL session message:

   ```
   STN00 Connected to STN version A66  2007/07/03 09:59 \OSMQA2.$ZPTY.#ZWN0002
   STN46 Secure SSH session: TN6530-8

   TACL (T9205H01 - 01AUG2007), Operating System H06, Release H06.11.00
   (C)1985 Tandem (C)2005 Hewlett Packard Development Company, L.P.
   CPU 3, process has no backup
   July 3, 2007  9:59:02
   ```

Starting SecureFTP (SFTP) Sessions with MR-Win6530

1. Make sure the SSH-ZPTY, SSH-ZTCP0, SSH-ZTCP1 processes are running.
2. Start MR-Win6530.
3. Create a new profile by selecting File > New Profile > transfer, then click **OK**. A window showing your local drive folder will show in the top half of the screen.
4. Select Options > Communications > SFTP (Secure Shell) (for the interface), then click **Configure**.
5. Configure Host, User ID, and optional Password; leave the port at default 22, then click **OK**. The host ip address can be found for the $ztcp0 or $ztcp1 process with the command:

   ```
   scf; info subnet $ztcp*.#*
   ```

6. In the Options dialog box click **Apply**, then **OK**.
7. Select **File**, then **Connect**.
8. There will be two windows on the screen, Local Path and Host Path, one will show folders on the PC, the other will show the files in the default volume on the host.
9. Select in the Options dialog box, Transfer Type of ASCII or binary file.
10. Enter the PC folder name, or use the buttons to select the folder for the Local Path.
11. Enter the \<system>.$<volume>.<subvolume> for the Host Path.
12. Double-click or drag the file to be transferred.
13. Make sure Source and Destination path and file names are correct, then click **OK**.

SP Tool

Now installed as part of the OSM Low-Level Link for easy access from the Tools menu in the Low-Level Link application (without requiring a second logon), it can also be installed as a separate product from the Master installer on the NSC DVD for direct access to the SP Tool (from the Windows Start menu) without logging on to the Low-Level Link.

WAN Wizard Pro

WAN Wizard Pro helps you configure SWAN concentrators and other software and hardware for the wide area network (WAN) and local area network (LAN). It is installed from the Master installer on the NSC DVD and accessed from the Windows Start menu.

OSM-Related Service Procedures

Many OSM Guided Procedures and Service Actions are tied directly to the OSM Service Connection. For example, performing a Replace action on many system resource objects launches the guided or documented procedure to guide you through the replacement.

The complete set of service procedures – including OSM procedures and the former CSSI content – is located in the Service Procedures section of the NTL Support and Service collection.

The CSSI snapshot is no longer installable from the NSC DVD. See the NTL Support and Service collection for the most up-to-date service procedures.

5 Getting Started With OSM Applications

This section introduces the OSM client interfaces, providing the following information for each application:

- Overview of basic purpose and functionality
- Description of enhancements and functional differences between OSM and TSM (for server-side differences, see Section 3, OSM Server-Based Components)

  NOTE: While OSM is required for NS-series servers and NonStop BladeSystems (TSM does not support them), this section compares OSM applications to their TSM predecessors for the benefit of readers familiar with TSM as their previous S-series system management tool.

- Procedure for how to launch and log on to OSM applications and related tools
- Reference to documentation for how to use the applications

The OSM client interfaces include:

OSM Service Connection

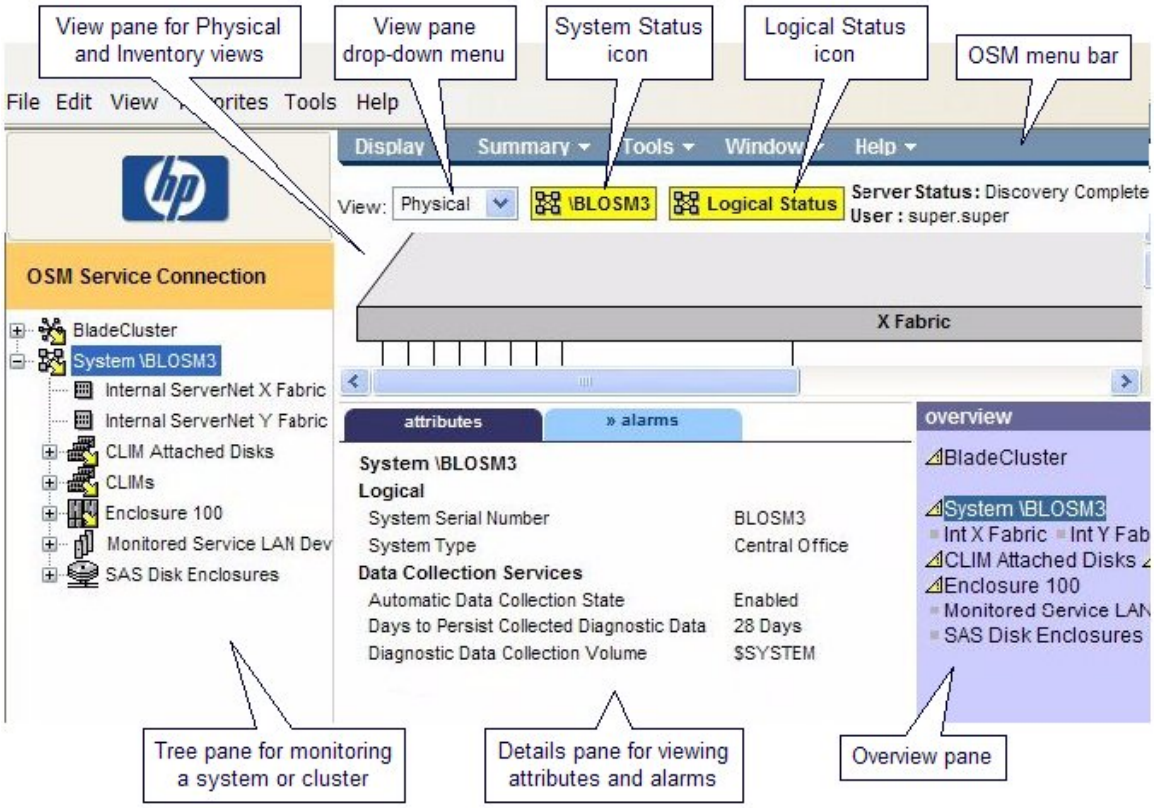
The OSM Service Connection is the primary OSM interface for monitoring and servicing your Integrity NonStop NS-series systems and NonStop ServerNet Clusters. It is also the OSM application with the most significant changes over its TSM predecessor, the TSM Service Connection (which cannot be used with Integrity NonStop NS-series systems, but the comparison remains for the benefit of those familiar with TSM on S-series). This section describes the visual and functional differences between the OSM Service Connection and the TSM Service Application, and how to establish an OSM Service Connection session.

User Interface

The OSM Service Connection provides a graphical user interface that allows you to monitor and service your NonStop systems and ServerNet Clusters. Not unlike the TSM Service Application, it contains graphical, hierarchical, and text detail representations of your system and cluster, as illustrated in Figure 1. With T0682 H02 ABU and later, the OSM toolbar has been redesigned to save space, with just text headings instead of graphic icons. It is now called the OSM menu bar. The Logical Status Button has been moved to a menu option under the Tools menu.

The OSM Service Connection is a browser-based application that resides on the server and is accessed through an Internet Explorer browser session on a system console. "Establishing an OSM Service Connection Session" (page 57) describes how to establish a connection to your system. For more information on using the OSM Service Connection, see the *OSM Service Connection User's Guide*.

Figure 1 Management Window for the OSM Service Connection



OSM-Specific Interface Differences

This list describes some of the changes between the visual display in the OSM Service Connection Management window and that of the TSM Service Application:

- There is no longer a tab to switch between System and Cluster views in the tree pane. Both system and cluster hierarchies appear in the same tree pane view.
- Use the drop-down menu in the nonscrolling area of the view pane to switch between Physical and Inventory views.
- The overview pane is now in the lower right corner of the Management window.
- To provide clarity for monitoring larger numbers of objects or nodes, OSM has been optimized for screen resolution of 1024 by 768 or higher. However, it supports resolution down to 800 by 600, and there is no minimum screen size.
- Group icons are smaller so that you can view more groups without scrolling.
- More consistent naming conventions, in the format object_type object_name (group.module.slot (if applicable)). For example, a disk named $K001-P is identified as: Disk $K001-P (1.1.15).
- Resource attributes are arranged in logical subgroups under the resource object. Some attribute names have changed.

Standard Internet Explorer Functionality

The OSM Service Connection is now launched in a secondary Internet Explorer browser window, so that it does not contain a standard Internet Explorer toolbar, which is incompatible with OSM. (See Figure 1 for an example. See "Establishing an OSM Service Connection Session" (page 57), for information about closing the initial Internet Explorer browser window.) Some standard Internet Explorer functionality can be used in conjunction with your OSM Service Connection session; other features cannot be used.

The following standard Internet Explorer functionality can be used:

- Find (Edit menu) works in some, but not all OSM panes. It works in the details pane, Inventory view (place your cursor to the left or right of the Save button), and most secondary dialogs; but does not work in the tree pane or Physical view.
- Print (File menu) works for the selected pane, but the Print dialog takes up to one minute to appear (during which time you cannot access the OSM window).

The following standard Internet Explorer functionality cannot be used during an OSM Service Connection session:

- Do not use File > New > Window from within a current OSM browser session to initiate another OSM session. Instead, you must launch a new browser window from outside the current window.
- Do not use the Go To, Stop, or Refresh options under the View menu, as they will end your current OSM Service Connection session. To refresh the OSM status for system or cluster resources, use the OSM "Rediscover Actions".
- Do not use Favorites>Add to Favorites to bookmark an OSM session. Instead, use Create Bookmark from the OSM Tools menu to create system bookmarks.

Functional Differences

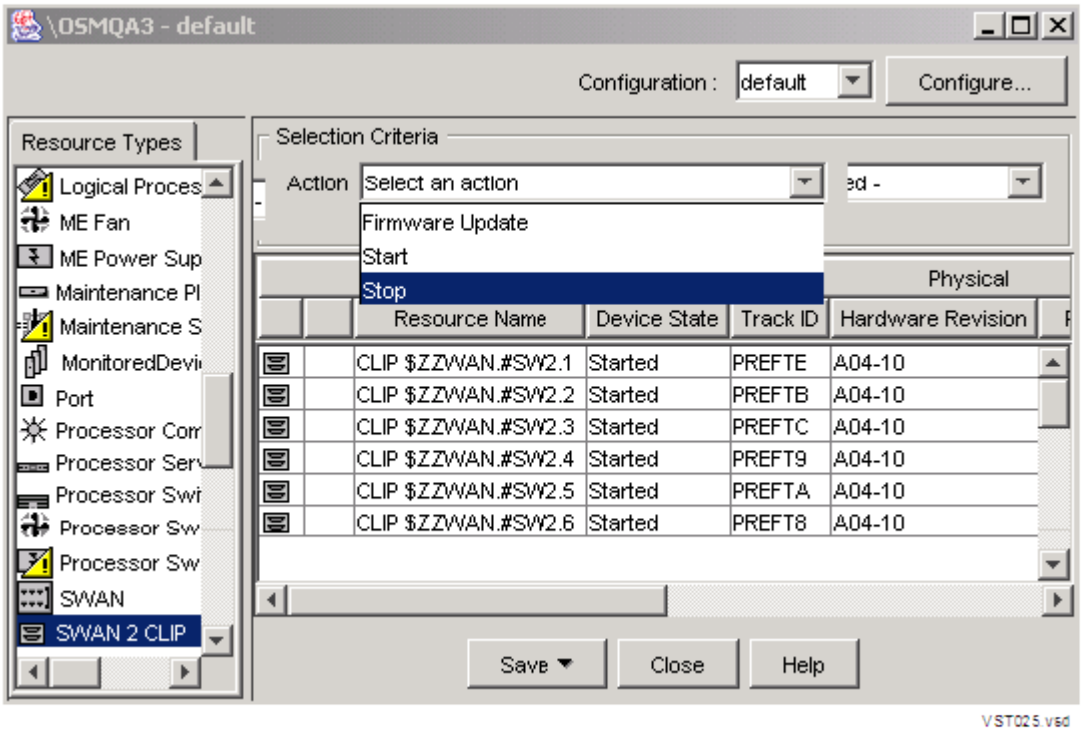
This section describes the functional differences between the OSM Service Connection and the TSM Service Application. The differences include:

Multi-Resource Actions Dialog Box

The Multi-Resource Actions dialog box is significant enhancement over TSM functionality. It is available from the Display menu, and is used to monitor or perform actions on any or all resources of the same type within your system simultaneously.

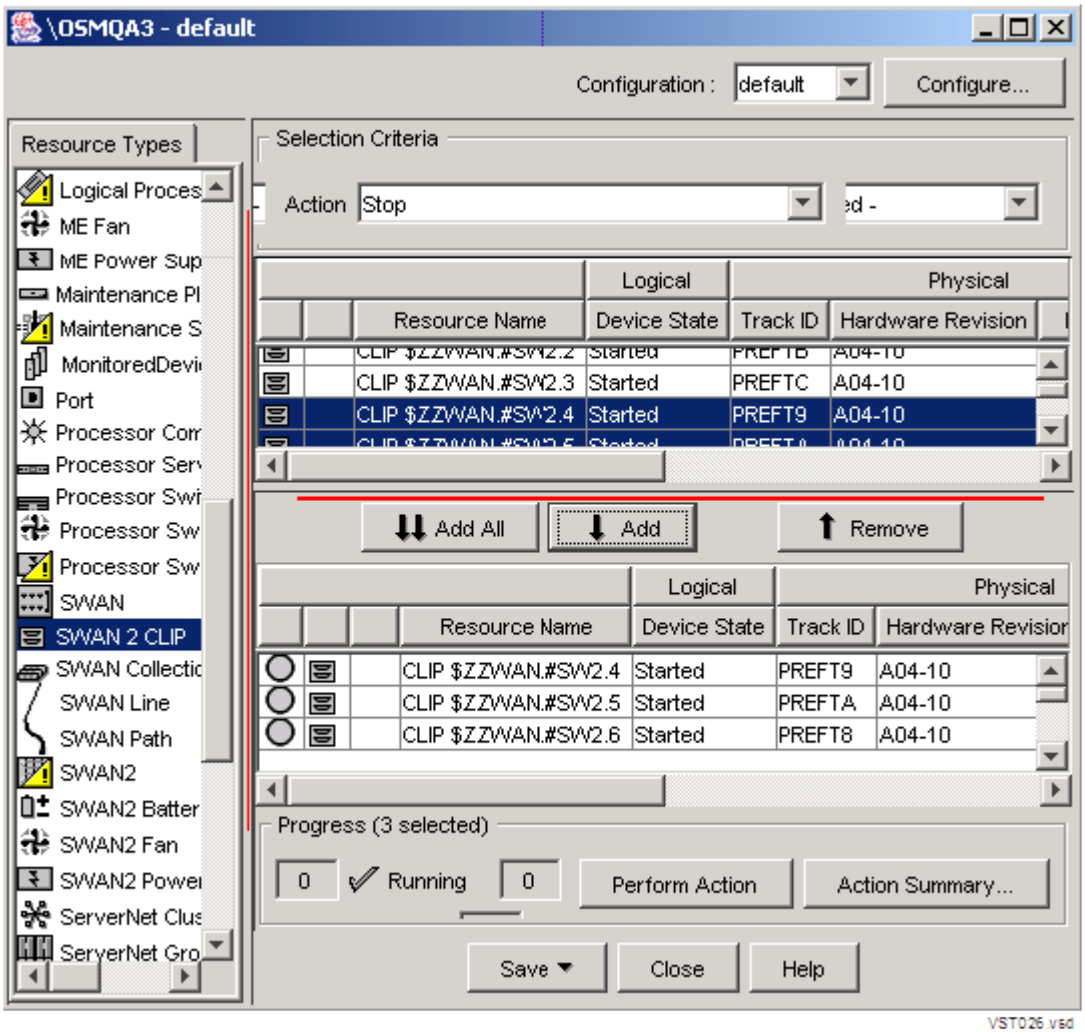
In Figure 3, the SWAN CLIP object has been selected from the list of Resource Types in the left pane. All SWAN CLIPs recognized by the system are then displayed in the right pane, along with a scrollable list of the attribute values for each CLIP. To perform an action on one or more of the SWAN CLIPs, select the desired action from the Action drop-down menu under Selection Criteria.

