Migration to Internet-based Remote Support is Imminent

HP Insight Remote Support Advanced

Vinay Gupta
NonStop Manageability Architect
Distinguished Technologist, HP

©2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice

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

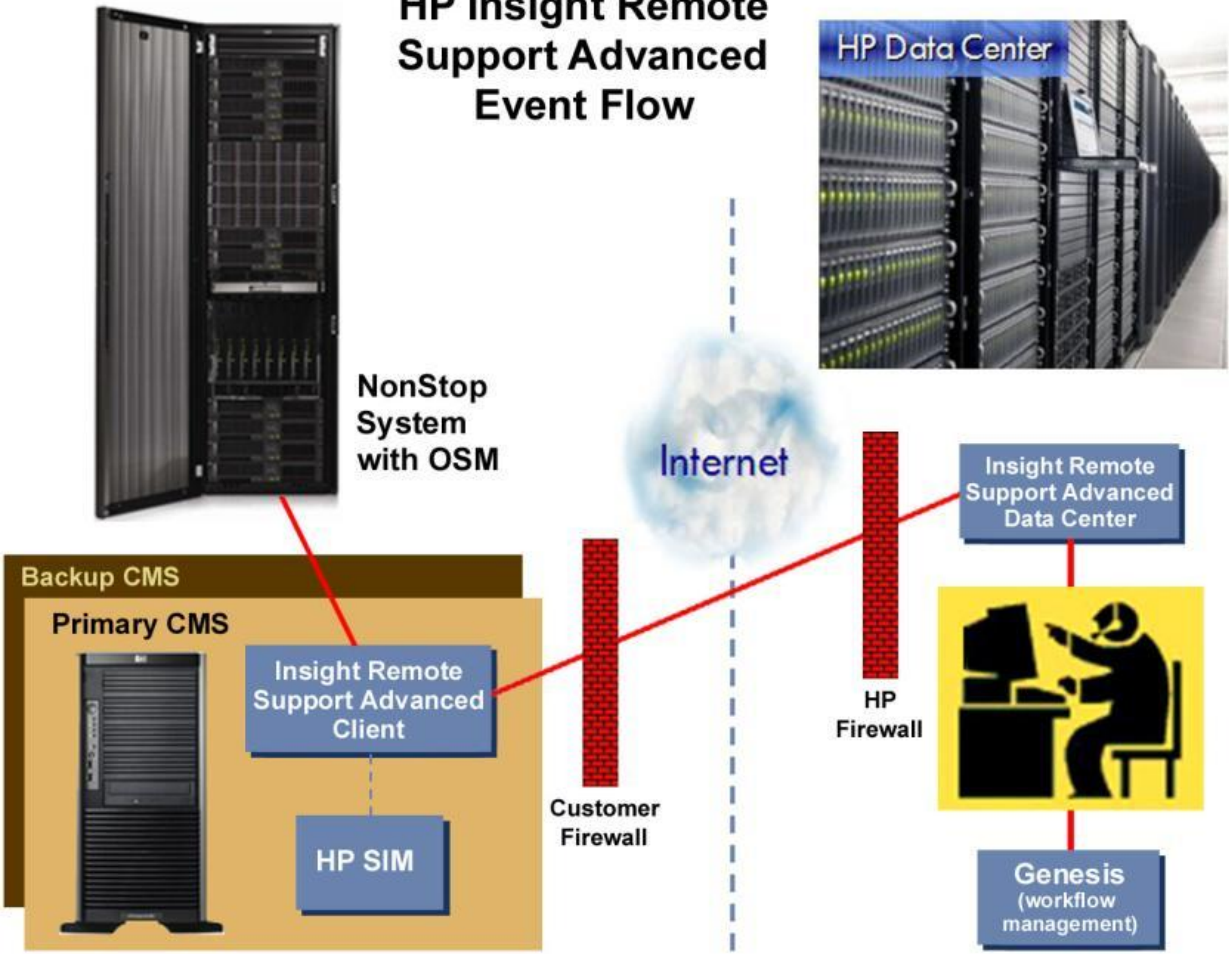
Modem-based remote support going away

- 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

HP Insight Remote Support Advanced Event Flow



HP Data Center

NonStop System with OSM

Internet

Backup CMS

Primary CMS

Insight Remote Support Advanced Client

HP SIM

Customer Firewall

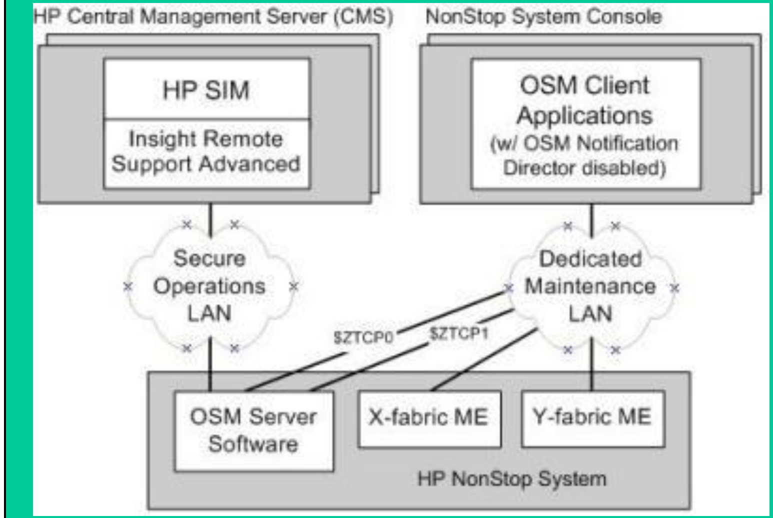
HP Firewall

Insight Remote Support Advanced Data Center

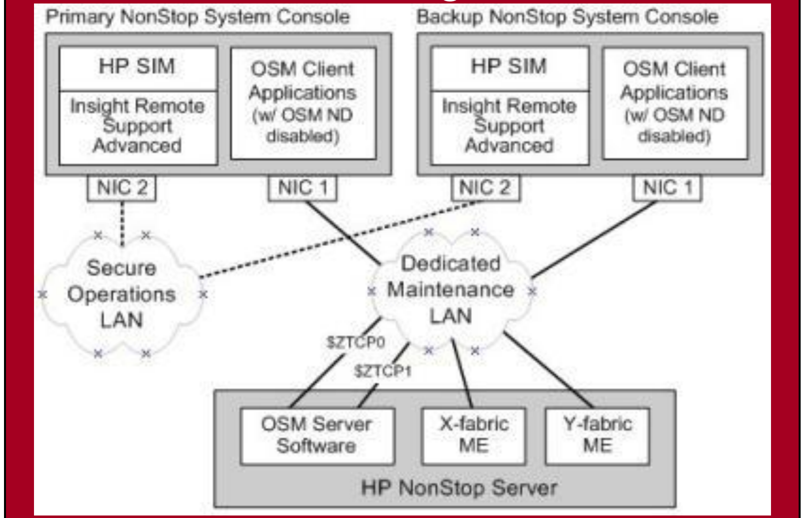
Genesis (workflow management)

