



Carrier VoIP

ATM/IP Solution-level Security and Administration

Document status: Standard
Document version: 04.04
Document date: 20 October 2006

Copyright © 2006, Nortel Networks
All Rights Reserved.

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.

ATM/IP Solution-level Security and Administration

ATTENTION

This document addresses all Nortel CVoIP solutions. Some statements may not apply to your solution.

New in this release

(I)SN09U is an extension of the (I)SN09 software release and supersedes both (I)SN09 and (I)SN09FF for CVoIP applications. (I)SN09 continues to be supported for TDM-only applications. The (I)SN09U software release incorporates all capabilities of (I)SN09, (I)SN09FF, and additional corrective content delivered as part of Nortel's (I)SN09 software robustness program. (I)SN09, (I)SN09FF, and (I)SN09U are valid terms for use within the (I)SN09U software release.

The following table highlights the features introduced in this release. Refer to the OSS Advanced Feature Guide for more information about new features in this release.

Note: The terms Passport and PVG have been re-branded in conjunction with the new Nortel brand simplified format. Passport is now referred to as the Nortel Multiservice Switch and PVG is now Media Gateway 7480/15000.

(I)SN09U ATM/IP features

Feature descriptions

Public Key Manager

Public Key manager provides centralized certificate management and tracking for all networks elements in Nortel solutions

Pass Phrase Protected Keys for SSH (IAW, IAC, PT-IP, UA-IP, ATM)

Feature descriptions

This feature enhances the existing secure outbound file transfer functionality by introducing the key-based (public key) authentication. The key-based authentication mechanism is provided as an additional option for the user. Hence, the user can select to use either the password-based or the key-based authentication while adding and changing the secure file transfer schedules in the SBA (billmtc) or OMDD (omui) user interface programs. The actual configuration details are documented in the configuration section.

Gateway Controller features

RMGC Security

The RMGC Security feature will enable secure communications between the RMGC (or RMGC/Audio Controller) and the Multimedia Terminal Adaptor (MTA)..

Support for SCTP Security on GWC

This feature enables IPSec on the GWC for the SCTP protocol using ESP transport mode and using IKE with preshared key for key negotiation.

MG 9000 features

MG9KEM SN09.1 CPR Robustness (UA-AAL1, UA-IP)

This feature will be supported for all the types of NEs present in subnet (e.g. discovered and undiscovered).

MG9K PKI Development (UA-IP)

This feature calls for using some functions of Public Key Infrastructure (PKI) to manage the generation and distribution of keys used to authenticate nodes participating in an IPSec session.

Integrated Element Management System (IEMS) features

IEMS - MS20X0 IPSEC CONFIGURATION SUPPORT (UA-IP)

This feature adds IPSec and IKE configuration capabilities to the MS 2000 node configuration tool. This will allow the craftsperson to enable IPSec for secure messaging between the IEMS and MS 2000 as well as configure the IPSec and IKE parameters necessary for the MS 2000 to securely send and receive messages to and from the GWC.

SPFS features

Disabling Non-secure Network Services in SPFS

This activity provides some configuration tools to assist customer in configuring the server based on their security policy. Upon completion of the fresh system installation or upgrade, the customer (security administrator) has the possibility to apply the security policy on the server via a command line interface.

Solutions

This document describes security and administration for the following solutions.

Solution name	
International IP solutions	Integrated Access Wireline (IAW)
	Integrated Access-Cable Media (IAC)
	Packet Transit-IP (PT-IP)
	Universal Access-IP (UA-IP)
International ATM solutions	Packet Transit-AAL2 (PT-AAL2)
North American IP solutions	Packet Trunking-IP (PT-IP) or Packet Trunking-AAL2 (PT-AAL2)
	Integrated Access-Cable Media (IAC)
	Universal Access-IP (UA-IP)
North American ATM solutions (see Note)	Universal Packet Access (UA-AAL1) Packet Trunking-AAL1 (PT-AAL1) There are three distinct architectures supported within the PT-AAL1 solution: • Packet Trunking-AAL1 (PT-AAL1) • Packet Trunking on XA-Core (PT-XA Core) • Packet Trunking on SN70EM (PT-SN70)
Note: Collectively, these two Succession solutions are referred to as ATM solutions.	

Overview of Security Architecture

The network security architecture for the CVoIP solutions uses Internet Protocol Security (IPSec) to protect the traffic between several network devices. This section describes some basic concepts related to the IPSec services used in the network.

Note: For more detailed IPSec information, refer to the appropriate Internet Engineering Task Force (IETF) RFC documentation, which can be found at <http://www.ietf.org>.

IPSec services

IPSec offers a set of security services that provide data integrity, authentication, and confidentiality (encryption). These services are provided through the use of traffic security protocols. In this solution only the ESP (Encapsulating Security Payload) traffic security protocol is supported.

Security associations

IPSec services are defined and executed through security associations (SA). An SA is a one-way relationship between two secure network elements. The SA is negotiated and it describes how two network components will use IPSec to communicate securely. To create bi-directional communication between the two network elements, two IPSec SAs must be created (one in each direction). SAs specify security parameters, such as, the IPSec protocol (ESP), the authentication and encryption algorithm, the keys, the lifetime of the keys and the lifetime of the SA.

Supported paths

IPSec is used to secure the following network paths:

- The Public Key manager provides centralized certificate management and tracking for all networks elements in the Nortel solution. The Public Key manager automates the management and replacement of device certificates for supported devices. In addition to this, a Web interface (PKGUI) is available to authorized users to perform a variety of manual actions. This GUI can be launched independently from a web browser or from within the IEMS client window. A new application managed object is added to IEMS to allow single sign-on launching and alarm integration for the Public Key manager with IEMS
- Gateway Controllers (GWCs) to a Cable Modem Termination System (CMTS), third-party Trunk Gateway Control Protocol (TGCP) gateways, or a Multimedia Terminal Adapter (MTA) line gateway (IAC solutions only)
- Media Gateway 9000 (MG 9000) to MG 9000 Manager and GWCs (UA-IP solutions only)

Note: Secure File Transfer Protocol (SFTP) or IPSec secures the FTP client on the MG 9000. IPSec also secures basic packet filtering on the MG 9000.

- Media Gateway 7400/15000 or Multiservice Switch 15000 to MDM devices and GWCs (PT-IP and UA-IP solutions only)
- MDM devices to MDM devices (PT-IP and UA-IP solutions only)

Note: SSH also secures the interface between two MDM devices. In addition, SSH provides the following functionality:

- secures the interface between MDM and IEMS
- provides a secure, one-hop interface between the IEMS client desktop and MDM
- secures the interface between the IEMS client desktop and Media Gateway 7400/15000 or Multiservice Switch 15000 CLUI access from MDM
- Call processing interfaces to and from the RTP Media Portal

Key management protocols

IPSec SAs are negotiated and established by exchanging security keys using one of the following key management protocols:

- Internet Key Exchange (IKE)

IKE creates an authenticated secure communication channel between two devices. This association is called an IKE SA. IKE then uses this secure association to negotiate IPSec SAs. IKE consists of two phases:

 - Phase 1: a shared secret is negotiated through a Diffie-Hellman key exchange (IKE SA is created)
 - Phase 2: IKE SA is used to negotiate IPSec. Only pre-shared key authentication is supported in the network (digital signature authentication or public key encryption authentication are not currently supported for IKE).
- Kerberos

Kerberos with Public Key support (using the PKINIT extension to the Kerberos IETF standard) is used to exchange keys and authenticate line gateways. MTA authentication process with the GWC requires a PacketCable Key Distribution Center (KDC) server, which grants authentication tickets to the line gateway. These tickets are used to authenticate the line gateway, and to establish a pair of IPSec SAs. The KDC is third-party equipment and must be integrated with the network. For more information on Kerberos

with PKINIT please refer to the packetcable security specification :
<http://www.packetcable.com/specifications>

Security connection policies

Connection policies define which security services will be applied to messages exchanged between two secure nodes in the network (identified by the IP address). Each connection policy associates an IP address (or a range of IP addresses) to one of the following actions:

- **BYPASS:** no IPSec services are applied to packets exchanged between the two nodes.
- **SECURE:** before an SA is established, an incoming packet is discarded, and an outgoing packet triggers key negotiation process (using IKE or Kerberos). When an SA is established, IPSec is applied to all incoming and outgoing packets. Incoming packets are authenticated and decrypted; outgoing packets are authenticated and encrypted before being sent.
- **DISCARD:** all packets are discarded between the two nodes.
- **FLEX:** this type of policy is not secure. The FLEX policy must only be used temporarily during the initial activation or de-activation of IPSec, when some gateways associated with the connection policy operate in a secure mode and some do not. The FLEX policy provides the flexibility of accepting secure and non-secure messages, so IPSec can be activated without a loss of service.

Each connection policy is identified by a policy ID number. The lower this number is, the greater is the priority of the policy.

GID/UID allocation guidelines

The introduction of central authentication capability through Nortel's Security services products brings forth a new complexity in managing the UID and GID values assigned in Posix based systems. It is now possible to create a conflict such that a centrally defined user has the same UID as one or more locally defined users.

For example: Local user 1 has a UID of 200. Local user 2 whose user id is defined in the central authentication system also has a UID of 200. If user 2 logs on to the local system that defines user 1 user account, user 2 will be able to modify user 1 files.

Furthermore, for systems that use Posix Groups the GID that is assigned in the central system can also conflict with local GID assignment, resulting in incorrect privileges being provided to a specific user.

For example: The local system has a group 'administrator' defined with GID 1010. User 1 has an account on the central system with central group 'read-only' defined centrally with GID 1010. When user 1 logs into the local system using his central account he will have 'administrator' privileges.

In order to defeat this issue, the local systems UID and GID allocation cannot conflict with the central authentication servers UID and GID allocations. The following table indicates the ranges that customers may use for assigning UIDs and GIDs both in the central authentication server and on local systems.

	UID Range	GID Range	Notes
Central Authentication and Authorization Servers Ranges			
IEMS Security Server	10001-14000	12101-14000	
CNM Security Server	14001-16000	14001-16000	
W-NMS Security Server	16001-18000	16001-18000	
MDM Security Server	18001-20000	18001-20000	
CDMA	51000-52999	10100-10499	
Other	22001-24000	22001-24000	
Local System Ranges			
Local system	30001-49999	30001-49999	

Network Security

Succession network security uses Succession Communication Server LAN (CS LAN) and subnet (VLAN) and firewalls to provide protection at the network level, component level, and management application level. The CS LAN must be a closed network and all access must be secure and controlled.

This section provides a brief overview of CS LAN and subnet and firewall protection.

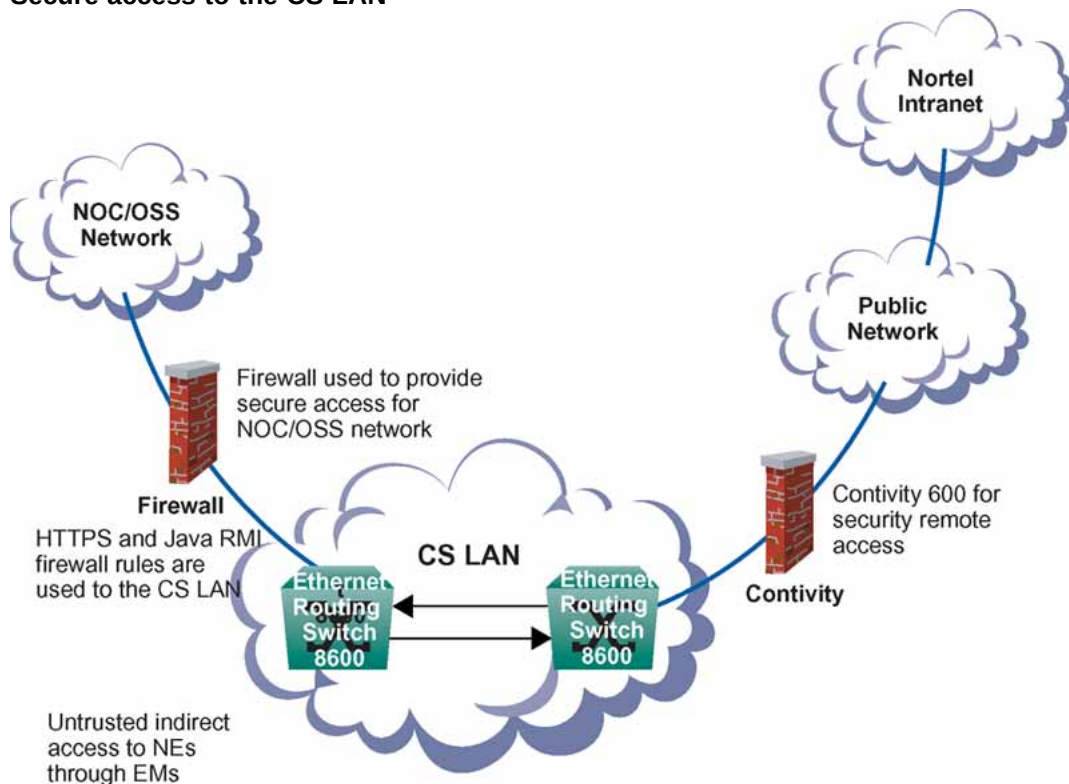
For details, please refer to the following:

- Nortel engineering guidelines for your solution
- ["Technical Publications" \(page 21\)](#)

CS LAN and Subnets (VLANs)

The following figure provides an overview of how firewalls and VPN technology provide secure access to the CS LAN for Network Operations Center (NOC) and Operations Support System (OSS) connectivity and remote field support.

Secure access to the CS LAN



The Communication Server LAN (CS LAN) provides this connectivity as required for those components that are co-located with the CS 2000 complex.

Different message flows are separated into the following subnets (or VLANs) on the CS LAN redundant routers:

- CallIP is used for Call Processing (or Call Signaling) traffic flows
- Bearer is used for RTP bearer traffic flows
- MLT is used for intra-Ethernet Routing Switch 8600 traffic flows
- SP-OAM is used for Service Provider OAM traffic flows (Optional)
- OAM is used for OAM&P traffic flows
- OOB is used for Out of Band OAM traffic flows

Note: The following components are not part of the Packet MSC network: CS 2000 compact, USP-Compact, MG 4000 out-of-band management interface, MG 9000 Server and MG 9000 Mid Tier, and IEMS.

The components that are configured in the Call Processing subnet are as follows:

- XA-Core and/or CS 2000 compact
- CS 2000 SAM21 (GWC and SC)
- SDM Call Processing interface
- SAM16 (UAS) Call Processing interface
- USP Call Processing interface
- USP-Compact
- MG 4000 out-of-band management interface (for UA-AAL1 only)

The components that are configured in the OAM&P messaging subnet are as follows:

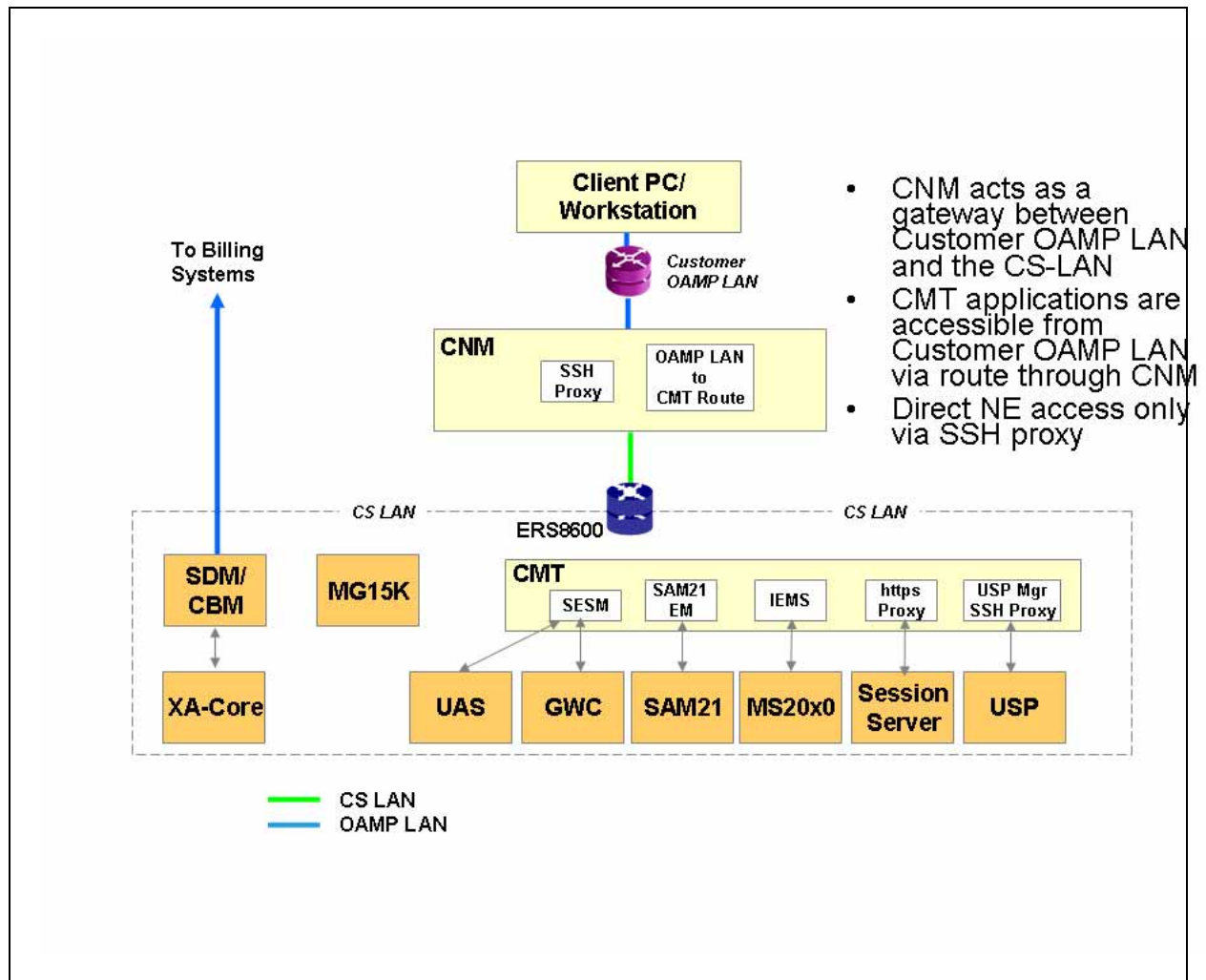
- CS 2000 Management Tools
- SDM Management interfaces
- USP Management interfaces
- USP Manager
- MDM server
- IEMS

The components that are configured in the Bearer subnet are as follows:

- UAS
- Media gateways
- IW-SPM
- MG 9000 (UA-AAL1 only)

CNM as a gateway

Figure 1
CS-LAN isolation



Domain Name Service in the OAM system

CVoIP OAM has required Domain Name Service (DNS) since (i)SN05. DNS resolution must be enabled on the Sun server to allow the security certificates to work, and must be enabled prior to the installation of the certificate. Refer to the procedure for Configuring Domain Name Service in ATM/IP Solution-level Configuration Management, NN10409-500 for more information.

The following element management servers and their clients use the DNS Service for the HTTPS protocol.

- CS 2000 Management components
- Audio Provisioning Server (APS)

- Media Gateway 9000 Manager (MG 9000 Manager)
- Integrated Element Management System (IEMS)

In addition, IEMS uses the DNS Service for client launching. IEMS utilizes HTTPS proxy on SPFS for launching some components.

Firewalls

Firewalls can be deployed as an optional security feature at the CS-LAN or Trunk Gateway sites. However, it is recommended to evaluate carefully the amount of traffic that might traverse a firewall, especially when Media Gateways are present in the location to be protected. This is because the most common firewalls have a Gigabit Ethernet as the highest capacity interface. Unfortunately, the throughput drop is on the order of 50-60 per cent, which can seriously impair performance and traffic engineering. Therefore, unless adequate firewall capacity is proven, it is strongly suggested not to rely on firewalls to protect bearer traffic but use instead traffic filtering on routers.

On the other hand, given the fairly small signaling traffic flows, the Call Processing subnet can be protected by a firewall without significant performance drops. The same can be said for the OAM&P subnet, where, depending on the network topology, a firewall is recommended given the sensitivity of the platforms.

The clients of the CS 2000 Management Tools and CS 2000 MG 9000 Manager are able to communicate with their respective server components through multiple firewalls (facing either the client or the server side) using a minimum number of configurable TCP/IP ports. In addition to allowing communication through the firewall, this functionality also ensures that the data is secure.

For details about firewall port configuration, please refer to the Nortel engineering guidelines for your solution and the CVoIP networks component customer documentation listed in "[Technical Publications](#)" ([page 21](#)).

HTTPS for GUI and HTML-based tools

You will only execute this procedure if you are not using Certificate Manager. If you are using the Certificate Manager, then refer to Nortel CVoIP IPsec Security Service Implementation Guide, NN10453-100.

HTTPS is used for Java GUI launching and HTML-based tools in all CVoIP solutions to secure otherwise unsecure messaging.

In a TCP connection to be secured via SSL, for example, an HTTPS interface, the server side of the connection must have an SSL certificate installed. Before operational communication can start, the certificate presented is validated by the SSL client. If the certificate is validated by the SSL client, further SSL handshake takes place to generate cryptographic keys used to secure the subsequent message exchanges between client and server. Note that standard SSL protocol also supports SSL client authentication. However, SSL client authorization is not used in Nortel CVoIP applications.

Note: To use HTTPS messaging, customers must have an X.509 certificate installed on the web server. If this is not already installed, refer to ["Installing or replacing an HTTPS certificate on an SPFS-based server"](#) (page 641) in this document.

Component Security

Overview

Security and administration options vary between CVoIP components and their managers as described below.

Communication Server 2000 Core Manager

The Communication Server 2000 Core Manager provides security for the CS 2000 Core. Core-managed peripherals including the MG 4000, the IW SPM, and the CS 2000 Core are managed from the CM Privclass interface.

The CS 2000 Core Manager is the Nortel operations, administration, and maintenance (OA&M) processing complex for the CS 2000 core. The CS 2000 Core Manager is an applications environment that allows operating companies to operate, administer, maintain and provision network components and services.

The CS 2000 Core Manager primarily uses Telnet/FTP and SSHlogin/SFTP (simple file transfer protocol) for secure file transfer with the CS 2000 Core.

Optionally, distributed computing environment (DCE) secure servers and Passwerks are available for secure file transfer with the CS 2000 Core. CS 2000 Core Manager provides passthrough only.

Media Gateway, Multiservice Switch and MDM

The Multiservice Data Manager (MDM), Multiservice Switch 15000, Media Gateway 7400/15000, and CS 2000 Communication Server LAN (ERS 8600) provide their own security. The MDM provides passthrough security only. The MDM allows users to manage security for Media Gateway 7400/15000.

Succession Server Platform Foundation Software

The Server Platform Foundation Software (SPFS) provides PAM-based user authentication and group-based user authorization for the management of the CS 2000 Management Tools applications, the MG 9000 Manager, Network Patch Manager, and USP Manager.

- PAM-based user authentication supports different authentication technologies without changing login services. For details about PAM, refer to "[PAM-based user authentication](#)" (page 283).
- Group-based authorization controls which operations a user is authorized to perform.

Integrated Element Management System (IEMS)

IEMS provides a security management engine that supports authentication and authorization of all user operations. IEMS security management offers the following functionality:

- centralized security administration
- use of Pluggable Authentication Module (PAM) for EMS modules
- transparent user login to component user interfaces
- audit trail for user and group accounts

The IEMS acts as a proxy to the central security administration system. Network elements and applications can be configured to use centralized security administration. To enable a device to use centralized security administration, the device must be configured to use the IEMS central security server to authenticate users and access user profile information. Refer to Centralized security administration overview.

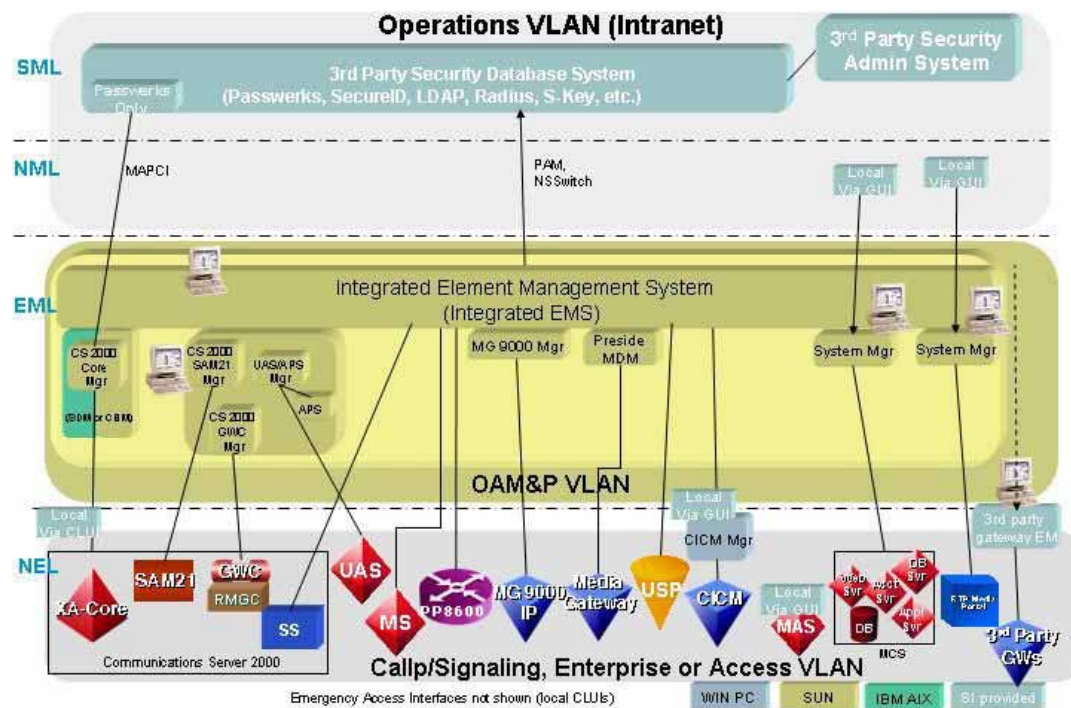
Line gateways

Line gateways are third-party network elements. Security mechanisms for these are vendor-specific. For details, refer to the vendor's documentation.

Security operations architecture

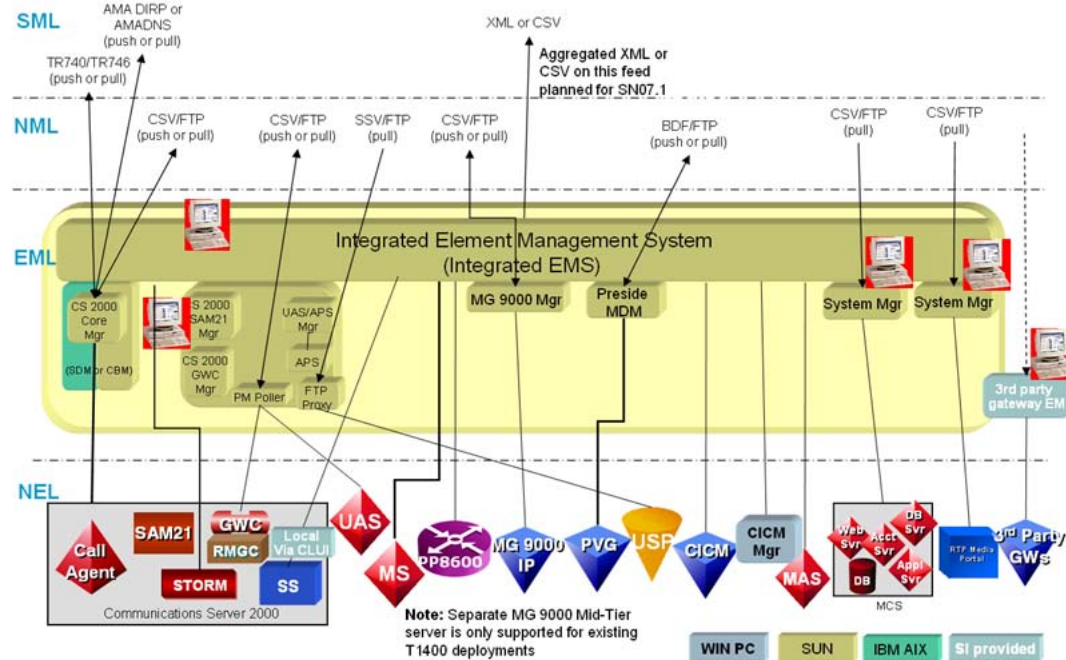
The following figure illustrates the security operations architecture for CS 2000 Server.

Security architecture for the CS 2000 Server (IP solutions)



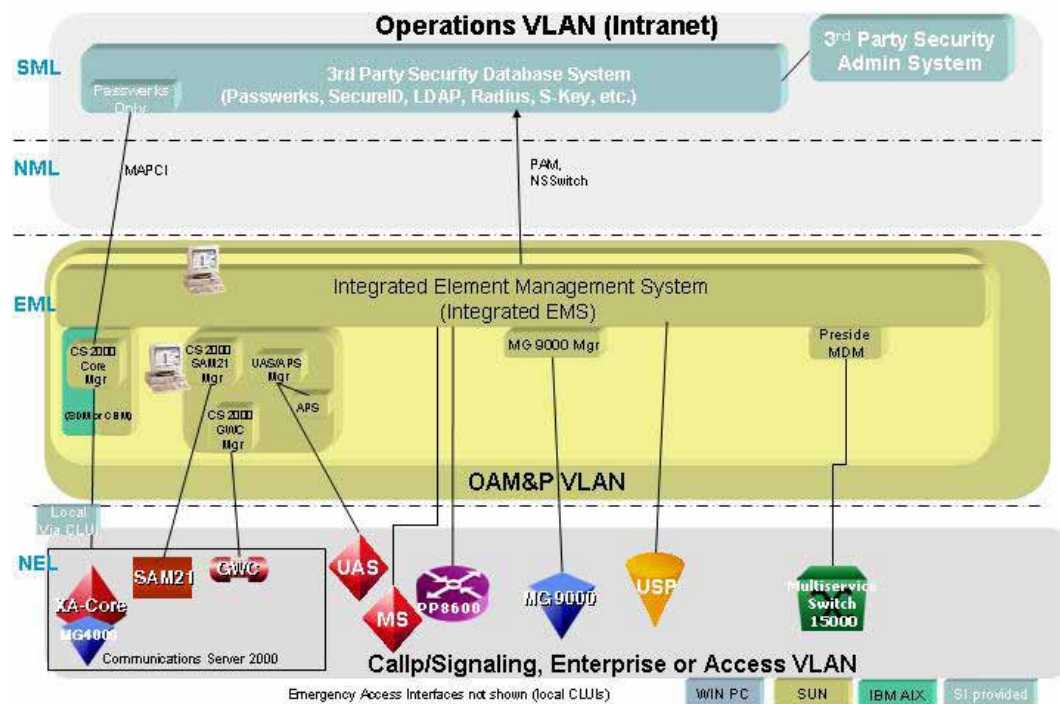
The following figure illustrates the security operations architecture for CS 2000 Server - Compact.

Security architecture for the CS 2000 Server - Compact (IP solutions)



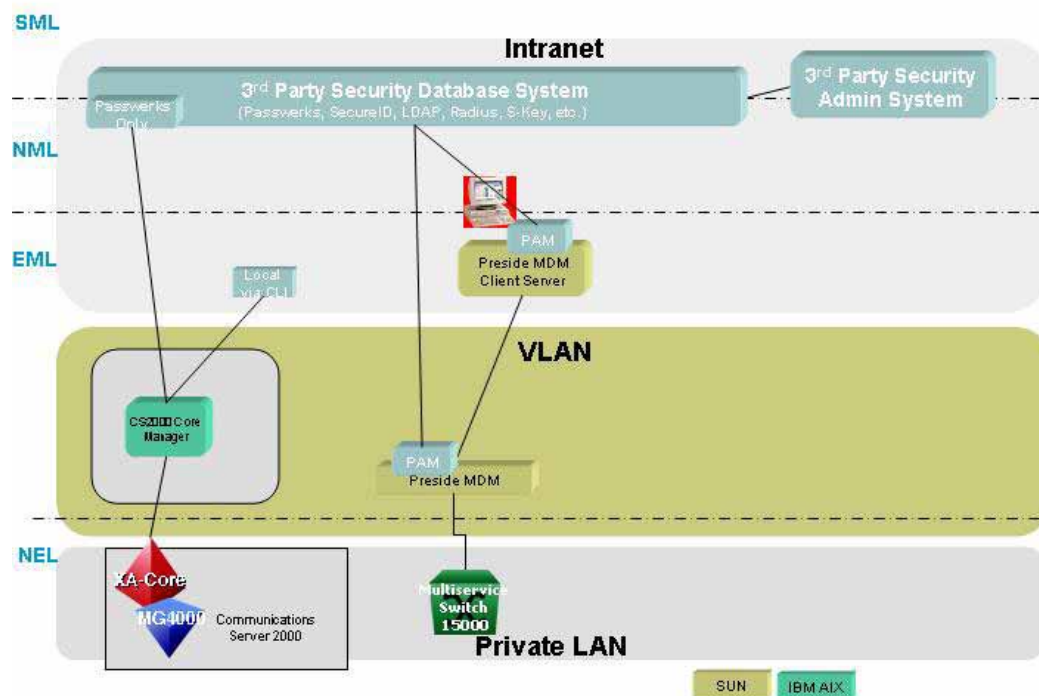
The following figure illustrates the security operations architecture for CS 2000 Server (UA-AAL1).

Security architecture for the CS 2000 Server (UA-AAL1)



The following figure illustrates the security operations architecture for CS 2000 Server (PT-AAL1).

Security architecture for the CS 2000 Server (PT-AAL1)



PT-XA Core or PT-SN70 solutions

If your switch is equipped with a CS 2000 Core Manager, it can provide security and administration management for the DMS-related and SPM-related equipment on the PT-XA Core or PT-SN70 switch. However, if your switch is not equipped with a CS 2000 Core Manager, the XA-Core (or SN70EM) and MAP provide security and administration management. Please refer to the previous section for details about secure file transfer.

Technical Publications

For detailed information about Succession Network Security and Administration, see the following Nortel technical publications (NTPs):

Nortel Network Security and System Administration technical publications

NTP serial number	Title
None	Please consult the Succession Network engineering guidelines documents for your solution. Contact your Nortel account manager for details.
NN10159-611	<i>USP Security and Administration</i>
NN10160-611	<i>USPc (compact) Security and Administration</i>

NTP serial number	Title
NN10161-611	<i>Universal Audio Server Security and Administration</i>
NN10162-611	<i>MG 9000 Security and Administration</i>
NN10163-611	<i>Spectrum Peripheral Module Security and Administration</i>
NN10164-611	<i>MG 4000 Security and Administration</i>
NN10165-611	<i>Interworking Spectrum Peripheral Module (ATM) Security and Administration</i>
NN10166-611	<i>Interworking Spectrum Peripheral Module (IP) Security and Administration</i>
NN10167-611	<i>Dynamic Packet Trunking Spectrum Peripheral Module (IP) Security and Administration</i>
NN10168-611	<i>Dynamic Packet Trunking Spectrum Peripheral Module (ATM) Security and Administration</i>
NN10170-611	<i>CS 2000 Core Manager Security and Administration</i>
NN10171-611	<i>Communication Server 2000 Security and Administration</i>
NN10174-611	<i>Succession Communication Server 3000 Security and Administration</i>
NN10175-611	<i>Call Agent Security and Administration</i>
NN10176-611	<i>STORM Security and Administration</i>
NN10177-611	<i>SAM21 Shelf Controller Security and Administration</i>
NN10213-611	<i>Gateway Controller Security and Administration</i>
NN10252-611	<i>CICM Security and Administration</i>
NN10180-611	<i>Nortel Multiservice Switch 15000, Media Gateway 15000 and MDM in CVoIP Networks Security and Administration PT-AAL1/UA-AAL1/UA-IP</i>
NN10275-909	<i>Succession Fault Management Logs Reference</i>
NN10337-611	<i>MS 2000 Series Security and Administration</i>
NN10346-611	<i>Session Server Security and Administration</i>
NN10336-611	<i>IEMS Security and Administration</i>
NN10367-111	<i>RTP Media Portal Basics</i>
NN10453-100	<i>CVoIP IPSec Security Service Implementation Overview</i>

Configuring the network with security

Purpose of this procedure

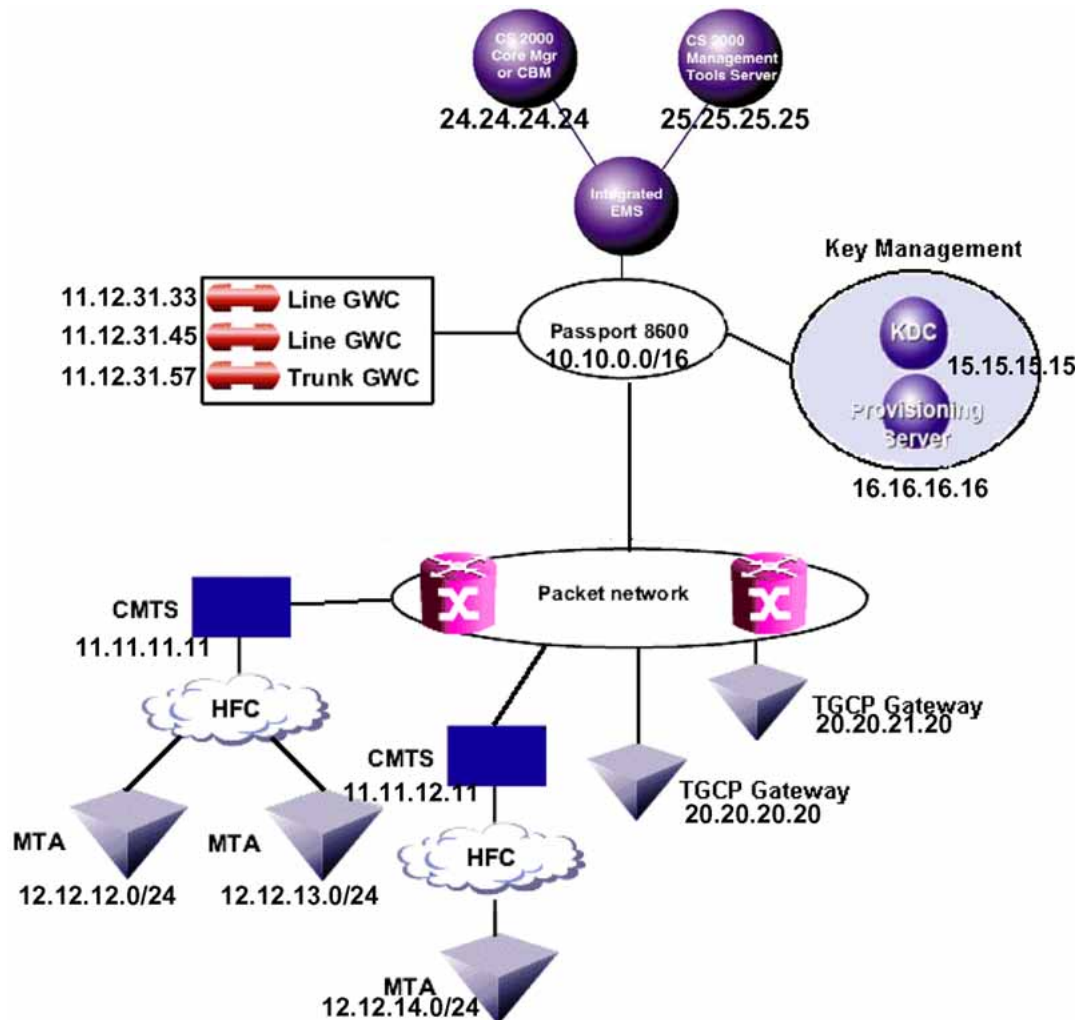
This procedure provides a high-level overview of the steps necessary to configure IP Security (IPSec) for CVoIP solutions.

IAC solutions

The following figure illustrates a sample IAC network and its components that are involved in IPSec.

Note: For simplicity, not all network elements are represented.

Sample IAC network architecture



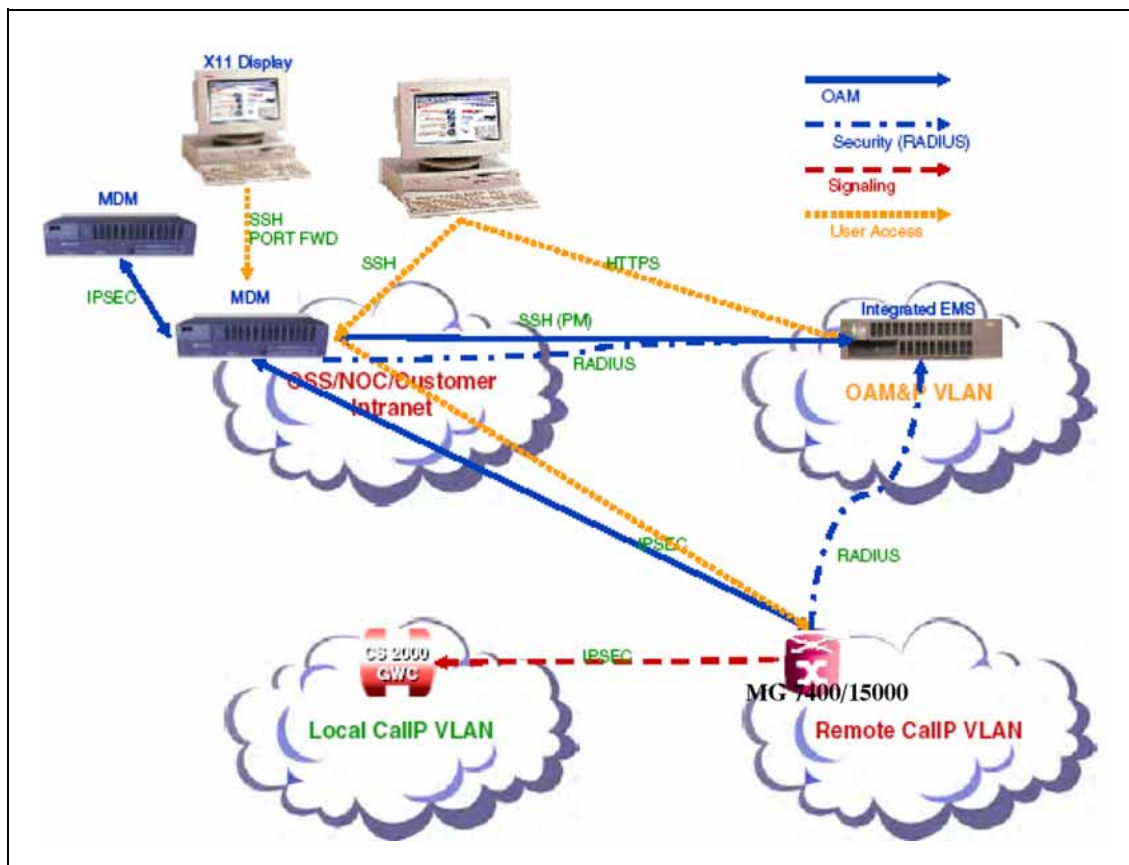
Identify all IP Addresses that need connect to the GWCs shown in the figure above. Populate the IPSEC Security Database using the following procedure.

PT-IP solutions

The following figure shows the security architecture for the Media Gateway 7400/15000.

Note: For simplicity, not all network elements are represented.

Sample PT-IP network architecture

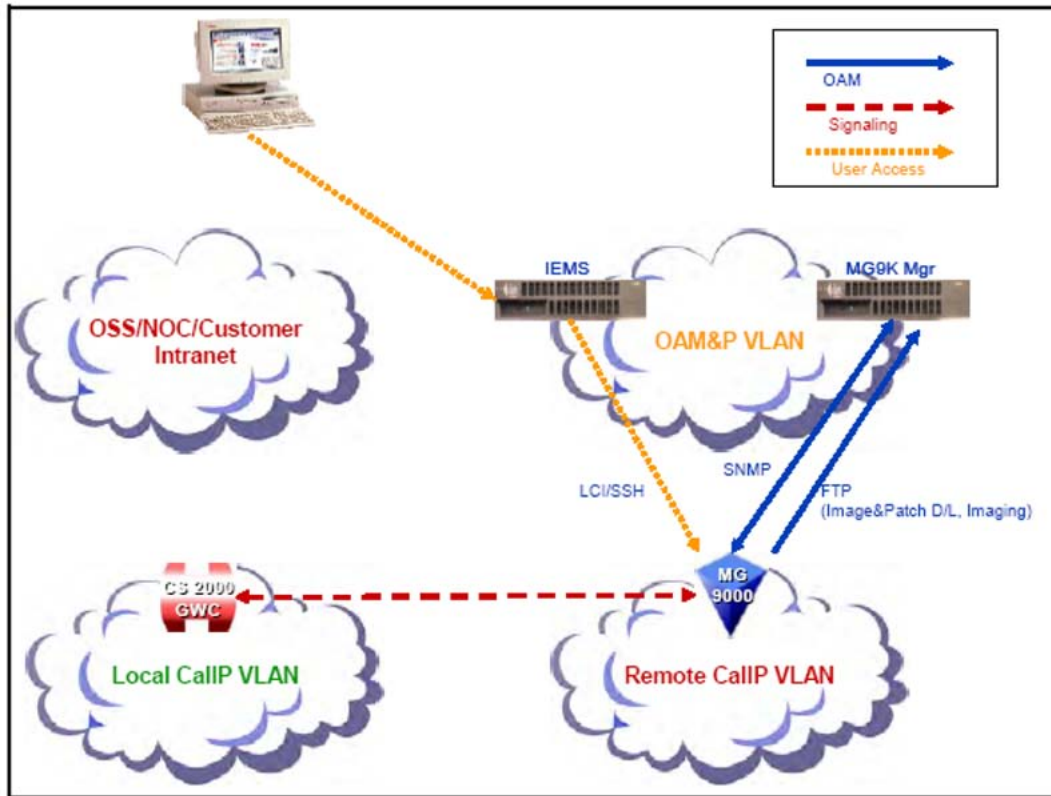


UA-IP solutions

The UA-IP solution supports the same security architecture for the Media Gateway 7400/15000 that is supported by PT-IP solutions. In addition, IPsec is supported for the MG 9000. The following figure shows the security architecture for the MG 9000.

Note: For simplicity, not all network elements are represented.

Sample UA-IP network architecture



When to use this procedure

Use this procedure to create the initial IPsec policy table after the network has been upgraded to (I)SN09.

Prerequisites

The network must be upgraded to (I)SN09.

IPsec has not been configured on any components.

You must have the IP addresses available for each node in the network.

Action

Enabling IPsec in the network

Step	Action

1	Determine your network configuration.

If you are operating a(n)	Do
IAC network	step 2
UA-IP network	step 9
PT-IP network	step 11

2	Configure a blanket DISCARD policy for all IP addresses: 0.0.0.0/1. Refer to the procedure "Configure a DISCARD connection policy" in <i>GWC Security and Administration</i> , NN10213-611.

3	Configure a BYPASS policy for the following IP addresses:

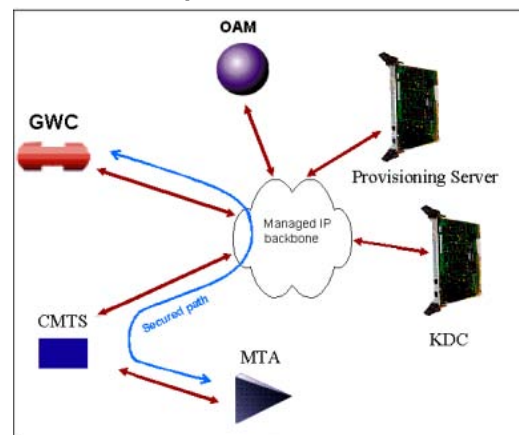
- Range of IP addresses of the ERS 8600 or CS LAN
- CS 2000 Core Manager or Core Billing Manager
- CS 2000 Management Tools server

Refer to procedure "Configure a BYPASS connection policy" in *GWC Security and Administration*, NN10213-611.

4	Configure a Security policy for all network elements which require security.

5	To configure the MTA to Line GWC path for security, perform the following steps.

MTA to GWC path

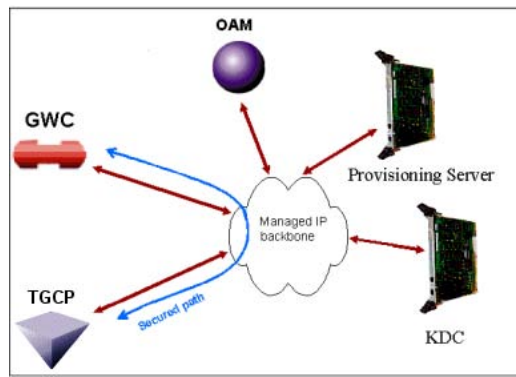


- a. Configure the GWC with Kerberos using the procedure 'Configure Kerberos Key Management' located in *GWC Security and Administration*, NN10213-611.
- b. Activate IPSec with Flex Policies using the procedure 'Activating IPSec using Flex Policies' located in *GWC Security and Administration*, NN10213-611.

Note: Use the 'Configure IPSec SECURE or FLEX connection policy with Kerberos' option in this procedure.

- 6 Secure the path from the TGCP GWs to the Trunk GWC by performing the following steps.

TGCP to GWC path

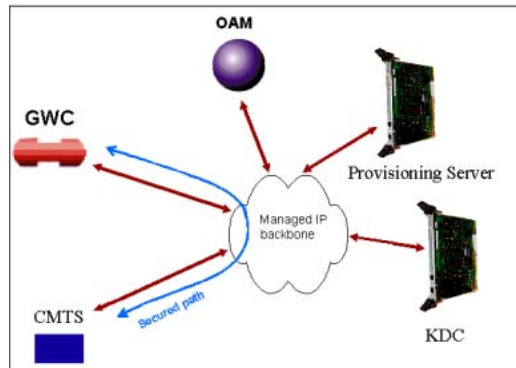


- a. Activate IPSec with Flex Policies using the procedure 'Activate or de-activate IPSec using FLEX policy' located in *GWC Security and Administration*, NN10213-611.

Note: Use the 'Configure IPSec SECURE or FLEX connection policy with IKE' option in this procedure.

- 7 Secure the path from the CMTS to the Line GWC by performing the following steps.

CMTS to GWC path



- a. Activate IPSec with Flex Policies using the procedure 'Activate or de-activate IPSec using FLEX policy' located in *GWC Security and Administration*, NN10213-611.

Note: Use the 'Configure IPSec SECURE or FLEX connection policy with IKE' option in this procedure.

- 8 Go to [step 12](#).
- 9 To secure the path between the MG 9000 and MG 9000 Manager, refer to the procedure "Setting up IPSec in the MG 9000 between the MG 9000 and MG 9000 Manager" in *MG 9000 Security and Administration*, NN10162-511.
- 10 To secure the path between the MG 9000 and the GWC, refer to the procedure 'Setting up IPSec between the MG 9000 and the GWC' in *MG 9000 Security and Administration*, NN10162-511.
- 11 To secure the Media Gateway 15000 or MDM, refer to the following procedures in *MSS 15000, MG 15000 and MDM Security and Administration (PT-AAL1/UA-AAL1/UA-IP)*, NN10180-612:
 - 'Preparing to secure the Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager network elements'
 - 'Using SSH to secure X11 desktop and IEMS connections with the MDM'
 - 'Hardening the Multiservice Data Manager Server platform'
 - 'Securing links between MDM Servers using IPSec'
 - 'Securing links between MDM Servers and MSS/MG15000 switches using IPSec'
 - 'Sending security audit logs from an MDM Server to IEMS'
 - 'Hardening the Multiservice Switch 15000 or Media Gateway 15000 platform'
 - 'Securing user access for the Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager components'
- 12 You have completed this procedure.

—End—

Deactivating Security in the network

Purpose of this procedure

This procedure provides a high-level overview of the steps necessary to deactivate IP Security (IPSec) in CVoIP solutions. This procedure does not disable security on any third-party devices. To deactivate security on third party devices, refer to the security documentation for the device.

Prerequisites

None

Action



CAUTION

Deactivating IPSec in the network will result in a loss of service until security has been deactivated on both network elements.

Step Action

Disabling IPSec in the network

- 1 Determine your network configuration.

If you are operating a(n)	Do
IAC network	step 2
UA-IP network	step 4
PT-IP network	step 6

- 2 Identify all the network elements for which you want to deactivate security. Refer to the procedure 'Activate or de-activate IPSec with FLEX policy' in *GWC Security and Administration*, NN10213-611.
- 3 Go to [step 7](#).
- 4 To remove the secure path between the MG 9000 and MG 9000 Manager, refer to the procedure 'Removing IPSec between the MG 9000 and the MG 9000 Manager' in *MG 9000 Security and Administration*, NN10162-511.

- 5 To remove the secure path between the MG 9000 and the GWC, refer to the procedure 'Removing IPSec between the MG 9000 and the GWC' in *MG 9000 Security and Administration*, NN10162-511.
- 6 To remove security on the Media Gateway 15000 or MDM, refer to procedure 'Disabling security features on Multiservice Switch 15000, Media Gateway 15000, and Multiservice Data Manager components' in *MSS 15000, MG 15000 and MDM Security and Administration*, NN10180-612.
- 7 You have completed this procedure.

—End—

Synchronized Backup Manager overview

Synchronized Backup Manager description

Throughout this document, the backup restore functionality delivered under this feature is referred to in three distinct ways:

- Synchronous Backup Restore Manager (SBRM) refers specifically to the IEMS launched synchronized backup/restore software. The SBRM controls/synchronizes the backup related activities across other components/devices which contain related backup software.
- Device Backup Restore Manager (DBRM) refers specifically to the component-/device-level backup software which is controlled by the SBRM.
- Backup Restore Manager is a generic term encompassing both SBRM and DBRM functionalities and in general simply refers to the software which is common to both.

The feature provides a centralized mechanism that allows the user to initiate a synchronous backup for the core components of the CVoIP Call Server. Providing this capability reduces the possibility of error caused by manual backup procedures on the various component platforms spread across the Call Server solution.

From (I)SN08, the Backup Manager will provide synchronous centralized control of the backup functionality resident within the following Call Server components

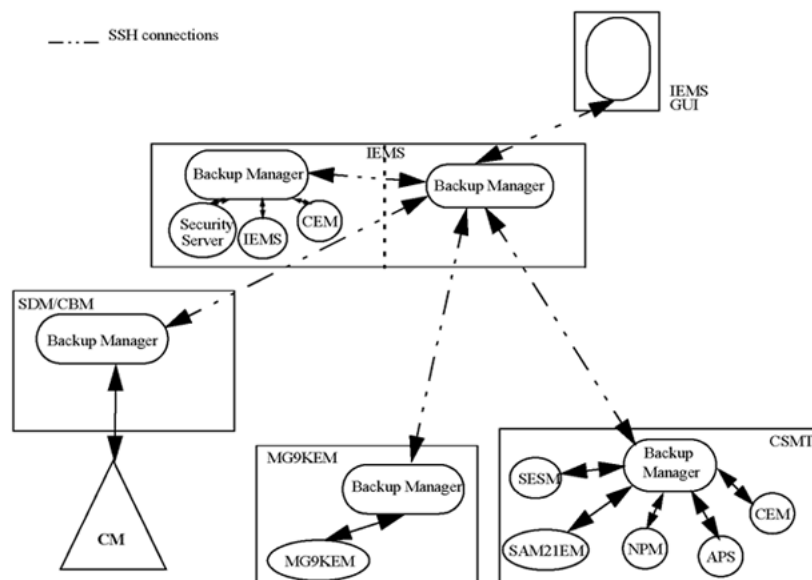
- CS 2000 Management Tools (CSMT) server
- MG 9000 Manager (MG9K) server
- Supernode Data Manager (SDM) / Core Billing Manager (CBM) server. The software on the SDM/CBM acts only to allow control of the XACore/3PC backup. no SDM/CBM data is backed up via the Backup Restore Manager software.
- Integrated Element Management System (IEMS) server

Note: The IEMS may reside with the CSMT (and other applications) on the CSMT server.

From the IEMS GUI, the user launches the SBRM command line interface and initiates a backup for the core components of the Succession Call Server. The SBRM receives the user request, and subsequently initiates a backup command sequence (using CLI commands over SSH) to execute a synchronous backup of the components. Once the backup is complete, the backup files are stored locally on each component.

The following figure shows a high-level functional overview of the SBRM.

High-level functional overview of the SBRM



Sequence of events to run the Synchronized Backup Manager

The component onto which the SBRM is being installed determines the sequence of events.

Installing and configuring SBRM on the SDM

To install and configure the Synchronized Backup Manager (SBRM) on the SDM, the following steps are required:

Step	Action
1	To install the Backup Restore Manager on the SDM, refer to procedure "Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager" in the <i>Nortel Carrier VoIP upgrade and patches</i> (NN10440-450) document.
2	To configure the bkmgrusr user ID and password on the SDM, refer to procedure, Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM.
3	To configure SSH between the backup manager restore servers, refer to procedure, "Configuring SSH between the backup restore manager servers" (page 58).

- 4 To configure core access for the SBRM through the SDM, refer to procedure, ["Configuring core access for SBRM through the CS 2000 Core Manager"](#) (page 51).
- 5 To create the backup user ID on the core for SBRM, refer to procedure, ["Creating the backup user ID on the core for SBRM"](#) (page 54).
- 6 To configure automated execution of backups, refer to procedure, ["Configuring the automated synchronous backup restore manager service"](#) (page 64).
- 7 Configure the specific Backup Restore Manager installations, setting the appropriate properties for the SBRM which resides in the IEMS and the individual component-level Backup Restore Managers which reside in the other platforms (for example, the CSMT and SDM).
- 8 Complete the common procedures for all components on page ["Common procedures for all components"](#) (page 34).

—End—

Installing and configuring SBRM on the CBM 850

To install and configure the Synchronized Backup Manager (SBRM) on the CBM 850, the following steps are required:

Step	Action
1	To install the Backup Restore Manager on the CBM 850, refer to procedure "Installing optional software on a CBM" in the <i>Nortel Carrier VoIP upgrade and patches</i> (NN10440-450) document . Note: No special configuration is required whilst performing this operation. Backup Restore Manager software to perform the manual bkfullsys, bkdata is already installed on the CBM.
2	To create the backup user ID on the core for SBRM, refer to procedure, "Creating the backup user ID on the core for SBRM" (page 54).
3	To configure SSH between the backup manager restore servers, refer to procedure, "Configuring SSH between the backup restore manager servers" (page 58).
4	To configure core access for SBRM through the CBM 850, refer to procedure "Configuring core access for SBRM through the CBM 850" (page 56).

- 5 Complete the common procedure for all components in this section, refer to procedure, ["Common procedures for all components"](#) (page 34).

—End—

Common procedures for all components

The following procedures are required in order to configure the SBRM on all components.

- To configure SSH between the backup manager restore servers (if not already completed), refer to procedure, ["Configuring SSH between the backup restore manager servers"](#) (page 58).

The following sections provide additional information regarding the SBRM:

- To configure automated execution of backups, refer to procedure, ["Configuring the automated synchronous backup restore manager service"](#) (page 64).
- To control the automated execution of backups, refer to procedure, ["Starting or stopping the automated synchronous backup restore manager service"](#) (page 69).

To configure the IEMS to support the SBRM, refer to the following procedures:

- To add the SBRM to the IEMS using the Java Web Start Client, refer to procedure, 'Adding a Synchronized Backup Restore Manager application (SBRM application)' in *IEMS Configuration Management*, NN10330-511.
- To add the SBRM to the IEMS using the web client, refer to procedure, 'Adding an SBRM application' in *IEMS Configuration Management*, NN10330-511.
- To launch the CLI for the SBRM using the IEMS Java Web Start Client, refer to the procedure, 'Launching CLI for SBRM application' in *IEMS Basics*, NN10329-111. The SBRM cannot be launch using the IEMS web client.

A network backup (that is, where several components are backed up at once) is invoked from the IEMS Backup Manager. In rare instances, it may be necessary to run various portions of the backup process on individual components/servers themselves. This capability is implemented as a CLUI interface, as in the following section.

Execution of a backup at the component-level

The CLUI interface to perform a backup at the component-level can be invoked by logging into the appropriate component via a Telnet session. Refer to procedure, ["Invoking the synchronous backup restore manager through telnet"](#) (page 73).

Hardware and software requirements

Backup Restore Manager functionality requires that the appropriate software is resident and configured in all platforms which require synchronized imaging. The Backup Restore Manager software itself is included in various platform software packages, including the SPFS and SDM. SPFS Backup Restore Manager functionality is used for integration of Call Server Management Tools (CSMT), the Media Gateway 9000 Element Manager (MG9KEM), the IEMS, and the CBM. The software on the SDM/CBM acts only to allow control of the XACore/3PC backup. No SDM/CBM data is backed up via the Backup Restore Manager software.

Requirements and restrictions

The following requirements and restrictions apply to Synchronized Backup Manager functionality from (I)SN08:

- All platforms requiring Backup Manager software functionality must be Java compatible and must provide a resident Java runtime system.
- Restore of generated synchronized backup images is not supported in the SBRM software. Existing manual restore procedures must be followed in order to utilize the backup images produced by the Backup Restore Manager.
- The Backup Restore Manager system does not perform automatic spooling of backup data/image files to secure/redundant servers. Customers are required to manage their own secure server archiving capabilities. The Backup Restore Manager system will publish data/image files in pre-determined/configurable directories on various servers:
 - SPSF Platform data/image file location: /data/bkresmgr/backup.
 - XACore/3PC data/image file location: Configurable
- Backup of program store and associated patches is not covered as part of the functionality associated with Synchronous Backup Restore Manager. If a customer needs to completely 'restore' a server/component, they will need to reinstall their applications and reapply the associated patches.
- The backup 'abort' command may require manual cleanup/removal of some backup files. The user will be notified at 'abort' command completion time if this is the case.

- The backup process itself can not be executed while certain constructive/destructive system audits are in progress (e.g. SESM's CS 2000 Data Integrity Audit). In general, if a backup is attempted while these audits are in progress, the backup attempt will be rejected. However, some constructive/destructive audits will be postponed when a backup request is received (e.g. MG9KEM Network Element Audit). The architecture of the system in question determines the appropriate behavior. In general, any system rejections of the backup request will result in an appropriate message being displayed to the Synchronous Backup Restore Manager client user.
- No system wide coordination between Synchronous Backup Restore Manager and other applications (eg. UpgradeManager, CS 2000 Audits, CM dump scheduling, etc.) is delivered. All application activity interdependencies must be manually managed by the user. For example, scheduled activities such as audits should be stopped during system backup. Also, any automated CM image dumps should be cancelled since the Synchronous Backup Restore Manager will be used to drive the dump within a synchronized system wide backup window.
- APS and NPM queries will be disallowed during backup. This is due to the applications being shut down during backup. Active clients will be informed of the application shutdown.
- Backup of the MG 9000 EM in isolation is not recommended due the CSMT platform data dependency. The MG 9000 EM database is hosted on the CSMT server.
- Synchronous Backup Restore Manager user authorization only controls the launch of the CLI. CLI Command specific authorization is not provided, therefore only users authorized to actually launch the Synchronous Backup Restore Manager CLI will be allowed to perform query commands at the Synchronous Backup Restore Manager CLI.
- The software on the SDM/CBM acts only to allow control of the XACore/3PC backup. No SDM/CBM data is backed up via the Backup Restore Manager software.

During the period when the backup is executing, user's of the various GUI and command line provisioning interfaces will be restricted from attempting actions which result in configuration and provisioning data changes. These restrictions include the following:

- Adding/deleting/updating GWCs at the Call Server Management Tools (CSMT) GUI or OSSGate interface.
- Adding/deleting/updating line service at the at the CSMT OSSGate interface.
- Manually invoking (or running via the scheduler) the various audits at the CSMT GUI.

- Adding/deleting/updating objects in the IEMS topology via the IEMS client.
- Adding/modifying collection jobs via the IEMS client.
- Using the Runtime Administration interface at the IEMS client to perform OSS configuration.
- Using the Security Administration interface at the Integrated client to add/delete Users/Groups/Operations.
- Using the Security Administration interface at the IEMS client to change a user password.
- Adding/deleting/updating Trunks/Carriers via the CSMT.
- Node provisioning/deprovisioning via the SAM21Manager.
- ATM connection set provisioning/deprovisioning via the SAM21 Manager.

Backup and restore

Backup and restore operations for CVoIP solutions are performed at the component level. They are performed on the components at different intervals during periods of low service activity. No provisioning or configuration changes are to be made during the backup and restore window.

ATTENTION

Back up all related devices in the solution during the same window of time. No changes are allowed to any related devices during this period until all backups are completed or those changes will not be captured as part of the coordinated backup and would be lost in case of the need to restore the system. For example, the CS 2000, CS 2000 GWC Manager, and MG 9000 Manager all share line service data and must be backed up in the same window.

Correspondingly all related devices need to be restored together to return the system to a known state. No changes are allowed to the system until the restoration is completed or data mismatches will result.

Backup operations

There are two types of backup operations for components of CVoIP solution: service data backup and fileset level backup.

Service data backup is typically performed once per day during a period of low activity. The following table lists components which are typically backed up using a service data backup.

Service data backup components

Component	Procedure (s)
NETWORK INTELLIGENCE	
CS 2000	"How to backup an XA-Core office image from disk to tape" (page 76)
Note 1: Service data from the SAM21, GWC, and MG 9000 is not backed up locally. It is backed up at the manager. The manager is backed up to tape using CS 2000 Core Manager or CS 2000 Management Tools procedures. Note 2: Service data from the IW SPM and MG 4000 is automatically backed up when the CS 2000 is backed up. Note 3: MDM backups are performed by copying the files to tape or an off box storage system through UNIX commands or CRON jobs. Note 4: A script purgeTempData.sh is provided in the /opt/nortel/iems/current/bin directory. This script will purge all event, alarm and performance data from the IEMS database. After purging the data it can't be retrieved. It deletes all events, alarms and performance data. To reduce the time taken to backup/restore, a user must stop the IEMS server and execute the purgeTempData.sh script to purge the events, alarms and performance data from the database.	

Component	Procedure (s)
Call Agent	"Call Agent backup" (page 86) "Backing up files to a DVD-RW" (page 89)
SAM21	none (See Note 1)
GWC	none (See Note 1)
Session Server	"Backing up the SST" (page 99) "Starting or stopping the automated synchronous backup restore manager service" (page 69)
Policy Controller	"Perform a manual backup of the Policy Controller database" (page 84)
Ethernet Routing Switch 8600	"Saving the Ethernet Routing Switch 8600 boot configuration file" (page 107)
UAS	"Backing up UAS configuration files" (page 109)
MS 2000 Series	For the following MS 2000 Series procedures, refer to the <i>Carrier VoIP Media Server 2000 Series Configuration Management</i> (NN10340-511). Displaying the MS 2000 Series node configuration: Configuring automated INI file backups Changing the SNMP community string password for a Media Server 2010 node Changing the SNMP community string password for a Media Server 2020 node Backing up all MS 2000 Series node INI files: Backing up INI files for all nodes Configuring the MS 2000 Series CLUI tool: Displaying Media Server 2010 node current configuration Displaying Media Server 2020 node current configuration
APS	"Backing up the APS-specific Oracle database and application files" (page 117)
USP	Administration: OAMP Workstation Backup
Real-time Transport Protocol (RTP) Media Portal	RTP Media Portal Basics, NN10367-111
CICM	CICM Security and Administration, NN10252-611
Note 1: Service data from the SAM21, GWC, and MG 9000 is not backed up locally. It is backed up at the manager. The manager is backed up to tape using CS 2000 Core Manager or CS 2000 Management Tools procedures. Note 2: Service data from the IW SPM and MG 4000 is automatically backed up when the CS 2000 is backed up. Note 3: MDM backups are performed by copying the files to tape or an off box storage system through UNIX commands or CRON jobs. Note 4: A script purgeTempData.sh is provided in the /opt/nortel/iems/current/bin directory. This script will purge all event, alarm and performance data from the IEMS database. After purging the data it can't be retrieved. It deletes all events, alarms and performance data. To reduce the time taken to backup/restore, a user must stop the IEMS server and execute the purgeTempData.sh script to purge the events, alarms and performance data from the database.	

Component	Procedure (s)
CORE NETWORK	
Multiservice Switch or Media Gateway devices	"Backing up a Multiservice Switch or Media Gateway device" (page 127)
GATEWAYS	
MG 15000	
MG 9000	none (See Note 1)
MG 4000	none (See Note 2)
IW SPM	none (See Note 2)
NETWORK MANAGEMENT	
CS 2000 Core Manager	"Starting or stopping the automated synchronous backup restore manager service" (page 69)
Core Element Manager	"Starting or stopping the automated synchronous backup restore manager service" (page 69)
CS 2000 Management Tools	"Performing a backup of oracle data on an SSPFS-based server" (page 135) "Performing a backup of file systems on an SPFS-based server" (page 140) "Starting or stopping the automated synchronous backup restore manager service" (page 69)
Integrated Element Management System	"Performing a backup of oracle data on an SSPFS-based server" (page 135) "Performing a backup of file systems on an SPFS-based server" (page 140) "Starting or stopping the automated synchronous backup restore manager service" (page 69)
IEMS centralized security server	"Backing up the central security server" (page 144)
Note 1: Service data from the SAM21, GWC, and MG 9000 is not backed up locally. It is backed up at the manager. The manager is backed up to tape using CS 2000 Core Manager or CS 2000 Management Tools procedures. Note 2: Service data from the IW SPM and MG 4000 is automatically backed up when the CS 2000 is backed up. Note 3: MDM backups are performed by copying the files to tape or an off box storage system through UNIX commands or CRON jobs. Note 4: A script purgeTempData.sh is provided in the /opt/nortel/iems/current/bin directory. This script will purge all event, alarm and performance data from the IEMS database. After purging the data it can't be retrieved. It deletes all events, alarms and performance data. To reduce the time taken to backup/restore, a user must stop the IEMS server and execute the purgeTempData.sh script to purge the events, alarms and performance data from the database.	

Component	Procedure (s)
MG 9000 Manager	"Performing a backup of oracle data on an SSPFS-based server" (page 135) "Performing a backup of file systems on an SPFS-based server" (page 140) "Starting or stopping the automated synchronous backup restore manager service" (page 69)
MDM	none (See Note 3)
Note 1: Service data from the SAM21, GWC, and MG 9000 is not backed up locally. It is backed up at the manager. The manager is backed up to tape using CS 2000 Core Manager or CS 2000 Management Tools procedures. Note 2: Service data from the IW SPM and MG 4000 is automatically backed up when the CS 2000 is backed up. Note 3: MDM backups are performed by copying the files to tape or an off box storage system through UNIX commands or CRON jobs. Note 4: A script purgeTempData.sh is provided in the /opt/nortel/iems/current/bin directory. This script will purge all event, alarm and performance data from the IEMS database. After purging the data it can't be retrieved. It deletes all events, alarms and performance data. To reduce the time taken to backup/restore, a user must stop the IEMS server and execute the purgeTempData.sh script to purge the events, alarms and performance data from the database.	

Fileset level backups back up the software as well as configuration data. This type of backup is performed after hardware changes, software updates or patches, or major reconfigurations. Fileset backup also need to be performed before a major upgrade. The following table provides a list of components with fileset level backup procedures.

Fileset level backup components

Component	Procedure (s)
NETWORK INTELLIGENCE	
GWC	Create a backup of the GWC load file in <i>Nortel Carrier VoIP upgrade and patches</i> (NN10440-450) document.
USP	Administration: Manual Backup
GATEWAYS	
Multiservice Switch or Media Gateway devices	"Backing up a Multiservice Switch or Media Gateway device" (page 127)
NETWORK MANAGEMENT	
CS 2000 Core Manager or CBM	Creating system image backup tapes (S-tapes) manually Configuring SBA backup volumes on the core

Frequency of backup operations

The following table lists each component along with how often backup operations are recommended to be performed.

Component backup frequency

Component	Backup Frequency
NETWORK INTELLIGENCE	
CS 2000MSC Server 1000 XA-Core	Weekly
Call Agent	Weekly
SAM21	See Note 1
GWC	See Note 1
Session Server	Weekly
CS 2000 CS LAN	Full backup - monthly, and prior to all migrations and patch operations and configuration changes
UAS	Daily
MS 2000 Series	Daily
APS	Daily
RTP Media Portal	Daily
CICM	Daily
USP	Full system backup - once a week. Modified (differential) backup - once a day
CORE NETWORK	
Multiservice switches	Full backup - monthly, and prior to all migrations and patch operations
GATEWAYS	
MG 9000	See Note 1
MG 4000	See Note 2
IW SPM	See Note 2
NETWORK MANAGEMENT	
CS 2000 Management Tools	Daily
Note 1: Service data from the SAM21, GWC, and MG 9000 is not backed up locally. It is backed up at the manager. The manager is backed up to tape using CS 2000 Core Manager or CS 2000 Management Tools procedures. Note 2: Service data from the IW SPM and MG 4000 is automatically backed up when the CS 2000 is backed up.	

Component	Backup Frequency
MG 9000 Manager	Daily
IEMS	Daily
Nortel MDM	Full backup - monthly, and prior to all migrations and patch operations. Incremental backup - weekly

Note 1: Service data from the SAM21, GWC, and MG 9000 is not backed up locally. It is backed up at the manager. The manager is backed up to tape using CS 2000 Core Manager or CS 2000 Management Tools procedures.

Note 2: Service data from the IW SPM and MG 4000 is automatically backed up when the CS 2000 is backed up.

Logging in to an SPFS-based server

Application

Use this procedure to log into a Server Platform Foundation Software (SPFS) server. This procedure provides the steps to establish a login session using SSH, which is secure, or telnet, which is not secure.

Some tasks will require that you log in to the server through the console (port A) using the root user ID and password.

Prerequisites

This procedure requires the following information:

- the IP address or host name of the server
In a two-server configuration, you need the physical IP address of the active or inactive server.
- a valid user id and password
- the root password if you need to perform a task on the server that requires root user privileges

Action

Perform the steps under one of the following headings to complete this procedure.

- Logging in using SSH
- Logging in using Telnet
- Logging in through the console

Logging in using SSH

Step	Action
At your workstation	
1	Establish an SSH session.
	If you have access to a workstation which supports the ssh command (Linux, for example) then proceed with step a .
	Otherwise, connect to the server using an SSH client and proceed to step 2 .
	a. Establish an SSH session to the server by typing
	> <code>ssh -l <user_id> <server></code>
	where

At your workstation

- 1 Establish an SSH session.

