Migration to Internet-based Remote Support is Imminent

HP Insight Remote Support Advanced

Vinay Gupta
NonStop Manageability Architect
Distinguished Technologist, HP
Agenda

• End of modem-based remote support
• Introduction of HP Insight Remote Support Advanced
• Supported configurations
• Hardware and software requirements
• CMS / NSC configurations
• Security design
• Remote Device Access (RDA) options
• References
Modem-based remote support going away

- HP NonStop system's modem-based remote support infrastructure, including remote monitoring (dial-out) and remote connectivity (dial-in), will be discontinued effective October 31, 2011.

- HP Insight Remote Support Advanced is the replacement for the modem-based remote support solution for NonStop systems.

- HP Insight Remote Support Advanced is HP's strategic solution to provide common remote support services across the full range of enterprise hardware.

- NonStop customers need to move to this go-forward solution.

- HP Insight Remote Support Advanced is qualified on all NonStop systems, including HP Integrity NonStop BladeSystems, HP Integrity NonStop NS-series servers, and NonStop S-series servers.
HP Insight Remote Support Advanced

- Proactive, web-based, remote monitoring and diagnostic tool to manage systems and devices
- Real-time monitoring of hardware events and automated notification to HP support center
- Remote troubleshooting and repair capabilities
- Internet connectivity to HP support
- Quick and secure connection
- A plug-in to HP SIM
- Support of all HP platforms
- Available at no extra cost as part of warranty, HP Care Pack Service or contractual support agreement with HP
Supported configurations

**Recommended configuration**

- Utilize centralized CMSs (Central Management Servers) to install HP SIM and Insight Remote Support Advanced
  - Requires OSM server to also run on non-maintenance LAN TCP/IP stacks
- Do not use NSC as a CMS
  - NSC resides in a dedicated maintenance LAN.
  - Using NSC as a CMS means only the NonStop systems in that maintenance LAN can be managed.
  - It results in multiple copies of HP SIM and Insight Remote Support Advanced and more maintenance costs.
- Install HP SIM and Insight Remote support Advanced on two CMSs for fault tolerance

**Alternate configuration**

- Install HP SIM and Insight Remote Support Advanced on two CMSs for fault tolerance
- Use either Insight Remote Support Advanced or OSM Notification Director, but NOT both, to monitor a NonStop system
Resource requirements

If using centralized CMSs
- Dual CMSs for fault-tolerance
- ProLiant server or ProLiant blade orderable from HP
- Windows Server 2003 or later
- HP SIM version 5.1 or later
- At least 3 GB of memory
- Dual CMSs for fault-tolerance

If using NSCs
- Dual NSCs for fault tolerance
- Windows Server 2003-based NSC
- HP SIM version 5.1 or later
- 4 GB of memory - to accommodate HP SIM, Insight Remote Support Advanced and other NSC applications
  - The latest NSCs have 4 GB of memory.
  - 2 GB memory upgrades are available for many NSC models.
  - Very old NSC models cannot be used as a CMS.
Latest NSC models shipped with 4 GB of memory

<table>
<thead>
<tr>
<th>NED NSC</th>
<th>HP Server</th>
<th>Shipped w/ Mem</th>
<th>Form Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSCR110 or NSCR210</td>
<td>DL320G6</td>
<td>4 GB</td>
<td>Rack mount</td>
</tr>
<tr>
<td>NSCD110 or NSCD210</td>
<td>ML110G6</td>
<td>4 GB</td>
<td>Deskside</td>
</tr>
</tbody>
</table>
NSCs upgradeable to 4 GB of memory

<table>
<thead>
<tr>
<th>NED NSCs*</th>
<th>HP Server</th>
<th>Shipped w/ Mem</th>
<th>Form Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSCR4</td>
<td>DL320 G5P</td>
<td>2 GB</td>
<td>Rack mount</td>
</tr>
<tr>
<td>BLCR4</td>
<td>DL320 G5P</td>
<td>2 GB</td>
<td>Rack mount</td>
</tr>
<tr>
<td>S7X-NSC8</td>
<td>ML110 G5</td>
<td>2 GB</td>
<td>Deskside</td>
</tr>
<tr>
<td>S7X-NSC8NM</td>
<td>ML110 G5</td>
<td>2 GB</td>
<td>Deskside</td>
</tr>
<tr>
<td>S7X-BLC8</td>
<td>ML110 G5</td>
<td>2 GB</td>
<td>Deskside</td>
</tr>
<tr>
<td>S7X-BLC8NM</td>
<td>ML110 G5</td>
<td>2 GB</td>
<td>Deskside</td>
</tr>
<tr>
<td>NSCR3</td>
<td>DL320 G5</td>
<td>1 GB</td>
<td>Rack mount</td>
</tr>
</tbody>
</table>
NSCs NOT upgradeable to 4 GB of memory

