

HP Insight Remote Support Advanced for NonStop



HP Part Number: 582661-004

Published: October 22, 2009

Edition: J06.03 and subsequent J-series RVUs, H06.03 and subsequent H-series RVUs, and G06.10 and subsequent G-series RVUs.

HP Confidential

© Copyright 2009 Hewlett-Packard Development Company, L.P.

Legal Notice

See Appendix : Legal Notice (page 11) for legal notices.

About This Document

This document describes the NonStop-specific details needed to install and configure HP Insight Remote Support Advanced (Insight RSA) for use in a NonStop environment. It is intended as a supplement to, not a substitute for, the documentation for installing and configuring HP SIM and Insight RSA. This document provides links to those documents and describes when and how to perform the additional steps required for the NonStop environment.

Supported Release Version Updates (RVUs)

This topic supports J06.03 and subsequent J-series RVUs, H06.03 and subsequent H-series RVUs, and G06.10 and subsequent G-series RVUs.

Intended Audience

This document is intended for customers or service providers who will install and configure HP Insight Remote Support Advanced for use in a NonStop environment. Note that you will need help from your customer support representative to complete some parts of the installation.

New and Changed Information in This Edition (582661-004)

Updated to add support for HP NonStop S-series servers. Special considerations for S-series servers are noted under “Requirements” and under steps 4 and 7 of the NonStop-Specific Tasks.

Recent Change History

582661-003: Under NonStop-Specific Tasks, step 2 was added to ensure that the WEBES DESTA.REG file settings are appropriate for managing NonStop systems.

582661-002: Updated to indicate that WEBES, installed as part of Insight RSA, was upgraded to WEBES 5.5 Patch 1, eliminating the need for the NonStop Support Patch called for in the original (-001) edition of this document.

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 docsfeedback@hp.com.

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

Using Insight RSA in the NonStop Environment

Introduction

HP Insight Remote Support Advanced (Insight RSA) is qualified for NonStop systems, including HP Integrity NonStop BladeSystems, Integrity NonStop NS-series servers, and NonStop S-series servers. Insight RSA is the go-forward remote support solution for NonStop systems, replacing both modem and HP Instant Support Enterprise Edition (ISEE) remote support solutions.

Insight RSA is a plug-in to HP Systems Insight Manager (SIM). It enhances HP SIM with intelligent event diagnosis and automatic, secure submission of hardware event notifications to HP support, including acknowledgment and status.

HP SIM and Insight RSA are installed on a Windows-based Central Management Server (CMS) (see “Requirements”); ideally, a central server to which incidents from all NonStop and other HP platforms in the customer data center are sent. This provides a single pane-of-glass for the remote support of the whole data center.

On NonStop systems, OSM server performs problem diagnosis and creates incident reports (IRs). The OSM server sends these IRs to Insight RSA, which in turn, forwards them to HP support.

Process Overview

Using Insight RSA in the NonStop environment requires some NonStop-specific details not covered in the HP SIM and Insight RSA documentation. This document is a supplemental guide to the documentation for those products, outlining the sequence of steps, providing links to those documents, and describing when and how to perform the additional NonStop-specific tasks required to start using Insight RSA. The process for getting started with Insight RSA in the NonStop environment involves:

- Ensuring that all “Requirements” for using Insight RSA in the NonStop environment have been met.
- Performing “Installation and Configuration of HP SIM and Insight RSA”. This process includes some NonStop-Specific Tasks to be performed at specific points in the process, including the disabling of the OSM Notification Director (ND), as described under “Insight RSA Migration Scenarios”.

Requirements

HP SIM and Insight RSA are installed on a Windows-based PC referred to as Central Management Server (CMS). Although HP supports using a qualified NonStop System Console (NSC) as a CMS, HP recommends that the NSC and CMS be two separate servers. For an NSC to be configured as the CMS, it must be running Windows 2003 Server and have at least 4 GB of memory. Insight RSA is currently supported for NonStop systems only on a CMS running Windows Server 2003.

Table 1 NonStop Server Software Requirements:

Product	Minimum Version
OSM Server	For HP Integrity NonStop BladeSystems or Integrity NonStop NS-series servers: T0682 ABU or later. For NonStop S-series servers: T0682 ABY or later.
RVU	J06.03 or later, H06.03 or later, G06.10 or later.