If you have access to a workstation which supports the ssh command (Linux, for example) then proceed with [step a](#).

Otherwise, connect to the server using an SSH client and proceed to [step 2](#).

- a. Establish an SSH session to the server by typing

```
> ssh -l <user_id> <server>
```

where

user_id is root or your user id

server is the IP address or host name of the SPFS-based server, or the physical IP address of the active or inactive server as required, in a two-server configuration

- 2 Use the following table to determine your next step.

If you receive	Do
a message indicating a host authentication issue and a request to continue the connection	step 3
a prompt for a password	step 4

ATTENTION

The prompt indicates SSH is verifying whether the server is a trusted host for the workstation. SSH performs the verification the first time SSH is run on a workstation.

- 3 Continue the connection by typing
`y`
 and pressing the Enter key.
- 4 Enter the password for root or your user id and press the Enter key.
- 5 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 9
two-server configuration	step 6

- 6 Ensure you are on the correct server by typing
`# ubmstat`
 and pressing the Enter key.
- 7 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 8
inactive server and the response is ClusterIndicatorACT	step 8

If you need to be on the	Do
active server and the response is ClusterIndicatorACT	step 9
inactive server and the response is ClusterIndicatorSTBY	step 9

- 8 You are logged in to the wrong server. Return to [step 1](#) to log in to the other server.
- 9 You have completed this procedure.
If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Logging in using Telnet

Step	Action

At your workstation

- 1 Establish a telnet session to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server is the IP address or hostname of the SPFS-based server, or the physical IP address of the active or inactive server in a two-server configuration

- 2 When prompted, enter your userid.

ATTENTION

You cannot log in using the root userid at this step.

- 3 When prompted, enter your password.
- 4 Use the following table to determine your next step.

If	Do
you need to log in as root	step 5
otherwise	step 7

- 5 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

6 When prompted, enter the root password.

7 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 11
two-server configuration	step 8

8 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

9 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 10
inactive server and the response is ClusterIndicatorACT	step 10
active server and the response is ClusterIndicatorACT	step 11
inactive server and the response is ClusterIndicatorSTBY	step 11

10 You are logged in to the wrong server. Log out of this server and return to [step 1](#) to log in to the other server.

11 You have completed this procedure.
If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Logging in through the console

Step	Action

At the console connected to the server

- 1 Log in to the server through the console (port A) using the root user ID and password. In a two-server configuration, log in to the active or inactive server as required.

- 2 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 6
two-server configuration	step 3

- 3 Ensure you are on the correct server by typing

`ubmstat`

and pressing the Enter key.

- 4 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 5
inactive server and the response is ClusterIndicatorACT	step 5
active server and the response is ClusterIndicatorACT	step 6
inactive server and the response is ClusterIndicatorSTBY	step 6

- 5 You are logged in to the wrong server. Log out of this server and return to [step 1](#) to log in to the other server.
- 6 You have completed this procedure.
If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM

Purpose

This procedure enables you to configure the bkmgrusr user ID and password in order for the Synchronous Backup Restore Manager (SBRM) to communicate with the Device Backup Restore Manager (DBRM) on the CS 2000 Core Manager.

Note: This procedure applies only to the CS 2000 Core Manager.

Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	CS 2000 Core Manager Security and Administration, NN10170-611
Displaying actions a user is authorized to perform	CS 2000 Core Manager Security and Administration, NN10170-611

Procedure

Configuring the bkmgrusr user ID and password for communication with SBRM

Step	Action

At your workstation

- 1 Log into the CS 2000 Core Manager on which the DBRM is installed as a user authorized to perform config-admin actions.
- 2 Create the user, "bkmgrusr":
`mkuser bkmgrusr`

- 3 Create the groups, "emsmtc", "emsadm", and "emsrw":

```
mkgroup emsmtc
mkgroup emsadm
mkgroup emsrw
```

- 4 Add the bkmgrusr user to the primary group, "maint", and to secondary groups, "emsmtc", "emsadm", "emsrw":

```
chuser pgrp=maint groups=emsmtc,emsadm,emsrw
home=/home/bkmgrusr admin=true shell=/bin/ksh bkmgrusr
```

Note: Although it may be unclear from the command syntax shown above, this command is entered on a single line. Therefore, when you enter this command, ensure that there is a space between **emsrw** and **home**, and that there is a space between **ksh** and **bkmgrusr**.

Confirm that the bkmgrusr user has been added to the required groups in step 4:

```
groups bkmgrusr
```

The system will display the groups that are associated with the bkmgrusr user.

- 5 Set the password for the bkmgrusr user:

```
passwd bkmgrusr
```

Note: The bkmgrusr user is disabled until this step is performed.

- 6 Log out of the CS 2000 Core Manager and then log back in as "bkmgrusr".

When the system prompts you, change the password for the bkmgrusr user.

- 7 Change to the home directory and create the ".ssh" directory:

```
cd /home/bkmgrusr
mkdir .ssh
chmod 700 .ssh
```

- 8 You have completed this procedure.

—End—

Configuring core access for SBRM through the CS 2000 Core Manager

Purpose

This procedure enables you to configure access to the core for the Synchronous Backup Restore Manager (SBRM). This procedure must be performed before the SBRM can automatically backup a core image.

Note 1: Perform the procedure, "[Creating the backup user ID on the core for SBRM](#)" (page 54) before you perform this procedure for the first time.

Note 2: This procedure should be performed to whenever the password for the core user password expires or is changed. This ensures that the password you set in this procedure matches that set for the user on the core.

Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	Security and Administration
Displaying actions a user is authorized to perform	Security and Administration

Procedures

Configuring core access for SBRM through the CS 2000 Core Manager

Step	Action

At the CS 2000 Core Manager

1	Log into the core manager with the login ID and password for a user authorized to perform config-admin actions.

- 2 Use the following table to determine your next step.

If	Do
you are using the CBM to perform this procedure (command line)	step 3
you are using the SDM to perform this procedure (SDM maintenance interface - SDMMTC)	step 5

- 3 At the command line prompt, change directory to the directory containing appropriate configuration script:
- ```
cd /opt/nortel/bkresmgr/cbm/scripts
```
- 4 Run the configuration script:
- ```
./bkmgr_config.sh
```
- Go to step 7.
- 5 Access the config level of the SDM maintenance interface:
- ```
sdmmtc config
```
- 6 From the list of filesets that displays, select the Succession Provisioning Data Sync Manager fileset (Backup Restore Manager fileset, SDM\_BKM.bkm) and then type **config**.
- 7 As the configuration script runs, you are first prompted for the user name. The user name is that which will be used to login to the core in order to initiate an image dump. The script restricts the name to a maximum of 16 characters. The user name you enter must first have been enabled on the core through the procedure, ["Creating the backup user ID on the core for SBRM" \(page 54\)](#)
- 8 As the script continues to run, you are then prompted for the user you entered (in step 7). The script restricts the password to a maximum of 16 characters. This password is the one that was set up through the procedure, ["Creating the backup user ID on the core for SBRM" \(page 54\)](#)
- 9 As the script continues to run, you are then prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored. You should ensure that this device has enough space to store the backup.
- 10 As the script continues to run, you are then prompted for the core type, either xa-core or Compact. This information is needed in order for the software to know whether the core will also have a Message Switch load.
- 11 You have completed this procedure.



---

—End—

---

## Creating the backup user ID on the core for SBRM

### Purpose

This procedure enables you to create the user ID on the core to enable the operation of the Synchronous Backup Restore Manager (SBRM). The types of operations that can be performed by this user are:

- set dump\_restore\_in\_progress field in ofcstd table
- start image dump
- ability to run itocci command set
- ability to perform diskut commands

**Note 1:** This procedure should be performed before you first perform the procedure, "Configuring core access for SBRM".

**Note 2:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Procedure

#### Creating the backup user ID on the core for SBRM

| Step | Action |
|------|--------|
|------|--------|

*At the CLI prompt on the core*

- 1 Enter the following command:

```
permit <backupuser> <backupuser_pswd> 4 10000 english
all
```

where

**<backupuser>** is the user name for the core, that is up to 16 characters in length, that will be used by SBRM for login

**<backupuser\_pswd>** is the password for the <backupuser> user you are creating, which can be up to 16 characters in length

**4** is the priority

**10000** is the stack size

**english** the language setting

**all** is the privilege setting

**Note 1:** If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

**Note 2:** If Enhanced Password Control is in effect on the CM and after the user is permitted on the switch, log into the core

manually with this user first. The core will prompt you to change the password at the first login after the login is permitted. Change the password and then perform the procedure, "Configuring core access for SBRM" using the <backupuser> user you have created and the changed password.

The SBRM does not have the ability to manage passwords. Therefore, you must re-run the configuration script in "Configuring core access for SBRM" to ensure that the password for the <backupuser> user

- 2 You have completed this procedure.

---

—End—

---

## Configuring core access for SBRM through the CBM 850

### Purpose

This procedure enables you to configure access to the core for the Synchronous Backup Restore Manager (SBRM). This procedure must be performed before the SBRM can automatically backup a core image.

**Note 1:** Perform the procedure, "[Creating the backup user ID on the core for SBRM](#)" (page 54) before you perform this procedure for the first time.

**Note 2:** This procedure should be performed whenever the password for the core user password expires or is changed. This ensures that the password you set in this procedure matches that set for the user on the core.

### Procedure

#### Configuring core access for SBRM

| Step | Action |
|------|--------|
|------|--------|

*At your workstation*

- |   |                                                                                                                                                                                                                                                                                                                                                                                                     |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Log into the Core and Billing Manager 850 (CBM 850).                                                                                                                                                                                                                                                                                                                                                |
| 2 | Change to the root user:<br><br><code>su - root</code>                                                                                                                                                                                                                                                                                                                                              |
| 3 | When prompted, enter the root password.                                                                                                                                                                                                                                                                                                                                                             |
| 4 | Change directory to the directory containing appropriate configuration script:<br><br><code>cd /opt/nortel/bkresmgr/cbm/scripts</code>                                                                                                                                                                                                                                                              |
| 5 | Run the configuration script:<br><br><code>./bkmgr_config.sh</code>                                                                                                                                                                                                                                                                                                                                 |
| 6 | As the script runs, you are first prompted for the user name. The user name is that which will be used to login to the core in order to initiate an image dump. The script restricts the name to a maximum of 16 characters. The user name you enter must first have been enabled on the core through the procedure, " <a href="#">Creating the backup user ID on the core for SBRM</a> " (page 54) |

- 7 As the script continues to run, you are then prompted for the user you entered (in step 6). The script restricts the password to a maximum of 16 characters. This password is the one that was set up through the procedure, "[Creating the backup user ID on the core for SBRM](#)" (page 54)
- 8 As the script continues to run, you are then prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored. You should ensure that this device has enough space to store the backup.
- 9 As the script continues to run, you are then prompted for the core type, either xa-core or Compact. This information is needed in order for the software to know whether the core will also have a Message Switch load.
- 10 You have completed this procedure.

---

—End—

---

## Configuring SSH between the backup restore manager servers

### Application

Use this procedure to configure the secure shell (SSH) between the Integrated Element Management system (IEMS) server where the synchronous backup restore manager (SBRM) software is installed, and the SPFS-based servers where the device backup restore manager (DBRM) software is installed.

Throughout the remainder of this procedure, the IEMS server will be referred to as the SBRM server and the SPFS-based servers will be referred to as the DBRM servers.

SSH provides authentication and secure communications over insecure channels.

This procedure contains the steps to generate the SSH key pair on the SBRM server and transfer the key pair to each DBRM server and the SDM platform in the network. It also contains the steps to transfer an existing SSH key pair from the SBRM server to new or existing DBRM servers and the SDM platform in the network.

### Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password for the SBRM server
- you need the password for the bkmgrusr on the DBRM servers to transfer the SSH key pair

The bkmgrusr is created on the DBRM server when SPFS is installed. To set or change the bkmgrusr password, refer to procedure ["Changing a user password on an SPFS-based server" \(page 362\)](#).

- you need the root password for the DBRM server when the DBRM server is a two-server configuration, to synchronize the SSH data between the two servers

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

|                            |  |
|----------------------------|--|
| <i>At your workstation</i> |  |
|----------------------------|--|

- 1 Log in to the SBRM server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
**server** is the IP address or host name of the IEMS server where the SBRM software is installed  
 In a two-server configuration, log in to the Active side using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su -
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change directory to where the backup restore manager configuration script is located by typing  

```
cd /opt/bkresmgr/admin/bin
```

 and pressing the Enter key.
- 6 Run the backup restore manager configuration script by typing  

```
./configure
```

 and pressing the Enter key.

*Example response:*

```
Backup Restore Manager Configuration
 1 - Backup Restore Manager SSH Setup
 2 - Automated Synchronous Backup Restore
 Manager Service
 X - exit
select - [X, 1-2]
```

- 7 Enter the number next to the 'Backup Restore Manager SSH setup' option in the menu.

*Example response:*

```
SSH Setup for Synchronous Backup Restore Manager
 1 - Generate SSH key and transfer to Device
 Backup Restore Manager servers
 2 - Transfer existing SSH key to Device
 Backup Restore Manager servers
 X - exit
select - [X, 1-2]
```

- 8 Use the following table to determine your next step.

| If you are                                                                | Do      |
|---------------------------------------------------------------------------|---------|
| configuring SSH for the first time, or changing the SSH key pair          | step 9  |
| transferring an existing SSH key to Device Backup Restore Manager servers | step 22 |

- 9 Enter the number next to the 'Generate SSH key and transfer to Device Backup Restore Manager servers' option in the menu.

*Example response:*

```
Generate SSH key for Synchronous Backup Restore
Manager and transfer to Device Backup Restore
Manager servers.
WARNING: Running this script will generate a new SSH
key for the bkmgrusr.
This new SSH key must be transferred to all existing
and new Device Backup Restore Manager servers.
Do you want to continue? [y/n]:
```

- 10 When prompted, confirm you want to continue by typing

**y**  
and pressing the Enter key.

*Example response:*

```
Generating SSH key for bkmgrusr.
Sun Microsystems Inc. SunOS 5.9 Generic
May 2002
Generating public/private rsa key pair.
Enter file in which to save the key
(/export/home/bkmgrusr/.ssh/id_rsa):
```

- 11 When prompted, press the Enter key to accept the default location and filename '/export/home/bkmgrusr/.ssh/id\_rsa' for the key.

If the default location and filename is not provided, enter '/export/home/bkmgrusr/.ssh/id\_rsa'.

If the location and filename '/export/home/bkmgrusr/.ssh/id\_rsa' already exists and you wish to overwrite, enter **y**. Otherwise, enter **n**.

*Example response:*

```
Your identification has been saved in /export/home/bk
mgrusr/.ssh/id_rsa.
Your public key has been saved in /export/home/bkmgru
sr/.ssh/id_rsa.pub.
The key fingerprint is:
```



```

33:99:17:f0:ac:2a:3a:86:a9:d9:76:65:e6:70:4b:6:8
bkmgrusr@comp5iems
Synchronizing files IF clustered node
Transfer existing SSH key to Device Backup Restore
Manager servers
WARNING: You must have the password for the bkmgrusr on
the Device Backup Restore Manager server to transfer
the SSH key.
Do you want to transfer the SSH key? [y/n]:

```

- 12** When prompted, confirm you want to transfer the SSH key pair by typing

**y**

and pressing the Enter key.

*Example response:*

```

Setting up to transfer SSH key to DBRM server.
Enter hostname or IP address of DBRM server to transfer
the SSH key to:

```

- 13** When prompted, enter the hostname or IP address of a DBRM server in your network.

*Example response:*

```

Platform type of DBRM server to transfer SSH key to:
 1 - SPFS
 2 - SDM
Enter platform type of DBRM server to transfer SSH key
to [1-2]:

```

- 14** When prompted, enter the number next to the platform type of the DBRM server.

The SPFS platform type is for servers hosting the CS 2000 Management Tools, MG 9000 Manager and Core and Billing Manager (CBM). The SDM platform type is an AIX platform containing core management software.

*Example response:*

```

Sun Microsystems Inc. SunOS 5.9 Generic
May 2002
The authenticity of host 'comp5iems (45.123.456.98)'
can't be established.
RSA key fingerprint is
ff:eb:a8:87:14:d0:82:28:5c:43:70:5a:ab:af:e6:f
d
Are you sure you want to continue connecting (yes/no)? :

```

- 15** When prompted, confirm you want to continue connecting by typing  
**yes**

and pressing the Enter key.

Warning: Permanently added 'comp5iems  
(45.123.456.98)' (RSA) to the list of known hosts.  
Password:

- 16** When prompted, enter the password for the bkmgrusr on the DBRM server.

*Example response:*

Transfer of SSH key to <server> complete.  
Is DBRM <server> a High Availability (HA) server?  
[y/n]:

- 17** When prompted, enter y if the DBRM server is a two-server configuration (HA), otherwise, enter n.

| If you entered | Do      |
|----------------|---------|
| y (yes)        | step 18 |
| n (no)         | step 21 |

#### ATTENTION

You need the password for the root user on the DBRM server to complete the steps that follow.

- 18** *Example response:*

WARNING: On HA DBRM servers, SSH setup is not complete unless one of the following steps is performed.

- a) The HA DBRM server <servername> is cloned.
- b) The SSH data on HA DBRM <servername> is manually synched.

WARNING: Choosing this option requires the root password for <servername>

Do you want to manually synchronize the SSH data on DBRM <servername> now [y/n]

- 19** When prompted, enter y if you want to manually synchronize the SSH data, otherwise, enter n.

| If you entered | Do      |
|----------------|---------|
| y (yes)        | step 20 |
| n (no)         | step 21 |

- 20** When prompted, enter the root password for the DBRM server

*Example response:*

Synchronization of SSH data on DBRM <servername> complete.

- 21** When prompted, indicate that you want to transfer the SSH key pair to the DBRM installation on the SBRM server in your network.

The SBRM always makes a SSH connection to the DBRM residing on the local server so that the local IEMS application is notified of the synchronized backup by way of SBRM to DBRM messaging.

- 22** Enter the number next to the "Transfer existing SSH key to Device Backup Restore Manager servers" option in the menu.

*Example response:*

```
Transfer existing SSH key to Device Backup Restore
Manager servers
```

```
WARNING: You must have the password for the bkmgrusr on
the Device Backup Restore Manager server to transfer
the SSH key.
```

```
Do you want to transfer the SSH key? [y/n] :
```

- 23** When prompted, confirm you want to transfer the SSH key pair by typing

**y**

and pressing the Enter key.

*Example response:*

```
Setting up to transfer SSH key to DBRM server.
```

```
Enter hostname or IP address of DBRM server to transfer
the SSH key to:
```

This returns you to step 13.

- 24** Exit the 'Backup Restore Manager SSH setup' level by typing

```
select - x
```

and pressing the Enter key.

- 25** Exit the 'Backup Restore Manager Configuration' level by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

---

—End—

---

## Configuring the automated synchronous backup restore manager service

### Application

Use this procedure to configure the synchronous backup restore manager (SBRM) service on the SPFS-based server where the SBRM software is installed, for automated execution of backups. You can configure the SBRM service to execute backups on a weekly or daily basis.

### Prerequisites

You need the root user ID and password for the SPFS-based server where the SBRM software is installed.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the SBRM server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
     **server** is the IP address or host name of the IEMS server where the SBRM software is installed  
 In a two-server configuration, log in to the Active side using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su -
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change directory to where the backup restore manager configuration script is located by typing  

```
cd /opt/bkresmgr/admin/bin
```

 and pressing the Enter key.

- 6 Run the backup restore manager configuration script by typing

```
./configure
```

and pressing the Enter key.

*Example response:*

```
Backup Restore Manager Configuration
1 - Backup Restore Manager SSH Setup
2 - Automated Synchronous Backup Restore
Manager Service
X - exit
select - [X, 1-2]
```

- 7 Enter the number next to the 'Automated Synchronous Backup Restore Manager Service' option in the menu.

*Example response:*

```
Automated Synchronous Backup Restore Manager Service
1 - Configure Automated Synchronous Backup Restore
Manager Service
2 - Start the Automated Synchronous Backup Restore
Manager Service
3 - Stop the Automated Synchronous Backup Restore
Manager Service
4 - View the Automated Synchronous Backup Restore
Manager Service Configuration
X - exit
select - [X, 1-4]
```

- 8 View the configuration settings as follows:

- a. Enter the number next to the 'View the Automated Synchronous Backup Restore Manager Service Configuration' option in the menu.

*Example response:*

```
The Automated Synchronous Backup Restore Manager
Service is not running
Automated Synchronous Backup Restore Manager Service
Configuration Settings
Backup Enabled : N
Backup Day : SUNDAY
Backup Hour : 24
```

- b. Use the following table to determine your next step.

| If you                                                               | Do      |
|----------------------------------------------------------------------|---------|
| want to change the configuration settings of the SBRM service        | step 9  |
| do not want to change the configuration settings of the SBRM service | step 11 |

**9** Change the configuration settings as follows:

- a. Enter the number next to the 'Configure Automated Synchronous Backup Restore Manager Service' option in the menu.

*Example response:*

```
Automated Synchronous Backup Restore Manager Service
Configuration
Configuring the Automated Synchronous Backup Restore
Manager Service does not START the service. Return
to the previous menu and select 'Start the Automated
Synchronous Backup Restore Manager Service' to start
the service.
Do you want the backup to run 1.daily or 2.weekly
[1/2] :
```

- b. When prompted, enter the number next to daily or weekly.

*Example response if daily is selected:*

```
Hour to run the Synchronous Backup Restore Manager
based on 24 hour clock:
Example 1 is 1 AM, 12 is noon, and 24 is midnight.
This is the hour on the <DAY> the Synchronous Backup
Restore Manager will execute a full backup.
Enter hour to run the Synchronous Backup Restore
Manager (default: 24)
```

*Example response if weekly is selected:*

```
Day of the week to run the Synchronous Backup
Restore Manager:
This is day of the week the Synchronous Backup
Restore Manager will execute a full backup.
1 - MONDAY
2 - TUESDAY
3 - WEDNESDAY
4 - THURSDAY
5 - FRIDAY
6 - SATURDAY
7 - SUNDAY
```

Enter day of week to run the Synchronous Backup Restore Manager (default: SUNDAY):

| If you selected | Do     |
|-----------------|--------|
| weekly          | step c |
| daily           | step d |

- c. When prompted, enter the number next to the day of the week on which you want the backup to execute, or press the Enter key to accept the default value.

*Example response:*

Hour to run the Synchronous Backup Restore Manager based on 24 hour clock:

Example 1 is 1 AM, 12 is noon, and 24 is midnight.

This is the hour on the <DAY> the Synchronous Backup Restore Manager will execute a full backup.

Enter hour to run the Synchronous Backup Restore Manager (default: 24)

- d. When prompted, enter the time of day at which you want the backup to execute, or press the Enter key to accept the default.

*Example response:*

Automated Synchronous Backup Restore Manager Service Configuration complete.

Configuring the Automated Synchronous Backup Restore Manager Service does not START the service. Return to the previous menu and select 'Start the Automated Synchronous Backup Restore Manager Service' to start the service.

- 10 Use the following table to determine your next step.

| If you                                              | Do                                                                 |
|-----------------------------------------------------|--------------------------------------------------------------------|
| want to start the automated SBRM service now        | perform procedure Enabling or disabling the automated SBRM service |
| do not want to start the automated SBRM service now | step 11                                                            |

- 11 Exit the 'Automated Synchronous Backup Restore Manager Service' level by typing

select - x

and pressing the Enter key.

- 12 Exit the 'Backup Restore Manager Configuration' level by typing

select - **x**

and pressing the Enter key.

You have completed this procedure.

---

—End—

---



# Starting or stopping the automated synchronous backup restore manager service

## Application

Use this procedure to start or stop the synchronous backup restore manager (SBRM) service on the SPFS-based server where the SBRM software is installed.

## Prerequisites

You need the root user ID and password for the SPFS-based server where the SBRM software is installed.

## Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

### *At your workstation*

- 1 Log in to the SBRM server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
     **server** is the IP address or host name of the IEMS server where the SBRM software is installed  
 In a two-server configuration, log in to the Active side using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change directory to where the backup restore manager configuration script is located by typing  

```
cd /opt/bkresmgr/admin/bin
```

 and pressing the Enter key.
- 6 Run the backup restore manager configuration script by typing

```
./configure
```

and pressing the Enter key.

*Example response:*

```
Backup Restore Manager Configuration
1 - Backup Restore Manager SSH Setup
2 - Automated Synchronous Backup Restore Manager
Service
X - exit
select - [X, 1-2]
```

- 7 Enter the number next to the 'Automated Synchronous Backup Restore Manager Service' option in the menu.

*Example response:*

```
Automated Synchronous Backup Restore Manager Service
1 - Configure Automated Synchronous Backup
Restore Manager Service
2 - Start the Automated Synchronous Backup
Restore Manager Service
3 - Stop the Automated Synchronous Backup
Restore Manager Service
4 - View the Automated Synchronous Backup
Restore Manager Service Configuration
X - exit
select - [X, 1-4]
```

- 8 Use the following table to determine your next step.

| If you want to                   | Do                      |
|----------------------------------|-------------------------|
| start the automated SBRM service | step <a href="#">9</a>  |
| stop the automated SBRM service  | step <a href="#">10</a> |

- 9 Start the SBRM service as follows:

- a. Enter the number next to the 'Start the Automated Synchronous Backup Restore Manager Service' option in the menu.

*Example response:*

```
Start the Automated Synchronous Backup Restore
Manager Service
WARNING: Running this script will start the
Automated Synchronous Backup Restore Manager Service
Starting the service does not initiate a backup
until the day and time configured.
Do you want to continue? - [y/n]:
```

- b. When prompted, confirm you want to start the SBRM service by typing

y

and pressing the Enter key.

*Example response:*

```
Registering with SERVMAN.
Starting the Automated Synchronous Backup Restore
Manager Service.
Starting AUTO_BACKUP_MANAGER through servstart
AUTO_BACKUP_MANAGER Started
```

- c. Proceed to step 11.

**10** Stop the SBRM service as follows:

- a. Enter the number next to the 'Stop the Automated Synchronous Backup Restore Manager Service' option in the menu.

*Example response:*

```
Stop the Automated Synchronous Backup Restore
Manager Service
WARNING: Running this script will stop the Automated
Synchronous Backup Restore Manager Service
Stopping the service does not abort a backup in
progress.
Do you want to continue? - [y/n]:
```

- b. When prompted, confirm you want to stop the SBRM service by typing

y

and pressing the Enter key.

*Example response:*

```
Stopping the Automated Synchronous Backup Restore
Manager Service.
Stopping group using servstop AUTO_BACKUP_MANAGER
Stopped
Deregistering with SERVMAN
```

**11** Exit the 'Automated Synchronous Backup Restore Manager Service' level by typing

```
select - x
```

and pressing the Enter key.

**12** Exit the 'Backup Restore Manager Configuration' level by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

---

—End—

---

## Invoking the synchronous backup restore manager through telnet

### Application

Use this procedure to run various portions of the synchronous backup restore manager (SBRM) process from the backup manager CLUI on an SPFS-based server where the Device Backup Restore Manager (DBRM) software resides, rather than from the CLUI on the Integrated Element Management System (EMS) server where the Synchronous Backup Restore Manager (SBRM) software resides.

All backups will be stored in a common file location. For example, '/opt/nortel/backup/\*'.

### Prerequisites

You need the root user ID and password for the SPFS-based server on which you are running the various portions of the SBRM process.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the SPFS-based server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server** is the IP address or host name of the SPFS-based server on which you are running the various portions of the SBRM process  
In a two-server configuration, log in to the Active side using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su -
```

and pressing the Enter key.
- 4 When prompted, enter the root password.

- 5 Change directory to where the backup restore manager script is located by typing

```
cd /opt/nortel/bkresmgr/cbm
```

and pressing the Enter key.

- 6 Start the backup restore manager by typing

```
./bkmgr
```

and pressing the Enter key.

- 7 Invoke the desired step of the backup process by typing

```
bkmgr> <command>
```

where

**command** is any one of the following commands:

- precheck
- stopprov
- dumpdata
- verify
- startprov
- activatenew

Refer to "[Additional information](#)" (page 74) for further information on commands.

You have completed this procedure.

---

—End—

---

## Additional information

The following commands are available through telnet:

- **commands**: Lists all the commands that are available in the SBRM CLUI
- **help [command]**: Displays information on the command, or all commands if no command is specified
- **exit** or **quit**: exits the SBRM CLUI
- **query status**: Displays the status of the backup at a high level, for example, 'Backup in progress' or 'Backup failed'
- **query status**: Displays the status of the backup at a high level. For example, 'Backup in progress' or 'Backup failed'

- query history: Displays information about most recent backup. For example, 'Last backup executed <date> <time> successful'.
- query inventory: Displays the components available for backup
- precheck: Performs a basic sanity check to ensure the system is in a state to perform a backup. For example, disk space check and subtending application health if applicable
- stopprov: Stops the provisioning process
- dumpdata: Backs up the critical data
- startprov: Starts the provisioning process (if stopped)
- verify: Checks the validity of the backed up data. For example, validates the database data
- activatenew: Marks the new backup data as the current backup

The following commands are not available through telnet:

- backup full: Performs a complete backup. If a failure is encountered, the process stops, and manual intervention is required to recover from the failure
- backup auto: Performs a complete backup. If a failure is encountered, the backup process will restore provisioning if it was stopped by the backup process
- backup abort: Aborts the backup after completion of the current step, and restarts provisioning if it was stopped by the backup process

## How to backup an XA-Core office image from disk to tape

### Application

Use this procedure to copy the office image files of an eXtended Architecture Core (XA-Core). Use this procedure to copy the office image files from a disk to a digital audio tape (DAT) cartridge in an XA-Core shelf.

### Interval

Perform this procedure each week or as indicated in the routine maintenance schedule for your office.

### Common procedures

There are no common procedures.

### Action

This procedure contains a summary flowchart and a list of steps. Use the flowchart to review the procedure. Follow the steps to perform this procedure.

#### How to backup an XA-Core office image from disk to tape

| Step              | Action                                                                                                                                                                                                  |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>At the MAP</b> |                                                                                                                                                                                                         |
| 1                 | To access the MAP CI level display, type:<br><code>&gt;QUIT ALL</code><br>and press the Enter key.<br>Example of a MAP response<br>CI:                                                                  |
| 2                 | To access the image table of contents (ITOC) user interface, type:<br><code>&gt;ITOCCI</code><br>and press the Enter key.<br>Example of a MAP response<br>ITOC User Interface is now active.<br>ITOCCI: |
| 3                 | To list the boot file for the XA-Core in ITOC, type:<br><code>&gt;LISTBOOTFILE XA</code><br>and press the Enter key.                                                                                    |



**Example of a MAP response**

Image table Of Contents for XA :

```

A Registered Generic Device File
L Date Time Name
R MM/DD/YYYY HH:MM:SS

0 * 05/17/1999 19:26:29 F02LIMAGE
IMG0517CY_CM

```

**Note:** The example of a MAP response identifies the autoload registered (ALR) image file by an asterisk (\*) in the ALR column. Each image file has an index number at the beginning of the tuple line. The ALR image in the example of a MAP response has an index number of 0. The XA-Core selects the ALR image file first to boot the switch. If the ALR image file does not boot the switch then the XA-Core selects the next image file. The next image file is by sequence of the index number from the top of the table.

- 4 To list the boot file for the message switch (MS) in ITOC, type

```
>LISTBOOTFILE MS
```

and press the Enter key.

**Example of a MAP response**

Image Table of Contents for MS :

```

A Registered Generic Device File
L Date Time Name
R MM/DD/YYYY HH:MM:SS

0 * 05/17/1999 19:26:29 F02LIMAGE
IMG0517CY_MS

```

- 5 Determine if the XA-Core and MS have image files that are autoload registered (ALR). The examples of a MAP response in steps <3> and <4> identify the ALR image files by an asterisk (\*) in the ALR column.

| If the image files are | Do      |
|------------------------|---------|
| ALR                    | step 6  |
| not ALR                | step 24 |

- 6 Record the names of the office image files for XA-Core and MS that are ALR. Also record the volume name that has these office image files The ALR image file is the file that you copy to the XA-Core tape.

**Note 1:** In the example of a MAP response in [step 3](#) , the name of the office image file for XA-Core is IMG0517CY\_CM. Image file IMG0517CY\_CM is ALR. Image file IMG0517CY\_CM is in volume F02LIMAGE.

**Note 2:** In the example of a MAP response in [step 4](#), the name of the office image file for the MS is IMG0517CY\_MS. Image file IMG0517CY\_MS is ALR. Image file IMG0517CY\_MS is in volume F02LIMAGE.

- 7 To quit the ITOCCI user interface, type:

>QUIT

and press the Enter key.

Example of MAP response

CI:

### At the shelf



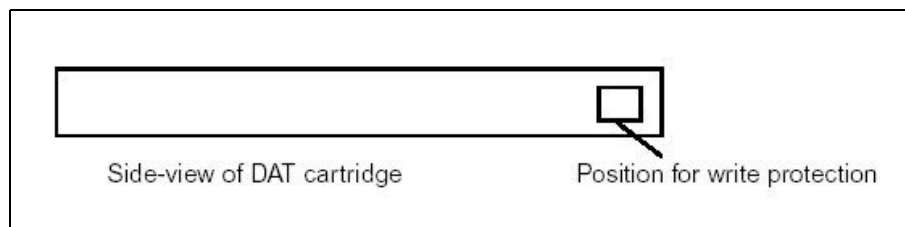
#### WARNING

##### Static electricity damage

Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP) when you handle the tape and packlet. The use of the wrist strap protects the packlets against damage caused by electrostatic discharge (ESD).

- 8 Determine from office records or office personnel if the DAT tape drive is clean. Refer to the XA-Core procedure 'How to clean the XA-Core tape drive' in the *XA-Core Maintenance Manual*, 297-8991-510.
- 9 Get a tape cartridge that has the approval of Nortel. Determine the tape planned for a backup of an office image. Determine the tape to use from the office records or from office personnel.
- 10 Make sure the tape write protection is at the position that permits recording (closed). The tape write protection is an entrance on one side of the tape that has a sliding door. The sliding door is open for write protection and closed to allow a write to the tape.

### Write protection of DAT cartridge



- 11 Insert the DAT tape cartridge into the XA-Core tape drive and close the drive door. The XA-Core tape drive is in the input/output processor (IOP) card of the XA-Core shelf.

**At the MAP****CAUTION****File of tape lost when formatted**

If the tape had files, the formatting of the tape loses the files. Make sure the tape has no files that your office needs.

- 12** To access the MAP disk utility, type:

```
>DISKUT
```

and press the enter key.

Example of a MAP response:

Disk utility is now active.

DISKUT:

- 13** To insert the tape in the MAP disk utility, type

```
>INSERTTAPE snp TAPE WRITELABEL label_name
```

and press the enter key.

where

**s** is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device

**nn** is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p** is the upper (U) or lower (L) packlet position of the IOP that has the tape device

**label\_name** is the alphanumeric name of the tape label that records the data. The name can be up to 32 characters long. If blank spaces are in the label name then enclose the label name with quotation marks.

Example of MAP input:

```
>INSERTTAPE F02UTAPE WRITELABEL IMAGE_1
```

Example of a MAP response

```
***** WARNING *****
Writing the label IMAGE_1 to tape volume
F02UTAPE on node CM will destroy all files
stored on this tape volume.
Do you want to continue?
Please confirm ("YES", "Y", "NO", or "N")
```

- 14** To confirm the command, type:

```
>YES
```

and press the enter key.

**Example of a MAP response:**

The INSERT operation may take up to 5 minutes to tension the tape.

A tape is now available to user on unit 0, node CM.  
Name IMAGE\_1 has been written to the tape label.

- 15** To list the files in the volume that contains the office image, type:

**>LISTFL vol\_name**

and press the enter key.

where

**vol\_name** is the name of the disk volume that contains the office image files

**Example of MAP input**

**>LISTFL F02LIMAGE**

**Example of a MAP response**

File information for volume F02LIMAGE:  
{NOTE: 1 BLOCK = 512 BYTES }

```

FILE NAME O R I O O V FILE MAX
NUM OF FILE LAST
 R E T P L L CODE REC
RECORDS SIZE MODIFY
 G C O E D D LEN
IN IN DATE
 C N FILE
BLOCKS

IMG0517CY_MS I F Y 0 1020
7542 15360 990517
IMG0517CY_CM I F Y 0 1020
165180 329728 990517

```

**Note:** A volume can have more files listed by command LISTVOLS than by command LISTFL in the MAP disk utility. The difference in the number of files between the commands is because of directory files not displayed by command LISTFL.

- 16** Begin the disk to tape backup process. To create a backup copy of the XA-Core image file, type:

**>BACKUP FILE file\_name snnp TAPE**

and press the Enter key.

where

**s** is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device  
**nn** is the number of the slot position on the XA-Core shelf for the IOP that has the tape device  
**p** is the upper (U) or lower (L) packlet position of the IOP that has the tape device

Example of MAP input:

```
>BACKUP FILE IMG0517CY_CM F02UTAPE
```

Example of a MAP response

FTFS file IMG0517CY\_CM on disk volume F02LIMAGE on node CM backed up as file IMG0517CY\_CM on tape device F02UTAPE on node CM.

| If the command was | Do      |
|--------------------|---------|
| successful         | step 17 |
| not successful     | step 24 |

- 17** To create a backup copy of the MS image file, type:

```
>BACKUP FILE file_name snnp TAPE
```

and press the enter key.

where

**file\_name** is the name of the MS image file that requires backup to tape  
**s** is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device  
**nn** is the number of the slot position on the XA-Core shelf for the IOP that has the tape device  
**p** is the upper (U) or lower (L) packlet position of the IOP that has the tape device

Example of MAP input

```
>BACKUP FILE IMG0517CY_MS F02UTAPE
```

Example of a MAP response

FTFS file IMG0517CY\_MS on disk volume F02LIMAGE on node CM backup up as file IMG0517CY\_MS on tape device F02UTAPE on node CM.

| If the command was | Do      |
|--------------------|---------|
| successful         | step 18 |
| not successful     | step 24 |

- 18** To check the backup copies of the image files on the tape, type

**>LISTFL snnp TAPE**

and press the enter key.

where

**s** is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device

**nn** is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p** is the upper (U) or lower (L) packet position of the IOP that has the tape device

Example of MAP input

**>LISTFL F02UTAPE**

Example of a MAP response

File information for tape volume F02UTAPE, node  
CM:

{Note: 1 BLOCK = 512 BYTES}

```

CREATE ORG FILE V FILE NUM OF REC FILE NAME
DATE TYPE CODE L SIZE IN RECORDS LEN
D BLOCKS IN FILE

```

```
990520 IMAG 0 329070 165180 1020 IMG0517CY_CM
990520 IMAG 0 15026 7542 1020 IMG0517CY_MS
```

- 19** To eject the tape from the MAP disk utility after the backup procedure completes, type

**>EJECTTAPE snnp TAPE**

and press the enter key.

where

**s** is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device

**nn** is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p** is the upper (U) or lower (L) packet position of the IOP that has the tape device

Example of MAP input

**>EJECTTAPE F02TAPE**

Example of a MAP response

The EJECT operation may take up to 5 minutes to position the tape to the beginning.

Rewind of tape F02UTAPE, unit 0, on node CM is completed.

This tape device is not available to the user now.

- 20** To exit the MAP disk utility and return to the MAP CI level, type  
>QUIT

and press the Enter key.

Example of a MAP response

CI:

***At the shelf***



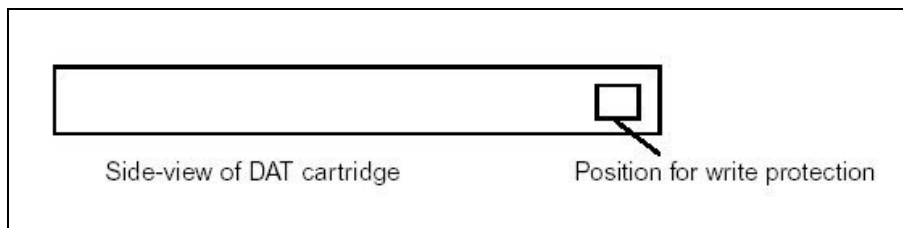
**WARNING**

**Static electricity damage**

Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP) when you handle the tape and packlet. The use of the wrist strap protects the packlets against damage caused by electrostatic discharge (ESD).

- 21** Remove the tape cartridge from the tape drive. Set the tape write protection to the position that does not permit recording (open). The tape write protection is an entrance on one side of the tape that has a sliding door. The sliding door is open for write protection and closed to allow a write to the tape.

**Write protection of DAT cartridge**



- 22** Store the tape cartridge per office procedure.
- 23** Go to step [25](#).
- 24** For additional help, contact the next level of support.
- 25** You have completed this procedure.

---

—End—

---

## Perform a manual backup of the Policy Controller database

### Purpose of this procedure

Use this procedure to perform a backup of the active Policy Controller unit Policy Controller application database. Use this procedure to make regular backup copies of the database or as a precautionary activity before starting any type of upgrade to the Policy Controller application. This procedure may be used as a standalone task or as part of a higher level upgrade activity.

### Limitations and Restrictions

#### ATTENTION

If you perform provisioning changes during this procedure, it can lead to database corruption and possible system outages. To ensure that you create an accurate and complete copy of the active unit database, verify that all provisioning changes are stopped before continuing this procedure.

### Prerequisites

#### ATTENTION

The Policy Controller database and the CS 2000 database must always be in sync. CS 2000 core images, CS 2000 GWC Manager Oracle database backups, and the Policy Controller application backups must always be maintained in sync for emergency recovery. To ensure they are in sync, perform images and backups at the same time.

### Action

| Step | Action |
|------|--------|
|------|--------|

#### *At the Policy Controller command line interface*

- |   |                                                                                                                                              |
|---|----------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Log onto the active Policy Controller unit and change to the root user.                                                                      |
| 2 | Change directory to the database directory by typing<br><pre># cd /opt/apps/database/solid/dbfiles</pre> and pressing the Enter key.         |
| 3 | Put a copy of the database for the active unit in the backup directory by typing<br><pre># cp solid.db /opt/apps/database/solid/backup</pre> |



and pressing the Enter key.

**Note:** If other backup copies of the database exist with the same filename, you have the option of deleting those files or putting the backup copy into the backup directory under a new file name.

**Example**

```
cp solid.db
/opt/apps/database/solid/backup/solid.db.backup1
```

- 4 For security purposes, ensure that a backup copy of the database file is transferred to a secure location.

Use the unix **scp** command to make a secure copy of the backup database file to a secure, remote server on your network. This server should be continuously available for cases where a restoration of the Policy Controller application database become necessary, such as during an upgrade rollback. A root password for the remote server may be required.

- 5 You have completed this procedure.

---

—End—

---

## Call Agent backup

The Call Agent uses two software loads. The first software load includes the platform software such as the operating system and system utilities. The second software load provides the call processing application.

This procedure describes how to make a backup of the call processing application. Images to be backed up are created either manually with the DUMP command, or automatically scheduled with entries in table IMAGEDEV and IMGSCHEDE.

---

### Step Action

---

#### At the MAP

- 1 List the available images to determine which image to backup. The image with the asterisk in the ALR column identifies the image that is set to Auto Load Record and is the image to backup.

```

CI:
>ITOC CI
ITOC User Interface is now active.
ITOC CI:
>LBF CM
Image Table Of Contents:
 A Registered Generic Device File
 L Date Time Name
 R MM/DD/YYYY HH:MM:SS

0 01/22/2003 10:29:53 SD00IMAGE1 SN04_JAN07_CM
1 01/22/2003 12:07:26 SD00IMAGE0 SN04_JAN22_CM
2 01/22/2003 13:00:50 SD00IMAGE0 BOTHELL 010903
3 * 01/30/2003 14:31:47 SD00IMAGE0 IMG_TO_BACKUP

```

#### At the Call Agent Manager

- 2 Log in to the inactive Call Agent and change directory to the location of the image.

The location of the image is identified by the value in the Generic Device column as follows:

#### /3PC

is prefixed in all cases

#### sd0x/

is taken from the first four characters in the Generic Device name

#### imagex/

is taken from the remaining characters in the Generic Device name

```
[mtc@hostname mtc]$ cd /3PC/sd00/image0
[mtc@hostname image0]$ ls -l IMG_TO_BACKUP
-rw-r--r-- 1 root root 225820860 Feb 27 11:37 IMG_TO_
[mtc@hostname image0]$
```

3

**ATTENTION**

Do not modify files at this level. Any modification to files must be completed through the MAP.

Open a file transfer protocol (FTP) session to the CS 2000 Core Manager and transfer the file.

```
[mtc@hostname image0]$ ftp <core_manager_ip>
Connected to <core_manager_ip>
220 <core_manager_ip> SFTP Server (Version 19.0.0.0 Nov 14
Name (<core_manager_ip>:mtc): root
Password: <root_passwd>
230 User root logged in.
ftp> bin
200 Type set to I.
ftp> cd /swd/3pc
250 CWD command successful.
ftp> put IMG_TO_BACKUP
local: IMG_TO_BACKUP remote: IMG_TO_BACKUP
227 Entering Passive Mode (10,40,44,6,195,224)
150 Opening data connection for IMG_TO_BACKUP (binary mode)
226 Transfer complete.
225820860 bytes sent in 332 secs (6.7e+02 Kbytes/sec)
ftp> bye
221 Goodbye.
```

**At the SDM**

4 Insert a DAT cassette.

**At the CS 2000 Core Manager**

5 Verify that the size of the transferred file is the same as in [step 2](#) and copy the file to tape.

```
cd /swd/3pc
ls -l
total 19816
-rw-r--r-- 1 swld swld 1527 Feb 27 12:40 000167C42C
-rw-r--r-- 1 swld swld 1527 Feb 26 17:58 000F07C430
-rw-rw-rw- 1 ftpuser maint 225820860 Feb 21 09:56 IMG_TO_B
tar cvf /dev/rmt0 IMG_TO_BACKUP
```

**Note:** Use the `rvf` argument to append to the tape. After the backup completes, optionally verify the integrity of the backup by using `tar tvf /dev/rmt0` to view the contents of the tape.

- 6 Use the `rm` command to erase the oldest image so the volume does not fill up.
- 7 This procedure is complete.

---

—End—

---

---

## Backing up files to a DVD-RW

---

### Application

Use this procedure to copy office images or all the files from a disk volume to a digital video disk read write optical disk (DVD-RW).

Rewritable DVDs (DVD+RW) will not work. Use a blank DVD-RW.



#### CAUTION

##### Maximum one volume per DVD-RW

Copy no more than one volume onto a DVD-RW. To copy multiple volumes, use a separate DVD-RW for each volume.

### Interval

Perform this procedure when required by your office.

### Common procedures

The UNIX commands `mkisofs` and `cdwr` are used. For information about these commands, type `man mkisofs` or `man cdwr` at a terminal prompt.

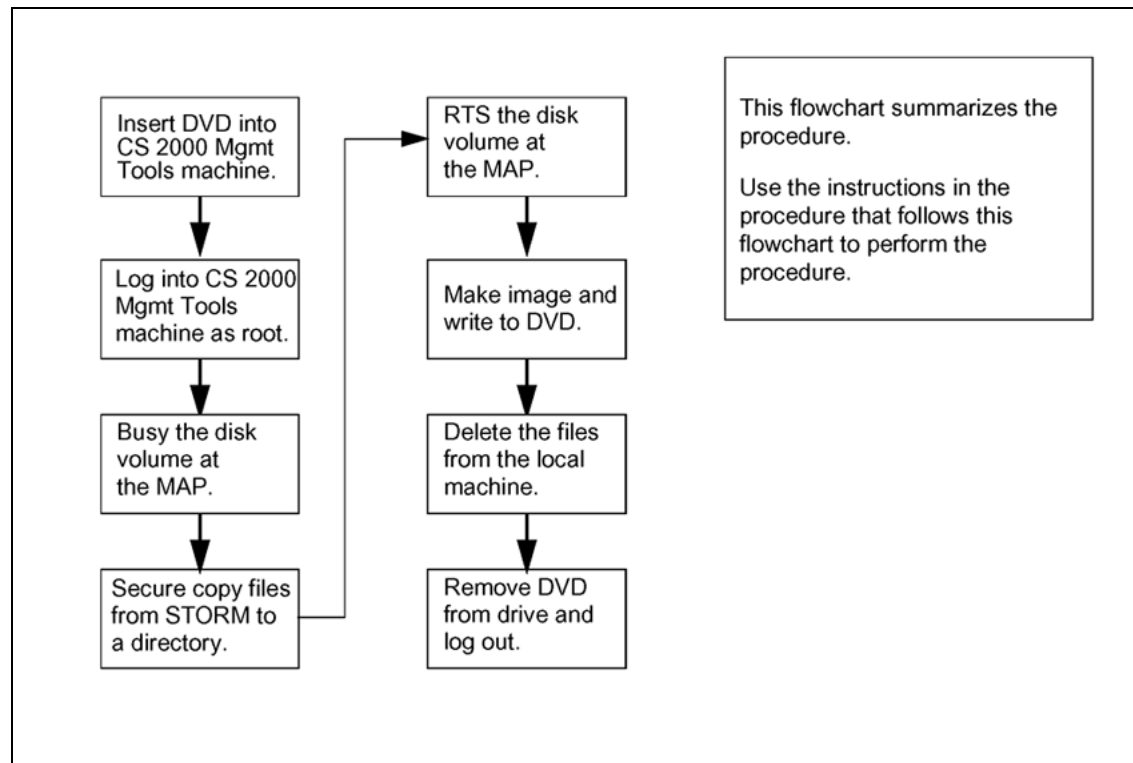
The IP addresses of the STORM units are determined in [step 1](#). The root password for STORM is needed. The root password for the CS 2000 Management Tools server is needed.

### Prerequisite

You need one or more blank DVD-RW disks to store the data.

### Action

This procedure contains a summary flowchart as a summary of the procedure. Follow the exact steps to perform this procedure.

**Summary of backing up files to a DVD-RW****Backing up files to a DVD-RW****Step Action****At the Call Agent Manager**

- 1 Quit the maintenance application and then use the mount command to determine the IP addresses of the STORM units.

```
> quit all
[mtc@ip_address mtc]$ mount
```

Determine which STORM unit provides sd00 and which provides sd01. This information is needed in [step 11](#).

```
[mtc@10.40.44.67 mtc]$ mount
/dev/ram0 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0622)
10.40.44.238:/nfsserv/3pc/mtc/tape0 on /TAPE type nfs (rw,rsiz=4096...
10.40.44.239:/nfsserv/3pc/mtc/tape1 on /TAPE1 type nfs (rw,rsiz=409...
10.40.44.238:/nfsserv/3pc/cs/sd00 on /3PC/sd00 type nfs (rw,rsiz=409...
10.40.44.239:/nfsserv/3pc/cs/sd01 on /3PC/sd01 type nfs (rw,rsiz=409...
10.10.11.238:/nfsserv/3pc/mtc/log0 on /var/log_mate type nfs (rw,rsi...
10.40.44.239:/nfsserv/3pc/mtc/log1 on /var/log type nfs (rw,rsiz=409...
```

**At the CS 2000 Management Tools server**

2

**CAUTION****Maximum one volume**

Copy only one volume onto a DVD-RW. To copy multiple volumes, use a separate DVD-RW for each volume.

Determine the volume to backup. Determine the volume from office records or from office personnel. Record the volume name.

- 3 Insert a DVD-RW into the DVD tray. If the CS 2000 Management Tools server is a pair of Sun Microsystems Netra 240 machines, put the DVD-RW into the machine with a lit USER LED on the faceplate.

**At a CS 2000 Management Tools server terminal**

- 4 Log in as a maintenance level user such as the maint user. Root permissions are used later in this procedure to write the DVD.

- 5 Change directory to /data and create a temporary directory to store the files:

```
$ cd /data
$ mkdir tmp
```

Do not change directory into tmp now. The tmp directory will hold the data to backup.

- 6 Determine the environment shell:

```
$ env | grep SHELL
SHELL=/bin/ksh
```

- 7 Set a filesize creation limit for this instance of the shell. Choose the **one** that is applicable to your shell. /bin/ksh is the default shell:

for /bin/ksh:

```
$ ulimit -f 2929688
```

for /bin/bash:

```
$ ulimit -f 1464844
```

for /bin/csh:

```
$ limit filesize 1500 megabytes
```

**At the MAP**

## 8 Determine the approximate size of the image or volume:

| Data to backup   | How to determine size                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |           |                  |        |        |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------------|--------|--------|------|------|--|------------------|-----|---------|------|--------|--|-------------|-----|----|----|------|--|-----|--|------|--------|--|------------------|-----|-------|-----|----|--------|------------------|-------|--------|--------|--------|--------|------------------|-------|--------|------|-------|--------|
| image            | <p>Listfile the volume that the image is in:</p> <pre>&gt; DISKUT; LF &lt;vol_name&gt;</pre> <div><pre>&gt; LF SD00ADUMP0</pre><p>File information for volume SD00ADUMP0:<br/>{NOTE: 1 BLOCK = 512 BYTES }</p><table><thead><tr><th>FILE NAME</th><th>O R I O O V FILE</th><th>MAX</th><th>NUM OF</th><th>FILE</th><th>LAST</th></tr><tr><th></th><th>R E T P L L CODE</th><th>REC</th><th>RECORDS</th><th>SIZE</th><th>MODIFY</th></tr><tr><th></th><th>G C O E D D</th><th>LEN</th><th>IN</th><th>IN</th><th>DATE</th></tr><tr><th></th><th>C N</th><th></th><th>FILE</th><th>BLOCKS</th><th></th></tr></thead><tbody><tr><td>S040210135002HIS</td><td>O V</td><td>0 255</td><td>276</td><td>27</td><td>040210</td></tr><tr><td>S040210135002_CM</td><td>I F Y</td><td>0 1020</td><td>220288</td><td>438855</td><td>040210</td></tr><tr><td>S040210135002_MS</td><td>I F Y</td><td>0 1020</td><td>7803</td><td>15546</td><td>040210</td></tr></tbody></table></div> <p>The approximate size of the image in megabytes is NUM OF RECORDS IN FILE / 1000:</p> <p><b>220288 / 1000 = 220 MB</b></p> | FILE NAME | O R I O O V FILE | MAX    | NUM OF | FILE | LAST |  | R E T P L L CODE | REC | RECORDS | SIZE | MODIFY |  | G C O E D D | LEN | IN | IN | DATE |  | C N |  | FILE | BLOCKS |  | S040210135002HIS | O V | 0 255 | 276 | 27 | 040210 | S040210135002_CM | I F Y | 0 1020 | 220288 | 438855 | 040210 | S040210135002_MS | I F Y | 0 1020 | 7803 | 15546 | 040210 |
| FILE NAME        | O R I O O V FILE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | MAX       | NUM OF           | FILE   | LAST   |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
|                  | R E T P L L CODE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | REC       | RECORDS          | SIZE   | MODIFY |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
|                  | G C O E D D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | LEN       | IN               | IN     | DATE   |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
|                  | C N                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           | FILE             | BLOCKS |        |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
| S040210135002HIS | O V                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 0 255     | 276              | 27     | 040210 |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
| S040210135002_CM | I F Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 0 1020    | 220288           | 438855 | 040210 |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
| S040210135002_MS | I F Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 0 1020    | 7803             | 15546  | 040210 |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |
| volume           | <p>Listvols the volume with the megabyte option:</p> <pre>&gt; DISKUT; LV SD00TEMP MB</pre> <p>Subtract FREE MBYTES from TOTAL MBYTES to determine the approximate size of the volume:</p> <p><b>400 - 340 = 60 MB</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |           |                  |        |        |      |      |  |                  |     |         |      |        |  |             |     |    |    |      |  |     |  |      |        |  |                  |     |       |     |    |        |                  |       |        |        |        |        |                  |       |        |      |       |        |

## 9 If backing up an entire volume, enter the DISKADM level and busy the volume:

```
> QUIT ALL
> DISKADM <sd0x>; BSY <volname>
```



> QUIT

**sd0x**

is SD00 or SD01

**volname**

is the name of the volume such as TEMP or ADUMP0

*The BSY command fails if applications have open files on any volume for the device. A busied disk may affect data recording or retrieval for applications. RTS the volume as soon as possible or convenient after copying the files.*

*If applications are active and writing to the volume, determine if the application can ROTATE the disk writing activity to a backup volume. If unsure, contact your next level of support.*

#### At a CS 2000 Management Tools server terminal

- 10** Ensure that enough disk space is available for the data to record. Twice the space determined in [step 8](#) is needed:

```
$ df -k /data
```

*The free space on the device that /data is mounted is printed. The value for "avail" is the number of free kilobytes. Divide that number by 1000 to determine the number of free megabytes. Ensure that there is free space for two times the size of the data to record.*

```
$ df -k /data
```

| Filesystem      | kbytes  | used  | avail   | capacity | Mounted on |
|-----------------|---------|-------|---------|----------|------------|
| /dev/md/dsk/d20 | 3082223 | 14412 | 2876454 | 5%       | /data      |

2876454 / 1000 = 2876 MB free

- 11** Secure copy the files from the STORM unit to the /data/tmp directory created in [step 5](#). Enter the root password for the STORM unit when prompted:

```
$ scp -r "root@<stormip>:</path_to_files>" /data/tmp
```

Note that there is a space before the /data/tmp argument.

**stormip**

is the IP Address of the STORM unit such as 10.40.44.238. Use the value determined in [step 1](#).

**/path\_to\_file**

is the absolute path to the files on the STORM unit to copy such as /nfsserv/3pc/cs/sd00/temp/\*

**Example**

Copy an office image named S040210135002\_CM from SD00ADUMP0:

```
$ scp -r "root@<stormip>:/nf-
sserv/3pc/cs/sd00/adump0/S040210135002_CM"
/data/tmp
```

The first time this command is issued, the secure copy program provides a prompt to exchange keys. Confirm the exchange with a "yes." The root password for the STORM unit is needed.

*The secure copy program provides a progress indicator during the copy. Wait for the copy to complete and the \$ prompt to return.*

**At the MAP**

- 12** If the volume was busied in [step 9](#), enter the DISKADM level and RTS the copied volumes:

```
> DISKADM <sd0x>; RTS <volname>
> QUIT
```

**At a CS 2000 Management Tools server terminal**

- 13** If only image files are transferred, and the files do not end in \_CM or \_MS, rename the files to include the file attributes IMG and 1020:

```
$ mv <image_filename> <image_filename>.IMG1020
```

**Example**

```
$ mv raleigh_04wk06 raleigh_04wk06.IMG1020
```

If the name of the image already ends in \_CM or \_MS, skip this step.

- 14** Change directory out of /data/tmp and make an ISO9660 image named dvdimage.iso with Rock Ridge extensions from the files in tmp:

```
$ cd /data
$ mkisofs -R -o /data/dvdimage.iso -r /data/tmp
```

*Status is printed to the terminal:*

**Create dvdimage.iso with mkisofs command**

```
$ mkisofs -R -o /data/dvdimage.iso -r /data/tmp
4.56% done, estimate finish Tue Feb 10 14:52:00 2004
9.11% done, estimate finish Tue Feb 10 14:52:00 2004
13.67% done, estimate finish Tue Feb 10 14:52:00 2004
...
95.67% done, estimate finish Tue Feb 10 14:52:05 2004
Total extents actually written = 109764
Total translation table size: 0
Total rockridge attributes bytes: 421
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 8000
109764 extents written (214 Mb)
$
```

- 15** Become the root user:

```
$ su - root
```

Provide the root password at the prompt.

- 16** Optionally verify the ISO9660 image:

```
lofiadm -a /data/dvdimage.iso /dev/lofi/1
mount -F hsfs /dev/lofi/1 /mnt
ls -asl /mnt
```

*The contents of the ISO 9660 image are displayed. These files will be written to the DVD-RW. Ensure the display looks similar to the following image.*

If the lofiadm command reports the error "lofiadm: could not map file /data/dvdimage.iso to /dev/lofi/1: Device busy," then the first loopback file driver is already in use. Reenter the command and substitute /dev/lofi/2 for /dev/lofi/1. Continue incrementing the number until the command succeeds and then use the successful value in the mount command.

If the mount command reports the error "mount: /dev/lofi/1 is already mounted, /mnt is busy, or allowable number of mount points exceeded," unmount the /mnt directory with the **umount /mnt** command and reenter the mount command.

**List contents of the ISO 9660 image**

```
lofiadm -a /data/dvdimage.iso /dev/lofi/1
mount -F hsfs /dev/lofi/1 /mnt
ls -asl /mnt
total 431996
 4 dr-xr-xr-x 2 root sys 2048 Apr 20 09:48 .
 2 drwxr-xr-x 33 root root 1024 Apr 20 11:16 ..
431990 -rw-r--r-- 1 maint maint 221178840 Apr 20 09:47 IMG_TO_BACKUP.img1
```

- 17** Determine the name of the DVD-RW device:

```
cdrw -l
```

*All optical disk devices are printed.*

**Determine the DVD-RW device name**

```
cdrw -l
Looking for CD devices...
 Node Connected Device Device type
-----+-----+-----
cdrom0 | TOSHIBA DVD-ROM SD-R6012 1033 | CD Reader/Writer
```

If the command responds with "No CD writers found or no media in the drive," and the CS 2000 Management Tools server is a cluster then verify that the DVD-RW is placed in the active unit. The active unit is identified by a lit USER LED on the face of the unit.

- 18** Optionally simulate (-S flag) recording the image to verify that the ISO 9660 image can be recorded on the DVD-RW. This step requires approximately 10 minutes:

```
cdrw -d <dvd_dev> -S -i /data/dvdimage.iso
```

**Example**

```
cdrw -d cdrom0 -S -i /data/dvdimage.iso
```

*The CDROM tray ejects after this simulation. **Close the CDROM tray and continue this procedure to write the DVD-RW.***

- 19** Record the image. This step requires approximately 10 minutes:

```
cdrw -d <dvd_dev> -i /data/dvdimage.iso
```

**Example**

```
cdrw -d cdrom0 -i /data/dvdimage.iso
```

*If the error response "Media in the device is not writable" is returned, verify that the CDROM tray is closed.*

*Approximately two minutes pass before progress is printed to the screen. After the first 1% is written, each additional percent requires about two seconds.*

#### CDRW command progress

```
cdrw -d cdrom0 -i /data/dvdimage.iso
Initializing device...done.
Preparing to write DVD
Writing track 1 ... 99 %
```

*Approximately nine minutes pass before the command completes.*

```
done.
done.
Finalizing (Can take up to 4 minutes)...done.
$
```

*The CDROM tray on the CS 2000 Management Tools server ejects. Close the CDROM tray and continue this procedure to verify the contents of the DVD-RW.*

- 20** Check that ISO9660 image recorded correctly:

```
ls -asl /cdrom/cdrom
```

*The contents of the DVD-ROM are printed.*

- 21** Unmount the DVD-RW, eject it, and exit from root privilege:

```
eject cdrom
```

If the ISO 9660 image was verified with the `lofiadm` command, remove the loopback file driver device:

```
umount /mnt
lofiadm -d /dev/lofi/1
```

If `/dev/lofi/2` was used above, substitute `/dev/lofi/2` in this command.

Exit from root privilege:

```
exit
$
```

*The dollar sign command prompt returns.*

- 22** Remove the local copies of the files:

```
$ rm /data/tmp/*
$ rm /data/dvdimage.iso
```

**At the CS 2000 Management Tools server**

- 23 Remove the DVD-RW from the tray and close the tray. Label the DVD-RW.
- 24 Store the DVD-RW per office procedure.
- 25 This procedure is complete.

---

—End—

---

## Backing up the SST

By default, the unit performs a backup of the database and critical files every day at 1:00 AM. Refer to ["Rescheduling backup time" \(page 101\)](#) to alter the schedule.

The contents of the backup are stored locally on each unit in the `/data/bkresmgr/backup` directory in tape archive (tar) format.

Security related files are not automatically backed up. Refer to ["Backing up security related files manually" \(page 102\)](#).

### Purpose of this procedure

Use this procedure to make a manual backup or change the backup time.

### Limitations and Restrictions

#### ATTENTION

SIP Gateway application provisioning activities must be suspended during the time of the database backup in order to ensure that an accurate and complete copy of the active unit database is created. However, call processing is not affected and there is no enforcement in the database to prevent provisioning.

Security related files must be backed up manually.

### Prerequisites

#### ATTENTION

The SIP Gateway application database must be in sync with the CS 2000 to ensure an accurate copy of the active unit database is created. Verify this condition using procedure ["Verifying synchronization status" \(page 105\)](#).

### Making a backup

Follow this procedure to make an immediate backup.

| Step | Action |
|------|--------|
|------|--------|

#### *At the NCGL CLI or IEMS client*

- 1 Log on to the **ACTIVE** unit and change to the root user.
- 2 Execute the command to make the backup by typing  
`/opt/apps/db_install/sd/bkup_ngss.sh`  
and pressing the Enter key.

The following output is printed to the screen and the backup is recorded to /data/bkresmgr/backup.

#### bkup\_ngss.sh response

```

- Move files

- Backup Solid database -

- Copy certificate files to backup directory -

- Copy commish files to backup directory -

- Copy web files to backup directory -

- Creating Meta-Data File Listing -

- Waiting for Solid DB to complete backup -

- Waiting for Solid DB to complete backup -

- Solid DB backup complete -

tar: Removing leading `/' from absolute path names in the archive
data/bkresmgr/temp/
```

← The backup pauses at this point while the database is backed up.

```
data/bkresmgr/temp/
data/bkresmgr/temp/gen_cert.txt
data/bkresmgr/temp/server.crt
data/bkresmgr/temp/trusted.crt
data/bkresmgr/temp/hosts
data/bkresmgr/temp/ntp.conf
data/bkresmgr/temp/ifcfg-eth0
data/bkresmgr/temp/netnodes
data/bkresmgr/temp/group
data/bkresmgr/temp/passwd
data/bkresmgr/temp/shadow
data/bkresmgr/temp/ssh_host_dsa_key.pub
data/bkresmgr/temp/ssh_host_key.pub
data/bkresmgr/temp/ssh_host_rsa_key.pub
data/bkresmgr/temp/server.xml
data/bkresmgr/temp/redirect.jsp
data/bkresmgr/temp/redirect_SSDFS.jsp
data/bkresmgr/temp/redirect_no-SSDFS.jsp
data/bkresmgr/temp/redirect_apps.php
data/bkresmgr/temp/META-DATA.txt
data/bkresmgr/temp/hostname.txt
data/bkresmgr/temp/solid.db
data/bkresmgr/temp/solid.ini
data/bkresmgr/temp/solmsg.out
```

The backup filename is located in /data/bkresmgr/backup and is identified by hostname, date, and time as indicated in the following example:



**Example**

*unit0.backupfile.2005-04-12\_17-10.tgz*

- 3 For security purposes, ensure that a copy of the backup file is transferred to a secure location.  
  
Use the **scp** command to make a secure copy of the backup file to a secure, remote server on your network. This server should be continuously available for cases where a restoration of the unit become necessary, such as during an upgrade rollback.
- 4 If security related files should be backed up, refer to ["Backing up security related files manually" \(page 102\)](#).
- 5 Repeat this procedure on the second unit.

---

—End—

---

## Rescheduling backup time

Each unit performs an automatic backup at 1:00 AM daily. Use the following procedure to change the schedule.

---

| Step | Action |
|------|--------|
|------|--------|

---

*At the NCGL CLI or IEMS client*

- 1 Log onto the unit and change to the root user.
- 2 Remove the existing backup schedule from the crontab by typing  
`/opt/apps/db_install/sd/uninstallBkres.sh`
- 3 Edit the backup schedule file by typing  
`vi /opt/apps/db_install/sd/backup.cron`  
*The file is opened for editing.*

```
Cron data file for NGSS Backup timings
0 1 * * * /opt/apps/db_install/sd/bkup_ngss.sh
```

- 4 Modify the first five fields (indicated by "0 1 \* \* \*" in the example). The fields are identified in order from left to right:
  - minute -- the minute of the hour that the command will run, values are 0 to 59
  - hour -- the hour of the day the command will run, values are 0 to 23 with 0 being midnight

- day -- the day of the month the command will run, values are 1 to 31, an asterisk indicates to run the command all days
- month -- the month of the year the command will run, values are 0 to 12, an asterisk indicates to run the command all months
- weekday -- the day of the week that the command will run, values are 0 to 6, with 0 being Sunday, an asterisk indicates to run the command all weekdays

Do not modify the sixth field (/opt/.../bkup\_ngss.sh).

When done, write and quit the file.

- 5 Install the newly created schedule in the crontab by typing  
`/opt/apps/db_install/sd/installBkres.sh`
- 6 After the scheduled time, verify that a backup file is created in the `/data/bkresmgr/backup` directory and that it is created at the new time, not the previously scheduled time.
- 7 Repeat this procedure on the second unit.

---

—End—

---

## Backing up security related files manually

The automatic backup does not backup the certificate.keystore or key files. This guards against loss or theft of the backup which would compromise the key without the operating company personnel knowing about the breach.

Copy the following files to a safe location:

- /opt/base/share/ssl/certificate.keystore
- /opt/base/share/ssl/gen\_cert.txt
- /opt/base/share/ssl/server.crt
- /opt/base/share/ssl/server.key
- /opt/base/share/ssl/trusted.crt
- /opt/base/synch\_local/common/etc/ssh/ssh\_host\_dsa\_key
- /opt/base/synch\_local/common/etc/ssh/ssh\_host\_key
- /opt/base/synch\_local/common/etc/ssh/ssh\_host\_rsa\_key

The following procedure provides a suggestion of how to backup these security related files.

| Step | Action |
|------|--------|
|------|--------|

**At the NCGL CLI or IEMS client**

- 1 Log in to either unit (usually the unit where the latest version of security certificates are stored), and change to root user.
- 2 Change directories to the /opt/base/share/ssl directory:  
`cd /opt/base/share/ssl`
- 3 Create a new directory to store backup copies of the certificate files:  
`mkdir <SNxx_ddmmyyyy>`  
where  
`SNxx_ddmmyyyy` is the name of the new directory based on the currently installed release of the system software (for example SN08) and the current date in the format ddmmyyyy
- 4 Copy the certificates to the newly created backup directory:  
`cp * <SNxx_ddmmyyyy>`

**ATTENTION**

Completing this step ensures that you have valid backup copies of the security certificates for restoring in case of an upgrade abort or rollback or for disaster recovery purposes.

- 5 Use the following table to determine your next step:

| If                                                                                    | Do                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| you want to make backup copies of the security certificates to a remote server        | Ensure that the remote host that will store the security related files is secure, that the host is unavailable to general users, and offers restricted access to personnel with security related responsibilities. Proceed to <a href="#">Step 6</a> |
| you do not want to make backup copies of the security certificates to a remote server | This procedure is complete.                                                                                                                                                                                                                          |

- 6 Secure copy the files to the remote server:  
`cd <SNxx_ddmmyyyy>scp *<user>@<remote_server>:</path>`  
where  
`user` is a valid user ID on the remote server

`remote_server` is the IP address of the remote server  
`/path` is where the file will be located on the remote server  
*The files are copied to the remote server.*

---

—End—

---

## Verifying synchronization status

### Purpose of this procedure

Use this procedure to determine the synchronization status of the two units.

### Limitations and restrictions

There are no restrictions for performing this procedure.

### Prerequisites

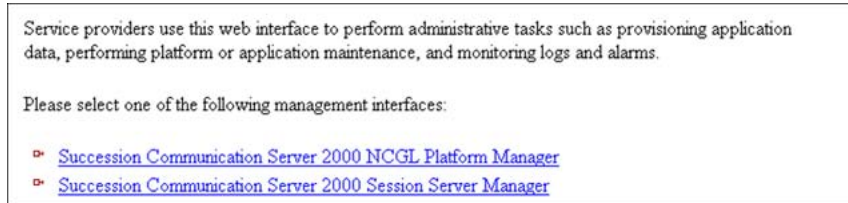
There are no prerequisites for performing this procedure.

### Action

| Step                                                        | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>At the CS 2000 Session Server Manager or IEMS client</i> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 1                                                           | Select <b>Carrier VoIP Communication Server 2000 Session Server Manager</b> from the launch point menu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                                                             |  <p>Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.</p> <p>Please select one of the following management interfaces:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Succession Communication Server 2000 NCGL Platform Manager</a></li> <li>▪ <a href="#">Succession Communication Server 2000 Session Server Manager</a></li> </ul> |
| 2                                                           | Select <b>Session Server &gt; Maintenance &gt; Application &gt; SIP Gateway</b> from the left side menu:                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                                             |  <p>The screenshot shows a tree view of the management interface. The path 'Session Server &gt; Maintenance &gt; Application &gt; SIP Gateway' is highlighted. The 'SIP Gateway' item is circled in red.</p>                                                                                                                                                                                                                                                                                  |
| 3                                                           | At the bottom of the SIP Gateway Maintenance panel, locate and click the <b>QueryInfo</b> button.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

*At the CS 2000 Session Server Manager or IEMS client*

- 1 Select **Carrier VoIP Communication Server 2000 Session Server Manager** from the launch point menu.



Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select **Session Server > Maintenance > Application > SIP Gateway** from the left side menu:



- 3 At the bottom of the SIP Gateway Maintenance panel, locate and click the **QueryInfo** button.

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| UnLocked             | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                |                                         |
|--------------------------------------------------------|-----------------------------------------|
| Administrative                                         | Control                                 |
| <div>Lock</div> <div>UnLock</div> <div>Shut Down</div> | <div>Suspend</div> <div>UnSuspend</div> |
| Refresh                                                | QueryInfo                               |

- 4 The synchronization status of the units is displayed at the bottom of the query results panel.

If the units are not in sync, check for alarm conditions.

|                                                 |
|-------------------------------------------------|
| Last Performed Operation: Query Number of Calls |
| Result: Passed                                  |
| Number Of Active Calls: 0                       |
| SIP Gateway is: In Sync                         |
| SIP Gateway Cold SwAct                          |

- 5 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

## Saving the Ethernet Routing Switch 8600 boot configuration file

The Ethernet Routing Switch 8600 boot configuration can be saved to a file using the Boot Monitor Command Line Interface (CLI). You must have access to the Boot Monitor CLI through a direct connection to the switch or a Telnet connection. For more information on accessing the Boot Monitor CLI, refer to 'Managing the Ethernet Routing Switch 8000 Series Switch Using the Command Line Interface Release 3.2,' 313194-\*

**Note:** You must be directly connected to the switch to initiate a Boot Monitor session. You can connect using a Telnet connection only if the Boot Monitor CLI is already active.

### Save the boot configuration

| Step                           | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>At the Boot Monitor CLI</i> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 1                              | <p>Issue the save command by typing</p> <pre>monitor# save &lt;save_type&gt; [file &lt;value&gt;] [verbose] [standby &lt;value&gt;] [backup &lt;value&gt;]</pre> <p>where</p> <p><b>save_type</b></p> <p>specifies what to save. Possible values for this parameter are config, bootconfig, log, and trace.</p> <p><b>file &lt;value&gt;</b></p> <p>is a filename in one of the following formats:</p> <ul style="list-style-type: none"> <li>• [a.b.c.d]: &lt;file&gt;</li> <li>• /pcmcia/&lt;file&gt;</li> <li>• /flash/&lt;file&gt;</li> </ul> <p><b>verbose</b></p> <p>saves default and current configuration. if you omit this parameter, only parameters you have changed are saved.</p> <p><b>standby &lt;value&gt;</b></p> <p>saves the specified file name to the standby CPU (currently not supported)</p> |

**backup <value>**

saves the specified file name and identifies the file as a backup file

Example

```
save config file ralph.cfg backup 2
```

**Note:** To save a file to the standby CPU, you must enable TFTP on the standby CPU. To enable TFTP, enter flags tftpd true in the Boot Monitor CLI or config bootconfig flags tftpd true in the Run-Time CLI.

**2** You have completed this procedure.

---

—End—

---



## Backing up UAS configuration files

All configuration data supporting the operation of the UAS is stored in configuration files. The configuration files include:

- uas.conf - containing configuration parameters that support the function of the UAS, including CG6000C card settings, Call Agent definition, APS hostname definition, network element settings, and conferencing service state definition
- ugw.conf - containing trunk configuration information for PRI Solutions
- snmpd.cnf - containing parameters that support the SNMP function, including management station address, SNMP user names, community names, and trap version
- hosts - containing parameters that support the function of the APS, including APS hostname and IP address
- atmhard.con - containing ATM bearer interface settings that link a local port ATM address to a particular ATM interface port
- atmconn.con - containing ATM bearer connections settings that provide the UAS with a remote gateway's name and ATM address
- mainsa.conf - containing Main Subagent program settings specifying the kinds of error and log messages to be sent to the management station
- atmSvcProfile.con - containing data on Switched Virtual Channel (SVC) traffic parameters associated with AAL2 SVCs
- atmhardloop.con - containing information associated with the loopback of SVCs

At the time of installation, the UAS is configured to automatically back up configuration files each day at 2:00 am. If an APS node is configured in the network, all UAS nodes in the network can be backed up to the APS node. If an APS node is not configured in the network, the configuration files for UAS nodes in the network can be backed up, instead, to a remote UNIX server. This procedure enables you to set up automatic backup to a remote server.

## Backing up UAS configuration files

| Step | Action |
|------|--------|
|------|--------|

### *At the Windows desktop interface*

- |   |                                                                                                                                                     |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | This step, which applies specifically to a Sun Solaris system, enables you to set up automatic configuration file system backup to a remote server. |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------|

- a. Open a command interface by performing the following steps:

- select **Start -> Run**
- type `cmd` in the window that displays
- press Enter

- b. Open a telnet session to the remote UNIX server and log in as the Root user. Then enter:

```
cd /;mkdir /opt;chmod 777 opt
cd /opt;
mkdir uas;chmod 777 uas
cd uas;
mkdir uas_conf_backup;chmod 777
uas_conf_backup
cd /
cd /opt/uas/uas_conf_backup
```

- c. Configure NFS to share the "/opt/uas" filesystem and start the NFS server:

```
echo "share -F nfs /opt/uas" >>
/etc/dfs/dfstab
```

**Note:** The commands from this point forward are specific for a Sun Solaris system.