<table>
<thead>
<tr>
<th>NED NSC</th>
<th>HP Server</th>
<th>Shipped w/ Mem</th>
<th>Form Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSCR2</td>
<td>DL320G4</td>
<td>1 GB</td>
<td>Rack mount</td>
</tr>
<tr>
<td>NSCR1</td>
<td>DL320G3</td>
<td>1 GB</td>
<td>Rack mount</td>
</tr>
<tr>
<td>S7X-NSC7 and earlier</td>
<td>varies</td>
<td>varies</td>
<td>Deskside</td>
</tr>
</tbody>
</table>
Reminder: End of support of NSC models as of December 2010

<table>
<thead>
<tr>
<th>S7X-NSC1</th>
<th>S7X-PC</th>
</tr>
</thead>
<tbody>
<tr>
<td>S7X-NSC2</td>
<td>S7X-PC1000</td>
</tr>
<tr>
<td>S7X-NSC3</td>
<td>S7X-PC2</td>
</tr>
<tr>
<td>S7X-NSC3NM</td>
<td>S7X-PC3</td>
</tr>
<tr>
<td>S7X-NSC4</td>
<td>S7X-PC3D</td>
</tr>
<tr>
<td>S7X-NSC4NM</td>
<td>S7X-IPAQ</td>
</tr>
<tr>
<td>S7X-NSC5</td>
<td>S7X-IPAQM</td>
</tr>
<tr>
<td>S7X-NSC5NM</td>
<td></td>
</tr>
</tbody>
</table>
HP Insight Remote Support
Advanced Security
Insight Remote Support Advanced security design

- HP Insight Remote Support Advanced is a support technology that involves the delivery of remote customer support using a public network infrastructure (Internet).

- HP faced security concerns and public perception issues similar to other e-business vendors who conduct security sensitive transactions using the Internet.

- In business today, many security sensitive transactions such as e-commerce, stock trades, and online banking, are executed securely over the Internet using the same industry standard security technologies utilized by Insight Remote Support Advanced.
Application, outbound and data security

### Application security

- CMS setup as defined by the customer’s IT security policy
- All updates downloaded by HP SIM digitally signed and verified before they are executed, to maintain the integrity and authenticity of the Insight Remote Support Advanced software and prevent unauthorized changes

### Outbound security

- Collection of incidents from monitored systems inside the customer’s IT environment
- External firewall between the CMS and the HP data center
- Outbound connection to HP using HTTPS to provide confidentiality and integrity of the information

### Data security

- Availability of the Insight Remote Support Advanced infrastructure maintained via high-availability HP servers
- Customer data housed in HP’s secured access data centers
- All collected data classified internally as HP private
- Data kept encrypted on the storage and backup media
- Access of the collected data allowed to only authorized HP support specialists
Inbound security

- Inbound connection to a customer-designated access server only
- Many remote access solutions available to meet customer’s security requirements, all using standard techniques that include SSH, IPSec and HTTPS
- Both hardware and software solutions available, which can be configured to ensure the customer control of the connection
- Customer option to monitor a support specialist’s activities
- Adherence by all HP support specialists to the same standard of business conduct as onsite HP engineers, and allowed to attempt a connection with the customer’s approval and a business need only
- Possible to restrict the access to only the HP support specialists assigned to the team
- Use of two-factor authentication internally in HP to control access to the HP access connectivity servers
- All connections, attempted and successful, to customer systems logged
Remote Device Access (RDA)
Options
Remote Device Access (RDA) options

- Attended RDA via HP Virtual Support Room (VSR), a web-based desktop-sharing application

- Unattended RDA via SSH tunneling
  - SSH tunnel terminated at a Customer Access System (CAS) deployed either in the customer DMZ or on a trusted network
    - SSH-Direct – SSH tunnel bare over the Internet
    - VPN Connectivity – SSH tunnel inside a VPN connection between HP and the customer
    - ISDN Connectivity – SSH tunnel over an ISDN connection*

* Not available in all countries
Attended RDA via Virtual Support Room (VSR)

- Light-weight, web-hosted meeting place for HP support specialists and customer
- No complex configuration or hardware setup
- Based on HP Virtual Rooms and offers web collaboration functionality, such as desktop sharing, file transfer and desktop control
- Session initiated by the HP support specialist
- Keys required to enter the VSR generated by the HP support specialist and shared with the customer via email or phone
- Keys valid for one hour only
- VSR server infrastructure owned and hosted by HP
- All sessions encrypted with AES-256 using SSL over HTTPS on port 443
- Possible to use web proxy servers to access the HP VSR infrastructure

- All actions requested by the support engineer must first be approved by the customer – via a popup permissions window.
- The customer can view in real time, and can suspend a session immediately if needed.
Unattended RDA via SSH tunneling

Relies on an SSH-2 tunnel between the support specialist’s desktop, and a designated Customer Access System (CAS) deployed either in the customer DMZ or on a trusted network, hosting the SSH server.