Figure 2 Multi-Resource Actions Dialog Box: SWAN CLIP Object Selected



In Figure 3, a continuation of the SWAN CLIP example, the Stop action has been selected from the list of available actions for the CLIP object. Using the Add or Add All buttons, select and move only the CLIPs you want to perform the action on to the blank list that appeared below the Add and Add All buttons. (The red lines in Figure 3 indicate where you can click and drag to resize the areas that these lines divide.) Then, click Perform Action to perform the Stop action on all CLIPs in that lower list. The progress bar below the list of selected CLIPs indicates the status of each individual Stop action (in this example, three CLIPs were chosen to be stopped. For information on failed actions, click Action Summary. You can update SWAN CLIP firmware and then restart the CLIPs using this dialog box in similar fashion.

Figure 3 Multi-Resource Actions Dialog Box: Performing a SWAN CLIP Action



The Multi-Resource Actions dialog box has a new look from G-series releases. Also, starting with H06.04, the Multi-Resource Actions dialog box features a Save button (below the Progress bar), which can be used to save a file, viewable in Microsoft Excel or Apache OpenOffice, containing the information displayed in the Multi-Resource Actions dialog box for either the selected resource type (SWAN CLIPs, in this case) or all system resources.

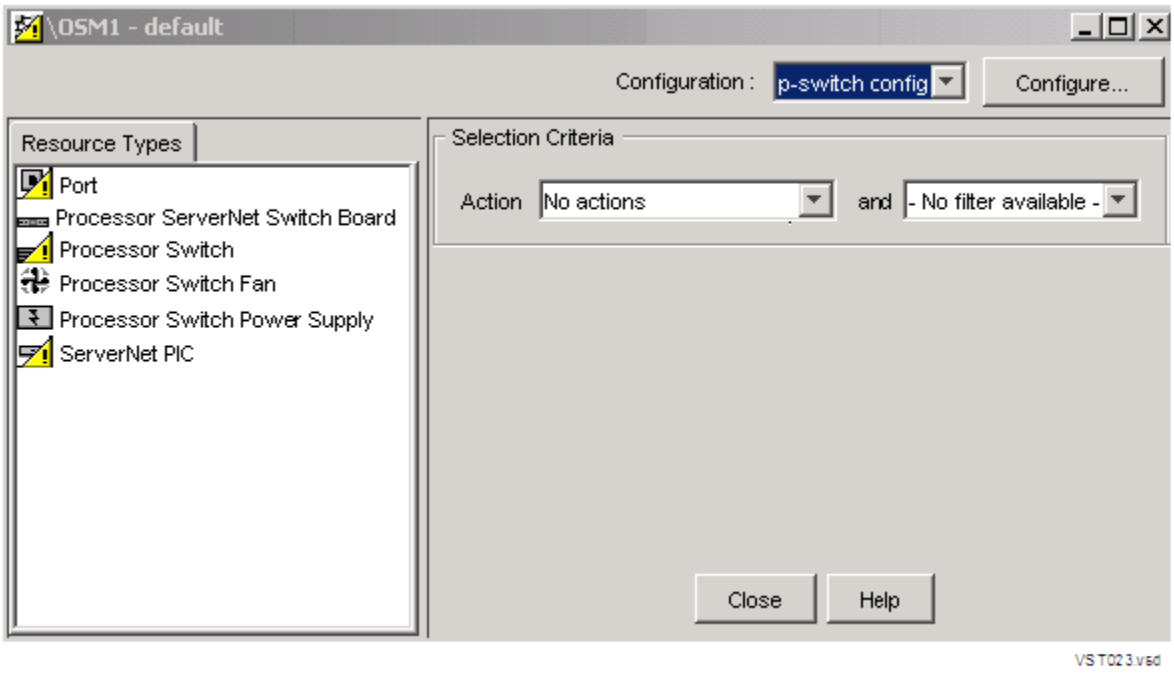
△ **CAUTION:** You should not use the Multi-Resource Actions dialog box to update ME firmware or ME FPGA simultaneously on both fabrics, or a system outage might occur.

Another feature of the Multi-Resource Actions dialog box for H-and J-series is that you can create and save a customized "Resource View" of your system. This makes it easy to monitor and service a select group of resources in one view. To create a customized resource view:

1. In the upper right corner of the Multi-Resource Actions dialog box, select default from the Configuration drop-down menu (or choose an existing customized view that you wish to change), then click Configure.
2. In the Multi-Resource Configuration window, choose default from the Configuration drop-down menu and enter a new name for the customized view you are creating (or again, you can choose an existing resource view to alter or build a new view from).
3. In the list of resources select only those resources that you want to appear in your customized view (it might be easiest to Deselect All, then click to re-select just the resources you want). Note: You cannot deselect resources while the name "default" appears in the Configuration window (see step 2).

4. Click Save to save this customized “Resource View.” To use this view in the future, choose it (by the name you gave it) from Multi-Resource Actions dialog box Configuration drop-down menu (instead of “default”). The next time you log on to the OSM Service Connection, it will also appear in the Resource Views drop-down menu, located under the Display menu.

Figure 4 Example of a Customized Resource View



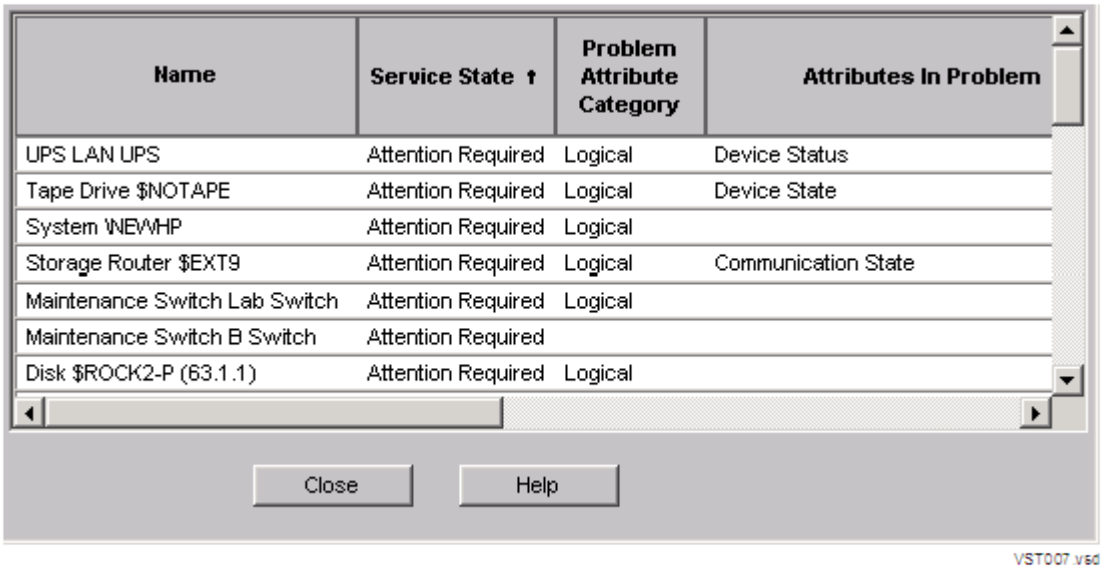
Problem Summary Dialog Box

The Problem Summary dialog box provides a summary of all system and cluster resources currently reporting problems.

The example in Figure 5 shows a summary of all problems on one system. The first line item indicates that a UPS is reporting a problem in its Service State and Device Status attributes.

The Problem Summary dialog box is resizable and scrollable, and you can sort by column heading to organize the information to suit your needs. Additional columns, not visible in this example, include alarms and attributes that you chose to acknowledge (see “Suppressing Alarms, Attributes, and Problem IRs”). Alarms not suppressed are represented by a Service State value other than OK (Attention Required or Service Required).

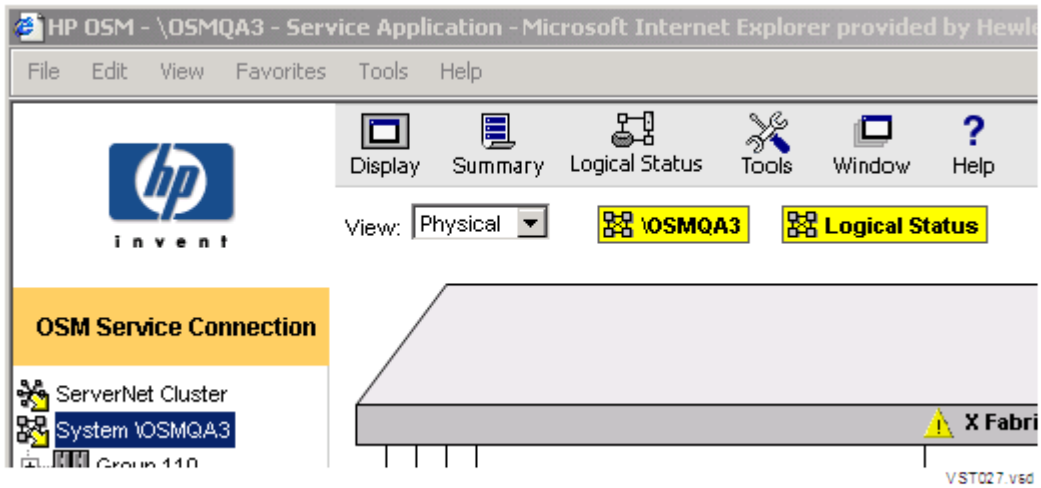
Figure 5 Problem Summary Dialog Box



Logical Status Information

The Logical Status icon and view are included in T0682 AAM and later. The Logical Status icon, displayed next to the System Status icon in the View pane toolbar (see Figure 6), gives you a quick indicator of the status of the components that are included in the Logical Status view – those being all disks, logical processors, LIFs, and SWAN paths on the system. As with the System Status icon, green indicates no problems; yellow indicates problem conditions exist on one or more object.

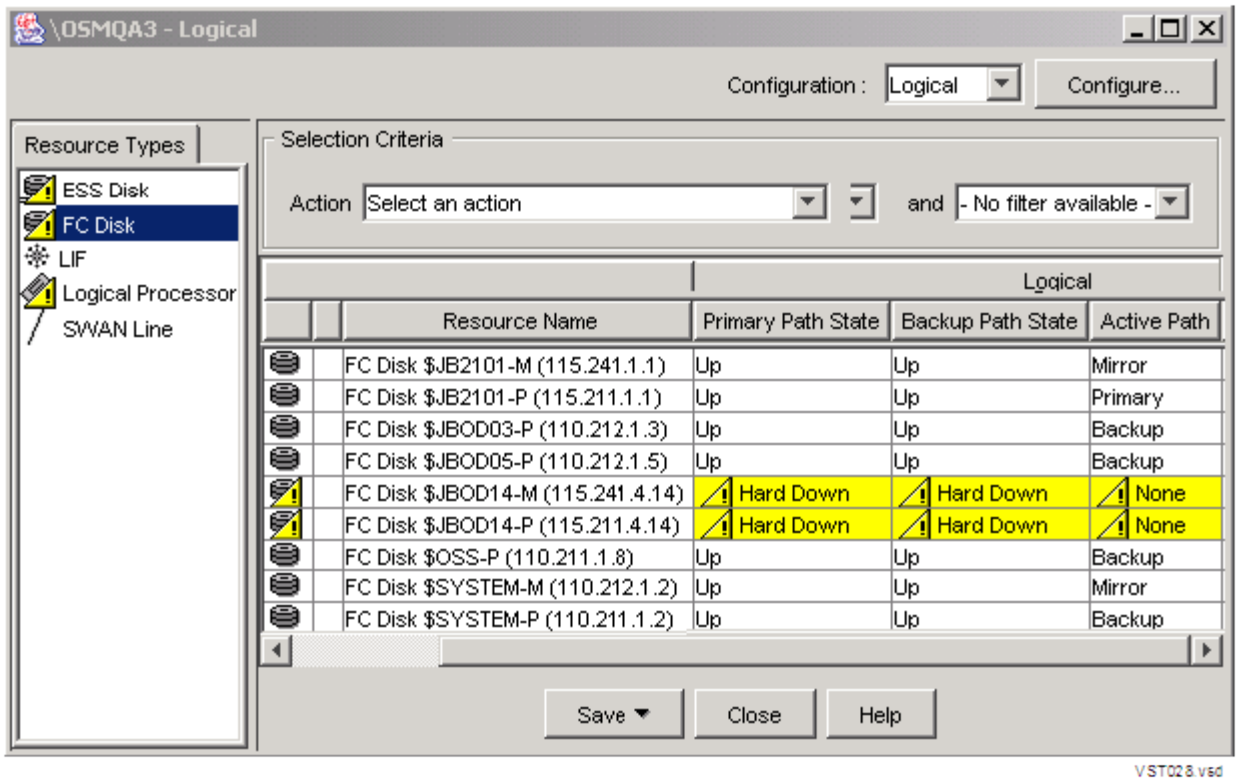
Figure 6 Logical Status Button and Icon



When the Logical Status icon turns yellow, as in Figure 6, click the Logical Status button, located just above the icon on the OSM toolbar (for T0682 H02 ABU and later, select Logical Status from the Tools menu instead). This displays a Logical Status dialog box (see Figure 7). It works like the Multi-Resource Actions dialog box, in that you can select which Logical Status component resource types you want to monitor. In this example, the user has selected the FC disk object, to take a closer look at all problems being reported by OSM on all Fibre Channel disks on the system.

Unlike the personalized Resource Views that can be created in the Multi-Resource Actions dialog box, the Logical Status dialog box is not customizable. And unlike the System Status icon, which will remain green if you suppress (or acknowledge) all problem conditions that exist on the system, the Logical Status icon remains yellow even if problem conditions reported on Logical Status components are suppressed.

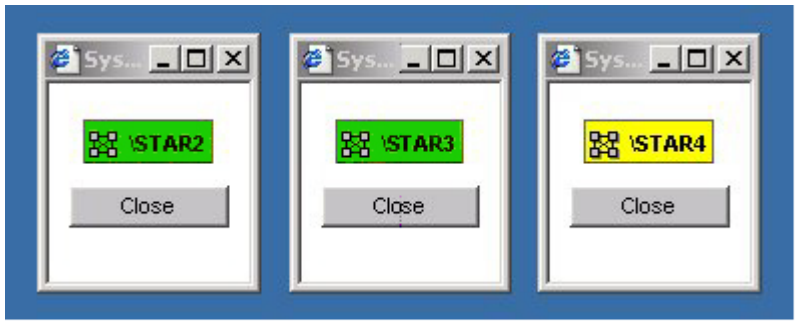
Figure 7 Logical Status View



System Status Window

If you are monitoring several systems simultaneously, OSM offers a more convenient tracking method of systems than resizing all of your Management windows. Select System Status from the Summary menu to create a small, separate window displaying just the system icon for each system. You can then minimize (but not close) all Management windows and track system health by the color of the system icon. An icon changes from green to yellow to indicate degraded conditions within the system or cluster (as Figure 8 illustrates). To investigate a system icon that turns yellow, maximize the corresponding Management window and expand the tree pane to identify the source of the degraded conditions.