```
/etc/init.d/nfs.server start
```

- d. Create a user login called "Administrator" that does not require a password:

```
/usr/sbin/useradd -d
/export/home/Administrator -g 1 -s /bin/ksh -m -u
1002 Administrator 2> /dev/null

passwd -d Administrator 2> /dev/null
```

- 2 At the local system console, enter the IP address of the remote server in the "Backup Storage IP" field of the Local Configuration Interface GUI screen, using the procedure "Modifying configuration parameters through the Local Configuration Interface GUI" in the document, NN10095-511, entitled "UAS Configuration Management."
- 3 You have completed this procedure.

---

—End—

---

## Restoring UAS configuration files

At the time of installation, the UAS is configured to automatically back up configuration files each day at 2:00 am. If an APS node is configured in the network, all UAS nodes in the network can be backed up to the APS node. If an APS node is not configured in the network, the configuration files for UAS nodes in the network can be backed up, instead, to a remote UNIX server.

The backed-up files can be restored should a catastrophic system event, such as a hard disk drive failure, create the need for a re-installation. The files are restored by manually transferring the files from the APS node or remote UNIX server to the UAS node after the UAS software (and NGS software, if necessary) has been re-installed. The backed-up files are located in the directory, /opt/uas/uas\_conf\_backup and include:

- C:\UAS\etc\UAS.conf (all configurations)
- C:\UAS\etc\ugw.conf (for a PRI gateway only)
- C:\UAS\etc\atmconn.con (ATM only)
- C:\UAS\etc\main.sa.conf (all configurations)
- C:\UAS\etc\atmhard.con (ATM only)
- C:\etc\srconf\agt\snmpd.cnf (all configurations)
- C:\Winnt\system32\drivers\etc\hosts (all configurations)
- C:\UAS\etc\atmSvcProfile.con (ATM only)
- C:\UAS\etc\atmhardloop.con (ATM only)

This procedure enables you to restore backed-up UAS configuration files that are stored either on an APS node or on a remote UNIX server.

## Restoring UAS configuration files

| Step | Action |
|------|--------|
|------|--------|

### ***At the Network Element Status panel of the Universal Audio Server Manager***

- |   |                                                                                                                                                 |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | In the Network Elements pane, select the appropriate UAS node.<br><i>Information about the node displays in the System Identification pane.</i> |
| 2 | In the pull-down list in the box labeled, "Please select," select Maintenance.                                                                  |
| 3 | In the Maintenance Tree pane, select "Node".                                                                                                    |

- 4 Click the node entry that displays in the table shown in the Node States pane.
- 5 Lock the node by clicking the "Lock Graceful" button located at the bottom of the Node States pane.

***At the Windows desktop interface***

- 6 Log in as Administrator.
- 7 Stop any applications that are running.
  - a. Access the "Services" window as follows:  
select **Start -> Programs -> Administrative Tools -> Services**
  - b. Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.
- 8 Perform the following steps:
  - a. Enter the following command:  
`cd\UAS\etc`
  - b. Access the APS server directory containing the backed up configuration files by entering the following:  
`mount * \\ <APS IP address>  
\opt\uas\uas_conf_backup\ <UAS node>  
\current (all of this command is entered on  
one line)`  
where  
  
`<APS IP address>` is the address of the server containing the backed up configuration files, and  
`<UAS node>` is the full directory path that contains the name of the UAS node that you are restoring the backed up configuration files to.
  - c. Execute the following command to confirm that the directory containing the backed-up configuration files is mounted:  
`net use`
  - d. Change directories to the location of the newly mounted configuration file backup directory by entering the following:  
`cd <mounted drive letter>`  
where  
  
`<mounted drive letter>` is the drive letter (for example, "F") displayed as the result of the previous command.

- e. List the contents of the configuration file backup directory by entering the following command in response to the prompt:

```
ls -l
```

The following backed up files should display:

- UAS.conf (for all configurations)
- ugw.conf (for a PRI gateway only)
- atmconn.conf (for ATM only)
- mainsa.conf (for all configurations)
- atmhard.conf (for ATM only)
- snmpd.cnf (for all configurations)
- hosts (for all configurations)
- atmSvcProfile.conf (for ATM only)
- atmhardloop.conf (for ATM only)

- f. Enter the following command to copy the contents of the mounted configuration file backup directory to the appropriate subdirectory on your UAS:

```
copy *.* c:\UAS\etc\
```

- g. Unmount the configuration file backup directory by entering the following command:

```
umount <drive letter>
```

where

<drive letter> is the drive letter that you entered in step d.

- h. At the system console, perform the following steps:

```
mv snmpd.cnf \etc\srconf\agt\snmpd.cnf
```

```
mv hosts \Winnt\system32\drivers\etc\hosts
```

- 9 Restart the network element by performing the following steps:

- a. Access the "Services" window as follows:

select **Start -> Programs -> Administrative Tools -> Services**

- b. Right-click PMGRdaemon service and select Start.

***At the Network Element Status panel of the Universal Audio Server Manager***

- 10 In the Network Elements pane, select the appropriate UAS node.

*Information about the node displays in the System Identification pane.*

- 11 In the pull-down list in the box labeled, "Please select," select Maintenance.
- 12 In the Maintenance Tree pane, select "Node".
- 13 Click the node entry that displays in the table shown in the Node States pane.
- 14 Unlock the node by clicking the "Unlock" button located at the bottom of the Node States pane.
- 15 You have completed this procedure.

---

—End—

---

## Restoring audio files to a UAS node

In the event that a re-installation of a UAS node is required due to an error condition, audio files must be restored to the unit when it becomes operational. This procedure allows you to enable audio provisioning to the node and to specify which audio files are to be restored to it.

**Note:** For more information about re-installation of a UAS node, contact your Nortel service representative.

### Restoring audio files to a UAS node

| Step                                                                                          | Action                                                                                                                                                                                                                                                                                                                                |    |    |                                                                                               |        |                                                              |        |
|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|-----------------------------------------------------------------------------------------------|--------|--------------------------------------------------------------|--------|
| <b>At your web browser interface</b>                                                          |                                                                                                                                                                                                                                                                                                                                       |    |    |                                                                                               |        |                                                              |        |
| 1                                                                                             | After the re-installation of the UAS node has been completed, determine whether you want to enable provisioning of the node occur during the next audio distribution cycle or immediately.                                                                                                                                            |    |    |                                                                                               |        |                                                              |        |
|                                                                                               | <table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>you want to enable provisioning of the node to occur during the next audio distribution cycle</td><td>step 2</td></tr> <tr> <td>you want audio provisioning of the node to occur immediately</td><td>step 3</td></tr> </table>                                                      | If | Do | you want to enable provisioning of the node to occur during the next audio distribution cycle | step 2 | you want audio provisioning of the node to occur immediately | step 3 |
| If                                                                                            | Do                                                                                                                                                                                                                                                                                                                                    |    |    |                                                                                               |        |                                                              |        |
| you want to enable provisioning of the node to occur during the next audio distribution cycle | step 2                                                                                                                                                                                                                                                                                                                                |    |    |                                                                                               |        |                                                              |        |
| you want audio provisioning of the node to occur immediately                                  | step 3                                                                                                                                                                                                                                                                                                                                |    |    |                                                                                               |        |                                                              |        |
| 2                                                                                             | Perform the procedure "Enabling provisioning of a UAS node" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite.<br><br><b>Note:</b> Provisioning of the node will begin during the next audio distribution cycle. The distribution cycle occurs once per hour.<br><br>a. Go to step 4. |    |    |                                                                                               |        |                                                              |        |
| 3                                                                                             | Perform the procedure "Provisioning a UAS node" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite.<br><br><b>Note:</b> Provisioning of the node will begin immediately although as much as a five-minute delay may occur before actual provisioning activity begins.                  |    |    |                                                                                               |        |                                                              |        |
| 4                                                                                             | You have completed this procedure.                                                                                                                                                                                                                                                                                                    |    |    |                                                                                               |        |                                                              |        |
| —End—                                                                                         |                                                                                                                                                                                                                                                                                                                                       |    |    |                                                                                               |        |                                                              |        |





## Backing up the APS-specific Oracle database and application files

To ensure successful recovery from a system problem that causes database file corruption, it is recommended that you periodically back up the database files that support operation of the APS. These files include:

- Oracle database
- Root database files
- non-Root database files

The Server Platform Foundation Software (SPFS) base software provides two utilities that enable you to back up these files: "bkfullora" and "bkfullsys".

The "bkfullora" utility backs up the Oracle database. This utility runs automatically each day at 1:00 am and backs up the database to a 4mm DAT tape. The utility can also be run manually to back up the database to a disk file.

The "bkfullsys" utility backs up the UNIX file system, including all of the "Root" and "non-Root" database files. This utility can only be run manually.

Instructions for performing the "bkfullora" and "bkfullsys" backup procedures are found in *ATM/IP Configuration Management*, NN10261-600.

In addition to these two utilities, two additional APS-specific utilities enable you to back up selected files, when only files required for APS operation must be restored. The "ips\_export\_db.sh" utility backs up the APS Oracle database. The "backup\_appl\_data.sh" utility backs up only the non-Root application files, "/audio\_files," "PROV\_data," "/user\_audio\_files," and Root application file, "/etc/inet/hosts." Both of these utilities can only be run manually.

This procedure enables you to perform a complete manual backup of the APS-specific Oracle database files and application files. It is recommended that this procedure be performed once per week.

## Backing up the APS-specific Oracle database and application files

| Step | Action |
|------|--------|
|------|--------|

### *In a telnet connection to the APS server*

- 1 Open an xterm window, and log in using the "maint" login and password.
- 2 Become the "root" user by entering:

```
su - root
```

- 3 Enter the following command to start the backup:  

```
ips_export_db.sh -diskonly
```

*The system displays a log of the backup activity.*
- 4 To ensure that the backup was successful, list the content of the tape on the terminal screen by entering the following commands:  

```
cd /audio_files/aps_db_backup
ls -l
```

*A listing of the backed-up files displays. Look in this list for "dmp" files.*

```
more README
```

*A timestamp displays, which should show the time and date of this backup.*

**Note:** At this point, you have completed the disk-only portion of the backup. Continue with the next step to complete the backup of the application files. The application files are backed up on tape.
- 5 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) DAT tape into the 4mm DAT drive on the APS server, and then rewind the tape by entering the following command:  

```
mt -f /dev/rmt/0c rewind
```
- 6 Enter the following command to start a backup of the application file systems on a single tape:  

```
/usr/ntdb/uas/scripts/backup_appl_data.sh
```

*The system displays a log of the backup activity.*
- 7 Rewind the backup tape by performing the following command:  

```
mt -f /dev/rmt/0c rewind
```
- 8 To ensure that the backup was successful, list the content of the tape on the terminal screen by entering the following command:  

```
tar tvf /dev/rmt/0c | more
```
- 9 Eject the backup tape, label it, and move the write-enable tab to the "read-only" position (white or grey tab is moved to the left where it cannot be seen), to prevent the data on the tape from being accidentally over-written. Store the tape for use later. Insert another write-enabled DAT tape into the drive to be used for the automatic Oracle system back up that runs daily at 1:00 a.m.
- 10 You have completed this procedure.

---

—End—

---



## Restoring the APS-specific Oracle database and application files

To ensure successful recovery from a system problem that causes database file corruption, you should periodically back up the database files that support operation of the APS. These files include:

- Oracle database
- Root database files
- Non-Root database files

The Server Platform Foundation Software (SPFS) base software provides utilities that enable you to restore these files. The "rsimpورا" utility restores the APS Oracle database files. The "ufsrestore" utility restores the UNIX file system, including all of the "Root" and "Non-Root" APS database files. The instructions for performing these backup procedures are found in the ATM/IP Configuration document, NN10276-500

In addition to these two utilities, two additional APS utilities and procedures enable you to restore selected files when only the files required for APS operation must be restored. The "ips\_export\_db.sh -restore" utility restores only the APS Oracle database. A procedure that utilizes the UNIX "tar" command enables you to restore the non-Root files, "/audio\_files," "/PROV\_data," "/user\_audiofiles," and Root file, "/etc/inet/hosts."

This procedure enables you to restore the APS-specific Oracle database and application files (/PROV\_data, /audio\_files, and /user\_audio\_files).

### Restoring the APS-specific Oracle database and application files

| Step                                                                                                                                                                          | Action                                                                            |    |    |                             |        |                             |        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----|----|-----------------------------|--------|-----------------------------|--------|
| <i>In a telnet connection to the APS server</i>                                                                                                                               |                                                                                   |    |    |                             |        |                             |        |
| 1                                                                                                                                                                             | Open an xterm window and log in using the "maint" login and password.             |    |    |                             |        |                             |        |
| 2                                                                                                                                                                             | Become the "root" user by entering:<br><br><code>su - root</code>                 |    |    |                             |        |                             |        |
| 3                                                                                                                                                                             | Determine whether you are restoring Oracle database files from tape or from disk. |    |    |                             |        |                             |        |
| <table> <tr> <th>If</th><th>Do</th></tr> <tr> <td>you are restoring from tape</td><td>step 4</td></tr> <tr> <td>you are restoring from disk</td><td>step 9</td></tr> </table> |                                                                                   | If | Do | you are restoring from tape | step 4 | you are restoring from disk | step 9 |
| If                                                                                                                                                                            | Do                                                                                |    |    |                             |        |                             |        |
| you are restoring from tape                                                                                                                                                   | step 4                                                                            |    |    |                             |        |                             |        |
| you are restoring from disk                                                                                                                                                   | step 9                                                                            |    |    |                             |        |                             |        |

- 4 Insert the appropriate "ORACLE" backup tape into the DDS-3 tape drive.

- 5 Rewind the backup tape by performing the following command:

```
mt -f /dev/rmt/0c rewind
```

- 6 Start the restoration of the APS Oracle database from the tape by entering the following command:

```
ips_export_db.sh -t /dev/rmt/0c -restore
```

**Note:** This command is entered on a single line.

Messages logging the progress of the restoration display on the screen. When you are prompted about continuing the restoration even if the current database will be destroyed, enter "y" (yes).

- 7 After the restoration of the Oracle database is complete, rewind the backup tape by performing the following command:

```
mt -f /dev/rmt/0c rewind
```

- 8 Eject the backup tape and store it for possible use later.

a. Go to step 10.

- 9 Start the restoration of the APS Oracle database from the disk by entering the following command:

```
ips_export_db.sh -diskonly -restore
```

**Note:** This command is entered on a single line.

Messages logging the progress of the restoration display on the screen. When you are prompted about continuing the restoration even if the current database will be destroyed, enter "y" (yes).

- 10 Insert the appropriate "application file" backup tape into the DDS-3 tape drive.

- 11 Change directory to the root directory:

```
cd /
```

- 12 Rewind the backup tape by performing the following command:

```
mt -f /dev/rmt/0c rewind
```

- 13 Restore the application files (/PROV\_data, /audio\_files, and /user\_audio\_files) by entering the following command:

```
tar xvf /dev/rmt/0c
```

- 14 When the restoration of the application files completes, remove the tape from the tape drive and store for possible use later. Insert

another write-enabled DAT tape into the drive to be used for the automatic Oracle system back up that runs daily at 1:00 a.m.

- 15** Verify that the application files have been restored by entering the following commands:

```
cd /PROV_data
```

```
ls -l
```

*The files should display on the screen.*

```
cd /user_audio_files
```

```
ls -l
```

*The files should display on the screen.*

```
cd /audio_files
```

```
ls -l
```

*The files should display on the screen.*

- 16** You have completed this procedure.

---

**—End—**

---

## Changing the APS Oracle account password

When the APS is installed, a default password is assigned to the Oracle account. This procedure enables you to change the default password, for added system security.

### Changing the APS Oracle account password

| Step | Action |
|------|--------|
|------|--------|

*In a telnet connection to the APS server*

- |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Open an xterm window and log in using the "root" login and password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 2 | <p>If you are unsure whether the password has been changed, obtain the current password by entering the following command:</p> <pre>getNTDBpasswd.ksh</pre> <p><i>The system displays the current Oracle account password.</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 3 | <p>Become the "Oracle" user by entering the following command:</p> <pre>su - oracle</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 4 | <p>Perform the following steps to change the Oracle account password:</p> <ol style="list-style-type: none"> <li>Enter the following command to run the script that enables you to change the password: <pre>/usr/ntdb/uas/scripts/setNTDBpasswd.ksh</pre> </li> <li>At the prompt, enter the current APS Oracle account password. <p><b>Note:</b> This is the password that you displayed in step 2.</p> </li> <li>At the prompt, enter the new APS Oracle account password.</li> <li>At the prompt, reenter the new APS Oracle account password. <p><i>The system changes the password in UNIX and in the Oracle database.</i></p> </li> <li>Enter the following command to exit from the Oracle user account: <pre>exit</pre> <p><i>This causes you to become the "root" user again.</i></p> </li> </ol> |
| 5 | <p>Restart the APS processes by entering the following command:</p> <pre>/opt/uas/aps/scripts/killDbServer.sh</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

*A message eventually displays indicating that APS restarted successfully.*

- 6** Enter the following commands to complete the password change:

```
cd /
. /etc/profile
. ./profile
```

- 7** You can now check the password change you have made by entering the following command:

```
getNTDBpasswd.ksh
```

*The system displays the current Oracle account password.*

- 8** You have completed this procedure.

---

—End—

---



---

## Administration: OAMP Workstation Backup

---

You can perform two types of backup on your OAMP workstation, manual and automatic. Manual backups are performed from the desktop by manually initializing the backup process. Automatic backups are performed according to the settings defined in the tape drive application.

### ATTENTION

Nortel Networks recommends that you use the automatic backups to ensure that the data that is stored on the tapes is up-to-date.

The OAMP workstation is equipped with a tape drive, software to support tape backup, and five blank data tapes. These tapes enable approximately one month's worth of backups to be kept on-site.

### ATTENTION

Nortel Networks recommends that you label the tapes to indicate the OAMP workstation associated with the backups to ensure that any recovery operations are performed from the correct tape.

## Backup schedule

You should create a schedule for your automatic backups to ensure up-to-date storage of the system configuration of your OAMP workstation.

### ATTENTION

Nortel Networks recommends that you perform a full system backup once a week and modified (differential) backups once a day.

## Manual backup

Nortel Networks recommends that you perform a manual backup of your OAMP workstation after initial installation.

To perform a manual backup of the system configuration for your OAMP workstation, refer to the documentation provided with your Colorado or Veritas software.

## Automatic backup configuration

There are two types of automatic backup: full system backup and modified (differential) system backup.

The full system backup saves all the files contained in the hard disk on your OAMP workstation.

The modified (differential) system backup saves only the files on the hard disk that have been modified since the last full system backup.

When you are using automatic backup, you must leave your OAMP workstation turned on with Windows running and ensure that there is a tape in the tape drive.

During the initial installation of your system, the tape drive application was configured to perform an automatic full system backup once a week, every Saturday at 1:00am. However, you can modify the settings in the tape drive application to suit your needs.

If you do not change the default setting for automatic full system backup, you need to swap out the tape every Friday.

In order for automatic backups to work, the tape drive scheduler icon must be active in the notification box in the taskbar with the automated daily backups option enabled, your OAMP workstation must remain on with Windows active, and a tape must be in the tape drive.

### **Verify the current modified system backup settings**

There is a tape drive configuration file associated with the modified system backup. To verify that the current settings in the configuration file matches the system requirements, refer to the tape drive documentation provided with the OAMP workstation.

### **View the current automatic backup schedule**

To view the current settings for automatic backup in the tape drive application, refer to the tape drive documentation provided with the OAMP workstation.

---

## Backing up a Multiservice Switch or Media Gateway device

---

This section describes using Service Data Backup and Restore to perform a basic back up of service data.

Backup copies only the configuration data of the Multiservice Switch 7400/15000 or Media Gateway 7400/15000. The service data views that make up the configuration data are found on the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 disk in a set of files in individual directories under the directory /provisioning. Backup also copies the special files that are found under the directory /provisioning/netsentry.

Service Data Backup and Restore provide three types of backup.

- A *full* backup copies all service data on the selected device or devices.
- An *incremental* backup copies only service data changed or created since the last backup. Like the full backup, you can perform an incremental backup on either one or multiple devices.
- A *selective* backup copies specific service data that you select. You can perform a selective backup on either one or multiple devices.

The following information applies to using the Service Data Backup and Restore tool to backup Multiservice Switch 7400/15000 or Media Gateway 7400/15000 nodes:

- ["Adding Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices to the backup list" \(page 129\)](#)
- ["Removing Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices from the backup list" \(page 130\)](#)
- ["Viewing the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 backup repository" \(page 130\)](#)
- ["Defining a specific userid and password for a Multiservice Switch 7400/15000 or Media Gateway 7400/1" \(page 131\)](#)
- ["Changing the Default User Authentication" \(page 131\)](#)
- ["Performing a full backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device" \(page 132\)](#)
- ["Performing an incremental backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 de" \(page 133\)](#)
- ["Performing a selective backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devic" \(page 133\)](#)

## Using the command line interface to perform backups

You can use the command line to perform full, incremental, or selective backups. You can perform multiple backups on multiple devices in a single command. You have the option of obtaining the backup information from a file.

Before you perform a backup, you need to start up the Backup Controller and Providers.

To display online help for this command, use the `-h` option on the command line.

### Procedure steps

Enter the following command as one continuous command:

```
/opt/MagellanNMS/bin/nsbck
[-full <devtype> <devname> <devaddr> <id> <pw>]
[-incr <devtype> <devname> <devaddr> <id> <pw>]
[-view <viewname> <devtype> <devname> <devaddr>
<id> <pw>] [-cdir <backup_dir_path> [-f
<backup_info_file>] [-chost <controller_address>]
[-nolog] | [-log [<logfile>]]
[-nc <#_concurrent_connections>]
```

where

- full indicates a full backup.
- incr indicates an incremental backup.
- view indicates a selective backup.
- devtype is the name of the device type, such as PASSPORT.
- devname is the name of the device.
- devaddr is the IP address of the device and has the format n.n.n.n.
- id is the userID for a Passport and the READ community string for a Passport 4400/4460.
- pw is the user password for a Passport and the WRITE community string for a Passport 4400/4460.
- viewname is the name of the view file for a selective backup.
- cdir is the backup directory used for this backup operation.
- f indicates that the backup information is obtained from a file.
- backup\_info\_file is the name of the file containing backup information. Each line in the file has the same format as the -full, incr, or -view options.
- chost indicates the remote Controller to be used in place of the Controller running on the local host.
- controller\_address is the address of the Controller and has the format host[:port]
- nolog indicates that output messages are to be discarded.

`-log` indicates that output messages go to stdout/stderr or to a log file. The default is stdout/stderr.

`logfile` is the name of the file to which output messages go. If not specified, the messages go to the file `mbrbackup.log` in the current directory (where the tool runs).

`-nc` indicates the number of concurrent backups to be performed. By default, SNMP Devices Backup tries to back up 5 different devices concurrently. This parameter is useful when you are backing up a large number of devices.

`#_concurrent_connections` is the number of concurrent backups.

## Backup file naming convention

The service data backup files have the following naming convention:

```
./<devtype>/<devname>/<timestamp>.<dataset>/ \ <datafiles...>
```

**Note:** The period (.) represents the SNMP Devices Backup and Restore root directory.

where

`devtype` is the device type (PP4400, or PP4460).

`devname` is the device name.

`timestamp` has the format `yyyymmddhhmmss`

`dataset` is the dataset name.

`<datafiles...>` are the names of one or more files that are backed up.

## Adding Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices to the backup list

Use this procedure to add devices to the list of devices that you wish to backup.

### Procedure steps

| Step | Action                                                                                                                                                 |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore. |
| 2    | Select the Backup Configuration tab.                                                                                                                   |
| 3    | Select Add to launch the Add Devices Dialog.                                                                                                           |
| 4    | From the left pane, select a group of devices or expand the group and use the Ctrl key to select a number of devices within a group.                   |
| 5    | From the drop down list, in the right pane, select a backup mode (Incremental or Full).                                                                |

- 6 If a specific userid and password is required for the device, enter the values in the user ID and Password fields and uncheck the Use default checkbox.
- 7 If you wish to use the default userid and password, click the Use default checkbox.
- 8 Click OK.  
The devices display in the Device List.

---

—End—

---

## Removing Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices from the backup list

Use this procedure to remove devices from the list of devices that you wish to backup.

### *Procedure steps*

| Step | Action                                                                                                                                                 |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore. |
| 2    | Select the Backup Configuration tab.                                                                                                                   |
| 3    | In the Device List, select the devices you wish to remove.                                                                                             |
| 4    | Click Remove.                                                                                                                                          |
| 5    | In the confirmation dialog, select Yes to confirm or No to cancel the removal.                                                                         |

---

—End—

---

## Viewing the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 backup repository

If the backup server is running locally, use the following procedure to view all the backup files in the backup repository.

**Procedure steps**

| Step  | Action                                                                       |
|-------|------------------------------------------------------------------------------|
| 1     | Telnet into the remote workstation with the appropriate userid and password. |
| 2     | Navigate to the repository directory.                                        |
| 3     | Use Unix directory commands to view the contents of the backup repository.   |
| —End— |                                                                              |

## Defining a specific userid and password for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 in the backup list

A specific userid and password can be defined when you add the node to the node list or you can set it later using the following procedure.

**Procedure steps**

| Step  | Action                                                                                                                                                 |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore. |
| 2     | Select the Backup Configuration tab.                                                                                                                   |
| 3     | Select a node in the Device List section.                                                                                                              |
| 4     | In the Device Details section, in the Authentication tab, enter a userid and password.                                                                 |
| 5     | Clear the Use default checkbox.                                                                                                                        |
| —End— |                                                                                                                                                        |

## Changing the Default User Authentication

Use the following procedure to define a default userid and password which is used for all node access unless overridden by a specific userid and password for the node.

**Procedure steps**

| Step  | Action                                                                                                                                                 |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore. |
| 2     | Select Options ->Set default authentication.                                                                                                           |
| 3     | Enter the userid and password in the appropriate fields.                                                                                               |
| 4     | Click OK.<br><br>The new userid and password are used on the next node access.                                                                         |
| —End— |                                                                                                                                                        |

## Performing a full backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

**Procedure steps**

| Step                                                      | Action                                                                                                                                                                                                   |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1                                                         | Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.                                                   |
| 2                                                         | Select the Backup Configuration tab.                                                                                                                                                                     |
| 3                                                         | Select Add to launch the Add Devices dialog.                                                                                                                                                             |
| 4                                                         | From the left pane, select a group of devices or expand the group and use the Ctrl key to select a number of devices within a group.                                                                     |
| 5                                                         | Select a device in the Device list:                                                                                                                                                                      |
| 6                                                         | Click in the Mode title and select Full from the drop-down list.                                                                                                                                         |
| 7                                                         | Click Backup.<br><br>The progress of the backup is displayed in the Messages area. If the backup is unsuccessful, an error dialog is displayed that specifies the device and the reason for the failure. |
| <b>Note:</b> To cancel a backup in progress click Cancel. |                                                                                                                                                                                                          |
| —End—                                                     |                                                                                                                                                                                                          |



## Performing an incremental backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to backup only backup files that are not already in the repository.

### *Procedure steps*

| Step | Action                                                                                                                                                                                                 |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.                                                 |
| 2    | Select the Backup Configuration tab.                                                                                                                                                                   |
| 3    | Select Add to launch the Add Devices dialog.                                                                                                                                                           |
| 4    | From the left pane, select a group of devices or expand the group and use the Ctrl key to select a number of devices within a group.                                                                   |
| 5    | Select a node in the nodes list.                                                                                                                                                                       |
| 6    | In the Mode title, select Incremental from the drop-down list.                                                                                                                                         |
| 7    | If you wish to specify a backup of views later than a specific date, enter the date in the date field. (for example July 3, 2005)                                                                      |
| 8    | Click Backup.<br><br>The progress of the backup is displayed in the Status area. If the backup is unsuccessful, an error dialog is displayed that specifies the device and the reason for the failure. |

**Note:** To cancel a backup in progress click Cancel.

---

—End—

---

## Performing a selective backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to backup only a single specified file to the repository.

**Procedure steps**

| Step | Action                                                                                                                                                                                                                                                                                                                                                                 |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.                                                                                                                                                                                                                 |
| 2    | Select the Backup Configuration tab.                                                                                                                                                                                                                                                                                                                                   |
| 3    | Select Add to launch the Add Devices dialog.                                                                                                                                                                                                                                                                                                                           |
| 4    | From the left pane, select a group of devices or expand the group and use the Ctrl key to select a number of devices within a group.                                                                                                                                                                                                                                   |
| 5    | Select a device in the Devices list.                                                                                                                                                                                                                                                                                                                                   |
| 6    | In the Mode title, select Selective from the drop-down list.<br>The Configuration column in the table is enabled.                                                                                                                                                                                                                                                      |
| 7    | Click in the Configuration cell to display a pull-down list that displays all the available views on the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.<br><br><b>Note:</b> This step may take a few seconds to complete because the application must access the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 and list all the views names. |
| 8    | Click Backup.<br><br>The progress of the backup is displayed in the Status area. If the backup is unsuccessful, an error dialog is displayed that specifies the device and the reason for the failure.<br><br><b>Note:</b> To cancel a backup in progress click Cancel.                                                                                                |

---

—End—

---

## Performing a backup of oracle data on an SPFS-based server

### Application

Use this procedure to perform a backup of oracle data on a Server Platform Foundation Software (SPFS)-based server (Sun Netra t1400 or Sun Netra 240).

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager

An oracle data backup is not required when the SPFS-based server is hosting the MG 9000 Manager.

- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

An oracle data backup is not required when the SPFS-based server is hosting the CBM.

If the SPFS-based server is hosting the IEMS, it is highly recommended to purge the IEMS event and performance data prior to executing the data backup. This reduces the size of the oracle space used by the IEMS, and therefore, reduces the backup time, and possibility of a backup failure. The purge capability is only available in (I)SN07 onward.

If the SPFS-based server is hosting the IEMS, it is highly recommended to purge the IEMS event and performance data prior to executing the data backup. This reduces the size of the oracle space used by the IEMS, and therefore, reduces the backup time, and possibility of a backup failure. The purge capability is only available in (I)SN07 onward.

Refer to the procedure 'Configuring dark office backups on an SPFS-based server' in ATM/IP Solution-level Configuration Management, NN10409-500.

#### ATTENTION

It is recommended that provisioning activities be put on hold during the time of the data backup.

## Prerequisites

This procedure has the following prerequisites:

- For a Sun Netra t1400, you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data
- for a Sun Netra 240, you need one or more blank CD-R, DVD-R, CD-RW or DVD-RW to store the data

The backup utility limits the storage to 4GB on a DVD-R and DVD-RW.

If you are using a new CD-RW or DVD-RW, or want to reuse an CD-RW or DVD-RW by erasing the contents, perform procedure 'Preparing a CD-RW or DVD-RW for use' in *ATM/IP Security and Administration document*, NN10402-600.

### ATTENTION

The database must be in sync with the Communication Server 2000 and the MG 9000 Manager (if present). Therefore, ensure you have the appropriate image of both before you proceed. Performing a restore from the Oracle database alone can cause data mismatches at the Communication Server 2000 and the MG 9000 Manager (if present).

## Action

### ATTENTION

In a two-server configuration, execute this procedure on the Active server.

| Step                       | Action                                                                                                                                                                                                                                                                                                                 |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>At the server</b>       |                                                                                                                                                                                                                                                                                                                        |
| 1                          | Insert the blank tape, CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of the Active server.                                                                                                                                                                        |
| <b>At your workstation</b> |                                                                                                                                                                                                                                                                                                                        |
| 2                          | Log in to the server by typing<br><pre>&gt; telnet &lt;server&gt;</pre> and pressing the Enter key.<br>where<br><pre>server</pre> is the IP address or hostname of the SPFS-based server on which you want to perform the backup<br>In a two-server configuration, enter the physical IP address of the active server. |

#### At the server

- 1 Insert the blank tape, CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of the Active server.

#### At your workstation

- 2 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  

```
server
```

is the IP address or hostname of the SPFS-based server on which you want to perform the backup  
In a two-server configuration, enter the physical IP address of the active server.

- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing  
`$ su -`  
 and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 If the server is hosting the IEMS, and you want to purge the event and performance data, do step [step 7](#), otherwise proceed to step [10](#).

**ATTENTION**

This step stops the IEMS server. Ensure it is acceptable at this time to stop the IEMS server application.

- 7 Stop the IEMS server by typing:  
`# servstop IEMS`  
 and pressing the Enter key.
- 8 Run the script to purge the data by typing  
`# /opt/nortel/iems/current/bin/purgeTempData.sh`  
 and pressing the Enter key.
- 9 Start the IEMS server by typing  
`# servstart IEMS`  
 and pressing the Enter key.
- 10 Use the following table to determine your next step.

| If you are using       | Do                      |
|------------------------|-------------------------|
| a tape for backup      | step <a href="#">11</a> |
| a CD or DVD for backup | step <a href="#">12</a> |

- 11 Rewind the tape by typing  
`# mt -f /dev/rmt/0 rewind`  
 and pressing the Enter key.
- 12 Back up the data by typing  
`$ /opt/nortel/SPFS/bks/bkdata`  
 and pressing the Enter key.

*Example response:*

Backup Completes Successfully

- 13** Use the following table to determine your next step

| If you are using       | Do      |
|------------------------|---------|
| a tape for backup      | step 14 |
| a CD or DVD for backup | step 16 |

- 14** List the content of the tape by typing

```
tar tvf /dev/rmt/0
```

and pressing the Enter key.

*Example response:*

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:16 2005 opt/oracle.dmp
.gz
-rw-rw-rw- 0/1 1007616 Mar 2 10:16 2005 opt/critdata.c
pio
```

- 15** Remove the tape from the drive, label it, write-protect it, and store it in a safe place. Proceed to

- 16** Reinsert the backup CD or DVD into the drive.

- 17** List the content of the CD or DVD by typing

```
tar tvf /cdrom/*bkdata/*.tar
```

and pressing the Enter key.

*Example response:*

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:17 2005 opt/oracle.dmp
.gz
-rw-rw-rw- 0/1 1007616 Mar 2 10:17 2005 opt/critdata.c
pio
```

*When a DVD backup spans more than one disk, all the DVDs with the exception of the last one produce a file error during the verification process. This error message does not interfere with the backup process but can reappear several times as the backup spans multiple disks.*

- 18** Ensure you are at the root directory level by typing

```
cd /
```

and pressing the Enter key.

- 19** Eject the CD by typing

```
eject cdrom
```

and pressing the Enter key.

*If the DVD drive tray does not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands in the order listed:*

```
/etc/init.d/volmgt stop
/etc/init.d/volmgt start
```

*Then press the eject button located on the front of the DVD drive.*

- 20** Remove the CD or DVD from the drive, label it, and store it in a safe place.
- 21** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.  
  
To restore the data from tape or CD/DVD, refer to procedure "Restoring the oracle data on an SPFS-based server" in *ATM/IP Security and Administration*, NN10402-600.

---

—End—

---

## Performing a backup of file systems on an SPFS-based server

---

### Application

Use this procedure to perform a backup of the file systems on a Server Platform Foundation Software (SPFS)-based server (Sun Netra t1400 or Sun Netra 240).

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

### Prerequisites

This procedure has the following prerequisites:

- You must perform a data backup prior to performing this procedure. Refer to procedure ["Performing a backup of oracle data on an SPFS-based server" \(page 135\)](#) to complete this task.

The data backup is not required prior to this procedure for the Core and Billing Manager (CBM) or the MG 9000 Manager.

- For a Sun Netra t1400, use a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data
- For Sun Netra 240, use one or more blank CD-R, CD-RW, DVD-R or DVD-RW disks to store the data

The backup utility limits the storage to 4 GB on a DVD-R and DVD-RW.

If you are using a new CD-RW or DVD-RW, or want to reuse a used CD-RW or DVD-RW and need to erase the contents, complete procedure "Preparing a CD-RW or DVD-RW for use" in *ATM/IP Security and Administration*, NN10402-600.

### Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform config-admin actions.



- You must obtain non-restricted shell access.

For CBM 850, root user ID and password are not required. Therefore, you are not required to change to the root user in steps 4 and 5 of this procedure.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

## Action

### ATTENTION

In a two-server configuration, execute this procedure on the Active server.

| Step                       | Action                                                                                                                                                                                                                                                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>At the server</b>       |                                                                                                                                                                                                                                                                                                                                  |
| 1                          | Insert the blank tape or DVD into the drive. In a two-server configuration, insert the blank DVD into the Active server.                                                                                                                                                                                                         |
| <b>At your workstation</b> |                                                                                                                                                                                                                                                                                                                                  |
| 2                          | Log in to the server by typing<br><code>&gt; telnet &lt;server&gt;</code><br>and pressing the Enter key.<br>where<br><code>server</code><br>is the IP address or host name of the SPFS-based server on which you are performing the backup<br>In a two-server configuration, enter the physical IP address of the active server. |
| 3                          | When prompted, enter your user ID and password.                                                                                                                                                                                                                                                                                  |
| 4                          | Change to the root user by typing<br><code>\$ su -</code><br>and pressing the Enter key.                                                                                                                                                                                                                                         |
| 5                          | When prompted, enter the root password<br>In a two-server configuration, ensure you are on the active server by typing <code>ubmstat</code> . If <code>ClusterIndicatorSTBY</code> is displayed in the response, which indicates you are on the inactive server, log out of                                                      |

#### At the server

- 1 Insert the blank tape or DVD into the drive. In a two-server configuration, insert the blank DVD into the Active server.

#### At your workstation

- 2 Log in to the server by typing  
`> telnet <server>`  
 and pressing the Enter key.  
 where  
`server`  
 is the IP address or host name of the SPFS-based server on which you are performing the backup  
 In a two-server configuration, enter the physical IP address of the active server.
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing  
`$ su -`  
 and pressing the Enter key.
- 5 When prompted, enter the root password  
 In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of

that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display ClusterIndicatorACT, which indicates you are on the active server

- 6 Use the following table to determine your next step.

| If you are using       | Do                     |
|------------------------|------------------------|
| a tape for backup      | <a href="#">step 7</a> |
| a CD or DVD for backup | <a href="#">step 8</a> |

- 7 Rewind the tape by typing  
`# mt -f /dev/rmt/0 rewind`  
 and pressing the Enter key.

- 8 Back up the file systems by typing  
`# /opt/nortel/SPFS/bks/bkfullsys`  
 and pressing the Enter key.

*Example response:*

Backup Completed Successfully

When using a DVD, the system will prompt you to insert another blank disk if more than one is needed.

- 9 Use the following table to determine your next step

| If you are using       | Do                      |
|------------------------|-------------------------|
| a tape for backup      | <a href="#">step 10</a> |
| a CD or DVD for backup | <a href="#">step 12</a> |

- 10 List the contents of the tape by typing  
`# gtar -tvMf /dev/rmt/0`  
 and pressing the Enter key.

- 11 Eject and remove the tape from the drive, label it, write-protect it, and store it in a safe place. Proceed to [step 19](#)

- 12 Insert the backup DVD into the drive. If the backup resides on multiple DVDs, insert the first backup DVD.

- 13 List the content of the CD or DVD by typing  
`# gtar -tvMf /cdrom/*bkfullsys*/*.tar`

and pressing the Enter key.

| If you                                            | Do      |
|---------------------------------------------------|---------|
| receive a prompt to prepare another volume        | step 14 |
| do not receive a prompt to prepare another volume | step 16 |

**14** Press the Return key

**15** Stop the gtar process by pressing the Ctrl and C keys

**16** Ensure you are at the root directory level by typing

```
cd /
```

and pressing the Enter key.

**17** Eject the DVD by typing

```
eject cdrom
```

and pressing the Enter key.

*If the disk drive tray will not open after you have determined that the disk drive is not busy and is not being read from or written to, enter the following commands:*

```
/etc/init.d/volmgt stop
```

```
/etc/init.d/volmgt start
```

*Then, retry the eject cdrom command previously shown and press the Enter key.*

**18** Remove the DVD from the drive, label it, and store it in a safe place.

| If the backup            | Do                                                             |
|--------------------------|----------------------------------------------------------------|
| resides on multiple DVDs | Insert the next backup DVD in the disk drive and go to step 13 |
| resides on a single DVD  | step 19                                                        |

**19** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

## Backing up the central security server

### Application

Use this procedure to back up the central security server. When the Security Services component is installed, the generic backup and restore script (brr\_security.sh) are registered with servman (bkmgr).

The NDS database and all files under the following directories are backed up using this procedure:

- /opt/nortel/config/3rd\_party/netscape
- /opt/nortel/config/3rd\_party/security/s1is
- /opt/nortel/config/applications/security
- /opt/nortel/data/3rd\_party/netscape
- /opt/nortel/data/3rd\_party/security/s1is
- /opt/nortel/data/applications/security

### Prerequisites

You must have root user privileges to perform this procedure.

### Action

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Establish a connection to the server where IEMS resides through telnet or SSH, using the host name or IP address of the server, and log in using the root user ID and password.  
  
In a two-server configuration, establish the connection to the active server using the physical IP address of the active server, and ensure you are on the active server using the `ubmstat` command.  
  
For detailed steps, refer to procedure Logging in to an SPFS-based server.
- 2 Use the following table to determine your next step.

| If                                      | Do                     |
|-----------------------------------------|------------------------|
| this server is hosting the CMT and IEMS | <a href="#">step 3</a> |
| this server is only hosting the IEMS    | <a href="#">step 6</a> |

- 3 Verify the status of the SESM server application by typing  
`servman query -status -group SESMSERVICE`  
 and pressing the Enter key.

- 4 Use the following table to determine your next step.

| If                                     | Do                     |
|----------------------------------------|------------------------|
| the SESM server application is running | <a href="#">step 6</a> |
| otherwise                              | <a href="#">step 5</a> |

- 5 Start the SESM server application by typing  
`servstart SESMSERVICE`  
 and pressing the Enter key.

- 6 Enter the backup manager utility by typing  
`/opt/bkresmgr/cbm/bkmgr`  
 and pressing the Enter key.

- 7 Start the backup by typing  
`backup full`  
 and pressing the Enter key.

- 8 Use the following table to determine your next step.

| If response is                                                    | Do                                  |
|-------------------------------------------------------------------|-------------------------------------|
| Backup succeeded.                                                 | <a href="#">step 9</a>              |
| Backup failed. For more detailed errors, refer to log file at ... | Contact your next level of support. |

- 9 Exit the backup manager utility by typing  
`quit`  
 and pressing the Enter key.

The Security Services configuration settings and data are backed up to the following file:

`/data/bkresmgr/<date><time>backupSS1.1<host_name>.tar`

- 10 You have completed this procedure.  
 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

## Backing up an SPFS-based security client

### Application

Use this procedure to obtain a list of the files that will be backed up from the client machine. To enable backup and restore of the security client, the files to be backed up are registered with servman during installation. The files backed up depend on the packages installed.

### Prerequisites

You must have root user privileges to perform this procedure.

### Action

| Step                                                 | Action                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>In a telnet connection to the security server</i> |                                                                                                                                                                                                                                                                                                                                                                                                             |
| 1                                                    | <p>Telnet to the server by typing</p> <pre>&gt; telnet &lt;server&gt;</pre> <p>and pressing the Enter key.</p> <p>where</p> <p><b>server</b> is the IP address or host name of the server where IEMS resides</p>                                                                                                                                                                                            |
| 2                                                    | When prompted, enter your user ID and password.                                                                                                                                                                                                                                                                                                                                                             |
| 3                                                    | <p>Change to the root user by typing</p> <pre>\$ su - root</pre> <p>and pressing the Enter key.</p>                                                                                                                                                                                                                                                                                                         |
| 4                                                    | When prompted, enter the root password.                                                                                                                                                                                                                                                                                                                                                                     |
| 5                                                    | <p>Enter the following command:</p> <pre>cat etc/critdata.conf</pre> <p><i>The system returns a list of all non-oracle data files that will be backed up from the client machine.</i></p>                                                                                                                                                                                                                   |
| 6                                                    | <p>Use the Synchronous Backup Restore Manager (SBRM) to backup the central security client data. When SBRM is run, all of the SPFS data, including the security client data and oracle data, is backed up. For details, see the procedure for "Starting or stopping the automated synchronous backup restore manager service" in <i>ATM/IP Solution-level Administration and Security</i>, NN10402-600.</p> |

7 You have completed this procedure.

---

—End—

---



## Administration: Manual Backup

If you change the external IP address of an Real-time Controller (RTC) system node in your system (or perform any other data provision changes on your system), you should immediately perform a backup operation and delete any data snapshots that were made before you changed the IP address. This ensures proper communication with your OAMP workstations.

### Performing a backup operation

| Step                           | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>At the OAMP workstation</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 1                              | Click <b>Administration&gt;backup</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 2                              | Enter a description of the data snapshot in the <b>snapshot-description</b> box. You can enter up to 32 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 3                              | Click the corresponding checkboxes to activate the following options, as appropriate: <ul style="list-style-type: none"> <li><i>transfer snapshot to alternate boot server</i><br/>Nortel Networks recommends that you enable this option. If you don't select this option, a warning dialog box appears. Click <b>Yes</b> to continue.</li> <li><i>set as active snapshot on alternate boot server</i><br/>Nortel Networks recommends that you enable this option. If you don't select this option, a warning dialog box appears. Click <b>Yes</b> to continue.</li> <li><i>delete oldest snapshot on alternate boot server if maximum reached (16)</i></li> <li><i>delete oldest snapshot on rtc if maximum reached (5)</i></li> </ul> |
| 4                              | Click <b>Create</b> to create the data snapshot. This can take several minutes, depending on system activity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 5                              | Click <b>Close</b> to close the Backup Active RTC window and return to the Administration window.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 6                              | If you selected <b>transfer snapshot to alternate boot server</b> on alt boot server, go to <a href="#">step 12</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 7                              | Click <b>Administration&gt;file-manager</b> . The File Manager window appears.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

- 8 Select the active RTC system node from the **Destination** list in the right window pane.
- 9 Select the new data snapshot from the **Snapshot** box in the Destination portion of the window. Make note of the timestamp of the data snapshot.
- 10 Copy the snapshot to your alternate boot server by clicking <--. An hourglass appears while the data snapshot is copied. The boxes in the **Source** portion (left window) of the window are updated with the information for the copied data snapshot when the copy operation is complete.

These files are large and can take several minutes to copy from an RTC system node to your alternate boot server.
- 11 When the file is transferred, click **Close**.
- 12 Update the Alternate Boot Snapshot using the ABS Settings ABS window:
  - a. Open the Alternate Boot Server (ABS) Configuration Manager window by clicking **ABS Settings** on the Administration>alternate-boot-server window.
  - b. Select an alternate snapshot by clicking the arrow button.
  - c. Click **Modify** to save your changes and close the window.
- 13 Your backup is complete.

---

—End—

---

## Using the Command Line Interface

The same backup procedure may be performed via the CLI. The command syntax is:

### **admin backup create**

"snapshot-description" abs-transfer-option abs-active-option  
rtc-delete-oldest-option abs-delete-oldest-option

where:

snapshot-description can be up to 32 characters and the other four options are set by entering either **y** (for enabled) or **n** (for disabled).

See "[Administration: Manual Backup](#)" (page 149) for option descriptions.

The following example creates a snapshot named "*my snapshot*", transfers it to the ABS and sets it as active. It also deletes the oldest snapshot on the rtc or abs, if the maximum number of snapshots is reached on either:

```
admin backup create "my snapshot" y y y y
```

A list of possible CLI return codes is as follows:

| Rcode      | Rcode text                                                                          |
|------------|-------------------------------------------------------------------------------------|
| 0x40100001 | snapshot-description must be string, length(1 - 32), no additional character filter |
| 0x40100002 | rtc-delete-oldest-option must be string, length(1 - 1), boolean (Y, y, N, n)        |
| 0x40100003 | abs-transfer-option must be string, length(1 - 1), boolean (Y, y, N, n)             |
| 0x40100004 | abs-active-option must be string, length(1 - 1), boolean (Y, y, N, n)               |
| 0x40100005 | abs-delete-oldest-option must be string, length(1 - 1), boolean (Y, y, N, n)        |
| 0x80100001 | missing snapshot-description                                                        |
| 0x80100002 | insufficient disk space on rtc                                                      |
| 0x80100003 | maximum number of snapshots reached on rtc                                          |
| 0x80100004 | maximum number of snapshots reached on abs                                          |
| 0x80100005 | unable to delete oldest snapshot on rtc                                             |
| 0x80100006 | unable to delete oldest snapshot on abs                                             |
| 0x80100007 | unable to transfer snapshot to abs                                                  |
| 0x80100008 | unable to set snapshot as active on abs                                             |
| 0x80100009 | unable to connect to abs, run abs test for details                                  |
| 0x8010000A | invalid combination of command options                                              |

## Creating system image backup tapes (S-tapes) manually

### Purpose

Use this procedure to create a system backup image manually.

### Prerequisites

You must be a user authorized to perform config-manage actions.

#### Procedures related to this procedure

| Procedure                                          |
|----------------------------------------------------|
| Logging in to the CS 2000 Core Manager             |
| Displaying actions a user is authorized to perform |

#### Procedures related to this procedure

| Procedure                                          |
|----------------------------------------------------|
| Logging in to the CS 2000 Core Manager             |
| Displaying actions a user is authorized to perform |

### Application

Create a system image backup tape (S-tape) manually.

**Note:** If you want to schedule automatic system image backups, refer to SDM Security and Administration document.

The system image includes the following:

- boot (startup) files
- AIX operating system
- system configuration data
- core manager software

### Prerequisites

#### ATTENTION

This procedure must be performed by a trained AIX system administrator authorized to perform config-manage actions.

**ATTENTION**

All volume groups on the core manager must be fully mirrored (Mirrored) before performing this procedure. If not, an error message is displayed.

**ATTENTION**

If your system includes the SuperNode Billing Application (SBA), you must use tape drive DAT0 to perform this procedure.

**ATTENTION**

The files under the /data file system are temporary files only, and are excluded from system image backup.

Perform a system image backup after the following events:

- initial installation and commissioning of the core manager
- changes to the configuration of disks or logical volumes
- installation of a new version of core manager platform software
- installation of new hardware
- changes or upgrades to existing hardware

A system image backup takes a minimum of 10 minutes to complete, depending on the size of your file systems.

**Recommended tapes**

To complete this procedure, use one of the digital audio tape (DAT) drive tapes approved by Nortel.

The brands approved by Nortel are: Hewlett Packard (HP), Maxell, Verbatim, Imation.

The tape lengths approved by Nortel are:

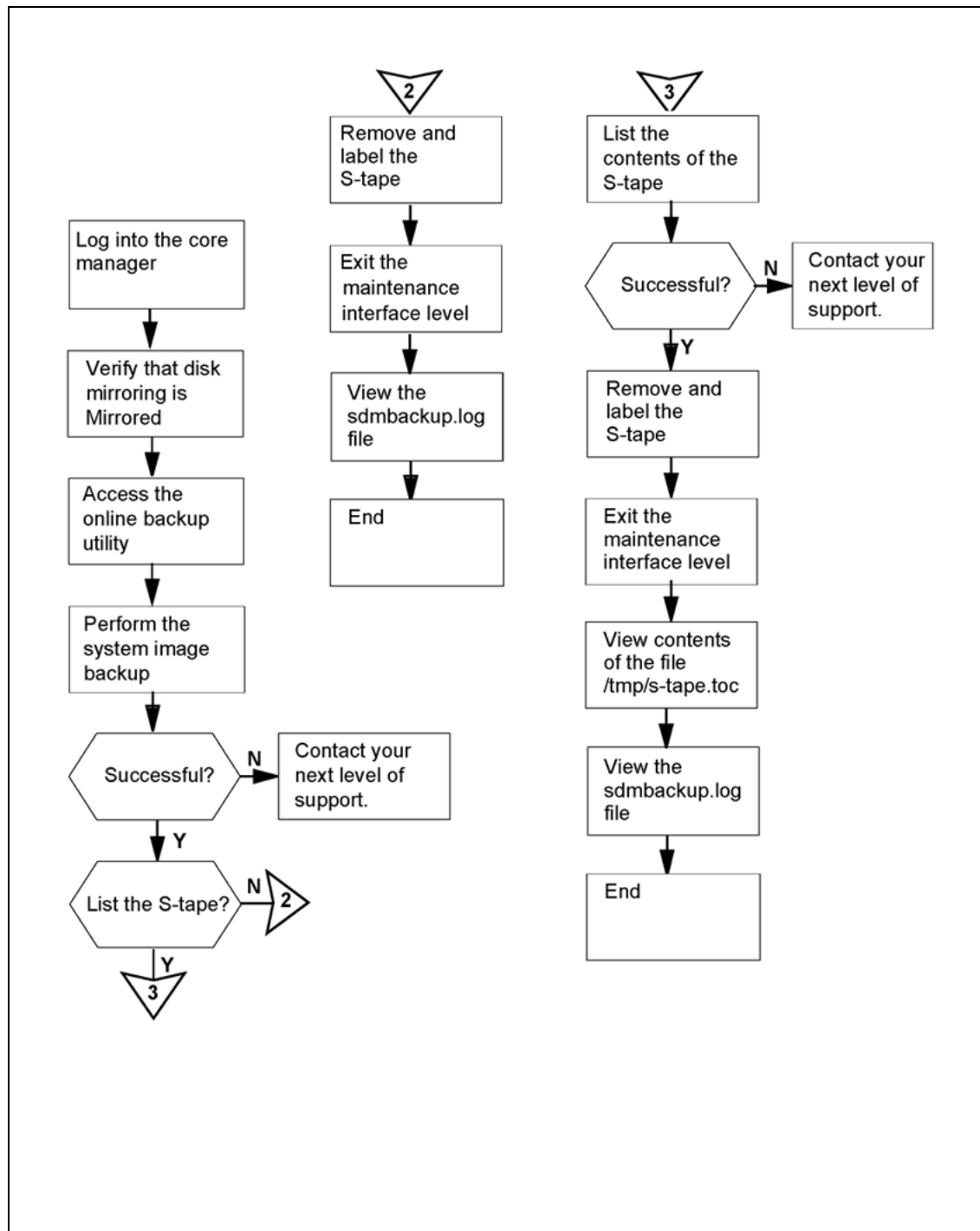
- 90-meter (90M)
- 125-meter (125M)
- 120-meter (120M)

The 125M tape is approved for UMFIOS only, assuming that your system is equipped with DDS3-capable devices to read the content of the tape.

**Procedure**

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the procedure.

## Summary of creating system image backup tapes (S-tapes)



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Creating system image backup tapes (S-tapes)

| Step | Action |
|------|--------|
|------|--------|

### At the local VT100 console

- 1 Log into the core manager as a user authorized to perform config-manage actions.

- 2 Access the maintenance interface:

```
sdmmtc
```



#### CAUTION

#### System mirroring must be MIRRORRED

You cannot perform this procedure until disk mirroring of all volume groups is Mirrored. If necessary, contact the personnel responsible for your next level of support. When disk mirroring is Mirrored, continue this procedure.

- 3 Access the storage menu level:

```
storage
```

*Example response:*

```
Volume Group Status
Free (MB)
rootvg Mirrored 608
Logical Volume Location Size (MB)
%full/threshold 1 / rootvg 20
25/ 80
2 /usr rootvg 192 85/ 90
3 /var rootvg 64 11/ 80
4 /tmp rootvg 24 6/ 90
5 /home rootvg 300 4/ 70
6 /sdm rootvg 300 44/ 90
Logical volumes showing: 1 to 6 of 6
```

| If the disks       | Do                            |
|--------------------|-------------------------------|
| are "Mirrored"     | step 4                        |
| are not "Mirrored" | contact next level of support |

- 4 Access the administration (Admin) menu level of the RMI:

```
admin
```

- 5 Access the System Image Backup and Restore Menu:

```
backup
```

*Example response:*

```
Currently there is a backup running on
```

```
bnode73.Please execute yours later.
Exiting . . .
```

**Note:** If another operator attempts to use the Backup and Restore utility when it is in use, an error message is displayed.

- 6 From the System Image Backup and Restore Menu, select Create a System Image on Tape (S-tape):

2

After you select option 2, you are prompted to select the tape drive.

*Example response:*

```
Select the tape drive you wish to use:
Enter 0 to return to previous menu
Enter 1 for tape drive DAT0 in Main Chassis-Slot 2
Enter 2 for tape drive DAT1 in Main Chassis-Slot 13
(0, 1 or 2) ==>
```

**Note:** Use tape drive DAT0 (option 1) if your system also includes SBA.

- 7 Select the tape drive to use:

<n>

where

<n> is the option (1 or 2) for the tape drive you wish to use

**Note:** If your system includes SBA, and you wish to use tape drive DAT1 (option 2), the following message is displayed:

*Example response:*

```
You have selected DAT 1. This is the default DAT drive
for the Billing application, and may currently be in
use for the emergency storage of billing records.
If you continue to use DAT 1, make sure that the
correct tape is in the drive, and that billing records
will not be lost during the backup restore operation.
Do you wish to continue with DAT 1? (y | n)
```

| If you                      | Do                                           |
|-----------------------------|----------------------------------------------|
| wish to continue using DAT1 | enter <b>y</b><br>press the <b>Enter</b> key |
| do not wish to use DAT1     | enter <b>n</b><br>press the <b>Enter</b> key |

The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.



After you select the tape drive, you are prompted to insert a tape in the drive you have selected.

*Example response:*

Please insert a 4mm DAT tape into the tape drive DAT0.

Caution:

This action will overwrite the content on the inserted tape. Do you want to proceed? ( y | n ) ==>

**At the core manager**



**CAUTION**

**System image backup tape**

Creating a system image overwrites the contents of the inserted tape. Ensure that you are using the correct tape before starting the system image backup. If your system includes SBA and you are using DAT1, ensure that the tape drive does not contain an SBA tape.

- 8 Ensure that the appropriate core manger tape drive contains a 4-mm digital audio tape (DAT) either 90 m or 120 m long. This tape will be designated as the system image backup tape (S-tape).

**Note:** For the complete list of approved tapes, refer to the "Recommended tapes" (page 153).

**At the local console**

- 9 When you are certain you are using the correct tape, enter:

y

- 10 Read the system message to determine if there is enough room on the temporary directory for the system image backup to proceed.

**Note:** If there is not enough room on the temporary directory, an error message appears.

*Example response:*

Rewinding the tape...

The /tmp directory is not big enough.

Trying to expand /tmp by 6600KB...

Failed to expand the /tmp directory because there isn't enough free disk space left on the rootvg.

Please erase some files under /tmp directory to create at least 6600KB for the full system image backup.

Enter any key and return to exit ==>

| If there is           | Do      |
|-----------------------|---------|
| enough disk space     | step 14 |
| not enough disk space | step 11 |

- 11** Erase enough files from the temporary directory to create the required amount of disk space specified in the error message:

```
rm -rf /tmp/ <filenames>
```

**Note:** If you have trouble erasing files from the temporary directory to free up disk space, contact the personnel responsible for your next level of support.

- 12** Execute the system image backup again.

The system image backup begins.

*Example response:*

```
Rewinding the tape...
Starting the system image backup on bnode73.
The backup takes a minimum of 10 minutes,
depending on the size of your file systems.
When the backup is complete, you will be asked to
remove the tape from the tape drive.
System image backup is in progress ...
```

**Note:** This backup process takes approximately 10 minutes to complete, depending on the amount of data stored on the disk.

- 13** Read the system message.

| If the backup             | Do                                 |
|---------------------------|------------------------------------|
| is successfully completed | step 14                            |
| fails                     | contact your next level of support |

- 14** The system informs you if the backup is successful. When the backup is complete, the system prompts you to remove the tape and label it as an S-tape.

*Example response:*

```
The tape backup started on Wed Oct 16 08:21:15 EDT 1997
completed successfully on Wed Oct 16 08:37:37 EDT 1997.
The log for this session has been added to "/var/adm/
sdmbackup.log".
Please remove the backup tape from the tape drive.
Label the tape as shown below and store it
in a safe place.
```

```

System Image Tape (S-tape)
The Machine Node Id: bnode73
Date: Wed Oct 16 08:37:37 EDT 1997
Eject the S-tape from the tape drive? (y | n) ==>

```

**15** Determine if you wish to eject the S-tape. Enter

- **y** to eject the tape, or
- **n** if you do not wish to eject the tape, and wish to list its contents.

| If you                      | Do      |
|-----------------------------|---------|
| you wish to list the S-tape | step 28 |
| protect and label the tape  | step 16 |

If you eject the tape, the screen displays "Tape ejected." below the information displayed in step 14. You are then prompted to return to the System Image Backup and Restore Main Menu.

*Response:*

```

Tape ejected.
Would you like to return to the previous
menu? (y | n)

```

**16** Place the write-protected tab of the S-tape in the open position, to prevent accidental erasure.

**17** When you are ready for the system to return to the System Image Backup and Restore Main Menu, enter

**y**

**18** Determine if the backup is successful.

The system informs you if the system image backup is successful, as shown in the response in step 14. You may also wish to view the `/var/adm/sdmbbackup.log` file or list the files on the S-tape.

| If                                                             | Do                                 |
|----------------------------------------------------------------|------------------------------------|
| you wish to view the <code>/var/adm/sdmbbackup.log</code> file | step 19                            |
| you wish to list the S-tape                                    | step 28                            |
| the backup is successful                                       | step 36                            |
| the backup fails                                               | contact your next level of support |

**19** Exit the System Image Backup and Restore Main Menu:

**0**

- 20 Exit the RMI:

```
quit all
```

- 21 Access the sdmbbackup.log file:

```
cd /var/adm
```

- 22 Scroll through the file:

```
more sdmbbackup.log
```

This screen informs you that the system image backup was completed successfully.

*Example response:*

```
bosboot: Boot image is 5881 512 byte blocks.
```

```
0+1 records in.
```

```
1+0 records out.
```

```
Backing up the system...
```

```
.....
```

```
0512 038 mksysb: Backup Completed Successfully.
```

```
The S-tape backup started on Wed Oct 16 09:24:07 EDT
```

```
1997
```

```
completed successfully on Wed Oct 16 09:36:03 EDT 1997
```

- 23 Determine if you wish to list the S-tape.

| If you                         | Do                      |
|--------------------------------|-------------------------|
| wish to list the S-tape        | step <a href="#">24</a> |
| do not wish to list the S-tape | step <a href="#">40</a> |

- 24 Return to the login directory:

```
cd
```

- 25 Access the RMI:

```
sdmmtc
```

- 26 Access the administration (Admin) menu level of the RMI:

```
admin
```

- 27 Access the System Image Backup and Restore Menu:

```
backup
```

- 28 From the System Image Backup and Restore Menu, select List Contents of the System Image Tape (S-tape):

```
3
```

- 29 After you select option 3, you are prompted to select the tape drive.

**Example response:**

```

Select a tape drive you wish to use:
 Enter 0 to return to previous menu
 Enter 1 for tape drive DAT0 in Main
Chassis-Slot 2
 Enter 2 for tape drive DAT1 in Main
Chassis-Slot 13
 (0, 1 or 2) ==>

```

**Note:** Use tape drive DAT0 (option 1) if your system also includes SBA.

**30** Select the tape drive:

<n>

where

<n> is the number (1 or 2) for the tape drive you wish to use

**Example response:**

```

You have selected DAT 1. This is the default DAT drive
for the Billing application, and may currently be in
use for the emergency storage of billing records.
If you continue to use DAT 1, make sure that the
correct tape is in the drive, and that billing records
will not be lost during the backup restore operation.
Do you wish to continue with DAT 1? (y | n)

```

If you do not wish to use DAT1, the system prompts you to return to the System Image Backup and Restore Menu.

| If you wish to      | Enter |
|---------------------|-------|
| continue using DAT1 | y     |
| not continue        | n     |

**Note:** If your system includes SBA, and you still wish to use DAT1 (option 2), the following message is displayed:

**31** After you select the tape drive, you are prompted to insert the S-tape into the tape drive that you selected in step 30.**Example response:**

```

Please insert your System Image Backup tape (S-tape)
into the tape drive DAT0 and allow at least 5 minutes
to complete the listing.
A log file will be saved in /tmp/s-tape.toc
Are you ready to proceed? (y | n)

```

**At the core manager**

- 32 Insert the S-tape into the tape drive.

**Note:** Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

***At the local VT100 terminal***

- 33 When you are ready to continue this procedure, enter:

y

- 34 The contents of the S-tape are displayed. When the listing is complete, the system prompts you to return to the System Image Backup and Restore Menu.

*Example response:*

```
Would you like to return to the previous menu? (y |
n)
```

- 35 Return to the System Image Backup and Restore Menu:

y

***At the core manager***

- 36 If you have not already done so, remove the S-tape from the tape drive by pressing the eject button on the tape drive.

- 37 Label the tape according to your office practices, and store it in a safe location.

- 38 If you ejected an SBA tape, reinsert the tape.

***At the local VT100 terminal***

- 39 Exit the System Image Backup and Restore Menu,:

0

**Note:** If you wish to exit the RMI, enter QUIT ALL.

- 40 You have completed this procedure.

---

—End—

---

## Configuring SBA backup volumes on the core

### Purpose

Use this procedure to configure backup volumes on IOP, 3PC, DDU, or SLM disks on the core for a billing stream. The maximum number of volumes that can be configured for a billing stream is either 69 or the maximum supported by the underlying hardware, whichever is less per stream.

The following table lists the disk drive backup volumes that you can configure for the BRISC and XA-core platforms.

| Platform                                        | Backup volume(s) |
|-------------------------------------------------|------------------|
| BRISC                                           | DDU or SLM       |
| XA-core (for releases prior to SDM16 or CS2E03) | DDU or IOP       |
| XA-core (for SDM16 or CS2E0 and higher)         | IOP              |

### Prerequisites

Prior to starting this procedure, you must be aware of the following:

- you must configure additional backup storage to prevent a temporary problem that forces the SBA into long-term backup mode
- the billing stream is aware that the replaced volumes exist, and recovers files from both the swapped-out and swapped-in sets of volumes as part of the recovery process
- the billing stream loses track of swapped-out volumes when a switch of activity (SwAct) or a restart is performed on the DMS or Communication Server 2000 prior to the completion of the recovery of the files
- there is a risk of losing some billing records when you reconfigure or swap-out backup volumes of a stream that is in backup mode during the transition process
- you must allow recovery to complete prior to a switch outage when you choose to swap out an active backup volume during an emergency situation. If not, the billing stream does not recognize the swapped-out volumes.

If you are using or migrating to a XAC16 system, your backup volumes must be on IOP volumes. If your current backup volumes are on SLM or DDU volumes and you are running a previous release, you must migrate to IOP volumes before upgrading to this release.

**ATTENTION**

**Ensure the size for backup volumes is sufficient.**

Refer to Disk space requirements (Calculation of DMS Switch Disk Space Requirements) in procedure Preparing for SBA installation and configuration. The absolute minimum size for backup volumes is 30MB.

**ATTENTION**

Backup volumes must be configured evenly across the available disks of the same disk type in your system.

## Procedures

Use the following procedures to configure SBA backup volumes on the core.

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Calculate disk space to contain backup volumes

| Step                  | Action                                                                                                                                                                                                                                                                                                              |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>At your system</b> |                                                                                                                                                                                                                                                                                                                     |
| 1                     | Write down the dms_disk_space value from the procedure Preparing for SBA installation and configuration (answer 31), which shows the amount of disk space required for the backup volumes.                                                                                                                          |
| 2                     | Determine the amount of disk space of each disk type in your system to be used for storing the backup volumes. Divide the value you recorded in <a href="#">step 1</a> by the maximum volume size supported for the appropriate disk types for your system, obtained from the following table. Record these values. |
| 3                     | Ensure that the backup volumes can fit on the disks in your system. Compare the values that you recorded in <a href="#">step 2</a> with the maximum                                                                                                                                                                 |

#### At your system

- Write down the dms\_disk\_space value from the procedure Preparing for SBA installation and configuration (answer 31), which shows the amount of disk space required for the backup volumes.
- Determine the amount of disk space of each disk type in your system to be used for storing the backup volumes. Divide the value you recorded in [step 1](#) by the maximum volume size supported for the appropriate disk types for your system, obtained from the following table. Record these values.

| Disk type | Maximum disks per core | Maximum volumes per device | Maximum volumes configurable for SBA | Maximum volume size |
|-----------|------------------------|----------------------------|--------------------------------------|---------------------|
| IOP       | 2                      | 32                         | 64                                   | 2GB                 |
| 3PC       | 2                      | 32                         | 64                                   | 2GB                 |
| DDU       | 10                     | 32                         | 69                                   | 64MB                |
| SLM       | 2                      | 32                         | 64                                   |                     |

- Ensure that the backup volumes can fit on the disks in your system. Compare the values that you recorded in [step 2](#) with the maximum



number of volumes supported for the disk types in your system, obtained from the table in [step 2](#). Determine the next step to perform:

| If the number of volumes obtained in <a href="#">step 2</a> | Do                                |
|-------------------------------------------------------------|-----------------------------------|
| is less than or equal to the maximum number allowed         | <a href="#">step 4</a>            |
| is greater than the maximum number allowed                  | contact the next level of support |

- 4 Determine the next steps to perform.

| To configure disk type | Use this procedure                                     |
|------------------------|--------------------------------------------------------|
| DDU                    | "Configuring DDU disk drive backup volumes" (page 165) |
| IOP                    | "Configuring IOP disk drive backup volumes" (page 169) |
| SLM                    | "Configuring SLM disk drive backup volumes" (page 172) |
| 3PC                    | "Configuring 3PC disk drive backup volumes" (page 174) |

---

—End—

---

## Configuring DDU disk drive backup volumes

| Step | Action |
|------|--------|
|------|--------|

**At the MAP**

- Post the billing stream:  

```
mapci;mtc;appl;sdmbil;post <stream_name>
```

where  
<stream\_name> is the name of the billing stream
- Obtain information about the existing backup volumes for the billing stream:  

```
conf view <stream_name>
```

where  
<stream\_name> is the name of the billing stream

SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

The system displays the name of each backup volume in the stream. Record each backup volume name for future reference.

- 3** Quit out of the MAPCI level:

```
quit all
```

- 4** Display and record the size of a volume and its number of free blocks:

```
dskut;sv <volume name>
```

where

<volume name> is the name of one of the volumes that you obtained and recorded in [step 2](#)

- 5** Repeat [step 5](#) for each volume name that you recorded in [step 2](#).

- 6** Create an eight-character, alphanumeric name for each of the new backup volumes that you determined in the procedure, "[Calculate disk space to contain backup volumes](#)" ([page 164](#)) and record each of these names for future reference.

DDU volume names can be up to eight alphanumeric characters in length, with the first four characters reserved for the disk prefix.

Logical volumes must be configured evenly across the disks.

- 7** Access the IOD level:

```
mapci;mtc;iod
```

- 8** Locate the DDUs:

```
listdev ddu
```

- 9** Record the DDU numbers and their respective IOC, CARD, and PORT locations for future reference.

- 10** Begin to busy a DDU:

```
ioc <ioc>
```

where

<ioc> is the IOC controlling the respective DDU

- 11** Display the DDU card:

```
card <ddu_card>
```

where

`<ddu_card>` is the DDU card number

- 12 Complete the busy process:

`bsy`

- 13 Confirm the DDU card number that you selected in [step 11](#) indicates a status of ManB.

- 14 Display the free space for this DDU:

`dskalloc <ddu #>`

where

`<ddu #>` is the DDU card number

Record the free space amount from the `dskalloc` command that is displayed, for future reference.

- 15 Determine DDU disk space availability.

| If you have                                                             | Do                      |
|-------------------------------------------------------------------------|-------------------------|
| located a DDU with sufficient disk space for the new backup volumes     | <a href="#">step 19</a> |
| not located a DDU with sufficient disk space for the new backup volumes | <a href="#">step 16</a> |

- 16 Return the DDU to service:

`rts`

- 17 Return to the IOC level:

`quit`

- 18 Repeat [step 10](#) through [step 17](#) until you locate a DDU with sufficient space for the new backup volumes.

- 19 Create a new logical volume:

`add <volume> <blocksize>`

where

`<volume>` is the backup volume name

`<blocksize>` is the size of the volume. Calculate this by multiplying the maximum volume size allowed for the DDU disk, which is shown in the table in [step 2](#) of the procedure "[Calculate disk space to contain backup volumes](#)" ([page 164](#)), by 1024.

#### Example

`add AMA8 51200`

This example prompts the system to create the logical volume D000AMA8, consisting of 51200 1024-byte blocks (50 Mbyte) of available disk space.

If you receive an error message while updating the last DDU volume with 64 Mbyte, this volume must be configured with a size less than 32767 blocks.

- 20** Verify the names of the volume identifiers:

`display`

- 21** Add an allocation volume to the root directory:

`diradd <backup_volume>`

where

`<backup_volume>` is the backup volume name

- 22** Update the volume identifiers:

`update`

- 23** Repeat [step 19](#) through [22](#) until each new logical volume has been created.

- 24** Exit the disk administration level:

`quit`

- 25** Return the DDU to service:

`mapci;mtc;iod;ddu <#> ;rts`

where

`<#>` is the DDU disk drive number (0 or 1) that you busied in [step 12](#)

- 26** Return to the MAPCI level:

`quit`

- 27** Configure the billing stream of the logical volumes you created in [step 19](#) through [23](#) once you receive confirmation that the files are successfully created. Performing the procedure, Configuring SBA backup volumes on a billing stream.

- 28** Exit back to the command prompt:

`quit all`

You must alert all operating company personnel who work on the core, and provide the names of the old and new backup volumes and the procedure you used to swap the volumes. They must

understand that any restarts or activity switch (SwAct) that occurs before the billing stream returns to normal mode can cause a loss of billing records.

It is imperative that the mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.

29 You have completed this procedure.

---

—End—

---

## Configuring IOP disk drive backup volumes

---

### Step Action

---

#### *At the MAP*

1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where

**<stream\_name>** is the name of the billing stream

2 Obtain information about the existing backup volumes for the billing stream:

```
conf view <stream_name>
```

where

**<stream\_name>** is the name of the billing stream

SBA does not support the configuration of more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

The system displays the name of each backup volume in the stream. Record each backup volume name for future reference.

3 Quit out of the MAPCI level:

```
quit all
```

4 Display and record the size of a volume and its number of free blocks:

```
diskut;lv <volume_name>
```

where

**<volume\_name>** is the name of one of the volumes that you obtained and recorded in [step 2](#)

- 5 Repeat [step 4](#) for each volume name that you recorded in [step 2](#).
- 6 Create an alphanumeric name, consisting of a maximum of twelve characters, for each of the new backup volumes that you determined in the procedure "[Calculate disk space to contain backup volumes](#)" ([page 164](#)). Record each of these names for future reference.

IOP volume names on the IOP disks can be up to twelve alphanumeric characters in length, with the first four characters reserved for the disk prefix.

Logical volumes must be configured evenly across the disks.

- 7 Access the disk administration level:

```
diskadm <disk prefix>
```

where

**<disk prefix>** is one of the prefixes assigned to the two disks; for example, F02L or F17D.

- 8 Determine the free disk space:

```
dd
```

- 9 Note the following example, which is a response to the command performed in [step 8](#), choosing the F02L disk name.

Disk drive information for F02L

```
Date last formatted : 2000/01/01 01:00:50.145 THU.
Date last modified : 2001/09/26 11:22:38.587 WED.
Total space for volumes : 4095 Mbytes
Total free space : 1014 Mbytes
Size of largest free segment : 1014 Mbytes
Total number of volumes : 14
```

1 Block = 512 bytes

- 10 Determine the size of the largest free segment.

| If the size of the largest free segment is                                       | Do                                                                       |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| greater than or equal to the maximum allowable volume size for the IOP disk type | <a href="#">step 11</a>                                                  |
| less than the maximum allowable volume size for the IOP disk type                | contact your next level of support before proceeding with this procedure |

- 11 Create a new logical volume:

```
cv <volume> <size> ftf s
```

where

<volume> is the backup volume name

<size> is the size of the volume. Compare the size recorded in [step 1](#) of the procedure "Calculate disk space to contain backup volumes" (page 164), with the allowable size for the IOP disk type (obtained from the table under [step 2](#) of the same procedure. The lesser of the two values must be entered as this size.

**Example**

```
cv AMA8 50 ftf s
```

This entry prompts the system to create the logical volume F17LAMA8, consisting of 50 Mbyte (102400 512-byte blocks) of available disk space.

- 12** Exit the disk administration level at the prompt:

```
quit
```

- 13** Repeat [step 7](#) through [12](#) until all new logical volumes have been created.

- 14** Exit to the command prompt:

```
quit all
```

- 15** Configure the billing stream of the logical volumes you created in [step 11](#) through [14](#) once you receive confirmation that the files are successfully created. Perform the procedure Configuring SBA backup volumes on a billing stream.

- 16** Exit back to the command prompt:

```
quit all
```

You must alert all operating company personnel who are associated with the DMS switch. Provide the names of the old and new backup volumes and the procedure you used to swap the volumes. They must be made aware of that any RESTARTs or SwActs that occur before the billing stream returns to normal mode can cause a loss of billing records.

Also, it is imperative that the mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.

- 17** You have completed this procedure.

---

—End—

---

## Configuring SLM disk drive backup volumes

| Step | Action |
|------|--------|
|------|--------|

### At the MAP

- 1 Post the billing stream:  

```
mapci;mtc;appl;sdmbil;post <stream_name>
```

where

**<stream\_name>** is the name of the billing stream
  - 2 Obtain the names of the existing backup volumes for the billing stream:  

```
conf view <stream_name>
```

where

**<stream\_name>** is the name of the billing stream

SBA does not support the configuration of more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

The system displays the name of each backup volume in the stream. Record each backup volume name for future reference.
  - 3 Quit out of the MAPCI level:  

```
quit all
```
  - 4 Display and record the size of a volume and its number of free blocks:  

```
diskut;lv <volume_name>
```

where

**<volume\_name>** is the name of one of the volumes that you obtained and recorded in [step 2](#)
  - 5 Repeat [step 4](#) for each volume name that you recorded in [step 2](#).
  - 6 Create an eight-character, alphanumeric name for each of the new backup volumes that you determined in the procedure "[Calculate disk space to contain backup volumes](#)" ([page 164](#)). Record each of these names for future reference.
- SLM volume names on the SLM disks can be up to eight alphanumeric characters in length for the core manager, with the first four characters reserved for the disk prefix.
- Logical volumes must be configured evenly across the disks.
- 7 Busy SLM 0:



```
mapci;mtc;iod;slm 0;bsy
```

- 8 Access the disk administration level:

```
diskadm <disk prefix>
```

where

**<disk prefix>** is one of the prefixes assigned to the two disks; for example, S00D or S01D

- 9 Determine the free disk space:

```
dd
```

- 10 Note the following example, which is a response to the command you performed in [step 9](#), choosing the S00D disk name.

