

Automated Remote Support Security With TSM or OSM on the HP NonStop™ S-Series and NS-Series

Introduction

Automated Remote Support is a service offered as a part of standard warranty and basic service agreements that help ensure the optimal performance and availability of HP NonStop™ Servers.

Automated Remote Support (ARS):

- Continuously monitors system hardware and software
- Proactively identifies problems which may lead to outages
- Automatically reports problems to the service provider, usually the HP Global Mission Critical Solution Centre (GMCSC)
- Speeds resolution through secure remote diagnosis and expert support

Automated Remote Support is implemented on NonStop™ S-Series and NS-Series servers using either TSM (Total System Management) or OSM (Open System Management), along with an integrated set of Microsoft Windows clients and NSK-based server applications running in a private LAN environment. (NSK is the NonStop Kernel Operating System.)

This paper focuses on the multiple levels of security built into TSM and OSM and the Automated Remote

Support service that enable remote sessions while protecting system security.

In this document, the term NSK security is used to indicate that NSK security is presented with a username and password, and NSK security functions determine whether the user is recognized. HP Safeguard, an additional security product, is NOT required, but if it is in use, NSK security will work with it.

For information on K-Series implementation of Automated Remote Support and related security measures, please see Appendix A.

General Remote Support Architecture

Automated Remote Support can be configured for automatic notification and/or remote access:

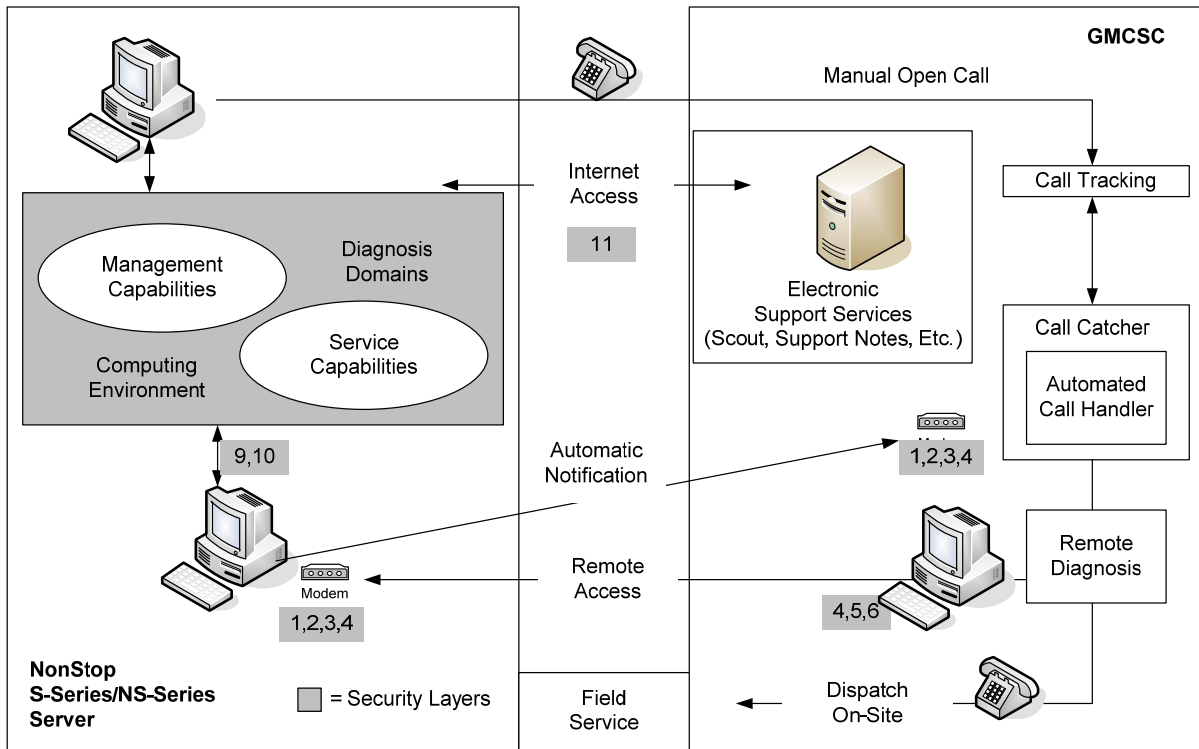
- **Automatic notification (dial-out)** allows TSM or OSM to notify the GMCSC of pending hardware and software problems
- **Remote access (dial-in)** allows the GMCSC to dial into the NonStop™ S-Series or NS-Series server to diagnose hardware or software problems