Supported configurations

Recommended configuration


HP Central Management Server (CMS)
NonStop System Console
HP SIM
Insight Remote Support Advanced
OSM Client Applications (w/ OSM Notification Director disabled)
Secure Operations LAN
Dedicated Maintenance LAN
$ZTCP0
$ZTCP1
OSM Server Software
X-fabric ME
Y-fabric ME
HP NonStop System

Alternate configuration


Primary NonStop System Console
Backup NonStop System Console
HP SIM
Insight Remote Support Advanced
OSM Client Applications (w/ OSM ND disabled)
HP SIM
Insight Remote Support Advanced
OSM Client Applications (w/ OSM ND disabled)
NIC 2
NIC 1
NIC 2
NIC 1
Secure Operations LAN
Dedicated Maintenance LAN
$ZTCP0
$ZTCP1
OSM Server Software
X-fabric ME
Y-fabric ME
HP NonStop Server

HP recommendations

- 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
- 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

NED NSC	HP Server	Shipped w/ Mem	Form Factor
NSCR110 or NSCR210	DL320G6	4 GB	Rack mount
NSCD110 or NSCD210	ML110G6	4 GB	Deskside

NSCs upgradeable to 4 GB of memory

NED NSCs*	HP Server**	Shipped w/ Mem	Form Factor
NSCR4	DL320 G5P	2 GB	Rack mount
BLCR4	DL320 G5P	2 GB	Rack mount
S7X-NSC8	ML110 G5	2 GB	Deskside
S7X-NSC8NM	ML110 G5	2 GB	Deskside
S7X-BLC8	ML110 G5	2 GB	Deskside
S7X-BLC8NM	ML110 G5	2 GB	Deskside
NSCR3	DL320 G5	1 GB	Rack mount

NSCs NOT upgradeable to 4 GB of memory

NED NSC	HP Server	Shipped w/ Mem	Form Factor
NSCR2	DL320G4	1 GB	Rack mount
NSCR1	DL320G3	1 GB	Rack mount
S7X-NSC7 and earlier	varies	varies	Deskside

Reminder: End of support of NSC models as of December 2010

- S7X-NSC1
- S7X-NSC2
- S7X-NSC3
- S7X-NSC3NM
- S7X-NSC4
- S7X-NSC4NM
- S7X-NSC5
- S7X-NSC5NM
- S7X-PC
- S7X-PC1000
- S7X-PC2
- S7X-PC3
- S7X-PC3D
- S7X-IPAQ
- S7X-IPAQM