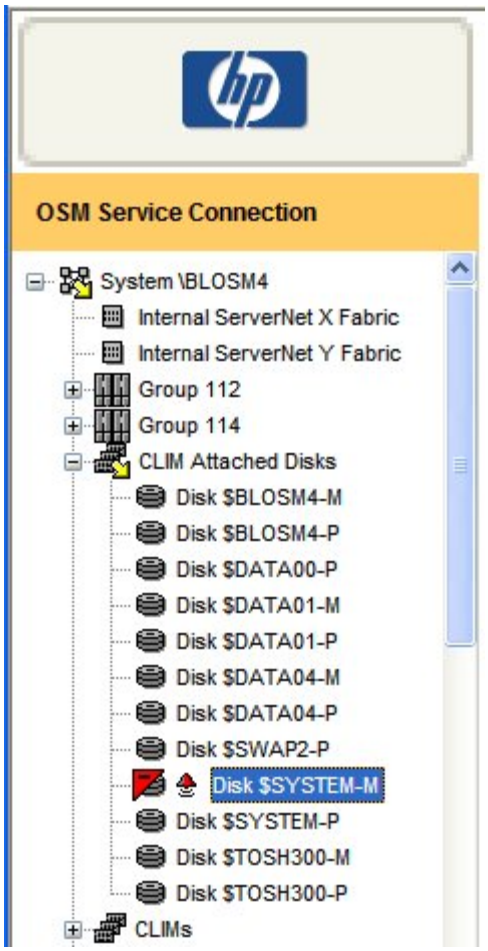
Figure 8 System Status Windows



Propagation of Subcomponent Problems

Alarms and problem attributes on resources in the OSM Service Connection are propagated up to parent objects. The OSM Tree pane displays a special icon over parent objects to indicate problems with subcomponents (as Figure 9 illustrates).

Figure 9 Propagation of Subcomponent State Problems



Suppressing Alarms, Attributes, and Problem IRs

Another feature in OSM is the ability to suppress alarms, attributes, and problem IRs. You can acknowledge a known problem and keep it from propagating problem conditions all the way up to the system icon (as Figure 10 illustrates).

In this example, you might want to suppress the problem attribute on the tape drive because it is a known problem and you do not want to miss other problems that arise on the system. After you suppress the problem attribute (see Figure 5-11), that resource's icon changes to show a yellow check mark. No container objects, up to and including the system icon, now show degraded conditions.

Figure 10 Before Applying Attribute Suppression

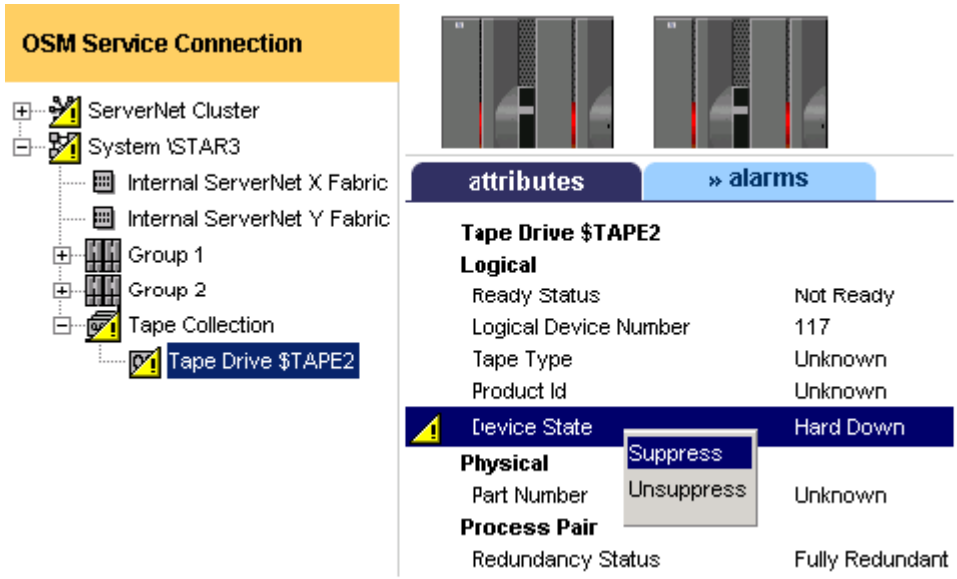
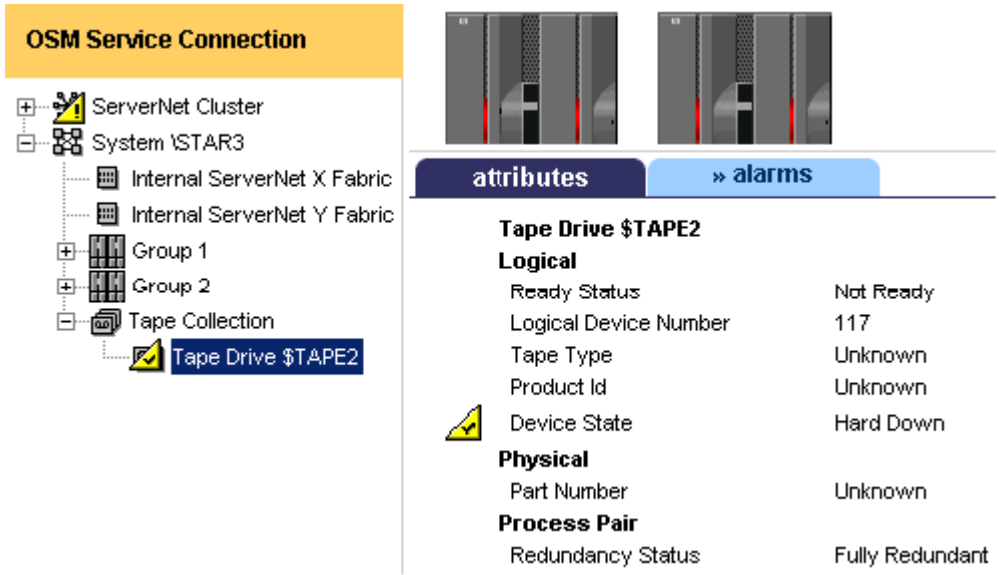


Figure 11 After Applying Attribute Suppression



Suppressing Problem Attributes

To suppress a problem attribute, select the attribute (in either the Attributes tab or the Attributes dialog box), right-click, and select **Suppress** (see Figure 10), the either **Temporary** or **Permanent** suppression. Select temporary to suppress as long the specific value of the attribute (Hard Down, in this example) remains the same. If you bring the tape drive up and then it returns to the Hard Down state, that value is no longer suppressed. Permanent suppression continues to suppress a value of Hard Down for this tape drive until you unsuppress it. OSM Rediscover actions have no effect on suppressed attributes.

With OSM version T0682 H02 ABX and later, suppression of attributes is persistent by default. That means attributes suppressed in the OSM Service Connection remain suppressed even after the OSM server has been stopped and restarted, unless the conditions for ending Temporary suppression have been met. To disable suppression persistence with OSM T0682 H02 ABX and later, see "Disabling Alarm and Attribute Suppression Persistence" (page 21) for the necessary OSMCONF parameter.

Persistence is not available in OSM versions prior to T0682 H02 ABX, meaning that all suppressed values revert to unsuppressed when the current OSM server session is ended.

To unsuppress a problem attribute, select the attribute, right-click, and select Unsuppress. You cannot suppress a Service State or Subcomponent State attribute. A Service State attribute of something other than OK is caused by one or more alarms on the resource. You must suppress the alarm to acknowledge (or clear) the Service State. To acknowledge a problem reported by the Subcomponent State attribute, you must find the root of the problem by expanding the object in the tree pane to find the one or more subcomponents causing problems to be propagated, then suppress those attributes or alarms.

Suppressing Alarms

To suppress an alarm, select the alarm (in either the Alarms tab or the Alarms dialog box), right-click, and select **Suppress**, the either **Temporary** or **Permanent**. If you select Temporary suppression and the same alarm is generated again on this object at a later time, state propagation will occur. If you select Permanent suppression and the same alarm is generated again on this object at a later time, state propagation will not occur. Even if the alarm is generated again in the future, state propagation does not occur until you unsuppress the alarm. OSM Rediscover actions have no effect on suppressed alarms.

With OSM version T0682 H02 ABX and later, suppression of alarms is persistent by default. That means alarms suppressed in the OSM Service Connection remain suppressed even after the OSM server has been stopped and restarted, unless the conditions for ending Temporary suppression have been met. To disable suppression persistence with OSM T0682 H02 ABX and later, see "Disabling Alarm and Attribute Suppression Persistence" (page 21) for the necessary OSMCONF parameter.

Persistence is not available in OSM versions prior to T0682 H02 ABX, meaning that all suppressed values revert to unsuppressed when the current OSM server session is ended.

To unsuppress an alarm, select the alarm, right-click, and select Unsuppress.

Suppressing BladeCluster Alarms

Available on OSM version T0682 H02 ABZ or later, the "Place Local Node in Service" action on the BladeCluster object allows you to prevent all other directly-connected nodes from remotely notifying (dialing out) an alarm as soon as SNETMON is stopped on the local node, or that node is halted. This alarm suppression only works on remote nodes that are running T0682 H02 ABZ or later as well. For more information, see the OSM Service Connection online help or the *NonStop BladeCluster Solution Manual*.

Suppressing Problem Incident Report Creation

A system-level action allows you to suppress the creation of Problem Incident Reports (IRs) and remote notifications (dial-outs) for a specified period of time.. This is often used by guided procedures or called for by service procedures to prevent remote notifications caused by activities related to the procedure. The default suppression time of 40 minutes can be changed in the OSMCONF file or extended for an action currently in progress by using the Extend Problem Incident Report Suppression Time action. Suppression can also be canceled at any time through the Unsuppress Problem Incident Report Creation action, also found under the System object.

With OSM T0682 AAY and later, you can also prevent ServerNet Problem IRs on one node from being propagated to other nodes on the same ServerNet Cluster (see "Suppressing Redundant IRs from ServerNet Cluster Nodes" (page 22)).

Rediscover Actions

Rediscover is supported as an action on all system and some cluster objects. For most objects, Rediscover is available only in the shortcut menu.

Rediscover causes OSM to refresh and reanalyze the object and all subcomponents. You can update all system resources by performing the Rediscover action under the System object, or save

time by just performing a Rediscover for the object you are concerned with at the time (and individual group or ServerNet adapter, for example).

Refresh refers to OSM updating the attribute values displayed in the OSM Service Connection interface. Reanalyze refers to the running of OSM incident analysis, which checks EMS event messages and creates alarms in OSM if certain conditions exist.

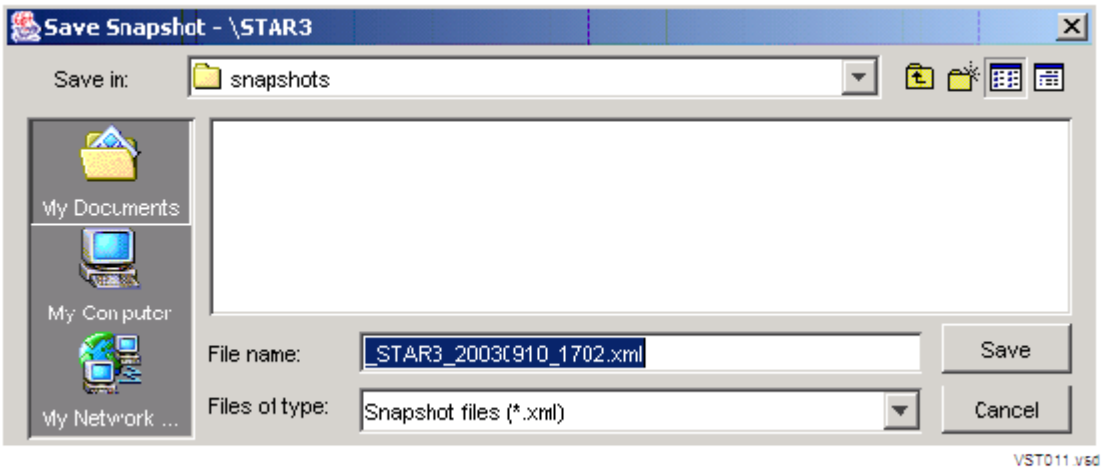
Snapshot Functionality

Snapshots preserve a view of your system at a point in time for use in diagnosing problems later or remotely. You can save snapshots from the OSM Service Connection client without having to change a configuration file setting (as was the case in TSM).

Saving Snapshots

Snapshots are created and saved manually from within the OSM Service Connection. Select Save Snapshot from the OSM Tools menu.

The suggested (default) name includes the system name and the date and time that the snapshot was created. The default location is ZSUPPORT>OSM>snapshots on your PC's local disk.

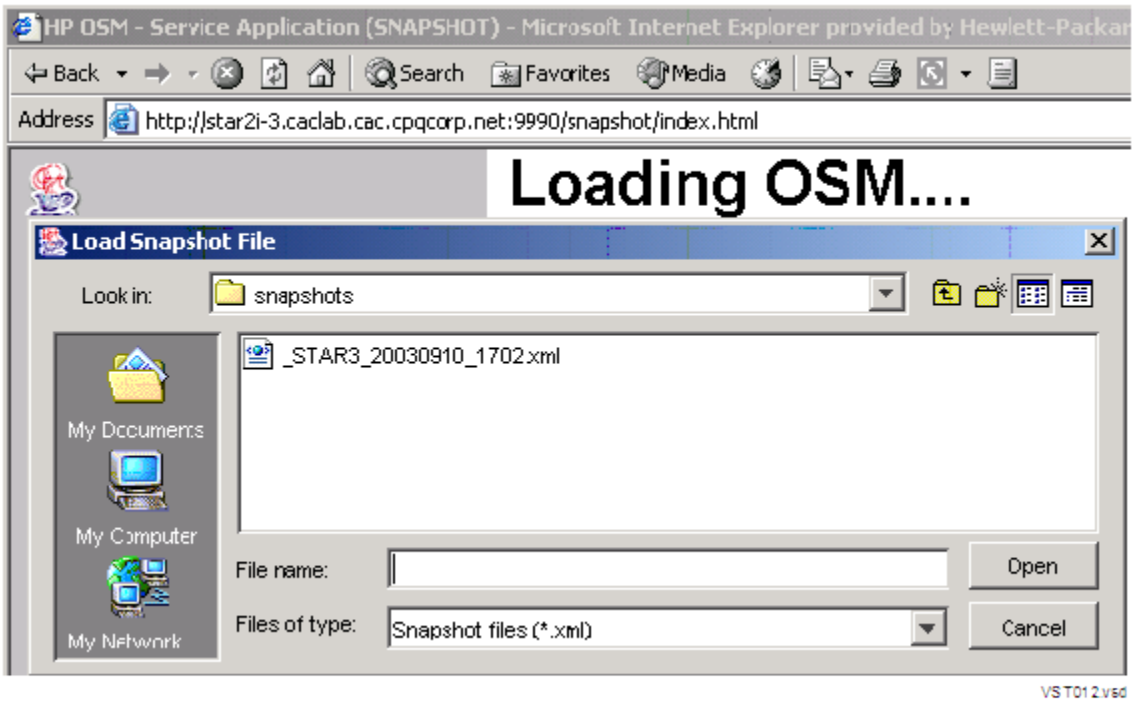


Loading Snapshots

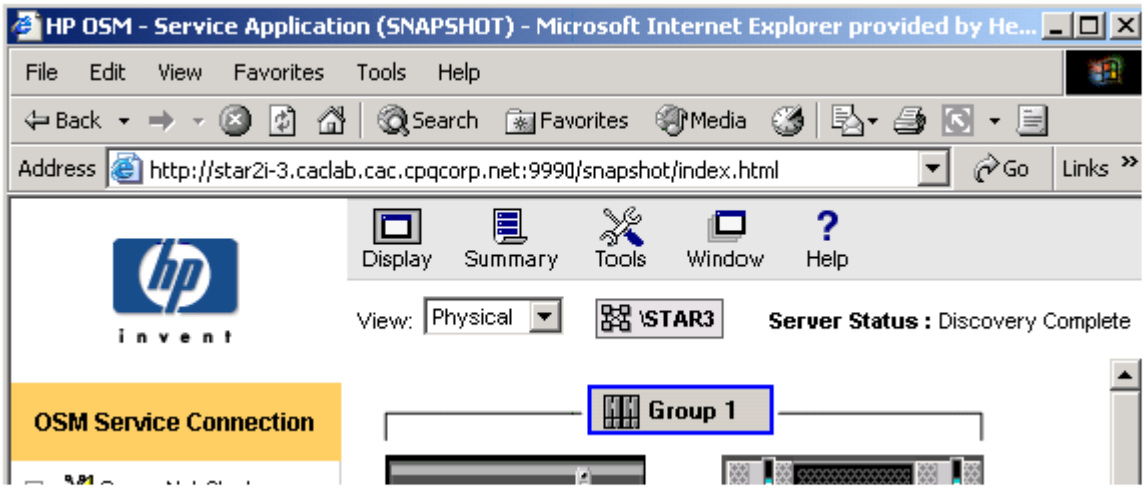
Snapshot files can be transferred to and loaded on any workstation capable of establishing an OSM Service Connection session. From the workstation containing the snapshot file:

1. Start a new Internet Explorer browser session.
2. In the address bar, enter the URL of any valid OSM service connection (it does not have to be the same system as the snapshot file you want to load), followed by snapshot/index.html.