Implementing Automated Remote Support requires a number of hardware and software components both at your site and at the GMCSC. The components are:

- A NonStop™ S-Series or NS-Series server running the NSK TSM or OSM Server
 - A local S-Series or NS-Series System Console (NSC Console) connected to your NonStop™ S-Series or NS-Series server(s) via a private LAN for modem-based dial-in and dial-out and internet event forwarding*
 - Remote support at the GMCSC to receive automatic notification of problems (dial-out), and when required and authorized, to conduct remote access (dial-in) diagnostic sessions
- * - ISEE is detailed later in the document.

The figure below depicts the remote support environment and highlights (in green boxes) the layers of security controls:

1. Physical (turn-off, password)
2. Communications (proper modem, proper protocol)
3. Windows NT workstation remote user access permission (requires configuring a user to allow remote access)
4. Windows NT username/password
5. Microsoft NetMeeting
6. NSK configuration and control
7. NSK operating system access
8. NSK operating system password
9. Registration/Secure UserID/Password



Automated Remote Support Environment and Security Levels

Remote support access is isolated by the NSC Console, which Serves as a firewall. There is no direct access to the NonStop™ S-Series or NS-Series server. Multiple S-Series or NS-Series servers can be managed by a single NSC Console, providing a single point of secure access for remote support.

Automated Notification Process and Security

A. Automatic Notification Overview

In the event of a problem, TSM or OSM on the NonStop™ S-Series or NS-Series server sends a problem report to the NSC Console, which can authorize, initiate connection, and send the problem report to the GMSCS. The system manager chooses whether to allow automatic notification or not.

If automatic notification for a category of Incident Reports (IRs) is enabled, IRs in that category will be sent. If automatic notification is not authorized, each notification must be actively authorized by the system manager. Connection fault tolerance requires two NSC Consoles — one configured as the primary notification point and the other configured as the backup. Automatic notification

can also be configured independently from remote access.

The system manager has complete control over the reporting of problems. Using the NSC Console, the manager can view the problem report and selectively authorize or reject the sending of any of the data associated with the problem report. These automatic notification configurations are made per system, not globally, for all of the systems reporting through the NSC Console. (The configuration information is kept on each individual system, so the same rules apply to both the primary and backup notification points. The default configuration is that all IRs require authorization; that is, no automatic notification is enabled). TSM or OSM on the NonStop™ S-Series or NS-Series server(s) forwards problem reports to the NSC Console client via a private LAN. Since there is no modem on the S-Series server or NS-Series, there is no direct access to servers other than via the LAN. The NSC Console is the focus for security access to the NonStop™ S-Series and NS-Series server(s).

Only TSM or OSM service data is sent to the GMSCS. The system manager can view and selectively authorize data that is reported. The manager can choose to:

HP NonStop S-Series and NS-Series Server Automated Remote Support

1. Actively authorize each notification
2. Automatically authorize reporting of all IRs without user intervention
3. Choose, by IR type, which ones are to be automatically reported and which require pre-authorization

The notification is over a PPP (Point-to-Point Protocol) connection. The GMCSC system receiving the notifications is accessible only to GMCSC personnel and is separated by a firewall from other HP networks.

B. TSM or OSM Components

TSM or OSM is available only on NonStop™ S-Series and NS-Series servers and is an integrated set of client/server applications running in a LAN environment. The applications use various protocols and communications methods depending upon the user access level.