```
Disk drive information for S00D
Drive name: S00D
Vendor Information : SEAGATE ST31051N 9470
Date last formatted : 2000/01/01 05:38:44.718
THU.
Date last modified : 1998/04/23 17:46:59.754
THU.
Total space for volumes : 1000 Mbytes
Total Free space : 174 Mbytes
Size of largest free segment : 174 Mbytes

1 Block = 512 bytes
```

| If the size of the largest free segment is                                       | Do                                 |
|----------------------------------------------------------------------------------|------------------------------------|
| greater than or equal to the maximum allowable volume size for the SLM disk type | <a href="#">step 11</a>            |
| less than the maximum allowable volume size for the SLM disk type                | contact your next level of support |

- 11 Create a new logical volume:

```
cv <volume> <volume_size> std
```

where

**<volume>** is the backup volume name

**<volume\_size>** is the size of the volume. Compare the size recorded in [step 1](#) of the procedure "Calculate disk space to contain backup volumes" (page 164) with the allowable size for the IOP disk type (obtained from the table under [step 2](#) of the same procedure. The lesser of the two values must be entered as this size.

#### Example

```
cv AMA8 50 std
```

This entry prompts the system to create the logical volume S00DAMA8, consisting of 50 Mbyte (102400 512-byte blocks) of available disk space.

- 12 Exit the disk administration level at the prompt:  
`quit`
- 13 RTS the SLM 0 disk drives that you busied in step 7 to an InSv state:  
`mapci;mtc;iod;slm 0;rts`
- 14 Exit to the command prompt:  
`quit all`
- 15 Repeat 7 to 14 until all volumes have been created.
- 16 Configure the billing stream of the logical volumes you created in step 11 through 14 once you receive confirmation that the files are successfully created, by performing the procedure Configuring SBA backup volumes on a billing stream
- 17 Exit back to the command prompt:  
`quit all`

You must alert all operating company personnel who are associated with the DMS switch. Provide the names of the old and new backup volumes and the procedure you used to swap the volumes. They must be made aware of that any RESTARTs or SwActs that occur before the billing stream returns to normal mode can cause a loss of billing records.

Also, it is imperative that the mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.
- 18 You have completed this procedure.

---

—End—

---

## Configuring 3PC disk drive backup volumes

---

| Step | Action |
|------|--------|
|------|--------|

---

### *At the MAP*

- 1 Post the billing stream:  
`mapci;mtc;appl;sdmbil;post <stream_name>`  
where

- `<stream_name>` is the name of the billing stream
- 2 Obtain information about the existing backup volumes for the billing stream:  
`conf view <stream_name>`  
 where  
`<stream_name>` is the name of the billing stream  
 SBA does not support the configuration of more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.  
 The system displays the name of each backup volume in the stream. Record each backup volume name for future reference.
  - 3 Quit out of the MAPCI level:  
`quit all`
  - 4 Display and record the size of a volume and its number of free blocks:  
`diskut;lv <volume_name>`  
 where  
`<volume_name>` is the name of one of the volumes that you obtained and recorded in [step 2](#)
  - 5 Repeat [step 4](#) for each volume name that you recorded in [step 2](#).
  - 6 Create a twelve-character, alphanumeric name for each of the new backup volumes that you determined in the procedure "[Calculate disk space to contain backup volumes](#)" ([page 164](#)). Record each of these names for future reference.  
 3PC volume names on the 3PC disks can be up to twelve alphanumeric characters in length, with the first four characters reserved for the disk prefix.  
 Logical volumes must be configured evenly across the disks.
  - 7 Access the disk administration level:  
`diskadm <disk_prefix>`  
 where  
`<disk_prefix>` is one of the prefixes assigned to the two disks; for example, FD00 or FD01
  - 8 Determine the free disk space:  
`dd`

- 9 Note the following example, which is a response to the command performed in [step 8](#), choosing the FD00 disk name.

Disk drive information for FD00

```
Date last formatted : 2000/01/01 01:00:50.145 THU.
Date last modified : 2001/09/26 11:22:38.587 WED.
Total space for volumes : 4095 Mbytes
Total free space : 1014 Mbytes
Size of largest free segment : 1014 Mbytes
Total number of volumes : 14
```

1 Block = 512 bytes

- 10 Determine the size of the largest free segment.

| If the size of the largest free segment is                                       | Do                                                                       |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| greater than or equal to the maximum allowable volume size for the IOP disk type | <a href="#">step 11</a>                                                  |
| less than the maximum allowable volume size for the IOP disk type                | contact your next level of support before proceeding with this procedure |

- 11 Create a new logical volume:

**cv <volume> <size> ftfs**

where

**<volume>** is the backup volume name

**<size>** is the size of the volume. Compare the size recorded in [step 1](#) of the procedure "[Calculate disk space to contain backup volumes](#)" ([page 164](#)) with the allowable size for the IOP disk type (obtained from the table under [step 2](#) of the same procedure. The lesser of the two values must be entered as this size.

**Example**

cv AMA8 50 ftfs

This entry prompts the system to create the logical volume FD00AMA8, consisting of 50 Mbyte (102400 512-byte blocks) of available disk space.

- 12 Exit the disk administration level at the prompt:

**quit**

- 13 Repeat [step 7](#) through [step 12](#) until all new logical volumes have been created.

- 14 Exit to the command prompt:  
`quit all`
- 15 Configure the billing stream of the logical volumes you created in [step 11](#) through [14](#) once you receive confirmation that the files are successfully created, by performing the procedure Configuring SBA backup volumes on a billing stream
- 16 Exit back to the command prompt:  
`quit all`  

You must alert all operating company personnel who are associated with the DMS switch. Provide the names of the old and new backup volumes and the procedure you used to swap the volumes. They must be made aware of that any RESTARTs or SwActs that occur before the billing stream returns to normal mode can cause a loss of billing records.

Also, it is imperative that the mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.
- 17 You have completed this procedure.

---

—End—

---

## Restore operations

Restore operations are performed when it is necessary to apply previously backed-up data to the current component. The following table lists the procedures used to restore CVoIP components.

### Component restoration procedures

| Component                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Procedure (s)                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| NETWORK INTELLIGENCE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                            |
| CS 2000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | "Bootting the XA-Core from a Reset Terminal" (page 181)                                                                                    |
| Call Agent                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | "Restoring a Call Agent" (page 186)<br>"Restoring files from a DVD-RW" (page 189)                                                          |
| SAM21                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | "Reloading or restarting a SAM21 Shelf Controller" (page 193)                                                                              |
| GWC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Restart or reboot a GWC card                                                                                                               |
| Session Server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Session Server - Trunks backup"Restoring SST" (page 200)                                                                                   |
| Policy Controller                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | "Prepare for a database restore on a Policy Controller unit" (page 206)"Perform a database restore to a Policy Controller unit" (page 211) |
| Ethernet Routing Switch 8600                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | "Resetting the Ethernet Routing Switch 8600 using a saved configuration file" (page 213)                                                   |
| UAS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | "Restoring UAS configuration files" (page 111) "Restoring audio files to a UAS node" (page 115)                                            |
| MS 2000 Series                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Restoring audio files to a Media Server 2000 Series node                                                                                   |
| APS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | "Restoring the APS-specific Oracle database and application files" (page 120)                                                              |
| USP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Administration: Restore Operations                                                                                                         |
| Real-time Transport Protocol (RTP) Media Portal                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | RTP Media Portal Basics, NN10367-111                                                                                                       |
| CICM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | CICM Security and Administration, NN10252-611                                                                                              |
| CORE NETWORK                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                            |
| <p><b>Note 1:</b> The IW SPM and MG 4000 are automatically restored when the CS 2000 is restored. The MG 9000 is restored when the MG 9000 Manager is restored.</p> <p><b>Note 2:</b> The MDM is restored by copying files from tape or an off box storage system through UNIX commands or CRON jobs.</p> <p><b>Note 3:</b> The USP Manager is restored using the two disaster recovery disks created in the Administration: Creating Disaster Recovery Floppy Disks procedure. Insert Disaster Recovery Disk #1 into the A: drive of your OAM&amp;P workstation and follow the instructions.</p> |                                                                                                                                            |

| Component                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Procedure (s)                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multiservice Switch or Media Gateway devices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | "Restoring Multiservice Switch or Media Gateway service data" (page 223)                                                                                                                                                                                                                         |
| GATEWAYS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                  |
| MG 9000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | none (See Note 1)                                                                                                                                                                                                                                                                                |
| MG 4000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | none (See Note 1)                                                                                                                                                                                                                                                                                |
| IW SPM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | none (See Note 1)                                                                                                                                                                                                                                                                                |
| NETWORK MANAGEMENT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                  |
| Core Element Manager (CEM)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | "Restoring Core Element Manager data " (page 229)                                                                                                                                                                                                                                                |
| CS 2000 Core Manager or CBM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Performing a full restore of the software from S-tape<br>Performing a partial restore of the software from S-tape<br>"Recovering backup files from lost backup volumes" (page 251)                                                                                                               |
| CS 2000 Management Tools                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | "Restoring the oracle data on an SPFS-based server" (page 254)<br>"Performing a full system restore on an SPFS-based server" (page 262)                                                                                                                                                          |
| IEMS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | "Restoring the oracle data on an SPFS-based server" (page 254)<br>"Performing a full system restore on an SPFS-based server" (page 262)<br><br><b>Note:</b> If the central security server is configured on the IEMS, a central security server restore is needed after the full system restore. |
| IEMS centralized security server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Restoring the central security server                                                                                                                                                                                                                                                            |
| MG 9000 Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | "Restoring the oracle data on an SPFS-based server" (page 254)<br>"Performing a full system restore on an SPFS-based server" (page 262)                                                                                                                                                          |
| MDM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | none (See Note 2)                                                                                                                                                                                                                                                                                |
| USP Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | none (See Note 3)                                                                                                                                                                                                                                                                                |
| <p><b>Note 1:</b> The IW SPM and MG 4000 are automatically restored when the CS 2000 is restored. The MG 9000 is restored when the MG 9000 Manager is restored.</p> <p><b>Note 2:</b> The MDM is restored by copying files from tape or an off box storage system through UNIX commands or CRON jobs.</p> <p><b>Note 3:</b> The USP Manager is restored using the two disaster recovery disks created in the Administration: Creating Disaster Recovery Floppy Disks procedure. Insert Disaster Recovery Disk #1 into the A: drive of your OAM&amp;P workstation and follow the instructions.</p> |                                                                                                                                                                                                                                                                                                  |

**ATTENTION**

When backing up devices that use certificates provided by the IEMS/Certificate Manager and/or Preshared Keys for IPSec, always note the versions of the data in the back-up image of the device. Due to the timing sensitivity of this data, a potential conflict can occur during restore between the version of the data in the back-up image versus the current version of the data.

See procedure *Restoring certificates and Pre-shared Keys for IPSec* in NTP NN10450-900, *Carrier Voice over IP Solutions Disaster Recovery Procedures*, for precautionary and recovery information. Nortel also recommends conducting regular full system backups and critical data backups according to corporate policy. This measure ensures that the most recent backup version is restored, and that a disaster recovery process is performed quickly.



---

## Booting the XA-Core from a Reset Terminal

---

**ATTENTION**

Booting the switch causes the switch to drop all calls.

This procedure boots the XA-Core from a reset terminal display.

**Note:** An image loads from a small computer systems interface (SCSI) device. The SCSI device can be in a disk or a digital audio tape (DAT).

### Common Procedures

There are no common procedures.

### Stepwise Procedure

Use this procedure to boot the XA-Core from a reset terminal display.

**CAUTION****Call your next level of support**

Contact your next level of support before performing this procedure.

**CAUTION****Extended service interruption**

A longer recovery time occurs for a switch boot from tape than a switch boot from disk.

To minimize recovery time, boot from disk.

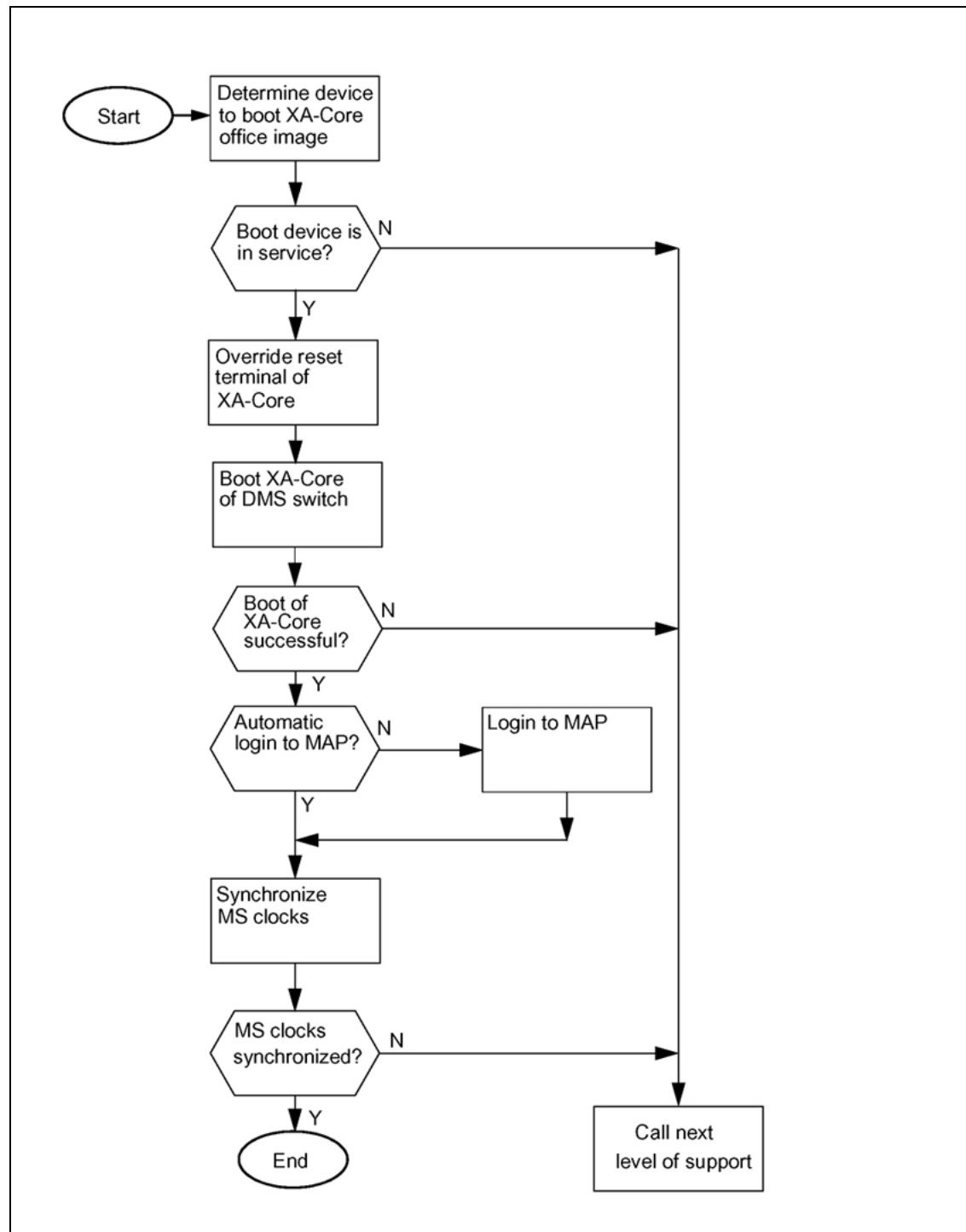
**CAUTION****Extended service interruption**

Log-in procedures can vary depending on your office configuration.

If you need additional help, contact your next level of support.

The following flowchart summarizes this recovery procedure.

**Note:** Press the <ENTER> key to execute typed commands.

**Booting an XA-Core from a reset terminal**

## How to boot an XA-Core from a reset terminal

| Step | Action |
|------|--------|
|------|--------|

### At your current location

- 1 Refer to office records and determine the name of the XA-Core recording device that contains the last office image file.

**Note:** The XA-Core recording device is a disk drive or a tape drive for a digital audio tape (DAT). Record the name of the XA-Core device.

### At the XA-Core shelf

- 2 Make sure that the disk drive or the tape drive that you recorded in [step 1](#) is in-service.

**Note:** The device is in-service when the green light-emitting diode (LED) is on (illuminated).

| If the device is | Do                      |
|------------------|-------------------------|
| in service       | <a href="#">step 3</a>  |
| not in service   | <a href="#">step 13</a> |

### At the XA-Core reset terminal

- 3 Override the XA-Core reset terminal by typing:

```
>\OVERRIDE
```

*Example of a reset terminal response*

```
NOW IN SERVICE AFFECTING MODE
```

- 4 Boot the XA-Core by typing:

```
>\BOOT <nn> <s> <p>
```

where

<nn> is the slot number parameter value to indicate the number of the physical shelf slot - 0 to 18

<s> is the side parameter value to indicate the circuit pack or packlet location in the physical shelf - front (f) or rear (r)

<p> is the position parameter value that indicates the IOP bay - either upper (u) or lower (l)

**Example**

```
>\BOOT 4 F L
```

*Example of system response:*

Warning: Boot command will take it out of service.

Please confirm ("YES", "Y", "NO", or "N")

Type **Y** to confirm the command.

- 5 Monitor the reset terminal display to determine if the switch has booted.

**Note:** The reset terminal displays a response to indicate a boot in progress. The response also displays diagnostic messages and alphanumeric addresses. When the switch has completely booted, a prompt appears on the display.

*One possible example of a reset terminal response*

CI:

>

*Another possible example of a reset terminal response*

FWCI>

| If the response has                  | Do                      |
|--------------------------------------|-------------------------|
| a prompt                             | <a href="#">step 6</a>  |
| no prompt after approximately 15 min | <a href="#">step 13</a> |

#### **At the MAP terminal**

- 6 Press the <BREAK> key to determine if you have to log in.

**Note:** The log-in message indicates that you have to manually log in. An automatic log in can occur if the office parameters have automatic log in.

*Example of a MAP response*

Please Login.

| If log in is  | Do                      |
|---------------|-------------------------|
| not automatic | <a href="#">step 7</a>  |
| automatic     | <a href="#">step 10</a> |

- 7 Login to the MAP terminal by typing:

>LOGIN

*Example of a MAP response*

Enter User Name

- 8 Enter your user name by typing:

><user\_name>

where

**<user\_name>** is the name of the user for the account.

*Example of a MAP response*

Enter Password

- 9 Enter the password by typing:

**><password>**

where

**<password>** is the name of the password for the account.

*Example of a MAP response*

SuperNode\_1 Logged in on 1997/01/15 at 20:37:17

- 10 Access the MS Clock level of the MAP display by typing:

**>MAPCI;MTC;MS;CLOCK**

- 11 Synchronize the clocks by typing:

**>SYNC**

| If the MAP response is  | Do                      |
|-------------------------|-------------------------|
| a successful completion | <a href="#">step 12</a> |
| a failure               | <a href="#">step 13</a> |

- 12 You have completed this procedure.

***Non-standard condition found***

- 13 For additional help, contact your next level of support.

---

—End—

---

## Restoring a Call Agent

This procedure describes how to restore an archived call processing application image from tape.



### CAUTION

#### Possible service interruption

Do not use this procedure when in an emergency situation with no stable call processing application image.

If in a situation without a restartable image, contact Nortel Global Network Product Support (GNPS) immediate. Attempting to use this method without a valid call processing application image could fail due to constant resets on the Call Agent.

## Restoring a Call Agent

### Step Action

*At the SDM*

- 1 Insert the DAT cassette with the image to restore.

*At the CS 2000 Core Manager*

- 2 Restore the image from tape. This step requires root privilege.

```
cd /swd/3pc
tar xvf /dev/rmt0
```

*At the Call Agent Manager*

- 3 Log in to the inactive Call Agent and change directory to the location in which to restore the image. Verify that enough disk space exists to hold the image.

```
[mtc@hostname mtc]$ cd /3PC/sd00/image0
[mtc@hostname image0]$ df -h .
Filesystem Size Used Avail Use% Mounted on
172.16.16.24:/nfsserv/3pc/cs/sd00
 8.0G 6.6G 1.4G 82% /3PC/sd00
```

- 4 Open a file transfer protocol (FTP) session to the CS 2000 Core Manager, and transfer the image. It may be necessary to become the super user to transfer the file.

```
[mtc@hostname image0]$ su
Password:<root_password>
[root@hostname image0]# ftp <core_manager_ip>
Connected to <core_manager_ip>
220 <core_manager_ip> SFTP Server (Version 19.0.0.0 Nov 14
Name (<core_manager_ip>:mtc): root
Password: <root_passwd>
230 User root logged in.
ftp> bin
200 Type set to I.
ftp> cd /swd/3pc %% or location of restored image
250 CWD command successful.
ftp> get IMG_TO_RESTORE
local: IMG_TO_RESTORE remote: IMG_TO_RESTORE
227 Entering Passive Mode (10,40,44,6,195,224)
150 Opening data connection for IMG_TO_RESTORE (binary mode
226 Transfer complete.
225820860 bytes received in 332 secs (6.7e+02 Kbytes/sec)
ftp> bye
221 Goodbye.
```

*At the MAP*

- 5 Enter the DISKUT level and use the **IMPORT** command to make the image available to the call processing application.

```
CI:
>DISKUT
Disk utility is now active.
DISKUT:
>IMPORT SD00IMAGE0 IMG_TO_RESTORE IMAGE 1020
 IMG_TO_RESTORE : Failed to get record length.
Import: IMG_TO_RESTORE size: 199 MB
 as: IMG_TO_RESTORE lrecl: 1020 type: image.

Attempting to import 1 file selected on SD00IMAGE0.

Imported IMG_TO_RESTORE as IMG_TO_RESTORE.

Imported 1 file successfully of 1 attempt on SD00IMAGE0.
>
```

If additional space is needed to import the image, the **IMPORT** command offers to expand the volume.

- 6 Set the image in the Image Table of Contents (ITOC).

```

>QUIT ALL
CI:
>ITOC CI
ITOC User Interface is now active.
ITOC CI:
>SBF CM IMG_TO_RESTORE 15
IMG_TO_RESTORE is registered in CM ITOC.
The updated ITOC is listed directly below.
Image Table Of Contents:
 A Registered Generic Device File
 L Date Time Name
 R MM/DD/YYYY HH:MM:SS

0 * 02/21/2003 16:59:04 SD01ADUMP1 3PC_LAB1_CSNNC06
1 02/24/2003 11:00:53 SD01ADUMP1 3PC_LAB1_CSNNC06
2 02/28/2003 08:15:29 SD00IMAGE0 IMG_TO_RESTORE
>

```

- 7 The restored image is now available for booting.  
This procedure is complete.

---

—End—

---



## Restoring files from a DVD-RW

### Application

Use this procedure to restore office images from a digital video disk read write optical disk (DVD-RW). Do not restore an image and overwrite one with the same name.

To restore a volume from DVD-RW, contact Nortel support personnel.

### Interval

Perform this procedure when required by your office.

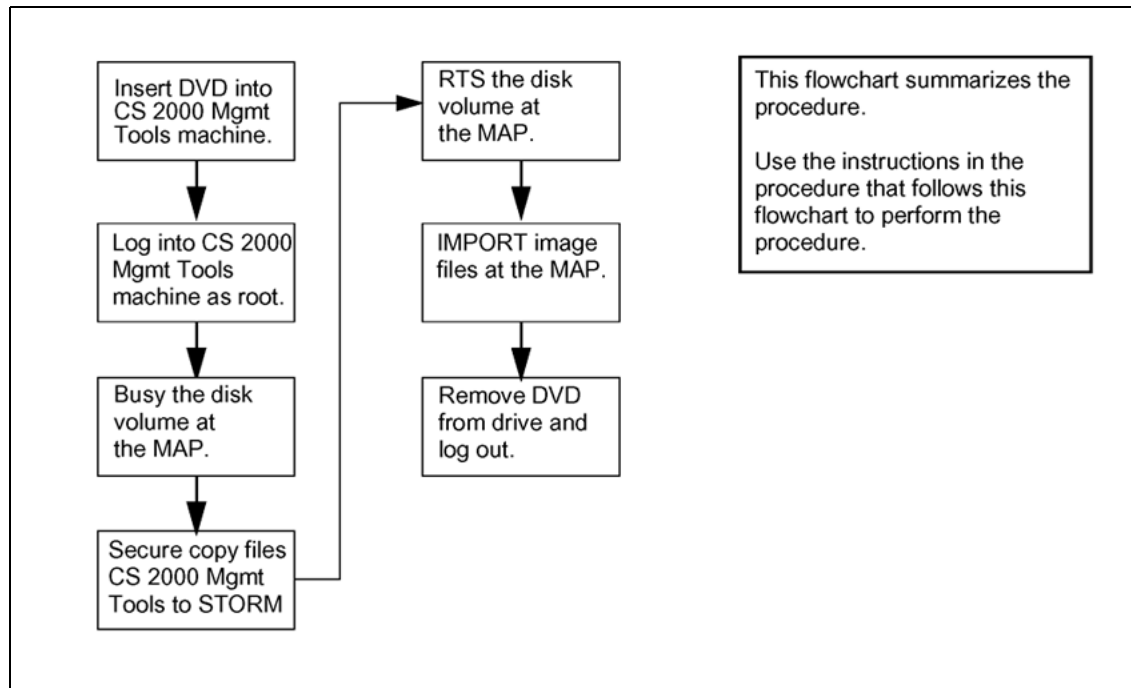
### Common procedures

Understanding of the **IMPORT** command in DISKUT, **SCANF** for listing volumes, and the **CBF**, **LBF**, and **SBF** commands in ITOCCI is required. The IP addresses of the STORM units are needed. Use the **mount** command from a Call Agent card to determine the addresses.

### Action

This procedure contains a summary flowchart as a summary of the procedure. Follow the exact steps to perform this procedure.

#### Summary of restoring files from a DVD-RW



---

| Step | Action |
|------|--------|
|------|--------|

---

**At the CS 2000 Management Tools server**

- 1 Insert the DVD-RW into the DVD tray. If the CS 2000 Management Tools server is a pair of Sun Microsystems Netra 240s, put the DVD in the unit with the USER LED lit.

*Volume management software on the CS 2000 Management Tools server operating system mounts the DVD-RW.*

- 2 List the contents:

```
$ ls -as /cdrom/cdrom0
```

*The contents of the DVD are printed.*

- 3 Change directory to the DVD-RW:

```
$ cd /cdrom/cdrom0
```

**At the MAP**

- 4 Enter the DISKADM level and busy the volumes to copy:

```
> DISKADM <sd0x>; BSY <volname>
```

```
> QUIT
```

**sd0x**

is SD00 or SD01

**volname**

is the name of the volume such as TEMP

*The BSY command fails if applications have open files on any volume for the device. A busied disk may affect data recording or retrieval for applications. Consider step 6 to RTS the volume as soon as possible or convenient after copying the files.*

*If applications are active and writing to the volume, determine if the application can ROTATE the disk writing activity to a backup volume. If unsure, contact your next level of support.*

**At a CS 2000 Management Tools server terminal**

- 5 Secure copy the files from the DVD-RW on the CS 2000 Management Tools server to one STORage Management (STORM) unit:

```
$ scp <image_files>
```

```
i^root@stormip>:~/path_to_files>i±
```

**image\_files**

is the file name for a single image file, or a wildcard expression such as "\*\_CM"

**stormip**

is the IP Address of the STORM unit such as 172.18.96.6

**/path\_to\_files**

is the absolute path to the files on the STORM unit to place the files such as /nfsserv/3pc/cs/sd00/image1

**Example**

Copy an office image named S040210135002\_CM to SD00IMAGE1:

```
$ scp S040210135002_CM
"root@<stormip>:/nfsserv/3pc/cs/sd00/image1"
```

**Note:** The first time this command is issued, the secure copy program provides a prompt to exchange keys. Confirm the exchange with a "y."

*The secure copy program provides a progress indicator during the copy. Wait for the copy to complete and the \$ prompt to return.*

**At the MAP**

- 6 Enter the DISKADM level and RTS the volume:

```
> DISKADM <sd0x>; RTS <volname>
> QUIT
```

- 7 Enter the DISKUT level and IMPORT the image files:

```
> DISKUT; IMPORT SD00IMAGE1
> QUIT
```

*The status of the IMPORT command is printed.*

**IMPORT result**

```
> IMPORT SD00IMAGE1
Attempting to import 1 file selected on SD00IMAGE1.

Imported S040210135002_CM as S040210135002_CM IMAGE 1020.

Imported 1 file successfully of 1 attempt on SD00IMAGE1.
```

- 8 List the contents of the volume so the file can be added to the Image Table of Contents (ITOC) in the next step:

```
> SCANF SD00IMAGE1
```

*The contents of the volume are printed.*

- 9 Enter ITOCCI and register the image in the ITOC:

```
> ITOCCI
> SBF CM S040210135002_CM <itoc_pos> <alr_flag>
```

**itoc\_pos**

is an integer between 0 and 15, and is a free position in the ITOC.

**alr\_flag**

if this image should be booted for the next restart, specify **ALR**. Otherwise, leave the field blank.

**Note:** To determine if a free position is available, use the **LBF CM** command. If all positions are used, clear the file in position 15. Determine which volume the position 15 is on, use **SCANF** to list that volume, and then use the **CBF CM FILE <image\_name>** command.

***At a CS 2000 Management Tools server terminal***

- 10** Unmount the DVD-RW, eject it, and exit from root privilege:

```
$ eject cdrom
```

***At the CS 2000 Management Tools server***

- 11** Remove the DVD-RW from the tray and close the tray.  
**12** Store the DVD-RW per office procedure.  
**13** This procedure is complete.

---

—End—

---

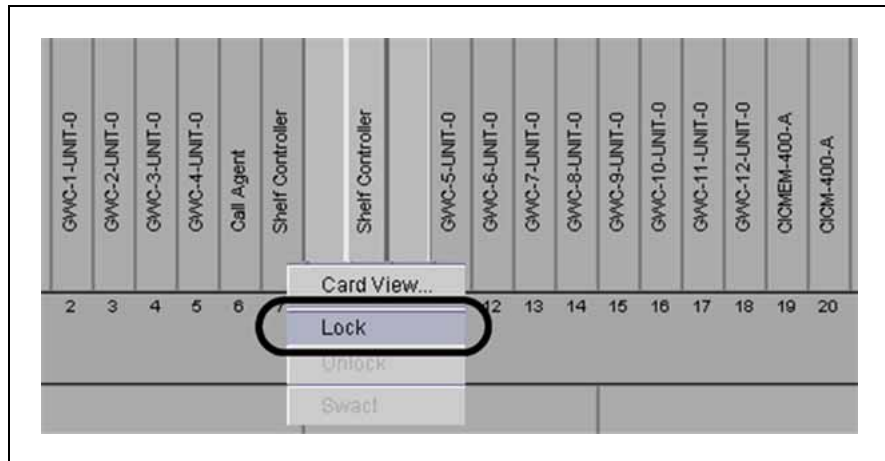
## Reloading or restarting a SAM21 Shelf Controller

### Reloading or restarting a SAM21 Shelf Controller

| Step | Action |
|------|--------|
|------|--------|

*At the CS 2000 SAM21 Manager client*

- 1 From the Shelf View, right click on the card and select Lock from the context menu.



- 2 Wait for the lock icon to appear on the selected card and the other SAM21 Shelf Controller to indicate that it is in simplex (alarm 2C on the other SAM21 Shelf Controller).
- 3 Right click on the card again and select Unlock from the context menu.
- 4 The card resets, downloads software, and reboots.
- 5 This procedure is complete.

—End—

---

## Restart or reboot a GWC card

---

### Purpose of this procedure

Use this procedure to stop all software processes on the GWC card, performs a hardware reset, and reloads the GWC card software from the CS 2000 Core Manager or Core and Billing Manager (CBM).

To restart software applications only, follow procedure ["Restart GWC card services"](#) (page 197).

### When to use this procedure

Use this procedure when you need to reboot a GWC card and force a GWC to download and execute a software load from the CS 2000 Core Manager or CBM.

### Prerequisites

To reduce the risk of service interruption, you can first busy the GWC applications on specific GWC nodes using the CS 2000 GWC Manager. Follow procedure "Disable (Busy) GWC card services" in *Gateway Controller Security and Administration* (NN10213-611).

### Action

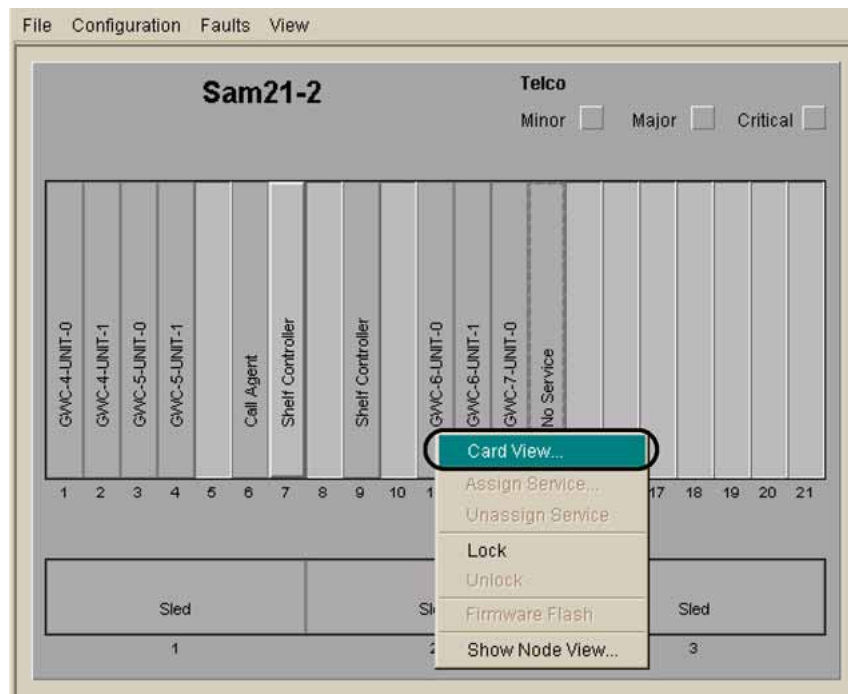
---

| Step | Action |
|------|--------|
|------|--------|

---

*At the CS 2000 SAM21 Manager client*

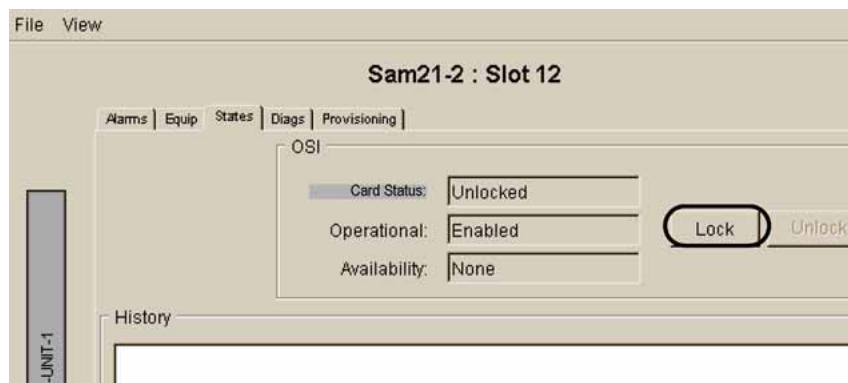
- |   |                                                                                                                     |
|---|---------------------------------------------------------------------------------------------------------------------|
| 1 | From the Shelf View, right-click the GWC card you want to reboot and select <b>Card View</b> from the context menu. |
|---|---------------------------------------------------------------------------------------------------------------------|



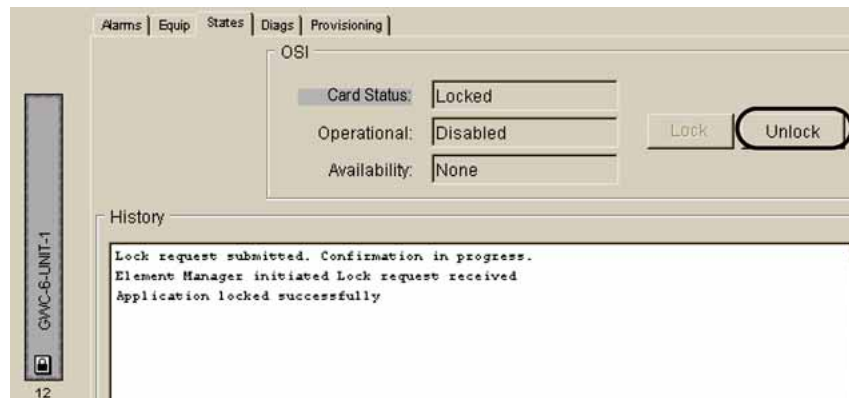
2 At the Card View, select the **States** tab.

3 Click the **Lock** button to lock the card.

The card must be busy (disabled) before you can lock it. If required, see procedure "Disable (Busy) GWC card services" in *Gateway Controller Security and Administration* (NN10213-611).



4 Wait until the Card Status is Locked and the History window indicates "Application locked successfully". Then, click the **Unlock** button.



- 5 Monitor the reboot process. Wait until the Card Status is "Unlocked" and the History window indicates "Bootloaded successfully".
- 6 This procedure is complete.

---

—End—

---



## Restart GWC card services

### Purpose of this procedure

Use this procedure to stop and restart call processing and network services on a standby GWC card.

To restart the hardware and software on an individual GWC card, follow procedure "[Restart or reboot a GWC card](#)" ([page 194](#)).

### When to use this procedure

Use this procedure on a GWC card to determine if a known fault is temporary or persistent and if the fault is limited to the GWC card in question.

### Prerequisites

To reduce the risk of service interruption, ensure that the card you are about to restart is in standby status. Otherwise, perform a call processing switch activity (SWACT) to change the card state from active to standby. If required, see procedure "Invoke a manual protection switch (warm SWACT)" in *Gateway Controller Security and Administration* (NN10213-611).

### Action

| Step                                            | Action                                                                                                                                             |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b><i>At the CS 2000 GWC Manager client</i></b> |                                                                                                                                                    |
| 1                                               | At the main CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.       |
| 2                                               | From the Contents of: Gateway Controller frame, select the appropriate GWC node you wish to restart.                                               |
| 3                                               | Click the <b>Maintenance</b> tab.                                                                                                                  |
| 4                                               | Locate the Activity State field for the GWC unit and determine which unit (card) is active (either unit 0 or unit 1) and which is in standby mode. |
| 5                                               | Click the <b>Busy (Disable)</b> button for the GWC unit on standby.                                                                                |

**Maintenance | Provisioning**

**GWC-7-UNIT-0**

|                       |                |                 |                |
|-----------------------|----------------|-----------------|----------------|
| Administrative state: | unlocked(1)    | Usage state:    | idle(1)        |
| Operational state:    | enabled(1)     | Stand by state: | coldStandby(2) |
| Activity state:       | standby(2) ←   | Swact state:    | noSwAct(0)     |
| Isolation state:      | notisolated(2) | Alarm state:    | 00 00 00 00    |
| Available state:      | 00 00 00 00    | Fault state:    | none(0)        |
| Loadname:             | GI070BN        |                 |                |

Save Image **Busy (Disable)** RTS (Enable) Card View

**GWC-7-UNIT-1**

|                       |                |                 |                     |
|-----------------------|----------------|-----------------|---------------------|
| Administrative state: | unlocked(1)    | Usage state:    | idle(1)             |
| Operational state:    | enabled(1)     | Stand by state: | providingService(3) |
| Activity state:       | active(1)      | Swact state:    | noSwAct(0)          |
| Isolation state:      | notisolated(2) | Alarm state:    | 00 00 00 00         |
| Available state:      | 00 00 00 00    | Fault state:    | none(0)             |
| Loadname:             | GI070BN        |                 |                     |

Save Image Busy (Disable) RTS (Enable) Card View

☐ Force Warm Swact Cold Swact

- 6 At the confirmation box, click **OK** to busy the standby GWC unit. Wait for the CS 2000 GWC Manager screen to update the Operational state of the card to disabled(2). This indicates that the card has been busied
- 7 Click the **RTS (Enable)** button to return the card to service.

**GWC-7-UNIT-0**

|                       |                |                 |                               |
|-----------------------|----------------|-----------------|-------------------------------|
| Administrative state: | locked(2) ←    | Usage state:    | idle(1)                       |
| Operational state:    | disabled(2) ←  | Stand by state: | coldStandby(2)                |
| Activity state:       | standby(2)     | Swact state:    | noSwAct(0)                    |
| Isolation state:      | notisolated(2) | Alarm state:    | minor(3), alarmOutstanding(4) |
| Available state:      | 00 00 00 00    | Fault state:    | none(0)                       |
| Loadname:             | GI070BN        |                 |                               |

Save Image Busy (Disable) **RTS (Enable)** Card View

**GWC-7-UNIT-1**

|                       |                |                 |                     |
|-----------------------|----------------|-----------------|---------------------|
| Administrative state: | unlocked(1)    | Usage state:    | idle(1)             |
| Operational state:    | enabled(1)     | Stand by state: | providingService(3) |
| Activity state:       | active(1)      | Swact state:    | noSwAct(0)          |
| Isolation state:      | notisolated(2) | Alarm state:    | 00 00 00 00         |
| Available state:      | 00 00 00 00    | Fault state:    | none(0)             |
| Loadname:             | GI070BN        |                 |                     |

After 30 seconds, the Administrative state field changes to unlocked and the Operational state field changes to enabled.

|                       |              |
|-----------------------|--------------|
| Administrative state: | unlocked (1) |
| Operational state:    | enabled (1)  |
| Activity state:       | standby (2)  |

The state change is automatic. However, if necessary, you can refresh the screen. At the top of the CS 2000 GWC Manager screen, click the **Windows** menu and select **Refresh GWC Status**.



8 This procedure is complete.

---

—End—

---

## Restoring SST

### Purpose of this procedure

Use this procedure to restore a backup copy of critical files to a unit.

### Limitations and Restrictions



#### CAUTION

Performing a restore of the SIP Gateway application database to the active unit is a service affecting activity and can cause data mismatches at the CS 2000.

### Prerequisites

You must have secure file transfer access, such as scp, to the unit from a remote host if the backup file is stored on a remote host.

Backups are also stored locally on each unit in directory `/data/bkresmgr/backup`.



#### CAUTION

Both units must be free of any Session Server Manager patches before the database is restored. This is accomplished by reinstalling the current version of the SIP Gateway application software (performed in step 1 below). It is not necessary to remove NCGL patches.

### Action

| Step | Action |
|------|--------|
|------|--------|

#### *At the NCGL CLI or IEMS client*

- 1 If either unit has Session Server Manager patches applied, reinstall the current application software on both units by performing the procedure "Upgrade/rollback/reinstall an SST application" in *Nortel Carrier Voice over IP Upgrade and Patches* (NN10440-450).

#### ATTENTION

Do not reapply any Session Server Manager patches after the reinstall.

***From the remote server where the backup database file is located***

- 2 If the backup is stored on a remote host, copy the backup file to the unit.

Backup files are unit-specific. Ensure the backup file being copied from the remote host is the file that was originally created on the unit.

To use a secure copy, type

```
scp <backupfile> mtc@ <ip_address> : <dest_dir>
```

where

**backupfile** is a value like unit0.backupfile.2005-04-12\_17-10.tgz and is identified by the hostname, date, and time that the backup occurred

**ip\_address** is the IP address of the unit

**dest\_dir** is the location to put the backupfile and is either blank to place it in /users/mtc, or a full path such as /data/bkresmgr/restore

*The database file is copied to the target unit. If the local workstation is not on the CS LAN, copy the backup file to the server hosting the CS 2000 Management Tools first, and then transfer it between the server hosting the CS 2000 Management Tools and the SST unit.*

#### **At the NCGL CLI or IEMS client**

- 3 Log in to the unit and change to the root user.
- 4 If the backup file was not transferred directly to /data/bkresmgr/restore, then move the backup file:

```
mv /users/mtc/<backupfile>
/data/bkresmgr/restore
```

If restoring a local backup, the backup file is located in /data/bkresmgr/backup.

- 5 Change directory to the restore directory:

```
cd /data/bkresmgr/restore
```

- 6 Uncompress the backup:

```
tar xvzf <backupfile>.tgz
```

*A listing of the files is printed to the screen and the files to restore are located in /data/bkresmgr/restore/data/bkresmgr/temp.*

- 7 Change directory to the files:

```
cd /data/bkresmgr/restore/data/bkresmgr/temp
```

*Jam the inactive unit and suspend call processing*

- 8 Repeat the previous steps in this procedure on the mate unit.

**At the CS 2000 Session Server Manager or IEMS client**

- 9 Select Session Server > Maintenance > Platform > Node Maintenance from the left side menu.  
*The Node Maintenance panel opens in the right side.*
- 10 Click Jam.  
*Two JInact alarms are raised.*
- 11 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu.  
*The SIP Gateway Maintenance page opens in the right side.*
- 12 Click Lock.
- 13 Click Suspend.
- 14 Perform any of the following restore activities and then perform "Unsuspend call processing and Unjam the inactive unit", later in this procedure.
  - [Restore the database](#)
  - [Restore system data](#)
  - [Restore web files](#)
  - Manually restoring security-related files These files are stored in a separate backup file, but restoring them as part of this procedure avoids an additional web server restart

*Restore the database***CAUTION**

Perform the following steps only if the database corruption has occurred on both units. If so, the database must be restored on the active unit.

**At the NCGL CLI or IEMS client**

- 15 Copy the database files:

```
cp -i solid.db
/opt/apps/database/solid/backup/solid.db

cp -i solid.ini
/opt/apps/database/solid/backup/solid.ini

cp -i solmsg.out
/opt/apps/database/solid/backup/solmsg.out
```

- 16 Set the attributes for the files in the backup directory:

```
chown soliddb /opt/apps/database/solid/backup/*
chgrp adm /opt/apps/database/solid/backup/*
chmod 700 /opt/apps/database/solid/backup/*
```

- 17 Restore the backup files:

```
/opt/apps/database/solid_install/restorebackup.sh
```

*The following status is printed to the screen. The database on the inactive unit is synchronized to the restored database on the active unit.*

```
Restoring database from backup
Stopping dbwatchdog.sh: [OK]
Stopping soliddb.sh: [OK]
Starting soliddb.sh: [OK]
Solid SQL Editor (teletype) v.04.10.0139
(C) Copyright Solid Information Technology Ltd 1993-2004
Execute SQL statements terminated by a semicolon.
Exit by giving command: exit;
Connected to 'tcp 1315'.
admin command 'hsb set primary alone'
 RC TEXT
 -- ----
 0 HotStandby server set to PRIMARY ALONE.
1 rows fetched.

admin command 'hsb netcopy'
 RC TEXT
 -- ----
 0 Copy started.
1 rows fetched.

SOLID SQL Editor exiting.
Starting dbwatchdog.sh: [OK]
```

- 18 If the database is the only item to restore, then unsuspend, unlock, and unjam the inactive unit. For assistance, refer to "Unsuspend call processing and Unjam the inactive unit," later in this procedure.

*Restore system data*

**At the NCGL CLI or IEMS client**

- 19 Copy the necessary files:

```
cd /data/bkresmgr/restore/data/bkresmgr/temp
cp -i hosts /etc
cp -i passwd /etc
cp -i group /etc
cp -i ntp.conf /etc
cp -i shadow /etc
cp -i ifcfg-eth0 /etc/sysconfig/network-scripts
cp -i netnodes /etc/sysconfig
```

```
cp -i ssh_host_dsa_key.pub
/opt/base/synch_local/common/etc/ssh

cp -i ssh_host_key.pub
/opt/base/synch_local/common/etc/ssh

cp -i ssh_host_rsa_key.pub
/opt/base/synch_local/common/etc/ssh
```

- 20 Set the permissions on the restored files:

```
chmod 755 /etc/hosts
chmod 755 /etc/passwd
chmod 755 /etc/shadow
chmod 755 /etc/group
chmod 755 /etc/sysconfig/netnodes
chmod 755
/etc/sysconfig/network-scripts/ifcfg-eth0

chmod 644
/opt/base/synch_local/common/etc/ssh/ssh_host_key.pub

chmod 644
/opt/base/synch_local/common/etc/ssh/ssh_host_dsa_key
.pub

chmod 644
/opt/base/synch_local/common/etc/ssh/ssh_host_rsa_key
.pub
```

- 21 Repeat the previous two steps on the mate unit.

*Restore web files*

***At the NCGI CLI or IEMS client***

- 22 Copy the files:

```
cd /data/bkresmgr/restore/data/bkresmgr/temp

cp -i redirect*.jsp
/opt/apps/webint/jakarta-tomcat-4.1.30/webapps/
<tag_name>/jsp

cp -i redirect_apps.php
/usr/local/apache/htdocs
```

*Unsuspend call processing and Unjam the inactive unit*

***At the CS 2000 Session Server Manager or IEMS client***

- 23 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu.
- 24 Click Unsuspend.



- 25 Click Unlock.
- 26 Select Session Server > Maintenance > Platform > Node Maintenance from the left side menu.
- 27 Click Unjam.
- 28 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

## Prepare for a database restore on a Policy Controller unit

---

### Purpose of this procedure

Use this procedure to prepare for a restoration of the Policy Controller application database from a backup copy.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of the high level upgrade activity "Perform an emergency maintenance release rollback activity" found in Upgrading the Policy Controller NTP, NN10431-461.

### Limitations and Restrictions



#### CAUTION

Performing a restore of the Policy Controller application database is a service affecting activity and can cause data mismatches at the Communication Server 2000.

#### ATTENTION

For security reasons, you can only copy the database file from a remote server to the /users/mtc directory on the unit and you must use the secure copy command `scp` to perform this activity.

Automatic backup of the Policy Controller application database occurs at 1:00 AM each day on both Policy Controller units. This configuration setting cannot be modified and does not impact the use of this procedure.

The name of the backup database file is *solid.db*. Do not modify this name.

### Prerequisites

You must have secure copy (`scp`) access to the Policy Controller unit from the remote system or other server location from where the database backup file *solid.db* is copied.

## Action

| Step | Action |
|------|--------|
|------|--------|

***From the remote server where the backup database file is located***

- 1 Log onto the remote server, locate and navigate to the directory where the backup copy of the database file is stored.
- 2 Secure copy the database file to the Policy Controller unit you are restoring a backup copy of the database to by typing  

```
$ scp solid.db mtc@<PC_IP_address>:
```

and pressing the Enter key.  
where  
**PC\_IP\_address** is the IP address of the Policy Controller unit  
*The database file is copied to the /user/mtc directory on the target Policy Controller unit. This is the only Policy Controller directory that files can be copied into from an external server.*

***At a Policy Controller command line interface***

- 3 Open a secure shell to the Policy Controller unit you are restoring a backup copy of the database to by typing  

```
> ssh -l <userid> <PC_IP_address>
```

and pressing the Enter key.  
where  
**userid** is a valid userid (like mtc) on the Policy Controller  
**PC\_IP\_address** is the IP address of the Policy Controller  
**Example**  

```
ssh -l mtc 45.128.54.12
```
- 4 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 Move the solid.db file you copied in [Step 2](#) from the /user/mtc directory to the /opt/apps/database/solid/backup directory by typing  

```
$ mv /users/mtc/solid.db
/opt/apps/database/solid/backup
```

and pressing the Enter key.

- 7 Change directory to the backup database directory by typing  

```
$ cd /opt/apps/database/solid/backup
```

and pressing the Enter key.
- 8 Verify that the correct version (based on the file date) of the solid.db database file that you want to restore is located in the directory by typing  

```
$ ls -l /opt/apps/database/solid/backup
```

and pressing the Enter key.

**ATTENTION**

The restorebackup.sh script does not run if you do not have the solid.ini and solmsg.out files located in the correct directory.

- 9 Verify that the presence of files *solid.ini* and *solmsg.out* files are also in the /opt/apps/database/solid/backup directory.
- 10 If the solid.ini file is not present, copy it into the backup directory by typing  

```
$ cp /opt/apps/database/solid/dbfiles/solid.ini
/opt/apps/database/solid/backup/solid.ini
```

and pressing the Enter key
- 11 If the solmsg.out file is not present, copy it into the backup directory by typing  

```
$ cp
/opt/apps/database/solid/dbfiles/solmsg.out
/opt/apps/database/solid/backup/solmsg.out
```

and pressing the Enter key
- 12 Change the ownership of all files in the backup directory by typing  

```
$ chown soliddb *
```

and pressing the Enter key.
- 13 Change the group of all files in the backup directory by typing  

```
$ chgrp adm *
```

and pressing the Enter key.
- 14 Change the access permissions for all files in the backup directory by typing  

```
$ chmod 600 *
```

and pressing the Enter key.

- 15 The database is now ready to be restored. You have completed this procedure. Return to the high-level activity.

---

—End—

---

## Additional information

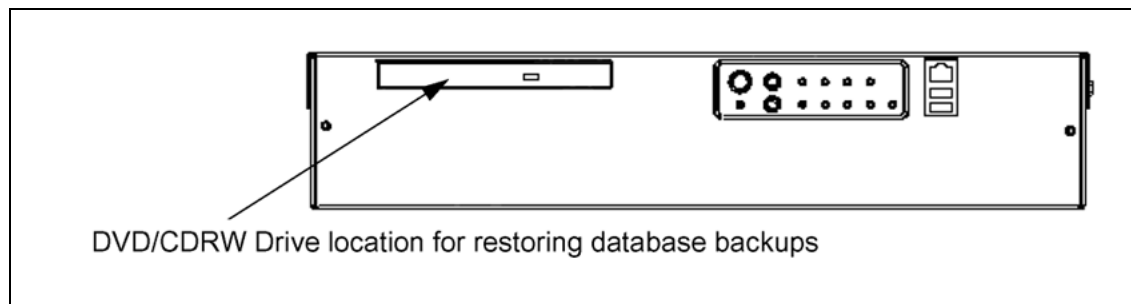
This section provides additional information regarding database restore activities.

### To restore a backup database saved to a CD.

If you must restore a database backup that has been saved to a CD, you must first copy the database file from the CD to the default backup directory on the active Policy Controller unit. The selected backup database file must be restored to the following location:

*/opt/apps/database/solid/backup/solid.db*

To restore a backup of the database file to the backup directory, you must use a Policy Controller command line interface to copy the database file from a CD or CD-RW disk containing a copy of the back up database file to the *opt/apps/database/solid/backup* directory.



Ensure that you remove the CD disk from the DVD/CDRW drive, and store it in a safe place when you are done.

### To restore a database backup save to another system

If you must restore a database backup that has been saved to another system, you must first copy the database file from the remote system back to the default backup directory on the active Policy Controller unit. The selected backup database file must be restored to the following location:

*/opt/apps/database/solid/backup*

To restore a backup of the database to the backup directory you must use a Policy Controller command line interface to copy the database file *solid.db* from the remote system to the *opt/apps/database/solid/backup* directory.

You may also be able to remote copy the backup database file from the remote system to the Policy Controller `opt/apps/database/solid/backup` directory. However, for security reasons, you may need to consult your site network administrator for instructions and permission to perform a remote copy.

## Perform a database restore to a Policy Controller unit

### Purpose of this procedure

Use this service impacting procedure to restore a Policy Controller application database from a backup copy to either the active or inactive Policy Controller units.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of the high level upgrade activity "Perform an emergency maintenance release rollback activity" found in the Policy Controller Upgrades NTP, NN10431-461.

### Limitations and Restrictions



#### CAUTION

Performing a restore of the Policy Controller application database is a service affecting activity and can cause data mismatches at the Communication Server 2000.

### Prerequisites

You must first have completed procedure ["Prepare for a database restore on a Policy Controller unit"](#) (page 206).

### Action

| Step | Action |
|------|--------|
|------|--------|

#### *At a Policy Controller command line interface*

- 1 Open a secure shell to the Policy Controller unit you are restoring a backup copy of the database to by typing  

```
> ssh -l <userid> <PC_IP_address>
```

and pressing the Enter key.  
where  
**userid** is a valid userid (like mtc) on the Policy Controller  
**PC\_IP\_address** is the IP address of either Policy Controller unit  
**Example**  

```
ssh -l mtc 45.128.54.12
```

- 2 Change to the root user by typing  
`$ su - root`  
and pressing the Enter key.
- 3 When prompted, enter the root password.
- 4 Change directories by typing  
`$ /opt/apps/database/solid_install`  
and pressing the Enter key.
- 5 Run the database restore script by typing  
`$ ./restorebackup.sh`  
and pressing the Enter key.
- 6 You have completed this procedure. Return to the high-level activity.

---

—End—

---



## Resetting the Ethernet Routing Switch 8600 using a saved configuration file

The Ethernet Routing Switch 8600 boot command allows you to reset or reboot the system using a saved configuration file. You must have access to the Boot Monitor CLI through a direct connection to the switch or a Telnet connection. For more information on accessing the Boot Monitor CLI, refer to 'Managing the Ethernet Routing Switch 8000 Series Switch Using the Command Line Interface Release 3.2,' 313194-\*.

**Note:** You must be directly connected to the switch to initiate a Boot Monitor session. You can only connect using a Telnet connection if the Boot Monitor CLI is already active.

### Resetting the Ethernet Routing Switch 8600 using a saved configuration file

| Step | Action |
|------|--------|
|------|--------|

#### *At the Boot Monitor CLI*

- Issue the boot command by typing  

```
monitor# boot [<file>] [config <value>]
```

where

**file** is the software image device and file name in the format [a.b.c.d:]<file> | /pcmcia/<file> | /flash/<file>. The file name, including the directory structure, can be up to 1024 characters.

**config <value>** is the software configuration device and file name in the format [a.b.c.d:]<file> | /pcmcia/<file> | /flash/<file>. The file name, including the directory structure, can be up to 1024 characters.
- You have completed this procedure.

---

—End—

---

## Restoring audio files to a Media Server 2000 Series node

In the event that a re-installation of a Media Server 2000 Series node is required due to an error condition, audio files must be restored to the unit when it becomes operational. This procedure allows you to enable audio provisioning to the node and to specify which audio files are to be restored to it.

**Note:** For more information about re-installation of a Media Server 2000 Series node, contact your Nortel service representative.

### Restoring audio files to a Media Server 2000 Series node

| Step | Action |
|------|--------|
|------|--------|

*At your web browser interface*

- 1 After the re-installation of the Media Server 2000 Series node has been completed, determine whether you want to enable provisioning of the node occur during the next audio distribution cycle or immediately.

| If                                                                                            | Do     |
|-----------------------------------------------------------------------------------------------|--------|
| you want to enable provisioning of the node to occur during the next audio distribution cycle | step 2 |
| you want audio provisioning of the node to occur immediately                                  | step 3 |

- 2 Perform the "Enabling provisioning of a Media Server 2000 Series node" (refer to the Media Server 2000 Series Configuration Management document).

**Note:** Provisioning of the node will begin during the next audio distribution cycle. The distribution cycle occurs once per hour.

- a. Go to step 4.

- 3 Perform the procedure "Provisioning a Media Server 2000 Series node" (refer to the Media Server 2000 Series Configuration Management document).

**Note:** Provisioning of the node will begin immediately although as much as a five-minute delay may occur before actual provisioning activity begins.

**4** You have completed this procedure.

---

**—End—**

---

## Administration: Restore Operations

You can use the restore operation to return your system to a configuration that was saved during a backup operation. The typical use of the restore operation is as follows:

- An emergency situation occurs that requires you to restore a system configuration from a stored data snapshot.
- You use the file manager function to ensure that there are copies of the data snapshot to be restored on both RTC system nodes.
- You make the data snapshot the boot snapshot for both RTC system nodes.
- You deactivate the linksets and change the path state of the application server process (ASP) paths to Down for your system, as appropriate.
- You perform a complete office recovery (COR) on your system, which means that you unseat the RTC system nodes, turn off both power switches on the shelf, reseal the RTC system nodes, and then restore power. Your stored data snapshot is now the running data snapshot.

Complete the following procedures to restore data snapshots stored on your alternate boot server or on the RTC system nodes.

**CAUTION**

Performing a COR on your system is service affecting. Nortel recommends that you do this during off-peak hours and that you ensure that a mated system is available.

**CAUTION**

Do not power down the shelf when the SCSI disk light on the RTC system node is on. To do so could cause a disk failure.

**CAUTION**

Wear wrist straps, and use standard antistatic precautions.

## Restoring a system configuration from a data snapshot stored on your alternate boot server

| Step | Action |
|------|--------|
|------|--------|

### At the OAMP workstation

- 1 Click **Administration>file-manager**.
- 2 Modify the boot data configuration at RTC12. For more information about modifying boot data configuration see, *USP Configuration Management* (NN10093-511).
- 3 Modify the boot data configuration at RTC15. For more information about modifying boot data configuration see, *USP Configuration Management* (NN10093-511).
- 4 Deactivate the linksets for your system.  
  
Deactivating the linksets aids in shutting down the application because the Network Elements connected to the USP can take action accordingly.  
  
For more information about deactivating linksets, see *USP Configuration Management* (NN10093-511).
- 5 Change the path state of the ASP paths to Down.  
  
Changing the path state of the ASP paths to down aids in shutting down the application because the Network Elements connected to the USP can take action accordingly.  
  
For more information about changing the state of an ASP path, see *USP Configuration Management* (NN10093-511).
- 6 Perform the following steps on the inactive RTC (slot15).
  - a. If the RTC system node is locked, proceed to [step 6b](#). Otherwise, click **Lock** and proceed to [step 6b](#).
  - b. If the RTC system node is offline, proceed to [step 7](#). Otherwise, click **Offline** and proceed to [step 7](#).
- 7 Make note of which RTC system node is the active RTC system node. This information is required later in the procedure.
- 8 Change the alternate boot snapshot. Go to ["Performing a backup operation" \(page 149\)](#).
- 9 To perform a COR on your system, do the following:
  - a. Unseat the RTC mission card for the inactive RTC system node. Ensure that the LED is off for the SCSI Disk Drive associated with this RTC system node before unseating the mission card.

To unseat the mission card, press outward on the top and bottom latches of the mission card to release it from the Communications Application Module (CAM) shelf.

Grasp the top and bottom latches of the mission card and gently pull it toward you to disconnect it from the associated TM. Do not remove the mission card from the CAM shelf.

Unseating the RTC card stops the write and read access to the SCSI card to avoid SCSI failure.

- b. Repeat [step 9a](#) for the RTC mission card for the active RTC system node.
- c. If there are extension shelves in the system, turn off the A and B power switches on the extension CAM shelves one by one from the maximum shelf number to the minimum shelf number. For example; shelf 4, shelf 3, and then shelf 2.
- d. Turn off both the A and B power switches on the rear of the control CAM shelf of your system.
- e. Reseat the RTC mission card for an RTC system node. To do this, gently slide the mission card back into place. Apply pressure to the faceplate until you feel resistance.

Snap the top and bottom latches of the mission card inward, toward one another. Two audible clicks can be heard when the mission card is seated properly.

- f. Repeat [step 9e](#) for the RTC mission card for the other RTC system node.
- g. Return power to the shelf. To do this, turn on both the A and B power switches on the rear of the control CAM shelf of your system.

Refer to the note recorded earlier in the procedure to know which RTC system node is active and which one is inactive.

System start up can take several minutes, depending on the configuration of your system.

- h. If there are extension shelves in the system, you must turn on both the A and B power switches on the rear of the extension shelves of the system one by one from the minimum shelf number to the maximum shelf number. For example; shelf 2, shelf 3, and then shelf 4.

System start up can take several minutes, depending on the configuration of your system.

- 10** Wait for the GUI to re-establish a connection after the USP recovers. To view system node status:

- a. Click **Configuration>platform>node**.
- b. Click the **Graphical View** tab.
- c. Confirm that all system nodes are enabled (green status light).

**ATTENTION**

Nortel recommends that you do not attempt any provisioning changes until all system nodes recover.

If the GUI fails to log in when it is re-establishing the connection, the boot snapshot may not contain the current user's user-account. Provide another valid user-account that is configured in the snapshot have just booted

- 11 Log into your system.
- 12 Open the RTC system node administration tab for the RTC system node in slot 12. To do this, click **Configuration>platform>node**. Click the **Graphical view** tab, then select slot 12.  
  
If the table is opened before the GUI reconnects to the RTC, the old data is displayed. After the GUI reconnects to the RTC, reload the table.
- 13 If the data snapshot descriptions match, proceed to [step 20](#). If the snapshot descriptions do not match, return to [step 1](#) and attempt the procedure again. If the procedure has failed twice in row, contact your next level of support.  
  
For the current active snapshot the snapshot-date and snapshot-version fields are empty.
- 14 Update the system time settings in the Set Date/Time window, click **Administration> Set Date/Time**.

**ATTENTION**

This step is not required if simple network time protocol (SNTP) is enabled for this system.

---

—End—

---

**CAUTION**

This procedure can overwrite existing data files on your workstation. Make sure you have a current data backup before you begin this procedure.

## Performing a restore operation from a backup tape

| Step | Action |
|------|--------|
|------|--------|

*At the Windows-based OAMP workstation*

- |    |                                                                                                                                                                           |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Insert the tape containing the data that you want to restore.                                                                                                             |
| 2  | Double-click the <b>Backup Exec</b> icon on the desktop if you are running a Veritas program or the <b>Colorado Backup II</b> icon if you are running a Colorado program. |
| 3  | Select <b>Restore files using the Restore Wizard</b> .                                                                                                                    |
| 4  | Click <b>OK</b> .                                                                                                                                                         |
| 5  | Click <b>Next</b> .                                                                                                                                                       |
| 6  | Select from media in the device.                                                                                                                                          |
| 7  | Click <b>Next</b> . The system loads the information from the backup tape.                                                                                                |
| 8  | Select the backup date and time for the data that you want to restore.                                                                                                    |
| 9  | Click <b>OK</b> . The system loads the information from the backup tape.                                                                                                  |
| 10 | Click the + button on the tree control to expand the tree box next to the C: drive. Select any directories that you want to restore.                                      |
| 11 | Click <b>Next</b> .                                                                                                                                                       |
| 12 | Click <b>Next</b> a second time.                                                                                                                                          |
| 13 | Select <b>Always replace the file on my computer</b> .                                                                                                                    |
| 14 | Click <b>Start</b> . The system restores the backup data.                                                                                                                 |
| 15 | Click <b>OK</b> .                                                                                                                                                         |
| 16 | The data restore procedure is complete.                                                                                                                                   |

—End—



### CAUTION

This procedure can overwrite existing USP data files on your workstation. Make sure you have a current data backup before you begin this procedure.



**ATTENTION**

Before performing this procedure, ensure that the ABS is installed in the workstation.

The root privilege is required to perform this procedure.

## Performing a restore operation from a backup CD-RW

| Step | Action |
|------|--------|
|------|--------|

### *At the Solaris-based OAMP workstation*

- 1 Remove the current USP data by entering the following command at the prompt:

**rm -Rf <USP data directory>**

**Example**