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

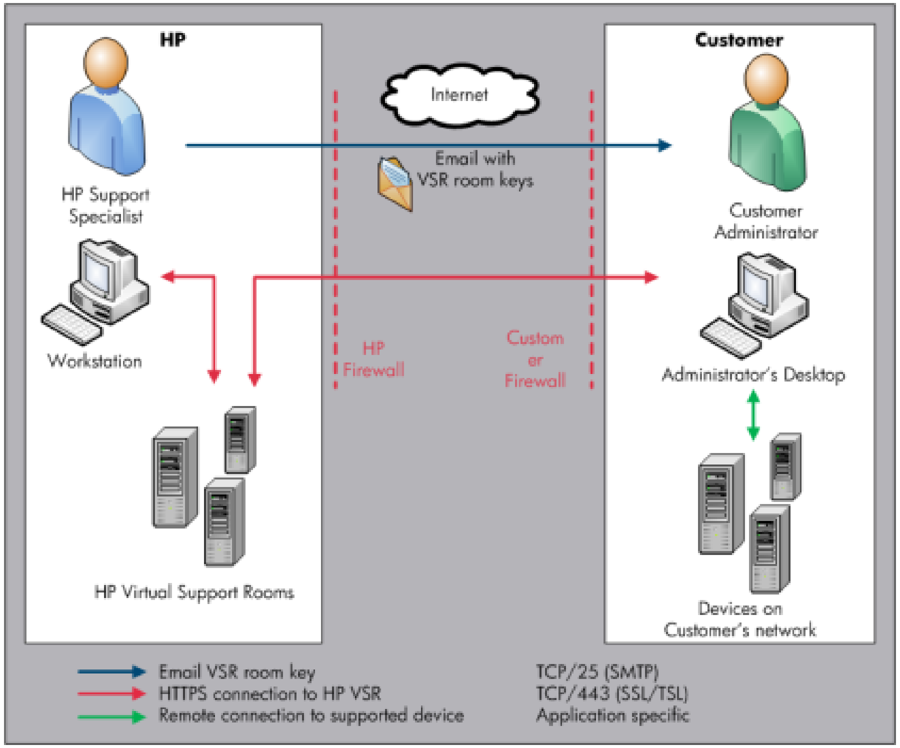
Remote Device Access (RDA) options

- 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

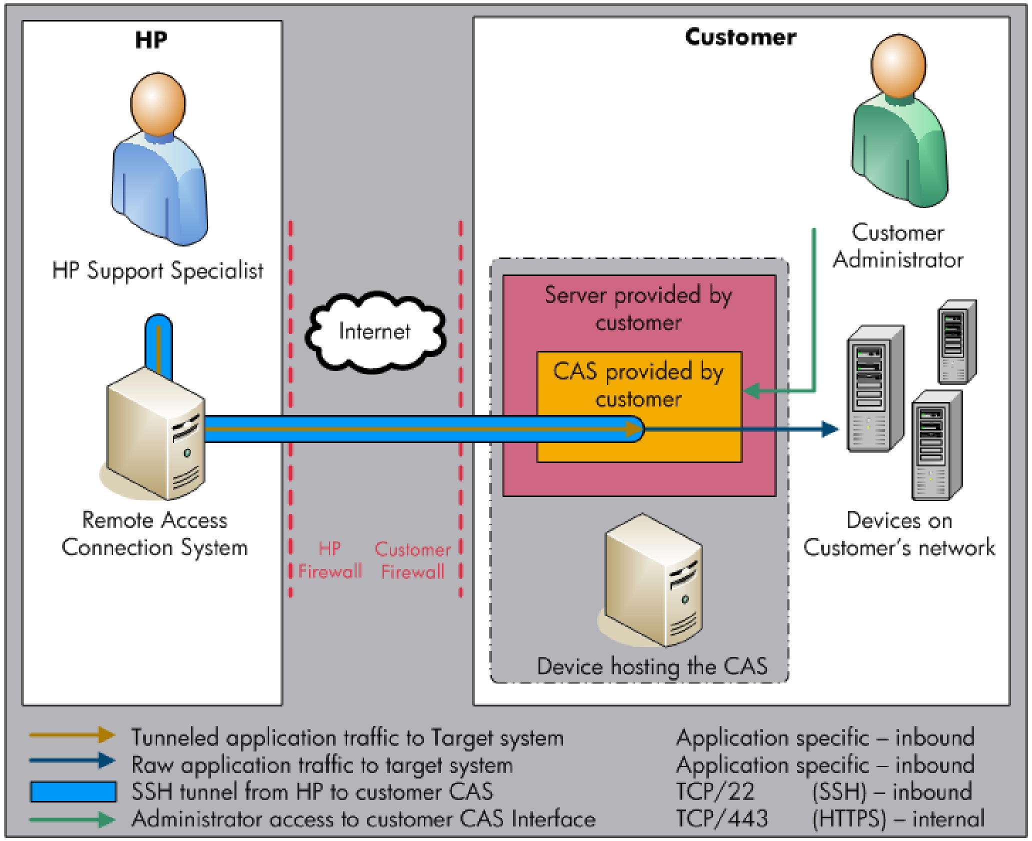
- Must run an SSH server, e.g., OpenSSH
- May run Windows, Linux, HP-UX, OpenVMS or Tru64
- Can be CMS
- Recommended to accept only SSH-2
- Recommended to use strong encryption, such as AES, Triple-DES, or AES-256
- Recommended to configure firewalls to allow access only from HP's access servers

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



HP

HP Support Specialist

Remote Access Connection System

Internet

HP Firewall

Customer Firewall

Customer

Customer Administrator

Server provided by customer

CAS provided by customer

Device hosting the CAS

Devices on Customer's network

Tunneled application traffic to Target system — Application specific – inbound

Raw application traffic to target system — Application specific – inbound

SSH tunnel from HP to customer CAS — TCP/22 (SSH) – inbound

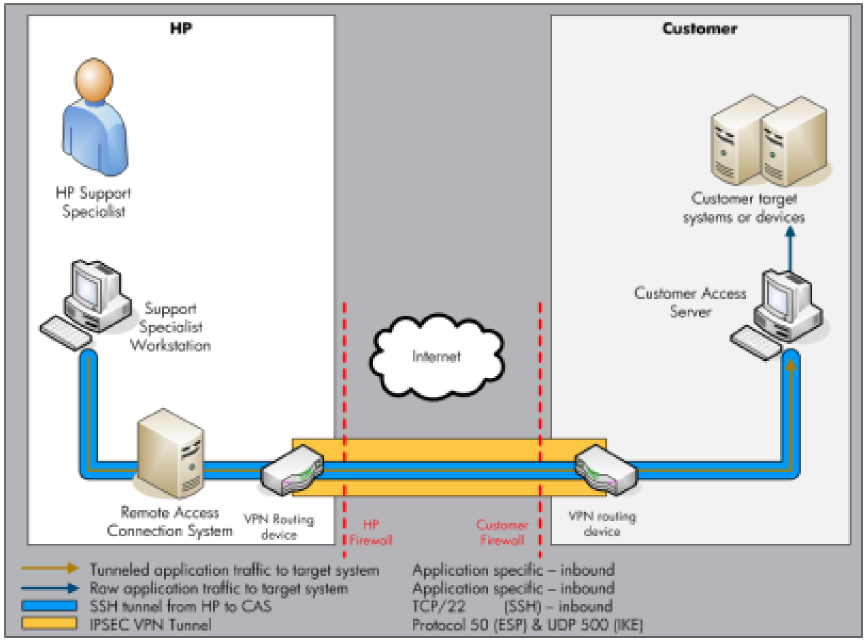
Administrator access to customer CAS Interface — TCP/443 (HTTPS) – internal

VPN Connectivity

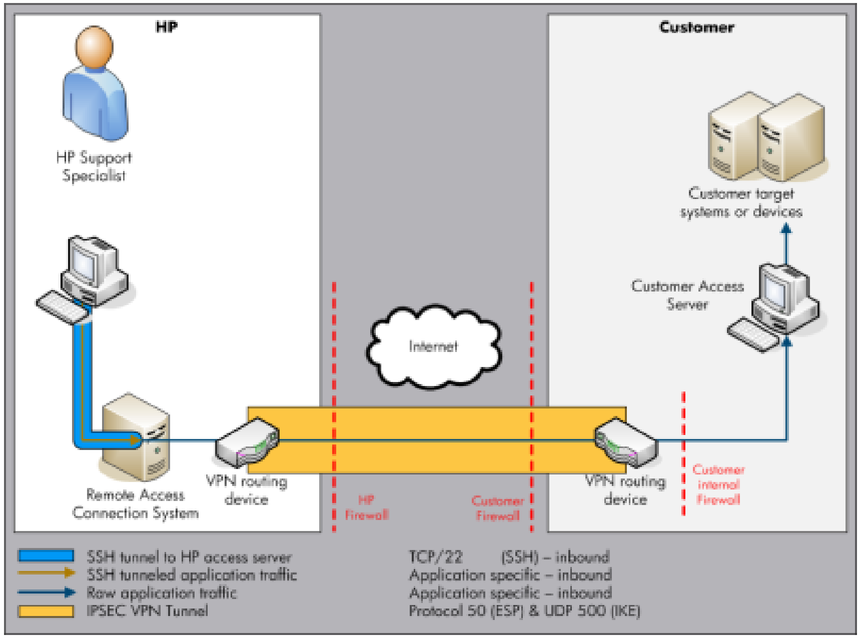
– All inbound connections protected inside a VPN connection terminated in customer's DMZ

– 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)


HP
Customer
HP Support Specialist
Support Specialist Workstation
Internet
Customer target systems or devices
Customer Access Server
Remote Access Connection System
VPN Routing device
HP Firewall
Customer Firewall
VPN routing device
Tunneled application traffic to target system
Raw application traffic to target system
SSH tunnel from HP to CAS
IPSEC VPN Tunnel
Application specific – inbound
Application specific – inbound
TCP/22 (SSH) – inbound
Protocol 50 (ESP) & UDP 500 (IKE)