- The TSM or OSM environment is made up of four client applications:
- The Service Connection Application (SC)
- The Low-Level Link Application (LLL)
- The Notification Director Application (ND)
- The EMS Event Viewer Application (EV)

C. The Service Connection Application Security

The TSM and OSM applications use TCP/IP for monitoring and control and FTP (File Transfer Protocol) for copying notification attachments from the NonStop™ S-Series or NS-Series server to the NSC Console. The TSM or OSM applications use NSK security for both of these functions.

1. Connection

The user is presented with a "Connect" dialog and log in, requiring a username and password. The username and password must have previously been established with NSK on the NonStop™ S-Series or NS-Series server. The username and password are encoded and passed along in application layer protocol requests.

2. Access

The Service Connection (SC) application is client software that runs on the NSC Console workstation to provide operations control of the NSK server. All operations access from the client software to the NonStop™ S-Series or NS-Series server requires NSK security. This can be categorized into two areas; general monitoring access (including discovery of the server components) and actions. General monitoring

access requires NSK security, but not a SUPER group logon. Monitoring access to the TSM or OSM server is used for discovery and informational access as well as for non-sensitive actions. Discovery and information requests gather information from the server but do not affect any of the resources on the system. In addition, there are some actions that do not affect resources on the system but provide useful information or interaction with the system.

The non-sensitive actions are "CRU Responsive Test" actions (known colloquially as "ping" actions), the System Session Responsive Test, and Notification Director Actions ("Get Pending Incident Reports" and "Generate Periodic Incident Report").

Actions, other than those covered above, require a SUPER group NSK logon. This includes powering on or powering off a disk, upping or downing a disk, running a "Test Verify" on any resource, resetting a CPU, resetting an SP, etc.

Controlling access to the server by providing usernames and passwords is entirely within the purview of the system manager. By monitoring access, the manager can see all resources in a system, the state of those resources, information about those resources (serial number, part number, tracking ID, revision level, firmware revision, etc.). Using action access with a SUPER group logon, the manager can control and modify the resources of the system.

In the private service LAN environment, security entails physical access to the NSC Console and allocation of NSK logons. Both of these aspects are totally within the system manager's control.

The Low-Level Link (LLL) runs on the NSC Console workstation to provide service control of the NSK server, either by the GMCSC or on-site service provider staff. All service access from the client software to the NonStop™ S-Series server requires Service Processor (SP) security. The NS-Series server requires Maintenance Entity (ME) security.

3. FTP

FTP is used to move attachments to Incident Reports (IRs). IRs are handled by the Notification Director (ND). If an attachment list is contained in a notification received by the NSC Console, the files in that attachment list are copied to the NSC Console. The user may then view the attachments, based on the type of the file. NSK security is used for the FTP session.

D. NSC Console Access and Notification Destinations

The ND application receives, displays, and allows you to take action on Incident Reports. It also allows you to configure remote access and automatic notification information, including sending Incident Reports to the service provider automatically.

The system manager determines which NSC Consoles will be used with a particular NonStop™ S-Series or NS-Series server for remote access and automatic notification. Configuration screens are provided in the ND application to establish this.

- The *destination workstation* is one to which TSM application notifications will be sent
- A *primary workstation* and a backup workstation are used for notification of Incident Reports.

Once the system manager has configured the NSC Consoles, there is no other security required at this level. Notifications will only be sent to the designated NSC Consoles; they are not broadcast.

Note that systems are shipped with manufacturing supplied IP addresses on both the NonStop™ S-Series and NS-Series server(s) (for the NSK service LAN and the SP or ME) and the NSC Console. The system will work out-of-the-box if a private service LAN is set up, including just one NonStop™ S-Series or NS-Series server and a single NSC Console. This allows for initial setup and confirmation that the system is running. The NSC Console and the server can either be left with the manufacturing-defined IP addresses or merged into your private service LAN environment. Changing of the IP addresses is required if:

- A second backup NSC Console is to be set up for use with one or more HP NonStop™ S-Series or NS-Series servers, or
- A second (or more) HP NonStop server is to be added to the private service LAN utilizing the same primary (and/or backup) NSC Console.