Table 2 CMS Software Requirements:

Product	Minimum Version	Notes
HP SIM	5.3 with HotFix, or later	HP SIM includes Remote Support Software Manager (RSSWM), which upon initialization, installs Insight RSA and the compulsory component packages.
Insight RSA	A.05.20 or later	Downloaded and installed by RSSWM.
WEBES	For G-series: 5.6 or later For H/J-series: 5.5 Patch 1 or later*	A component of RSA, installed by RSSWM.
		* If already installed, WEBES 5.5 with NonStop Support Patch is supported also. If you install WEBES 5.5 Patch 1 over the earlier 5.5 version with NonStop Support Patch, you can overwrite the existing WEBM.jar file.
Remote Support Eligible Systems List	A.05.20.24 or later	A component of RSA, installed by RSSWM.

Installation and Configuration of HP SIM and Insight RSA

This section includes both pointers to the HP SIM and Insight RSA documents for installing and configuring HP SIM and Insight RSA and a list of NonStop-Specific Tasks to be performed at particular points during the installation and configuration process. Be sure to consult the NonStop-Specific Tasks section as you install and configure HP SIM and Insight RSA, for the appropriate time to perform those additional tasks.

Install and configure HP SIM and Insight RSA by following the instructions provided in the following manuals (or appropriate later versions), which can be found at <http://docs.hp.com/en/netsys.html>, under the headings noted for each:

- *HP Systems Insight Manager 5.3 with SP1 Installation and Configuration Guide for Microsoft Windows*, located under the **HP Systems Insight Manager** heading.
- *A.05.20 Remote Support Pack CMS Prerequisites and Managed Systems Configuration Guide*, located under the **Remote Support Pack** heading.
- *A.05.20 Remote Support Pack CMS Registration, Configuration, and Usage Guide*, located under the **Remote Support Pack** heading.

NonStop-Specific Tasks

1. After installing HP SIM 5.3, download and install the HotFix Update Kit for HP SIM 5.3 - MS Windows (this is also required for HP SIM 5.3 with SP1). It is available at: http://h18013.www1.hp.com/products/servers/management/hpsim/dl_windows.html.



NOTE: When you install the kit, it will stop the HP SIM service, add the fixes and then restart HP SIM. Wait to discover your NonStop systems in HP SIM until called for in this procedure.

2. There are two settings in the WEBES DESTA.REG file that must be set appropriately to ensure NonStop compatibility.
 - a. From a DOS prompt on the CMS, perform the following commands to specify the required values for the wbem.useip and wbem.destname parameters:
 - `desta dri set wbem.useip t`
 - `desta dri set wbem.destname`
 - b. Perform the following commands to make the changes to the DESTA.REG file take effect:
 - `net stop desta_service`
 - `net start desta_service`

3. Disable the OSM Notification Director (ND), as described under “Insight RSA Migration Scenarios”, before performing step 4 to enable Insight RSA.
4. After disabling the OSM ND, add the appropriate flags (depending on the type of NonStop system) to your OSMCONF file in order for each system to be monitored by Insight RSA and to enable dial-out to Insight RSA/WEBES.

- For NonStop BladeSystems, add:

```
IR_Alert=YES
Schema#NSK_DialoutConfiguration#Method#IrCalloutPathTest#OSMDisplayable = {"OSM_SC"}
EnableNDDData=OFF
```

- For NonStop NS-series servers, add:

```
IR_Alert=YES
Schema#NSK_DialoutConfiguration#Method#IrCalloutPathTest#OSMDisplayable = {"OSM_SC"}
EnableNDDData=OFF
UseSSL=ON
```

- For NonStop S-series servers, add:

```
IR_Alert=YES
UseSSL=ON
```



NOTE: After editing your OSMCONF file, you must restart the OSM server for the changes to take effect.

5. Discover each NonStop system in HP SIM (using the discovery method described in the HP SIM manual). After each system has been discovered, enable it for Insight RSA by entering the following NonStop entitlement values through the **Edit System Properties** page in HP SIM. That page is accessed from the **Tools & Links** tab on each NonStop server's home page (as pictured below):

- Under System Information > Identification: enter **NonStop** in the Product number field.

System Information

Identification

Preferred system name:

Prevent the Discovery process from changing this system name

Serial number:

Product number:

- Under Contract and Warranty Information > Entitlement Information:
 - System Country code: select the appropriate country from the drop-down menu.
 - Entitlement type: enter **System Handle**
 - Entitlement ID: enter **NSKSUPPORT**

Contract and Warranty Information

Entitlement Information

Customer-Entered serial number:

Customer-Entered product number:

System Country code:

Entitlement type:

Entitlement ID:

Click **OK** to save changes.