With SSH


HP
Customer
HP Support Specialist
Customer target systems or devices
Customer Access Server
Internet
Remote Access Connection System
VPN routing device
HP Firewall
Customer Firewall
VPN routing device
Customer internal Firewall
SSH tunnel to HP access server
SSH tunneled application traffic
Raw application traffic
IPSEC VPN Tunnel
TCP/22 (SSH) – inbound
Application specific – inbound
Application specific – inbound
Protocol 50 (ESP) & UDP 500 (IKE)

Without SSH

VPN routers

hpVPN

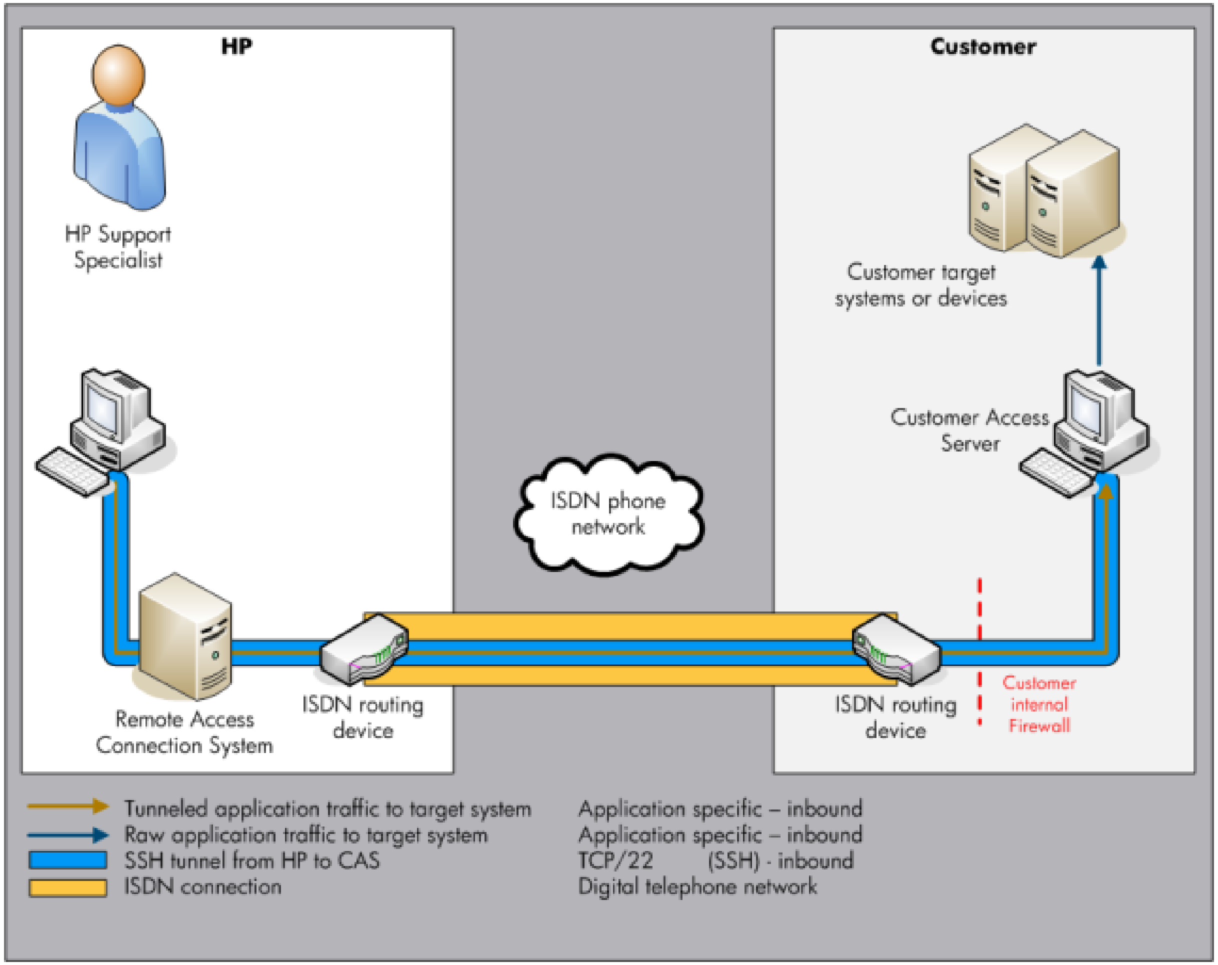
- HP provided router, deployed in the customer's DMZ
- Establishes an IPsec VPN connection with a Customer Premises Equipment (CPE) router, at the customer's site
- Software and router configurations on both ends maintained by HP
- Uses triple-DES encryption and SHA-1 HMAC
- Only connections from authorized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


HP
HP Support Specialist
Remote Access Connection System
ISDN routing device
ISDN phone network
Customer
Customer target systems or devices
Customer Access Server
ISDN routing device
Customer internal Firewall
Tunneled application traffic to target system
Application specific – inbound
Raw application traffic to target system
Application specific – inbound
SSH tunnel from HP to CAS
TCP/22 (SSH) - inbound
ISDN connection
Digital telephone network

References and Contacts

References
Web pages

NonStop Operations Management	http://www.hp.com/go/nonstop/operationsmanagement
HP Systems Insight Manager (SIM)	http://www.hp.com/go/hpsim
HP Remote Support Advanced	http://h18013.www1.hp.com/products/servers/management/insight-remote-support/supportpack/index.html?jumpid=reg_R1002_USEN

References

Manuals

HP SIM Manuals	http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?lang=en&cc=us&taskId=101&prodClassId=10008&contentType=SupportManual&docIndexId=64255&prodTypeId=18964&prodSeriesId=489496
HP Insight Remote Support Advanced Manuals	http://www.hp.com/go/insightremoteadvanced-docs
HP Insight Remote Support Advanced for NonStop Manual	http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c02121539/c02121539.pdf
HP Remote Support Advanced Security Overview	http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c02482637/c02482637.pdf