The configuration of IP addresses is entirely at the discretion of the system manager. However, the service LAN based on the Ethernet ports on the two Processor Multifunction CRUs of group 1 (in slots 50 and 55) on S-Series servers or P-switches on NS-Series servers must be kept in the same subnet.

E. Notification Director Application Security

The Notification Director (ND) handles all of the processing for Incident Reports (IR). When an IR is authorized (either manually or automatically), and if there is an attachment list, the ND uses FTP to copy all files in the attachment list from the NonStop™ S-Series or NS-Series server. In addition, the ND writes pertinent information regarding the delivery of the IR back to the NonStop™ S-Series or NS-Series server. This includes authorization, notification, and confirmation information.

The ND, at the primary and backup NSC Consoles, must be running at all times to provide for delivery of IRs. The user must log into the ND when it is started and enter an NSK user-name and password. This NSK logon will be used to ensure NSK security whenever an IR arrives. In all cases, the user names and passwords the ND needs are encrypted and stored on the client.

The actions used to write back information about the delivery of the IR are done using the NSK username and password entered for that system in the ND. This NSK username and password does not need to be a member of the SUPER group. NSK security will operate the same as for the Service Connection Application.

F. Secure Sockets Layer (SSL) Security

With G06.27, Secure Sockets Layer (SSL) was introduced in OSM.

SSL provides secure communication between the OSM server and OSM client applications, such as OSM Service Connection and OSM Notification Director.

With SSL enabled, all the data communication between OSM server and OSM clients is encrypted.

SSL also allows the OSM server to communicate with HP Systems Insight Manager (SIM) product over a secure connection

G. Service Processor/Maintenance Entity Security

The security for the SP/ME sessions are provided by an RPC session, which is established between the application on the NSC Console and the Service Processor/Maintenance Entity on the NonStop™ Himalaya S-Series/NS-Series server. A username and password are provided in a Connect dialog. This is not NSK security, but

shared security which both MSPs/ME's (Master Service Processors/Maintenance Entities) provide. Up to eighteen usernames and passwords can be configured for the SP.

H. EMS Event Viewer Security

The EMS Event Viewer (EV) can be launched from the SC application. The username and password entered in any previous Connect dialog of the SC application are not passed to the EV when it is launched. The username and password will need to be re-entered. The username and password is then used to set up a session with the event distribution software on the NonStop™ S-Series/NS-Series server. . If the EV is invoked from the desktop, the NSK username and password is required.

Remote Access Process and Security

On a NonStop™ S-Series/NS-Series Server, there are two support access points: the NSK operating system and the Service Processor/Maintenance Entity. Remote access for both access points is via the NSC Console and configured and controlled by the system manager.

When the GMCSC needs remote access to diagnose a hardware or software problem, a connection is made from the GMCSC into the NSC Console. This connection is established using Microsoft NetMeeting, a Microsoft software product designed for remote service access.

A. NT Security

The first level of remote access security is NT security. NT RAS (Remote Access Service) must be configured before remote access can occur. Beyond RAS, the NT user must be allowed to operate over a remote connection. If this configuration is not done, the connection will fail, even if the correct username and password are used. (The default NT user is not given remote access. The system manager must use the NT User Manager application to enable remote login by the GMCSC user.)

B. NetMeeting Security

Once a connection to the NT system is established using RAS, a connection to the Microsoft NetMeeting software must be established. This can only happen if the NetMeeting application is already running on the NSC Console. NetMeeting relies on the NT RAS security username (must be part of the administrators group) and password that must be entered before any connection to a NonStop™ S-Series or NS-Series server can be attempted. The system manager controls the assignment of

the NT RAS username and password. All remote communications over NetMeeting are encrypted.