6. Repeat steps 3-5 for each NonStop system to be monitored by Insight RSA.
7. Upon completion, each system should now be monitored by Insight RSA. You can test this functionality on each system by using the **Test Incident Report Delivery Paths** action, located under the System object in the OSM Service Connection. The action triggers a periodic incident report. If the system is being monitored by Insight RSA:
 - HP SIM displays an event on the Event Tab indicating that the NonStop server incident has been reported. For NonStop BladeSystems and NS-series servers, see “**Known Issues**” regarding possible invalid OSM event.
 - If the system is a NonStop S-series server, OSM issues an event indicating the success (event 1102) or failure (event 1103) of the IR delivery to all configured paths, and an OSM alarm is created if the delivery fails on any configured paths.



NOTE: For NonStop S-series servers only, you can install and use Insight RSA on more than one CMS for fault tolerance. To use this configuration, repeat steps 1-7 on additional CMS.

If you install and configure Insight RSA on more than one CMS that manages NonStop BladeSystems or NS-series servers, be sure to perform discovery of those systems in HP SIM on only one CMS, to avoid duplicate dial-outs.

Insight RSA Migration Scenarios

This section describes four scenarios for migrating from using the OSM Notification Director to Insight RSA. When directed to, during step 3 of the NonStop-Specific Tasks, follow the steps listed under the scenario that matches your existing console environment and configuration.



NOTE: Either Insight RSA or the OSM Notification Director, but not both, must be configured to monitor a NonStop system. HP does not support a NonStop system being configured for both Insight RSA and OSM Notification Director support at the same time.

At this time, NonStop NS-series servers and NonStop BladeSystems can be monitored by Insight RSA on only one CMS at a time (see “Known Issues”).

Scenario 1: You are using the OSM ND to monitor just one Nonstop system from a single NSC.

1. Disable the following services by selecting Start > Control Panel > Administrative Tools > Services > *service_name*. Be sure to not only stop the service, but change its Startup Type to **Disabled**.
 - Remote Proxy Service
 - OSM Notification Director Monitor
2. Rename the following executable files, located in C:\OSM\bin, to prevent them from being inadvertently launched. For example, add a “.txt” extension after the “.exe” to render them no longer executable.
 - NDMonSvr.exe
 - OsmNd32.exe
3. (Optional) To remove the OSM Notification Director and Remote Proxy Service Start Menu shortcuts from the console, delete the following folders from C:\Documents and Settings\All Users\Start Menu\Programs\HP OSM:
 - OSM Notification Director
 - Remote Proxy
4. Return to step 4 of NonStop-Specific Tasks to complete the process of enabling Insight RSA.

Scenario 2: You are using the OSM ND to monitor just one Nonstop system from two NSCs (a primary and backup NSC).

1. Follow steps 1–3 under Scenario 1 to disable and remove the OSM ND on the primary NSC.
2. Follow steps 1–3 under Scenario 1 to disable and remove the OSM ND on the backup NSC.
3. Return to step 4 of NonStop-Specific Tasks to complete the process of enabling Insight RSA.

Scenario 3: You are using the OSM ND to monitor multiple Nonstop systems from a single NSC.

Identify one Nonstop system at a time upon which to perform these Insight RSA migrate steps:

1. Launch the OSM ND and from the Systems menu select **Edit Systems List**.
2. Select the name of the system upon which you are performing the migration and click **Delete** (and click **Yes** in response to the confirmation dialog box).



NOTE: This step also deletes the system from the Systems List in the OSM Low-Level Link, so you will need to add it once again from the Low-Level Link in order to connect to the system from that application.

3. Return to step 4 of NonStop-Specific Tasks to complete the process of enabling Insight RSA on each NonStop system. However, be sure to return to this Scenario 3 procedure and repeat steps 1-3 for each of the NonStop systems to be migrated to Insight RSA.
4. If all NonStop systems have been migrated to Insight RSA, follow steps 1–3 under Scenario 1 to disable the OSM ND. However, if some NonStop systems will continue to be monitored by the ND, do not perform those steps to disable and remove the ND.

Scenario 4: You are using the OSM ND to monitor multiple NonStop systems from two NSCs (a primary and backup NSC).

Identify one Nonstop system at a time upon which to perform these Insight RSA migrate steps. Starting with the backup NSC:

1. Launch the OSM ND and from the Systems menu select **Edit Systems List**.
2. Select the name of the system upon which you are performing the migration and click **Delete** (and click **Yes** in response to the confirmation dialog box).



NOTE: This step also deletes the system from the Systems List in the OSM Low-Level Link, so you will need to add it once again from the Low-Level Link in order to connect to the system from that application.