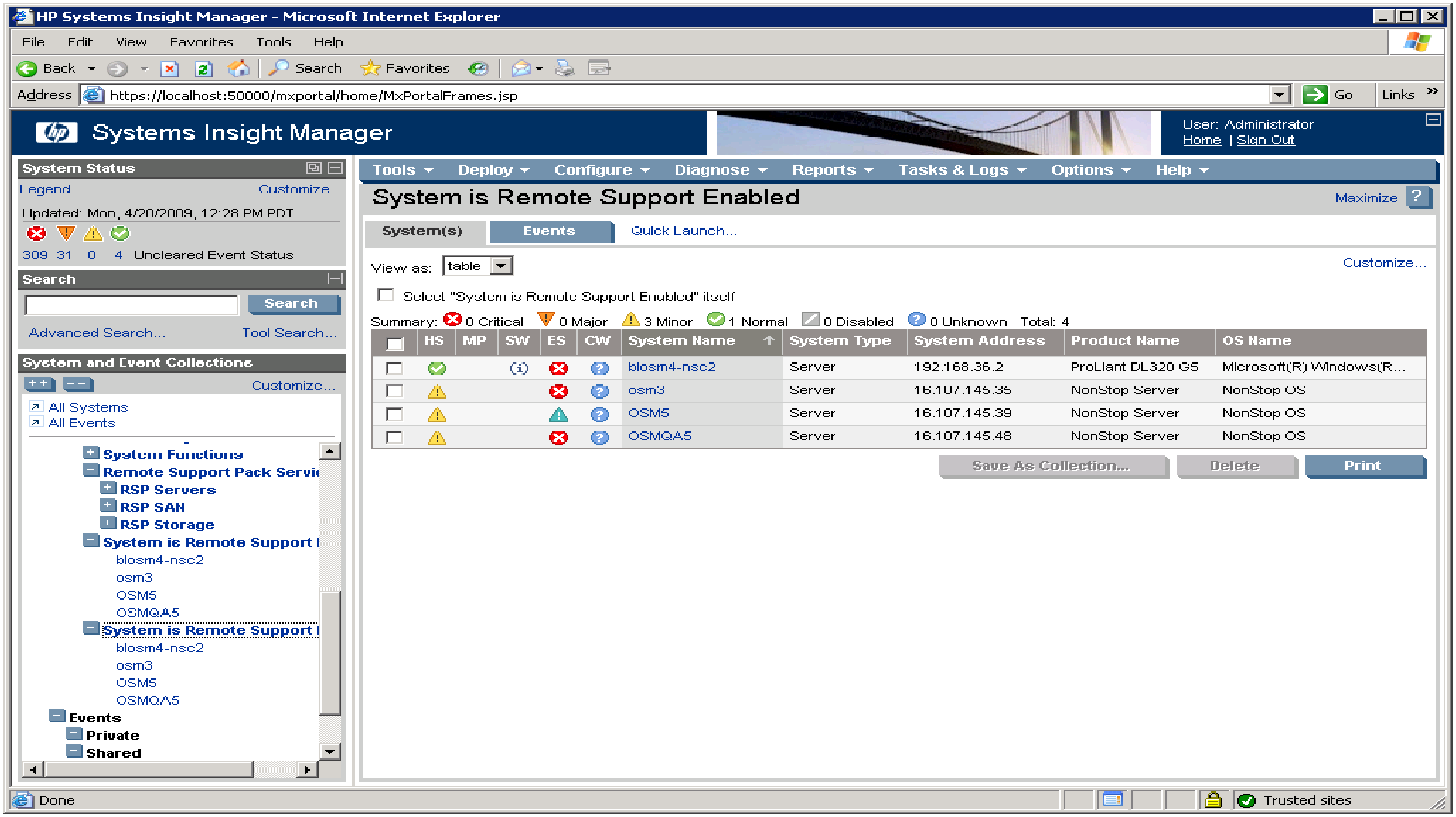
References

Support notes

HP Insight Remote Support Advanced for NonStop	S09057F
Discontinuation of Modem-Based Remote Support	S10052

Outcomes that matter.

NonStop system showing up under Insight Remote Support Advanced supported systems