C. NSK Server Security

The third level of security is NSK security. Once the connection is made, the GMCSC starts the SC application and runs a Connect dialog specifying the IP address of the customer's NonStop™ S-Series or NS-Series server. Because the NonStop™ S-Series or NS-Series server IP addresses are not part of the RAS PPP address pool, starting SC without going through NetMeeting will not allow any LAN access to the NonStop™ S-Series or NS-Series server.

D. Session Security

Once a connection is established and TSM or OSM applications are run on the NSC Console, the same security mechanisms discussed above apply for NSK security, RPC sessions, and FTP sessions. The NSK TSM or OSM Server utilizes NSK security, requiring an NSK logon for access. The Service Processor/ME provides the username and password security.

E. Audit Trail

There are two kinds of audit provided by TSM/OSM.

The Low-Level Link provides the ability to show the set of active sessions as reported by the SP or ME. This is provided through the Sessions menu item in the Display menu after System Discovery has completed. This display shows all active LAN RPC sessions with the SP or ME from any NSC Console.

An audit trail of Service Connection operation is maintained on NSK in the ZSERVICE.ZZUSERS file. The following occurrences will be logged in that file:

- Any validation of NSK security,
- An Authorization Failure, where the NSK username and password fail to validate, and
- An action on any object.

When the ZZUSERS file becomes full (500 entries), it is renamed to \$ZSERVICE.ZZUSERS2 file and the ZZUSERS file is started anew.

F. Access and Security Precautions

TSM or OSM provides two levels of access: monitoring access and action access. The level of access is governed by the NSK logon provided by the system manager.

Monitoring access allows a user to see what is on a system, information about the resources on a system, the state of the resources on a system,

HP NonStop S-Series and NS-Series Server Automated Remote Support

and the alarms (if any) on a system. However, with monitoring access, a user cannot perform operations on a system that will affect the resources on that system (short of physically pulling a CRU on a system). Monitoring access is provided with any valid NSK logon.

Actions access allows a user to perform operations on a system which may affect the performance or availability of that system. A user could replace a CRU, upgrade firmware, test or verify resources, or clear a disk. Actions access requires a SUPER group logon.

Although remote support has security features, the system manager must configure and manage the security environment. The system manager has total control over the configuration and deployment of modems and the security of those modems. Remote support uses NSK security and does not impose requirements for particular logon IDs or passwords specifically for support, although actions access requires a SUPER group logon. The system manager should manage NSK security normally in terms of usernames and passwords. SUPER.SUPER and SUPER.CE are available by default, but the manager may remove or change these as well. You are advised to change the Service Processor and NetMeeting passwords periodically and notify the GMSC of the change. Do not let unauthorized personnel have access to passwords.

ISEE

HP Instant Support Enterprise Edition (ISEE) is a proactive, web-based, remote monitoring and diagnostic tool that helps manage your systems and devices. ISEE provides continuous hardware event monitoring and automated notification to identify and prevent potential critical problems.

The ISEE architecture incorporates a number of security technologies to protect your network and support data. Strong encryption, authentication, and industry-standard security protocols and best practices are integrated at the physical, operational, network, and application levels of the ISEE architecture, providing a multi-level, layered security structure.

For NonStop installations, the ISEE client is installed on your NonStop System Console (NSC) and works with HP NonStop Open System Management (OSM) software to monitor your NonStop servers and forward vital system information to HP support. ISEE will only work with OSM and will **not** work with TSM.

With ISEE installed and selected on the NonStop Console, events are routed through an internet connection to HP services rather than utilizing the current modem dial out capability.

Requirements

Hardware

In addition to the standard NSC hardware requirements, a second LAN connection is required to implement ISEE. One for connecting to the NonStop system via the dedicated service LAN as in use today, and a second to provide the ISEE internet connectivity via the customers secure operations LAN. System consoles shipped by HP today will include two NICs. For system consoles without a built-in second NIC, a USB Ethernet adapter cable can be used to provide this ISEE connectivity.