3. In the Load Snapshot File dialog box, navigate to the snapshot file you want to view and click Open.



The snapshot looks like a regular OSM Service Connection session, except that "(SNAPSHOT)" appears in the title bar and the system icon in the view pane (\STAR3 in this example) is gray instead of yellow or green, which is used to indicate status in active OSM Service Connection sessions.



Limitations:

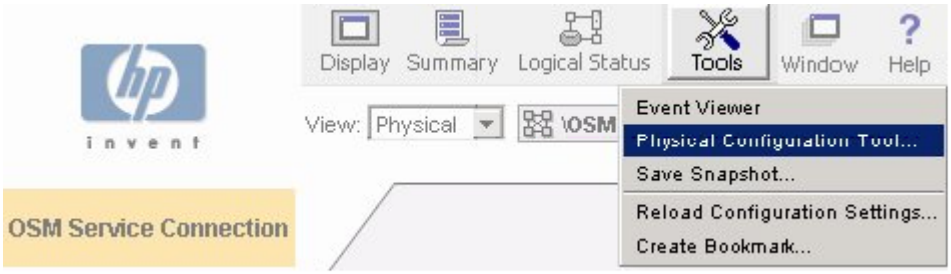
- You cannot use an existing OSM browser window to load a new snapshot or to start a new OSM Service Connection session.
- You cannot be logged on to a server and have a snapshot loaded at the same time in the same window. However, you can be logged on to a server and view a snapshot by using two separate browser windows.

Physical Configuration Tool

With T0682 H02 AAN and later, the OSM Service Connection provides the Physical Configuration Tool. You can use it to create and save a physical display of the racks in which your modular NS-series system or NonStop BladeSystem resides.

To launch the tool, within the OSM Service Connection, select Physical Configuration Tool from the Tools menu on the OSM menu bar (see Figure 12).

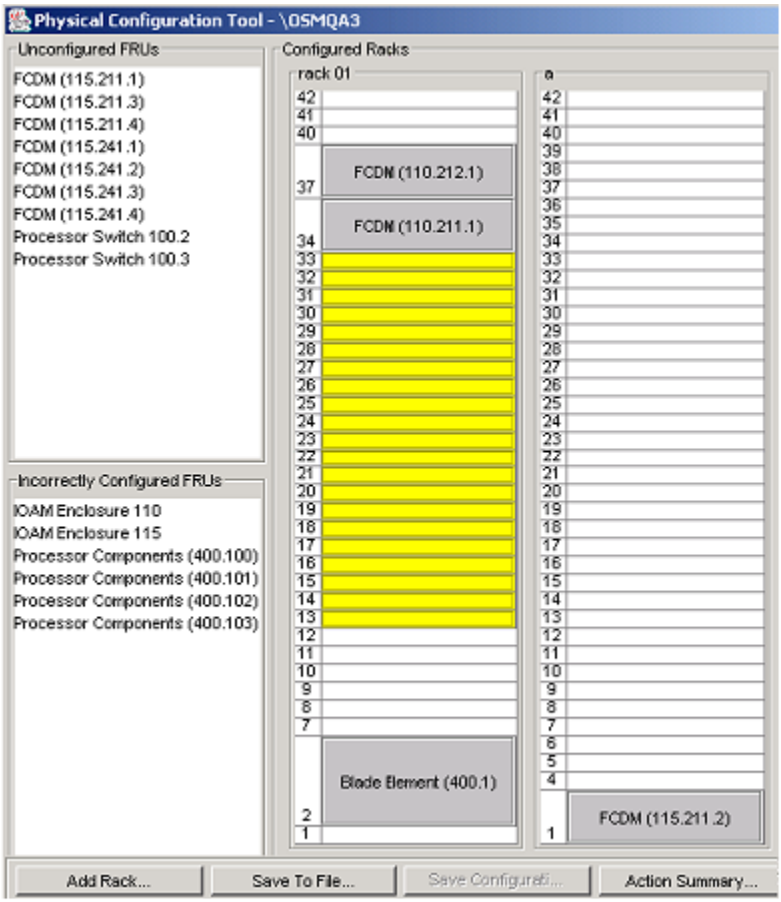
Figure 12 Launching the Physical Configuration Tool



When first launched, the Physical Configuration Tool displays whatever OSM knows about the current physical configuration of your system (see Figure 13 (page 56)). This information is based solely on Rack Name and Rack Offset values assigned by OSM users through individual Set Physical Location actions on modular components. The Set Physical Location action is available for Blade Elements, FCDMs, IOAM Enclosures, VIO Modules (which is how OSM represents VIO enclosures), Processor Switch Modules, and Processor Components (LSUs). The problems with this information include:

- Components not assigned Rack Name and Rack Offset values are displayed in the Unconfigured FRUs pane rather than in the Configured Racks pane (the upper left pane, as illustrated in Figure 13).
- Components given even slightly overlapping Rack Offset values are displayed in the Incorrectly Configured FRUs pane (the lower left pane, as illustrated in Figure 13). Their locations in the Configured Racks pane are displayed as yellow, unlabeled areas (also illustrated in Figure 13).
- If you moved a component but did not use the action to update it, it continues to be displayed in the old (incorrect) location.
- If Rack Names are not precise. For example, if one FCDM is designated as Rack 1, another in the same rack is designated as rack 01, the Physical Configuration Tool displays those as two separate racks.

Figure 13 Physical Configuration Tool Before Modifying



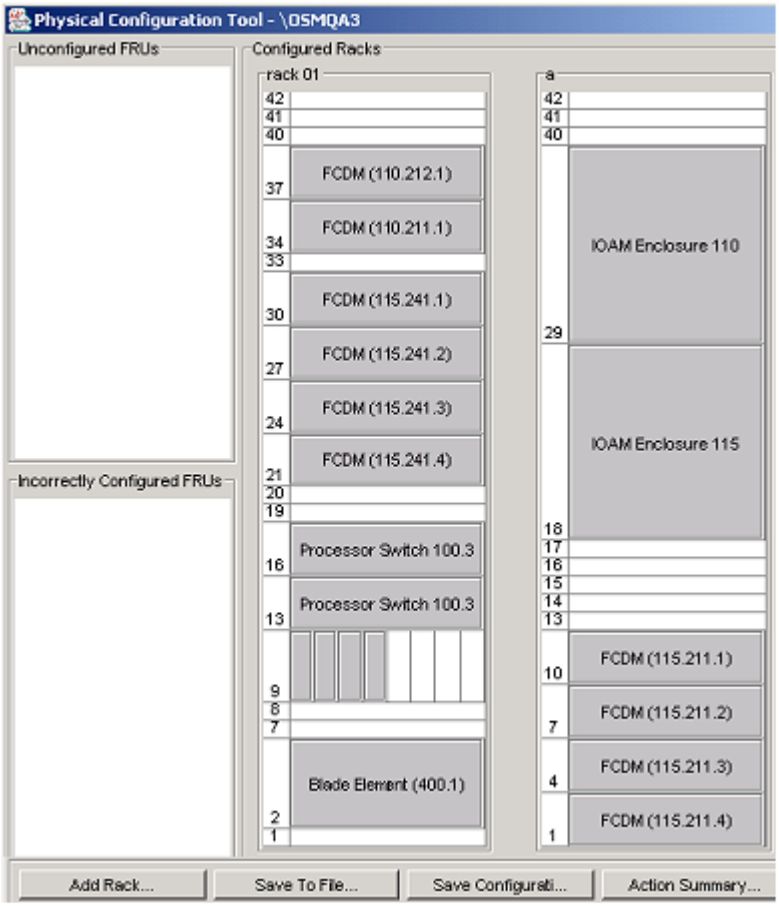
Now, with the Physical Configuration Tool, there is no need to use the Set Physical Location action* to specify Rack Name or Rack Offset. Instead, use the Physical Configuration Tool to:

- Drag and drop components between and within the panes to accurately depict your actual physical configuration.
- Click Add Rack to add new racks to the Configured Racks pane.
- Save the physical view for future use within the Physical Configuration Tool and even save the view to an HTML file for use outside of OSM.

* See "Example: No Previous Rack Names or Rack Offsets Assigned" (page 57).

Once you have used the Physical Configuration Tool to move all modular components from the Unconfigured FRUs pane and the Incorrectly Configured FRUs pane to their correct locations, and resolved any overlapping areas (displayed as yellow in the Configured Racks pane), your physical view should look more like the one pictured in Figure 14 (page 57)).

Figure 14 Physical Configuration Tool After Modifying



Example: No Previous Rack Names or Rack Offsets Assigned

If the modular components in your system were never assigned Rack Name and Rack Offset values through Set Physical Location actions, you should find them listed in the Unconfigured FRUs pane when you first launch the Physical Configuration Tool.

1. Click Add Rack to create representations of the racks in your system.
2. Drag and drop the modular components to the appropriate location in each rack.
3. Click Save Configuration to save the view you have created for future use from within the Physical Configuration Tool.

Miscellaneous Changes

- There is no Status Log menu option to launch the Windows Event Viewer because the OSM Service Connection does not reside on the PC and therefore does not create Windows events.
- You cannot launch a terminal emulator session from the OSM Service Connection; it is available from the OSM Low-Level Link and from the Windows Start menu.
- Quick-key accelerators are reserved for standard Internet Explorer functionality; therefore, they are not customizable for OSM.

Establishing an OSM Service Connection Session

You can initiate an OSM Service Connection session in two ways. The first is quicker if you meet the qualifications.

Method 1: Using Home Page Bookmarks

This method is available only if you have installed the OSM Console Tools client component, and can only be used for direct access to an OSM Service Connection session only if you have an

OSM bookmark for the system you want to access. If not installed, or the home page does not display an OSM bookmark for your system, see "Method 2: Without Client Installation or Bookmarks".

NOTE: You can create OSM Bookmarks in one of two ways. The home page launched by using the Start menu shortcut automatically converts your existing TSM system list to bookmarks that you use for accessing systems through OSM (if those systems are now running OSM server software). You can also create your own bookmarks for future use from within the OSM Service Connection. Once you are logged on to a system, select **Create Bookmark** from the OSM Tools menu. If you save the bookmark to the OSM Service Connection folder automatically created in your Internet Explorer Favorites directory, these bookmarks also appear on the home page the next time you launch it.

1. From the Start menu, select All Programs > HP OSM > OSM Service Connection.
2. From the left column of the OSM Service Connection home page, select a bookmark for the system you want to access. These bookmarks include the ones created automatically from your existing TSM system list and any additional ones you created during previous OSM sessions.
3. Proceed to "Logging On".

Figure 15 OSM Service Connection Home Page

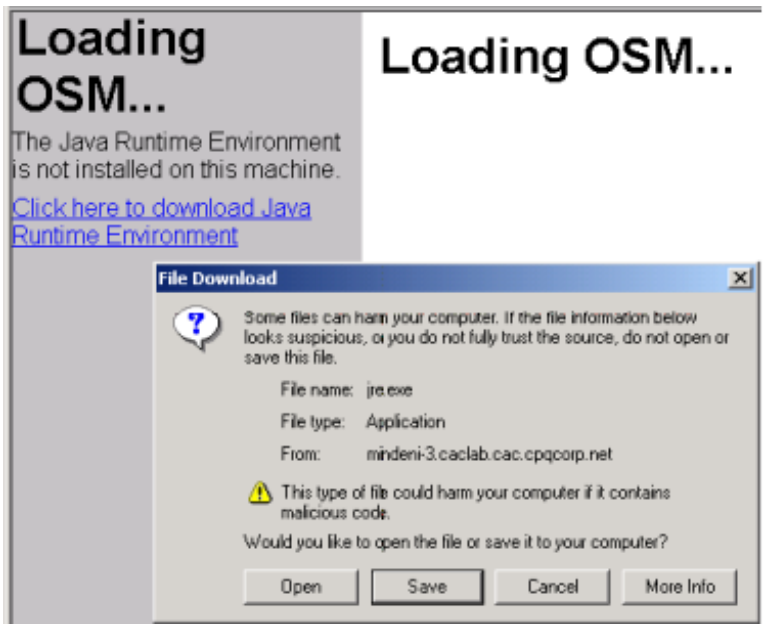
Method 2: Without Client Installation or Bookmarks

1. Launch a new* Internet Explorer browser window.
2. In the Internet Explorer Address dialog box, enter a system URL. Either:
3. Press Enter.
4. Proceed to "Logging On".

* Never reuse an existing OSM session window or launch a new browser window from the Internet Explorer menu bar of an existing OSM session window.

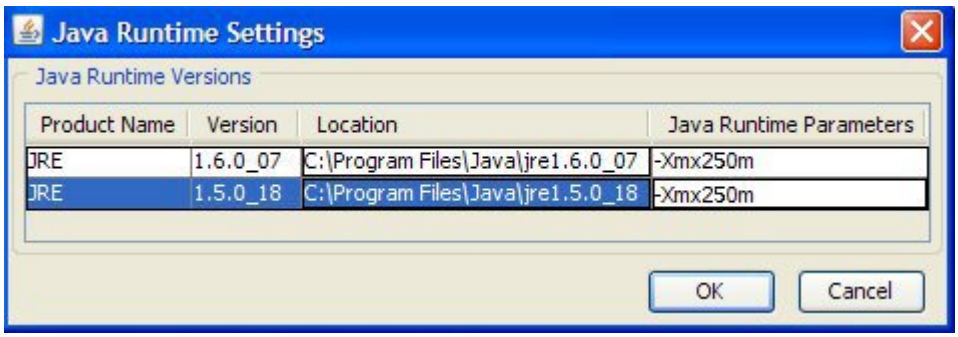
1. The first time you try to establish an OSM Service Connection session, you are prompted to "download Java Runtime Environment." Select Open and install it according to instructions (accepting typical and default options).

△ **CAUTION:** Do not upgrade Java Runtime Environment on your PC unless prompted to do so by OSM. OSM currently supports Java 5, Update 22 (and later) and Java 6, Update 35 (and later), but not Java 7. Upgrading to an unsupported version can cause OSM server to stop running or not work properly.



Upon installing a supported version of Java Runtime Environment on your console, you can ensure peak OSM performance by checking to make sure a particular runtime parameter is set:

1. Close all Internet Explorer windows.
2. Go to Start > Control Pane > **Java**.
3. In the Java Control Panel dialog box, select the **Java** tab.
4. Under "Java Applet Runtime Settings," click **View**.
5. In the Java Runtime Settings dialog box, make sure that `-Xmx150m` is entered under the "Java Runtime Parameters" column for each supported JRE version listed. If running Windows 7, `-Xmx250m` should be entered instead.