Address: https://localhost:50000/mxportal/home/MxPortalFrames.jsp

Updated: Mon, 4/20/2009, 12:28 PM PDT

✖ 309 ▼ 31 ⚠ 0 ✓ 4 Uncleared Event Status

System is Remote Support Enabled

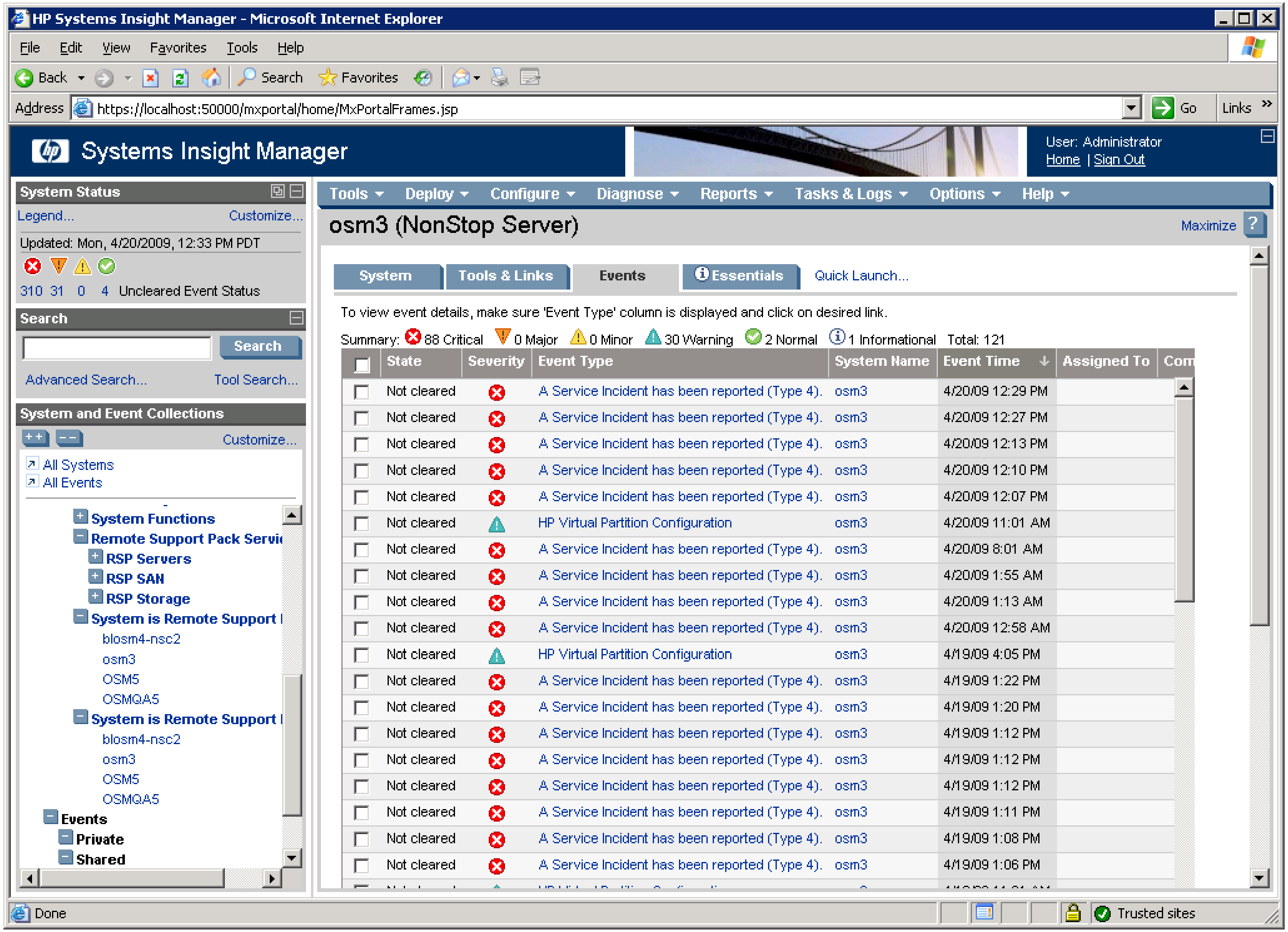
View as: table

□ Select "System is Remote Support Enabled" itself

Summary: ✖ 0 Critical ▼ 0 Major ⚠ 3 Minor ✓ 1 Normal 0 Disabled ? 0 Unknown Total: 4

□	HS	MP	SW	ES	CW	System Name	System Type	System Address	Product Name	OS Name
□	✓		ⓘ	✖	?	blosm4-nsc2	Server	192.168.36.2	ProLiant DL320 G5	Microsoft(R) Windows(R...
□	⚠			✖	?	osm3	Server	16.107.145.35	NonStop Server	NonStop OS
□	⚠			⚠	?	OSM5	Server	16.107.145.39	NonStop Server	NonStop OS
□	⚠			✖	?	OSMQA5	Server	16.107.145.48	NonStop Server	NonStop OS

Service incident creation event in Events tab of a NonStop system


HP Systems Insight Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://localhost:50000/mxportal/home/MxPortalFrames.jsp
Go Links
Systems Insight Manager
User: Administrator
Home | Sign Out
System Status
Legend... Customize...
Search
Search
Advanced Search... Tool Search...
System and Event Collections
Customize...
All Systems
All Events
System Functions
Remote Support Pack Servi
RSP Servers
RSP SAN
RSP Storage
System is Remote Support
blosm4-nsc2
osm3
OSM5
OSMQA5
System is Remote Support
blosm4-nsc2
osm3
OSM5
OSMQA5
Events
Private
Shared
Tools Deploy Configure Diagnose Reports Tasks & Logs Options Help
Maximize
System Tools & Links Events Essentials Quick Launch...
Done
Trusted sites

Updated: Mon, 4/20/2009, 12:33 PM PDT

310 31 0 4 Uncleared Event Status

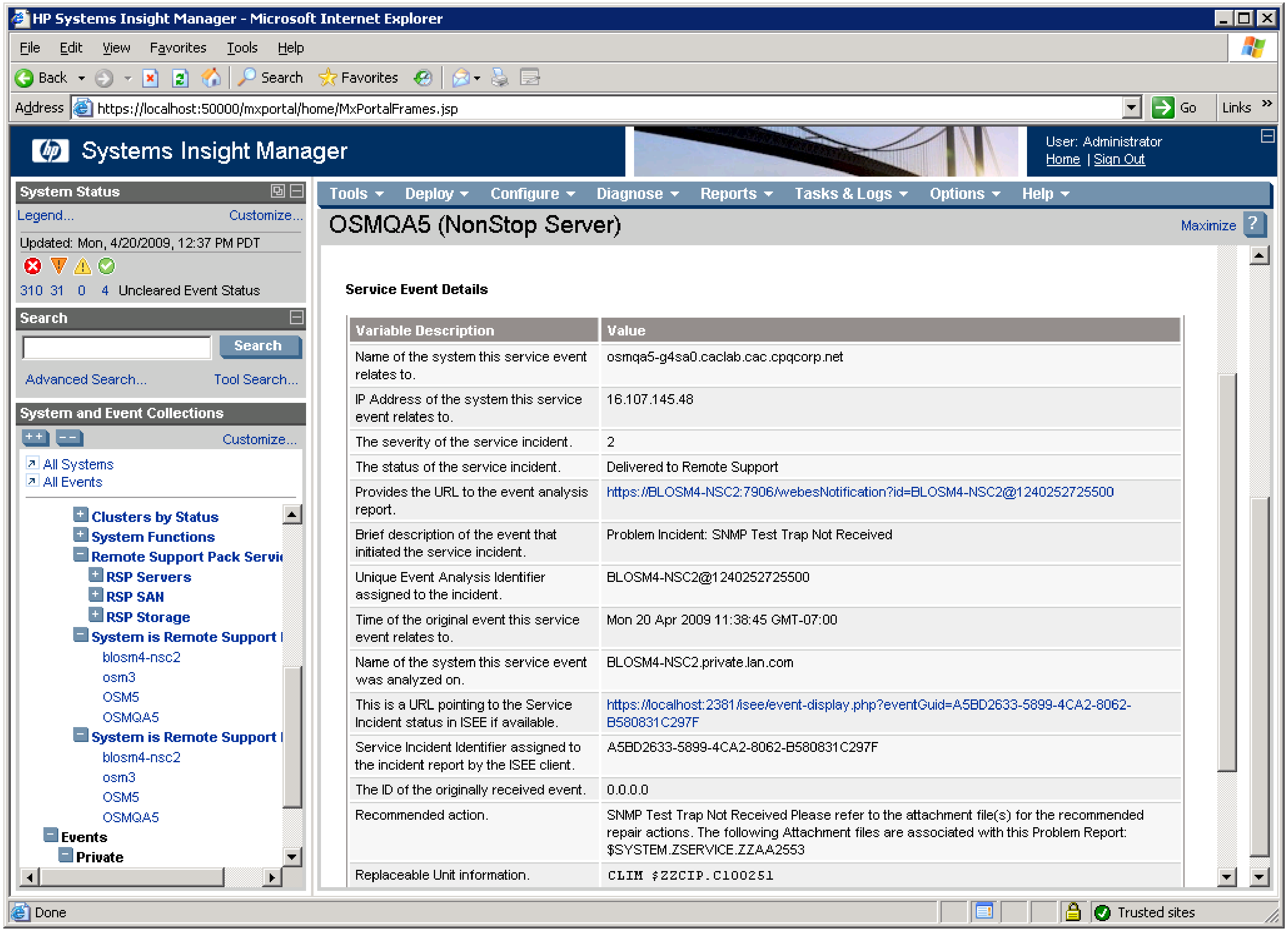
osm3 (NonStop Server)

To view event details, make sure 'Event Type' column is displayed and click on desired link.