```
rm -Rf /opt/usp/ntssgusp/abs/sites
```

- 2 Insert the CD-RW containing the USP data that you want to restore into the CD-ROM drive.

- 3 Go to the partition where the ABS is installed by entering the following:

**cd <partition>**

**Example**

```
cd /
```

The ABS is installed in the root partition by default.

- 4 Restore the USP data by entering the following command:

**ufsrestore xf /<cdrom directory>/<dumped filename>**

**Example**

```
ufsrestore xf /cdrom/cdrom0/usp_data_20051115.dmp
```

The <cdrom directory> is the directory where your CD-ROM is mounted.

The following is displayed; enter what is in bold text when prompted:

You have not read any volumes yet.

Unless you know which volume your file(s) are on you should start with the last volume and work towards the first.

Specify next volume #: **1**

If the data files are large, it can take several minutes to restore the data.

set owner mode for '.'? **[yn]** **n**

Directories already exist, set modes anyway? [yn] **n**

- 5** Go to the root directory by entering the following:

**Example**  
`cd /`

- 6** Restore the DHCP configuration data by entering the following command:

**ufsrestore xf /<cdrom directory>/<dumped filename>**

**Example**  
`ufsrestore xf /cdrom/cdrom0/dhcp_20051115.dmp`

The following is displayed; enter what is in bold text when prompted:

You have not read any volumes yet.

Unless you know which volume your file(s) are on you should start with the last volume and work towards the first.

Specify next volume #: **1**

If the data files are large, it can take several minutes to restore the data.

Set owner mode for ' . '? [yn] **n**

Directories already exist, set modes anyway? [yn] **n**

- 7** Copy the NFS configuration file back by entering the following:

**cp /<cdrom directory>/dfstab /etc/dfs/dfstab**

**Example**  
`cp /cdrom/cdrom0/dfstab /etc/dfs/dfstab`

- 8** Restart the NFS server by entering the following commands:

**/etc/init.d/nfs.server stop**

**/etc/init.d/nfs.server start**

- 9** The data restore procedure is complete. Remove the CD-RW from the CD-ROM drive and return it to its regular storage location.

- 10** You have completed this procedure.

---

—End—

---

---

## Restoring Multiservice Switch or Media Gateway service data

---

This section describes using Service Data Backup and Restore to restore backed up service data from the backup site to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.

The Service Data Backup and Restore tools provide three types of restore:

- A *full* restore restores all backed up service data to the selected device or devices.
- An *incremental* restore restores service data based on a specified date. Like the full restore, you can perform an incremental restore on either one or multiple devices.
- A *selective* restore restores specific service data that you select. Like the full restore, you can perform a selective restore on either one or multiple devices.

**Note:** It is not recommended that an active file (current view) be restored on a Multiservice Switch 7400/15000 or Media Gateway 7400/15000. When you restore the current view, you may overwrite the existing current view with different content. This action will cause an outage of the Backup and Restore tool.

The following information applies to using the Service Data Backup and Restore tool to perform a restore for Multiservice Switch 7400/15000 or Media Gateway 7400/15000 nodes:

- ["Adding Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices to the restore list" \(page 224\)](#)
- ["Removing Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices from the restore list" \(page 224\)](#)
- ["Defining a specific userid and password for a Multiservice Switch 7400/15000 or Media Gateway 7400/1" \(page 225\)](#)
- ["Performing a full restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device" \(page 225\)](#)
- ["Performing an incremental restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 d" \(page 226\)](#)
- ["Performing a selective restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devi" \(page 227\)](#)
- ["Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data" \(page 228\)](#)

## Adding Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices to the restore list

Use the following procedure to add devices to the Devices List.

---

| Step | Action |
|------|--------|
|------|--------|

---

### *Procedure steps*

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore
- 2 Select the Restore Configuration tab.
- 3 Click Add to open the Add Device dialog.
- 4 Select a group of devices or expand the group and use the Ctrl key to select a number of devices.
- 5 Select the appropriate restore mode, from the Mode column (full or incremental).
- 6 If a specific userid and password is required for the device, enter the values in the User ID and Password fields and uncheck the Use default checkbox.
- 7 If you wish to use the default userid and password, click the Use default checkbox.
- 8 Click OK.  
  
The IP addresses for the devices are retrieved from HGDS and the device displays in the Devices list.  
  
For devices that are not in HGDS, you are prompted for their IP address. If you are prompted for an IP address, do [Step 9](#).
- 9 If you know the IP address, enter the correct IP address in the form and click OK and the device is added to the Devices list.  
  
If the IP address is unknown or the device is not valid, press Cancel and the device is not added to the Devices list.

---

—End—

---

## Removing Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices from the restore list

Use this procedure to remove nodes from the list of nodes that you wish to backup.

| Step | Action |
|------|--------|
|------|--------|

**Procedure steps**

- |   |                                                                                                                                                       |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore |
| 2 | Select the Restore Configuration tab.                                                                                                                 |
| 3 | In the Device List, select the devices you wish to remove.                                                                                            |
| 4 | Click Remove.                                                                                                                                         |
| 5 | In the confirmation dialog, select Yes to confirm or No to cancel the removal.                                                                        |

---

—End—

---

## Defining a specific userid and password for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device in the restore list

A specific userid and password can be defined when you add the device to the restore list or you can set it later using the following procedure.

| Step | Action |
|------|--------|
|------|--------|

**Procedure steps**

- |   |                                                                                                                                                        |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore. |
| 2 | Select a device.                                                                                                                                       |
| 3 | In the Device Details section, enter a userid and password.                                                                                            |
| 4 | Clear the Use default checkbox.                                                                                                                        |

---

—End—

---

## Performing a full restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to copy all the files from the repository back to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.

| Step | Action |
|------|--------|
|------|--------|

**Procedure steps**

- |   |                                                                                                                                                                                               |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.                                        |
| 2 | Select the Restore Configuration tab.                                                                                                                                                         |
| 3 | Click Add to open the Add Device dialog.                                                                                                                                                      |
| 4 | Select a group of devices or expand the group and use the Ctrl key to select a number of devices.                                                                                             |
| 5 | Select a device from the Device List.                                                                                                                                                         |
| 6 | Click in the Mode title and select Full from the drop-down list.                                                                                                                              |
| 7 | Click Restore.                                                                                                                                                                                |
| 8 | After a successful restore, you need to activate the restored data. See <a href="#">"Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data"</a> (page 228). |

---

—End—

---

## Performing an incremental restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to copy files, based on a specific date, from the repository back to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.

| Step | Action |
|------|--------|
|------|--------|

**Procedure steps**

- |   |                                                                                                                                                       |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->PassportService Data Backup/Restore. |
| 2 | Select the Restore Configuration tab.                                                                                                                 |
| 3 | Click Add to open the Add Device dialog.                                                                                                              |
| 4 | Select a group of devices or expand the group and use the Ctrl key to select a number of devices.                                                     |
| 5 | Select a device from the Device List.                                                                                                                 |

- 6 Click in the Mode title and select Incremental from the drop-down list.
- 7 Define a date in the date column. (For example, July 4, 2005)  
All the files, with the date and time that are not greater than the specified date, will be restored.
- 8 Click Restore.
- 9 After a successful restore, you need to activate the restored data. See ["Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data" \(page 228\)](#).

---

—End—

---

## Performing a selective restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to copy a specific file from the repository back to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.

| Step | Action |
|------|--------|
|------|--------|

### *Procedure steps*

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->PassportService Data Backup/Restore.
- 2 Select the Restore Configuration tab.
- 3 Click Add to open the Add Device dialog.
- 4 Select a group of devices or expand the group and use the Ctrl key to select a number of devices.
- 5 Select a device from the Device List.
- 6 Click in the Mode title and select Selective from the drop-down list.
- 7 In the View column, select the desired view from the repository using the drop-down list.  
  
**Note:** This step may take a few seconds to complete because the application must access the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 and list all the views names.
- 8 Click Restore.

- 9 After a successful restore, you need to activate the restored data. See ["Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data"](#) (page 228).

---

—End—

---

## Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data

Restore restores the backup configuration data onto the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 disk. After a successful restore, perform the following procedure to activate the restored data.

---

| Step | Action |
|------|--------|
|------|--------|

---

### *Procedure steps*

- |   |                                                                                                                                                                                                |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Establish a telnet session to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.                                                                                                  |
| 2 | Download to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 any required application software missing from the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 disk. |
| 3 | Enter provisioning mode.                                                                                                                                                                       |
| 4 | Activate the restored view and confirm the activation.                                                                                                                                         |
| 5 | If required, commit the activated view.                                                                                                                                                        |

---

—End—

---



## Restoring Core Element Manager data

### Application

Use this procedure to restore Core Element Manager (CEM) data.

The backup procedure is performed through the Synchronous backup restore manager (SBRM). See Synchronized Backup Manager overview in *ATM/IP Solution-level Administration and Security*, NN10402-600 for details. The information needed by the Core Element Manager to restore data is located in `/opt/nortel/cem/data/coreEMS/configBackup`.

### Prerequisites

You must have root user privileges to perform this procedure.

### Action

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Telnet to the server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
**server** is the IP address or host name of the server where the CEM resides
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su -
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Make sure that the `/opt/nortel/cem/data/coreEMS/configBackup` directory contains the following files:
  - data\_dir
  - ldapConfig.tar
  - nodes.tar
  - server

Enter:

```
ls /opt/nortel/data/coreEMS/configBackup
```

- 6 Make sure that CEM is not running by typing:

```
servquery -status -group CEM
```

and pressing the Enter key.

*Example response:*

CEM server STOPPED

- 7 If the CEM server is running, stop the CEM server by typing:

```
servstop CEM
```

and pressing the Enter key.

*Example response:*

CEM server successfully stopped

- 8 Run the restore script by typing

```
#!/opt/nortel/cem/data/coreEMS/nodes/server/bin/postRestore.sh
```

and pressing the Enter key.

- 9 You have completed this procedure.

---

—End—

---

## Performing a full restore of the software from S-tape

### Purpose

Use this procedure to perform a full restore of the core manager software load from the system image backup tape (S-tape).

### Prerequisites

You must be a user authorized to perform fault-admin actions.

For information on how to log in to the core manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Procedures related to this procedure

| Procedure                                          | Document                    |
|----------------------------------------------------|-----------------------------|
| Logging in to the CS 2000 Core Manager             | Security and Administration |
| Displaying actions a user is authorized to perform | Security and Administration |

### Application

#### ATTENTION

You must be a trained AIX system administrator authorized to perform fault-admin actions.

#### ATTENTION

You must mirror all volume groups on the core manager before you perform this procedure. If you perform this procedure when disk mirroring is not at the Mirrored state, the system displays an error message.

#### ATTENTION

If your system includes the SuperNode Billing Application (SBA), you must use tape drive DAT0 to perform this procedure.

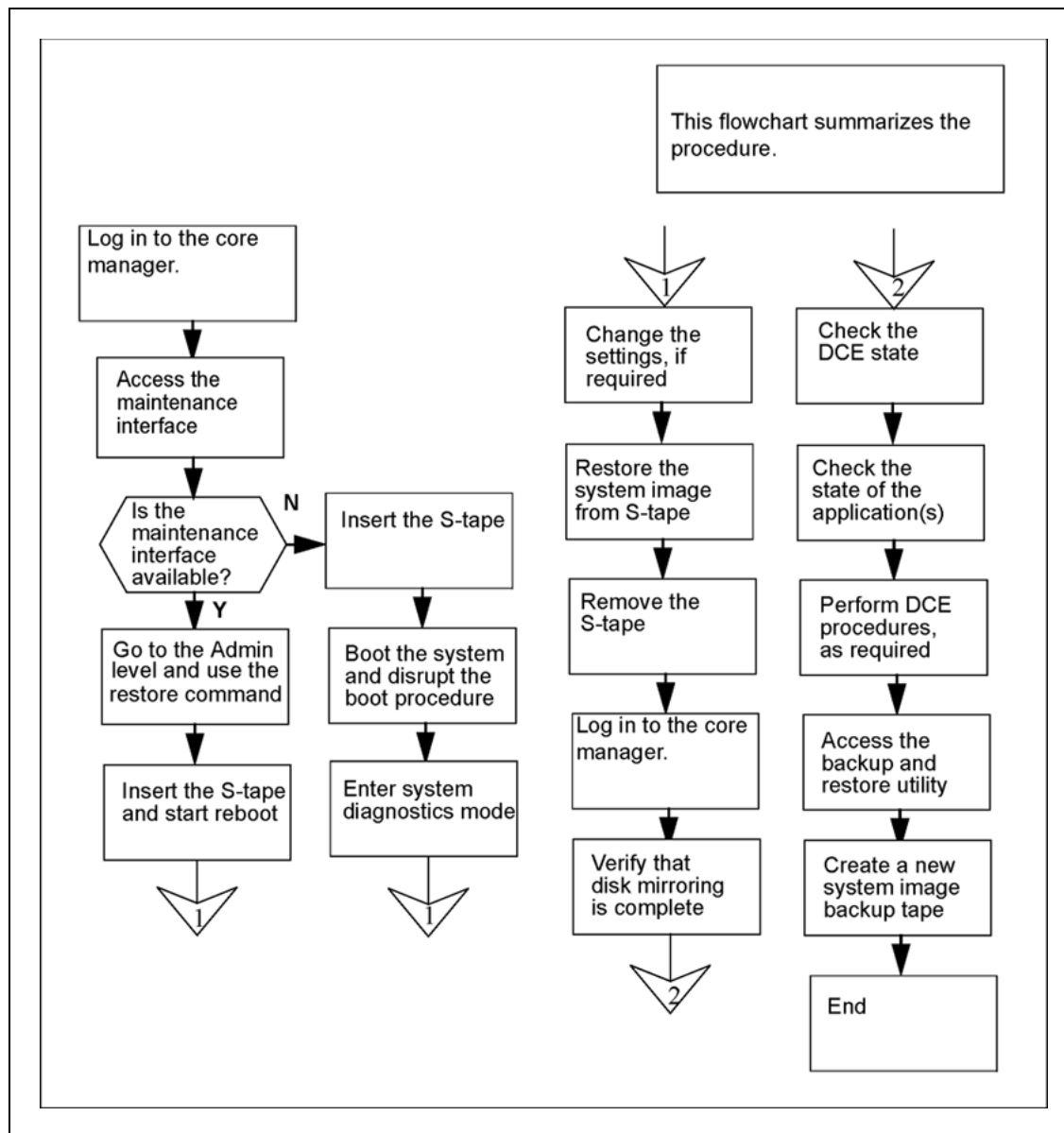
### Interval

Perform this procedure when the core manager is out-of-service due to a corrupted software load.

## Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the recovery tasks.

### Summary of performing a full restore of the software from the S-tape



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Performing a full restore of the software from S-tape

| Step | Action |
|------|--------|
|------|--------|

*At the local VT100 console*

- 1 Log into the CS 2000 Core Manager as a user authorized to perform fault-admin actions.

- 2 Access the maintenance interface:

```
sdmmtc
```

- 3 Determine if the core manager maintenance interface is available.

| If                                                  | Do                      |
|-----------------------------------------------------|-------------------------|
| core manager maintenance interface is available     | <a href="#">step 4</a>  |
| core manager maintenance interface is not available | <a href="#">step 10</a> |

- 4 Access the administration (Admin) level:

```
admin
```

- 5 Perform a full restore of the core manager:

```
restore
```

*Example response:*

```
Select the tape drive you want to restore from, or type
Abort to abort:
```

```
Enter 0 for the tape drive in the main chassis slot 2.
```

```
Enter 1 for the tape drive in the main chassis slot 3.
```

- 6 Choose the tape drive to use.

| If                                        | Do      |
|-------------------------------------------|---------|
| you want to use the tape drive in slot 2  | enter 0 |
| you want to use the tape drive in slot 13 | enter 1 |

- 7 When prompted, confirm that you want to proceed:

```
y
```

*Example response:*

```
Insert the backup-tape into the tape drive in the main
chassis slot 2. When completed press [Enter] to start
the restore.
```

- 8 Insert the back-up tape (S-tape) into the tape drive you specified (slot 2 or 13).

**Note:** Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

- 9 Press the Enter key to start the restore process, and proceed to [step 17](#).

**Note:** When you press the Enter key, the system starts the restore procedure by rebooting the core manager from the selected tape drive.

*At the core manager*

- 10 Ensure that one of the core manager tape drives (slot 2 or 13 in the main chassis) contains the system image backup tape (S-tape).

**Note:** Use tape drive DAT0 (option for performing a full restore from an S-tape) if your system also includes SBA.

*At the Modular Supervisory Panel*

- 11 Reboot the core manager. If the prompt is available at a local VT100 console, reboot the core manager:

`shutdown -Fr`

If the prompt is not available, reboot the core manager by turning the power off, then on, using the MSP breaker that supplies power to the core manager.

*At the local VT100 console*

- 12 When the system displays "COLD Start", press the Break key or the Esc key twice to interrupt the boot process. The system takes about 4 minutes to initialize.
- 13 Continue depending on the prompt displayed on the monitor.

| If the prompt is             | Do                      |
|------------------------------|-------------------------|
| FX-Bug                       | <a href="#">step 16</a> |
| FX-Bug and you are in a menu | <a href="#">step 14</a> |
| FX-Diag                      | <a href="#">step 15</a> |

- 14 From the selection menu, select Go to System Debugger:

3

Go to [step 16](#).

- 15** Switch the directory to FX-Bug:

```
sd
```

- 16** View the input/output devices on the core manager to verify the address of the tape drive from the FX-Bug prompt. Enter:

```
Fx-Bug> ioi
```

*Example response:*

| CLUN        | DLUN | CNTRL-TYPE | DADDR | DTYPE | RM | Inquiry-Data |
|-------------|------|------------|-------|-------|----|--------------|
| 1           | 0    | IO         | 0     | \$00  | N  | SEAGATE      |
| ST11200N ST |      |            |       |       |    |              |
|             |      |            |       |       |    | 31200 0660   |
| 3           | 0    | IO         | 0     | \$00  | N  | SEAGATE      |
| ST12400N    |      |            |       |       |    |              |
|             |      |            |       |       |    | ST32430      |
| 0660        |      |            |       |       |    |              |
| 1           | 50   | IO         | 5     | \$01  | Y  | ARCHIVE      |
| Python      |      |            |       |       |    |              |
|             |      |            |       |       |    | 28388-XXX    |
| 5.45        |      |            |       |       |    |              |
| 6           | 0    | IO         | 0     | \$00  | N  | SEAGATE      |
| ST11200N    |      |            |       |       |    |              |
|             |      |            |       |       |    | ST31230      |
| 0660        |      |            |       |       |    |              |
| 8           | 0    | IO         | 0     | \$00  | N  | SEAGATE      |
| ST12400N    |      |            |       |       |    |              |
|             |      |            |       |       |    | ST32430      |
| 0660        |      |            |       |       |    |              |
| 6           | 50   | IO         | 5     | \$01  | Y  | ARCHIVE      |
| Python      |      |            |       |       |    |              |
|             |      |            |       |       |    | 28388-XXX    |
| 5.45        |      |            |       |       |    |              |

**Note:** In the example response, the tape drive is ARCHIVE.

- 17** If you receive the FX-Bug prompt, then continue with this step. Otherwise, go to [step 19](#).

```
Fx-Bug> pboot <address_for_Archive_Python>
```

In the example, the following are valid choices:

- pboot 1 50 if the tape drive is located in slot 2
- pboot 6 50 if the tape drive is located in slot 13

- 18** Wait about 4 minutes until the system completes the reboot.

- 19** The system prompts you to define the console setting and the language setting. Define the console setting by selecting option 1 and pressing the Enter key.

**Note 1:** In case of any failures, contact your next level of support.

**Note 2:** When you define the console setting, the system does not echo the entry "1" on the screen.

- 20** Enter 1 to select the language setting, and press the Enter key. The Welcome to Base Operating System Installation and Maintenance menu is then displayed.

- 21** Select "Change/Show Installation Settings and Install":

2

The system displays the System Backup Installation and Settings menu.

*Example response:*

```
System Backup Installation and Settings
Either type 0 and press Enter to install with the
current settings, or type the number of the setting you
want to change and press Enter.
```

```
Setting: Current
Choice(s):
1 Disk(s) where you want to install hdisk0...
 Use Maps No
2 Shrink File System No
>>> 0 Install with the settings listed above.
```

**Note:** The string "..." shown under Current Choice(s) indicates that more than one disk is currently in use.

- 22** The default disk for the installation is hdisk0 which is located in slot 2 of the main chassis. If your core manager contains one disk drive in each domain of the main chassis, accept the default setting. If you have additional disk drives, you may wish to change the settings.

| If                                      | Do                      |
|-----------------------------------------|-------------------------|
| you want to change the current settings | <a href="#">step 23</a> |
| you want to use the current settings    | <a href="#">step 27</a> |

- 23** Change the disks where you want to install the backup image:

1

The system displays the Change Disk(s) Where You Want to Install menu.

*Example response:*

```
Change Disk(s) Where You Want to Install
```



Type one or more numbers for the disk(s) to be used for installation and press Enter. To cancel a choice, type the corresponding number and Press Enter. At least one bootable disk must be selected. The current choice is indicated by >>>.

| Name          | Location | Code          | Size(MB) | VGStatus |
|---------------|----------|---------------|----------|----------|
| Bootable Maps |          |               |          |          |
| >>>1          | hdisk0   | c1-f2-00-0,0  | 4056     | rootvg   |
| Yes           | No       |               |          |          |
| >>>2          | hdisk5   | c1-f13-00-0,0 | 4056     |          |
| rootvg        | Yes      | No            |          |          |
| 3             | hdisk1   | c1-f4-00-0,0  | 4056     | other    |
| vg            | Yes      | No            |          |          |
| 4             | hdisk2   | c1-f4-00-1,0  | 4056     | other vg |
| Yes           | No       |               |          |          |
| 5             | hdisk3   | c2-f1-00-0    | 02043    | other vg |
| Yes           | No       |               |          |          |

This menu displays the list of all available disks on which you can install the system backup image. The currently selected disks are indicated by >>> symbols.

**Note:** The system backup must be installed on one disk in each domain to achieve fault-tolerant operation. Valid choices in the example in [step 23](#) are hdisk0 and hdisk5. The rootvg disks for installation must have location codes

- c1-f2-00-0 for domain 0, and
- c1-f13-00-0 for domain 1.

**24** To select a disk or disks, enter the number of the disk, and press the Enter key.

**25** To deselect a selected disk, enter its number again and press the Enter key.

**26** When you have finished entering the settings, the System Backup Installation and Settings menu is displayed. Enter

0

and return to [step 22](#).

**27** Accept the current settings:

0

This begins the restore process and lasts at least 30 min. During the restore process, the monitor displays the approximate percentage of the tasks completed, and the elapsed time.

**Note 1:** If an error message appears at the end of the restore process, datavg did not import successfully. Contact the next level of support.

**Note 2:** You must manually re-boot the system if you are performing this procedure as part of the "Removing an I/O expansion chassis (NTRX50EC)" procedure in the Upgrades document. In this scenario, go to [step 28](#).

**Note 3:** As part of the restore process, the system reboots automatically and displays the login prompt. Continue with [step 29](#).

- 28** At the FX-bug prompt, manually boot the system:

```
FX-bug> pboot 1 0
```

*At the core manager*

- 29** Remove the S-tape from the tape drive when the reboot is completed, and store it in a secure location.

*At the local or remote terminal*

- 30** Log in to the core manager as a user authorized to perform fault-admin actions. Press the Enter key when you see the "TERM=(vt100)" prompt.

- 31** Start the core manager maintenance interface:

```
sdmmtc
```

- 32** Access the storage level:

```
> storage
```

*Example response:*

| volume Groups | Status   | Free (MB) |
|---------------|----------|-----------|
| rootvg        | Mirrored | 2032      |
| datavg        | Mirrored | 11712     |

| Logical Volume | Location | Size (MB) | % full/ |
|----------------|----------|-----------|---------|
| threshold 1 /  | rootvg   |           | 88      |
| 11/80          |          |           |         |
| 2 /usr         | rootvg   | 600       | 29/90   |
| 3 /var         | rootvg   | 200       | 5/70    |
| 4 /tmp         | rootvg   | 24        | 5/90    |
| 5 /home        | rootvg   | 304       | 5/70    |
| 6 /sdm         | rootvg   | 504       | 24/90   |
| 7 /data        | datavg   | 208       | 7/ 80   |

Logical volumes showing: 1 to 7 or 7

- 33 Determine the mirror status of the disks.

| If the disks are            | Do                      |
|-----------------------------|-------------------------|
| Mirrored                    | <a href="#">step 35</a> |
| Integrating or Not Mirrored | <a href="#">step 34</a> |

- 34 You cannot continue this procedure until disk mirroring is Mirrored. If necessary, contact the personnel responsible for your next level of support. When disk mirroring is at the Mirrored state, continue this procedure.

- 35 Access the LAN level:

`lan`

- 36 Check the state of DCE.

*Example response:*

DCE State: SysB

- 37 Access the application (APPL) level to check the state of any DCE-based applications:

`appl`

and pressing the Enter key.

*Example response:*

```
Application State
1 Table Access Service .
2 Log Delivery Service .
3 OM Access Service .
4 Secure File Transfer Fail
5 Enhanced Terminal Access Fail
6 Exception Reporting Fail
Applications showing 1 to 6 of 6
```

- 38

#### ATTENTION

DCE and DCE-based applications can fail if the key tab files restored from tape contain obsolete keys.

If the DCE state is displayed as SysB at the LAN menu level of the RMI ([step 35](#)), and the logs displayed indicate an error with the security client service in DCE, restore the service by performing the following procedures in the CS 2000 Core Manager Configuration Management document:

- "Removing a CS 2000 Core Manager from a DCE cell"

- "Configuring a CS 2000 Core Manager in a DCE cell"
- 39 If some DCE-based applications are faulty (Fail state, see [step 37](#)), try to restore them by busying (BSY) and returning to service (RTS) the applications from the SDM APPL level (see [step 37](#)).
  - 40 If this approach fails, restore them by performing the procedure to add the application server to the DCE cell in the CS 2000 Core Manager Configuration Management document.
  - 41 You must create a new system image backup tape. Refer to the procedure "Creating system image backup tapes (S-Tapes)" in the CS 2000 Core Manager Security and Administration document.
  - 42 You have completed this procedure.

---

—End—

---

## Performing a partial restore of the software from S-tape

### Purpose

Use this procedure to restore individual files or sets of files from the system image backup tape (S-tape).

### Prerequisites

You must be a user authorized to perform fault-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Procedures related to this procedure

| Procedure                                          | Document                    |
|----------------------------------------------------|-----------------------------|
| Logging in to the CS 2000 Core Manager             | Security and Administration |
| Displaying actions a user is authorized to perform | Security and Administration |



#### CAUTION

Use this procedure at the discretion of the system administrator.

Perform a partial restore only if you are familiar with the files, and know exactly which files are to be restored. If you restore the wrong files, you may inadvertently corrupt core manager software.

#### ATTENTION

This procedure must be performed by a trained AIX system administrator authorized to perform fault-admin actions.

#### ATTENTION

All volume groups on the core manager must be fully mirrored (Mirrored) before performing this procedure. If you attempt to perform this procedure when disk mirroring is not Mirrored, an error message is displayed on the screen.

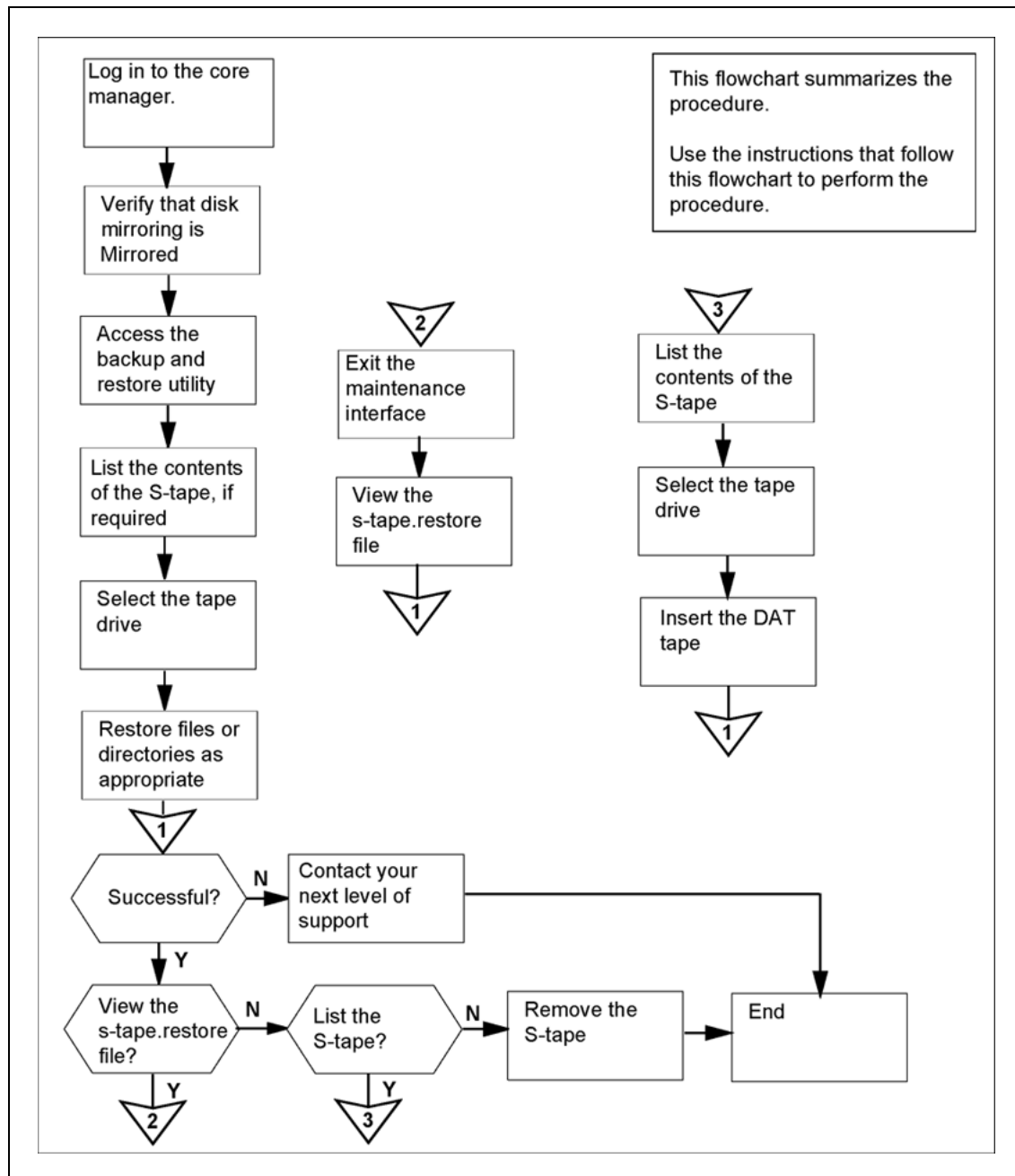
**ATTENTION**

If your system includes the SuperNode Billing Application (SBA), use tape drive DAT0 to perform this procedure.

**Action**

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the recovery tasks.

## Summary of Partial restore from the system image tape (S-tape)



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Partial restore from the system image tape (S-tape)

| Step | Action |
|------|--------|
|------|--------|

*At the local or remote console*

**1** Log into the core manager as the user authorized to perform fault-admin actions.

**2** Access the maintenance interface:

```
sdmmmtc
```

**3** Access the storage level:

```
storage
```

*Example response:*

| Volume Groups<br>(MB) | Status   | Free  |
|-----------------------|----------|-------|
| rootvg                | Mirrored | 2032  |
| datavg                | Mirrored | 11712 |

| Logical Volume<br>Size (MB) | Location | %full/threshold 1 / |
|-----------------------------|----------|---------------------|
|                             | rootvg   | 88                  |
| 2 /usr                      | rootvg   | 600                 |
|                             |          | 29/90               |
| 3 /var                      | rootvg   | 200                 |
|                             |          | 5/70                |
| 4 /tmp                      | rootvg   | 24                  |
|                             |          | 5/90                |
| 5 /home                     | rootvg   | 304                 |
|                             |          | 5/70                |
| 6 /sdm                      | rootvg   | 504                 |
|                             |          | 24/90               |
| 7 /data                     | datavg   | 208                 |
|                             |          | 7/80                |

Logical volumes showing: 1

to 7 of 7

**4** Determine the Mirror status of the disks.

| If the disks are | Do                     |
|------------------|------------------------|
| Mirrored         | <a href="#">step 6</a> |
| not Mirrored     | <a href="#">step 5</a> |



**CAUTION**

You cannot perform this procedure until disk mirroring of all volume groups is Mirrored.

- 5 If necessary, contact the personnel responsible for your next level of support. When disk mirroring is Mirrored, continue this procedure.

- 6 Access the administration (Admin) menu level of the RMI:

`admin`

- 7 Access the System Image Backup and Restore Menu:

`backup`

**Note 1:** If disk mirroring for all volume groups is not Mirrored, the system displays an error message. The system then prompts you to return to the System Image Backup and Restore menu.

**Note 2:** If another person attempts to use the backup and restore utility when it is in use, an error message is displayed on the screen.

*Example response:*

Currently there is a backup running on bnode73.  
Please execute yours later.  
Exiting...

- 8 Determine the contents of the tape.

| If you                         | Do                      |
|--------------------------------|-------------------------|
| wish to list the S-tape        | <a href="#">step 9</a>  |
| do not wish to list the S-tape | <a href="#">step 17</a> |

- 9 From the System Image Backup and Restore Menu, select "List Contents of the System Image Tape (S-tape)":

3

- 10 After you select option 3, you are prompted to select the tape drive.

*Example response:*

Select a tape drive you wish to use:  
Enter 0 to return to previous menu  
    Enter 1 for tape drive DAT0 in main  
Chassis-Slot 2  
    Enter 2 for tape drive DAT1 in Main  
Chassis-Slot 13

( 0, 1 or 2 ) ==>

**Note:** Use tape drive DAT0 (option 1) if your system also includes SBA.

- 11** Enter the number for the tape drive you want to use (1 or 2), and press the Enter key.

**Note:** If your system includes SBA, and you still wish to use DAT1 (option 2), the following message is displayed:

*Response:*

You have selected DAT 1. This is the default DAT drive for the Billing application, and may currently be in use for the emergency storage of billing records. If you continue to use DAT 1, make sure that the correct tape is in the drive, and that billing records will not be lost during the backup restore operation. Do you wish to continue with DAT 1? ( y | n )

- if you wish to continue using DAT1, enter y
- if you do not wish to use DAT1, enter n

The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

- 12** After you select the tape drive, the system prompts you to insert the S-tape into the appropriate tape drive.

*Example response:*

Please insert your System Image Backup tape (S-tape) into the tape drive DAT0 and allow at least 5 minutes to complete the listing. A log file will be saved in /tmp/s-tape.toc. Are you ready to proceed? ( y | n )

*At the core manager*

- 13** Insert the S-tape into the tape drive you selected.

**Note:** Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

*At the local or remote VT100 console*

- 14** When you are ready to continue this procedure, enter:

y

The contents of the S-tape are listed on the screen. When the listing is complete, the system prompts you to return to the System Image Backup and Restore Menu.

*Example response:*

```
Would you like to return to the previous menu?
(y | n)
```

- 15** Return to the System Image Backup and Restore Menu:

y

- 16** Determine if the file or directory has been restored.

| If you are listing the contents of the tape to verify | Do                      |
|-------------------------------------------------------|-------------------------|
| that the file has been restored                       | <a href="#">step 25</a> |
| the file name or directory that you wish to restore   | <a href="#">step 17</a> |

- 17** From the System Image Backup and Restore Menu, select "Restore Files from the System Image Tape (S-tape)":

4

- 18** After you select option 4, you are prompted to select the tape drive.

*Example response:*

```
Select a tape drive you wish to use:
Enter 0 to return to previous menu
 Enter 1 for tape drive DAT0 in Main
Chassis-Slot 2
 Enter 2 for tape drive DAT1 in Main
Chassis-Slot 13
(0, 1 or 2) ==>
```

**Note:** Use tape drive DAT0 (option 1) if your system also includes SBA.

- 19** Enter the number for the tape drive you want to use (1 or 2).

**Note:** If your system includes SBA, and you still wish to use tape drive DAT1 (option 2), the following message is displayed:

*Example response:*

```
You have selected DAT 1. This is the default DAT drive
for the Billing application, and may currently be in
use for the emergency storage of billing records.
If you continue to use DAT 1, make sure that the
correct tape is in the drive, and that billing records
will not be lost during the backup/restore operation.
```

Do you wish to continue with DAT 1? ( y | n )

- if you wish to continue using DAT1, enter y
- If you do not wish to use DAT1, enter n

The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

- 20** After you select the tape drive, you are prompted to insert the S-tape into the appropriate tape drive. A warning is displayed advising that this procedure must only be completed by qualified core manager system administrators. The warning also advises that files and directories must be entered exactly as they appear in the file listing. Insert the S-tape in the appropriate tape drive.

**Note:** Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

*Example response:*

Are you ready to enter the name of the file or directory? ( y | n )

- 21** Continue this procedure:

y

*Example response:*

Enter the name of the directory or file that you wish to restore as

./<your-full-path>/<your-file-or-directory>.

Note: Tape processing may take a few minutes to complete. A log file /tmp/s-tape.restore will be created.

==>

- 22** Enter the full path name of the directory or file that you wish to restore, exactly as shown in the file listing, including "/" at the beginning.

**Note 1:** A log file /tmp/s-tape.restore is created when the restore is completed.

**Note 2:** An error message is displayed if the restore is unsuccessful. If this occurs, go to [step 25](#).

- 23** During the restore process, the screen does not display any additional information. When the file restore is complete, the file you have restored is displayed. The system then prompts you to return to the System Image Backup and Restore Menu.

*Example response:*

Would you like to return to the previous menu? ( y |  
n )

**Note:** If the restore has failed, an error message is displayed before the prompt, advising you to list the contents of the tape, and perform the procedure again.

- 24 Return to the System Image Backup and Restore Menu:

y

- 25 Determine if the restore was successful. The system displays the file that you have restored, as described in [step 23](#). You may also wish to view the s-tape.restore file or list the files on the S-tape.

| If                                       | Do                                 |
|------------------------------------------|------------------------------------|
| the restore is successful                | <a href="#">step 32</a>            |
| the restore failed                       | contact your next level of support |
| you wish to view the s-tape.restore file | <a href="#">step 26</a>            |
| you wish to list the S-tape              | <a href="#">step 9</a>             |

- 26 Exit the System Image Backup and Restore Menu:

0

- 27 Exit the maintenance interface:

quit all

- 28 Access the s-tape.restore file:

cd /tmp

- 29 Scroll through the file:

more s-tape.restore

- 30 Continue pressing the Enter key until the files that you have restored, and the date of the restore, are displayed.

- 31 Determine if the restore was successful.

| If         | Do                                 |
|------------|------------------------------------|
| successful | <a href="#">step 33</a>            |
| failed     | contact your next level of support |

- 32 Exit the System Image Backup and Restore Menu:

0

**Note:** If you then wish to exit the maintenance interface, type quit all and press the Enter key.

*At the core manager*

**33** Remove the S-tape and store it in a secure place.

**34** You have completed this procedure.

---

—End—

---

# Recovering backup files from lost backup volumes

## Purpose

Use this procedure to recover backup files from lost backup volumes. The procedure swaps back old volumes as the primary backup volumes.

## Application

You need to recover backup files from lost backup volumes if the SBA cannot track backed up files when the SWACT and RESTART processes occur when you perform procedure "Configuring SBA backup volumes" in the Accounting document.

## Prerequisites

Before starting the procedure, you need

- the names of the swapped out volumes
- to have performed "Configuring SBA backup volumes on the core" in the Accounting document, and the SBA has completed its recovery of the volumes from the backup volumes you configured during these procedures.

## Action

### Procedure 1

#### Recovering backup files from lost backup volumes

| Step | Action |
|------|--------|
|------|--------|

#### *At the MAP*

- |   |                                                                                                                                                                                                                                   |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Post the billing stream:<br><pre>&gt; mapci;mtc;appl;sdbil;post &lt;stream_name&gt;</pre> where<br><stream_name> is the name of the billing stream.                                                                               |
| 2 | Quit back to the appl;sdbil level:<br><pre>&gt; quit</pre>                                                                                                                                                                        |
| 3 | Confirm that the names of the billing stream's existing backup volumes are the swapped in volumes you created earlier:<br><pre>&gt; conf view &lt;stream_name&gt;</pre> where<br><stream_name> is the name of the billing stream. |

**Note:** SBA does not support the configuration of more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

- 4 Read the notes you made when you performed the procedure, "Configuring SBA backup volumes on the core" in the Accounting document, to confirm that the backup volumes that you listed in [step 3](#) are the backup volumes you created with that procedure.

| If the backup volume names are                                          | Do                                                                                                        |
|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| the backup volume names configured when you performed the procedure     | continue with <a href="#">step 5</a>                                                                      |
| not the backup volume names configured when you performed the procedure | determine if someone else reconfigured the backup volumes before you continue with <a href="#">step 5</a> |

- 5 Access the billing level:  

```
> mapci;appl;sdmbil
```
- 6 Configure the billing stream of the logical volumes you created when you performed the procedure, "Configuring SBA backup volumes on the core" in the Accounting document:

```
> addvol <stream_name> <volume1> ... <volume5>
```

where

**<stream\_name>** is the name of the billing stream  
**<volume1> ... <volume5>** is the volume name. Up to five volumes (with each entry separated by a space) can be added at one time.

**Example**

To add five volumes, the command is:

```
addvol AMA S00DAMA S01DAMA S02DAMA S03DAMA S04DAMA
```

Repeat this step until all of the volumes have been added to the stream, and then proceed to [step 7](#).

- 7 Exit back to the command prompt:

```
> quit all
```

**Note 1:** The non-empty backup volumes are automatically detected by the SBA audits. In addition, the SBA places the billing stream into recovery mode and the volumes from the original backup volumes are sent to the core manager.



**Note 2:** You must provide, to all operating company personnel who work on the core, the names of the old and new backup volumes and the procedure you used to swap the volumes. They must be made aware that any restarts or switch of activity (SwAct) that occur before the billing stream returns to normal mode can cause a serious loss of billing records.

The mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.

8      You have completed this procedure.

---

—End—

---

## Restoring the oracle data on an SPFS-based server

### Application

Use this procedure to restore the oracle data from a backup tape or DVD on a Server Platform Foundation Software (SPFS)-based server (Sun Netra t1400 or Sun Netra 240). Also use this procedure to restore the data that was automatically backed up to a file on the server by the backup restore manager.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

Restoring the oracle data is not applicable to the MG 9000 Manager or the CBM as they do not use an oracle database.

### Prerequisites

You need the tape or DVD on which you backed up the oracle data. If the data was backed up by the backup restore manager, you need the name of the file located in directory /data/bkresmgr/backup.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

|                      |  |
|----------------------|--|
| <i>At the server</i> |  |
|----------------------|--|

- 1 Use the following table to determine how to start this procedure.

| If                         | Start at step          |
|----------------------------|------------------------|
| restoring from tape or DVD | <a href="#">step 2</a> |
| restoring from a file      | <a href="#">step 3</a> |

- 2 Insert the tape or DVD on which you backed up the oracle data, into the drive. If restoring the data from a file, start at [step 3](#).

**At your workstation**

- 3 Log in to the server.  
`> telnet <server>`  
 and pressing the Enter key.  
 where  
**server** is the IP address or host name of the SPFS-based server on which you are performing the data restore
- 4 When prompted, enter your user ID and password.
- 5 Change to the root user.  
`$ su -`  
 and press the Enter key.
- 6 When prompted, enter the root password.
- 7 Verify the permissions on the restore log directory (bkslog).  
`# ls -alrt /var/opt/nortel`  
 and press the Enter key.

**Example response**

```
total 22
lrwxrwxrwx 1 root succssn 28 Dec 22 2003
gwc -> /net/47.141.126.131//swd/gwc
drwxrwxr-x 4 root other 512 Dec 22 2003 .
drwxr-xr-x 7 root sys 512
Sep 10 12:41 ..
drwxr-xr-x 2 oracle oinstall 512
Dec 8 15:58 db
```

```
drwxrwxrwt 2 root other 6656 Dec
15 19:56 bkslog
```

| If the permissions of bkslog | Do                     |
|------------------------------|------------------------|
| are drwxrwxrwt               | <a href="#">step 9</a> |
| are not drwxrwxrwt           | <a href="#">step 8</a> |

- 8 Change the permissions of bkslog.  

```
chmod 1777 /var/opt/nortel/bkslog
```

and press the Enter key.
- 9 Determine if server applications have been stopped.  

```
servquery -status all
```

and press the Enter key.
- 10 If not already done, stop the server applications that run on the server.

| For                                              | Refer to                                                                                                                                                                                                                                  |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CS 2000 Management Tools server applications     | Stopping the SESM server application<br><a href="#">"Starting the SAM21 Manager server application" (page 541)</a><br><a href="#">"Stopping the NPM server application" (page 578)</a><br>ATM/IP Security and Administration, NN10402-600 |
| MG 9000 Manager and mid-tier server applications | MG 9000 Security and Administration, NN10162-611, if required                                                                                                                                                                             |
| IEMS server application                          | IEMS Security and Administration, NN10336-611, if required                                                                                                                                                                                |

- 11 Verify the permissions, owner and group of /data/oradata by typing:  

```
#ls -l /data
```

and pressing the Enter key.

*Example response:*

```
drwxr-xr-x 7 oracle oinstall 512 Oct
16 18:13 oradata
```

- 12 Use the following table to determine the next step:

| If                                                                                                                         | Go to                   |
|----------------------------------------------------------------------------------------------------------------------------|-------------------------|
| permission is "drwxr-xr-x"<br>owner is "oracle" and<br>group is "oinstall" as shown in the<br>example in the previous step | <a href="#">step 14</a> |
| values do not match the example<br>in the previous step                                                                    | <a href="#">step 13</a> |

- 13 Change the permission, owner and group of /data/oradata by typing:

```
#chmod 755 /data/oradata
```

and pressing the Enter key

```
#chown oracle /data/oradata
```

and pressing the Enter key

```
#chgrp oinstall /data/oradata
```

and pressing the Enter key

- 14 Verify the permissions, owner and group of /data/oradata/arch by typing:

```
#ls -l /data/oradata
```

and pressing the Enter key.

*Example response:*

```
drwxr-xr-x 4 oracle oinstall 512
Oct 16 18:36 arch
```

- 15 Use the following table to determine the next step:

| If                                                                                                                         | Go to                   |
|----------------------------------------------------------------------------------------------------------------------------|-------------------------|
| permission is "drwxr-xr-x"<br>owner is "oracle" and<br>group is "oinstall" as shown in the<br>example in the previous step | <a href="#">step 17</a> |
| values do not match the example<br>in the previous step                                                                    | <a href="#">step 16</a> |

- 16 Change the permission, owner and group of /data/oradata/arch by typing:

```
#chmod 755 /data/oradata/arch
```

and pressing the Enter key

```
#chown oracle /data/oradata/arch
```

and pressing the Enter key

```
#chgrp oinstall /data/oradata/arch
```

and pressing the Enter key

- 17** Use the following table to determine your next step.

| If                         | Do                      |
|----------------------------|-------------------------|
| restoring from tape or DVD | <a href="#">step 18</a> |
| restoring from a file      | <a href="#">step 20</a> |

- 18** Restore the database from backup tape or DVD.

```
$ /opt/nortel/SPFS/bks/rsdata
```

and press the Enter key.

- 19** Remove the tape from the drive, or eject the DVD from the drive as follows:

- a. Ensure you are at the root directory level.

```
cd /
```

and press the Enter key.

- b. Eject the DVD.

```
eject cdrom
```

and press the enter key.

If the DVD drive tray does not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
/etc/init.d/volmgt stop
```

```
/etc/init.d/volmgt start
```

Press the eject button located on the front of the DVD drive.

- c. Remove the DVD from the drive.

Proceed to [step 21](#).

- 20** Restore the database from the backup file.

```
$ /opt/nortel/SPFS/bks/rsdata -f /data/bkresmgr/backup
/<filename>
```

and press the Enter key.

| Variable   | Value                                                                |
|------------|----------------------------------------------------------------------|
| <filename> | is the name of the backup file created by the backup restore manager |

- 21** Verify that the database restored properly.

```
queryAllFaults
```

and press the Enter key.

If an alarm appears like the following, the database was not restored properly:

```
*** SPFS330 Import of Oracle data caused corruption
ORA-22337: Error importing Oracle data cs2kaps=rtp6ba
ckupsesm;NODE=rtp6backupsesm;CLASS=SW;SWTYPE=Database
Fri Jun 10 15:48:59 2005
```

- 22** Use the information in the following table to determine the next step.

| If                                    | Do                      |
|---------------------------------------|-------------------------|
| no alarm appears                      | <a href="#">step 23</a> |
| alarm appears                         | contact Nortel          |
| the database did not restore properly | contact Nortel          |

- 23** Use the following table to determine your next step.

| If                           | Do                      |
|------------------------------|-------------------------|
| WebPKProxy is configured     | <a href="#">step 24</a> |
| WebPKProxy is not configured | <a href="#">step 27</a> |

- 24** Restore the WebPKProxy.

```
ls /data/pkclient/certificates
```

and press the Enter key.

- 25 Use the following table to determine your next step.

| If                                                                                                                                                                         | Do                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| the following files are associated with this machine: <ul style="list-style-type: none"> <li>• CA1_Cert.pem</li> <li>• CA2_Cert.pem</li> <li>• TRUSTED_Cert.pem</li> </ul> | <a href="#">step 26</a> |
| the above files do not exist                                                                                                                                               | <a href="#">step 27</a> |

- 26 Reconfigure WebPKProxy as follows:

- a. From the CLI, select Configuration ---> Security Services Configuration ---> Certificate Manager Certificate Installation ---> install\_certs.

Wait for the script to complete. Verify that no errors displayed.

- b. From the CLI, select Configuration ---> Security Services Configuration ---> WebPKProxy/PKClient---> register\_pkclient.
- c. Enter the host name of the Certificate Manager.

The Certificate Manager box must be fully functional for this step to succeed.

Wait for the script to complete. Verify that no errors displayed.

- 27 Start the server applications that run on the server.

| For                                              | Refer to                                                                                                                                                                                                                                  |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CS 2000 Management Tools server applications     | Stopping the SESM server application<br><a href="#">"Starting the SAM21 Manager server application" (page 541)</a><br><a href="#">"Stopping the NPM server application" (page 578)</a><br>ATM/IP Security and Administration, NN10402-600 |
| MG 9000 Manager and mid-tier server applications | the MG 9000 Security and Administration document, NN10162-611, if required                                                                                                                                                                |
| IEMS server application                          | the IEMS Security and Administration document, NN10336-611, if required                                                                                                                                                                   |



If one or more applications do not start, contact Nortel for assistance.  
You have completed this procedure.

---

—End—

---

## Performing a full system restore on an SPFS-based server

### Application

Use this procedure to perform a full system restore from backup media on a Server Platform Foundation Software (SPFS)-based server (Sun Netra t1400 or Sun Netra 240).

A full system restore consists of reverting to the previous release of SPFS, restoring the file systems, and restoring the oracle data.

#### ATTENTION

After performing a full system restore on IEMS you must also perform a subsequent central server restore. Refer to: *Restoring the Central Security Server* in *IEMS Administration and Security*, NN10336-611

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

Restoring the oracle data is not applicable to the CBM as it does not use an oracle database.

#### ATTENTION

System logs indicating application and database errors, will be generated until the file systems and oracle data are restored on the system using this procedure and procedure ["Restoring the oracle data on an SPFS-based server" \(page 254\)](#). No database errors will be generated on the CBM as it does not use an oracle database.

### Prerequisites

This procedure has the following prerequisites:

- you need SPFS CD disk #1 for the release you are reverting to
- you need the tape or DVD on which you backed up the file systems
- you need the tape or DVD on which you backed up the oracle data

## Action

Use one of the following methods according to your office configuration.

- "Simplex configuration (one server)" (page 263)
- "High-availability configuration (two servers)" (page 265)

Only the "Simplex configuration (one server)" (page 263) is applicable to perform a full system restore from tape on a Sun Netra t1400 server.

### Simplex configuration (one server)

| Step                                                                                                                                                                                             | Action                                                                                                                                                                                                                                                                                                                                                            |                   |    |      |        |     |        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|----|------|--------|-----|--------|
| <b>At the server console</b>                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                   |                   |    |      |        |     |        |
| 1                                                                                                                                                                                                | Log in to the server through the console (port A) using the root user ID and password.                                                                                                                                                                                                                                                                            |                   |    |      |        |     |        |
| 2                                                                                                                                                                                                | Bring the system to the OK prompt by typing<br><code># init 0</code><br>and pressing the Enter key.                                                                                                                                                                                                                                                               |                   |    |      |        |     |        |
| 3                                                                                                                                                                                                | Insert SPFS CD disk#1 into the drive.                                                                                                                                                                                                                                                                                                                             |                   |    |      |        |     |        |
| 4                                                                                                                                                                                                | Use the following table to determine your next step.                                                                                                                                                                                                                                                                                                              |                   |    |      |        |     |        |
| <table border="1"> <thead> <tr> <th>If restoring from</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>tape</td> <td>step 5</td> </tr> <tr> <td>DVD</td> <td>step 6</td> </tr> </tbody> </table> |                                                                                                                                                                                                                                                                                                                                                                   | If restoring from | Do | tape | step 5 | DVD | step 6 |
| If restoring from                                                                                                                                                                                | Do                                                                                                                                                                                                                                                                                                                                                                |                   |    |      |        |     |        |
| tape                                                                                                                                                                                             | step 5                                                                                                                                                                                                                                                                                                                                                            |                   |    |      |        |     |        |
| DVD                                                                                                                                                                                              | step 6                                                                                                                                                                                                                                                                                                                                                            |                   |    |      |        |     |        |
| 5                                                                                                                                                                                                | Insert the tape on which you backed up the file systems, into the drive.                                                                                                                                                                                                                                                                                          |                   |    |      |        |     |        |
| 6                                                                                                                                                                                                | At the OK prompt, restore the system by typing<br><code>OK boot cdrom - restore</code><br>and pressing the Enter key.                                                                                                                                                                                                                                             |                   |    |      |        |     |        |
| 7                                                                                                                                                                                                | When prompted, accept the software license restrictions by typing<br><code>ok</code><br>and pressing the Enter key.<br><br>The system reboots.<br><br>If the restore process fails at this point due to one or more disks not being labeled, which is reported as 'Bad Magic Number in Disk Label', refer to procedure 'Labelling disks on an SPFS-based server'. |                   |    |      |        |     |        |

If restoring from DVD, you will be prompted to insert Volume 1 of the backup DVD into the drive. Insert the DVD on which you backed up the file systems. During the restore process, the system will prompt you for additional Volumes if more than one DVD was used during the backup of file systems.

The restore process can take several hours to complete depending on the number and size of the files that are being restored.

Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.

**8** Eject the backup DVD from the drive as follows:

- a. Ensure you are at the root directory level by typing

```
cd /
```

and pressing the Enter key.

- b. Eject the DVD by typing

```
eject cdrom
```

and pressing the Enter key.

If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
/etc/init.d/volmgt stop
```

```
/etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.

- c. Remove the backup DVD from the drive.

**9** Use the following table to determine your next step.

| If the server is hosting                  | Do                      |
|-------------------------------------------|-------------------------|
| this SPFS-based server is hosting the CBM | step <a href="#">13</a> |
| otherwise                                 | step <a href="#">10</a> |

**10** List the oracle groups by typing

```
groups oracle
```

and pressing the Enter key.

| If the output is                       | Do      |
|----------------------------------------|---------|
| oinstall data dbs or oinstall dbs data | step 12 |
| oinstall dba data                      | step 11 |

- 11 Correct the oracle groups by typing  

```
usermod -g oinstall -G data,dba oracle
```

 and pressing the Enter key.
- 12 Restore the oracle data using procedure ["Restoring the oracle data on an SPFS-based server" \(page 254\)](#). Once the data restore is complete, execute step 13 of this procedure.
- 13 Reboot the server by typing  

```
init 6
```

 and pressing the Enter key.
- 14 Ensure the node is active by typing  

```
cd/opt/nortel/sspfs/ha
```

```
./ActivateNode
```

---

—End—

---

### High-availability configuration (two servers)

---

| Step | Action |
|------|--------|
|------|--------|

---

***At the console connected to the inactive node***

- 1 Log in to the inactive node through the console (port A) using the root user ID and password.
- 2 Bring the system to the OK prompt by typing  

```
init 0
```

 and pressing the Enter key.

***At the console connected to the active node***

- 3 Log in to the active node through the console (port A) using the root user ID and password.
- 4 Bring the system to the OK prompt by typing

```
init 0
```

and pressing the Enter key.

- 5 Insert SPFS DVD disk#1 into the drive.

- 6 At the OK prompt, restore the system by typing

```
OK boot cdrom - restore
```

and pressing the Enter key.

- 7 When prompted, accept the software license restrictions by typing

```
ok
```

and press the Enter key.

The system reboots.

- 8 When prompted, insert Volume 1 of the DVD on which you backed up the file systems, into the drive.

During the restore process, the system will prompt you for additional Volumes if more than one CD or DVD was used during the backup of file systems.

The restore process can take several hours to complete depending on the number and size of the files that are being restored.

Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.

- 9 Eject the backup DVD from the drive as follows:

- a. Ensure you are at the root directory level by typing

```
cd /
```

and pressing the Enter key.

- b. Eject the DVD by typing

```
eject cdrom
```

and pressing the Enter key.

If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
/etc/init.d/volmgt stop
```

```
/etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.

- c. Remove the backup CD or DVD from the drive.

- 10 Use the following table to determine your next step.

| If the server is hosting                  | Do      |
|-------------------------------------------|---------|
| this SPFS-based server is hosting the CBM | step 14 |
| otherwise                                 | step 11 |

- 11 List the oracle groups by typing

```
groups oracle
```

and pressing the Enter key.

| If the output is                       | Do      |
|----------------------------------------|---------|
| oinstall dba data                      | step 13 |
| oinstall data dbs or oinstall dbs data | step 12 |

- 12 Correct the oracle groups by typing

```
usermod -g oinstall -G data,dba oracle
```

and pressing the Enter key.

- 13 Restore the data using procedure ["Restoring the oracle data on an SPFS-based server" \(page 254\)](#). Once the data restore is complete, execute steps 14 and 15 of this procedure.

- 14 Reboot the server by typing

```
init 6
```

and pressing the Enter key.

- 15 Ensure the node is active by typing

```
cd/opt/nortel/sspfs/ha
```

```
./ActivateNode
```

- 16 Re-image the inactive node using the active node's image. If required, refer to procedure ["Cloning the image of one node in a cluster to the other node" \(page 528\)](#).

You have completed this procedure.

---

—End—

---

## Labelling disks on an SPFS-based server

### Application

Use this procedure when, during a full system restore, a failure occurred due to one or more disks not being labeled, which is reported as "Bad Magic Number in Disk Label". This procedure applies to labeling disks on a Server Platform Foundation Software (SPFS)-based server, Sun Netra t1400 or Sun Netra 240.

### Prerequisites

This procedure has the following prerequisites:

- the system is at the OK prompt
- the SPFS Installation CD disk#1 from which you were attempting a full system restore is still in the drive

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

**At the server console**

- 1 At the OK prompt, boot the system by typing  
OK **boot cdrom -s**  
and pressing the Enter key.
- 2 At the shell prompt, access the disk partitioning and maintenance utility by typing  
\$ **format**  
and pressing the Enter key.
- 3 Specify disk 0 by typing  
\$ **0**  
and pressing the Enter key.
- 4 Use the following table to determine your next step.

| If                                  | Do                     |
|-------------------------------------|------------------------|
| prompted to label the disk (disk 0) | step <a href="#">5</a> |
| otherwise                           | step <a href="#">6</a> |



- 5 Confirm you want to label the disk by typing

**yes**

and pressing the Enter key.

- 6 Specify disk 1 by typing

`format> disk 1`

and pressing the Enter key.

- 7 Use the following table to determine your next step.

| If                                  | Do     |
|-------------------------------------|--------|
| prompted to label the disk (disk 1) | step 8 |
| otherwise                           | step 9 |

- 8 Confirm you want to label the disk by typing

**yes**

and pressing the Enter key.

- 9 Use the following table to determine your next step.

| If your server is a | Do      |
|---------------------|---------|
| Sun Netra t1400     | step 10 |
| Sun Netra 240       | step 16 |

- 10 Specify disk 2 by typing

`format> disk 2`

and pressing the Enter key.

- 11 Use the following table to determine your next step.

| If                                  | Do      |
|-------------------------------------|---------|
| prompted to label the disk (disk 2) | step 12 |
| otherwise                           | step 13 |

- 12 Confirm you want to label the disk by typing

**yes**

and pressing the Enter key.

- 13 Specify disk 3 by typing

`format> disk 3`

and pressing the Enter key.

- 14** Use the following table to determine your next step.

| If                                  | Do                      |
|-------------------------------------|-------------------------|
| prompted to label the disk (disk 3) | step <a href="#">15</a> |
| otherwise                           | step <a href="#">16</a> |

- 15** Confirm you want to label the disk by typing

**yes**

and pressing the Enter key.

- 16** Exit the disk partitioning and maintenance utility by typing

`format> quit`

and pressing the Enter key.

- 17** Reboot the server by typing

`# init 0`

and pressing the Enter key.

- 18** Return to procedure "[Performing a full system restore on an SPFS-based server](#)" (page 262), and execute again.

---

—End—

---

# Restoring the central security server

## Application

Use this procedure to restore the security server from a backup file.

### ATTENTION

SSL uses certificates. Certificates from one server cannot be used on another server. If you want to take a backup file from a server where SSL is implemented and restore to a different server, you must perform the procedure "Replacing HTTPS certificate on security server for SunOne component" in *ATM/IP Solution-level Administration and Security*, NN10402-600 after the restore is completed. This script is run to set up IS authentication, session, and policy traffic to operate under SSL.

Note that servers in the same high availability cluster can use the same SSL certificate.

Note that if the restored IS SSL certificate has expired, you must perform the procedure in "Replacing HTTPS certificate on security server for SunOne component" in *ATM/IP Solution-level Administration and Security*, NN10402-600 after the restore is completed.

## Prerequisites

This procedure has the following prerequisites:

- You must have root user privileges.
- You must have a backup tar file created using the procedure for "[Backing up the central security server](#)" (page 144).

## Action

Perform the following steps to restore central security server data.

| Step | Action |
|------|--------|
|------|--------|

### *At your workstation*

- 1 Telnet to the server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
**server** is the IP address or host name of the server  
 If you are upgrading the active server, telnet to the active server. If you are upgrading the inactive server, telnet to the inactive server.
- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing:

```
$ su - root
```

and pressing the Enter key.

- 4 When prompted, enter the root password.

| If                                                                                                       | Do                     |
|----------------------------------------------------------------------------------------------------------|------------------------|
| you are performing this procedure during an upgrade on the inactive server of a two-server configuration | <a href="#">step 7</a> |
| otherwise                                                                                                | <a href="#">step 5</a> |

- 5 Stop the security services by doing the following:

- a. Type:

```
servstop RADSVR
```

and press the Enter key.

- b. Type:

```
servstop IS
```

and press the Enter key.

- c. Type:

```
servstop WEBSERVICES
```

and press the Enter key.

- 6 List the available security server backup files and determine the backup file to be restored by typing:

```
ls /data/bkresmgr
```

and pressing the Enter key.

The format of the security server backup files are  
 <data><time>backupSS1.1<host\_name>.tar

Note the name of the security server backup file you intend to restore. You will need this information in a later step.

- 7 Change directories by typing:

```
cd /opt/nortel/applications/security/current_slisext
/swmgmt/bin
```

and pressing the Enter key.

- 8 Determine if SAML is enabled on the workstation by looking at the nsswitch.conf file.

Type:

```
vi /etc/nsswitch.conf
```

press the enter key

if: the following is seen:

```
passwd: files
```

```
group: files
```

do: continue to step 10

if: saml is seen in the two lines, for example:

```
passwd: saml files
```

```
group: saml files
```

do: continue to step 9

**9** Disable SAML by typing:

```
vi /etc/nsswitch.conf
```

press the enter key

replace the "passwd:" & "group:" lines with the following:

```
passwd: files
```

```
group: files
```

save and close the file

**10** Perform the restore operation by typing:

```
./brr_security.sh -restore /data/bkresmgr/<date><time>backupSS1.1<host_name>.tar
```

where <date><time>backupSS1.1<host\_name>.tar is the backup file from which you are restoring.

Press the Enter key.

| If                                                                                                       | Do                      |
|----------------------------------------------------------------------------------------------------------|-------------------------|
| you are performing this procedure during an upgrade on the inactive server of a two-server configuration | <a href="#">step 13</a> |
| otherwise                                                                                                | <a href="#">step 11</a> |

**11** Restart the security services by doing the following:

a. Type:

```
servstart WEBSERVICES
```

and press the Enter key.

b. Type:

```
servstart IS
```

and press the Enter key.

c. Type:

```
servstart RADSVR
```

and press the Enter key.

**12** Enable SAML by typing:

```
vi /etc/nsswitch.conf
```

and press the Enter key.

replace the passwd: & group: lines with the following:

```
passwd: saml files
group: saml files
```

save and close the file.

**13** If the restored image was backed up from a different server with a different certificate or if the restored certificate has expired, follow the procedure in "Replacing HTTPS certificate on security server for SunOne component" in *ATM/IP Solution-level Administration and Security*, NN10402-600 to replace the invalid or expired certificate on the IEMS Server.

**14** Select your next step.

| If you are restoring a server        | Do                      |
|--------------------------------------|-------------------------|
| in a simplex configuration           | <a href="#">step 17</a> |
| in a high-availability configuration | <a href="#">step 15</a> |

**15** Select your next step.

| If                                                                                                       | Do                      |
|----------------------------------------------------------------------------------------------------------|-------------------------|
| you are performing this procedure during an upgrade on the inactive server of a two-server configuration | <a href="#">step 17</a> |
| otherwise                                                                                                | <a href="#">step 16</a> |

**16** Clone the active server to the inactive server. For details, see "Cloning the image of one node in a cluster to the other node" in *ATM/IP Solution-level Administration and Security*, NN10402-600.

**17** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

## Domain Naming Service

---

A Domain Name Server (DNS) serves two independent functions in the CS LAN. The DNS functions are provided by a standard DNS server to be provided by the customer. There are two DNS functions:

- the first OAM DNS function is required in an OAM&P system. See ["DNS in an OAM and P system" \(page 276\)](#).

**Note:** The workaround to deploying DNS is to modify the etc/host files for each of the client machines that access the Succession OAM servers using fully qualified domain names (FQDN) which resolve those names in the client machines. However, to use this workaround, you need to configure each client machine and modify each client machine when network changes occur.

- the second DNS function is needed only in a small line gateway deployment, and is optional. See ["DNS in a small line gateway application" \(page 278\)](#).

### DNS in an OAMP system

The DNS service is used in two ways for the OAM system.

- Firstly, DNS is used to secure client /server interaction using the HTTPS protocol. HTTPS is activated by the installation of a security certificate on the Sun server. The browser uses the certificate to authenticate the server and encrypt the connection in both directions between the client desktop browsers and the element management (EM) servers. This protects passwords and user information used within the system. This DNS service is customer provided and can be located in the OAM&P/NOC LAN.
- Secondly, an internal Nortel usage in the CO-LAN is used by IEMS. IEMS uses the DNS service for data encryption.

DNS is required by HTTPS in Succession OAM. The client desktop browser asks the EM server for the security certificate. The browser must determine if the security certificate is valid and not supplied from an untrusted source. To determine validity of the security certificate the browser will match the Fully Qualified Domain Name (FQDN) of the server hostname in the certificate with the trusted list located in the DNS service. This is done through a DNS lookup. If the DNS lookup works, then the browser continues to validate the rest of the certificate information. It checks with the Certificate Authority (CA) to see if the certificate is valid or not.



If DNS is not provided in the CVoIP OAM and the EM servers are not added as valid entries in a customer's DNS server, the browser will get a failed look up on the FQDN in the certificate. If this fails, the rest of the certificate is not validated, and no HTTPS connection is established to the server.

CVoIP OAM has optionally supported DNS since (I)SN05, but is required from (I)SN07 as secure client access becomes the only supported configuration. DNS resolution must be enabled on the Sun server to allow the security certificates to work, and must be enabled prior to the installation of the certificate. Refer to the procedure for Configuring Domain Name Service in ATM/IP Solution-level Configuration Management, NN10409-500 for more information. The following EM servers and their clients use the DNS Service for the HTTPS protocol.

- CS 2000 Management components
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager (MG 9000 Manager)
- USP Manager GUI
- Integrated Element Management System (IEMS)

**Note:** In addition, IEMS uses the DNS Service for IEMS Server to IEMS Client data encryption via Secure Socket Layer (SSL).

- Access to the following clients via HTTPS access proxy:
  - STORM from (I)SN06.2
  - CICM from (I)SN07
  - Session Server from (I)SN07

**Note:** A maximum of only five DNS entries is needed for each CO (CS 2000 Logical Call Server) to match the IP address to the FQDN.

## OAM DNS service configuration

Each of the EM servers defined in an office must be added. This includes all of the virtual IP address and hostnames, along with the physical IP addresses and hostnames.

Each of the clients that access any of the CVoIP servers need to reference the DNS server that has been configured with the EM server entries.

The OAM&P servers must be added to the customer's intranet DNS servers prior to installing security certificates. It is recommended that the certificates are installed at the end of the OAM&P installation process and prior to the upgrade of an existing system.

### Types of certificate

There are three types of security certificates that can be used.

- a certificate granted from a well known certificate granting authority (CA)
- company generated: used when the operating company has its own internal CA
- self signed: created locally on the server

These certificates differ in the level of trust that needs to be assigned to a server. This is based on how the server is used.

- If the server is used in a public way, such as for e-commerce websites, then a certificate from a CA is required.
- If the server is used internally within a company, then the company generated certificate can also be used.
- If the server is used in a more restricted manner, then a self-signed certificate can also be used to protect the client to server communications. However, when the server is accessed, the browser presents the certificate and asks whether the certificate can be trusted. If the user answers 'yes', the server can be accessed. If the user answers 'no', nothing further will be received from the server.

**Note:** A certificate obtained from a CA must include a PEM header and must not have a password.

### DNS in a small line gateway application

The second DNS application is optional and is needed only in a small line gateway deployment, whereas the OAM DNS must be shared across COs and OSSs and across client workstations and remote access. This use of DNS in a small line gateway allows for a more streamlined provisioning of small line gateways by associating the MAC-FQDN for the small line gateway with the gateway IP address, allowing the gateway's IP address in GWC Manager to be set to 0.0.0.0. You can also use DNS when the Redirecting Media Gateway Controller (RMGC) is used for the IAW or IAC solutions to provide ease of engineering GWs across GWCs.

For security reasons, it is not recommended or supported for the DNS for the small lines gateway applications to be the same as the OAM DNS. Protocols and services should not be shared between the subscriber access and the OAM operations sections of the networks. The OAM DNS must be shared across COs, the operator's internal operations LAN, and OSSs.

### Redundant DNS servers

The DNS deployment model recommends that more than one DNS server is deployed in the event that a DNS server is down. It is also recommended that the redundant DNS servers have the identical information configured

on each. Standard DNS products and standard DNS deployment policies and capabilities support both of these recommendations. The DNS servers need to be accessible from the LANs where the client desktop computers are connected. The DNS servers may also be connected to the rest of the DNS network in the customer's internal network. The customer must define the domain assigned to each office and the hostnames that are given to the servers in the office.

## Group-based User Authorization

This section provides overview information about CVoIP security domains and user groups and references to documentation containing user logs.

### SPFS Security User Groups

A number of new Secure Platform Foundation Software (SPFS) security domains and user groups are now available. The domains and user groups a user is assigned to control which operations the user is authorized to perform.

The SPFS user group domains and their target systems are as follows:

- **ln.** This includes line services, line cards, v5.2 services, and small line gateways (port level).
- **trk.** This includes trunks, trunk-based services, v5.2 services, small trunking gateways (port level), carrier, and carrier-based services.
- **mg.** This includes small and large gateways, including UAS, CICM, and Media Gateway.
- **mgc.** This includes CS 3000, CS 2000, USP, GWC, CS 2000 SAM21, MCS 5200, 3PC, and Storm.
- **ems.** This includes SPFS-based managers, SDM, , MDM,MDP, KDC, and others.

The following table maps the available Succession roles and user groups.

Succession User Group Definitions map

| Role                            | Domain  |          |               |          |          |
|---------------------------------|---------|----------|---------------|----------|----------|
|                                 | Line    | Trunk    | Media Gateway | MGC      | EMS/EML  |
| Administration (adm)            | lnadm   | trkadm   | mgadm         | mgcadm   | emsadm   |
| Read/Write (rw)                 | lnrw    | trkrw    | mgrw          | mgcrw    | emsrw    |
| Read Only (ro)                  | lnro    | trkro    | mgro          | mgcro    | emsro    |
| Subscriber Provisioning (sprov) | lnsprov | trksprov | mgsprov       | mgcsprov | emssprov |
| Maintenance (mtc)               | lnmtc   | trkmtc   | mgmtc         | mgcmtc   | emsmtc   |

With group-based authorization, users are created and associated with different groups based on the operations they perform.

Administration of security accounts is not permitted from the client side.

Only users with permissions to login to the Succession Communication Server 2000 Management Tools and who belong to the user group succssn on the server can perform security administration activities.

For details about managing user accounts, refer to your Succession networks component documentation.

For details about assigning users to secondary user groups, see Setting up local user accounts on an SSPFS-based server.