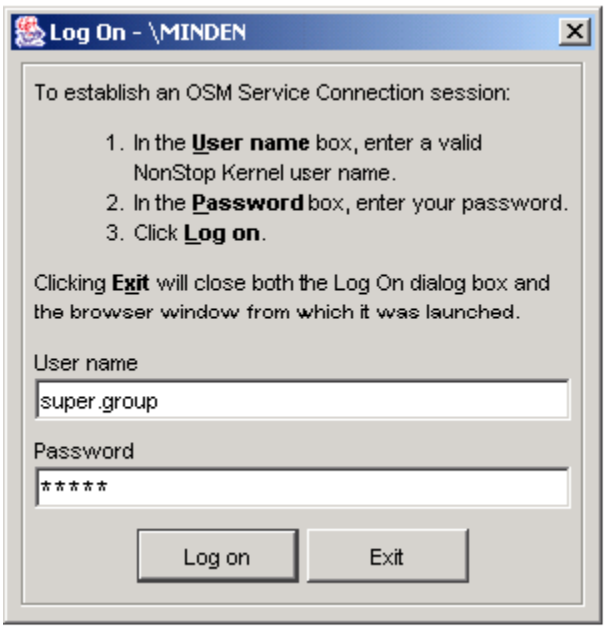


6. Click **OK** to dismiss both the Java Runtime Settings and Java Control Panel dialog boxes.

2. If you were prompted to download Java Runtime Environment, repeat the launching procedure you used to get to this point ("Method 1: Using Home Page Bookmarks" or "Method 2: Without

Client Installation or Bookmarks"). You should not be prompted to download Java or restart again (unless JRE is upgraded in a future OSM server SPR).

3. If a dialog box asks you to "trust the signed applet distributed by Hewlett-Packard," you must select Always or Yes. If you select Always, you will not be prompted again in subsequent OSM logon attempts.
4. You might also be prompted to "trust an SSL certificate distributed by Hewlett-Packard." You must select Always before OSM system discovery completes, or the OSM Toolbar might appear blank.
5. In the Log On dialog box, enter a valid user name and password and click Log on.



Starting with G06.24, an OSM Service Connection session is launched in a secondary Internet Explorer browser window to eliminate the standard IE toolbar buttons which took up screen space and were largely incompatible with OSM. The initial window, visible briefly before being hidden behind the window in which the OSM session is established, is blank except for the following instructions:

You should close that browser window as instructed (and click "Yes" to confirm your intention to close the window) and not use it for other purposes.

OSM Guided Procedures and Service Actions

OSM provides service functionality through a combination of guided procedures and interactive service actions. Unlike TSM, OSM guided procedures are integrated into the OSM Service Connection (and are launched by OSM actions) rather than being launched separately from the Start menu.

Table 2 lists and describes the OSM guided procedures and service actions that apply to NonStop BladeSystems, NonStop NS-series servers, NonStop ServerNet Clusters, and legacy NonStop S-series components.

Table 2 OSM Guided Procedures and Service Actions

Function	How to Access
Replace CLIMs and CLIM Hard Drives	OSM guided procedure launched by an action on the CLIM and CLIM Hard Disk objects to make the replacement of CLIMs and CLIM Hard Drives more automated.
Register CLIMs with Key Managers	OSM guided procedure launched by an action on the CLIMs (container) object. It supports NonStop Volume Level Encryption by providing a simple and secure method for registering CLIMs with Enterprise Secure Key Managers.
Perform Data Sanitization	OSM guided procedure launched by an action of the same name on the System object in the OSM Service Connection. It provides a simple and secure method for erasing all data from disk drives that are to be retired from service. For more information, see the online help available from within the guided procedure.
Get SMARTSSD Wear Status Summary	OSM guided procedure that allows you to view and save a summary of the SMARTSSD wear status for any or all Solid State SAS disk drives on the system. It displays the same SMARTSSD Wear Gauge values for each drive as the Show SMARTSSD Wear Gauge action that is available on individual Solid State SAS disk drives. This guided procedure allows you to display the information for multiple (any or all selected) drives in a single interface and to save the resulting data, if desired, in `.csv` (or comma delimited) format for use in Microsoft Excel or Apache OpenOffice (which is available in OSM Console Tools T0634 ABD and later).
Modular I/O and Integrity NonStop NS-Series Hardware	
Replace IOAM Enclosure or (subcomponent) ServerNet Switch Board	OSM guided procedure* launched by **Replace IOAM Enclosure or ServerNet Switch Board** action on the IOAM Enclosure or **Replace** action on the ServerNet Switch Board. * On an HP Integrity NonStop NS14000 series or NS1000 system in which there is an IOAM enclosure, these are documented rather than guided procedures.
Replace a Fibre Channel ServerNet adapter (FCSA)	Interactive **Replace** action on the FCSA object (along with online help from Help button).
Replace P-Switch module or (subcomponent) ServerNet Switch Board	OSM guided procedure launched by the **Replace** action on the P-Switch module or **Replace** action on the ServerNet Switch Board.
Replace Blade Element component	Documented procedures launched by **Replace** action on the Blade Element object to replace entire Blade Element, front panel display, processor board, memory board, reintegration board, fan, optics adapter, or I/O interface board. A **Replace** action on the Blade Element Power Supply object launches a procedure for replacing that component.
Replace LSU component	Documented procedures launched by **Replace** action on the Processor Components object
Blade Complex Firmware Update	OSM guided procedure launched by the **Firmware Update** action on the Blade Complex object, to update Blade Element firmware in the each Blade Complex. For Integrity NonStop NS1000 and NS5000T systems, a documented firmware update procedure is launched from the Blade Element object instead.

Table 2 OSM Guided Procedures and Service Actions *(continued)*

Function	How to Access
Replace (FCDM) Disk Drive Enclosure or component	Documented procedure launched by **Replace** action on the enclosure or component to be replaced.
Replace 4-Port ServerNet Extender (4PSE)	Documented procedure launched by **Replace** action on the 4PSE object (Integrity NonStop NS14000 or NS1000 servers with IOAM enclosure only).
Check Storage Dependence on ServerNet Fabric Bring Up and Balance Storage Paths	OSM guided procedures, launched by actions of the same names on the System object in the OSM Service Connection, help you prepare for and recover from activities that disrupt ServerNet traffic on one fabric.
Replacing a VIO Logic Board and other components	For Integrity NonStop NS14000 or NS1000 servers with VIO enclosures only, documented replacement procedures are launched by **Replace** action on the VIO Module, VIO Logic Board, VIO G4SA, Optical Extender PIC, VIO Power Supply, and VIO Fan objects.
NonStop S-Series Hardware (applicable to NS-series as a legacy attachment)	
Replace IOMF or SNDA	OSM guided procedures launched by **Replace** action on the CRU to be replaced.
Replace Power Supply	Interactive **Replace** action on the Power Supply to be replaced.
ServerNet Cluster	
Adding a node to a ServerNet Cluster	OSM guided procedure launched by **Add Node to ServerNet Cluster** action on the System object. This is used for adding the system as a member of either a ServerNet Cluster or BladeCluster.
Replace Switch Component	OSM Guided procedure launched by **Replace** action on both 6770 and 6780 switch modules.
Update Topology	Interactive **Update Topology** action that guides you in updating the network topology of a ServerNet cluster.
Troubleshoot ServerNet Fabric	Interactive **External Loopback Test** action for ServerNet PICs on IOMF2 CRU.
Unique to NonStop BladeSystems	
Replace Processor Blade	Documented procedure launched by **Replace** action on the processor blade to be replaced.
Replace ServerNet Switch	Documented procedure launched by **Replace** action on the ServerNet switch to be replaced.
Install Core License File	This action, located on the System object, launches an OSM guided procedure that copies the core license file from $SYSTEM to the specified alternate system disk.

For more information about performing OSM actions, including interactive actions, see the *OSM Service Connection User's Guide* (also available as online help within the OSM Service Connection). For more information about a specific guided procedure, see the online help within that guided procedure. The guided procedure interface is launched when you click Perform Action for the action associated with each guided procedure.

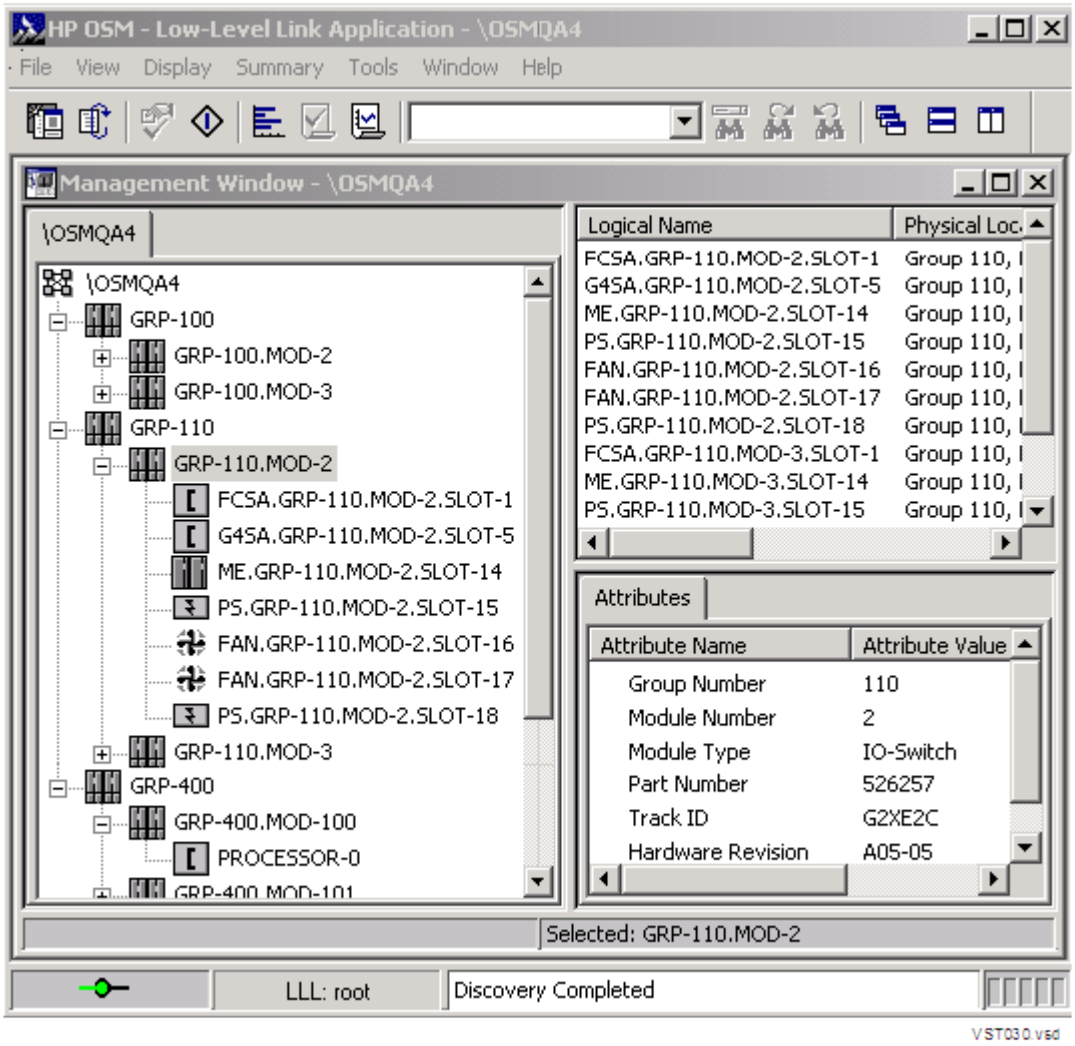
OSM Low-Level Link

The OSM Low-Level Link (LLL), one of the OSM Client-Based Applications, is primarily designed for down-system support. It enables you to communicate with a server even when the NonStop Kernel operating system is not running. Additionally, some actions performed on a running server,

such as priming a processor for reload, also require you to use the Low-Level Link. The OSM installer (on the NonStop System Console Installer DVD) installs the LLL only if you select the dedicated service LAN option during installation.

NOTE: The features described in this section will vary by Low-Level Link version, as noted.

Figure 16 OSM Low-Level Link Main Window

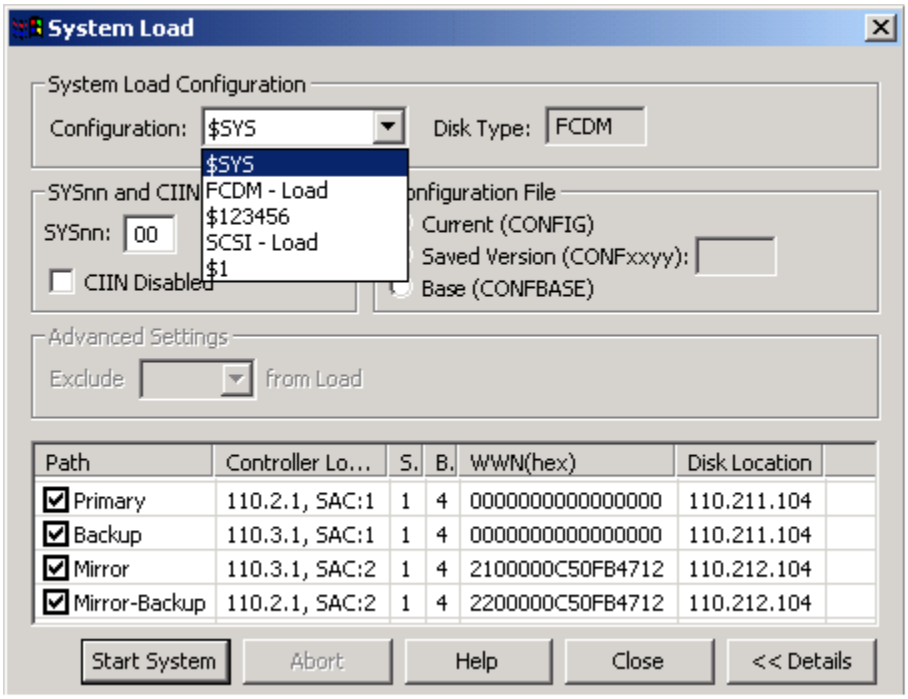


The OSM Low-Level Link looks and functions like the TSM Low-Level Link Application, with the following exceptions:

- Only the OSM Low-Level Link supports NonStop BladeSystems, NS-series servers and S-series modular I/O. Rather than through service processors, the OSM LLL communicates with NonStop systems through the maintenance entities (MEs). For NS-series, they are located in the ServerNet switch boards in p-switch modules; for NonStop BladeSystems, they are located in the ServerNet switches in the blade enclosure.
- The OSM Low-Level Link allows you to copy and update HSS firmware file required for all NonStop systems running J-series software except for NS2000 series systems.

  NOTE: For a user (other than the default users preconfigured on NonStop system consoles) to perform the "Update HSS" or "Copy HSS Files" action, you must give that user the necessary OpenSSH permissions on the NSC, as described in "Configuring Non-Default Users".

- Additional options for logging on to ServerNet switches or CLIMs in addition to System List (see Figure 17 (page 66)). Logging on to a CLIM (available with T0633 ABB and later) allows you to configure the CLIM and/or update CLIM software.
- Actions unique to the OSM Low-Level Link include a Configure Module action for IOAM, VIO, and p-switch modules, and a Power On System action.
- A System Load dialog box allows you to load the system from a fibre channel or SCSI disk and to choose alternate system disk configurations (saved on the console or via the OSM Service Connection) from the System Load Configuration drop-down menu. With T0633 ABB and later, there is also an option to load the system from a CLIM-attached disk.



- A new option in the Processor Status dialog box allows you to specify how often the Processor Status bar is refreshed.
- The SP Tool can now be launched from within the OSM Low-Level Link, by selecting Advanced Service Processor Tool from the Tools menu.
- The OSM Low-Level Link displays only an Inventory view in the View pane, not a Physical view.