3. Move to the primary NSC and repeat steps 1 and 2 above (under Scenario 4).
4. Return to step 4 of NonStop-Specific Tasks to complete the process of enabling Insight RSA on each NonStop system. However, be sure to return to this Scenario 4 procedure and repeat steps 1-4 for each of the NonStop systems to be migrated to Insight RSA.
5. On the backup NSC: if all NonStop systems being monitored by this console have been migrated to Insight RSA, follow steps 1-3 under Scenario 1 to disable the OSM ND. However, if some NonStop systems will continue to be monitored by the ND, do not perform those steps to disable and remove the ND.
6. On the primary NSC: if all NonStop systems being monitored by this console have been migrated to Insight RSA, follow steps 1-3 under Scenario 1 to disable the OSM ND. However, if some NonStop systems will continue to be monitored by the ND, do not perform those steps to disable and remove the ND.

Known Issues

These issues apply to NonStop NS-series servers and NonStop BladeSystems only, not for NonStop S-series servers:

- Insight RSA cannot be used in a fault-tolerant CMS configuration for these systems at this time. If you install and configure Insight RSA on more than one CMS that manages NonStop BladeSystems or NS-series servers, be sure to perform discovery of those systems in HP SIM on only one CMS, to avoid duplicate dial-outs.
- The following invalid OSM subsystem event is always created, even when an Incident Report has successfully been delivered to the CMS. Ignore this event and look at the HP SIM Events tab to see the actual delivery status of the Incident Report.

OSM subsystem event 1103. An Incident Report has failed to be delivered.
Reason: Incident report delivery path not configured.

Fallback

In the event you wish to fall back from Insight RSA to using the OSM Notification Director, perform the following tasks as appropriate (depending on whether you deleted or simply disabled the ND during the migration to Insight RSA):

- Either stop the HP Systems Insight Manager service, if you will not be using HP SIM at all (Start > Control Panel > Administrative Tools > Services), or just delete the individual NonStop system(s) from HP SIM, if you will continue to use HP SIM to monitor other systems.
- Remove the OSMCONF flags inserted during the OSMCONF configuration task, then restart the OSM server for these changes to take effect.
- As applicable, undo the steps performed to disable the OSM Notification Director and Remote Proxy Service during **Scenario 1** of the Insight RSA migration. If you deleted the OSM Notification Director and Remote Proxy Service Start Menu shortcuts, you would need to reinstall those products. If not, simply rename the files back to their original names and restart the services.
- If individual systems were deleted from the OSM Notification Director (as called for in **Scenarios 3 and 4**), reconfigure each NonStop system within the OSM Notification Director.

Legal Notice

Legal Notice

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Export of the information contained in this publication may require authorization from the U.S. Department of Commerce.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation.

Intel, Pentium, and Celeron are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java is a U.S. trademark of Sun Microsystems, Inc.

Motif, OSF/1, UNIX, X/Open, and the "X" device are registered trademarks, and IT DialTone and The Open Group are trademarks of The Open Group in the U.S. and other countries.

Open Software Foundation, OSF, the OSF logo, OSF/1, OSF/Motif, and Motif are trademarks of the Open Software Foundation, Inc. OSF MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THE OSF MATERIAL PROVIDED HEREIN, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. OSF shall not be liable for errors contained herein or for incidental consequential damages in connection with the furnishing, performance, or use of this material.

© 1990, 1991, 1992, 1993 Open Software Foundation, Inc. The OSF documentation and the OSF software to which it relates are derived in part from materials supplied by the following: © 1987, 1988, 1989 Carnegie-Mellon University. © 1989, 1990, 1991 Digital Equipment Corporation. © 1985, 1988, 1989, 1990 Encore Computer Corporation. © 1988 Free Software Foundation, Inc. © 1987, 1988, 1989, 1990, 1991 Hewlett-Packard Company. © 1985, 1987, 1988, 1989, 1990, 1991, 1992 International Business Machines Corporation. © 1988, 1989 Massachusetts Institute of Technology. © 1988, 1989, 1990 Mentat Inc. © 1988 Microsoft Corporation. © 1987, 1988, 1989, 1990, 1991, 1992 SecureWare, Inc. © 1990, 1991 Siemens Nixdorf Informationssysteme AG. © 1986, 1989, 1996, 1997 Sun Microsystems, Inc. © 1989, 1990, 1991 Transarc Corporation. OSF software and documentation are based in part on the Fourth Berkeley Software Distribution under license from The Regents of the University of California. OSF acknowledges the following individuals and institutions for their role in its development: Kenneth C.R.C. Arnold, Gregory S. Couch, Conrad C. Huang, Ed James, Symmetric Computer Systems, Robert Elz. © 1980, 1981, 1982, 1983, 1985, 1986, 1987, 1988, 1989 Regents of the University of California.