**Note:**

**CS 2000 SAM21 Manager Action/Permission/Groups Mapping**

|                                                          | Permission Required | mgc-adm | mgc-rw | mgc-mtc | mgc-sprov | mgc-ro |
|----------------------------------------------------------|---------------------|---------|--------|---------|-----------|--------|
| <b>Subnet</b>                                            |                     |         |        |         |           |        |
| Add new SAM21 NE                                         | nortel.mgc.iprov    | x       | x      |         |           |        |
| Modify existing SAM21 NE properties                      | nortel.mgc.iprov    | x       | x      |         |           |        |
| Decommission SAM21 NE                                    | nortel.mgc.iprov    | x       | x      |         |           |        |
| <b>Frame</b>                                             |                     |         |        |         |           |        |
| View SAM21 Shelf                                         | nortel.mgc.ro       | x       | x      | x       | x         | x      |
| Reprovision SAM21 Node                                   | nortel.mgc.iprov    | x       | x      |         |           |        |
| <b>Shelf</b>                                             |                     |         |        |         |           |        |
| Configurations - IPoA Services - View Services           | nortel.mgc.ro       | x       | x      | x       | x         | x      |
| Configurations - IPoA Services - Configure Services      | nortel.mgc.iprov    | x       | x      |         |           |        |
| Configurations - ATM PMC addresses - View addresses      | nortel.mgc.ro       | x       | x      | x       | x         | x      |
| Configurations - ATM PMC addresses - Configure addresses | nortel.mgc.iprov    | x       | x      |         |           |        |
| Alarm Browser                                            | nortel.mgc.ro       | x       | x      | x       | x         | x      |
| View Cards                                               | nortel.mgc.ro       | x       | x      | x       | x         | x      |
| View Subnet                                              | nortel.mgc.ro       | x       | x      | x       | x         | x      |
| <b>SC Card</b>                                           |                     |         |        |         |           |        |
| - Lock/unlock                                            | nortel.mgc.mtc      | x       | x      | x       |           |        |

|                           | Permission Required | mgc-adm | mgc-rw | mgc-mtc | mgc-sprov | mgc-ro |
|---------------------------|---------------------|---------|--------|---------|-----------|--------|
| - Diagnostic              | nortel.mgc.mtc      | x       | x      | x       |           |        |
| - State -swact            | nortel.mgc.mtc      | x       | x      | x       |           |        |
| - View Subnet             | nortel.mgc.ro       | x       | x      | x       | x         | x      |
| - View SAM21 Shelf        | nortel.mgc.ro       | x       | x      | x       | x         | x      |
| <b>NSS Cards</b>          |                     |         |        |         |           |        |
| - Lock/unlock             | nortel.mgc.mtc      | x       | x      | x       |           |        |
| - Assign/Unassign Service | nortel.mgc.iprov    | x       | x      |         |           |        |
| - Modify Provisioning     | nortel.mgc.iprov    | x       | x      |         |           |        |
| - Diagnostic              | nortel.mgc.mtc      | x       | x      | x       |           |        |
| - View Subnet             | nortel.mgc.ro       | x       | x      | x       | x         | x      |
| - View SAM21 Shelf        | nortel.mgc.ro       | x       | x      | x       | x         | x      |
| - View Mate Card          | nortel.mgc.ro       | x       | x      | x       | x         | x      |

## Reference Information

For security logs, please refer to the following documents:

| NTP number  | Document                                                                                |
|-------------|-----------------------------------------------------------------------------------------|
| NN10170-611 | <i>CS 2000 Core Manager Security and Administration</i>                                 |
| NN10180-611 | <i>MSS 15000, MG 15000 and MDM in Security and Administration PT-AAL1/UA-AAL1/UA-IP</i> |
| NN10275-909 | <i>Carrier Voice Over IP Fault Management Logs Reference (multi-volumes)</i>            |

---

## PAM-based user authentication

---

### Overview

Carrier Voice over IP (CVoIP) network components use the pluggable authentication module (PAM) framework to support different authentication technologies without changing login services. PAM preserves existing system environments while supporting security services such as login, rlogin, and telnet.

PAM can be used to integrate login services with different authentication technologies, such as RSA, DCE, Kerberos, S/Key, and smart card based authentication systems. Thus, PAM enables networked applications to operate in different customer environments which utilize different security mechanisms.

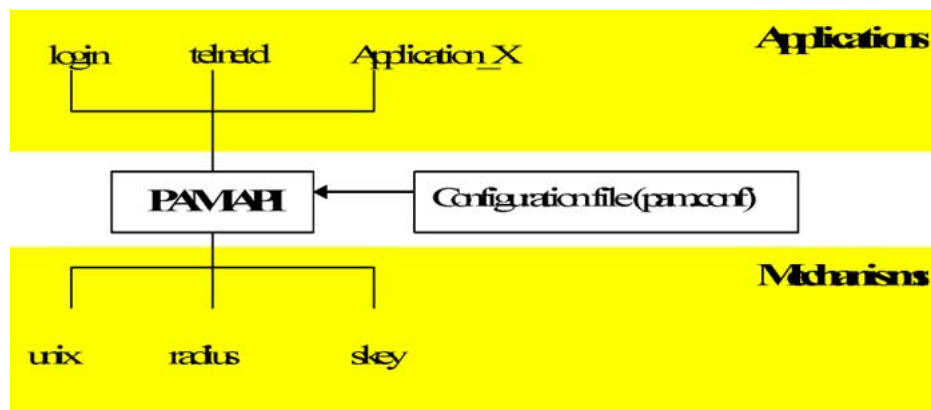
CVoIP solutions' use of PAM provides unified user login interfaces for the following client applications:

- Audio Provisioning Server (APS) Manager
- CS 2000 Management Tools
- Network Patch Manager (NPM)
- Line Maintenance Manager (LMM)
- Trunk Maintenance Manager (TMM)
- CS 2000 SAM21 Manager
- Batch Configuration Monitor
- MG 9000 Manager
- IEMS
- CICM Manager
- USP and USP Manager

PAM addresses the following user access requirements for the Succession Element and Sub-Element Manager (SESM) and the Server Platform Foundation Software (SPFS) platform:

- Authentication - verify user identity. Set the user credentials like user ID and group ID.
- Password control - manage password aging, changes, and control password strength.
- Account control - check if the user account is active according to expiration date, time-of-day, method or origin of access.

- Session management - Open and close sessions. Log information about the current session.



### PAM features

PAM functionality includes the following:

- Provides an abstraction layer so that applications can use numerous security services via PAM modules.
- Has a common API for applications, independent of the operating system, so that applications are not tied to specific security services.
- Has a common SPI (Service Provider Interface) for interfacing to security services.
- The system administrator, not the application, decides on the user authentication mechanism on a per application basis. Thus, changes in the security policy have no impact on the applications.
- For CMT applications the user can be authenticated once with all authentication protocols without retyping the password (excludes Trunk Maintenance Manager (TMM), Batch Provisioning Tool, and MG 9000 Manager)
- Provides a unified login in the presence of different mechanisms. Otherwise, the user often is expected to know about the authentication command of the new authentication module (for example, `kinit`, `dce_login`) after logging into the system, which is not user-friendly.

### System Administration Advantages

PAM provides system administrators with the flexibility to do the following:

- Choose any authentication service available on a system to perform end-user authentication for an application.
- Manage user accounts centrally.



- Add new authentication service modules to a system and make them available without having to modify any applications.
- Incorporate mapping services to map user names and authentication tokens between different authentication domains.

## CICM element manager interface with PAM

---

### Overview

Carrier Voice over IP (CVoIP) user authentication services can use a single centralized third party server which provides authentication services to CVoIP management systems via a pluggable authentication module (PAM) on the IEMS platform.

From (I)SN07 onwards, the CICM element manager is integrated into the CVoIP centralized user authentication strategy. The CICM element manager interfaces to PAM via the HTTPS PAM+ proxy on IEMS.

Prior to (I)SN07, the user name and password supplied when logging into the element manager corresponded to local user accounts on the CICM element manager. From (I)SN07 onwards, the user name and password can be configured to be a global CVoIP account managed on a centralized authentication database which interfaces to CVoIP management tools via the PAM+ proxy located on the IEMS.

Centralized user authentication via the SPFS PAM proxy is not available to TDM deployments of CICM or if connectivity is lost between the CICM element manager and the SPFS platform.

- For TDM deployments, the authentication functionality passes control of the authentication back to the standard mechanism used for CICM.
- For CVoIP deployments, a method of local user authentication is also provided for use when connectivity is lost to the IEMS platform. Users can select local authentication by prefixing their user name with a period (.). This allows users to access their local user account in the CICM element manager when the PAM proxy is out of service.

For more information on CICM integration with PAM+ proxy, see CICM Configuration Management, NN10240-511.

## Security Tools and Utilities

This section lists Carrier VoIP network management components and available security applications.

### Login Security

| Management Component                                  | Login Security                                                                                                                        |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| APS GUI                                               | PAM                                                                                                                                   |
| Nortel VPN Router 600 formerly known as Contivity 600 | Local database                                                                                                                        |
| CS 2000 Core Manager                                  | Local database                                                                                                                        |
| <b>CS 2000 Management Components (CS2M)</b>           |                                                                                                                                       |
| • APS Manager                                         | PAM                                                                                                                                   |
| • CS 2000 SAM21 Manager                               | PAM                                                                                                                                   |
| • GWC Manager                                         | PAM                                                                                                                                   |
| • Lines/Trunks/Nodes Provisioning                     | PAM                                                                                                                                   |
| • LMM GUI                                             | PAM                                                                                                                                   |
| • Lines Configuration (Servord+)                      | PAM                                                                                                                                   |
| • NPM                                                 | PAM                                                                                                                                   |
| • TMM GUI                                             | PAM                                                                                                                                   |
| • UAS Manager                                         | PAM                                                                                                                                   |
| • MS 2000 Series Configuration Tool                   | PAM                                                                                                                                   |
| • MG 9000 Manager                                     | PAM                                                                                                                                   |
| <b>CS 2000 Management Tools Platform Access</b>       |                                                                                                                                       |
| • Telnet                                              | PAM                                                                                                                                   |
| • FTP Server                                          | SSH PAM<br>FTP does not use PAM directly, but if a user is not found in the ProFTP user database, it authenticates the user with PAM. |
| Media Gateway 7480                                    | Local database                                                                                                                        |
| Media Gateway 15000                                   | Local database                                                                                                                        |
| Ethernet Routing Switch 8600 Device Manager           | Local database                                                                                                                        |
| - Device Manager: Local database                      |                                                                                                                                       |
| - Platform access: RADIUS or local database           |                                                                                                                                       |
| MDM                                                   | PAM                                                                                                                                   |
| IEMS                                                  | PAM                                                                                                                                   |
| <b>USP Manager</b>                                    |                                                                                                                                       |

| Management Component                                                                                                                                   | Login Security                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• USP Manager GUI</li><li>• Citrix</li></ul>                                                                     | <ul style="list-style-type: none"><li>PAM</li><li>Local database</li></ul>                                                                                  |
| <b>XA Core Manager (SDM platform)</b>                                                                                                                  |                                                                                                                                                             |
| <ul style="list-style-type: none"><li>• FTP Server</li><li>• SFTP</li><li>• SBA</li><li>• ETA/ATA</li><li>• SFT01</li><li>• SFT2 (SSH-based)</li></ul> | <ul style="list-style-type: none"><li>Local database</li><li>Local database</li><li>Local database</li><li>DCE</li><li>DCE</li><li>Local database</li></ul> |

---

## Centralized security administration overview

---

IEMS provides centralized administration, authentication, authorization, and security logging for most components in the solution.

IEMS provides a pluggable security architecture based on the Pluggable Authentication Module (PAM) and Name Services Switch (NSS).

This architecture provides the following features:

- central administration of user accounts and user groups
- central authentication. Authentication of centrally administered user accounts is performed by the central security server.
- central authorization. Authorization information needed to support user access control is securely managed and provided by the central security server.
- single sign-on (SSO). This capability enables the user to access multiple network elements, applications, and features from a single login session. Session information for a user is shared between IEMS and networks elements which support SSO.
- the ability to plug in a third-party authentication or authorization solution
- the ability to generate centralized security logging for successful and failed authentications

The following table lists the devices and applications that support central security administration features.

To configure a device to use centralized security, refer to the documents listed in the following table. You should configure a device to use central security only after the IEMS central security server has been configured and activated in the network.

## Central security administration - supported devices

| Network element/EMS platform                                                                                                             | Device authentication and authorization method | Documentation reference                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| USP                                                                                                                                      | HTTPS                                          | <i>USP Administration and Security</i> , NN10159-611                                                                      |
| Ethernet Routing Switch 8600                                                                                                             | RADIUS                                         | <i>Configuring and Managing Security</i> , 314724-B                                                                       |
| SPFS<br>CS 2000 Management Tools<br>Audio Provisioning Server (APS)<br>Network Patch Manager (NPM)<br>MG 9000 Manager<br>MG9000 Mid-Tier | PAM_RADIUS and<br>NSS_SAML                     | <i>ATM/IP Solution-level Administration and Security</i> , NN10402-600                                                    |
| IEMS                                                                                                                                     | HTTPS                                          | <i>IEMS Administration and Security</i> , NN10336-611                                                                     |
| CICM Manager                                                                                                                             | HTTPS                                          | <i>CICM Configuration</i> , NN10240-511                                                                                   |
| Multiservice Data Manager (toolset)                                                                                                      | PAM_RADIUS<br>NSS_SAML                         | <i>MSS 15000, MG 15000 and MDM in VoIP Networks Administration and Security - Securing Network Elements</i> , NN10180-612 |
| Multiservice Data Manager (Operator Client)                                                                                              | SAML over HTTPS                                | <i>MSS 15000, MG 15000 and MDM in VoIP Networks Administration and Security - Securing Network Elements</i> , NN10180-612 |
| Media Gateway 7480/15000/20000                                                                                                           | RADIUS                                         | <i>MSS 15000, MG 15000 and MDM in VoIP Networks Administration and Security - Securing Network Elements</i> , NN10180-612 |
| Multiservice Switch 15000                                                                                                                | RADIUS                                         | <i>MSS 15000, MG 15000 and MDM in VoIP Networks Administration and Security - Securing Network Elements</i> , NN10180-612 |
| GWC                                                                                                                                      | HTTP                                           | No device-specific configuration needed                                                                                   |

| Network element/EMS platform | Device authentication and authorization method | Documentation reference                                               |
|------------------------------|------------------------------------------------|-----------------------------------------------------------------------|
| MG 9000                      | RADIUS                                         | <i>MG 9000 Administration and Security</i> , NN10162-611              |
| CS 2000 Core Manager (SDM)   | PAM_RADIUS                                     | <i>CS 2000 Core Manager Administration and Security</i> , NN10170-611 |

The following table lists IEMS single sign-on launch points.

#### IEMS single sign-on launch points

| Network element/EMS platform/application | IEMS launch point                           |
|------------------------------------------|---------------------------------------------|
| USP                                      | USP Command Line<br>USP Manager             |
| CS 2000 Management Tools                 | CS 2000 Management Tools                    |
| GWC Manager                              | GWC Manager<br>GWC Manager Network View GUI |
| SAM21 Manager                            | SAM21 Manager                               |
| UAS Manager                              | UAS Manager                                 |
| LMM                                      | LMM                                         |
| TMM                                      | TMM                                         |
| OSSGate                                  | BPT Servlet                                 |
| MG9000 Manager                           | MG9000 Manager                              |
| MG9000 Mid-Tier                          |                                             |
| APS                                      | APS Manager<br>APS Application              |
| NPM                                      | NPM                                         |
| QOS                                      | QOS Command Line                            |
| SPFS                                     | SPFS Command Line (except CBM platform)     |
| SDM platform                             | SDM Command Line                            |

## Authentication and authorization

Network elements and applications can be configured to use centralized security administration. To enable a device to use centralized security administration, the device must be configured to use the IEMS central security server to authenticate users and access user profile information.

IEMS Central Security Server uses PAM to process the authentication requests and NSSwitch to return user privilege and user profile information to network elements and applications.

### **PAM services**

PAM provides authentication services for clients in the managed network. Customers have the option to use the PAM services that come pre-bundled with the security server or to provide their own. For details on configuring PAM, see ["Configuring the IEMS central security server in the network" \(page 460\)](#).

When a request is forwarded to the IEMS PAM Service Provider (SPI), then authentication is performed against data provisioned and administered by the security administration application on the IEMS client.

Conversely, when PAM services are provided by a customer, incoming authentication requests are forwarded to the customer SPI for resolution against their remote database.

### **NSSwitch services**

NSSwitch provides services to obtain group and profile information for users. Centralized access to network resources depends on the definition of a common set of user groups to map security access for each user. The Nortel Networks solution provides a number of predefined user groups to address the full range of OAM&P functions required across a managed network. For details of these user groups and their categorization, see the "User groups" section in ["Setting up local user accounts on an SPFS-Based Server" \(page 338\)](#).

Customers can configure NSSwitch to use the service pre-bundled with IEMS or, as with PAM services, provide their own service remotely. When the pre-bundled service is used, group and user profile information is administered from the IEMS security administration GUI. For details, see ["Configuring a third-party Pluggable Authentication Module" \(page 470\)](#).

If NSSwitch services are configured to use a third party system, it is important to note that this security solution supports only the NSSwitch group and password (including shadow) databases. Although other database types may be defined in NSSwitch, they are not used by the central security feature.

### **Authorization domains**

For the mapping details of IEMS devices to authorization domains, see ["Mapping of IEMS devices to authorization domains" \(page 487\)](#).



## Single sign-on (SSO)

The single sign-on feature allows users transparent access to multiple network elements and applications through a single login. Once a user has been successfully authenticated for the first time (by user login), an SSO token is created by the IEMS security server that will be used to authenticate the same user on subsequent login attempts.

Network elements and applications use a single sign-on (SSO) interface on the central security server to request SSO tokens whenever authentication is required.

Media Gateway 7480/15000/20000, Multiservice Switch 15000, Ethernet Routing Switch 8600 and MDM do not support SSO.

## Ports requirements

The following table lists details of port usage.

| Process                                           | Port Occupied  | Communication    |
|---------------------------------------------------|----------------|------------------|
| Performance (FTP or SFTP push)                    | Std.           | TCP (out)        |
| SSH                                               | 22             | TCP (in)         |
| TokenAdmin GUI and HTTPS Pam proxy (non-SSL mode) | 80, 8080       | TCP (in)         |
| Trap Port                                         | 162 (default)  | UDP (in and out) |
| TokenAdmin GUI and HTTPS Pam proxy (SSL mode)     | 443, 8443      | TCP (in)         |
| Syslog client                                     | 514            | UDP (out)        |
| LDAPS                                             | 636            | TCP (in)         |
| RADIUS server                                     | 1812           | UDP (in and out) |
| SNMP Agent Port                                   | 8001 (default) | UDP (in)         |
| Java Client Server Communication                  | 9004, 9005     | TCP (in)         |
| NT STD Export                                     | 8555           | TCP (in)         |
| SCC2-Export Port                                  | 8556           | TCP (in)         |
| IEMS Server Web Server                            | 9090 (default) | HTTP (in)        |
| IEMS Server Web Server                            | 9091 (default) | HTTPS (in)       |
| IEMS Tomcat                                       | 18005, 18009   | TCP (in)         |
| SunONE IS (SSL mode)                              | 58081          | TCP (in)         |

## Limitations and restrictions

The following are limitations and restrictions:

- the maximum number of provisionable central security users is 1000
- third party pluggability is supported for SunONE directory server 5.1 for LDAP
- for third party pluggability, the only pam.conf edits and the only nns witch.conf edits that are supported are ldap. For details of pam\_ldap edits, see ["Configuring a third-party Pluggable Authentication Module" \(page 470\)](#).
- password aging notification is not supported by the following:
  - CICM Manager
  - USP
  - Ethernet Routing Switch 8600
  - Media Gateway 7480/15000/20000
  - Multiservice Switch 15000
  - GWC
  - MG 9000
- Central authentication for FTP is not supported as there is no local caching of user data on the local machine after authentication with a remote server.
- Centrex IP Client Manager (CICM) Element Manager only supports central authentication. CICM Manager does not support single sign-on (SSO).
- The procedure for deleting a user's central account must be followed. If the procedure for disabling or deleting a user session is not followed correctly
  - the user's home directories may be accessible to a new user who inherits the same user ID as the original user
  - the new user who inherits the same user ID as the original user will not be able to log in to the SPFS security clients
- a certificate must be installed on the IEMS server, before installing IEMS software, to ensure that the system operates correctly
- the total number of groups that a user can belong to cannot exceed sixteen
- a user name is a string of no more than eight bytes consisting of alphabetic characters and numeric characters. The first character

should be alphabetic, and the field should contain at least one lower case alphabetic character.

- a group name consists of characters from the set of lower case alphabetic characters and numeric characters
- IEMS allows you to configure user ID ranges. Sun Solaris security clients such as SPFS use a user ID to uniquely identify a user. The default IEMS user ID range is 10001-12000. You can change the IEMS user ID. You must ensure that there is no conflict between the new IEMS user ID range and the Sun Solaris system user ID range in /etc/passwd. Such a conflict may severely impact system operation. The following table lists Sun Solaris system accounts and user IDs.

| Sun Solaris system accounts and user IDs                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| root:0, daemon:1, bin:2, sys:3, adm:4, lp:71, uucp:5, nuucp:9, listen:37, nobody:60001, noaccess:60002, nobody4:65534, sshd:100, maint:101, npm:102, npmftp:103, ptm:104, mgems:105, www:106, patcher:107, poller:108, certuser:109, sam21em:110, anonymous:111, image:112, pfrs:113, ntssg:50015, FIELD:50016, oracle:50017, patch:50018 |

- Media Gateway 7480/15000/20000, Multiservice Switch 15000, and MDM do not support SSO.
- User accounts provisioned in the Central Security Administration system:
  - must not have the same numerical user ID or user name as user accounts provisioned in local Unix files on the IEMS server. If a conflict exists where a central user account has the same user name or numerical user ID as a local IEMS server account, then login with the central account may fail on some devices.
  - can not have the same numerical group ID or group name as user groups provisioned in local Unix files on the IEMS Server. If a conflict exists where a central user group has the same group name or numerical group ID as a local IEMS group, then login involving the central user group may fail on some devices.
  - For the reasons explained above, user/group names or numerical IDs among different security database systems should not have duplicate entries. The Carrier VoIP groups listed in the "[Secondary user groups](#)" (page 340) table are pre-defined by the IEMS Security Administration system and are an exception to this rule. The Carrier VoIP groups exist in both the IEMS server local Unix files and the Central Security Administrations system.
- When configuring /etc/nsswitch.conf for use with third party security modules, the saml nsswitch entry must always appear before the files

entry in the nsswitch stack. The following is an example of the password and group database entries:

**Example**

passwd: ldap saml files

group: ldap saml files

## Centralized user access management using IEMS

In VoIP solutions, IEMS maintains a single set of userids for access to all the Multiservice Data Manager workstations, Multiservice Switch 15000 switches and Media Gateway 15000 switches in the associated regional office. This centralization promotes ease of managing the userids across multiple switches and workstations, and reduces the time to make necessary changes.

### IEMS user access management

IEMS provides detailed access authorization by setting the scope for the operations assigned to a group. This scope defines the restricted access for the operation in that group. IEMS procedures provide for:

- configuring user settings
- configuring scope and group settings

For details on using IEMS to manage user access, refer to *NN10336-611 IEMS Security and Administration*.

### Local access requirements

Some MDM userids and groups must be maintained locally on the MDM Server. Local userids are used to access MDM functionality if the connection to the IEMS is not available. MDP tools can only be accessed using local userids. and lists the userids and groups that remain as local userids and groups after the migration of userids to the IEMS. Other userids may be maintained locally as required.

When changing the password for a locally defined MDM userid, use the command: `passwd -r files <userid>`. Otherwise, the password change request is sent to IEMS.

### MDM local userids

|                                                                                        |                                                |
|----------------------------------------------------------------------------------------|------------------------------------------------|
| root:Super-User                                                                        | noaccess:No Access User                        |
| daemon:x:1:1::/:                                                                       | wpms:Workstation Performance Monitoring System |
| bin:x:2:2::/usr/bin:                                                                   | Nortel:nortel from NNswmgmt                    |
| sys:x:3:3::/:                                                                          | sshd:sshd privsep                              |
| <b>Note:</b> For <mdpadmin>, use the MDP administrator userid set during installation. |                                                |

|                                                                                        |                           |
|----------------------------------------------------------------------------------------|---------------------------|
| adm::Admin                                                                             | <mdpadmin>:mdp administor |
| nobody:Nobody                                                                          |                           |
| <b>Note:</b> For <mdpadmin>, use the MDP administrator userid set during installation. |                           |

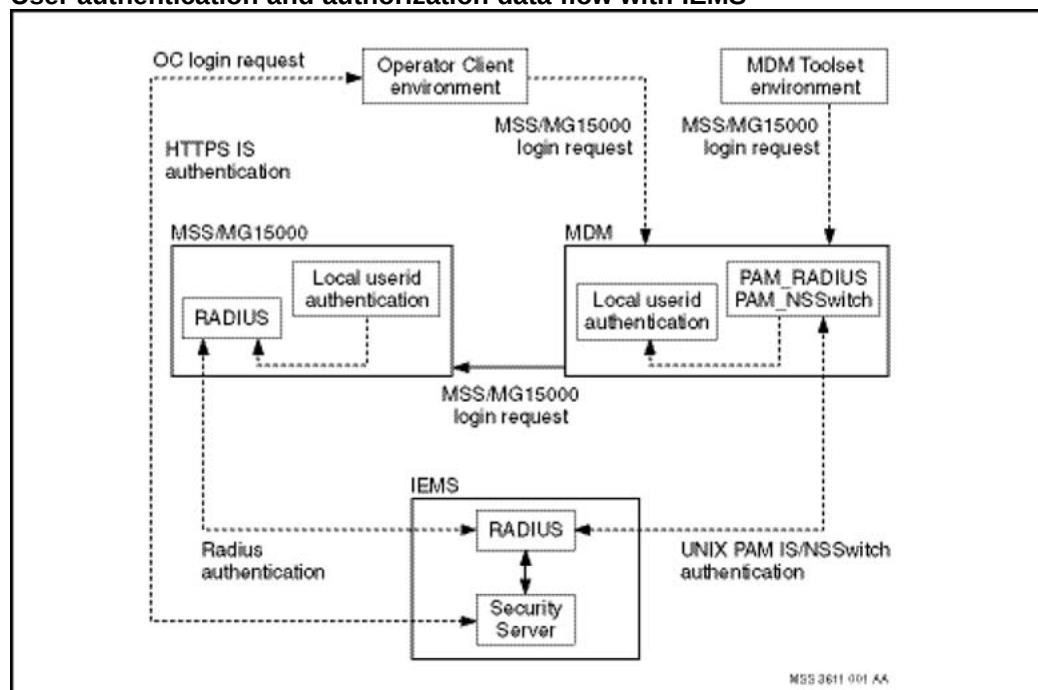
**MDM local groups**

|                                                                                        |       |          |            |
|----------------------------------------------------------------------------------------|-------|----------|------------|
| root                                                                                   | adm   | staff    | noaccess   |
| other                                                                                  | uucp  | daemon   | nogroup    |
| bin                                                                                    | tty   | sysadmin | nortel     |
| sys                                                                                    | nuucp | nobody   | <mdpgroup> |
| <b>Note:</b> For <mdpagroup>, use the MDP administrator group set during installation. |       |          |            |

Some MSS/MG15000 userids must also be maintained as local userids. In case that the connection to IEMS is unavailable, userids for GMDR and PMSP access are required, as well as a local userid with an impact of debug.

**Authentication data flow using IEMS central AAA service**

"User authentication and authorization data flow with Integrated EMS" (page 299) shows the data flow for user authentication and authorization in VoIP solutions using IEMS central AAA service.

**User authentication and authorization data flow with IEMS****MDM Toolset environment**

The MDM sends an MDM Toolset login message via the PAM\_RADIUS interface to the IEMS security server for authentication. When the IEMS security server authenticates a valid userid, it returns information on the authorization level associated with the userid to the MDM. The MDM uses the PAM\_NSSwitch interface to determine the associated user information for the MDM system, such as valid groups, shell, and other UNIX information. If the userid is not found on the IEMS system, then MDM local user authentication is invoked.

**Operator Client environment**

Once the Operator Client application on the desktop is launched, a login window appears. If IEMS has a security certificate configured, the certificate window appears before the login information can be entered. The login information is sent from the desktop to the IEMS security server where the userid/password is authenticated. If the userid is valid, the associated group information is returned to the Operator Client application where the authorized tools are activated.

**MSS/MG15000**

MSS/MG15000 login requests are sent to the node where they are first compared with the local users. If the userid is not found locally, it is sent via a RADIUS client interface to the IEMS system. When the IEMS security server authenticates the userid, it sends the group's

authorization information back to the MSS using the RADIUS interface. The MSS/MG15000 switch maps this information onto the associated access control components (scope, impact, etc).

## IEMS user group mappings

The IEMS user groups and the mapping of the MDM and MSS/MG15000 access privileges onto these groups are shown in [Appendix "Mapping of Multiservice Data Manager, Multiservice Switch 15000 and Media Gateway 15000 access privi"](#) (page 675).

For more information on administering IEMS groups, see *NN10336-611 IEMS Security and Administration*.

## Administration procedures for IEMS central AAA service

The following administration procedures are used on the MDM Server and MSS/MG15000 switches:

- ["Updating the MDM Server when the Integrated EMS amadmin password changes"](#) (page 300)
- ["Updating the MDM Server when the Integrated EMS RADIUS shared secret changes"](#) (page 301)
- ["Updating the MSS/MG15000 switch when the Integrated EMS RADIUS shared secret changes"](#) (page 301)

### Updating the MDM Server when the IEMS amadmin password changes

If the password for the IEMS userid *amadmin* changes, the PAM\_NSSwitch software on the MDM Server must be updated with the new password.

**Note:** Make sure that the new password for the IEMS *amadmin* userid is distributed to the MDMServer site using a secure method.

### Procedure steps

| Step | Action                                                                                                                                                  |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Log in to the MDM Server as root.                                                                                                                       |
| 2    | Execute the following commands: <pre>cd /opt/nortel/applications/security/current_nssaml/sw mgmt/bin ./configure_nssaml.sh -subcomponent password</pre> |
| 3    | At the prompt, enter the new IEMS <i>amadmin</i> password.<br><br>The following shows a sample output for the <code>configure_nssaml.sh</code> command: |



```
Note: Configuring component nssaml
Note: Configuring password subcomponent
Enter the password: <IEMS_admadmin_password>
```

---

—End—

---

### Variable definitions

| Variable           | Definition                                              |
|--------------------|---------------------------------------------------------|
| <IEMS_amadmin_pwd> | is the new password for the IEMS <i>amadmin</i> userid. |

### Updating the MDM Server when the IEMS RADIUS shared secret changes

If the IEMS RADIUS shared secret changes, the PAM\_RADIUS software on the MDM Server must be updated with the new RADIUS shared secret.

**Note:** Make sure that the new RADIUS shared secret is distributed to the MDM Server site using a secure method.

### Procedure steps

| Step  | Action                                                                                                                                                              |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | Log in to the MDM Server as root.                                                                                                                                   |
| 2     | Execute the following commands:<br><br><pre>cd /opt/nortel/applications/security/current_pamradclt /swmgmt/bin ./configure_pamradclt.sh -subcomponent servers</pre> |
| 3     | Enter the IEMS RADIUS shared secret as prompted.                                                                                                                    |
| —End— |                                                                                                                                                                     |

### Updating the MSS/MG15000 switch when the IEMS RADIUS shared secret changes

If the IEMS RADIUS shared secret changes, the RADIUS client software on the MSS/MG15000 switch must be updated with the new RADIUS shared secret.

**Note:** Make sure that the new RADIUS shared secret is distributed using a secure method.

### Procedure steps

| Step  | Action                                                                                                         |
|-------|----------------------------------------------------------------------------------------------------------------|
| 1     | Log in to the MSS/MG15000 switch as system administrator.                                                      |
| 2     | Enter provisioning mode:<br><code>start prov</code>                                                            |
| 3     | Obtain the provisioning file:<br><code>copy prov</code>                                                        |
| 4     | Change the RADIUS shared secret:<br><code>set Ac Radius Server/0 sharedSecret &lt;new_shared_secret&gt;</code> |
| 5     | Verify the provisioning change:<br><code>check prov</code>                                                     |
| 6     | Save the provisioning change:<br><code>save prov</code>                                                        |
| 7     | Activate the provisioning change:<br><code>activate prov</code>                                                |
| 8     | Confirm the provisioning change:<br><code>confirm prov</code>                                                  |
| 9     | Commit the provisioning change:<br><code>commit prov</code>                                                    |
| 10    | Exit provisioning mode after the commit is complete:<br><code>end prov</code>                                  |
| —End— |                                                                                                                |

### Variable definitions

| Variable            | Definition                            |
|---------------------|---------------------------------------|
| <new_shared_secret> | is the new IEMS Radius shared secret. |

## Updating the MDM Server when the IEMS IP address changes

If the IEMS IP address changes, the PAM\_RADIUS software on the MDM Server must be updated with the new IP address.

### Procedure steps

| Step  | Action                                                                                                                                                              |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | Log in to the MDM Server as root.                                                                                                                                   |
| 2     | Execute the following commands:<br><br><pre>cd /opt/nortel/applications/security/current_pamradclt /swmgmt/bin ./configure_pamradclt.sh -subcomponent clients</pre> |
| 3     | Enter the IEMS IP address as prompted.                                                                                                                              |
| —End— |                                                                                                                                                                     |

## Updating the MSS/MG15000 switch when the IEMS IP address changes

If the IEMS IP address changes, the RADIUS client software on the MSS/MG15000 switch must be updated with the new IP address.

### Procedure steps

| Step | Action                                                                                                         |
|------|----------------------------------------------------------------------------------------------------------------|
| 1    | Log in to the MSS/MG15000 switch as system administrator.                                                      |
| 2    | Enter provisioning mode:<br><br><pre>start prov</pre>                                                          |
| 3    | Obtain the provisioning file:<br><br><pre>copy prov</pre>                                                      |
| 4    | Change the I EMS IP address:<br><br><pre>set Ac Radius Server/0 serverIpAddress &lt;new_IEMS_IPad dr&gt;</pre> |
| 5    | Verify the provisioning change:<br><br><pre>check prov</pre>                                                   |
| 6    | Save the provisioning change:<br><br><pre>sav prov</pre>                                                       |

- 7      Activate the provisioning change:  
          `activate prov`
- 8      Confirm the provisioning change:  
          `confirm prov`
- 9      Commit the provisioning change:  
          `commit prov`
- 10     Exit provisioning mode after the commit is complete:  
          `end prov`

---

—End—

---

### Variable definitions

| Variable          | Definition                  |
|-------------------|-----------------------------|
| <new_IEMS_IPAddr> | is the new IEMS IP address. |

### Updating JWS software when the MDM Server host name changes

If the host name of the MDM Server changes, the JWS software must be configured to launch to the new host name.

#### Procedure steps

| Step | Action                                                                                                                                                                                                            |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Log in to the MDM Server as root.                                                                                                                                                                                 |
| 2    | Edit the configuration file:<br><pre>vi /opt/nortel/config/applications/desktop/jws/mft/resources/desktop/DesktopGUI.jnlp</pre> Change the host name references to the new host name.<br>Save and close the file. |

---

—End—

---

### Updating the MDM Server when the IEMS host name changes

If the IEMS host name changes, the MDM Server must be updated with the new host name.

---

**Procedure steps**

| Step                     | Action                                                                                                                                          |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 1                        | Log in to the MDM Server as root.                                                                                                               |
| 2                        | Execute the following commands:<br><pre>cd /opt/nortel/applications/security/current_isclient<br/>/swmgmt/bin<br/>./configure_isclient.sh</pre> |
| 3                        | Enter the IEMS host name as prompted.                                                                                                           |
| <hr/> <b>—End—</b> <hr/> |                                                                                                                                                 |

## IEMS secure launch to Ethernet Routing Switch 8600 overview

---

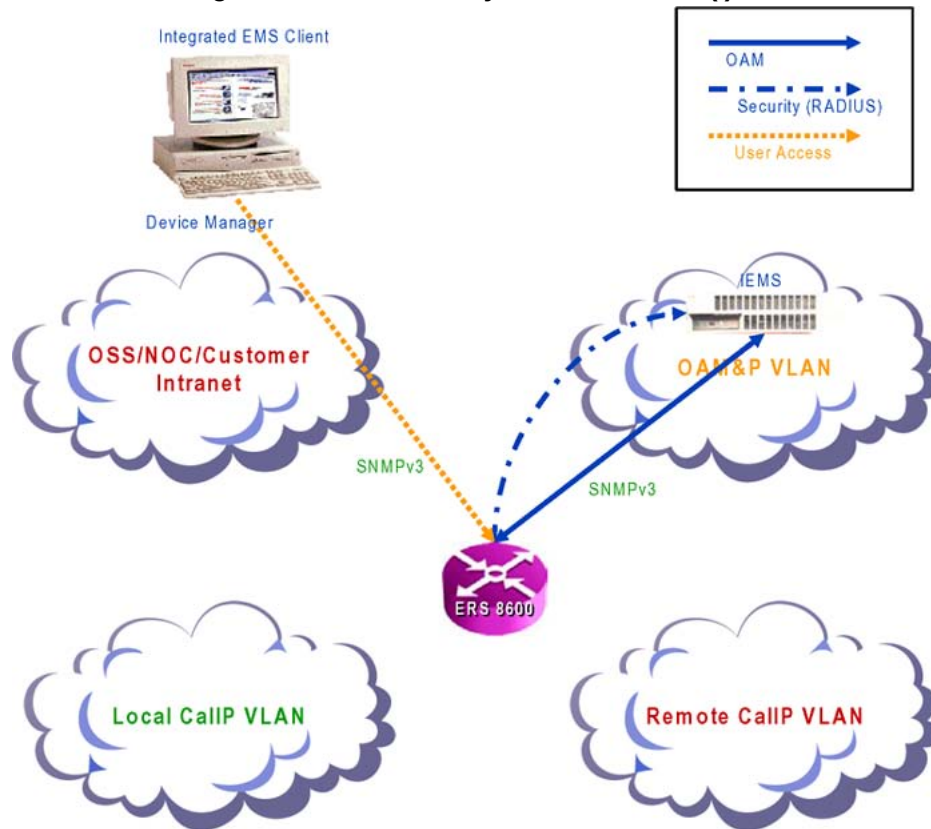
From (I)SN08 enhances security measures for communications between management applications and the Ethernet Routing Switch 8600. The management applications include IEMS and Device Manager. All communications between OAM applications and the Ethernet Routing Switch 8600 must be authenticated and encrypted. Authentication and encryption is provided by SNMPv3 and SSHv2. The following security measures are introduced:

- SNMPv3/USM secures all OAM interfaces between the Ethernet Routing Switch 8600, Device Manager, and IEMS
- SNMPv3/USM supports AuthPriv mode
- IEMS uses Device Manager in secure SNMP mode for installation, configuration, and launching procedures
- new engineering rules apply to open and closed ports on the Ethernet Routing Switch 8600

Configuration is required for Ethernet Routing Switch 8600, IEMS, and Device Manager. Configuration on the Ethernet Routing Switch 8600 must be completed before the configuration of IEMS and Device Manager. For details of configuration procedures, see *IEMS Configuration Management*, NN10330-511.

For an illustration of the security architecture for the Ethernet Routing Switch 8600, see the following figure.

**Figure 2**  
**Ethernet Routing Switch 8600 security architecture for (I)SN08**



## Routine maintenance for CVoIP components

---

This section provides a list of procedures used to perform routine maintenance for CVoIP components. Routine maintenance is required on components to ensure the components continue normal operation over time. The procedures are divided into the following categories:

- "Tasks to be performed after four or eight hours" (page 309)
- "Tasks to be performed daily" (page 309)
- "Tasks to be performed after twenty-five hours" (page 309)
- "Tasks to be performed weekly" (page 309)
- "Tasks to be performed monthly" (page 309)
- "Tasks to be performed every six weeks" (page 311)
- "Tasks to be performed every three to six months" (page 311)
- "Tasks to be performed every six months" (page 312)
- "Tasks to be performed annually" (page 312)



- "Tasks to be performed per office schedule" (page 312)

#### Tasks to be performed after four or eight hours

| Component            | Task                 | Document                                                   | Notes                                                                      |
|----------------------|----------------------|------------------------------------------------------------|----------------------------------------------------------------------------|
| CS 2000 Core Manager | Clean the DAT drive  | <i>CS 2000 Core Manager Fault Management</i> , NN10082-911 | Clean the DAT drive after the first 4 hours of use for each new cartridge. |
| XA-Core/Call Agent   | Clean the tape drive | <i>XA-Core Maintenance Manual</i> , 297-8991-510           | Clean the tape drive after the first 4 hours of operation.                 |

#### Tasks to be performed daily

| Component | Task                           | Document                                         | Notes |
|-----------|--------------------------------|--------------------------------------------------|-------|
| XA-Core   | Check and adjust the TOD clock | <i>XA-Core Maintenance Manual</i> , 297-8891-510 |       |

#### Tasks to be performed after twenty-five hours

| Component            | Task                 | Document                                                   | Notes                                                                                              |
|----------------------|----------------------|------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| CS 2000 Core Manager | Clean the DAT drive  | <i>CS 2000 Core Manager Fault Management</i> , NN10082-911 | Clean the DAT drive after each 25 hours of use for each used cartridge.                            |
| XA-Core              | Clean the tape drive | <i>XA-Core Maintenance Manual</i> , 297-8891-510           | Clean recording heads after 25 hrs of read/ write operation or according to your office standards. |

#### Tasks to be performed weekly

| Component                | Task                                                                           | Document                                                    | Notes                                                                                  |
|--------------------------|--------------------------------------------------------------------------------|-------------------------------------------------------------|----------------------------------------------------------------------------------------|
| CS 2000 Management Tools | Clean the DAT drive on the Netra t1400/240                                     | <i>ATM/IP Solution-level Fault Management</i> , NN10408-900 | Clean the DAT drive every 1 to 8 weeks depending on the number of tapes used each day. |
| USP                      | Set the date and time on the OAM&P workstation and the USP to synchronize them | <i>USP Administration and Security</i> , NN10159-611        |                                                                                        |

#### Tasks to be performed monthly

| Component                | Task                   | Document                                                                                                                                                    | Notes                        |
|--------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| CS 2000 Management Tools | Inspect the air filter | <i>ATM/IP Solution-level Security and Administration</i> , NN10408-900<br><i>Netra t1400/240 Installation and User's Guide</i> . Link to Sun documentation: | Nortel Networks Confidential |

| Component                               | Task                                         | Document                                                                                                                                                                                                                                                                | Notes                                                                                                                                                         |
|-----------------------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GWC                                     | Inspect the SAM21 filter                     | <a href="http://sunsolve.sun.com/data/806/806-0575/pdf/806-0575-10.pdf">http://sunsolve.sun.com/data/806/806-0575/pdf/806-0575-10.pdf</a><br>Go to: <a href="http://mcg.motorola.com">http://mcg.motorola.com</a> and search for the specific CPX822 product documents. | Filters last from 3 to 6 months depending on environmental conditions.                                                                                        |
| Multiservice Switch/Media Gateway 15000 | Inspect and vacuum equipment                 | <i>Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade</i> , NN10600-130                                                                                                                                                    | Vacuuming reduces the frequency that air filters need to be changed. May need to inspect and vacuum more frequently, depending upon environmental conditions. |
| ERS 8600                                | Inspect and clean 8010co Chassis air filter  | <i>Installing and Maintaining the Passport 8010co Chassis and Components</i> , 312746-C                                                                                                                                                                                 | Inspect monthly and replace every three months or more frequently, depending on environmental conditions.                                                     |
| MDM                                     | Inspect the air filter.                      | <i>Netra T1400/1405 Installation and User's Guide</i> . Link to Sun documentation: <a href="http://sunsolve.sun.com/data/806/806-0575/pdf/806-0575-10.pdf">http://sunsolve.sun.com/data/806/806-0575/pdf/806-0575-10.pdf</a>                                            |                                                                                                                                                               |
| UAS                                     | Inspect the SAM21 filter                     | Go to: <a href="http://mcg.motorola.com">http://mcg.motorola.com</a> and search for the specific CPX822 product documents.                                                                                                                                              | Filters last from 3 to 6 months depending on environmental conditions.                                                                                        |
| USP                                     | Inspect and clean the fan filter             | <i>USP Administration and Security</i> , NN10159-611                                                                                                                                                                                                                    | This task may need to be performed more frequently depending on environmental conditions                                                                      |
| USP                                     | Test the LAN-to-LAN remote access connection | <i>USP Administration and Security</i> , NN10159-611                                                                                                                                                                                                                    |                                                                                                                                                               |

| Component          | Task                                      | Document                                             | Notes |
|--------------------|-------------------------------------------|------------------------------------------------------|-------|
| USP                | Test the dial-up remote access connection | <i>USP Administration and Security</i> , NN10159-611 |       |
| XA-Core/Call Agent | Test wrist-strap grounding cords          | <i>XA-Core Maintenance Manual</i> , 297-8991-510     |       |

**Tasks to be performed every six weeks**

| Component          | Task                             | Document                                         | Notes |
|--------------------|----------------------------------|--------------------------------------------------|-------|
| XA-Core/Call Agent | Replace the cooling unit filters | <i>XA-Core Maintenance Manual</i> , 297-8991-510 |       |

**Tasks to be performed every three to six months**

| Component                | Task                                  | Document                                                                                                                                                                                                                     | Notes                                                                                                     |
|--------------------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| GWC                      | Replace the SAM21 filter              | Go to: <a href="http://mcg.motorola.com">http://mcg.motorola.com</a> and search for the specific CPX822 product documents.                                                                                                   | This task may need to be performed more frequently depending on environmental conditions.                 |
| CS 2000 Management Tools | Replace the air filter                | <i>Netra T1400/1405 Installation and User's Guide</i> . Link to Sun documentation: <a href="http://sunsolve.sun.com/data/806/806-0575/pdf/806-0575-10.pdf">http://sunsolve.sun.com/data/806/806-0575/pdf/806-0575-10.pdf</a> | This task may need to be performed more frequently depending on environmental conditions                  |
| UAS                      | Replace the SAM16 air filter          | Go to: <a href="http://mcg.motorola.com">http://mcg.motorola.com</a> and search for the specific CPX822 product documents.                                                                                                   | Filters last from 3 to 6 months depending upon environmental conditions.                                  |
| ERS 8600                 | Replace the 8010co Chassis air filter | <i>Installing and Maintaining the Passport 8010co Chassis and Components</i> , 312746-C                                                                                                                                      | Inspect monthly and replace every three months or more frequently, depending on environmental conditions. |
| MDM                      | Replace the air filter                | <i>Netra T1400/1405 Installation and User's Guide</i> . Link to Sun documentation:                                                                                                                                           | Inspect monthly and replace every three months or more                                                    |

<http://sunsolve.sun.com/data/806/806-0575/pdf/806-0575-10.pdf>

frequently, depending on environmental conditions.

#### Tasks to be performed every six months

| Component          | Task                            | Document                                         | Notes |
|--------------------|---------------------------------|--------------------------------------------------|-------|
| XA-Core/Call Agent | Schedule tape drive maintenance | <i>XA-Core Maintenance Manual</i> , 297-8891-510 |       |

#### Tasks to be performed annually

| Component | Task                                                                              | Document                                             | Notes |
|-----------|-----------------------------------------------------------------------------------|------------------------------------------------------|-------|
| GWC       | Replace the three air filters from the front of the fan sleds on the SAM21 shelf. | <i>GWC Fault Management</i> , NN10202-911            |       |
| USP       | Tighten the screws on the cable connections, power cables, and shelf monitoring   | <i>USP Administration and Security</i> , NN10159-611 |       |

#### Tasks to be performed per office schedule

| Component                               | Task                   | Document                                                                                                             | Notes       |
|-----------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------|-------------|
| Core Billing Manager                    | Clean the DVD drive    | Refer to the documentation for your hardware platform                                                                |             |
| CS 2000 Core Manager                    | Check local access     | no formal procedure required                                                                                         |             |
| CS 2000 Core Manager                    | Check remote access    | no formal procedure required                                                                                         |             |
| Multiservice Switch/Media Gateway 15000 | Replace a cooling unit | <i>Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade</i> , NN10600-130 | as required |

| Component                               | Task                                                                                                                                 | Document                                                                                                             | Notes                                                               |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| Multiservice Switch/Media Gateway 15000 | Replacing an air filter                                                                                                              | <i>Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade</i> , NN10600-130 | as required                                                         |
| MG 9000                                 | Replace an air filter element                                                                                                        | <i>MG 9000 Fault Management</i> , NN10074-911                                                                        | as required                                                         |
| Session Server                          | Clean the DVD-rom drive                                                                                                              | HP Carrier-Grade Server cc3310 Product Guide, HP part number: cc3310_Product                                         | acquire HP guide from HP.com website                                |
| Session Server                          | Monitor the fan exhaust colwings for dust buildup. There are no air filters or fan filters on the Session Server chassis to replace. | no formal procedure required                                                                                         | Refer to your site maintenance guidelines for removing excess dust. |
| Session Server                          | After each upgrade or MR is applied electronically, clean up unused iso images in the /opt/swd directory                             | no formal procedure required                                                                                         |                                                                     |
| XA-Core/Call Agent                      | Returning a card, packlet, or assembly to Nortel                                                                                     | <i>XA-Core Maintenance Manual</i> , 297-8991-510                                                                     |                                                                     |
| XA-Core                                 | Delete a volume on an XA-Core disk                                                                                                   | <i>XA-Core Maintenance Manual</i> , 297-8991-510                                                                     |                                                                     |

## CS 2000 Management Tools security and administration

---

### Overview

Security on the CS 2000 Management Tools server is achieved using Pluggable Authentication Module (PAM). PAM is a Unix programming interface that has the ability to integrate with different authentication mechanisms such as Distributed Computing Environment (DCE).

The default authentication mechanism for the CS 2000 Management Tools server is Unix. However, if desired, the authentication mechanism can be changed from Unix to DCE. If required, refer to procedure ["Changing the authentication mechanism between UNIX and DCE"](#) (page 507).

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and SAM21 Element Manager) are able to communicate with their respective server-side application through multiple firewalls facing either the client or the server side, using a minimum number of configurable TCP/IP ports. Communication through multiple firewalls is achieved using a Socks proxy, which is started when the server is started.

The Trunk Maintenance Manager (TMM) and Batch Configuration Monitor do not use a Socks proxy.

The server-side Socks port has a default value of 10080, and the client-side Socks port has a default value of 10090. If the default value is not acceptable, you can change the default value of the server-side and client-side ports using procedure "Configuring client/server ports on an SPFS-based server for secure firewall communications" in the *ATM/IP Solution-level Configuration Management* document, NN10409-500.

### Centralized security administration

Centralized security administration is provided through the Integrated Element Management System (IEMS). IEMS provides a comprehensive architecture based on PAM and Name Service Switch (NSS). This architecture provides the following features:

- central administration of user accounts
- central authentication and authorization of centrally managed user accounts
- single sign-on (SSO) between the IEMS and applications that support SSO
- third-party authentication and authorization plug-in capability

The IEMS central security server uses PAM to process the authentication requests and NSSwitch to return user privilege and user profile information to the CS 2000 Management Tools applications.

Activating central security administration in the network consists of the following activities:

- configuring and activating the IEMS central security server in the network (refer to procedure ["Configuring the IEMS central security server in the network"](#) (page 460))
- configuring a central security client, which refers to all the SPFS-based servers that host the OAM&P applications (refer to procedure ["Configuring an SPFS-based central security client"](#) (page 463))

To configure the single sign-on (SSO) token time-out values, which are the time the Single Sign-On (SSO) token can remain idle before it becomes invalid, and the time the SSO token id can be used before it expires, refer to procedure ["Configuring the Single Sign-On token"](#) (page 483).

### **Client Session Monitor**

The Client Session Monitor (CSM) allows the viewing of reports that display the currently active client application sessions for each user. In (I)SN09, CSM tracks MG9000 element manager and CS 2000 client starts and stops. The GUIs for the following CS 2000 clients are tracked using CSM:

- CS 2000 Management Tools Server
- Network Patch Manager (NPM)
- Line Maintenance Manager (LMM)
- Gateway Control Manager (GWC Manager)
- SAM21 Manager

CSM also provides the ability to view reports containing historical data regarding client application usage by user, date, or device. Using this data, clients can retrieve the details concerning the last time a given user successfully authenticated against the system using a password.

The information in these reports are automatically refreshed every minute unless the viewer wishes to customize the refresh rate.

### **User accounts**

As of the (I)SN07 release, you can centrally manage the user accounts on the CS 2000 Management Tools server, through the Integrated Element Management System (IEMS) central security server, or you can continue to locally manage the user accounts.

If you opt to centrally manage the user accounts, the following procedures must be completed:

The steps to migrate existing user accounts that are to be centrally managed, are included in the procedures.

- ["Configuring the IEMS central security server in the network" \(page 460\)](#)
- ["Configuring an SPFS-based central security client" \(page 463\)](#)

Users of Nortel OAM&P client applications must belong to the primary group "succssn" for login access, and to one or more secondary user groups to specify the operations the user is authorized to perform. A list of secondary user groups is provided in procedure [Setting up local user accounts on an SPFS-based server](#).

To add new users to the IEMS central security server, refer to the *IEMS Security and Administration document*, NN10336-611.

### **Password aging**

Password aging for local user accounts applies to all user accounts, including the root user account. A password is valid for eight weeks, and the user receives a warning at login two weeks before the password expires. In the event the root password fails with su: Sorry, use procedure ["Changing a user password on an SPFS-based server" \(page 362\)](#).

Password aging for centrally managed user accounts, is configurable. Refer to procedure, "Setting a user profile" in the *IEMS Security and Administration document* IEMS Security and Administration document, NN10336-611.

### **Client login sessions**

For security purposes, login session timeouts are provisioned for the following GUI and CLUI client applications:

- CS 2000 Management Tools GUI
- Network Patch Manager GUI and CLUI
- Line Maintenance Manager GUI
- Gateway Controller Manager GUI
- SAM21 Manager GUI
- Trunk Maintenance Manager GUI
- Batch Configuration Monitor GUI
- OSSGate CLUI
- Batch Provisioning Tool CLUI
- Audio Media Server CLUI



The login session timeouts that are provisioned are as follows:

- user inactivity timeout, which specifies the amount of time a client session can be inactive before the user is required to log in again
- user termination timeout, which specifies the amount of time a user has to log in again before the user is forced to exit the client session

Both timeouts have a default value of 10 minutes, which you can modify using procedure ["Modifying login session timeouts on an SPFS-based server "](#) (page 515).

## Backup and restore

You can back up file systems and oracle data on a Server Platform Foundation Software (SPFS)-based server using a Digital Audio Tape (DAT) for Sun Netra t1400-type servers, or a CD or DVD for Sun Netra 240-type servers.

A full system backup on the SPFS-based server that hosts the CS 2000 Management Tools involves backing up the following information:

- oracle data
- file systems
- APS audio files when APS is present

It is highly recommended you perform a full system backup before and after you upgrade the SPFS and application software on the SPFS-based server. The relevant procedures are as follows:

- ["Performing a backup of oracle data on an SSPFS-based server"](#) (page 135).
- ["Performing a backup of file systems on an SPFS-based server"](#) (page 140).
- ["Performing a backup of APS audio files to tape"](#) (page 545) for Sun Netra t1400-type servers, or ["Performing a backup of APS audio files to CD or DVD"](#) (page 547) for Sun Netra 240-type servers.

You can also schedule a full system backup that overwrites a previous one on a backup media or copy the last successful Oracle backup to a DVD or tape when performing an automated data backup on a Server Platform Foundation Software (SPFS)-based server. This functionality is designed for use in 'dark office' conditions where you need to copy backup data more than once before the backup media, DVD or tape, is ejected from the server.

The relevant procedure to perform a restore from backup media are as follows:

- ["Performing a full system restore on an SPFS-based server"](#) (page 262).

- "Restoring the oracle data on an SPFS-based server" (page 254).
- Performing a restore of APS audio files from tape for Sun Netra t1400-type servers, or Performing a restore of APS audio files from CD for Sun Netra 240-type servers.

### File system backup

Applications and the system have several sets of configuration files with static information about the system configuration and operating parameters. This information is backed up in-service using standard Unix commands and a Solaris utility called SNAPFS which takes a snapshot of the file system.

The file system layout on SPFS-based servers is as follows:

| File system       | Types of information stored in file system                                                                                   |
|-------------------|------------------------------------------------------------------------------------------------------------------------------|
| /                 | operating system software and administrations                                                                                |
| /var              | operating system software and administrations                                                                                |
| /data             | application data in flat files                                                                                               |
| /opt              | third-party software as Platform common services                                                                             |
| /opt/nortel       | Nortel applications                                                                                                          |
| /data/oradata     | Oracle data files (applies to SPFS-based servers that host the CS 2000 Management Tools, APS, and IEMS)                      |
| /data/qca         | QoS Collector Application (QCA) data (applies to SPFS-based servers that host the CS 2000 Management Tools)                  |
| /data/mg9kem/logs | MG 9000 Manager logs (applies to SPFS-based servers that host the MG 9000 Manager)                                           |
| /PROV_data        | audio transaction files before they are sent to the UAS (applies to SPFS-based servers that host the APS)                    |
| /user_audio files | audio uploaded from the user desktop prior to its import into the database (applies to SPFS-based servers that host the APS) |
| /audio_files      | audio data that has been imported into the database (applies to SPFS-based servers that host the APS)                        |

File systems "/", "/var", "/data", "/opt", and "/opt/nortel" are present on every SPFS-based server. The other file systems vary according to the applications installed on the server.

### Oracle data backup

The application data in the Oracle database is not automatically backed up. You can enable automated Oracle data backups, where the system backs up all application data in the Oracle database on a daily basis at a specified time to a DAT, CD or DVD.

To view or change the current configuration settings for automated backup of Oracle data, refer to procedure Configuring automated data backups on an SSPFS-based server.

Data on a CD or DVD cannot be overwritten, therefore, you must insert a blank CD or DVD into the drive prior to the next scheduled backup.

If you leave the same DAT in the drive, the contents of the DAT will be replaced with the new backup data when the backup is scheduled to run. If you want to preserve the daily backup of your application data, remove the DAT from the drive and insert a new one prior to the next scheduled backup. It is recommended that you label the DAT with the date, time and content (oracle data backup).

#### **ATTENTION**

In order to maintain network functionality, the CS 2000 Management Tools persistent data in the Oracle database and the associated CORE/CM tables must match at all times. Therefore, it is recommended that the CS 2000 Management Tools support person modify the automated oracle data backup schedule to run in parallel to the CORE Image Dump schedule. This will ensure that there are always CORE Images and CS 2000 Management Tools database backups that are 100% identical in configuration information.

### **Centralized backups**

The Backup Restore Manager provides centralized control of backup capabilities for the following core components of the Communication Server 2000:

- XA-core
- CS 2000 Management Tools
- MG 9000 Manager
- Integrated Element Management System (IEMS)
- Core Billing Manager (CBM)

The Backup Restore Manager consists of the Synchronous Backup Restore Manager (SBRM) software that resides on the IEMS server, and the Device Backup Restore Manager (DBRM) software that resides on the components. The SBRM software controls and synchronizes backup-related activities across the components through the DBRM software on the components.

The DBRM software on the CBM is only present to enable backups on the XA-core or third-party core. Data on the CBM itself is not backed up through the SBRM.

The SBRM is launched through the IEMS GUI, and enables backups of database tables, configuration files, and property files on the various components. Backup of program store and associated patches is not included in the functionality.

On SPFS-based components, the backup file is placed in directory "/data/bkresmgr/backup". On the XA-core or third-party core, the location of the backup file is configurable.

Restore of the backup image is not supported. To perform a restore from the backup image, refer to procedure [Restoring the oracle data on an SPFS-based server](#).

Prior to using the SBRM, the secure shell (SSH) must be configured between the IEMS server where the SBRM software is installed, and the components where the DBRM software is installed. If required, refer to procedure ["Configuring SSH between the backup restore manager servers"](#) (page 58).

To configure the SBRM for automated execution of backups, refer to procedure ["Configuring the automated synchronous backup restore manager service"](#) (page 64).

## Security alarms and logs

Security alarms and logs are produced by SPFS under the following conditions:

- SPFS detects that the logging system (Syslog) is no longer writing logs. The resulting alarm provides real-time notification to the multiservice access platform (MSAP) administrator if the MSAP security log fails to record important events. After Syslog resumes writing logs, a log is written to the /var/log/customerlog file.
- any security-affecting parameter is added, modified, or deleted using CLI. These security logs use the SPFS logging API and generate logs employing the same format. Following an attempt to modify a security-affecting parameter, the security log will contain a description of the action, an action identifier, the identity of the user, source address of the user, and the date and time when the action occurred. These logs are stored in the /var/log/securitylog file.
- expiration of certificates, system and local accounts or their passwords, or attempts to add, modify, or delete key material including cryptographic keys, userids, passwords, and SNMP community strings. Key material is any information used to authenticate a user on another machine. Also created by IEMS, these alarms and logs provide a means of preventing tampering with key material.

- CSM processes the notification of authentication and client lifetime events. Besides producing security logs, if CSM can not decrypt the information received to register authentication or client lifetime events, an information log is produced. Since these logs are information-only logs, there are no alarms or OMs associated with them. Both security and information logs are stored in the /var/log/securitylog file.

For details about the specific security alarms and logs produced by each of these conditions, see the *ATM/IP Solution-level Security and Administration* document, NN10402-600.

## Tools and utilities

Security and administration procedures are performed on the SPFS-based server where the CS 2000 Management Tools reside.

## Procedures

The security and administration procedures available for the CS 2000 Management Tools are listed under one of the following categories:

- ["Local user accounts and passwords" \(page 321\)](#)
- ["Centralized security configuration" \(page 322\)](#)
- ["Security" \(page 322\)](#)
- ["Backup and restore" \(page 322\)](#)
- ["Client and server applications" \(page 323\)](#)
- ["Administration" \(page 324\)](#)

### Local user accounts and passwords

The following table lists the procedures available for local user accounts and passwords.

#### Local user accounts and passwords procedures

| Procedure                                                                              |
|----------------------------------------------------------------------------------------|
| <a href="#">"Changing the Oracle user password on an SPFS-based server" (page 336)</a> |
| <a href="#">"Changing the APS Oracle account password" (page 123)</a>                  |
| Setting up local user accounts on an SSPFS-based server                                |
| Changing an expired root password on an SPFS-based server                              |
| Creating local and central restricted shell user accounts on an SPFS-based server      |
| Deleting local user accounts from an SPFS-based server                                 |
| <a href="#">"Changing the Oracle user password on an SPFS-based server" (page 336)</a> |
| <a href="#">"Changing a user password on an SPFS-based server" (page 362)</a>          |

**Procedure**

"Setting the Oracle Listener password on an SSPFS-based server" (page 437)  
 Configuring OSSGate password control

For details about managing user accounts on network components, refer to your Carrier Voice over IP component documentation (see [Technical Publications](#)).

**Centralized security configuration**

The following table lists the procedures available for centralized security configuration.

**Centralized security configuration procedures****Procedure**

"Configuring the IEMS central security server in the network" (page 460)  
 "Configuring an SPFS-based central security client" (page 463)  
 Configuring the security server SunONE component  
 Reverting the client server to its previous configuration  
 "Configuring the Single Sign-On token" (page 483)

**Security**

The following table lists the procedures available for security.

**Security procedures****Procedure**

"Changing the authentication mechanism between UNIX and DCE" (page 507)  
 "Setting secure FTP proxy" (page 512)  
 "Modifying login session timeouts on an SPFS-based server" (page 515)

**Backup and restore**

The following table lists the procedures available for backup and restore.

**Backup and restore procedures****Procedure**

"Configuring Automated Data Backups on an SPFS-Based Server" (page 520)  
 "Performing a backup of oracle data on an SSPFS-based server" (page 135)  
 "Performing a backup of file systems on an SPFS-based server" (page 140)  
 "Performing a backup of APS audio files to tape" (page 545)  
 "Performing a backup of APS audio files to CD or DVD" (page 547)

**Procedure**

"Performing a full system restore on an SPFS-based server" (page 262)  
 "Restoring the oracle data on an SPFS-based server" (page 254)  
 Performing a restore of APS audio files from tape  
 Performing a restore of APS audio files from CD  
 "Cloning the image of one node in a cluster to the other node" (page 528)

**Centralized backup and restore**

The following table lists the procedures available for centralized backup and restore.

**Centralized backup and restore procedures****Procedure**

"Configuring SSH between the backup restore manager servers" (page 58)  
 "Configuring the automated synchronous backup restore manager service" (page 64)  
 "Invoking the synchronous backup restore manager through telnet" (page 73)

**Client and server applications**

The following table lists the procedures available for the client and server applications.

**Client and server applications procedures****Procedure**

Starting the SESM server application  
 "Starting the SAM21 Manager server application" (page 541)  
 "Starting the NPM server application" (page 543)  
 "Starting the APS server application" (page 550)  
 Launching CS 2000 Management Tools and NPM client applications  
 Accessing the Network Patch Manager CLUI  
 "Starting the batch provisioning tool" (page 569)  
 "Connecting to OSSGate" (page 571)  
 "Changing modes within OSSGate" (page 573)  
 Stopping the SESM server application  
 "Stopping the SAM21 Manager server application" (page 576)  
 "Stopping the NPM server application" (page 578)  
 "Stopping the APS server application" (page 580)

**Procedure**

"Connecting to OSSGate" (page 571)  
"Starting and stopping the PM Poller" (page 583)  
"Starting and stopping the QoS Collector Application" (page 590)  
"Starting the OMPUSH server application" (page 601)  
"Stopping the OMPUSH server application" (page 603)  
"Starting or stopping the automated synchronous backup restore manager service" (page 69)  
"Initializing the NPM database" (page 611)

**Administration**

The following table lists the procedures available for administration.

**Administration procedures****Procedure**

"Increasing the size of a file system on an SPFS-based server" (page 628)  
"Verifying disk utilization on an SSPFS-based server" (page 639)  
"Installing or replacing an HTTPS certificate on an SPFS-based server" (page 641)  
"Performing a backup of oracle data on an SPFS-based server " (page 135)  
Clearing the JWS cache on a client workstation



## Changing the password warning threshold on the central security server

### Application

Use this procedure to change the system-wide password warning threshold for user accounts managed by the IEMS Security Server.

The new system-wide password warning threshold takes effect when passwords of existing user accounts are reset or when new user accounts are created.

### Prerequisites

You must have root user privileges to perform this procedure.

### Action

| Step                       | Action                                                                                                                                                                                                  |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>At your workstation</i> |                                                                                                                                                                                                         |
| 1                          | Telnet to the server by typing<br><code>&gt; telnet &lt;server&gt;</code><br>and pressing the Enter key.<br>where<br><b>server</b> is the IP address or host name of the server where IEMS resides      |
| 2                          | When prompted, enter your user ID and password.                                                                                                                                                         |
| 3                          | Change to the root user by typing<br><code>\$ su - root</code><br>and pressing the Enter key.                                                                                                           |
| 4                          | When prompted, enter the root password.                                                                                                                                                                 |
| 5                          | Change to the directory where the global password warning script is located by typing:<br><code>/opt/nortel/applications/security/current_slisext/sw<br/>mgmt/bin</code><br>and pressing the Enter key. |
| 6                          | Run the global password warning script by typing:                                                                                                                                                       |

`./updateGlobalPasswdWarning.sh`

and pressing the Enter key.

- 7 When prompted, enter the number of days you want to set. Press the Enter key.
- 8 You have completed this procedure.

---

**—End—**

---

---

## Changing the amAdmin password

---

### Application

Use this procedure to change the amAdmin password. The amAdmin account is an application account used internally by the IEMS security server components. It is not a user account and thus cannot be used for actual user logins.

**ATTENTION**

Changing the amAdmin password disrupts any existing security sessions and so it is recommended that this procedure is performed as a scheduled event.

**ATTENTION**

Passwords are changed in client machines first and then on the server. This means that changing the password on the client machine will prevent further logins using centrally administered accounts until the password has been changed on the server. As such, it is recommended that passwords on clients running critical applications are changed last. This means that the unavailability of centrally administered accounts will exist for a shorter period of time on these clients.

**ATTENTION**

If you allow passwords of the system accounts listed above to expire, all access to the system using centrally administered accounts will be denied until the passwords are reset. In this case, local emergency accounts must be used to access all applications or devices. It is strongly recommended that the value for the number of days before the password expires is set to zero (never expire).

**ATTENTION**

When you run the `configure_nssaml.sh` script to set the NSSwitch SPI passwords and the `is_passwd.sh` to set the Identity server passwords, you must set the passwords to the same value.

### Prerequisites

None

### Action

Perform the following steps:

- On each remote NSS-SAML client (not located on an IEMS server), starting with the least critical, change the NSSwitchSPI password ([step 1](#) through [step 13](#)).
- On the inactive IEMS security server, change the NSSwitchSPI password ([step 14](#) through [step 19](#)).

- On the active IEMS security server, change the NSSwitchSPI and the Identity Server passwords ([step 20](#) through [step 26](#)).

---

**Step    Action**


---

***At your workstation***

- 1      Telnet to the active remote NSS-SAML client by typing  
          > **telnet <server>**  
          and pressing the Enter key.  
          where  
              **server** is the IP address or host name of the server where the  
              NSS-SAML client resides
  - 2      When prompted, enter your user ID and password.
  - 3      Change to the root user by typing  
          \$ **su - root**  
          and pressing the Enter key.
  - 4      When prompted, enter the root password.
  - 5      Change the NSSwitchSPI password by typing:  
          /opt/nortel/applications/security/current\_nsssaml/swmgmt/bin/configure\_nsssaml.sh  
          -subcomponent password  
          and pressing the Enter key.
  - 6      When prompted, enter the new password.
  - 7      Telnet to the inactive remote NSS-SAML client by typing  
          > **telnet <server>**  
          and pressing the Enter key.  
          where  
              **server** is the IP address or host name of the server where the  
              NSS-SAML client resides
  - 8      When prompted, enter your user ID and password.
  - 9      Change to the root user by typing  
          \$ **su - root**  
          and pressing the Enter key.
  - 10     When prompted, enter the root password.
-

- 11 Change the NSSwitchSPI password by typing:  

```
/opt/nortel/applications/security/current_nsssaml/swmgmt/bin/configure_nsssaml.sh
```

```
-subcomponent password
```

 and pressing the Enter key.
- 12 When prompted, enter the new password.
- 13 Repeat [step 1](#) through [step 12](#) for each remote NSS-SAML client (not located on an IEMS server), starting with the least critical.
- 14 Log in to the inactive IEMS security server as root by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  

```
server
```

 is the IP address or host name of the server where the IEMS security server resides
- 15 When prompted, enter your user ID and password.
- 16 Change to the root user by typing  

```
$ su - root
```

 and pressing the Enter key.
- 17 When prompted, enter the root password.
- 18 Change the NSSwitchSPI password by typing:  

```
/opt/nortel/applications/security/current_nsssaml/swmgmt/bin/configure_nsssaml.sh
```

```
-subcomponent password
```

 and pressing the Enter key.
- 19 When prompted, enter the new password.
- 20 Telnet to the active IEMS security server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  

```
server
```

 is the IP address or host name of the server where the IEMS resides
- 21 When prompted, enter your user ID and password.
- 22 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

**23** When prompted, enter the root password.

**24** Change the NSSwitchSPI password by typing:

```
/opt/nortel/applications/security/current_nsssaml/swmgmt/bin/configure_nsssaml.sh
-subcomponent password
```

and pressing the Enter key.

**25** When prompted, enter the new password.

**26** Change the Identity server password to the same value as the NSSwitch SPI password by entering:

```
/opt/nortel/applications/security/current_isclient/bin/is_passwd.sh -is_passwd write
-exp <n>
```

where

**n** is the number of days after which the password for the amadmin account will expire. It is strongly recommended that the value for the number of days before the password expires is set to zero (never expire).

**27** When prompted, enter the new password.

**28** Enter the new password again.

**29** You have completed this procedure.

---

—End—

---

## Changing the system account passwords on the central security server

### Application

Use this procedure to change passwords and set their expiry status to "never expire" on the following system accounts in a single operation on the IEMS security server:

administrator, ndsadmin, puser, dsameuser, amldapuser, replication manager

The system accounts listed above are application accounts used internally by the IEMS security server components. They are not user accounts and therefore cannot be used for actual user login.

#### ATTENTION

The passwords of the system accounts listed above are not automatically propagated to the second server in a high-availability (two-server) configuration. Therefore, the password and expiry change procedures described in this section must be performed on both servers.

#### ATTENTION

The server automatically restarts if this procedure is performed on the active server and so it is recommended that this procedure is performed as a scheduled event.

#### ATTENTION

If you allow passwords of the system accounts listed above to expire, all access to the system using centrally administered accounts will be denied until the passwords are reset. In this case, local emergency accounts must be used to access all applications or devices. It is strongly recommended that all steps in this procedure are performed to avoid any outage to central security servers.

### Prerequisites

To perform this procedure, you must have root user privileges.

### Action

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Change the amadmin password for the NSS-SAML client on the active and inactive IEMS Security servers. For details, see ["Changing the amAdmin password" \(page 327\)](#).

- 2 Telnet to the active server by typing  
`> telnet <server>`  
 and pressing the Enter key.  
 where  
**server** is the IP address or host name of the server where IEMS resides
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing  
`$ su - root`  
 and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 Change to the directory where the change password script is located by typing:  
`cd /opt/nortel/applications/security/core_1.1.0/bin/`  
 and pressing the Enter key.
- 7 To change the system account passwords on the active server, type:  
`./ ss_change_passwd.sh`  
 and press Enter.

| If you are performing this procedure in | Do                                |
|-----------------------------------------|-----------------------------------|
| a simplex configuration                 | you have completed this procedure |
| a high availability (HA) configuration  | go to the next step               |

- 8 Telnet to the inactive server by typing  
`> telnet <server>`  
 and pressing the Enter key.  
 where  
**server** is the IP address or host name of the server where IEMS resides
- 9 When prompted, enter your user ID and password.
- 10 Change to the root user by typing



```
$ su - root
```

and pressing the Enter key.

- 11** When prompted, enter the root password.

- 12** Change to the directory where the change password script is located by typing:

```
cd /opt/nortel/applications/security/core_1.1.0/bin/
```

and pressing the Enter key.

- 13** To change the system account passwords on the inactive server, type:

```
./ ss_change_passwd.sh -local
```

and press Enter.