For more information about configuring or using the OSM Low-Level Link, see the OSM Low-Level Link online help.

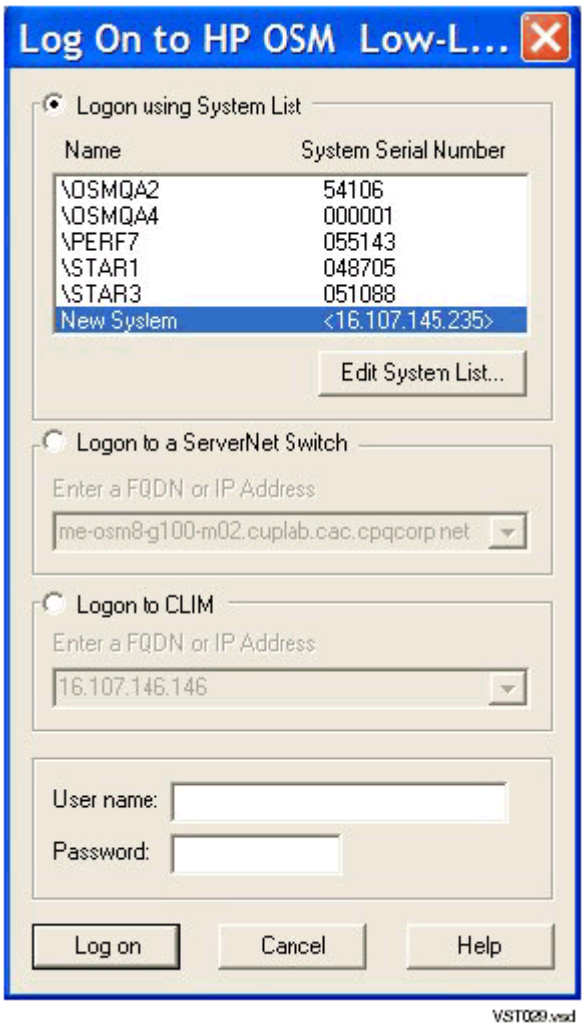
For a complete list of Problems Corrected and Known Problems Remaining, see the T0633 softdoc.

Launching and Logging On

From the Start menu, select All Programs > HP OSM > OSM Low-Level Link.

In the Log On dialog box, you can log on using either a system name (as in the TSM LLL) or by using a host name or IP address. Enter a valid user name and password, then click Log On or press Enter.

Figure 17 OSM Low-Level Link Log On Dialog Box



If the system you want to access does not appear in the System list, click Edit System List, and enter the IP addresses for the system you want to access.

OSM Event Viewer

Like the OSM Service Connection, the OSM Event Viewer is a browser-based application that is installed and resides on your server and is accessed through an Internet Explorer browser session on your system console. The OSM Event Viewer allows you to retrieve, view, and save events from any EMS formatted log files ($0, $ZLOG, or an alternate collector) for rapid assessment of system problems. It also provides event details such as cause, effect, and recovery information.

For more information on using the OSM Event Viewer, see the OSM Event Viewer online help.

Figure 18 OSM Event Viewer Main Window

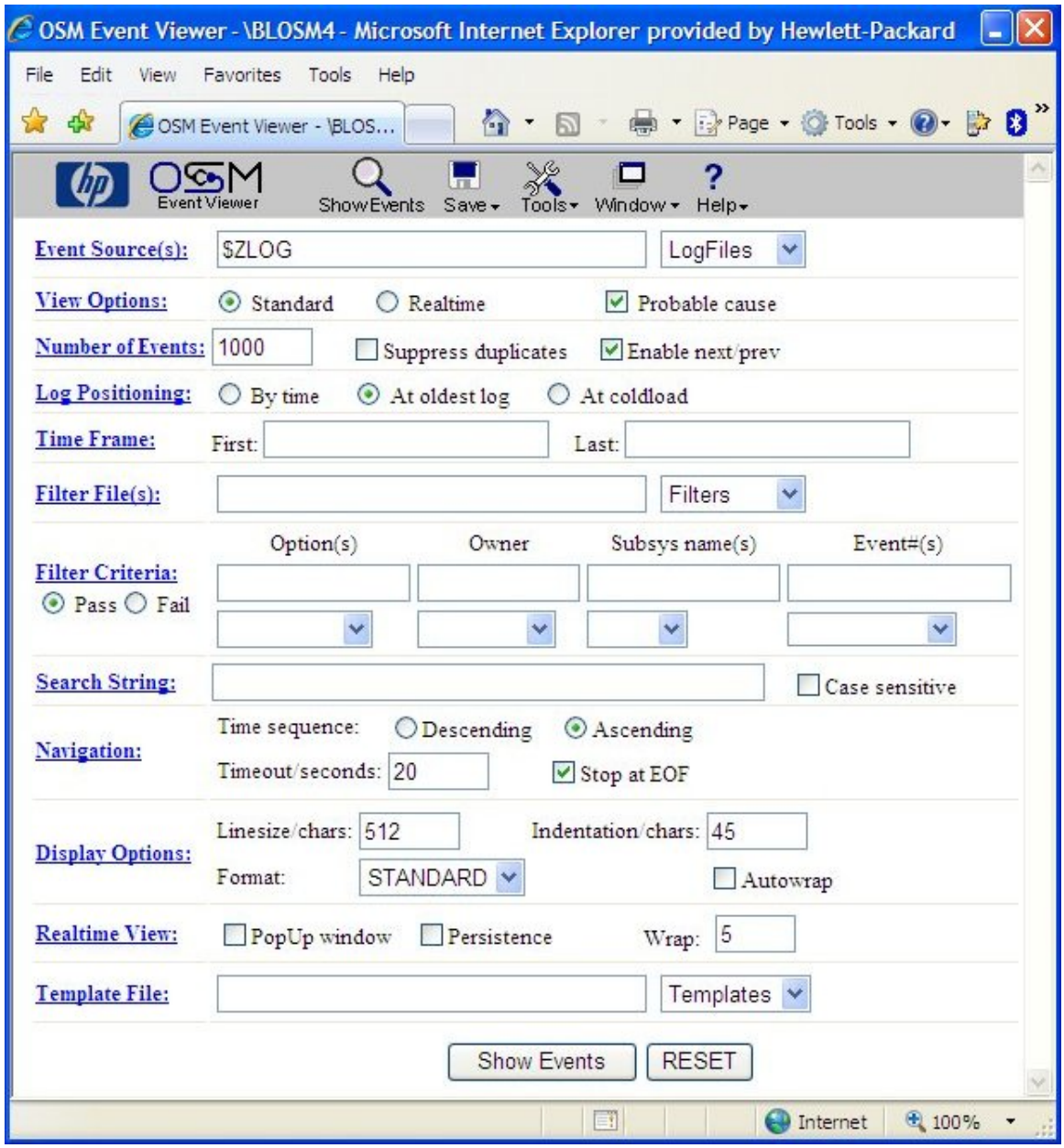
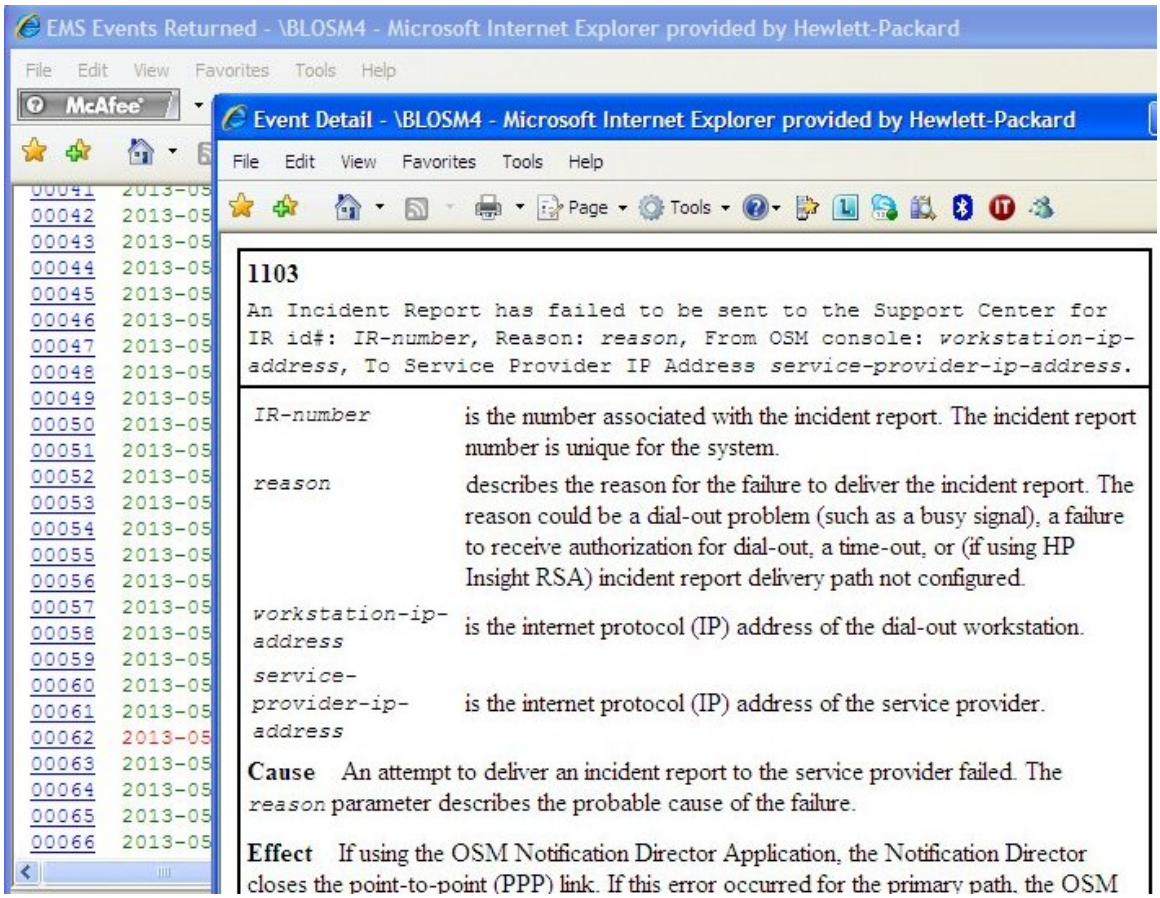


Figure 19 OSM Event Viewer Event Details



Functional Differences

The OSM Event Viewer was designed to incorporate the best features Web ViewPoint and the TSM EMS Event Viewer. It has been enhanced frequently during recent OSM releases. For a complete list of enhancements and Problems Corrected, see the T0682 softdoc.

With OSM version T0682 H02 ABP and later, the OSM Event Viewer has a new security feature whereby an event viewer session left idle for more than 20 minutes expires, requiring you to log on again before you can access that session again. This time-out period is configurable by inserting parameters into your OSMCONF file, as described in "Configuring Event Viewer Security Timeout" (page 27).

With OSM version T0682 H02 ADD (or later), the OSM Event Viewer allows you to view events time-stamped in the same time zone as the system on which they were logged. For more information, see the OSM Event Viewer online help.

Launching and Logging On

You can launch and log on to the OSM Event Viewer in three different ways:

Methods 1 and 2 are the same for the OSM Event Viewer as for the OSM Service Connection (see "Method 1: Using Home Page Bookmarks" (page 57) and "Method 2: Without Client Installation or Bookmarks" (page 59)), with these exceptions:

- In Method 1, select All Programs > HP OSM > OSM Event Viewer instead of the OSM Service Connection.
- In Method 2, specify port 9991 instead of 9990.

For Method 3, if you have an active OSM Service Connection session, select Event Viewer from the OSM Tools menu to launch an Event Viewer session for the system you are logged on to.

NOTE:

- The OSM Event Viewer uses a pop-up logon dialog box. If you do not find an initial logon dialog box on the screen, or hidden behind other windows, check the settings for the Internet Explorer menu item **Tools -> Pop-up Blocker**.
- SSL encryption interacts with the URL you enter in the Internet Explorer address bar. With T0682 H02 ADD or later SPRs, or if the `OSMCONF` file contains `UseSSL = On`, the OSM Event Viewer uses the `https` protocol. If you enter `http://` at the beginning of the URL, the event viewer server will attempt to redirect Internet Explorer to use `https://` instead. Sometimes the **Internet Explorer Enhanced Security Configuration** and **zone** security settings interfere with this redirection, so that the screen remains blank. To correct this issue, change the OSM Event Viewer URL prefix to `https://`. This issue does not currently affect the OSM Service Connection.
- SSL encryption requires server certificates for SSL. If your site has not installed site-specific SSL certificates, the default OSM certificates are used. The default OSM certificates are self-signed, so that Internet Explorer displays a warning in the initial web page for the OSM Event Viewer and in following displays in the address bar at the top of the Internet Explorer display. This behavior is expected. You can click on **Certificate Error** on the right side of the address bar to get a link to view the SSL certificate and verify that it is an OSM certificate. OSM is not a Trusted Root Authority. The default OSM certificates provide encryption, but not with the full level of security expected after installing your own site-specific SSL certificates. The OSM Service Connection is able to suppress these warnings for the default OSM certificates, but this is not possible for the OSM Event Viewer.

OSM System Inventory Tool

The OSM System Inventory Tool is a standalone application used to create a hardware or firmware inventory file of one or more NonStop systems running OSM. The resulting file can be saved in .csv (or comma delimited) format for use in Microsoft Excel or Apache OpenOffice (which is available in OSM Console Tools T0634 ABD and later).

The OSM System Inventory tool is available as part of OSM Console Tools, T0634AAL or later. Starting with T0634AAM (H06.08), the OSM System Inventory Tool can also be configured to create an inventory file of certain numeric sensor data (attribute values reported by OSM).

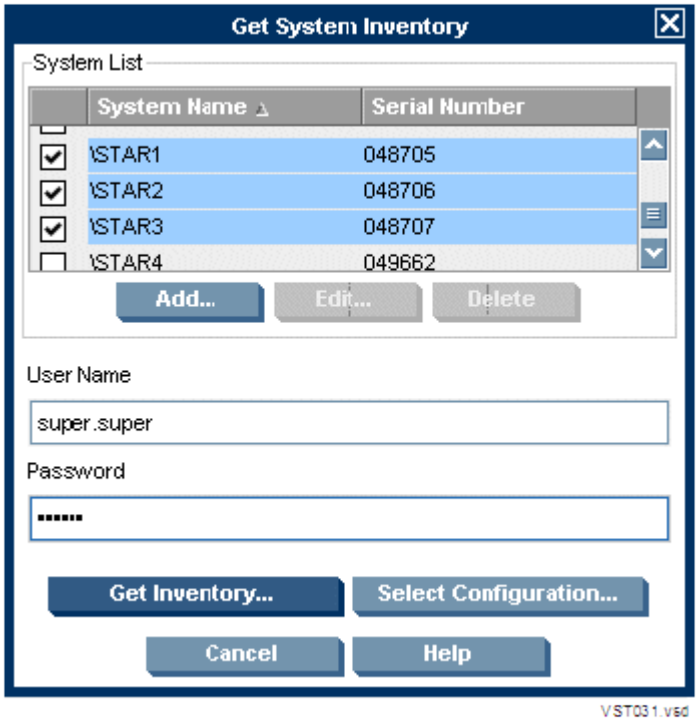
During installation, if not already installed, the version of Java Runtime Environment required by the inventory tool will automatically be installed on the console.

Launching and Logging On

From the Start menu, select All Programs > HP OSM > OSM System Inventory Tool.

To create an inventory file, select one or more systems from the System List (as shown in Figure 20), enter a valid user name and password, and click Get Inventory.

Figure 20 OSM System Inventory Tool



For more information on using the OSM System Inventory Tool, see the online help available from within the application.