Summary: 88 Critical 0 Major 0 Minor 30 Warning 2 Normal 1 Informational Total: 121

□	State	Severity	Event Type	System Name	Event Time	Assigned To	Com
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/20/09 12:29 PM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/20/09 12:27 PM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/20/09 12:13 PM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/20/09 12:10 PM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/20/09 12:07 PM		
□	Not cleared	⚠	HP Virtual Partition Configuration	osm3	4/20/09 11:01 AM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/20/09 8:01 AM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/20/09 1:55 AM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/20/09 1:13 AM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/20/09 12:58 AM		
□	Not cleared	⚠	HP Virtual Partition Configuration	osm3	4/19/09 4:05 PM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/19/09 1:22 PM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/19/09 1:20 PM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/19/09 1:12 PM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/19/09 1:12 PM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/19/09 1:12 PM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/19/09 1:11 PM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/19/09 1:08 PM		
□	Not cleared	⊗	A Service Incident has been reported (Type 4).	osm3	4/19/09 1:06 PM		

Problem incident details



Updated: Mon, 4/20/2009, 12:37 PM PDT

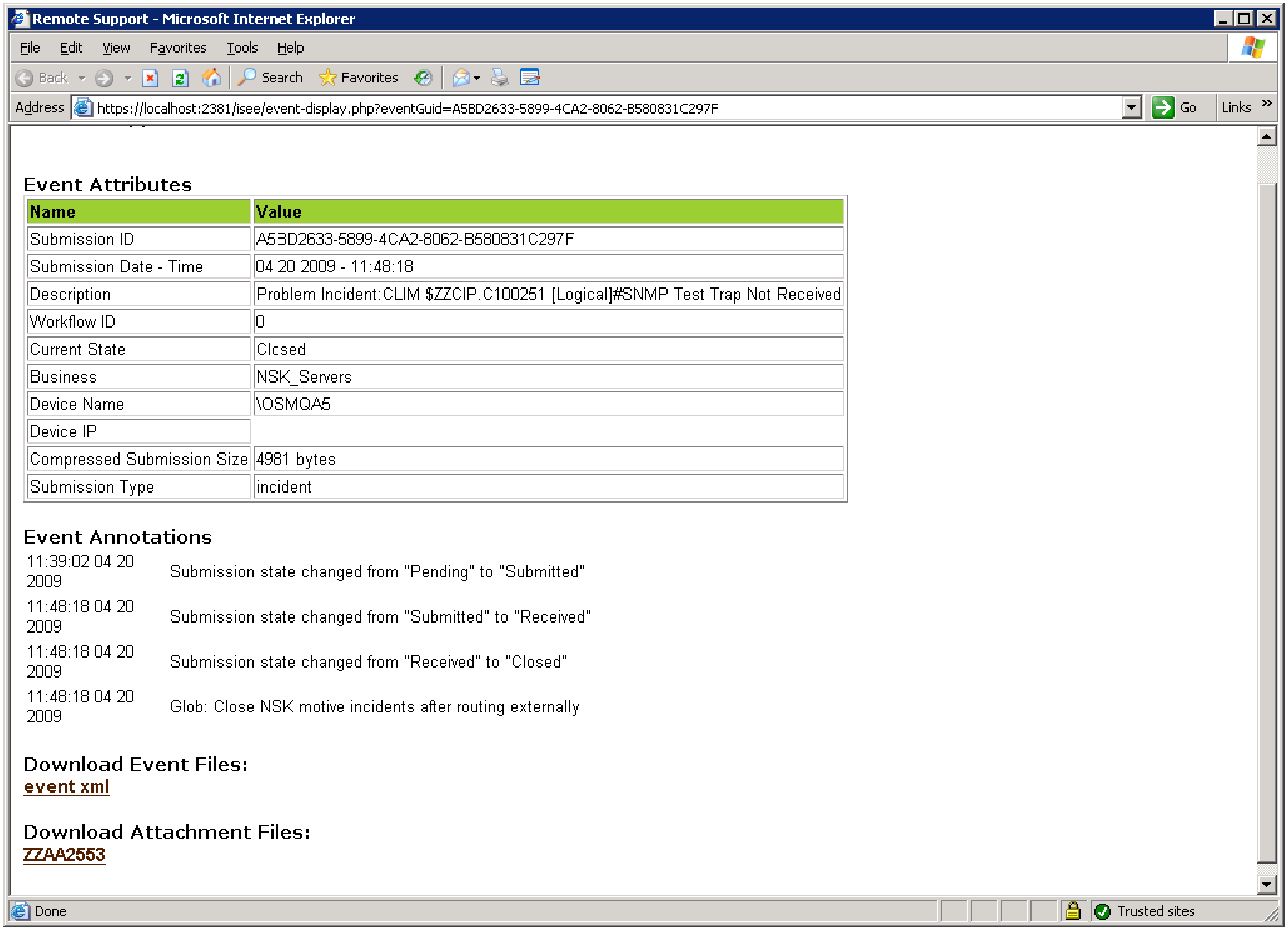
310 31 0 4 Uncleared Event Status

OSMQA5 (NonStop Server)

Service Event Details

Variable Description	Value
Name of the system this service event relates to.	osmqa5-g4sa0.caclab.cac.cpqcorp.net
IP Address of the system this service event relates to.	16.107.145.48
The severity of the service incident.	2
The status of the service incident.	Delivered to Remote Support
Provides the URL to the event analysis report.	https://BLOSM4-NSC2:7906/webesNotification?id=BLOSM4-NSC2@1240252725500
Brief description of the event that initiated the service incident.	Problem Incident: SNMP Test Trap Not Received
Unique Event Analysis Identifier assigned to the incident.	BLOSM4-NSC2@1240252725500
Time of the original event this service event relates to.	Mon 20 Apr 2009 11:38:45 GMT-07:00
Name of the system this service event was analyzed on.	BLOSM4-NSC2.private.lan.com
This is a URL pointing to the Service Incident status in ISEE if available.	https://localhost:2381/isee/event-display.php?eventGuid=A5BD2633-5899-4CA2-8062-B580831C297F
Service Incident Identifier assigned to the incident report by the ISEE client.	A5BD2633-5899-4CA2-8062-B580831C297F
The ID of the originally received event.	0.0.0.0
Recommended action.	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: $SYSTEM.ZSERVICE.ZZAA2553
Replaceable Unit information.	CLIM $ZZCIP.C100251