- 14** You have completed this procedure.

---

—End—

---

## Changing the saml password on an SPFS-based central security client

### Application

Use this procedure to change the saml password on an SPFS-based central security client.

### Prerequisites

You need root user privileges to complete this procedure.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the client server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
**server** is the IP address or host name of the SPFS-based client server
- 2 When prompted, enter the user ID and password for an account that was migrated to the IEMS central security server.
- 3 Change to the root user by typing  

```
$ su - root
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Access the command line interface by typing  

```
cli
```

 and pressing the Enter key.
- 6 Enter the number next to the 'Configuration' option in the menu, and press the Enter key.
- 7 Enter the number next to the 'Security Services Configuration' option in the menu, and press the Enter key.

- 8 Enter the number next to the 'PAM Configuration' option in the menu, and press the Enter key.
- 9 Enter the number next to the 'Central Security Client Configuration' option in the menu, and press the Enter key.
- 10 Enter the number next to the 'saml\_passwd\_conf' option in the menu, and press the Enter key.

*Example response*

```
=== Executing "saml_passwd_conf"
"Enter the SAML password (default: slisamadmin):
mypassword
Confirm Settings
SAML Password: slisamadmin
Enter 'ok' to commit changes
Enter 'quit' to exit
Enter anything else to re-enter settings
```

- 11 Confirm the settings by typing

ok

and pressing the Enter key.

*Example response*

```
Configure Password Successful
=== "saml_passwd_conf" completed successfully
```

You have completed this procedure.

---

—End—

---

## Changing the Oracle user password on an SPFS-based server

### Application

Use this procedure to change the default Oracle passwords on a Server Platform Foundation Software (SPFS)-based server.

Refer to procedure ["Changing the APS Oracle account password"](#) (page 123), to change the Oracle account default password.

#### ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the Active server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server** is the IP address or host name of the SPFS-based server  
In a two-server configuration, log in to the active server using its physical IP address.
- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing  
`$ su -`  
and pressing the Enter key.
  - 4 When prompted, enter the root password.
  - 5 Change to the Oracle user by typing  
`# su - oracle`  
and pressing the Enter key.
  - 6 Change the password by typing  
`$ /opt/nortel/SPFS/db/pfsora_set_pwd <userID>`  
and pressing the Enter key.  
where  
`userID` is the user ID of the Oracle user  
Example response:  
Enter new password for user SYSTEM:
  - 7 When prompted, enter the new password for the system.  
*Example response:*  
Re-enter new password:
  - 8 When prompted, enter the password a second time to confirm the password.  
*Example response:*  
Please wait...  
Successfully changed password for Oracle user SYSTEM
- The command takes approximately 15 to 20 seconds to execute.  
You have completed this procedure.

---

—End—

---

## Setting up local user accounts on an SPFS-Based Server

### Application

Use this procedure to add local user accounts on a Server Platform Foundation Software (SPFS)-based server and assign them to user groups. Also use this procedure to assign existing user accounts to user groups. For information on user groups, see ["Additional information" \(page 340\)](#).

If you choose to centrally manage your user accounts, refer to procedure "Adding new users" in *IEMS Administration and Security* (NN10336-611).

If you want to launch the ping and traceroute operations that are performed remotely on SPFS-based platforms from a centralized GUI on Integrated Element Management System (IEMS), refer to procedures "Running a ping test on the GWC network element or SPFS platform" and "Running a traceroute test on the GWC network element or SPFS platform" in *IEMS Overview* (NN10329-111).

#### ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

### Prerequisites

To perform this procedure, you need to have the root user ID and password to log in to the server.

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where

**server** is the IP address or host name of the SSFPS-based server

In a two-server configuration, log in to the active server using its physical IP address.

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

| If you are                                          | Do      |
|-----------------------------------------------------|---------|
| adding a new user                                   | step 6  |
| assigning an existing user to secondary user groups | step 11 |

6 Add the user to the primary user group *succssn* by typing

```
useradd -d /export/home/<userid> -g succssn -G
<any additional groups> -m <userid>
```

and press the Enter key.

where

**userid** is a variable for the user name

7 Create a password for the user you just added by typing

```
passwd -r files <userid>
```

and press the Enter key.

where

**userid** is the user name you added in the previous step

8 When prompted, enter a password of at least three characters.

It is not recommended to set a password with an empty value. Use a minimum of three characters.

9 When prompted, enter the password again for verification.

10 Proceed to step 13.

11 Determine which groups the user currently belongs to by typing

```
groups <userid>
```

and pressing the Enter key.

where

**userid** is a variable for the user name

**12** Note the user groups the user currently belongs to.

**13** Assign the user to one or more secondary user groups by typing

```
usermod -g succssn -G <groupA,groupB,...>
<userid>
```

and pressing the Enter key.

where

**groupA, groupB,...** are the secondary user groups (see table "Secondary user groups" (page 340)) and any other user groups you noted in step 12 to which the user already belonged. Include a comma between groups, but no space.

**userid** is a variable for the user name

Example input for a user who can perform line and trunk maintenance operations

```
usermod -g succssn -G lnmtc,trkmtc johndoe
```

The usermod command overwrites any previous user groups.

Therefore, anytime you enter this command, specify all the user groups for the user.

You have completed this procedure.

---

—End—

---

## Additional information

Users of the Nortel OAM&P client applications must belong to the primary user group succssn for login access. Users must also belong to one or more secondary user groups listed in the following table, which specify the operations a user is authorized to perform.

### Secondary user groups

|          |         |          |        |          |        |
|----------|---------|----------|--------|----------|--------|
| trkadm   | lnadm   | mgcadm   | mgadm  | emsadm   | secadm |
| trkrw    | lnrw    | mgcrw    | mgrw   | emsrw    | secrw  |
| trksprov | lnsprov | mgcsprov | mgspov | emssprov | secmtc |
| trkmtc   | lnmtc   | mgcmte   | mgmtc  | emsmte   | secro  |
| trkro    | lnro    | mgcro    | mgro   | emsro    |        |



A secondary user group consists of

- a user group domain
- a user group operation

### User group domain

A user group domain defines the range of applications to which a user group applies. The user group domains are listed in the following table:

| Domain | Application mapping                                                                        |
|--------|--------------------------------------------------------------------------------------------|
| trk    | trunks, trunk-based services, small trunking gateways (port level), carrier-based services |
| ln     | line services, line cards, small line gateways (port level)                                |
| mgc    | CS2K, CS3K, USP, GWC, SAM21, IMS, 3PC, Storm, CS 2000 SAM21 Manager, CS 2000 GWC Manager   |
| mg     | small and large gateways such as UAS, line gateways, trunk gateways                        |
| ems    | SDM, MDM, MDP, KDC, device manager, NPM                                                    |

### User group operation

A user group operation dictates the operations a user can perform using the Nortel OAM&P client applications. The user group operations are listed in the following table:

| Operation                       | User role mapping                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adm (administration)            | Can reconfigure, access all functions, setup fundamental configuration, commission (add, delete, rehome), base frames and systems (SAM21 frames, call servers, large gateways), and run service-impacting diagnostics. The adm user can also do rw, sprov, mtc, and ro user operations. |
| rw (read/write)                 | Can view and change configuration and status, commission and reconfigure elements (GWCs, cards, shelves). The rw user can also do sprov, mtc, and ro user operations.                                                                                                                   |
| mtc (maintenance)               | Can view status and configuration, make changes to status, and run service-impacting diagnostics. The mtc user can also do sprov and ro user operations.                                                                                                                                |
| sprov (subscriber provisioning) | Can view status and configuration and change provisioning data, but cannot change maintenance state or do base component configuration. The sprov user can also do ro user operations.                                                                                                  |
| ro (read-only)                  | Can view status and configuration, but cannot make changes.                                                                                                                                                                                                                             |

When assigning users to secondary user groups, use the tables that follow, which provide a mapping between commands and secondary user groups. The list of the available tables is as follow:

- "Node provisioning operations" (page 342)
- "Audit operations" (page 344)
- "Carrier provisioning operations" (page 345)
- "Alarm operations" (page 345)
- "Internet transparency operations" (page 345)
- "Trunk provisioning operations" (page 346)
- "Trunk maintenance operations" (page 346)
- "ADSL provisioning operations" (page 347)
- "Line provisioning operations" (page 348)
- "Line maintenance operations" (page 349)
- "V5.2 provisioning operations" (page 349)
- "Patching operations" (page 351)
- "Automated upgrade operations" (page 352)
- "Ping and traceroute operations" (page 352)

The mappings of commands to secondary user groups in the tables in this section do not apply to Multiservice Data Manager (MDM) when installed on a SPFS-based server.

#### Node provisioning operations

| Command                                                           | User group |       |        |          |       |
|-------------------------------------------------------------------|------------|-------|--------|----------|-------|
|                                                                   | mgcadm     | mgcrw | mgcmte | mgcsprov | mgcro |
| Disassociate a media gateway (MG) from a gateway controller (GWC) |            | x     |        |          |       |
| Associate an MG with a GWC                                        |            | x     |        |          |       |
| Change the provisioning data for an MG                            |            | x     |        |          |       |
| Query site info                                                   |            |       |        |          | x     |

| Command                                                   | User group |       |        |          |       |
|-----------------------------------------------------------|------------|-------|--------|----------|-------|
|                                                           | mgcadm     | mgcrw | mgcmte | mgcsprov | mgcro |
| Query a GWC                                               |            |       |        |          | x     |
| Query an MG                                               |            |       |        |          | x     |
| change MG GWCEM data                                      |            | x     |        |          |       |
| Get policy enforcement point (PEP) server data            |            |       |        |          | x     |
| Query a GWC PEP connection                                |            |       |        |          | x     |
| Get dynamic quality of service (DQoS) policies data       |            |       |        |          | x     |
| Add or change a network address translations (NAT) device |            | x     |        |          |       |
| Query a NATdevice                                         |            |       |        |          | x     |
| Add, change, delete a media proxy (MP)                    |            | x     |        |          |       |
| Add, change, delete resource usage (RU)                   |            | x     |        |          |       |
| Query RU                                                  |            |       |        |          | x     |
| Add, change, delete limited bandwidth links (LBL)         |            | x     |        |          |       |
| Query LBL                                                 |            |       |        |          | x     |
| Display call agent identification (ID)                    |            |       |        |          | x     |
| Set or change call agent ID                               |            | x     |        |          |       |
| Change root middleboxes                                   |            | x     |        |          |       |

| Command                                                  | User group |       |        |          |       |
|----------------------------------------------------------|------------|-------|--------|----------|-------|
|                                                          | mgcadm     | mgcrw | mgcmte | mgcsprov | mgcro |
| Add, modify, or decommission a SAM21 network element     |            | x     |        |          |       |
| Reprovision a SAM21 node                                 |            | x     |        |          |       |
| Configure IPoA services, ATM PMC addresses               |            | x     |        |          |       |
| View alarms, cards, subnet, shelf, mate shelf, mate card |            |       |        |          | x     |
| Lock/unlock a card                                       |            |       | x      |          |       |
| Perform diagnostics                                      |            |       | x      |          |       |
| Modify provisioning                                      |            | x     |        |          |       |
| Perform a swact                                          |            |       | x      |          |       |
| Firmware flash                                           |            |       | x      |          |       |
| Assign/unassign services                                 |            | x     |        |          |       |

**Audit operations**

| Command                       | User group |       |        |          |       |
|-------------------------------|------------|-------|--------|----------|-------|
|                               | mgcadm     | mgcrw | mgcmte | mgcsprov | mgcro |
| Configure audit               | x          |       |        |          |       |
| Run audit                     | x          |       |        |          |       |
| Get audit description         |            |       |        |          | x     |
| Get audit configuration       |            |       |        |          | x     |
| Get list of registered audits |            |       |        |          | x     |

| Command                | User group |       |        |          |       |
|------------------------|------------|-------|--------|----------|-------|
|                        | mgcadm     | mgcrw | mgcmtd | mgcsprov | mgcro |
| Retrieve audit report  |            |       |        |          | x     |
| Take action on problem | x          |       |        |          |       |

**Carrier provisioning operations**

| Command               | User group |       |        |          |       |
|-----------------------|------------|-------|--------|----------|-------|
|                       | trkadm     | trkrw | trkmtc | trksprov | trkro |
| Add carrier           |            | x     |        |          |       |
| Delete carrier        |            | x     |        |          |       |
| Get endpoint          |            |       |        |          | x     |
| Get carrier           |            |       |        |          | x     |
| Get carrier by filter |            |       |        |          | x     |

**Alarm operations**

| Command            | User group |       |        |          |       |
|--------------------|------------|-------|--------|----------|-------|
|                    | emsadm     | emsrw | emsmtd | emssprov | emsro |
| View/filter alarms |            |       |        |          | x     |

**Internet transparency operations**

| Command | User group |       |        |          |       |
|---------|------------|-------|--------|----------|-------|
|         | mgcadm     | mgcrw | mgcmtd | mgcsprov | mgcro |

| Add, delete, change SPC            | x |   |   |   |   |
|------------------------------------|---|---|---|---|---|
| Query SPCs                         |   |   |   |   | x |
| Set network VCAC                   | x |   |   |   |   |
| Add, delete, change a network zone | x |   |   |   |   |
| Query one or all network zones     |   |   |   |   | x |
| addMPGroup                         | x | x |   |   |   |
| changeMPGroup                      | x | x |   |   |   |
| queryMPGroup                       | x | x | x | x | x |
| deleteMPGroup                      | x | x |   |   |   |
| addVPN                             | x | x |   |   |   |
| deleteVPN                          | x | x |   |   |   |
| queryVPN                           | x | x | x | x | x |

**Trunk provisioning operations**

| Command         | User group |       |        |          |       |
|-----------------|------------|-------|--------|----------|-------|
|                 | trkadm     | trkrw | trkmtc | trksprov | trkro |
| Get tuple       |            |       |        |          | x     |
| Get tuple range |            |       |        |          | x     |
| Add tuple       |            | x     |        |          |       |
| Replace tuple   |            | x     |        |          |       |
| Delete tuple    |            | x     |        |          |       |

**Trunk maintenance operations**

| Command | User group |       |        |          |       |
|---------|------------|-------|--------|----------|-------|
|         | trkadm     | trkrw | trkmtc | trksprov | trkro |

| Post by trunk CLLI                  |  |  |   |  | x |
|-------------------------------------|--|--|---|--|---|
| Maintenance by trunk CLLI           |  |  | x |  |   |
| Post by gateway                     |  |  |   |  | x |
| Maintenance by gateway              |  |  | x |  |   |
| Post by carrier                     |  |  |   |  | x |
| Maintenance by carrier              |  |  | x |  |   |
| D-channel Post by trunk CLLI        |  |  |   |  | x |
| D-channel maintenance by trunk CLLI |  |  | x |  |   |
| ICOT                                |  |  | x |  |   |
| Set Auto Refresh                    |  |  |   |  | x |

**ADSL provisioning operations**

| Command                 | User group |      |       |         |      |
|-------------------------|------------|------|-------|---------|------|
|                         | Inadm      | Inrw | Inmtc | Insprov | Inro |
| Get subscriber          |            |      |       |         | x    |
| Add subscriber          |            |      |       | x       |      |
| Add cross connection    |            |      |       | x       |      |
| Modify subscriber       |            |      |       | x       |      |
| Modify cross connection |            |      |       | x       |      |

| Command                 | User group |      |       |         |      |
|-------------------------|------------|------|-------|---------|------|
|                         | Inadm      | Inrw | Inmtc | Insprov | Inro |
| Delete subscriber       |            |      |       | X       |      |
| Delete cross connection |            |      |       | X       |      |

**Line provisioning operations**

| Command                                                                                                                                                                        | User group |      |       |         |      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------|-------|---------|------|
|                                                                                                                                                                                | Inadm      | Inrw | Inmtc | Insprov | Inro |
| ECHO, QX75, QBB, QBERT, QCM, QCOUNTS, QCPUGNO, QDCH, QDN, QDNA, QGRP, QHLR, QIT, QLEN, QLRN, QLT, QMODEL, QMSB, QPHF, QPRIO, QSCONN, QSCUGNO, QSIMR, QSL, QTOPSPOS, QTP, QWUCR |            |      |       |         | X    |
| QCUST, QDNSU, QDNWRK, QHA, QHASU, QHU, QLENWRK, QLOAD, QMADN, QNCOS, QPDN                                                                                                      | X          |      |       |         |      |
| All other supported commands for line provisioning                                                                                                                             |            |      |       | X       |      |



**Line maintenance operations**

| Command                        | User group |      |       |         |      |
|--------------------------------|------------|------|-------|---------|------|
|                                | Inadm      | Inrw | Inmtc | Insprov | Inro |
| Validate line using DN CLLI    |            |      |       |         | x    |
| Validate line using TID CLLI   |            |      |       |         | x    |
| Get line post info             |            |      |       |         | x    |
| Busy line                      |            |      | x     |         |      |
| Return line to service         |            |      | x     |         |      |
| Force release line             |            |      | x     |         |      |
| Installation busy line         |            |      | x     |         |      |
| Cancel deload                  |            |      | x     |         |      |
| Get CM CLLI                    |            |      |       |         | x    |
| Get endpoint state             |            |      |       |         | x    |
| GetGwlp                        |            |      |       |         | x    |
| run all TL1 line test commands |            |      | x     |         |      |

**V5.2 provisioning operations**

| Com-mand                           | User group |        |         |           |        |        |        |         |          |        |
|------------------------------------|------------|--------|---------|-----------|--------|--------|--------|---------|----------|--------|
|                                    | trka dm    | trk rw | trk mtc | trksp rov | trk ro | Ina dm | I nr w | I nm tc | Insp rov | I nr o |
| Add, delete, modify V5.2 interface |            | x      |         |           |        |        | x      |         |          |        |

| Com-<br>mand                                                                                        | User group |           |            |              |           |           |              |               |             |              |
|-----------------------------------------------------------------------------------------------------|------------|-----------|------------|--------------|-----------|-----------|--------------|---------------|-------------|--------------|
|                                                                                                     | trka<br>dm | trk<br>rw | trk<br>mtc | trksp<br>rov | trk<br>ro | lna<br>dm | l<br>nr<br>w | l<br>nm<br>tc | lnsp<br>rov | l<br>nr<br>o |
| View<br>all V5.2<br>interfac<br>es                                                                  |            |           |            |              | x         |           |              |               |             | x            |
| View<br>signall<br>ing cha<br>nnel<br>inform<br>ation<br>entry,<br>update<br>list (V5<br>Prov)      |            |           |            |              | x         |           |              |               |             | x            |
| Add,<br>modify,<br>delete<br>signalli<br>ng cha<br>nnel<br>inform<br>ation<br>entry<br>(V5Pr<br>ov) |            | x         |            |              |           |           | x            |               |             |              |
| View<br>ringing<br>cadenc<br>e map<br>ping,<br>update<br>list (V5<br>Ring)                          |            |           |            |              | x         |           |              |               |             | x            |
| Add,<br>modify,<br>delete<br>ringing<br>cadenc<br>e mapp<br>ing (V5<br>Ring)                        |            | x         |            |              |           |           | x            |               |             |              |

| Com-<br>mand                                                                                | User group |           |            |              |           |           |              |               |             |              |
|---------------------------------------------------------------------------------------------|------------|-----------|------------|--------------|-----------|-----------|--------------|---------------|-------------|--------------|
|                                                                                             | trka<br>dm | trk<br>rw | trk<br>mtc | trksp<br>rov | trk<br>ro | lna<br>dm | l<br>nr<br>w | l<br>nm<br>tc | lnsp<br>rov | l<br>nr<br>o |
| View sign<br>alling<br>charac<br>teristic<br>profile,<br>update<br>list (V5<br>Sig)         |            |           |            |              | x         |           |              |               |             | x            |
| Add,<br>delete,<br>modify<br>sign<br>alling<br>charac<br>teristic<br>profile<br>(V5Sig<br>) |            | x         |            |              |           |           | x            |               |             |              |
| View carrier<br>-to-int<br>erface<br>and<br>interfa<br>ce-to-<br>carrier<br>mappin<br>gs    |            |           |            |              | x         |           |              |               |             | x            |

**Patching operations**

| Command                                                             | User group |       |        |          |       |
|---------------------------------------------------------------------|------------|-------|--------|----------|-------|
|                                                                     | emsadm     | emsrw | emsmtc | emssprov | emsro |
| apply, remove,<br>activate, deac<br>tivate, auditd,<br>restart, and | x          |       |        |          |       |

| Command                                 | User group |       |        |          |       |
|-----------------------------------------|------------|-------|--------|----------|-------|
|                                         | emsadm     | emsrw | emsmtc | emssprov | emsro |
| smartimage from the NPM GUI or CLUI     |            |       |        |          |       |
| Software image from MG 9000 Manager GUI |            | x     |        |          |       |

### Automated upgrade operations

| Command                             | User group |       |        |          |         |       |       |        |          |       |
|-------------------------------------|------------|-------|--------|----------|---------|-------|-------|--------|----------|-------|
|                                     | emsadm     | emsrw | emsmtc | emssprov | emsmkro | mgadm | mgcrw | mgcmtc | mgcsprov | mgcro |
| Access and run the GWC upgrade CLUI |            |       | x      |          |         |       |       | x      |          |       |
| Access and run the SC upgrade CLUI  |            |       | x      |          |         |       |       | x      |          |       |

### Ping and traceroute operations

| Command                                                                                                             | User group |       |        |
|---------------------------------------------------------------------------------------------------------------------|------------|-------|--------|
|                                                                                                                     | emsadm     | emsrw | emsmtc |
| Launch remote ping                                                                                                  | x          | x     | x      |
| Launch remote traceroute                                                                                            | x          | x     | x      |
| These operations are for remote operations performed on SPFS platforms but launched from a centralized GUI on IEMS. |            |       |        |

- "Node provisioning operations" (page 353)

- "Audit operations" (page 355)
- "Carrier provisioning operations" (page 356)
- "Alarm operations" (page 356)
- "Internet transparency operations" (page 356)
- "Trunk provisioning operations" (page 357)
- "Trunk maintenance operations" (page 357)
- "Patching operations" (page 358)
- "Automated upgrade operations" (page 358)

#### Node provisioning operations

| Command                                                           | User group |       |        |          |       |
|-------------------------------------------------------------------|------------|-------|--------|----------|-------|
|                                                                   | mgcadm     | mgcrw | mgcmte | mgcsprov | mgcro |
| Disassociate a media gateway (MG) from a gateway controller (GWC) |            | x     |        |          |       |
| Associate an MG with a GWC                                        |            | x     |        |          |       |
| Change the provisioning data for an MG                            |            | x     |        |          |       |
| Query site info                                                   |            |       |        |          | x     |
| Query a GWC                                                       |            |       |        |          | x     |
| Query an MG                                                       |            |       |        |          | x     |
| change MG GWCEM data                                              |            | x     |        |          |       |
| Get policy enforcement point (PEP) server data                    |            |       |        |          | x     |
| Query a GWC PEP connection                                        |            |       |        |          | x     |
| Get dynamic quality of service (DQoS) policies data               |            |       |        |          | x     |

| Command                                                   | User group |       |        |          |       |
|-----------------------------------------------------------|------------|-------|--------|----------|-------|
|                                                           | mgcadm     | mgcrw | mgcmte | mgcsprov | mgcro |
| Add or change a network address translations (NAT) device |            | x     |        |          |       |
| Query a NATdevice                                         |            |       |        |          | x     |
| Add, change, delete a media proxy (MP)                    |            | x     |        |          |       |
| Add, change, delete resource usage (RU)                   |            | x     |        |          |       |
| Query RU                                                  |            |       |        |          | x     |
| Add, change, delete limited bandwidth links (LBL)         |            | x     |        |          |       |
| Query LBL                                                 |            |       |        |          | x     |
| Display call agent identification (ID)                    |            |       |        |          | x     |
| Set or change call agent ID                               |            | x     |        |          |       |
| Change root middleboxes                                   |            | x     |        |          |       |
| Add, modify, or decommission a SAM21 network element      |            | x     |        |          |       |
| Reprovision a SAM21 node                                  |            | x     |        |          |       |
| Configure IPoA services, ATM PMC addresses                |            | x     |        |          |       |
| View alarms, cards, subnet, shelf, mate shelf, mate card  |            |       |        |          | x     |

| Command                                                     | User group |       |        |          |       |
|-------------------------------------------------------------|------------|-------|--------|----------|-------|
|                                                             | mgcadm     | mgcrw | mgcmte | mgcsprov | mgcro |
| Lock/unlock a card                                          |            |       | x      |          |       |
| Perform diagnostics                                         |            |       | x      |          |       |
| Modify provisioning                                         |            | x     |        |          |       |
| Perform a swact (refer to the notes that follow this table) |            |       | x      |          |       |
| Firmware flash                                              |            |       | x      |          |       |
| Assign/unassign services                                    |            | x     |        |          |       |

**Audit operations**

| Command                       | User group |       |        |          |       |
|-------------------------------|------------|-------|--------|----------|-------|
|                               | mgcadm     | mgcrw | mgcmte | mgcsprov | mgcro |
| Configure audit               | x          |       |        |          |       |
| Run audit                     | x          |       |        |          |       |
| Get audit description         |            |       |        |          | x     |
| Get audit configuration       |            |       |        |          | x     |
| Get list of registered audits |            |       |        |          | x     |

| Command                | User group |       |        |          |       |
|------------------------|------------|-------|--------|----------|-------|
|                        | mgcadm     | mgcrw | mgcmte | mgcsprov | mgcro |
| Retrieve audit report  |            |       |        |          | x     |
| Take action on problem | x          |       |        |          |       |

**Carrier provisioning operations**

| Command               | User group |       |        |          |       |
|-----------------------|------------|-------|--------|----------|-------|
|                       | trkadm     | trkrw | trkmtc | trksprov | trkro |
| Add carrier           |            | x     |        |          |       |
| Delete carrier        |            | x     |        |          |       |
| Get endpoint          |            |       |        |          | x     |
| Get carrier           |            |       |        |          | x     |
| Get carrier by filter |            |       |        |          | x     |

**Alarm operations**

| Command            | User group |       |        |          |       |
|--------------------|------------|-------|--------|----------|-------|
|                    | emsadm     | emsrw | emsmte | emssprov | emsro |
| View/filter alarms |            |       |        |          | x     |

**Internet transparency operations**

| Command                 | User group |       |        |          |       |
|-------------------------|------------|-------|--------|----------|-------|
|                         | mgcadm     | mgcrw | mgcmte | mgcsprov | mgcro |
| Add, delete, change SPC | x          |       |        |          |       |
| Query SPCs              |            |       |        |          | x     |
| Set network VCAC        | x          |       |        |          |       |



| Command                            | User group |       |        |          |       |
|------------------------------------|------------|-------|--------|----------|-------|
|                                    | mgcadm     | mgcrw | mgcmte | mgcsprov | mgcro |
| Add, delete, change a network zone | x          |       |        |          |       |
| Query one or all network zones     |            |       |        |          | x     |

**Trunk provisioning operations**

| Command         | User group |       |        |          |       |
|-----------------|------------|-------|--------|----------|-------|
|                 | trkadm     | trkrw | trkmtc | trksprov | trkro |
| Get tuple       |            |       |        |          | x     |
| Get tuple range |            |       |        |          | x     |
| Add tuple       |            | x     |        |          |       |
| Replace tuple   |            | x     |        |          |       |
| Delete tuple    |            | x     |        |          |       |

**Trunk maintenance operations**

| Command                      | User group |       |        |          |       |
|------------------------------|------------|-------|--------|----------|-------|
|                              | trkadm     | trkrw | trkmtc | trksprov | trkro |
| Post by trunk CLLI           |            |       |        |          | x     |
| Maintenance by trunk CLLI    |            |       | x      |          |       |
| Post by gateway              |            |       |        |          | x     |
| Maintenance by gateway       |            |       | x      |          |       |
| Post by carrier              |            |       |        |          | x     |
| Maintenance by carrier       |            |       | x      |          |       |
| D-channel Post by trunk CLLI |            |       |        |          | x     |

| Command                             | User group |       |        |          |       |
|-------------------------------------|------------|-------|--------|----------|-------|
|                                     | trkadm     | trkrw | trkmtc | trksprov | trkro |
| D-channel maintenance by trunk CLLI |            |       | x      |          |       |
| ICOT                                |            |       | x      |          |       |
| Set Auto Refresh                    |            |       |        |          | x     |

**Patching operations**

| Command                                                                                       | User group |       |        |          |       |
|-----------------------------------------------------------------------------------------------|------------|-------|--------|----------|-------|
|                                                                                               | emsadm     | emsrw | emsmtc | emssprov | emsro |
| apply, remove, activate, deactivate, auditd, restart, and smartimage from the NPM GUI or CLUI | x          |       |        |          |       |
| Software image from MG 15000 Manager GUI                                                      |            | x     |        |          |       |

**Automated upgrade operations**

| Command | User group |       |        |          |         |     |     |     |     |     |
|---------|------------|-------|--------|----------|---------|-----|-----|-----|-----|-----|
|         | emsadm     | emsrw | emsmtc | emssprov | emsmkro | mgc | mgc | mgc | mgc | mgc |
|         | adm        | rw    | mtc    | ov       | ro      | adm | rw  | tc  | sp  | ro  |
|         |            |       |        |          |         |     |     |     | v   |     |

| Access and run the GWC upgrade CLUI |  |  | x |  |  |  |  | x |  |  |
|-------------------------------------|--|--|---|--|--|--|--|---|--|--|
| Access and run the SC upgrade CLUI  |  |  | x |  |  |  |  | x |  |  |

## Deleting local user accounts from an SPFS-based server

### Application

Use this procedure to delete local user accounts from a Server Platform Foundation Software (SPFS)-based server.

If you are centrally managing your user accounts, refer to procedure "Deleting users" in the *IEMS Security and Administration* document, (NN10336-611).

#### ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the Active server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server** is the IP address or host name of the SPFS-based server  
In a two-server configuration, log in to the active server using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su -
```

and pressing the Enter key.

- 4 When prompted, enter the root password.

**ATTENTION**

Do not delete the following critical user IDs from the server:

root, sshd, maint, npm, npmftp, ptm, mgems, www, patcher, poller,  
certuser, sam21em, anonymous, image, pfrs, ntssg, FIELD, oracle, nortel

- 5 Delete the user from the server by typing

# `userdel <userid>`

and pressing the Enter key.

where

`userid` is a variable for the user name

You have completed this procedure.

---

—End—

---

## Changing a user password on an SPFS-based server

### Application

Use this procedure to change a user password on a Server Platform Foundation Software (SPFS)-based server.

#### ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the Active server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
     **server** is the IP address or host name of the SPFS-based server  
 In a two-server configuration, log in to the active server using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing
- 4 When prompted, enter the root password.
- 5 Change the password for a specific user by typing  

```
passwd -r files <userid>
```

 and pressing the Enter key.  
 where

**userid** is a variable for the user's login identification

- 6 When prompted, enter a password of at least three characters.  
It is not recommended to set a password with an empty value. Use a minimum of three characters.
- 7 When prompted, enter the password again for verification.  
You have completed this procedure.

---

—End—

---

## Stopping and starting the DDMS proxy

### Application

#### ATTENTION

Use this procedure only if you have been directed here from the Optional post-upgrade tasks in *Core Manager Upgrades*, NN10060-461, after a software upgrade.

Use this procedure to stop and start the DDMS proxy on the CS 2000 Management Tools server. The DDMS proxy enables communication between the CS 2000 Management Tools server and the core.

### Prerequisites

There are no prerequisites for this procedure.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Establish a login session to the inactive server, using one of the following methods:

| If using          | Do     |
|-------------------|--------|
| telnet (unsecure) | step 2 |
| ssh (secure)      | step 3 |

- 2 Log in to the server using telnet (unsecure) as follows:
  - a. Log in to the server by typing
 

```
> telnet <server>
```

 and pressing the Enter key.
 

where

**server** is the physical IP address of the inactive server
  - b. When prompted, enter your user ID and password.
  - c. Change to the root user by typing
 

```
$ su - root
```

 and pressing the Enter key.



- d. When prompted, enter the root password.  
Proceed to step 4.
- 3 Log in using ssh (secure) as follows:
  - a. Log in to the server by typing
 

```
> ssh -l root <server>
```

 and pressing the Enter key.  
 where  
**server** is the physical IP address of the inactive server  
 If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.
  - b. When prompted, enter the root password.

- 4 Use the following table to determine your next step.

| If you upgraded the CS 2000 Core Manager from |  | Do     |
|-----------------------------------------------|--|--------|
| SN07                                          |  | step 5 |
| SN08                                          |  | step 8 |

- 5 Stop the DDMS proxy by typing
 

```
/opt/nortel/NTsesm/admin/scripts/ddmsproxy stop
```

 and pressing the Enter key.
- 6 Start the DDMS proxy by typing
 

```
/opt/nortel/NTsesm/admin/scripts/ddmsproxy start
```

 and pressing the Enter key.
- 7 Proceed to step 14.
- 8 Access the command line interface by typing
 

```
cli
```

 and pressing the Enter key.

*Example response*

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
```

select -

- 9** Enter the number next to the "Configuration" option in the menu.

*Example response*

Configuration

1 - NTP Configuration  
2 - Apache Proxy Configuration  
3 - OAMP Application Configuration  
4 - CORBA Configuration  
5 - IP Configuration  
6 - DNS Configuration  
7 - Syslog Configuration  
8 - Remote Backup Configuration  
9 - Database Configuration  
10 - NFS Configuration  
11 - Bootp Configuration  
12 - Restricted Shell Configuration  
13 - Security Services Configuration  
14 - Disk Drive Upgrade  
15 - Login Session  
16 - Location Configuration  
17 - Cluster Configuration  
18 - Succession Element Configuration  
19 - snmp\_poller (SNMP Poller Configuration)  
20 - backup\_config (Backup Configuration)  
X - exit  
Select -

- 10** Enter the number next to the "Succession Element Configuration" option in the menu.

*Example response:*

Succession Element Configuration

1 - NPM Application Configuration  
2 - SESM Application Configuration  
3 - SAM21EM Application Configuration  
4 - PSE Application Configuration  
5 - RESMON Application Configuration  
6 - OMPUSH Application Configuration  
7 - DDMSProxy Application Configuration  
X - exit  
select -

- 11** Enter the number next to the "DDMSProxy Application Configuration" option in the menu.

*Example response*

DDMSProxy Application Configuration

1 - ddmsproxy\_query (query the status of  
ddmsproxy service)

```
2 - ddmsproxy_stop (stop the ddmsproxy service)
3 - ddmsproxy_start (start the ddmsproxy
 service)
X - exit
select -
```

- 12** Enter the number next to the "ddmsproxy\_stop" option in the menu.

*Example response*

```
===Executing "ddmsproxy_stop"
ddmsproxy service stopping
=== "ddmsproxy_stop" completed successfully
```

- 13** Enter the number next to the "ddmsproxy\_start" option in the menu.

*Example response*

```
===Executing "ddmsproxy_start"
ddmsproxy service starting
=== "ddmsproxy_start" completed successfully
```

- 14** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

—End—

---

## Stopping and starting the Apache Web Server and Tomcat Servlet Container

### Application

#### ATTENTION

Use this procedure only if you have been directed here from the Post-upgrade procedures in the Upgrades section. Perform this procedure after a software upgrade.

Use this procedure to stop and start the Apache Web Server and Tomcat Servlet Container components on the CS 2000 Management Tools server.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

*At your workstation*

- 1 Telnet to the CS 2000 Management Tools server by typing  

```
> telnet <IP address>
```

  
and pressing the Enter key.  
where  
**IP address** is the IP address of the CS 2000 Management Tools server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

  
and pressing the Enter key.
- 4 When prompted, enter the root password.

- 5 Use the following table to determine your next step.

| If you want to                                           | Do     |
|----------------------------------------------------------|--------|
| stop the Apache web server and Tomcat servlet container  | step 6 |
| start the Apache web server and Tomcat servlet container | step 7 |

- 6 Stop the Apache Tomcat component by typing  
`# /etc/init.d/apache stop`  
and pressing the Enter key.
- 7 Start the Apache Tomcat component by typing  
`# /etc/init.d/apache start`  
and pressing the Enter key.
- 8 You have completed this procedure.

---

—End—

---

---

## Configuring the Apache Web Server for HTTPS Proxy

---

### Application

Use this procedure to configure the Apache Web Server on a Server Platform Foundation Software (SPFS) based server for HTTPS proxy.

To perform this procedure for Session Server Lines, refer to the procedure *Linking the Provisioning and System Manager to SESM* in NN10437-111.

#### ATTENTION

The preferred location to configure the Apache Web Server for HTTPS proxy is on the SPFS-based server that hosts the Integrated Element Management System (IEMS). If the IEMS is not present in the network, configure the Apache Web Server for HTTPS proxy on the SPFS-based server that hosts the CS 2000 Management Tools.

You can provision a maximum of 100 IP addresses for use in HTTPS proxy.

Configuring the Apache Web Server for HTTPS proxy is applicable to the following components:

- Storage Management (STORM)
- Session Server Trunks
- Centrex IP Client Manager (CICM) and CICM Element Manager
- Session Server Lines

### Prerequisites

This procedure has the following prerequisites:

- You need the root user ID and password for the SPFS-based server.
- If you are adding a component to the proxy, you need to know what entries are required for the component. If you do not know what entries are required, refer to the applicable Configuration document in the following list for specific instructions on how to add the component to the proxy:
  - *STORM Configuration Management*, NN10110-511
  - *Session Server Configuration Management*, NN10338-511
  - *CICM Configuration Management*, NN10240-511

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

***At your workstation***

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server** is the IP address or host name of the SPFS-based server on which you are configuring the proxy
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su -
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Access the command line interface by typing  

```
cli
```

and pressing the Enter key.
- 6 Enter the number next to the "Configuration" option in the menu and press the enter key.
- 7 Enter the number next to the "Apache Proxy Configuration" option in the menu and press the enter key.
- 8 Use the following table to determine your next step:

| If you want to                 | Do      |
|--------------------------------|---------|
| add an entry in the proxy      | step 9  |
| delete an entry from the proxy | step 10 |
| list the entries in the proxy  | step 11 |
| exit                           | step 12 |

- 9 Enter the number next to the "add\_proxy\_conf" option in the menu.  
Follow the prompts to add the component to the proxy. If you do not know what entries are required, refer to the applicable Configuration document in the following list for specific instructions on how to add the component to the proxy:

**ATTENTION**

Using "x" and "X" for tagnames is not supported in SPFS.

- *STORM Configuration Management*, NN10110-511
- *Session Server Configuration Management*, NN10338-511
- *CICM Configuration Management*, NN10240-511

Return to step 8.

- 10** Enter the number next to the "del\_proxy\_conf" option in the menu, and follow the prompts to delete the component from the proxy.

Return to step 8.

- 11** Enter the number next to the "list\_proxy\_conf" option in the menu.  
Return to step 8.

- 12** Exit each menu level of the command line interface to eventually return to the command prompt, by typing

`select - x`

and pressing the Enter key.

You have completed this procedure.

---

—End—

---



## Configuring OSSGate password control

### Application

Use this procedure to configure OSSGate password control. When OSSGate password control is turned on, the password will not be echoed on the screen when logging in.

### Prerequisites

You need root user privileges to perform this procedure.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
**server** is the IP address or host name of the CS 2000 Management Tools server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Access the command line interface by typing  

```
cli
```

 and pressing the Enter key.

#### *Example response*

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

- 6** Enter the number next to the "Configuration" option in the menu.

*Example response*

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Application Configuration
5 - CORBA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
select -
```

- 7** Enter the number next to the "Succession Element Configuration" option in the menu.

*Example response*

```
Succession Element Configuration
1 - SESM Application Configuration
2 - SAM21EM Application Configuration
3 - NPM Application Configuration
4 - PSE Application Configuration
5 - DDMSProxy Application Configuration
6 - OMPUSH Application Configuration
7 - RESMON Application Configuration
X - exit
select -
```

- 8** Enter the number next to the "SESM Application Configuration" option in the menu.

*Example response*

```
SESM Application Configuration
1 - SESM_configuration (SESM Application Configuration)
X - exit
select -
```

- 9** Enter the number next to the "SESM configuration" option in the menu.

*Example response*

```
=== Executing "SESM_configuration"
SESM configuration
1 - SESM common configuration (IP addresses, Market,
CM CLLI)
2 - SESM database tools
3 - SESM related applications configuration (MG9K, LMM,
CICM, CS2KSS)
4 - SESM provisioning configuration
5 - SESM logging configuration (syslog, sesm debug log)
6 - view sesm configuration settings
7 - SESM refresh properties
X - exit
select -
```

- 10** Enter the number next to the "SESM provisioning configuration" option in the menu.

*Example response*

```
SESM Provisioning Configuration
1 - XML Trunk Provisioning configuration
2 - OSSGate Provisioning configuration
3 - Office Provisioning Type configuration
X - exit
select -
```

- 11** Enter the number next to the "OSSGate Provisioning configuration" option in the menu.

*Example response*

```
SESM OSSGate Provisioning Configuration
Enter the Primary Port OSSGate will use for telnet
connections (default: 10023):
```

- 12** When prompted, press the Enter key to accept the default value for the primary port, or enter another value for the primary port if desired.

*Example response*

```
Enter the Secondary Port OSSGate will use for telnet
connections (default: 11023):
```

- 13** When prompted, press the Enter key to accept the default value for the secondary port, or enter another value for the secondary port if desired.

*Example response*

```
Enter the OSSGate Timeout period, in seconds (default:
600):
```

- 14** When prompted, press the Enter key to accept the default value for the timeout period, or enter another value for the timeout period if desired.

*Example response*

```
Do you wish to have OSSGate Port Forwarding on for SSH
[y/n]:
```

- 15** When prompted, indicate whether you want to have OSSGate port forwarding turned on for SSH.

*Example response*

```
Do you wish to turn on/off OSSGate Password Control
option (when this option is turned on, OSSGate will
not echo password on screen when logging into it)
[default:off]:
```

- 16** When prompted, indicate whether you want to turn on OSSGate password control, or press the Enter key to accept the default value.

*Example response*

```
Primary Port: 10023
Secondary Port: 11023
Timeout: 600
Port Forwarding for SSH: no
Password Control: on
Are these information correct? (y or n):
```

- 17** When prompted, confirm the configuration by typing

**y**

and pressing the Enter key.

*Example response*

```
Updating the property files with changed values, please
wait...
Reloading the changed property values into memory,
please wait...
```

- 18** Exit each level of the SESM configuration to eventually return to the root directory level by typing

**select - x**

and pressing the Enter key.

You have completed this procedure.

---

—End—

---

## Changing an expired root password on an SPFS-based server

### Application

Use this procedure to change the root password on a Server Platform Foundation Software (SPFS)-based server in the event that it has expired.

Perform this procedure when your root password failed with `su: Sorry.`

#### ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

### Prerequisites

Before you perform this procedure, ensure you entered the root password without the Caps Lock key on. Also ensure the password was not changed.

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

| Step | Action |
|------|--------|
|------|--------|

#### *At the server console*

- 1 Log in to the Active server through the console (port A) using the root user ID and the expired root password.
- 2 When prompted, enter the old (expired) password.
- 3 When prompted, enter a password of at least three characters.  
It is not recommended to set a password with an empty value. Use a minimum of three characters.
- 4 When prompted, enter the password again for verification.  
You have completed this procedure.

—End—



## Creating local and central restricted shell user accounts on an SPFS-based server

### Application

Use this procedure to create local and central restricted shell user accounts on a Server Platform Foundation Software (SPFS)-based server. Once the accounts are created, the restricted shell is used to perform non-administrative Command Line User Interface (CLUI) functions on the SPFS platform.

Users with restricted shell user accounts have a restricted command set with which to work. For information on the restricted command set, see ["Restricted command set" \(page 381\)](#).

A new package called NTRashell delivers and sets up the restricted shell on SPFS-based servers. Installation of the NTRashell package results in the following actions:

- linkage of the /usr/bin/rash to the rksh shell in the /usr/bin/rksh directory
- creation of a /etc/skell.rash directory for the default .profile and .login files
- creation of basebin and appbin directories in the /usr/rbin directory
- creation of symbolic links in the restricted access shell that execute all supported Solaris and SPFS commands
- delivery of the wrapped su command

If you want to create central restricted shell user accounts, refer to procedure 'Adding new users' in the Integrated Element Management System (IEMS) Security and Administration document, NN10336-611.

### Prerequisites

To perform this procedure, you need to have the root user ID and password to log in to the server.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- |   |                                                                                                            |
|---|------------------------------------------------------------------------------------------------------------|
| 1 | Log in to the Active server by typing<br><pre>&gt; telnet &lt;server&gt;</pre> and pressing the Enter key. |
|---|------------------------------------------------------------------------------------------------------------|

where

**server** is the IP address or host name of the SSFPS-based server

- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  
`$ su - root`  
 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Use the following table to determine your next step.

| If you are                                                               | Do     |
|--------------------------------------------------------------------------|--------|
| adding restricted shell access to a local user account                   | step 6 |
| registering restricted access shell executables one file at a time       | step 7 |
| registering restricted access shell executables by adding multiple files | step 8 |

- 6 Allow a local user access to the restricted shell and make *succssn* their primary user group by typing

```
useradd -g succssn -G mgcadm,emsadm -s
/usr/bin/rash -d /export/home/ <user id> -m -k
/etc/skel.rash <user id>
```

and pressing the Enter key.

where

**userid** is a variable for the user name

In the command above, the user's primary user group is *succssn* while the secondary groups are *mgcadm* and *emsadm*. Also, the shell was specified (*-s /usr/bin/rash*), the skeleton directory created (*-k /etc/skel.rash*), and a home directory set up (*-d /export/home/<user id>*). This home directory contains the contents of the skeleton directory including the user's profile with a list of the restricted bin directories the user can access.

If you are not a member of the *emsadm* or *secadm* groups, a message displays stating you do not have permission to execute the *su* command when you attempt to log in as root.

- 7 Register restricted access shell executables one at a time by typing



```
servman register -group newapp -rash
'<fullpath;name>'
```

and pressing the Enter key.

where

**<fullpath;name>** is the complete path to the executable file and the symbolic link name in the restricted shell bin directory you added in the step 6.

## 8 Register multiple restricted access shell executables by typing

```
servman register -group oldapp -rash
'<fullpath1;name*fullpath2;name2>'
```

and pressing the Enter key.

where

**<fullpath1;name\*fullpath2;name2>** is the complete path to the executable file and the symbolic link name in the restricted shell bin directory you added in the step 6. The wildcard character is used in this example to delimit the number of multiple files being added.

---

—End—

---

## Restricted command set

The restricted access shell is characterized by a limited command set. The limited command set is comprised of base-level and application-level commands.

Access to the shell's built-in commands remain functional for users with restricted shell accounts. Refer to the `shell_builtins` man page for a list of those commands, by typing `man shell_builtins` at a command prompt.

## Base-level commands

Base-level commands include Solaris resident commands and SPFS delivered commands. The base-level commands are listed in the following table:

| Command  | Comment/usage                                                                 |
|----------|-------------------------------------------------------------------------------|
| alias    | create or remove a pseudonym or shorthand for a command or series of commands |
| awk      | pattern scanning                                                              |
| basename | deliver portions of path names                                                |

| Command     | Comment/usage                                                                 |
|-------------|-------------------------------------------------------------------------------|
| cat         | concatenate and display files                                                 |
| cli         | SPFS command line interface (used mainly for configuration changes)           |
| cut         | cut out selected fields of each line of a file                                |
| df          | displays number of free disk blocks and files                                 |
| dirname     | deliver portions of path names                                                |
| gethostname | get or set name of current host                                               |
| grep        | search a file for a pattern                                                   |
| id          | return user identity                                                          |
| iostat      | report I/O statistics                                                         |
| ipcs        | report inter-process communication facilities status                          |
| kill        | terminate or signal processes                                                 |
| less        | browse or page through a text file                                            |
| ls          | list contents of directory                                                    |
| more        | browse or page through a text file                                            |
| netstat     | show network status                                                           |
| ping        | send ICMP (ICMP6) ECHO_REQUEST packets to network hosts                       |
| ps          | report process status                                                         |
| servquery   | query the status of SPFS applications                                         |
| sort        | sort, merge, or sequence check text files                                     |
| su          | wrapper that only allows users in group emsadm or secadm to access Solaris su |
| top         | provides system and process status                                            |
| head        | display the first few lines of a file                                         |
| tail        | display the last few lines of a file                                          |
| traceroute  | print the route that packets take to the network host                         |
| vmstat      | report virtual memory statistics                                              |

### Application-level commands

Application-level commands are listed in the following table:

| Command                                                       | Comment/usage                           |
|---------------------------------------------------------------|-----------------------------------------|
| npm                                                           | Network Path Manager (NPM) CLUI         |
| gwcad-min.sh                                                  | Gateway Controller Element Manager CLUI |
| bpt                                                           | Bulk Provisioning Tool (bpt)            |
| sam21em                                                       | SAM21 Element Manager CLUI              |
| SNMP Poller executables need not be provisioned at this time. |                                         |
| OMPUSH executables need not be provisioned at this time.      |                                         |

Currently, IEMS allows the servquery, -status all, swact, servstart IEMS, and init 6 commands to be executed on the SPFS element in an unrestricted shell when the user logs in as the root user using ssh. IEMS will continue to function in this manner for the (I)SN09 release.

## Querying the status of non-secure network services

This section describes the procedures to query the status of common, tool, and other non-secure network services (for example, ftp, telnet, time and daytime).

### Application

To enable or disable non-secure network services, refer to the procedures [Enabling non-secure network services](#) and [Disabling non-secure network services](#).

### Prerequisites

This procedure has no prerequisites.

### Action

Perform the following steps to complete this procedure.

| Step                       | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |          |    |                   |                        |              |                        |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----|-------------------|------------------------|--------------|------------------------|
| <b>At your workstation</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |          |    |                   |                        |              |                        |
| 1                          | Establish a login session to the server, using one of the following methods:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |          |    |                   |                        |              |                        |
|                            | <table border="1"> <thead> <tr> <th>If using</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>telnet (unsecure)</td> <td><a href="#">step 2</a></td> </tr> <tr> <td>ssh (secure)</td> <td><a href="#">step 3</a></td> </tr> </tbody> </table>                                                                                                                                                                                                                                                                                                                                                            | If using | Do | telnet (unsecure) | <a href="#">step 2</a> | ssh (secure) | <a href="#">step 3</a> |
| If using                   | Do                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |          |    |                   |                        |              |                        |
| telnet (unsecure)          | <a href="#">step 2</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |          |    |                   |                        |              |                        |
| ssh (secure)               | <a href="#">step 3</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |          |    |                   |                        |              |                        |
| 2                          | Log in to the SPFS-based server using telnet (unsecure) as follows: <ol style="list-style-type: none"> <li>Log in to the server by typing:<br/> <code>&gt;telnet &lt;server&gt;</code><br/>             and pressing the Enter key.<br/>             where<br/> <code>server</code><br/>             is the IP address or host name of the SPFS-based server</li> <li>When prompted, enter your user ID and password.</li> <li>Change to the root user by typing<br/> <code>\$ su - root</code><br/>             and pressing the Enter key.</li> <li>When prompted, enter the root password.</li> </ol> |          |    |                   |                        |              |                        |

e. Proceed to step 4.

**3** Log in to the SPFS-based server using SSH (secure) as follows:

- a. Log in to the server by typing  
`> ssh -l root <userid>`  
 and pressing the Enter key.

where

*server*

is the IP address or host name of the SPFS-based client server.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

- b. When prompted, enter the root password.

**4** Navigate to the Security Services Configuration menu within the command line interface as follows:

- a. Access the command line interface by typing  
`# cli`  
 and pressing the Enter key.

**Example response**

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - Exit
select -
```

- b. Enter the number next to the "Configuration" option in the menu.

**Example response**

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Configuration
5 - COBRA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Disk Drive Upgrade
```

```

16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - Exit
select -

```

- c. Enter the number next to the "Security Services Configuration" option in the menu.

#### Example response

```

Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp
and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -

```

- 5 Determine whether you choose to query the status of common services (for example, ftp and telnet), tools services (for example, time and daytime), or other services.

| To query        | Do      |
|-----------------|---------|
| common services | step 6  |
| tools services  | step 9  |
| other services  | step 12 |

- 6 Enter the number next to the "Common Inet Services (ftp, tftp, telnet, snmp and nfs)" option in the menu.

#### Example response

```

Common Inet Services (ftp, tftp, telnet, snmp and nfs)
1 - query_common_inetd (Services State Query)
2 - enable_common_inetd (Enable a service registered in
inetd.conf)
3 - disable_common_inetd (Disable a service registered
in inetd.conf)
x - exit

```

```
select -
```

- 7 Enter the number next to the “Query Common Inet (Services State Query)” option in the menu. The status of the common network services is displayed, as in the following example.

**Example response**

```
Common Inet Services States
0 - telnet Enabled
1 - ftp Enabled
2 - tftp Enabled
3 - snmp Disabled
4 - nfs_server Enabled
5 - nfs_client Enabled
=== | query_common_inetd | execution completed
```

- 8 Proceed to step 14.

- 9 Enter the number next to the “Tools Inet Services (time, daytime)” option in the menu.

**Example response**

```
Tools Inet Services (time, daytime)
1 - query_tool_inetd (Services State Query)
2 - enable_tool_inetd (Enable a service registered in
inetd.conf)
3 - disable_tool_inetd (Disable a service registered in
inetd.conf)
x - exit
select -
```

- 10 Enter the number next to the “Query tool inetd (Services State Query)” option in the menu. The status of the tools network services is displayed, as in the following example.

**Example response**

```
Toolnet Services States
0 - time Enabled
1 - daytime Enabled
=== | query_tool_inetd | execution completed
```

- 11 Proceed to step 14.

- 12 Enter the number next to the “Other Inet Services” option in the menu.

**Example response**

```
Other Inet Services
1 - query_tool_inetd (Services State Query)
2 - enable_tool_inetd (Enable a service registered in
inetd.conf)
```

```
3 - disable_tool_inetd (Disable a service registered in
inetd.conf)
x - exit
select -
```

- 13** Enter the number next to the “Quert tool inetd (Services State Query)” option in the menu. The status of other network services is displayed, as in the following example.

Only enabled services are displayed.

**Example response**

```
Other Inet Services States
0 - dtspc stream /usr/dt/bin/dtspcd
1 - 100134/1 tli /usr/lib/krb5/ktkt_warnd
2 - 100229/1-2 tli /usr/sbin/rpc.metad
3 - 100230/1 tli /usr/sbin/rpc.metamhd
4 - 100242/1 tli /usr/sbin/rpc.metamedd
5 - 100424/1 tli /usr/lib/ST/stfsloader
x - exit
select -
```

- 14** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

---

—End—

---



## Enabling non-secure network services

### Application

This section describes the procedures to query the status of common, tool, and other non-secure network services (for example, ftp, telnet, time and daytime).

Use this procedure to enable common, tool, and other non-secure network services (for example, ftp, telnet, time and daytime). To disable a non-secure network service, refer to the procedure [Disabling non-secure network services](#). To view the status of non-secure network services, refer to the procedure ["Querying the status of non-secure network services "](#) (page 384).

### Prerequisites

This procedure requires you to have root user privileges.

For CBM users, refer to the following prerequisites section.

#### Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access.

- You must be a user in a role group authorized to perform config-admin actions.
- You must obtain non-restricted shell access.

For CBM 850, root user ID and password are not required. You can use your own user ID in [step 1](#) in this procedure.

For more information on how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

*At your workstation*

- |   |                                                                                                                    |
|---|--------------------------------------------------------------------------------------------------------------------|
| 1 | Establish a connection to the active server through telnet or SSH, and log in using the root user ID and password. |
|---|--------------------------------------------------------------------------------------------------------------------|

- 2 Navigate to the Security Services Configuration menu within the command line interface as follows:

- a. Access the command line interface by typing

```
cli
```

and pressing the Enter key

*Example response*

```
Command Line Interface
```

```
1 - View
2 - Configuration
3 - Other
X - Exit
select -
```

- b. Enter the number next to the “Configuration” option in the menu.

*Example response*

```
Configuration
```

```
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Configuration
4 - COBRA Configuration
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - Exit
select -
```

- c. Enter the number next to the “Security Services Configuration” option in the menu.

*Example response*

```
Security Services Configuration
```

```
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
```

```

4 - Common Inet Services (ftp, tftp, telnet, snmp
and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -

```

The procedure to enable non-secure network services is the same regardless of whether you are disabling common, tools, or other services. The following procedure shows the steps required for the common services (Common Inet Services in the menu), although it also applies to the Tools Inet Services and Other Inet Services menu options.

- 3 Enter the number next to the “Common Inet Services (ftp, tftp, telnet, snmp and nfs)” option in the menu.

*Example response*

```

Common Inet Services (ftp, tftp, telnet, snmp and nfs)
1 - query_common_inetd (Services State Query)
2 - enable_common_inetd (Enable a service registered in
inetd.conf)
3 - disable_common_inetd (Disable a service registered
in inetd.conf)
x - exit
select -

```

- 4 Enter the number next to the “Enable Common Inetd (Enable a service registered in inetd.conf)” option in the menu.

*Example response*

```

=== Executing "enable_common_inetd"
Common Inet Services States
0 - telnet Disabled
1 - ftp Enabled
2 - tftp Enabled
3 - snmp Enabled
4 - nfs_server Enabled
5 - nfs_client Enabled
Select service number to enable [0-5]:

```

- 5 Enter the number next to the network service you wish to enable.

*Example response*

```

Operating system control files updated.
Operating system deamon re-initialized on mate.

```

```
=== "enable_common_inetd" execution completed
```

An audit log of services enabled using this procedure is maintained and stored in the file `/var/log/auditlog`.

- 6 If you choose to enable other network services, return to step 3. To confirm the service has been enabled, refer to the procedure ["Querying the status of non-secure network services "](#) (page 384).
- 7 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

---

—End—

---

## Disabling non-secure network services

### Application

Use this procedure to disable common, tool, and other non-secure network services (for example, ftp, telnet, time and daytime). To enable a non-secure network service, refer to the procedure [Enabling non-secure network services](#). To view the status of non-secure network services, refer to the procedure ["Querying the status of non-secure network services "](#) (page 384).

### Prerequisites

This procedure requires you to have root user privileges.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

*At your workstation*

- 1 Establish a login session to the server, using one of the following methods:

| If using          | Do     |
|-------------------|--------|
| telnet (unsecure) | step 2 |
| ssh (secure)      | step 3 |

- 2 Log in to the SPFS-based server using telnet (unsecure) as follows:

- a. Log in to the server by typing:

```
> telnet <server>
```

and pressing the Enter key

where

*server*

is the IP address or host name of the SPFS-based server

- b. When prompted, enter your user ID and password.
- c. Change to the root user by typing

```
$ su -root
```

and pressing the Enter key

- d. When prompted, enter the root password.
  - e. Proceed to step 4
- 3** Log in to the SPFS-based server using SSH (secure) as follows:
- a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key

where

*server*

is the IP address or host name of the SPFS-based client server.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.

- b. When prompted, enter the root password.

- 4** Navigate to the Security Services Configuration menu within the command line interface as follows:

- a. Access the command line interface by typing

```
cli
```

and pressing the Enter key

*Example response*

Command Line Interface

```
1 - View
2 - Configuration
3 - Other
X - Exit
select -
```

- b. Enter the number next to the “Configuration” option in the menu.

*Example response*

Configuration

```
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Configuration
4 - COBRA Configuration
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
```

```

11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - Exit
select -

```

- c. Enter the number next to the “Security Services Configuration” option in the menu.

*Example response*

```

=== Executing "enable_common_inetd"
Common Inet Services States
0 - telnet Disabled
1 - ftp Enabled
2 - tftp Enabled
3 - snmp Enabled
4 - nfs_server Enabled
5 - nfs_client Enabled
Select service number to enable [0-5]:

```

The procedure to disable non-secure network services is the same regardless of whether you are disabling common, tools, or other services. The following procedure shows the steps required for the common services (Common Inet Services in the menu), although it also applies to the Tools Inet Services and Other Inet Services menu options.

- 5 Enter the number next to the “Common Inet Services (ftp, tftp, telnet, snmp and nfs)” option in the menu.

*Example response*

```

Common Inet Services (ftp, tftp, telnet, snmp and nfs)
1 - query_common_inetd (Services State Query)
2 - enable_common_inetd (Enable a service registered in
inetd.conf)
3 - disable_common_inetd (Disable a service registered
in inetd.conf)
x - exit
select -

```

- 6 Enter the number next to the “Disable Common Inetd (Disable a service registered in inetd.conf)” option in the menu.

*Example response*

```

=== Executing "disable_common_inetd"
Common Inet Services States
0 - telnet Enabled
1 - ftp Enabled
2 - tftp Enabled
3 - snmp Enabled
4 - nfs_server Enabled
5 - nfs_client Enabled
Select service number to enable [0-5]:

```

- 7** Enter the number next to the network service you wish to disable.

*Example response*

```

Warning. This operation may affect other application(s
) or package(s) installed on the system.
There were no application/package registered for this
service.
Applications may still use this service without
registration.
Are you sure you want to proceed [yes/no]:

```

Disabling a network service takes effect immediately. Current sessions depending on the service are not affected, but all new sessions depending on the service will be rejected.

- 8** If you choose to abort disabling the network service, enter no at the prompt and return to step 5. If you choose to disable the selected service, enter yes at the prompt.

*Example response*

```

Operation confirmed by operator. Log will be
generated.
Operating system control files updated.
Operating system daemon re-initialized on mate.
=== "disable_common_inetd" execution completed

```

An audit log of services disabled using this procedure is maintained and stored in the file /var/log/auditlog.

- 9** If you choose to disable other network services, return to step 5. To confirm the service has been disabled, refer to the procedure ["Querying the status of non-secure network services "](#) (page 384).
- 10** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.



---

—End—

---

## Querying users defined in proftpd

### Application

Use this procedure to query the proftpd userlist and view their login group, default path, and password requirement.

### Prerequisites

This procedure has no prerequisites.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

*At your workstation*

- 1 Establish a login session to the server, using one of the following methods:

| If using          | Do     |
|-------------------|--------|
| telnet (unsecure) | step 2 |
| ssh (secure)      | step 3 |

- 2 Log in to the SPFS-based server using telnet (unsecure) as follows:

- a. Log in to the server by typing:

```
> telnet <server>
```

and pressing the Enter key

where

*server*

is the IP address or host name of the SPFS-based server

- b. When prompted, enter your user ID and password.

- c. Change to the root user by typing

```
$ su -root
```

and pressing the Enter key

- d. When prompted, enter the root password.

- e. Proceed to step 4

- 3 Log in to the SPFS-based server using SSH (secure) as follows:

- a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key

where

*server*

is the IP address or host name of the SPFS-based client server.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

- b. When prompted, enter the root password.

- 4 Navigate to the Security Services Configuration menu within the command line interface as follows:

Access the command line interface by typing

```
cli
```

and pressing the Enter key

*Example response*

```
Command Line Interface
```

```
1 - View
2 - Configuration
3 - Other
X - Exit
select -
```

- 5 Enter the number next to the “Configuration” option in the menu.

*Example response*

```
Configuration
```

```
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Configuration
4 - COBRA Configuration
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
```

```
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - Exit
select -
```

- 6** Enter the number next to the “Security Services Configuration” option in the menu.

*Example response*

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp and
nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

- 7** Enter the number next to the “proftpd User Configuration” option in the menu.

*Example response*

```
proftpd User Configuration
1 - query_proftpd_users (Query users defined
in proftpd)
2 - add_proftpd_user (Add a user to proftpd)
3 - add_dflt_GWC_anonymous_user (Restore the
GWC anonymous user)
4 - del_proftpd_user (Delete a given user
from proftpd)
5 - query_user_registry (Query the packages
registered for ftp users)
x - exit
select -
```

- 8** Enter the number next to the “query\_proftpd\_users (Query users defined in proftpd)” option in the menu.

*Example response*

```
== Executing "query_proftpd_users"
```

List of already defined users.

| Userid    | Groupid | Default_path          | Passwd_Reqr |
|-----------|---------|-----------------------|-------------|
| patcher   | other   | /data/npm/Au          | on          |
| certuser  | maint   | /export/home/certuser | off         |
| anonymous | maint2  | /data/swd             | off         |
| image     | other   | /var/opt/nortel/gwc   | on          |

=== "query\_proftpd\_users" execution completed

Other procedures exist to manage the list of proftpd users, including:

- Adding a user to proftpd
- Adding the default GWC anonymous user to proftpd
- Deleting a user from proftpd
- Querying the packages registered for ftp users

- 9** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

---

—End—

---

## Adding a User to Proftpd

### Application

Use this procedure to add and configure a user to proftpd.

### Prerequisites

This procedure requires you to have root user privileges.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

*At your workstation*

- 1 Establish a login session to the server, using one of the following methods:

| If using          | Do     |
|-------------------|--------|
| telnet (unsecure) | step 2 |
| ssh (secure)      | step 3 |

- 2 Log in to the SPFS-based server using telnet (unsecure) as follows:

- a. Log in to the server by typing:

```
> telnet <server>
```

and pressing the Enter key

where

*server*

is the IP address or host name of the SPFS-based server.

- b. When prompted, enter your user ID and password.
- c. Change to the root user by typing

```
$ su -root
```

and pressing the Enter key

- d. When prompted, enter the root password.
- e. Proceed to step 4

- 3 Log in to the SPFS-based server using SSH (secure) as follows:

- a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key

where

*server*

is the IP address or host name of the SPFS-based client server.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter the root password.

- 4 Navigate to the Security Services Configuration menu within the command line interface as follows:

Access the command line interface by typing

```
cli
```

and pressing the Enter key

*Example response*

```
Command Line Interface
```

```
1 - View
2 - Configuration
3 - Other
X - Exit
select -
```

- 5 Enter the number next to the “Configuration” option in the menu.

*Example response*

```
Configuration
```

```
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Configuration
5 - COBRA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
```

```
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - Exit
select -
```

- 6** Enter the number next to the “Security Services Configuration” option in the menu.

*Example response*

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp and
nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

- 7** Enter the number next to the “proftpd User Configuration” option in the menu.

*Example response*

```
proftpd User Configuration
1 - query_proftpd_users (Query users defined
in proftpd)
2 - add_proftpd_user (Add a user to proftpd)
3 - add_dflt_GWC_anonymous_user (Restore the
GWC anonymous user)
4 - del_proftpd_user (Delete a given user
from proftpd)
5 - query_user_registry (Query the packages
registered for ftp users)
x - exit
select -
```

- 8** Enter the number next to the “add\_proftpd\_user (Add a user to proftpd)” option in the menu

*Example response*

```
== Executing "add_proftpd_users"
```



List of already defined users.

| Userid    | Groupid | Default_path          | Passwd_Reqr |
|-----------|---------|-----------------------|-------------|
| patcher   | other   | /data/npm/Au          | on          |
| certuser  | maint   | /export/home/certuser | off         |
| anonymous | other   | /var/opt/nortel/gwc   | on          |
| image     | maint2  | /data/swd             | off         |

Please enter default user path (path must exists):

- 9** Enter the default path, such as **/tmp** at the prompt and press the Enter key.

*Example response*

Please enter user\_id:

- 10** Enter the user ID, for example, **bloggsj** at the prompt and press the Enter key.

*Example response*

Please enter user\_id:

- 11** Enter the user's group ID, for example, **maint2** at the prompt and press the Enter key.

*Example response*

Are there aliases for user bloggsj

<aliases separated by space/enter for none>:

- 12** Enter any aliases for the user ID entered in step 10, separated by spaces. Press the enter key when you have finished entering aliases, or if none exist.

*Example response*

Is password required for bloggsj in group maint2 (y/n):



### CAUTION

*It is strongly recommended that a password be applied to all ftp accounts in order to comply with your relevant security policies and guidelines. Creating an ftp account without a password is the equivalent to creating an anonymous ftp account and should be avoided at all times.*

- 13** Determine whether a password is required for this new user, and enter y or n appropriately followed by the Enter key.

*Example response*

User is defined locally or centrally

*Example response*

When a user does not exist on the system You need to do: `useradd -g maint2 bloggsj`

- 14** If example response 1 is shown (that is, the user is already defined locally or centrally), skip to step 16.
- 15** Enter **y** at the prompt to add the new user to the system (necessary prior to adding the proftpd account)
- If you enter **n** at this prompt, the user may not have access until the account is defined.
- 16** Depending on whether you requested a password for this account in step 12, proceed as follows:

| If                             | Do      |
|--------------------------------|---------|
| you requested a password       | step 17 |
| you did not request a password | step 18 |

- 17** The system prompts you to enter the user's new password twice.

*Example response*

Enter user password:  
Re-enter user password:

Enter the password twice, once at each prompt.

- 18** *Example response*  
Is default path read only (y/n):

- 19** Determine whether to choose the default path to be read only, and enter **y** or **n** appropriately, followed by the Enter key.

*Example response*

Is default path write only (y/n):

- 20** Determine whether to choose the default path to be write only, and enter **y** or **n** appropriately, followed by the Enter key.

*Example response*

Is user allowed to change directory (y/n):

- 21** Determine whether to choose the user to be able to change directory to that other than the default directory and enter **y** or **n** appropriately, followed by the Enter key.

*Example response*

Is user allowed to create/delete dir (y/n):

- 22** Determine whether to choose the user to be able to create and delete directories and enter **y** or **n** appropriately, followed by the Enter key.

*Example response*

Is user allowed to delete files (y/n):

- 23** Determine whether to choose the user to be able to delete files and enter **y** or **n** appropriately, followed by the Enter key.

*Example response*

Is user allowed to rename files (y/n):

- 24** Determine whether to choose the user to be able to rename files and enter **y** or **n** appropriately, followed by the Enter key.

*Example response*

User attributes entered were:  
 UID:bloggsj GID:maint2 Path:/tmp  
 Alias(es) for bloggsj:  
 File system attributes:  
 READonly:NO WRITEonly:NO  
 CHANGEDir:NO ADD/DEL\_dir:NO  
 DEL\_file:YES RENAME\_file:YES  
 Proceed with current user attributes (y/n):y

- 25** Confirm the summary of your request is correct, and proceed as follows:

| If                             | Do                      |
|--------------------------------|-------------------------|
| the information is not correct | step <a href="#">26</a> |
| the information is correct     | step <a href="#">29</a> |

- 26** Enter **n** at the prompt, and press the Enter key.

*Example response*

Do you want to re-enter the values (y/n):

- 27** If you choose to re-enter the values, enter **y** and press the Enter key. Return to step 9.
- 28** If you do not choose to re-enter the values, and instead choose to cancel the creation of this proftpd user account, enter **n** and press the Enter key. Either return to step 8 to start again and add a different proftpd user account, or skip to step [31](#) to end this procedure.
- 29** Enter **y** at the prompt, and press the Enter key. The system creates the proftpd user account.

*Example response*

```
=== "add_proftpd_user " execution completed
```

- 30** If you choose to add other proftpd user accounts, return to step 8.
- 31** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

---

—End—

---

## Adding the default GWC anonymous user to proftpd

### Application

Use this procedure to add the default GWC anonymous user account to proftpd. The anonymous user account has the following configuration:

- username: anonymous
- Usergroup: maint2
- Default directory: /data/swd
- Require password: no
- File access: read only

### Prerequisites

This procedure requires you to have root user privileges.

### Action

Perform the following steps to complete this procedure.

| Step                       | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |          |    |                   |        |              |        |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----|-------------------|--------|--------------|--------|
| <b>At your workstation</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |          |    |                   |        |              |        |
| 1                          | Establish a login session to the server, using one of the following methods:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |          |    |                   |        |              |        |
|                            | <table border="1"> <thead> <tr> <th>If using</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>telnet (unsecure)</td> <td>step 2</td> </tr> <tr> <td>ssh (secure)</td> <td>step 3</td> </tr> </tbody> </table>                                                                                                                                                                                                                                                                                                                                                     | If using | Do | telnet (unsecure) | step 2 | ssh (secure) | step 3 |
| If using                   | Do                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |          |    |                   |        |              |        |
| telnet (unsecure)          | step 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |          |    |                   |        |              |        |
| ssh (secure)               | step 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |          |    |                   |        |              |        |
| 2                          | Log in to the SPFS-based server using telnet (unsecure) as follows: <ol style="list-style-type: none"> <li>a. Log in to the server by typing:<br/> <code>&gt;telnet &lt;server&gt;</code><br/>             and pressing the Enter key.<br/>             where<br/> <code>server</code><br/>             is the IP address or host name of the SPFS-based server.</li> <li>b. When prompted, enter your user ID and password.</li> <li>c. Change to the root user by typing<br/> <code>\$ su - root</code><br/>             and pressing the Enter key.</li> </ol> |          |    |                   |        |              |        |

- d. When prompted, enter the root password.
  - e. Proceed to step 4.
- 3** Log in to the SPFS-based server using SSH (secure) as follows:
- a. Log in to the server by typing  
    `> ssh -l root <server>`  
    and pressing the Enter key.  
  
    where  
  
    server  
  
    is the IP address or host name of the SPFS-based client server.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

- b. When prompted, enter the root password.
- 4** Navigate to the Security Services Configuration menu within the command line interface as follows:
- a. Access the command line interface by typing  
    `# cli`  
    and pressing the Enter key.

*Example response*

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - Exit
select -
```

- 5** Enter the number next to the “Configuration” option in the menu.

*Example response*

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Configuration
5 - COBRA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
```

```

14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - Exit
select -

```

- 6** Enter the number next to the “Security Services Configuration” option in the menu.

*Example response*

```

Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp and
nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -

```

- 7** Enter the number next to the “proftpd User Configuration” option in the menu.

*Example response*

```

Security User Configuration
1 - query_proftpd_users (Query users defined
in proftpd)
2 - add_proftpd_user (Add a user to proftpd)
3 - add_dflt_GWC_anonymous_user (Restore the
GWC anonymous user)
4 - del_proftpd_user (Delete a given user
from proftpd)
5 - query_user_registry (Query the packages
registered for ftp users)
x - exit
select -

```

- 8** Enter the number next to the “add\_dflt\_GWC\_anonymous\_user (Restore the GWC anonymous user)” option in the menu.

*Example response*

```
=== Executing "add_dflt_GWC_anonymous_user"
```

```
List of already defined users
```

| Userid   | Groupid | Default_path              | Passwd_Reqr |
|----------|---------|---------------------------|-------------|
| patcher  | other   | /data/npm/Au              | on          |
| certuser | maint   | /export/home/cer<br>tuser | off         |
| image    | other   | /var/opt/nortel/<br>gwc   | on          |

```
=== "add_dflt_GWC_anonymous_user" execution completed
```

- 9** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

---

—End—

---



## Deleting a user from proftpd

### Application

Use this procedure to delete an existing user from proftpd.