Terminal Emulator File Converter

The Terminal Emulator File Converter is part of OSM Console Tools, T0634AAN or later. It is used to convert OSM Service Connection-related OutsideView session files to MR-Win6530 format. For more information on the Terminal Emulator File Converter, see the *NonStop System Console Installer Guide* and the online help available within the tool.

To launch it from the Windows Start menu, select All Programs > HP OSM > Terminal Emulator File Converter.

OSM Certificate Tool

The OSM Certificate Tool is part of OSM Console Tools, T0634AAQ or later. It is used – for NonStop BladeSystems only – to facilitate communication between OSM and the Onboard Administrators (OAs) in the blade enclosures. It creates and uploads certificates that enable OSM to invoke the OA web interface, logon to an OA, and make SOAP calls without having to provide a username and password each time).

To launch it from the Windows Start menu, select All Programs > HP OSM > OSM Certificate Tool.

For information on how to use the OSM Certificate Tool, see the online help available within the tool.

NonStop Maintenance LAN DHCP DNS Configuration Wizard

Installed as part of OSM Console Tools, T0634 ABB and later, the NonStop Maintenance LAN DHCP DNS Configuration Wizard replaces the CLIM Boot Service Configuration Wizard. It can be used to configure the DHCP and DNS servers required for NonStop J-series systems and any NonStop systems with CLIMs attached. The wizard is also used to configure FTP, TFTP, and BOOTP servers. (BOOTP servers apply only to all NonStop systems running J-series software except for NS2000 series systems and make the Halted State Services (HSS) files available for processors to boot from.) For systems that require these services, it is important to have two, and only two, sources

of these services on the dedicated service LAN, and that they be hosted on either two NonStop system consoles or two designated CLIMs.

To take advantage of significant enhancements in both the wizard and accompanying online help, you should install and use the wizard included in OSM Console Tools, T0634 ABE (or later). How to effectively use the wizard depends the current state of those services on your dedicated service LAN and whether or not the NonStop Maintenance LAN DHCP DNS Configuration Wizard has previously been used on one or both system consoles on that LAN. The online help in version T0634 ABE and later includes the topic "Guide to Using the NonStop Maintenance LAN DHCP DNS Configuration Wizard," which can help you select the appropriate course of action for your scenario.

When using the NonStop Maintenance LAN DHCP DNS Configuration Wizard to migrate DHCP, TFTP, DNS, and BOOTP services between NonStop system consoles and CLIMs, refer to the appropriate documented service procedure, located in the NonStop Technical Library, to make sure that all preparatory and follow-up steps are completed:

- *Changing the DHCP, DNS, or BOOTP Server from System Consoles to CLIMs*
- *Changing the DHCP, DNS, or BOOTP Server from CLIMs to System Consoles*

NOTE: For a user (other than the default users preconfigured on NonStop system consoles) to use the wizard, you must give that user the necessary OpenSSH permissions on the NSC, as described in "Configuring Non-Default Users".

Down System CLIM Firmware Update Tool

Installed as part of OSM Console Tools, T0634 ABB and later, the Down System CLIM Firmware Update Tool is used, in conjunction with the Prepare for Down System CLIM Firmware Update action in the OSM Service Connection, for updating firmware/BIOS for all CLIM components during planned system down time, such as during RVU upgrades. For more information, see the *NonStop Cluster I/O Protocols (CIP) Configuration and Management Manual* and the online help available from within the tool.

The Down System CLIM Firmware Update Tool requires:

- OSM Service Connection SPR T0682 H02 ACV or later.
- SSH SPR T0801 ABA or later.

NOTE: For a user (other than the default users preconfigured on NonStop system consoles) to perform the "Prepare for Down System CLIM Firmware Update" action, you must give that user the necessary OpenSSH permissions on the NSC, as described in "Configuring Non-Default Users".

Configuring Non-Default Users

For a user (other than the default users preconfigured on NonStop system consoles) to perform certain OSM actions, you must give the local or domain user the necessary OpenSSH permissions for both primary and backup NonStop system consoles. Those actions include:

- The "Prepare for Down System CLIM Firmware Update" action in the OSM Service Connection.
- The "Update HSS" and "Copy HSS Files" actions in the OSM Low-Level Link.
- Any action in the NonStop Maintenance LAN DHCP DNS Configuration Wizard that involves connecting to the peer NSC.

NOTE: The default users preconfigured on NonStop system consoles by manufacturing include Administrator, NSC_Administrator, and GCSC. Those user IDs get the necessary OpenSSH permissions when OpenSSH is installed, as part of the Console CLIM Utilities (T0697), through the NSC Master Installer.

The command that you must execute on the NonStop system console for non-default users varies depending on whether it is a local user or a domain user:

- For a **local** user, enter:

  ```
  sshuser -s user-name -u user-name -f passwd-file
  ```

- For a **domain** user, enter:

  ```
  sshuser -s domain-name\user-name -u user-name -d domain-name -f passwd-file
  ```

Where:

domain-name	The name of the domain.
user-name	The NSC user name to be configured.
passwd-file	The location of the `passwd` file in the `etc` directory under the `OpenSSH` installed directory. For example: `C:\Program Files\OpenSSH\etc\passwd`

The `sshuser` command only applies to the NSC on which it is executed. You must also execute that command on the other NSC.

A Leveraging Your Registry Settings

Use this procedure to migrate your OSM registry settings to other system consoles.

NOTE: This procedure is designed to save you time and effort in the event that you want to leverage and share your existing OSM registry settings with other system consoles; this procedure is not required to use OSM software.

1. On your system console that you want to migrate OSM registry settings from, select Run from the Start menu.
2. Enter regedit and click OK.
3. In the Registry Editor, navigate to HKEY_LOCAL_MACHINE>SOFTWARE>Hewlett Packard>OSM>Configuration and select CurrSystem.
4. From the Registry menu, select Export Registry File.
5. Enter a file name of OSM.reg and save the file.
6. Transfer the OSM.reg file to the desktop of the system console you want to migrate the settings to.
7. Open the OSM.reg file. Click Yes, then click OK to the Registry Editor confirmation dialog boxes and close the Registry Editor dialog box.
8. When you launch the OSM Low-Level Link, you should see the system names that were in the settings you imported from. When you launch the OSM Service Connection or OSM Event Viewer from the Start menu shortcut, you should see a list of bookmarks for the same systems in the left column of the home page. You can click a bookmark to initiate an OSM session instead of opening an Internet Explorer browser and entering a system URL.

B Troubleshooting

This section lists problems that can occur under particular conditions or configurations and describes how to avoid or recover from the problems. For a complete list of OSM fixes and known problems, see the softdoc for each OSM product.

OSM Service Connection Problems

The OSM toolbar appears blank

See the note under step 4 of logging on (page 61).

"Malicious Alerts" message during OSM client installation

If your PC has script blocking enabled in recent version of Norton Anti-Virus, you will get a "Malicious Alerts" message during OSM client installation.

To recover: Disable script blocking in Norton Anti-Virus during installation.

Error when downloading the jre.exe for Java 2 Runtime Environment

The first time you attempt to establish an OSM Service Connection session, you are instructed to "Click here to download Java Runtime Environment." If you wait a few seconds before clicking either the Open or the Save button, you will end up with a corrupted file and will get an error.

To recover:

1. Close the current Internet Explorer browser window.
2. Open a new browser window and request a service connection as before (using a system URL or bookmark).
3. Click to download Java Runtime Environment, then click either Open or Save immediately after the File Download dialog box is displayed. Choosing Open is recommended because the time-out problem is less likely to occur.

"Page cannot be displayed" error when launching the Service Connection (before Log On dialog box appears)

Ignore the standard Internet Explorer tips such as clicking the Refresh button. Close the current Internet Explorer browser window and try the following steps:

1. Check that OSM server software is running on the NonStop NS-series server you are trying to access. At an SCF prompt, enter the following:

   ```
   status process $zzkrn.#*
   ```

2. Confirm that you are using a valid system URL for the server you are trying to access.
3. Open a new browser window and try again.

"Error 500," "Page cannot be displayed," or "Initial Analysis in Progress" (after providing user name and password)

If one of the panes in the OSM Management window displays an "Error 500" or "Page cannot be displayed" message, or if the Server Status on the view pane title bar reports "Initial Analysis in Progress," you have attempted to establish a service connection before OSM server software has fully discovered the system.

To recover: Close the current Internet Explorer browser window, wait a few minutes (discovery time varies with the size of the system), then open a new browser window and try again.

OSM Service Connection update problems or actions not displayed

You might experience similar problems if your Internet Explorer proxy settings are not configured properly. The following Internet Explorer options should be deselected: "Use automatic configuration script" and "Use a proxy server for your LAN."

To avoid: From the Internet Explorer Tools menu, select Internet Options>Connections tab>LAN Settings.

Display problems within the OSM Service Connection interface

Disks and PMF CRUs show up outside of the group they are supposed to be inside of because the display font is set incorrectly.

To avoid: Go to Start>Settings>Control Panel>Display, click the Settings tab, and then click Advanced. Change the Display Font Size to Small Fonts. Click OK to close both the Advanced window and the Display Control Panel. Reboot your PC.

You should also make sure you have the latest video drivers installed on your PC

"ActiveX errors" in Internet Explorer

Internet Explorer 6.0 is required for OSM. ActiveX error messages indicate that you are using an older version of Internet Explorer. Version 6.0 can be installed from the HP NonStop System Console Installer DVD.

OSM Low-Level Link Problems

OSM Low-Level Link not installed

The OSM Low-Level Link is installed from the OSM or Master installers on the HP NonStop System Console Installer DVD only when you choose the "dedicated service LAN" option during the installation.

To recover: If you do not have a start menu shortcut for the Low-Level Link (Start > All Programs > HP OSM > OSM Low-Level Link), insert the NSC Installer DVD and re-install OSM, choosing the "dedicated service LAN" option. See the hardware installation manual for your NonStop NS-series server or NonStop BladeSystem for information on connecting your system console and servers using a dedicated service LAN.

OSM Event Viewer Problems

Cannot establish Event Viewer session with a system

$ZOEV may not be running on the server. Start it by using:

```
scf start process $zzkrn.#osm-oev
```

Saved events are not the ones you intended to save

When you save a page of events (returned by the Event Viewer) after using the Next button, the events that are saved may not be the ones you intended (because of an Internet Explorer preference setting).

To avoid: Do one of the following for either a one-time or permanent fix:

- One-time fix: In the Save As dialog box, change the file type from "Web Page, complete" to "Web Page, HTML only."
- Permanent fix: Select Internet Options from the Tools menu. Click Settings (under "Temporary Internet files" and set "Check for newer versions of stored pages" to Automatically.

C Configuring SNMP Access for Monitored Service LAN Devices

Starting with OSM T0682 H02 AAY and later, SNMP access information is required to start monitoring a UPS or maintenance switch.

- For a UPS, you must enter the appropriate community strings for both the SNMP Read Access Community and SNMP Write Access Community.
- For a maintenance switch, you must enter the appropriate community string for the SNMP Read Access Community.

The community string and its associated access privileges for both SNMP Read Access Community and SNMP Write Access Community are established by the administrator for each device.

OSM assumes the default community string for each device (listed in the sections that follow). If a device was started with other values prior to upgrading to T0682 H02 AAY (or later), OSM reports the device as Not Responding and the repair action instructs you to stop monitoring the device, then perform the Start Monitoring UPS or Start Monitoring Maintenance Switch action using the SNMP community string(s) as set by the administrator.

The following sections describes how an administrator can change default values for:

- "SNMP Read/Write Access for UPS"
- "SNMP Read Access for Maintenance Switch"

SNMP Read/Write Access for UPS

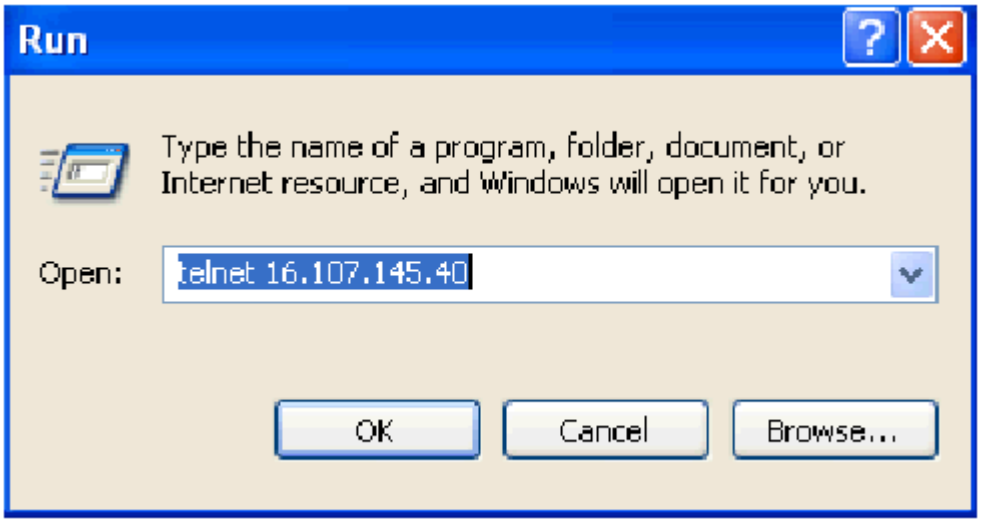
The default values for SNMP Read and Write Access are:

Information Required by the Start Monitoring UPS Action	Community String	Access
SNMP Read Access Community	public	Read Only
SNMP Write Access Community	private	Read/Write

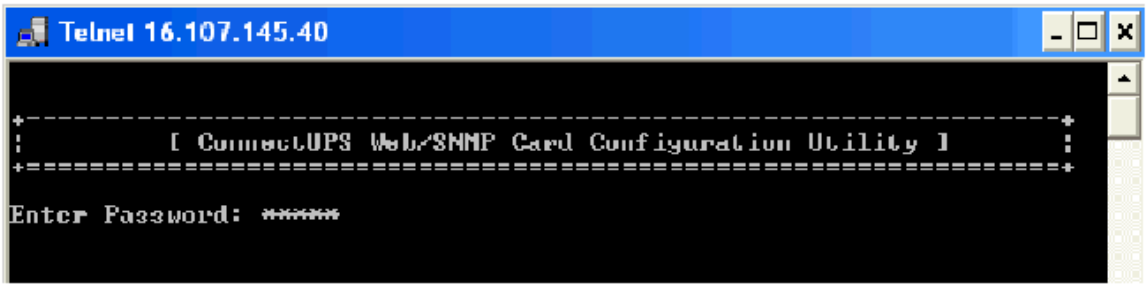
An administrator for the UPS can modify the default community strings and their associated access privileges by following these steps:

NOTE: If OSM is currently monitoring the UPS, use the Stop Monitoring action (located under the UPS object) before making changes to the SNMP configuration.

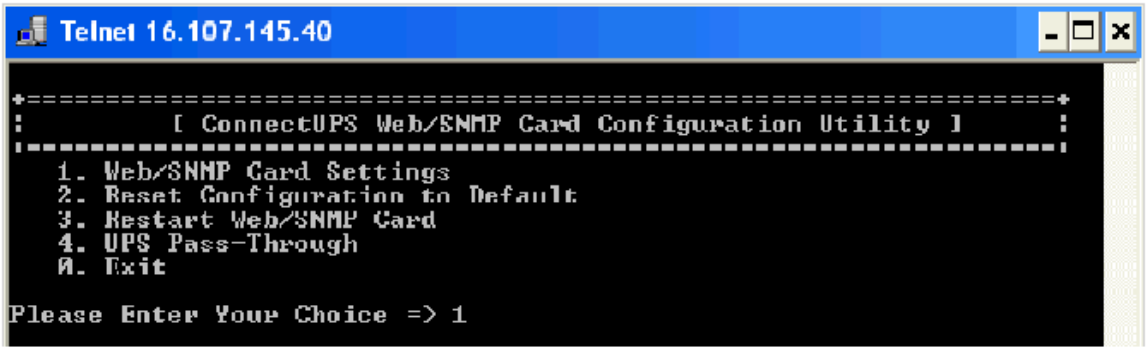
1. Initiate a telnet session with the IP address of the UPS.