Software

Your system console must meet the following minimum requirements in order to utilize ISEE.

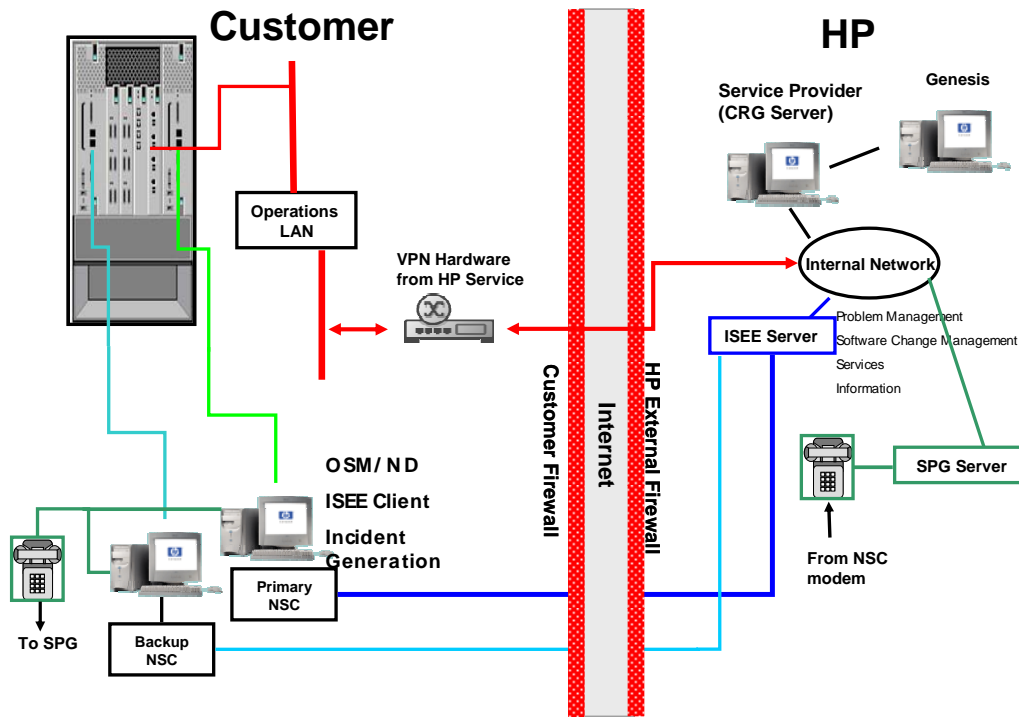
- Windows XP Console with SP1
- Notification Director - T0632 G06 AAK or later release

In addition, T0682 G06 AAC or later release of OSM server software should be installed.

You also need to install the following software on the NSC:

- Windows ISEE Client (A.03.90) - available from the HP software depot – MS Windows ISEE Client A.03.90.880 Feb2005 or later release

Example of ISEE incident management for NonStop Servers



For more information on ISEE, please contact your local account team.

You can also get further information from the following web site:

<http://h20219.www2.hp.com/services/cache/10709-0-0-225-121.aspx>

Appendix A: K-series Implementation

Prior to the NonStop™ Himalaya S-Series and NS-Series, NSK-based systems used TMDS (Tandem Maintenance and Diagnostic System) and SysHealth for service management and sent problem reports to the Global Mission Critical Solution Center (GMSCC) via the Remote Maintenance Interface (RMI) using proprietary protocols.

TMDS and SysHealth are point products which run on the NonStop™ Himalaya K-Series server using a block mode user interface. Since these applications were run in a TAEL environment, security was NSK security.

For more information about Automated Remote Support

In the U.S., call 1-800-255-5010
Or call your country's Global Mission Critical Solution Center listed at
<http://h71014.www7.hp.com/GMCSCphone.html>

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States and/or other countries. All other product names mentioned herein may be trademarks or registered trademarks of their respective companies.

HP Services shall not be liable for technical or editorial errors or omissions contained here in. The information in this document is subject to change without notice.