**Customer Access System (CAS)**
- Central point for customers to control remote access into their environment.
- Customers determine the login of each HP user individually to allow or deny specific services or access to specific systems within their network.

**Customer-owned CAS**
- Must run an SSH server, e.g., OpenSSH
- May run Windows, Linux, HP-UX, OpenVMS or Tru64
- Can be CMS
- Recommended to accept only SSH-2
- Recommended to use strong encryption, such as AES, Triple-DES, or AES-256
- Recommended to configure firewalls to allow access only from HP’s access servers

**Virtual CAS**
- HP-preferred method, provided for free
- Software-only solution running on CMS
- Provides an administration web interface
- Implements X.509 certificate-based authentication
- Provides fine-granularity access control; e.g., customers can specify user level access to targets including TCP ports
- Polls HP for software updates or security patches, providing the customer full control on how and when to apply them
SSH-Direct

- The quickest and easiest unattended RDA solution
- Need to provide only an Internet routable IP address for the CAS to HP, and allow one of the HP access servers to access it on port 22
- Supports customer-owned and virtual CAS
VPN Connectivity

- All inbound connections protected inside a VPN connection terminated in customer’s DMZ

- Support of both with and without SSH tunneling
  - SSH recommended for better end-to-end security and enhanced functionality (e.g., file transfer capabilities and application tunneling)
VPN routers

**hpVPN**
- HP provided router, deployed in the customer’s DMZ
- Establishes an IPsec VPN connection with a Customer Premises Equipment (CPE) router, at the customer’s site
- Software and router configurations on both ends maintained by HP
- Uses triple-DES encryption and SHA-1 HMAC
- Only connections from authorized HP systems allowed by access lists on the CPE

**Customer-Owned Router (COR) VPN**
- Can be ProCurve, 3Com, Cisco IOS, Cisco PIX, Check Point, Stonesoft, Juniper, Nortel or any other VPN router
- IPSec VPN established by HP with a customer-owned router
- Managed and configured by the customer
- Connections configured tailored to the customer’s requirements
ISDN Connectivity

- SSH port-forwarding over ISDN (Integrated Service Digital Network)
- Offered in some countries only
References and Contacts
## References

### Web pages

<table>
<thead>
<tr>
<th>Service</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>NonStop Operations Management</td>
<td><a href="http://www.hp.com/go/nonstop/operationsmanagement">http://www.hp.com/go/nonstop/operationsmanagement</a></td>
</tr>
<tr>
<td>HP Systems Insight Manager (SIM)</td>
<td><a href="http://www.hp.com/go/hpsim">http://www.hp.com/go/hpsim</a></td>
</tr>
</tbody>
</table>
## References

### Manuals

<table>
<thead>
<tr>
<th>Manual Type</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP SIM Manuals</td>
<td><a href="http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?lang=en&amp;cc=us&amp;taskId=101&amp;prodClassId=10008&amp;contentType=SupportManual&amp;docIndexId=64255&amp;prodTypeId=18964&amp;prodSeriesId=489496">http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?lang=en&amp;cc=us&amp;taskId=101&amp;prodClassId=10008&amp;contentType=SupportManual&amp;docIndexId=64255&amp;prodTypeId=18964&amp;prodSeriesId=489496</a></td>
</tr>
</tbody>
</table>
### References

**Support notes**

<table>
<thead>
<tr>
<th>HP Insight Remote Support Advanced for NonStop</th>
<th>S09057F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discontinuation of Modem-Based Remote Support</td>
<td>S10052</td>
</tr>
</tbody>
</table>
Outcomes that matter.
NonStop system showing up under Insight Remote Support Advanced supported systems
Service incident creation event in Events tab of a NonStop system
Problem incident details