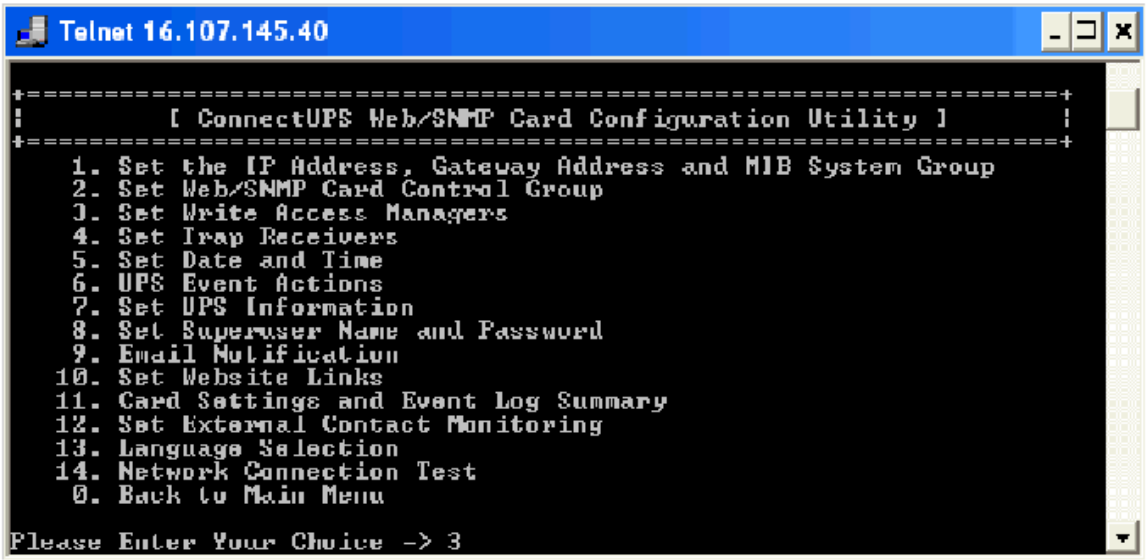
2. Enter administrator password.



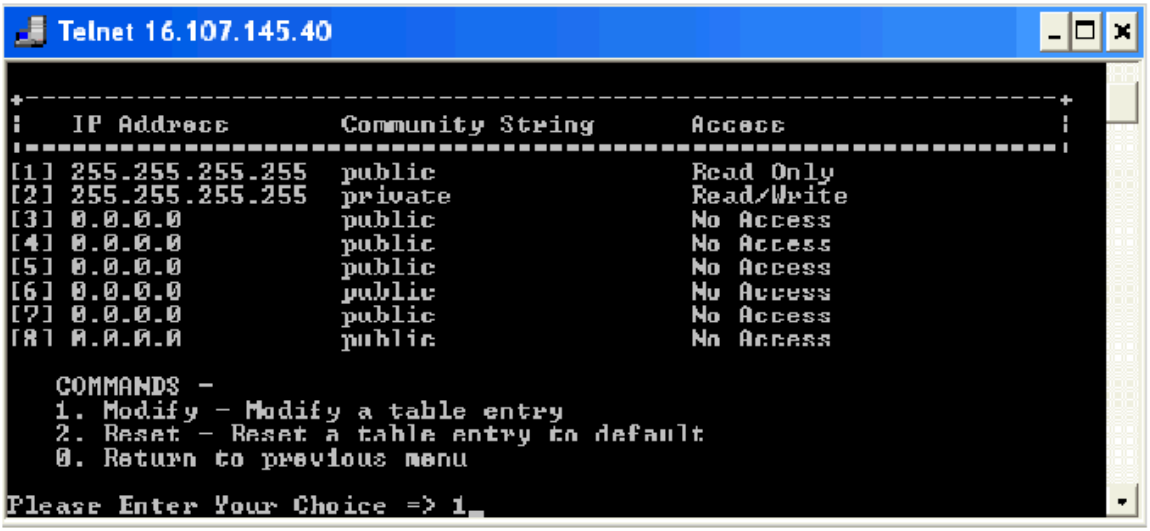
3. Enter "1" to select Web/SNMP Card Settings.



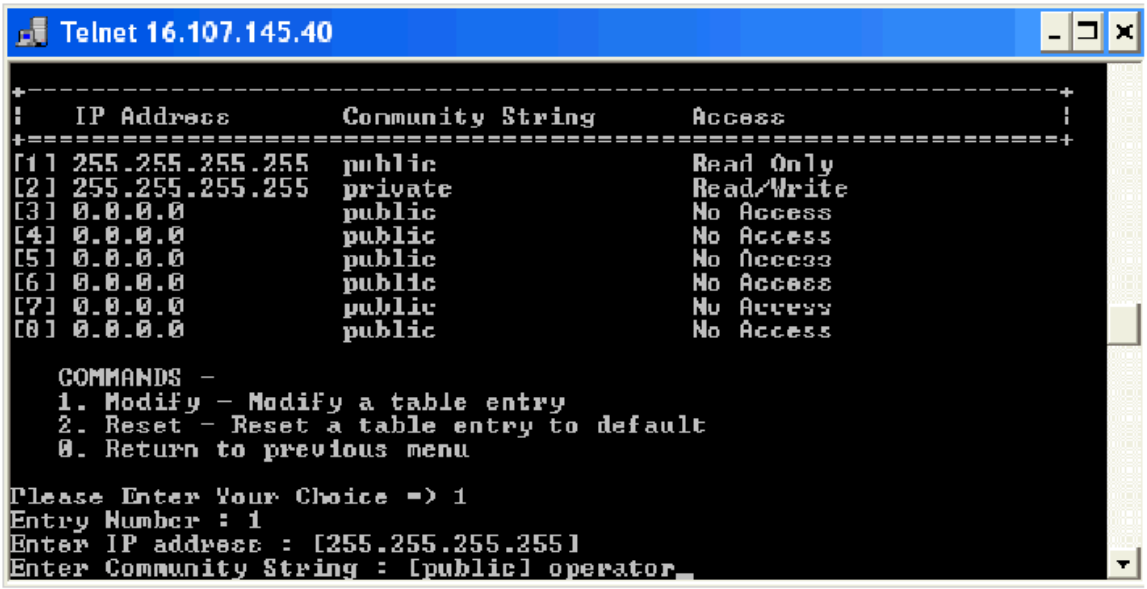
4. Enter "3" to select Set Write Access Managers.



5. Enter "1" to modify a table entry.



6. Use the Enter key to navigate to the field you want to change. In this example, the Community String for the Read Only (or SNMP Read Access Community) group was changed from "public" to "operator."



7. After all changes are completed in telnet, use the OSM Service Connection to perform the Start Monitoring UPS action – using the appropriate strings for SNMP Read Access Community and SNMP Write Access Community – in order for OSM to resume monitoring the UPS.

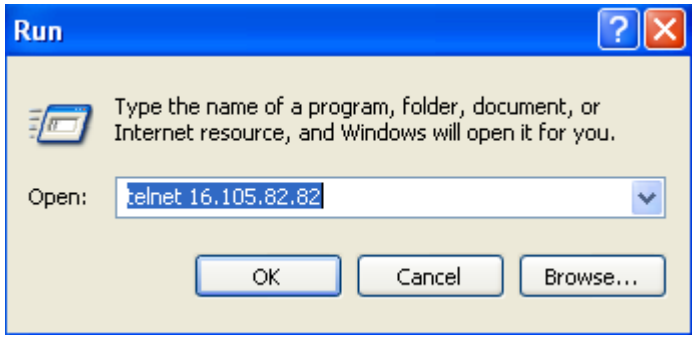
SNMP Read Access for Maintenance Switch

The default value for SNMP Read Access Community name is “public.” Write access is “Restricted;” however, write access is not required for OSM operations.

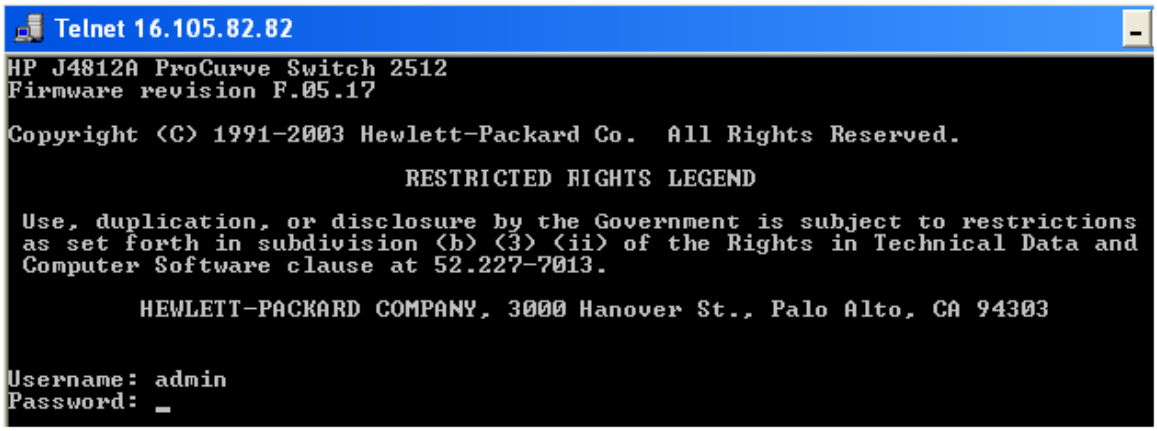
An administrator for the maintenance switch can modify the default community strings and their associated access privileges by following these steps:

NOTE: If OSM is currently monitoring the maintenance switch, use the Stop Monitoring action (under the Maintenance Switch object) before making changes to the SNMP configuration.

1. Initiate a telnet session with the IP address of the maintenance switch.

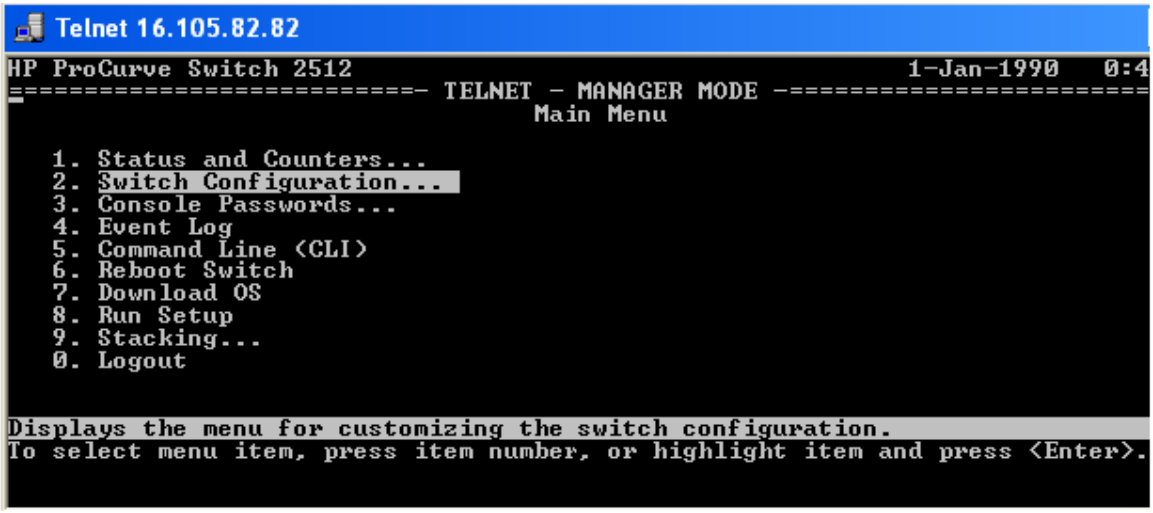


2. Enter username and password.

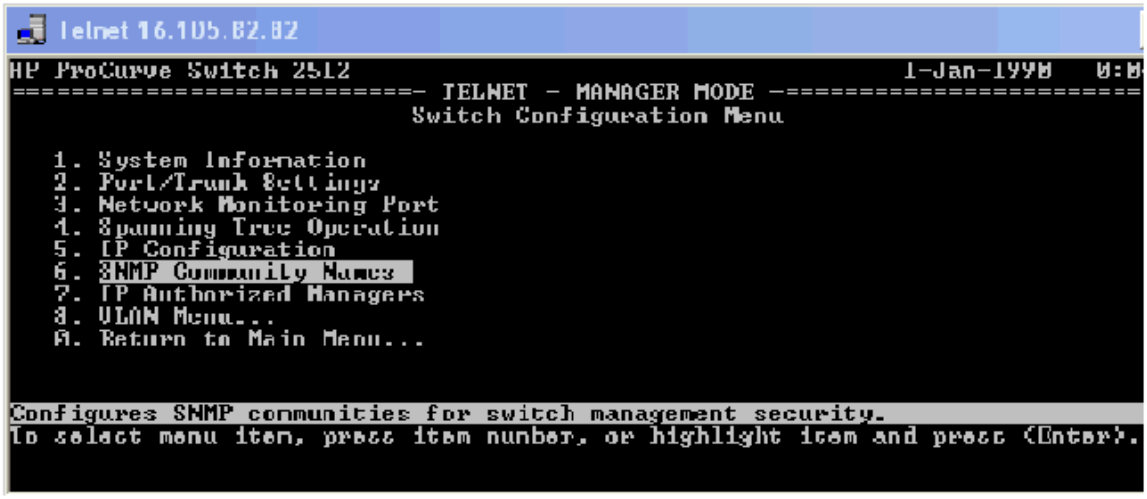


3. Enter “menu” to get to the Main Menu.

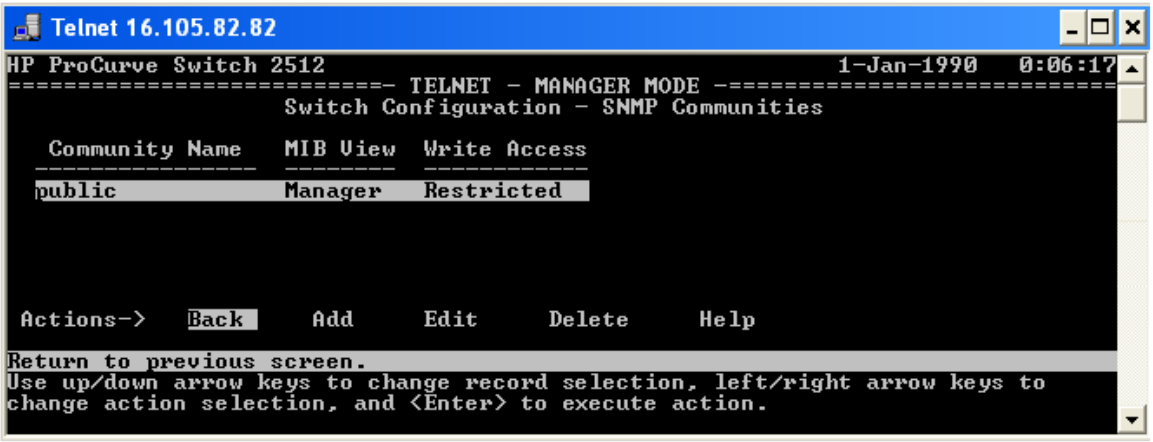
4. Enter “2” to select the Switch Configuration Menu.



5. Enter "6" to modify SNMP Community Names.



6. Follow the online instructions to Add or Edit an entry.



7. After all changes are completed in telnet, use the OSM Service Connection to perform the Start Monitoring Maintenance Switch action – using the appropriate string for the SNMP Read Access Community – in order for OSM to resume monitoring the maintenance switch.

Index

P

R

S

T

U

V

W