Service event status details



Remote Support - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://localhost:2381/isee/event-display.php?eventGuid=A5BD2633-5899-4CA2-8062-B580831C297F
Go Links
Done
Trusted sites

Event Attributes

Name	Value
Submission ID	A5BD2633-5899-4CA2-8062-B580831C297F
Submission Date - Time	04 20 2009 - 11:48:18
Description	Problem Incident:CLIM $ZZCIP.C100251 [Logical]#SNMP Test Trap Not Received
Workflow ID	0
Current State	Closed
Business	NSK_Servers
Device Name	\OSMQA5
Device IP	
Compressed Submission Size	4981 bytes
Submission Type	incident

Event Annotations

11:39:02 04 20 2009	Submission state changed from "Pending" to "Submitted"
11:48:18 04 20 2009	Submission state changed from "Submitted" to "Received"
11:48:18 04 20 2009	Submission state changed from "Received" to "Closed"
11:48:18 04 20 2009	Glob: Close NSK motive incidents after routing externally

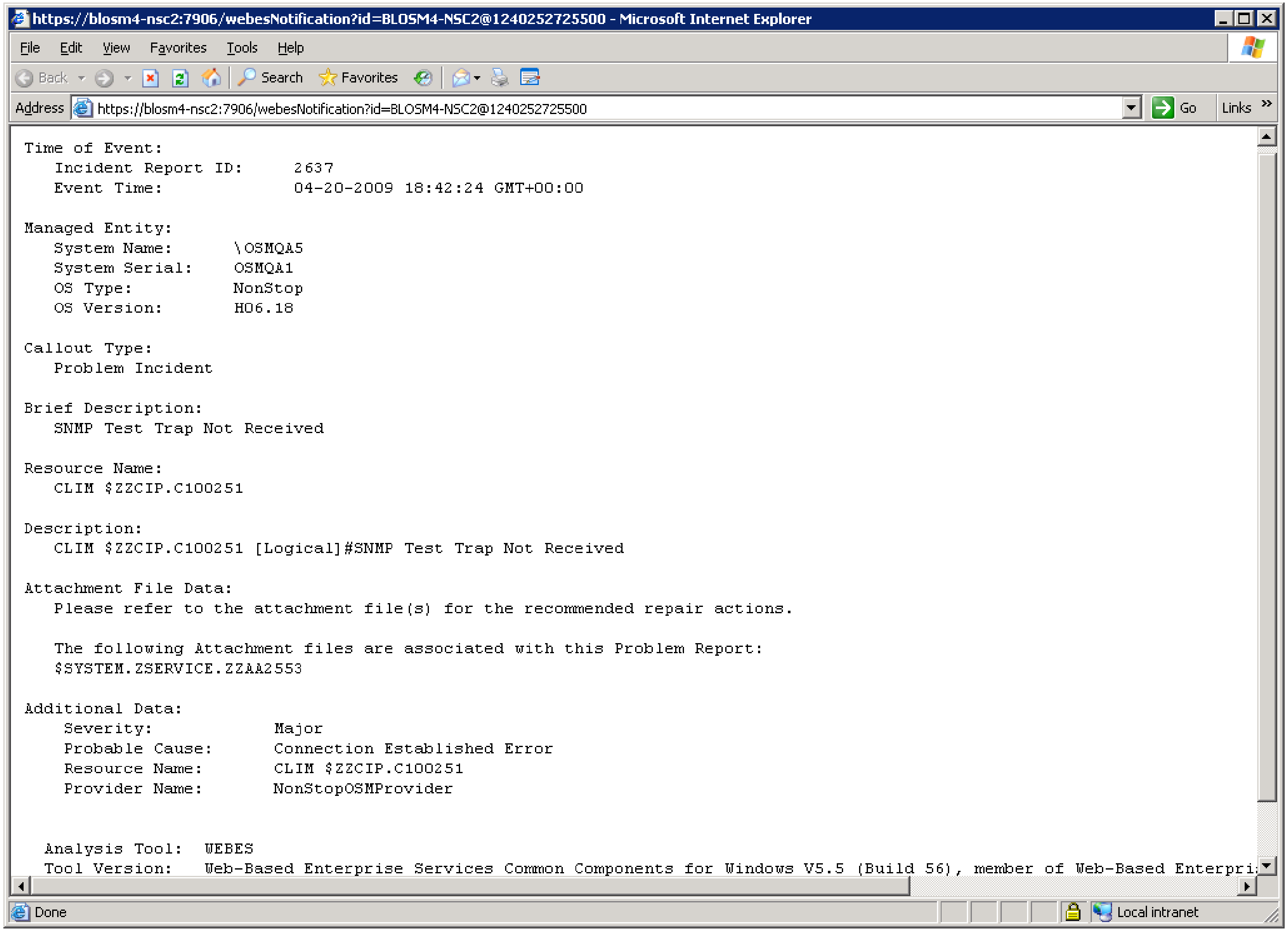
Download Event Files:

event xml

Download Attachment Files:

ZZAA2553

Problem incident analysis report



https://blosm4-nsc2:7906/webesNotification?id=BLOSM4-NSC2@1240252725500 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://blosm4-nsc2:7906/webesNotification?id=BLOSM4-NSC2@1240252725500
Go Links
Done
Local intranet

```
Time of Event:
   Incident Report ID:     2637
   Event Time:             04-20-2009 18:42:24 GMT+00:00

Managed Entity:
   System Name:      \OSMQA5
   System Serial:    OSMQA1
   OS Type:          NonStop
   OS Version:       H06.18

Callout Type:
   Problem Incident

Brief Description:
   SNMP Test Trap Not Received

Resource Name:
   CLIM $ZZCIP.C100251

Description:
   CLIM $ZZCIP.C100251 [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.ZZAA2553

Additional Data:
    Severity:             Major
    Probable Cause:       Connection Established Error
    Resource Name:        CLIM $ZZCIP.C100251
    Provider Name:        NonStopOSMProvider


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