Service Event Details

<table>
<thead>
<tr>
<th>Variable Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the system this service event relates to.</td>
<td>OSMQA5-gssag0.cacab.cac.cpq.corp.net</td>
</tr>
<tr>
<td>IP Address of the system this service event relates to.</td>
<td>16.107.146.46</td>
</tr>
<tr>
<td>The severity of the service incident.</td>
<td>2</td>
</tr>
<tr>
<td>The status of the service incident.</td>
<td>Delivered to Remote Support</td>
</tr>
<tr>
<td>Provides the URL to the event analysis report.</td>
<td><a href="https://BIOSM4-NSC2:7800/webseNotification?id=BIOSM4-NSC2@1240252725500">https://BIOSM4-NSC2:7800/webseNotification?id=BIOSM4-NSC2@1240252725500</a></td>
</tr>
<tr>
<td>Brief description of the event that initiated the service incident.</td>
<td>Problem Incident: SNMP Test Trap Not Received</td>
</tr>
<tr>
<td>Unique Event Analysis Identifier assigned to the incident.</td>
<td>BIOSM4-NSC2@1240252725500</td>
</tr>
<tr>
<td>Time of the original event this service event relates to.</td>
<td>Mon 20 Apr 2009 11:38:45 GMT 07:00</td>
</tr>
<tr>
<td>Name of the system this service event was analyzed on.</td>
<td>BIOSM4-NSC2.private.corp.com</td>
</tr>
<tr>
<td>This is a URL pointing to the Service Incident Status in IDEE if available.</td>
<td><a href="https://localhost:2381/lmc/eo/event-display.php?eventGuid=A6BC0233-3509-4CA2-6062-B5600831C297F">https://localhost:2381/lmc/eo/event-display.php?eventGuid=A6BC0233-3509-4CA2-6062-B5600831C297F</a></td>
</tr>
<tr>
<td>Service incident identifier assigned to the incident report by the IDEE client.</td>
<td>A6BC0233-3509-4CA2-6062-B5600831C297F</td>
</tr>
<tr>
<td>The ID of the originally received event.</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Recommended action.</td>
<td>SNMP Test Trap Not Received Please refer to the attachment file(s) for the recommended repair actions. The following Attachment files are associated with this Problem Report:</td>
</tr>
<tr>
<td>Replaceable Unit information.</td>
<td>OLYM #2BC1P.0100261</td>
</tr>
</tbody>
</table>
Service event status details

Event Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submission ID</td>
<td>A5B02533-5899-4CA2-0062-B500081C297F</td>
</tr>
<tr>
<td>Submission Date-Time</td>
<td>04.20.2009 - 11:48:18</td>
</tr>
<tr>
<td>Description</td>
<td>Problem Incident: CLIM $ZCOP.C100251 [Logical]#SNMP Test Trap Not Received</td>
</tr>
<tr>
<td>Workflow ID</td>
<td></td>
</tr>
<tr>
<td>Current State</td>
<td>Closed</td>
</tr>
<tr>
<td>Business</td>
<td>NSK_Servers</td>
</tr>
<tr>
<td>Device Name</td>
<td>\OSMQA6</td>
</tr>
<tr>
<td>Device IP</td>
<td></td>
</tr>
<tr>
<td>Compressed Submission Size</td>
<td>4981 bytes</td>
</tr>
<tr>
<td>Submission Type</td>
<td>incident</td>
</tr>
</tbody>
</table>

Event Annotations

- 11:39:02 04 20 2009: Submission state changed from "Pending" to "Submitted"
- 11:43:18 04 20 2009: Submission state changed from "Submitted" to "Received"
- 11:43:18 04 20 2009: Submission state changed from "Received" to "Closed"
- 11:43:18 04 20 2009: Close NSK motive incidents after routing externally

Download Event Files:
event.xml

Download Attachment Files:
ZZAA2553
Problem incident analysis report

Time of Event:
Incident Report ID: 2637
Event Time: 04-20-2002 18:42:14 GMT+00:00

Managed Entity:
System Name: \\OSNQ15
System Serial: OSNQ15
OS Type: NonStop
OS Version: M98.10

Callout Type:
Problem Incident

Brief Description:
SNMP Test Trap Not Received

Resource Name:
CLIM %ZSCIP.C1002S1

Description:
CLIM %ZSCIP.C1002S1 [Logical]#SNMP Test Trap Not Received

Attachment File Data:
Please refer to the attachment file[s] for the recommended repair actions.

The following Attachment files are associated with this Problem Report:
%SYSTEM.ZSERVICE.ZZLAD.SEZS

Additional Data:
Severity: Major
Probable Cause: Connection Established Error
Resource Name: CLIM %ZSCIP.C1002S1
Provider Name: NonStopOSMProvider

Analysis Tool: WEDES
Tool Version: Web-Based Enterprise Services Common Components for Windows V5.5 (Build 56), member of Web-Based Enterprise Services

Done