### Prerequisites

This procedure requires you to have root user privileges.

### Action

Perform the following steps to complete this procedure.

| Step                       | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |          |    |                   |        |              |        |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----|-------------------|--------|--------------|--------|
| <b>At your workstation</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |          |    |                   |        |              |        |
| 1                          | Establish a login session to the server, using one of the following methods:                                                                                                                                                                                                                                                                                                                                                                                                                                      |          |    |                   |        |              |        |
|                            | <table border="1"> <thead> <tr> <th>If using</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>telnet (unsecure)</td> <td>step 2</td> </tr> <tr> <td>ssh (secure)</td> <td>step 3</td> </tr> </tbody> </table>                                                                                                                                                                                                                                                                                                     | If using | Do | telnet (unsecure) | step 2 | ssh (secure) | step 3 |
| If using                   | Do                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |          |    |                   |        |              |        |
| telnet (unsecure)          | step 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |          |    |                   |        |              |        |
| ssh (secure)               | step 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |          |    |                   |        |              |        |
| 2                          | Log in to the SPFS-based server using telnet (unsecure) as follows:                                                                                                                                                                                                                                                                                                                                                                                                                                               |          |    |                   |        |              |        |
|                            | <ol style="list-style-type: none"> <li>Log in to the server by typing:<br/> <code>&gt;telnet &lt;server&gt;</code><br/> and pressing the Enter key.<br/> where<br/> <code>server</code><br/> is the IP address or host name of the SPFS-based server.</li> <li>When prompted, enter your user ID and password.</li> <li>Change to the root user by typing<br/> <code>\$ su - root</code><br/> and pressing the Enter key.</li> <li>When prompted, enter the root password.</li> <li>Proceed to step 4.</li> </ol> |          |    |                   |        |              |        |
| 3                          | Log in to the SPFS-based server using SSH (secure) as follows:                                                                                                                                                                                                                                                                                                                                                                                                                                                    |          |    |                   |        |              |        |
|                            | <ol style="list-style-type: none"> <li>Log in to the server by typing<br/> <code>&gt; ssh -l root &lt;server&gt;</code><br/> and pressing the Enter key.</li> </ol>                                                                                                                                                                                                                                                                                                                                               |          |    |                   |        |              |        |

where

server

is the IP address or host name of the SPFS-based client server.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter the root password.

- 4 Navigate to the Security Services Configuration menu within the command line interface as follows:

- a. Access the command line interface by typing

```
cli
```

and pressing the Enter key.

*Example response*

```
Command Line Interface
```

```
1 - View
```

```
2 - Configuration
```

```
3 - Other
```

```
X - Exit
```

```
select -
```

- 5 Enter the number next to the "Configuration" option in the menu.

*Example response*

```
Configuration
```

```
1 - NTP Configuration
```

```
2 - Apache Proxy Configuration
```

```
3 - DCE Configuration
```

```
4 - OAMP Configuration
```

```
5 - COBRA Configuration
```

```
6 - IP Configuration
```

```
7 - DNS Configuration
```

```
8 - Syslog Configuration
```

```
9 - Remote Backup Configuration
```

```
10 - Database Configuration
```

```
11 - NFS Configuration
```

```
12 - Bootp Configuration
```

```
13 - Restricted Shell Configuration
```

```
14 - Security Services Configuration
```

```
15 - Disk Drive Upgrade
```

```
16 - Login Session
```

```
17 - Location Configuration
```

```
18 - Cluster Configuration
```

```
19 - Succession Element Configuration
```

```
20 - snmp_poller (SNMP Poller Configuration)
```

```
21 - backup_config (Backup Configuration)
```

```
X - Exit
```

select -

- 6 Enter the number next to the "Security Services Configuration" option in the menu.

*Example response*

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp and
nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

- 7 Enter the number next to the "proftpd User Configuration" option in the menu.

*Example response*

```
Security User Configuration
1 - query_proftpd_users (Query users defined
in proftpd)
2 - add_proftpd_user (Add a user to proftpd)
3 - add_dflt_GWC_anonymous_user (Restore the
GWC anonymous user)
4 - del_proftpd_user (Delete a given user
from proftpd)
5 - query_user_registry (Query the packages
registered for ftp users)
x - exit
select -
```

- 8 Enter the number next to the "del\_proftpd\_user (Delete a given user from proftpd)" option in the menu.

*Example response*

```
=== Executing "del_proftpd_user"
List of already defined users
```

| Userid   | Groupid | Default_path          | Passwd_Reqr |
|----------|---------|-----------------------|-------------|
| patcher  | other   | /data/npm/Au          | on          |
| certuser | maint   | /export/home/certuser | off         |

| Userid    | Groupid | Default_path        | Passwd_Reqr |
|-----------|---------|---------------------|-------------|
| anonymous | maint2  | /data/swd           | off         |
| image     | other   | /var/opt/nortel/gwc | on          |

```
=== "add_dflt_GWC_anonymous_user" execution completed
```

- 9** Enter the userID of the user to be deleted from proftpd at the prompt, and press the Enter key.

*Example response*

```
Please enter group_id:
```

- 10** Enter the GroupID associated with the UserID you are deleting, and press the Enter key

*Example response*

```
Deleting ftp users may affect application(s) internal
or external to this server.
```

```
Are you sure you want to delete anonymous maint2 (y/n):
```

- 11** Confirm you wish to delete the selected user.

| If                                 | Do                      |
|------------------------------------|-------------------------|
| you do not wish to delete the user | step <a href="#">12</a> |
| you wish to delete the user        | step <a href="#">13</a> |

- 12** At the prompt, enter **n**, and press the Enter key.

*Example response*

```
User delete aborted.
```

```
=== "del_proftpd_user" execution completed
```

Skip to step [14](#).

- 13** At the prompt, enter **y** to confirm you wish to delete the user, and press the Enter key.

*Example response*

```
Target user: anonymous
```

```
Target group: maint2
```

```
Preserved configuration file.
```

```
Updated configuration file.
```

```
Configuration successful.
```

```
Successfully deleted anonymous maint2.
```

- 14** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

---

**—End—**

---

## Querying the packages registered for ftp users

### Application

Use this procedure to query the packages/applications registered for proftpd users.

### Prerequisites

This procedure has no prerequisites.

### Action

Perform the following steps to complete this procedure.

| Step                       | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |          |    |                   |        |              |        |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----|-------------------|--------|--------------|--------|
| <b>At your workstation</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |          |    |                   |        |              |        |
| 1                          | Establish a login session to the server, using one of the following methods:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |          |    |                   |        |              |        |
|                            | <table border="1"> <thead> <tr> <th>If using</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>telnet (unsecure)</td> <td>step 2</td> </tr> <tr> <td>ssh (secure)</td> <td>step 3</td> </tr> </tbody> </table>                                                                                                                                                                                                                                                                                                                                                                                                                         | If using | Do | telnet (unsecure) | step 2 | ssh (secure) | step 3 |
| If using                   | Do                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |          |    |                   |        |              |        |
| telnet (unsecure)          | step 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |          |    |                   |        |              |        |
| ssh (secure)               | step 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |          |    |                   |        |              |        |
| 2                          | Log in to the SPFS-based server using telnet (unsecure) as follows: <ol style="list-style-type: none"> <li>Log in to the server by typing:<br/> <code>&gt;telnet &lt;server&gt;</code><br/>             and pressing the Enter key.<br/>             where<br/> <code>server</code><br/>             is the IP address or host name of the SPFS-based server.</li> <li>When prompted, enter your user ID and password.</li> <li>Change to the root user by typing<br/> <code>\$ su - root</code><br/>             and pressing the Enter key.</li> <li>When prompted, enter the root password.</li> <li>Proceed to step 4.</li> </ol> |          |    |                   |        |              |        |
| 3                          | Log in to the SPFS-based server using SSH (secure) as follows: <ol style="list-style-type: none"> <li>Log in to the server by typing<br/> <code>&gt; ssh -1 root &lt;server&gt;</code></li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                     |          |    |                   |        |              |        |

and pressing the Enter key.

where

*server*

is the IP address or host name of the SPFS-based client server.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter the root password.

**4** Navigate to the Security Services Configuration menu within the command line interface as follows:

a. Access the command line interface by typing

```
cli
```

and pressing the Enter key.

*Example response*

```
Command Line Interface
```

```
1 - View
```

```
2 - Configuration
```

```
3 - Other
```

```
X - Exit
```

```
select -
```

**5** Enter the number next to the “Configuration” option in the menu.

*Example response*

```
Configuration
```

```
1 - NTP Configuration
```

```
2 - Apache Proxy Configuration
```

```
3 - DCE Configuration
```

```
4 - OAMP Configuration
```

```
5 - COBRA Configuration
```

```
6 - IP Configuration
```

```
7 - DNS Configuration
```

```
8 - Syslog Configuration
```

```
9 - Remote Backup Configuration
```

```
10 - Database Configuration
```

```
11 - NFS Configuration
```

```
12 - Bootp Configuration
```

```
13 - Restricted Shell Configuration
```

```
14 - Security Services Configuration
```

```
15 - Disk Drive Upgrade
```

```
16 - Login Session
```

```
17 - Location Configuration
```

```
18 - Cluster Configuration
```

```
19 - Succession Element Configuration
```

```
20 - snmp_poller (SNMP Poller Configuration)
```

```
21 - backup_config (Backup Configuration)
X - Exit
select -
```

- 6** Enter the number next to the “Security Services Configuration” option in the menu.

*Example response*

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp and
nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

- 7** Enter the number next to the “proftpd User Configuration” option in the menu.

*Example response*

```
Security User Configuration
1 - query_proftpd_users (Query users defined
in proftpd)
2 - add_proftpd_user (Add a user to proftpd)
3 - add_dflt_GWC_anonymous_user (Restore the
GWC anonymous user)
4 - del_proftpd_user (Delete a given user
from proftpd)
5 - query_user_registry (Query the packages
registered for ftp users)
x - exit
select -
```

- 8** Enter the number next to the “query\_user\_registry (Query the packages registered for ftp users)” option in the menu.

*Example response*

```
=== Executing "query_user_registry"
Package(s) registered for ftp user(s)
```



Table may be empty if no package has registered.

| <b>Userid</b> | <b>Groupid</b> | <b>Package</b>   |
|---------------|----------------|------------------|
| anonymous     | maint2         | BootP GWC loader |

=== "add\_dflt\_GWC\_anonymous\_user" execution completed

- 9** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

select - x

and pressing the Enter key.

You have completed this procedure.

---

—End—

---

## Installing an initial WebPKProxy Certificate

### Application

Use this procedure to perform an initial installation of a WebPKProxy certificate supplied by the Certificate Manager for Apache and Tomcat on the application client box.

### Prerequisites

This procedure has the following prerequisites:

- Ensure a certificate has been produced for the application client box by first following the procedure, Generating WEBPKPROXY certificates.
- You know the root password on the application client box.
- You have a login username and password combination with secadm group access on the Certificate Manager server.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

**1** Establish a connection to the application client box through telnet or SSH, and log in using the root user ID and password. For detailed steps, refer to procedure "Logging in to an SPFS-based server".

**2** Change to the certificates directory by typing

```
cd /data/pkclient/certificates
```

and press the Enter key.

**3** Confirm you are in the correct directory by typing

```
pwd
```

and press the Enter key.

*Example response*

```
/data/pkclient/certificates
```

**4** Ensure the directory is empty by typing

```
ls -l
```

*Example response*

```
total 0
```

- 5 If the directory is not empty, delete the files by typing

```
rm *
```

and press the Enter key.

- 6 Issue the following command and make a note of the output. You will require this information in a later step.

```
hostname
```

and press the Enter key.

*Example response*

```
ucars0063c
```

- 7 Proceed with this procedure as follows:

| If hostname discovered in step 6                                                     | Do      |
|--------------------------------------------------------------------------------------|---------|
| is the same as the Certificate Manager hostname (that is, on the same machine)       | step 8  |
| is not the same as the Certificate Manager hostname (that is, on different machines) | step 10 |

- 8 Copy the certificates exported by the PKGUI Public Key Manager by typing the following three commands

```
cp /data/NTPkmgr/cert/export/CA* .
cp /data/NTPkmgr/cert/export/TRUSTED_Cert* .
cp /data/NTPkmgr/cert/export/<hostname>* .
```

where

*hostname*

is the hostname of the application client box, as discovered in step 6.

- 9 Proceed to step 11.

- 10 Use secure FTP to retrieve the WebPKProxy certificates from the Certificate Manager server by typing the following at the command prompt:

If this is the first time you have used secure FTP, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

You will be prompted for a password for the account used after each of the sftp commands.

```
sftp <username>@<ip address>:/data/NTPkmgr/cert/expo
rt/CA* .
sftp <username>@<ip address>:/data/NTPkmgr/cert/export/
TRUSTED_Cert* .
sftp <username>@<ip address>:/data/NTPkmgr/cert/expor
t/<hostname>* .
```

where

*username*

is the user name of an account on the Certificate Manager box with secadm group privileges.

*ip address*

is the IP address of the Certificate Manager server.

*hostname*

is the hostname of the application client box, as discovered in step 6.

- 11** Confirm five files have been successfully copied and check the permissions of the files by typing

```
ls -l
```

and pressing the Enter key.

*Example response*

```
-rwxr-x--- 1 root other 1603 Feb 6 11:00 CA1_Cert.pem
-rwxr-x--- 1 root other 1603 Feb 6 11:00 CA2_Cert.pem
-rwxr-x--- 1 root other 1522 Feb 6 11:00 TRUSTED_Cert.pem
-rwxr-x--- 1 root other 1522 Feb 6 11:00
ucars0063c.mycompany.com_Cert.pem
-rwxr-x--- 1 root other 1278 Feb 6 11:00
ucars0063c.mycompany.com_Key.pem
```

- 12** Navigate to the Security Services Configuration menu within the command line interface as follows:

- a. Access the command line interface by typing

```
cli
```

and pressing the Enter key.

*Example response*

```
Command Line Interface
```

```
1 - View
```

```
2 - Configuration
```

```
3 - Other
```

```
X - Exit
select -
```

- b. Enter the number next to the “Configuration” option in the menu.

**Example response**

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Configuration
4 - COBRA Configuration
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - Exit
select -
```

- c. Enter the number next to the “Security Services Configuration” option in the menu.

**Example response**

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp
and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

- 13** Enter the number next to the “PKManager Certificate Installation” option in the menu.

*Example response*

```
PKManager Certificate Installation
1 - install_certs (Install Certificates supplied by
PKManager)
x - exit
select -
```

- 14**



**CAUTION**

Installing certificates will restart the webserver.

Any clients using the webserver will lose their connection.

Enter the number next to the “install\_certs (Install Certificates supplied by PKManager)” option in the menu. Confirm the output does not produce any errors, and is similar to that shown in this step. If errors are shown, contact your next level of support.

*Example response*

```
=== Executing "install_certs"
Stopping group using servstop
Apache Web Service Stopping
WEBSERVER Stopped
Stopping group using servstop
 PID TTY TIME CMD
 19956 ? 1:37 java
 PID TTY TIME CMD
 19956 ? 1:37 java
 PID TTY TIME CMD
 19956 ? 1:37 java
 PID TTY TIME CMD
 19956 ? 1:37 java
 PID TTY TIME CMD
 19956 ? 1:37 java
 PID TTY TIME CMD
 19956 ? 1:37 java
 PID TTY TIME CMD
 19956 ? 1:37 java
WEBSERVICES Stopped
Stopping group using servstop
WEBSERVER Stopped
Starting WEBSERVER through servstart
Found valid security certificate, starting Web Services
with SSL support... Apache Web Service Starting
WEBSERVER Started Key import successful. Stopping
group using servstop
 PID TTY TIME CMD
```

```
WEBSERVICES Stopped
Starting WEBSERVICES through servstart
WEBSERVICES Started
Certificates have been updated.
=== "install_certs" execution completed
```

- 15** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

- 16** You must now register which machine will act as the Certificate Manager. To perform this step, refer to the procedure "WebPKProxy registration".

---

—End—

---

## Installing a WEBPKPROXY certificate to clear PKM306 alarm

### Application

Use this procedure to replace and install a new WebPKProxy certificate supplied by the PKManager for Apache and Tomcat on the application client box.

### Prerequisites

This procedure has the following prerequisites:

- A new certificate has been supplied automatically by the Certificate Manager and a PKM306 log was generated.
- You know the root password on the application client box.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Establish a connection to the application client box through telnet or SSH, and log in using the root user ID and password. For detailed steps, refer to procedure "Logging in to an SPFS-based server".

- 2 Change to the certificates directory and confirm by typing

```
cd /data/pkclient/certificates
pwd
```

#### *Example response*

```
/data/pkclient/certificates
```

- 3 Ensure the necessary files are present in this directory by first typing

```
ls -l
```

#### *Example response*

```
-rwxr-x--- 1 root other 1603 Feb 3 10:06 CA1_Cert.pem
-rwxr-x--- 1 root other 1603 Feb 3 10:06 CA2_Cert.pem
-rw-r--r-- 1 root other 4728 Feb 3 11:12 cert.bundle
-rw-r--r-- 1 root other 925 Feb 3 11:12 key.pkcs8
-rw-r--r-- 1 root other 4452 Feb 3 11:12 pkclientKeystore
```



```

-rwxr-x--- 1 root other 1522 Feb 3 10:06 TRUSTED_Cert.pem
-rwxr-x--- 1 root other 1522 Feb 3 10:06
<hostname>.<domain>_Cert.pem
-rwxr-x--- 1 root other 1278 Feb 3 10:06
<hostname>.<domain>_Key.pem

```

where

*hostname*

is the hostname of the current device.

*domain*

is the configured domain of the organization.

- 4 Verify the certificate active date and time listed in the Certificate Manager is earlier than the date and time stamp of the certificate files listed in step 3. If they are not, contact your next level of support.

- 5 Confirm that the following files are present. If not, contact your next level of support.

- key.pkcs8
- pkclientKeystore

- 6 Navigate to the Security Services Configuration menu within the command line interface as follows:

- a. Access the command line interface by typing

```
cli
```

and pressing the Enter key.

*Example response*

```
Command Line Interface
```

```
1 - View
2 - Configuration
3 - Other
X - Exit
select -
```

- b. Enter the number next to the “Configuration” option in the menu.

*Example response*

```
Configuration
```

```
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Configuration
4 - COBRA Configuration
5 - IP Configuration
```

```
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - Exit
select -
```

- c. Enter the number next to the “Security Services Configuration” option in the menu.

*Example response*

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp
and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

- 7 Enter the number next to the “PKManager Certificate Installation” option in the menu.

*Example response*

```
PKManager Certificate Installation
1 - install_certs (Install Certificates supplied by
PKManager)
x - exit
select -
```

8

**CAUTION****Installing certificates will restart the webserver.**

Any clients using the webserver will loose their connection.

Enter the number next to the “install\_certs (Install Certificates supplied by PKManager)” option in the menu. Confirm the output does not produce any errors, and is similar to that shown in this step.

*Example response*

```

=== Executing "install_certs"
Stopping group using servstop
Apache Web Service Stopping
WEBSERVER Stopped
Stopping group using servstop
 PID TTY TIME CMD
 19956 ? 1:37 java
 PID TTY TIME CMD
 19956 ? 1:37 java
 PID TTY TIME CMD
 19956 ? 1:37 java
 PID TTY TIME CMD
 19956 ? 1:37 java
 PID TTY TIME CMD
 19956 ? 1:37 java
 PID TTY TIME CMD
 19956 ? 1:37 java
 PID TTY TIME CMD
 19956 ? 1:37 java
WEBSERVICES Stopped
Stopping group using servstop
WEBSERVER Stopped
Starting WEBSERVER through servstart
Found valid security certificate, starting Web Services
with SSL support... Apache Web Service Starting
WEBSERVER Started Key import successful. Stopping
group using servstop
 PID TTY TIME CMD
WEBSERVICES Stopped
Starting WEBSERVICES through servstart
WEBSERVICES Started
Certificates have been updated.
=== "install_certs" execution completed

```

9

Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

- 10 You must now register which machine will act as the Certificate Manager. Refer to the procedure "WebPKProxy registration" in order to finish the certificate installation.

---

—End—

---

## WEBPKPROXY registration

### Application

Use this procedure to register WEBPKPROXY and PKClient with the Certificate Manager.

### Prerequisites

This procedure has the following prerequisites:

- Either the Installing an initial WebPKProxy certificate procedure or the Replacing a WebPKProxy certificate procedure has been executed.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 If you are already logged in to the application client box as the root user, proceed to step 3, otherwise proceed to step 2.
- 2 Establish a connection to the application client box through telnet or SSH, and log in using the root user ID and password. For detailed steps, refer to procedure Logging in to an SPFS-based server.
- 3 Change to the certificates directory and confirm by typing  

```
cd /data/pkclient/certificates
pwd
```

#### *Example response*

```
/data/pkclient/certificates
```

- 4 Ensure the necessary files are present in this directory by first typing  

```
ls -l
```

#### *Example response*

```
-rwxr-x--- 1 root other 1603 Feb 3 10:06 CA1_Cert.pem
-rwxr-x--- 1 root other 1603 Feb 3 10:06 CA2_Cert.pem
-rw-r--r-- 1 root other 4728 Feb 3 11:12 cert.bundle
-rw-r--r-- 1 root other 925 Feb 3 11:12 key.pkcs8
-rw-r--r-- 1 root other 4452 Feb 3 11:12 pkclientKeystore
-rwxr-x--- 1 root other 1522 Feb 3 10:06 TRUSTED_Cert.pem
```

```
-rwxr-x--- 1 root other 1522 Feb 3 10:06
<hostname>.<domain>_Cert.pem
-rwxr-x--- 1 root other 1278 Feb 3 10:06
<hostname>.<domain>_Key.pem
```

where

*hostname*

is the hostname of the current device

*domain*

is the configured domain of the organization

- 5 Confirm that the following files are present. If not, contact your next level of support.
  - key.pkcs8
  - pkclientKeystore
- 6 Wait 10 minutes to ensure the Java application has finished installing the certificate.
- 7 Navigate to the Security Services Configuration menu within the command line interface as follows:
  - a. Access the command line interface by typing

```
cli
```

and pressing the Enter key.

*Example response*

Command Line Interface

```
1 - View
2 - Configuration
3 - Other
X - Exit
select -
```

- b. Enter the number next to the “Configuration” option in the menu.

*Example response*

Configuration

```
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Configuration
4 - COBRA Configuration
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
```

```

9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - Exit
select -

```

- c. Enter the number next to the “Security Services Configuration” option in the menu.

*Example response*

```

Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp
and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -

```

- 8 Enter the number next to the “WebPKProxy/PKClient Configuration” option in the menu.

*Example response*

```

WebPKProxy/PKClient Configuration
1 - register_pkclient (Register
WebPKProxy/PKClient with PKManager)
x - exit
select -

```

- 9 Enter the number next to the “register\_pkclient (Register WebPKProxy/PKClient with PKManager)” option in the menu.

*Example response*

```

=== Executing "register_pkclient"
Enter the hostname of where PKManger is installed?

```

- 10** At the prompt, enter the hostname of where the Certificate Manager is installed and press the Enter key.

The Certificate Manager must be fully functional or this step will fail.
- 11** Wait for the script to finish, and verify no errors or warnings were seen.
- 12** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.
- 13** Verify that the PKM306 alarm has been cleared for this server. If the PKM306 alarm is not cleared, contact your next level of support.

You have completed this procedure.

---

—End—

---



## Setting the Oracle Listener password on an SPFS-based server

### Application

The Oracle Listener requires a password to perform most operations within the listener interactive command prompt. A password is required to perform operations such as stop or services. This procedure demonstrates how to specify your current password.

When the system is installed, the default Oracle Listener password is set to 'oracle'. To change this default password, use procedure "[Setting the Oracle Listener password on an SSPFS-based server](#)" (page 437)

#### ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the Active server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server** is the IP address or host name of the SPFS-based server

In a two-server configuration, log in to the active server using its physical IP address.

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the Oracle Listener application by typing

```
lsnrctl
```

and pressing the Enter key.

*Example response*

```
Welcome to LSNRCTL, type "help" for information.
LSNRCTL>
```

6 Initiate the password setting by typing

```
LSNRCTL> set password
```

and pressing the Enter key.

*Example response*

```
Password:
```

7 Type your current password at the prompt and press the Enter key.

*Example response*

```
The command completed successfully
```

8 Exit the Oracle Listener application by typing

```
LSNRCTL> quit
```

and pressing the Enter key.

You have completed this procedure.

---

—End—

---

## Changing the Oracle Listener password on an SPFS-based server

### Application

The default password for the Oracle Listener is set to oracle during the installation of the Server Platform Foundation Software (SPFS). This procedure provides the steps to change the Oracle Listener password on an SPFS-based server.

#### ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

#### Step Action

##### *At your workstation*

- 1 Log in to the Active server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
**server** is the IP address or host name of the SPFS-based server  
 In a two-server configuration, log in to the active server using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su -
```

 and pressing the Enter key.

- 4 When prompted, enter the root password.
- 5 Access the Oracle Listener application by typing  
`# lsnrctl`  
and pressing the Enter key.  
*Example response:*  
Welcome to LSNRCTL, type "help" for information.
- 6 Initiate the password change by typing  
`LSNRCTL> change password`  
and pressing the Enter key.  
*Example response*  
Old password:
- 7 When prompted, enter the old (current) password.  
*Example response*  
New password:
- 8 When prompted, enter the new password.  
*Example response*  
Reenter new password:
- 9 When prompted, enter the new password again to confirm it.  
*Example response*  
Connecting to  
(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)  
(HOST=47.143.107.192) (PORT=1521)))  
Password changed for LISTENER  
The command completed successfully
- 10 Initiate the password setting by typing  
`LSNRCTL> set password`  
and pressing the Enter key.  
*Example response*  
Password:
- 11 When prompted, enter the new password.  
*Example response*  
The command completed successfully
- 12 Save the new password by typing  
`LSNRCTL> save_config`

and pressing the Enter key.

*Example response*

```
Connecting to
(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)
(HOST=47.143.107.192) (PORT=1521)))
Saved LISTENER configuration parameters.
Listener Parameter File
/opt/oracle/product/8.1.7/network/admin/listener.ora
Old Parameter File
/opt/oracle/product/8.1.7/network/admin/listener.bak
The command completed successfully
```

**13** Exit the Oracle Listener application by typing

```
LSNRCTRL> quit
```

and pressing the Enter key.

You have completed this procedure.

---

—End—

---

## Changing the system IP address on an SPFS server

### Application

Use this procedure to change the system IP address on both a simplex, one-unit cluster, and two-unit HA cluster.

Starting with the SN08 release, the system is limited to two virtual IP addresses and the private interface IPs (uplink1) cannot be changed.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

*At your workstation*

#### 1 Access the system console as a root user.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the `udstat -a` command.

For detailed steps, refer to procedure Logging in to an SPFS-based server, and follow the steps for logging in through the console.

*Example output from active unit:*

```
cluster-unit0:/>udstat -a
/data: ACTIVE normal UP clean
/data_oradata (/data/oradata): ACTIVE normal UP clean
/data_qca (/data/qca): ACTIVE normal UP clean
```

*Example output from inactive unit:*

```
cluster-unit1:/>udstat -a
/data: STANDBY normal UP clean
```

For a simplex and one-unit cluster, there is only one unit. Log into unit console as user ROOT.

#### 2 Re-configure the system IP address through the SPFS CLI utility.

Start the SPFS CLI tool by running the command "`c1i`" in an xterm obtained from the previous step. In case of a simplex and one-unit cluster, the CLI does not ask for two IP addresses, as displayed in the following example.

- a. Once the CLI menu is available, select **"2 - Configuration"** in the main menu, by typing number 2 and pressing return.
- b. In the next level of the Configuration menu, select **"6 - IP Configuration"** by typing number 6 and pressing return.
- c. In the next level of the IP Configuration menu, select **"2 - config\_data (Configure System Data IP Addresses)"**, by typing number 2 and pressing return.

*The CLI displays WARNING / CAUTION messages, and the current System IP configuration, for example:*

```
hostname: wcars949
ip address: 47.135.180.252
additional virtual ip addr: 47.135.181.117
application: iems
```

- d. The CLI prompts for the new hostname and IP addresses. For each data, the CLI provides the current configuration as the default value, and you can simply type in return to accept the default value.

*Example:*

```
Enter primary cluster IP address (default:
47.142.108.186): 47.142.108.185
Enter cluster hostname for 47.142.108.185
(default: durham): apex
Enter unit zero IP address (default:
47.142.108.69): 47.142.108.211
Enter unit one IP address (default:
47.142.108.70): 47.142.108.212
```

- e. The CLI displays the new IP configurations again, and requests you to confirm the change. Type **"ok"** to accept the settings.

*Example:*

```
Enter "ok" to accept current settings
Enter "quit" to exit
Enter anything else to re-enter settings
```

- f. After this point, the CLI displays various messages that can help with system debugging. At the end, the CLI reminds you that a system restart is required.

*Example:*

```
The network changes have been made, however the
cluster requires a restart of both units
login to the standby unit and issue the Solaris
command "shutdown -i 6 -y"
after the standby unit has rebooted, login to the
active unit and issue
```

```
the Solaris command "shutdown -i 6 -y". This
will cause a swact
After the swact is complete, the new network
settings are in effect
=== "config_data" completed successfully
```

### **3 System restart to activate the new IP configuration**

- a. For a simplex and one-unit cluster, run the command  

```
shutdown -i 6 -y
```
- b. In case of a two-unit cluster, you need to do the following:
  - i. Login to the inactive (standby) unit as ROOT, and issue the command  

```
shutdown -i 0 -y
```

or

```
init 0
```

This will cause the inactive unit to shutdown to the "ok" prompt and stay there.
  - ii. Reboot the active unit with the command  

```
shutdown -i 6 -y
```

or

```
init 6
```
  - iii. Once the active unit has rebooted, boot the inactive unit with the command  

```
boot
```

at the "ok" prompt of the inactive unit.
  - iv. Once the inactive unit has booted, the cluster should quickly re-sync and be in-service with the new IP addresses.

Any applications that require re-configuration (such as SESM), should run their configure command now.

- 4** You have completed this procedure.

---

—End—

---



## Configuring IPSec and IKE on an SPFS-based server

### Application

Use this procedure to configure IP Security (IPSec) and Internet Key Exchange (IKE) on a Server Platform Foundation Software (SPFS)-based server, for secure communication with downstream interfaces.

### Prerequisites

IPSec and IKE configuration parameters that are provisioned on the OSS must match the corresponding parameters configured through this procedure.

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

When performing this procedure, each time you enter x when it is a valid response to a CLI tool prompt, you exit from the current menu level of the interface. Repeatedly entering x eventually enables you to exit from the CLI tool.

### Procedures

Use the following table to determine the procedure to perform.

| Procedure to perform                                                                 |
|--------------------------------------------------------------------------------------|
| "Procedure to access CLI in order to perform IPSec and IKE configuration" (page 445) |
| "Procedure to add an IPSec rule" (page 448)                                          |
| "Procedure to delete an IPSec rule" (page 451)                                       |
| "Procedure to list an IPSec rule" (page 451)                                         |
| "Procedure to add an IKE rule" (page 452)                                            |
| "Procedure to delete an IKE rule" (page 454)                                         |
| "Procedure to list IKE entries" (page 455)                                           |
| "Procedure to change a preshared key for an IKE entry" (page 455)                    |

### Procedure to access CLI in order to perform IPSec and IKE configuration

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- |   |                       |
|---|-----------------------|
| 1 | Telnet to the server: |
|---|-----------------------|

**telnet <server>**

where

**server** is the IP address or host name of the SPFS-based server on which you want to configure IPsec and IKE.

**2** When prompted, enter your user ID and password.

**3** Change to the root user:

**su - root**

**4** When prompted, enter the root password.

**5** Access the command line interface:

**cli**

*Example response*

```
Command Line Interface 1 - View
2 - Configuration
3 - Other
X - exit
select -
```

**6** Enter the number next to the 'Configuration' option in the menu.

*Example response*

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Application Configuration
5 - CORBA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)
19 - backup_config (Backup Configuration)
X - exit
Select -
```

**7** Enter the number next to the "IP Configuration" option in the menu.

*Example response*

IP Configuration

```

1 - config_router (Configure Default Router and
 Netmask)
2 - config_data (Configure System Data IP
 Addresses)
3 - ipsecike_config (Configure IPSec/IKE Rules)
X - exit
select -

```

- 8 Enter the number next to the "ipsecike\_config" option in the menu.

*Example response*

IPSec/IKE Configuration Menu

```

1 - IPSec Configuration
2 - IKE Configuration
X - exit
Select -

```

| If                                     | Do      |
|----------------------------------------|---------|
| you wish to configure IPSec parameters | step 9  |
| you wish to configure IKE parameters   | step 10 |

- 9 Enter the number next to the "IPSec Configuration" option in the menu.

*Example response*

IPSec Configuration Menu

```

1 - Add IPSec entry
2 - Delete IPSec entry
3 - List All IPSec entries
X - exit
Select -

```

| If                               | Procedure to perform                                           |
|----------------------------------|----------------------------------------------------------------|
| you wish to add an IPSec rule    | <a href="#">"Procedure to add an IPSec rule" (page 448)</a>    |
| you wish to delete an IPSec rule | <a href="#">"Procedure to delete an IPSec rule" (page 451)</a> |
| you wish to list all IPSec rules | <a href="#">"Procedure to list an IPSec rule" (page 451)</a>   |

- 10 Enter the number next to the "IKE Configuration" option in the menu.

*Example response*

IKE Configuration Menu

```

1 - Add IKE entry
2 - Delete IKE entry

```

```

3 - List IKE entries
4 - Change Preshared key for IKE entry
X - exit
Select -

```

| If                                                  | Procedure to perform                                              |
|-----------------------------------------------------|-------------------------------------------------------------------|
| you wish to add an IKE entry                        | "Procedure to add an IKE rule" (page 452)                         |
| you wish to delete an IKE entry                     | "Procedure to delete an IKE rule" (page 454)                      |
| you wish to list IKE entries                        | "Procedure to list IKE entries" (page 455)                        |
| you wish to change a preshared key for an IKE entry | "Procedure to change a preshared key for an IKE entry" (page 455) |

- 11 When you have completed the configuration, and you wish to exit from the CLI tool, exit each menu level of the command line interface by entering x in response to the select prompt.
- 12 You have completed this procedure.

---

—End—

---

### Procedure to add an IPSec rule

| Step | Action |
|------|--------|
|------|--------|

#### *At the CLI tool IPSec Configuration Menu*

- 1 Enter the number next to the 'Add IPSec entry' option in the menu. The CLI tool displays a collection of prompts for IPSec rule parameters, as shown in the following.

#### *Example response*

```

Enter the Remote IP Address:
Enter the Remote Port No [1-65535,all]:
Enter the Local IP Address [<IP address>]:
Enter the Local Port No [1-65535,all]:
Enter the Upper Layer Protocol
[any,udp,tcp,icmp]:
Enter the Direction [in,out,both]:
Enter the Action [ipsec,drop,bypass]:
Enter the ESP Header
Authentication Algorithm [md5,sha 1,none,any]:
Encryption Algorithm [none,Null,des,3des,
aes,blowfish]:
Enter the AH Header

```

Authentication Algorithm [md5,sha1,none,any] :

Use the following table to determine the information to enter in response to each of the prompts.

| Field                                                                                                                                                                     | Entry                                                      | Explanation                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote Address                                                                                                                                                            | a numeric internet IP address of the form: www.xxx.yyy.zzz | source address on incoming packets and destination address on outgoing packets                                                                                                               |
| Remote Port                                                                                                                                                               | 1-65535,all                                                | IP port of the remote system communicating with the server                                                                                                                                   |
| Local Address<br>This is the cluster IP address if the system is an HA cluster configuration. If the system is a simplex configuration, this is the address of this node. | a numeric internet IP address of the form: www.xxx.yyy.zzz | destination address on incoming packets and source address on outgoing packets                                                                                                               |
| Local Port                                                                                                                                                                | 1-65535,all                                                | IP port of this server                                                                                                                                                                       |
| Upper Layer Protocol                                                                                                                                                      | any,udp,tcp,icmp                                           | determines which protocol traffic this entry is matched against                                                                                                                              |
| Direction                                                                                                                                                                 | in,out,both                                                | determines whether this entry is for inbound or outbound traffic                                                                                                                             |
| Action                                                                                                                                                                    | bypass,drop,ipsec                                          | determines the action to be taken when the traffic pattern is matched                                                                                                                        |
| ESP Encryption                                                                                                                                                            | none,any,NULL,DES,3DES                                     | encryption algorithm that will be used to apply the IPsec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to 'ipsec'.     |
| ESP Authentication                                                                                                                                                        | none,any,SHA1,MD5                                          | authentication algorithm that will be used to apply the IPsec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to 'ipsec'. |
| AH Authentication                                                                                                                                                         | none,any,SHA1,MD5                                          | authentication algorithm that will be used to apply the IPsec AH protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to 'ipsec'.  |

You will be prompted to save the entries, edit the entries, or abort and lose all of the entry information you have entered in this session.

| If                                                                                     | Do                                                       |
|----------------------------------------------------------------------------------------|----------------------------------------------------------|
| you wish to save the IPSec rule entries                                                | Enter <b>save</b><br>You have completed this procedure   |
| you wish to edit the IPSec rule entries                                                | Enter <b>edit</b><br>and go to step 2                    |
| you wish to abort and lose all entry information that you have entered in this session | Enter <b>abort</b><br>You have completed this procedure. |

- 2 If you have chosen to edit the IPSec rule entries, the CLI tool displays the IPSec rule entries you have made in this session. You may change any of the entries that you have made.

*Example*

```
Remote IP Address [47.135.210.64]:
Remote Port No [all]:
Local IP Address [47.135.210.119]:
Local Port No [all]:
Upper Layer Protocol [any]:
Direction [both]:
Action [ipsec]:
ESP Encryption Algorithm [3des]
ESP Authentication Algorithm [sha1]:
AH Authentication Algorithm [md5]:
```

After you have completed making any changes and press Enter, you are prompted to either save the new IPSec rule configuration, edit the configuration again, or abort the session and lose all of the changes you have made.

| If                                                                                     | Do                                                       |
|----------------------------------------------------------------------------------------|----------------------------------------------------------|
| you wish to save the IPSec rule entries                                                | Enter <b>save</b><br>You have completed this procedure.  |
| you wish to edit the IPSec rule entries again                                          | Enter <b>edit</b> and repeat this step.                  |
| you wish to abort and lose all entry information that you have entered in this session | Enter <b>abort</b><br>You have completed this procedure. |

—End—

**Procedure to delete an IPsec rule****Step Action****At the CLI tool IPsec Configuration Menu**

- 1 Enter the number next to the 'Delete IPsec entry' option in the menu. The CLI tool displays the IPsec rules that have been configured, as shown in the following.

*Example response*

```

indexID raddr laddr lport rport dir status

1 47.130.222.110 47.130.222.90 all all both up
2 47.130.222.88 47.130.222.7 all all both down
Enter the indexID of rule to be deleted (x to exit) -

```

Enter the number next to the IPsec rule that you want to delete.

*The CLI tool displays the entries for the IPsec rule that you want to delete.*

Respond to the prompts to delete the rule.

- 2 You have completed this procedure.

—End—

**Procedure to list an IPsec rule****Step Action****At the CLI tool IPsec Configuration Menu**

- 1 Enter the number next to the 'List All IPsec entries' option in the menu. The CLI tool displays the IPsec rules that have configured, as shown in the following.

*Example response*

```

indexID raddr laddr lport rport dir status

1 47.130.222.110 47.130.222.90 all all both up
2 47.130.222.88 47.130.222.7 all all both down
Enter the indexID of rule to be detailed (x to exit) -

```

Enter the number next to the IPsec rule whose details you want to display.

*The CLI tool displays the entries for the IPsec rule that you selected.*

You may choose either to enter another rule whose details you wish to display or you may exit to a previous menu level.

- 2 You have completed this procedure.

---

—End—

---

### Procedure to add an IKE rule

| Step | Action |
|------|--------|
|------|--------|

#### At the CLI tool IKE Configuration Menu

- 1 Enter the number next to the 'Add IKE entry' option in the menu. The CLI tool displays a collection of prompts for IKE rule parameters, as shown in the following.

#### Example response

```
Enter the Remote IP Address:
Enter the Local IP Address [<IP address>]:
Enter the Oakley Group [1,2,5]:
Enter the Authentication Method [preshared]:
Enter the Encryption Algorithm [des,3des]:
Enter the Authentication Algorithm [md5,sha1]:
Enter the PFS Group ID [0,1,2,5]:
Enter the IKE Lifetime value:
Enter the IKE Lifetime unit [secs,min,hrs]:
Enter the IPSec Lifetime Value:
Enter the IPSec Lifetime unit [secs,min,hrs]:
Enter the IKE Preshared Key file location (full
path):
```

Use the following table to determine the information to enter in response to each of the prompts.

The preshared key, in hex format, should be stored in a file on the system. You will need to provide this file when you are configuring the IKE rule.

| Field          | Entry                                                      | Explanation                                                                      |
|----------------|------------------------------------------------------------|----------------------------------------------------------------------------------|
| Remote Address | a numeric internet IP address of the form: www.xxx.yyy.zzz | IP address of the remote system communicating with this server                   |
| Local Address  | a numeric internet IP address of the form: www.xxx.yyy.zzz | IP address of this server                                                        |
| Oakley Group   | 1 (768 bit),<br>2 (1024 bit),<br>5 (1536 bit)              | the Oakley Diffie-Hellman group used for IKE Security Association key derivation |



| Field                 | Entry                                                                                                  | Explanation                                                                                                                                |
|-----------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Method | Preshared                                                                                              | authentication method used for IKE phase 1                                                                                                 |
| Encryption            | DES,<br>3DES                                                                                           | specifies the encryption algorithm for a security association                                                                              |
| Authentication        | SHA1,<br>MD5                                                                                           | specifies the authentication algorithm for a security association                                                                          |
| PFS Group ID          | 0 (do not use Perfect Forward Secrecy for IPSec SAs),<br>1 (768 bit),<br>2 (1024 bit),<br>5 (1536 bit) | Oakley Diffie-Hellman group used for IPSec Security Association key derivation                                                             |
| Preshared Key File    | String (file name with full path)                                                                      | Specifies the file with complete path that contains the preshared key. This file contains the preshared key for this Security Association. |
| IKE Lifetime          | Maximum allowed value is 2419200 seconds, 40320 minutes, 672 hours, or 28 days                         | Specifies the lifetime for an IKE phase 1 Security Association                                                                             |
| IPSec Lifetime        | Maximum allowed value is 2419200 seconds, 40320 minutes, 672 hours, or 28 days                         | Specifies the lifetime for an IPSec Security Association                                                                                   |

You will be prompted to either save the entries, edit the entries, or abort and lose all of the entry information you have entered in this session.

| If                                                                                     | Do                                                           |
|----------------------------------------------------------------------------------------|--------------------------------------------------------------|
| you wish to save the IKE rule entries                                                  | Enter <b>save</b><br><br>You have completed this procedure.  |
| you wish to edit the IKE rule entries                                                  | Enter <b>edit</b><br>and go to step 2                        |
| you wish to abort and lose all entry information that you have entered in this session | Enter <b>abort</b><br><br>You have completed this procedure. |

- 2 If you have chosen to edit the IKE rule entries, the CLI tool displays the IKE rule entries you have made in this session. You may change any of the entries that you have made.

**Example**

```

Remote IP Address [47.135.214.53]:
Local IP Address [47.135.214.30]:
Oakley Group [2]:
Authentication Method [preshared]:
Encryption Algorithm [3des]:
Authentication Algorithm [sha1]:
PFS Group ID [0]
IKE Lifetime value [400]:
IKE Lifetime Unit [secs]:
IPSec Lifetime Value [400]:
IPSec Lifetime Unit [secs]:
IKE Preshared key File location [/tmp/site1]:

```

After you have completed making any changes and press Enter, you will be prompted to either save the new IKE rule configuration, edit the configuration again, or abort the session and lose all of the changes you have made.

| If                                                                                     | Do                                                       |
|----------------------------------------------------------------------------------------|----------------------------------------------------------|
| you wish to save the IKE rule entries                                                  | Enter <b>save</b><br>You have completed this procedure.  |
| you wish to edit the IKE rule entries again                                            | Enter <b>edit</b><br>and repeat this step.               |
| you wish to abort and lose all entry information that you have entered in this session | Enter <b>abort</b><br>You have completed this procedure. |

---

—End—

---

**Procedure to delete an IKE rule**

| Step | Action |
|------|--------|
|------|--------|

**At the CLI tool IKE Configuration Menu**

- 1 Enter the number next to the 'Delete IKE entry' option in the menu. The CLI tool displays the IKE rules that have configured, as shown in the following.

**Example response**

```

indexID raddr laddr

1 47.135.142.53 47.135.142.30
2 47.130.221.88 47.130.221.7
Enter the indexID of rule to be deleted (x to exit) -

```

Enter the number next to the IKE rule that you want to delete.

*The CLI tool displays the entries for the IKE rule that you want to delete.*

Respond to the prompts to delete the rule.

- 2 You have completed this procedure.

---

—End—

---

## Procedure to list IKE entries

| Step | Action |
|------|--------|
|------|--------|

### At the CLI tool IKE Configuration Menu

- 1 Enter the number next to the 'List IKE entries' option in the menu. The CLI tool displays the IKE rules that have been configured, as shown in the following.

*Example response*

```

indexID raddr laddr

1 47.135.142.53 47.135.142.30
2 47.130.221.88 47.130.221.7
Enter the indexID of rule to be detailed (x to exit) -
```

Enter the number next to the IKE rule whose details you want to display.

*The CLI tool displays the entries for the IKE rule that you selected.*

You may choose either to enter another rule whose details you wish to display or you may exit to a previous menu level.

- 2 You have completed this procedure.

---

—End—

---

## Procedure to change a preshared key for an IKE entry

| Step | Action |
|------|--------|
|------|--------|

### At the CLI tool IKE Configuration Menu

- 1 Enter the number next to the 'Change Preshared key for IKE entry' option in the menu. The CLI tool displays the IKE rules that have been configured.

*Example*

```

indexID raddr laddr

1 47.135.142.53 47.135.142.30
2 47.130.221.88 47.130.221.7
Enter the indexID of rule whose key is to be changed
(x to exit) -

```

Enter the number next to the IKE rule whose key is to be changed. The CLI tool displays the entries for the IKE rule that you selected, as shown in the following:

*Example*

```

Remote IP Address [47.135.214.53]:
Local IP Address [47.135.214.30]:
Oakley Group [2]:
Authentication Method [preshared]:
Encryption Algorithm [3des]:
Authentication Algorithm [sha1]:
PFS Group ID [0]
IKE Lifetime [400]:
IPSec Lifetime [800]:
IKE Preshared key [*****]:
Do you wish to change key for above IKE rule Select
[Yes, No, Exit (x)] -

```

In response to the prompts, enter Yes to change to key, enter the full path location of the preshared key file, and confirm the change.

- 2 You have completed this procedure.

---

—End—

---

## Configuring IPSec and IKE on the OSS

### Application

Use this procedure to configure IP Security (IPSec) and Internet Key Exchange (IKE) on the OSS. Included are steps both to add IPSec/IKE to the OSS and to remove IPSec/IKE from the OSS. In this procedure, the OSS is assumed to be a Solaris 5.9 machine.

### Prerequisites

IPSec and IKE configuration parameters that are provisioned on the OSS must match the corresponding parameters provisioned on the server to which a secure connection is being configured.

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Procedures

Use the following table to determine the procedure to perform.

| Procedure to perform                                            |
|-----------------------------------------------------------------|
| "Configuring IPSec on the OSS (Solaris 5.9 machine)" (page 457) |
| "Removing IPSec from the OSS (Solaris 5.9 machine)" (page 458)  |

### Configuring IPSec on the OSS (Solaris 5.9 machine)

| Step | Action |
|------|--------|
|------|--------|

#### At the OSS

- 1 Make required changes in the following files on the OSS. The changes correspond to the server to which the secure connection is being configured.

- /etc/inet/ipsecinit.conf
- /etc/inet/ike/config
- /etc/inet/secret/ike.preshared

When IPSec and IKE are configured on an SPFS-based server through the CLI tool, sample downstream configuration files are generated. These files are 'downstream.ipsec' and 'downstream.ike', located in the /etc/inte/remotesystem/solaris directory on the SPFS-based server. The information in these two files can be used to update the files shown in the preceding.

- 2 Enable IPsec communication from the OSS by performing the following steps:
  - restart theiked daemon:
 

```
pkill in.iked
```

```
/usr/bin/inet/in.iked
```
  - activate IPsec policy:
 

```
ipseccnf -a /etc/inet/ipsecinit.conf
```
- 3 You have completed this procedure.

---

—End—

---

If the SPFS software load for release (I)SN09 is running on the OSS, the CLI tool can be used for configuring IPsec on the OSS. The procedure to use is "Configuring IPsec and IKE on an SPFS-based server" located in *ATM/IP Solution-level Security and Administration*, NN10402-600.

### Removing IPsec from the OSS (Solaris 5.9 machine)

| Step | Action |
|------|--------|
|------|--------|

#### At the OSS

- |   |                                                                                                                                                                                                                                                                                                                                  |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Remove the appropriate IPsec and IKE entries from the following files. These entries correspond to the server from which the secure connection is being removed. <ul style="list-style-type: none"> <li>• /etc/inet/ipsecinit.conf</li> <li>• /etc/inet/ike/config</li> <li>• /etc/inet/secret/ike.preshared</li> </ul>          |
| 2 | Remove the IPsec security from the link by performing the following steps: <ul style="list-style-type: none"> <li>• restart theiked daemon:               <pre>pkill in.iked</pre> <pre>/usr/bin/inet/in.iked</pre> </li> <li>• activate IPsec policy:               <pre>ipseccnf -a /etc/inet/ipsecinit.conf</pre> </li> </ul> |
| 3 | You have completed this procedure.                                                                                                                                                                                                                                                                                               |

---

—End—

---

If the SPFS software load for release (I)SN09 is running on the OSS, the CLI tool can be used for removing IPsec from the OSS. The procedure to use is "Configuring IPsec and IKE on an SPFS-based server" located in *ATM/IP Solution-level Security and Administration*, NN10402-600.

## Configuring the IEMS central security server in the network

### Application

Use this procedure to configure and activate the Integrated Element Management System (IEMS) central security server in the network. The IEMS acts as a proxy to the central security administration system.

#### ATTENTION

Only one IEMS central security server can be configured in the network.

#### ATTENTION

Reverting to the previous configuration of the server is not supported. A rollback of the Server Platform Foundation Software (SPFS) must be performed to revert the security server to its previous configuration.

#### ATTENTION

User accounts managed by IEMS in previous releases will be automatically migrated from the IEMS Oracle database to the MFT NDS database when upgrading to IEMS (I)SN09.

### Prerequisites

This procedure has the following prerequisites:

- you have root user privileges
- the Integrated Element Management System (IEMS) is already installed or upgraded on the server, and it is running Server Platform Foundation Software (SPFS).
- an HTTPS certificate has been properly installed on the server prior to installing or upgrading the IEMS. If required, refer to procedure ["Installing or replacing an HTTPS certificate on an SPFS-based server"](#) (page 641). The Integrated security server and SunONE component will be automatically configured during installation or upgrade to enable the secure SSL mode.

### Action

Perform the following steps to complete this procedure.

| Step | Action                                                                                                                        |
|------|-------------------------------------------------------------------------------------------------------------------------------|
| 1    | <p>Delete the user accounts you want to add to the IEMS central security server.</p> <p>a. Telnet to the server by typing</p> |



```
> telnet <server>
```

and pressing the Enter key.

where

**server** is the IP address or host name of the SPFS-based client server

- b. When prompted, enter the user ID and password for an account that was migrated to the IEMS central security server.

- c. Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- d. When prompted, enter the root password.

- e. Delete the user account by typing

```
userdel <userid>
```

and pressing the Enter key.

where

**userid** is a variable for the user name

Repeat this step for each user account you want to migrate to the IEMS central security server.

- 2 If the central administration system is the IEMS, launch the Security Administration tool of the IEMS, and add the user accounts you want to centrally manage. If required, refer to 'Adding new users' in *IEMS Security and Administration*, NN10336-611.

If the central security administration application is a third-party application and not the IEMS, follow the procedures in the third party documentation

All users added through the IEMS Security Administration tool, are by default assigned to the "succssn" user group for login access.

- 3 Complete PAM and NSSwitch configuration as follows:

At installation or upgrade, the IEMS replaces the existing PAM and NSSwitch configuration files (pam.conf and nsswitch.conf) with new PAM and NSSwitch configuration files that use the IEMS security application. If the pam.conf or nsswitch.conf files had any special edits, you must re-edit the file to add those special edits.

You can use the IEMS PAM and NSSwitch SPIs, which are pre-bundled with the IEMS load, or you can use your own third-party PAM and NSSwitch SPIs. The Distributed Computing Environment (DCE) and the Lightweight Directory Access Protocol (LDAP) PAM

and NSSwitch SPIs are the third-party PAM and NSSwitch SPIs that are supported. If required, refer to procedure "[Configuring a third-party Pluggable Authentication Module](#)" (page 470).

- 4 If necessary, add the SPFS platform to the IEMS topology. For an SPFS platform user account to be authorized, the SPFS platform must be a RADIUS client of the central security server. For details, see "Adding a Server Platform Foundation Software (SPFS) platform" in IEMS Configuration, NN10330-511.

If a centrally managed restricted access user account is created through the IEMS security application, then the home directory and profile are automatically created. In this case, you do not need to manually configure the user account for platform access.

- 5 You have completed this procedure.

---

—End—

---

## Configuring an SPFS-based central security client

### Application

Use this procedure to configure an SPFS-based central security client to use the Integrated Element Management System (IEMS) central security server.

#### ATTENTION

You can revert to the previous configuration of the client server using procedure ["Reverting the client server to its previous configuration "](#) (page 479).

In the event you want to reconfigure the central security client to use a new IEMS server IP, perform steps [step 2](#) and [step 3](#) of this procedure.

### Prerequisites

This procedure has the following prerequisites:

- you have root user privileges
- the IEMS central security server is already configured and activated in the network (see procedure ["Configuring the IEMS central security server in the network"](#) (page 460), if required)
- perform this procedure on each SPFS-based server that is not the IEMS central security server to activate centralized security

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Migrate the user accounts you want to centrally manage, from the local security database on the SPFS-based client to the central administration system as follows:

It is recommended to migrate all user accounts that exist on SPFS-based servers to the central administration system with the following exceptions:

root, daemon, bin, sys, adm, lp, uucp, nuucp, listen, nobody, noaccess, nobody4, sshd, maint, npm, npmtftp, ptm, mgems, www, patcher, poller, certuser, sam21em, anonymous, image, pfrs, ntssg, FIELD, and oracle.

**ATTENTION**

It is strongly recommended to migrate all local user accounts (except the mentioned list above) to the IEMS central administration system. If local user accounts are not migrated, you have to ensure the local user name does not conflict with an IEMS central administration system user.

There is no way to prevent the creation of centralized accounts that are duplicates of local accounts that exist on the SPFS client machines. In the event that duplicate accounts are created, the IEMS account is used.

- a. If the central administration system is the IEMS, launch the Security Administration tool of the IEMS, and add the user accounts plus any additional required user groups you want to centrally manage. If required, refer to "Adding new users", "Adding new groups", and "Assigning a user to a group" in *IEMS Security and Administration*, NN10336-611.

All users added through the IEMS Security Administration tool, are by default assigned to the *succssn* user group for login access.

- b. Delete the user accounts you just added to the IEMS central security server.

Log in to the client server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server** is the IP address or host name of the SPFS-based client server

- c. When prompted, enter the user ID and password for an account that was migrated to the IEMS central security server.
- d. Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- e. When prompted, enter the root password.
- f. Delete the user account by typing

```
userdel <userid>
```

and pressing the Enter key.

where

**userid** is a variable for the user name

Repeat this step for each user account you migrated to the IEMS central security server.

**2** Configure the IEMS security server address as follows:

- a. Access the command line interface by typing

```
cli
```

and pressing the Enter key.

*Example response*

```
Command Line Interface
```

```
1 - View
2 - Configuration
3 - Other
X - Exit
select -
```

- b. Enter the number next to the "Configuration" option in the menu.

*Example response*

```
Configuration
```

```
1 - NTP Configuration
2 - Apache Proxy Configuration
3- OAMP Application Configuration
4- CORBA Configuration
5- IP Configuration
6- DNS Configuration
7- Syslog Configuration
8- Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
Select -
```

- c. Enter the number next to the "Security Services Configuration" option in the menu.

*Example response*

```
Security Services Configuration
```

```
1 - Socks Configuration
2 - IEMS Server Location Configuration
```

```
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp
and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
Select -
```

- d. Enter the number next to the "Security Server Location Configuration" option in the menu.

*Example response*

```
IEMS Server Location Configuration
1 - security_server_ip (Configure Security Server
IP)
x - exit
select
```

- e. Enter the number next to the "security\_server\_ip" option in the menu.

*Example response*

```
===Executing "security_server_ip"
Enter Server IP Address (default 0.0.0.0):
```

- f. When prompted, enter the virtual IP address of the security server, or press the Enter key to accept the default value if one is specified.

*Example response*

```
Enter Fully Qualified Domain Name (default : no
default):
```

- g. When prompted, enter the Fully Qualified Domain Name (FQDN) of the security server, or press the Enter key to accept the default value if one is specified.

*Example response*

```
Server IP: 47.135.214.83
Fully Qualified Domain Name: ca.nortel.com
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

- h. Accept the IP address and FQDN you just entered by typing

**ok**

and pressing the Enter key.

*Example response*

```
=== "security_server_ip" completed successfully
```

- i. Return to the Security Services Configuration menu, by typing

```
select - x
```

and pressing the Enter key.

*Response*

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
x - exit
select -
```

- 3 Configure PAM and NNSwitch SPI configuration as follows:

RADIUS client and RADIUS server should not be configured on the same box.

- a. Enter the number next to the "PAM Configuration" option in the menu.

*Example response*

```
PAM Configuration
1 - Central Security Client Configuration
x - exit
select -
```

- b. Enter the number next to the "Central Security Client Configuration" option in the menu.

*Example response*

```
Central Security Client Configuration
1 - pam_orig (Use Default PAM Configuration)
2 - pam_radius (Use Security Server)
3 - saml_passwd_conf (Configure saml password)
x - exit
select -
```

- c. Enter the number next to the "pam\_radius" option in the menu.

*Example response*

```
===Executing "pam_radius"
Activating pam radius components
Security Server IP: 45.12.23.56
Security Server Fully Qualified Host Name:
test3iems.us.nortel.com
Enter the Shared Secret (default: nortelnetworks):
```

- d. When prompted, enter the shared secret, or press the Enter key to accept the default value if one is specified.

*Example response*

```
Enter Radius Client Timeout (default: 12):
```

- e. When prompted, enter the Radius Client timeout (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

*Example response*

```
Enter SAML Connection Timeout (default: 20):
```

- f. When prompted, enter the SAML connection timeout (used to establish SAML connections with the Security Server) or press the Enter key to accept the default value if one is specified.

*Example response*

```
Enter SAML Request Timeout (default: 10):
```

- g. When prompted, enter the SAML request timeout (used to communicate with the Security Server) or press the Enter key to accept the default value if one is specified.

*Example response with default values*

```
** Confirm Settings **
Security Server IP: 45.12.23.56
Security Server Domain Name: test3iems.us.nortel.com
Shared Secret: nortelnetworks
Radius Client Timeout: 12
SAML Connection Timeout: 20
SAML Request Timeout: 10
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

- h. Accept the PAM configuration update by typing

**ok**

and pressing the Enter key.

*Example response*

```
Configuring pam_radius
configuring nsssaml
Updating PAM Configuration to use IEMS Security
Server
Restarting name service daemon
=== "pam_radius" completed successfully
```



- i. Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

- j. If the pam.conf file had any special edits, you must re-edit the file to add those special edits.

**4** To configure a saml password, from the menu prompt in step 3b above:

- a. enter the number next to the "saml\_passwd\_conf (Configure saml password)" option
- b. when prompted, enter the default SAML password (slisamadmin) or a new password you have chosen:

*Example response*

```
** Confirm Settings **
SAML Password: slisamadmin
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
ok
Configure Password Successful
=== "saml_passwd_conf" completed
successfully
```

**5** If necessary, add the SPFS platform to the IEMS topology. For an SPFS platform user account to be authorized, the SPFS platform must be a RADIUS client of the central security server. For details, see "Adding a Server Platform Foundation Software (SPFS) platform" in IEMS Configuration, NN10330-511.

If a centrally managed restricted access user account is created through the IEMS security application, then the home directory and profile are automatically created. In this case, you do not need to manually configure the user account for platform access.

You have completed this procedure.

---

—End—

---

## Configuring a third-party Pluggable Authentication Module

### Application

Use this procedure to configure a third-party Pluggable Authentication Module (PAM) on the Integrated Element Management System (IEMS) central security server. The following third-party Pluggable Authentication Modules (PAMs) are supported:

- "Lightweight Directory Access Protocol (LDAP) PAM" (page 470)

### Prerequisites

To perform this procedure, you need to have the root user ID and password for the IEMS central security server, and the LDAP prerequisites below.

#### LDAP prerequisites

To configure LDAP PAM, an LDAP server must already be configured with support for Solaris Native LDAP schema.

Information on LDAP schema, is available at the following link:

<http://docs.sun.com/app/docs/db?q=ldap+configuration+guide&p=doc%2F806-5580>

To configure IEMS Server as an LDAP Client, LDAP PAM and Nsswitch modules must be activated on the server.

### Action

Perform the following steps to complete this procedure.

#### Lightweight Directory Access Protocol (LDAP) PAM

| Step | Action |
|------|--------|
|------|--------|

##### *At the LDAP server*

- 1 Add users and user groups to LDAP server as follows:  
For details on user groups, refer to procedure [Setting up local user accounts on an SSPFS-based server](#), if required.  
  
To configure LDAP Security, an LDAP server must be configured with support for Solaris Native LDAP schema and Proxy Authentication. Consult your LDAP server manual for instructions to configure the LDAP server to support Solaris Native LDAP schema.
  - a. Log in to the LDAP server.

- b. Add the necessary user groups to the LDAP server. Consult the LDAP server instructions to add the 25 Succession user groups to the LDAP server.

The user groups are listed below with their corresponding group ID.

- succssn:105
- trkadm:1001, trkrw:1002, trksprov:1003, trkmtc:1004, trkro:1005
- lnadm:1006, lnrw:1007, lnspov:1008, lnmtc:1009, lnro:1010
- mgcadm:1011, mgcrw:1012, mgcsprov:1013, mgcmtec:1014, mgcro:1015
- mgadm:1016, mgrw:1017, mgsprov:1018, mgmtc:1019, mgro:1020
- emsadm:1021, emsrw:1022, emssprov:1023, emsmtec:1024, emsro:1025
- secadm:1026, secrw: 1027, secprov: 1028, secmtc: 1029, secro: 1030

Below is a sample ldif file to add the 'succssn' group:

```
dn: cn=succssn,ou=group,dc=labnet,dc=us
dc=nortel,dc=com,o=internet
changetype: add
cn:succssn
gidnumber: 105
memberuid: kcaudill
memberuid: ferreira
objectclass: top
objectclass: posixGroup
```

Consult your LDAP server manual for information on loading data into the directory server.

- c. Add users to the LDAP server, and associate them to user groups. Consult your LDAP server instructions to add users to the LDAP server and associate them to usergroups.

Below is a sample ldif file to add a user:

```
dn: uid=kcaudill,ou=people,dc=us,dc=nortel,dc=com
cn: kelly Caudill
givenname: Kelly
sn: Caudill
gidnumber: 105
homedirectory: /tmp
uidnmuber: 10002
ojectclass: top
```

```
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: posixaccount
objectclass: account
objectclass: shadowwaccount
uid: kcaudill
shadowlastchange: 6445
loginshell: /bin/ksh
gecos: Kelly Caudill
userpassword: mypassword
```

Consult your LDAP server manual for information on loading data into the directory server.

### *At your workstation*

- 2 Log in to the IEMS server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server** is the IP address or host name of the IEMS central security server on which you want to change the PAM
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 Save a backup copy of the nsswitch.conf file, which is located in the /etc directory.
- 7

#### **ATTENTION**

The **ldapclient** command reconfigures the nsswitch.conf file. It is strongly recommended that you make a backup of nsswitch.conf before executing the **ldapclient** command, and then restore the backup nsswitch.conf file after the **ldapclient** command completes.

Configure the Solaris Native LDAP client and set up proxy authentication on the client using the **ldapclient** command.

Information on the **ldapclient** command, is available at the following link:

<http://docs.sun.com/app/docs/db?q=ldap+configuration+guide&p=doc%2F806-5580>

- 8 Replace the nsswitch.conf file with the backup copy of the nsswitch.conf file.
- 9 Edit the /etc/nsswitch.conf file as follows:
  - a. Add 'ldap' as the first option for the password and group.  
The entries will look similar to 'passwd: ldap files' and 'group: ldap files' after the change.  
This enables the group information to come from LDAP.
- 10 Restart the name service daemon as follows:
  - a. # /etc/init.d/nssd stop
  - b. # /etc/init.d/nssd start
- 11 Edit the /etc/pam.conf file to include LDAP entries as follows:
  - a. Add pam\_ldap with sufficient setting as the first entry for 'other auth', 'sesm auth', and 'secclient auth' iems entries in the '/etc/pam.conf' file as indicated:
    - change 'other auth' to 'other auth sufficient /usr/lib/security/\$ISA/pam\_ldap.so.1'
    - change 'sesm auth' to 'sesm auth sufficient /usr/lib/security/\$ISA/pam\_ldap.so.1 try\_first\_pass'
    - change 'secclient auth' to 'secclient auth sufficient /usr/lib/security/\$ISA/pam\_ldap.so.1'
  - b. Add pam\_ldap with sufficient setting as the first entry for 'other account', 'sesm account', and 'secclient account' iems entries in the '/etc/pam.conf' file as indicated:
    - change 'other account' to 'other account sufficient /usr/lib/security/\$ISA/pam\_ldap.so.1'
    - change 'sesm account' to 'sesm account sufficient /usr/lib/security/\$ISA/pam\_ldap.so.1 try\_first\_pass'
    - change 'secclient account' to 'secclient account sufficient /usr/lib/security/\$ISA/pam\_ldap.so.1'
  - c. Add pam\_ldap with sufficient setting as the first entry for 'other session', 'sesm session', and 'secclient session' iems entries in the '/etc/pam.conf' file as indicated:
    - change 'other session' to 'other session sufficient /usr/lib/security/\$ISA/pam\_ldap.so.1'

- change 'sesm session' to 'sesm session sufficient /usr/lib/security/\$ISA/pam\_ldap.so.1 try\_first\_pass'
- change 'secclient session' to 'secclient session sufficient /usr/lib/security/\$ISA/pam\_ldap.so.1'

You have completed this procedure.

When the LDAP authentication mechanism is selected, you must use the UNIX passwd command with the `-r` option to specify a repository. For example, if you want to change the password for a local UNIX user, the command is "**passwd -r files <userid>.**"

---

—End—

---

## Configuring the security server SunOne component to use a new HTTPS certificate

### Application

Use this procedure to make the SunOne component use the new server certificate to run in secure mode on the central security server and central security clients.

The activation of SunOne SSL mode is now automatic (part of install/upgrade).

Use one of the methods below according to your office configuration:

- "Simplex configuration (one server)" (page 475)
- "High-availability configuration (two servers)" (page 477)

### Prerequisites

An HTTPS certificate must already be installed on the Integrated Element Management System (IEMS) server. If required, refer to procedure ["Installing or replacing an HTTPS certificate on an SPFS-based server" \(page 641\)](#) to install the Apache server's certificate.

### Action

Perform the following steps to complete this procedure.

#### Simplex configuration (one server)

| Step | Action |
|------|--------|
|------|--------|

##### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server** is the IP address or host name of the IEMS server on which you want to configure the security SunOne component
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.

- 4 When prompted, enter the root password.
- 5 Reconfigure the SunOne IS client environment on the system to use SSL by typing

```
/opt/nortel/applications/security/current_slisext/sw
mgmt/bin/configure_slisext.sh -ssl
```

and pressing the Enter key.

The above command is entered on one line.
- 6 Restart the Web Server as follows:
  - a. Stop the Web Server by typing

```
servstop WEBSERVER
```

and pressing the Enter key.
  - b. Start the Web Server by typing

```
servstart WEBSERVER
```

and pressing the Enter key.
- 7 Restart the Web Services as follows:
  - a. Stop Web services by typing

```
servstop WEBSERVICES
```

and pressing the Enter key.
  - b. Start Web Services by typing

```
servstart WEBSERVICES
```

and pressing the Enter key.
- 8 Restart the Radius server as follows:
  - a. Stop the Radius server by typing

```
servstop RADSVR
```

and pressing the Enter key.
  - b. Start the Radius server by typing

```
servstart RADSVR
```

and pressing the Enter key.
- 9 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

---

—End—

---



**High-availability configuration (two servers)****Step Action*****At your workstation***

- 1 Log in to the Active server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server** is the IP address or host name of the Active IEMS server on which you want to configure the security SunOne component
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Reconfigure the SunOne IS client environment on the Active server to use SSL by typing  

```
/opt/nortel/applications/security/current_slisext/sw
mgmt/bin/configure_slisext.sh -ssl
```

and pressing the Enter key.  
The above command is entered on one line.
- 6 Initiate a failover by typing  

```
swact /Y
```

and pressing the Enter key.
- 7 Reconfigure the SunOne IS client environment on the newly Active server to use SSL by typing  

```
/opt/nortel/applications/security/current_slisext/sw
mgmt/bin/configure_slisext.sh -ssl
```

and pressing the Enter key.  
The above command is entered on one line.
- 8 Restart the Web Server on the newly Active server as follows:
  - a. Stop the Web Server by typing  

```
servstop WEBSERVER
```

and pressing the Enter key.

- b. Start the Web Server by typing

```
servstart WEBSERVER
```

and pressing the Enter key.

- 9 Restart the Radius server on the newly Active server as follows:

- a. Stop the Radius server by typing

```
servstop RADSVR
```

and pressing the Enter key.

- b. Start the Radius server by typing

```
servstart RADSVR
```

and pressing the Enter key.

- 10 Restart Web Services on the newly Active server as follows:

- a. Stop Web services by typing

```
servstop WEBSERVICES
```

and pressing the Enter key.

- b. Start Web Services by typing

```
servstart WEBSERVICES
```

and pressing the Enter key.

- 11 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

---

—End—

---

## Reverting the client server to its previous configuration

### Application

Use this procedure if you configured an SPFS-based central security client to use the Integrated Element Management System (IEMS) central security server, but want to revert to its previous configuration, which is not to use the IEMS central security server.

### Prerequisites

To perform this procedure, you need to have root user privileges.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
**server** is the IP address or host name of the SPFS-based server on which you want to revert the configuration
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Configure PAM as follows:
  - a. Access the command line interface by typing  

```
cli
```

 and pressing the Enter key.

#### *Example response*

```
Command Line Interface
1 - View
```

```
2 - Configuration
3 - Other
select -
```

- b. Enter the number next to the 'Configuration' option in the menu.

*Example response*

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3- OAMP Application Configuration
4- CORBA Configuration
5- IP Configuration
6- DNS Configuration
7- Syslog Configuration
8- Remote Backup Configuration
9- Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19- snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
Select -
```

- c. Enter the number next to the 'Security Services Configuration' option in the menu.

*Example response*

```
Security Services Configuration
1 - Socks Configuration
2 - Security Server Location Configuration
3 - PAM Configuration
4 - Common Inet Services (ftp, tftp, telnet, snmp
and nfs)
5 - Tools Inet Services (time, daytime)
6 - Other Inet Services
7 - proftpd User Configuration
8 - PKManager Certificate Installation
9 - WebPKProxy/PKClient Configuration
10 - query_registry (Query Network Services Package
Registration)
x - exit
select -
```

- d. Enter the number next to the 'PAM Configuration' option in the menu.

*Example response*

```
PAM Configuration
 1 - Central Security Client Configuration
x - exit
select -
```

- e. Enter the number next to the 'Central Security Client Configuration' option in the menu.

*Example response*

```
Central Security Client Configuration
 1 - pam_orig (Use Default PAM Configuration)
 2 - pam_radius (Use Security Server)
 3 - saml_passwd_conf (Configure saml password)
x - exit
select -
```

- f. Enter the number next to the 'pam\_orig' option in the menu.

*Example response*

```
===Executing "pam_orig"
Switching to original PAM configuration
Enter 'ok' to continue
Enter anything else to exit
```

- g. Accept to switch to the original PAM configuration by typing

**ok**

and pressing the Enter key.

*Example response*

```
Stopping pam_radius
Deconfiguring pam_radius
=== "pam_orig" completed successfully
```

- h. Exit each menu level of the command line interface to eventually exit the command line interface , by typing

**select - x**

and pressing the Enter key.

- 6** Re-provision the user accounts in Unix. In a two-server configuration, reprovision the user accounts on the active server. If required, refer to procedure Setting up local user accounts on an SSPFS-based server.

You have completed this procedure.

---

—End—

---

## Configuring the Single Sign-On token

### Application

Use this procedure to configure the values for the Single Sign-On (SSO) token and view the current SSO values. The SSO values are the time the Single Sign-On (SSO) token can remain idle before it becomes invalid, and the time the SSO token id can be used before it expires.

The SSO capability enables users to access multiple network elements, applications, and features from a single login session.

### Prerequisites

You need root user privileges.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
     **server** is the IP address or host name of the SPFS-based server on which you want to configure the SSO token
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Access the command line interface by typing  

```
cli
```

 and pressing the Enter key.

#### *Example response*

```
Command Line Interface
1 - View
```

```

2 - Configuration
3 - Other
X - exit
select -

```

- 6** Enter the number next to the 'Configuration' option in the menu.

*Example response*

```

Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Application Configuration
5 - CORBA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20- snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - exit
Select -

```

- 7** Enter the number next to the 'Succession Element Configuration' option in the menu.

*Example response*

```

Succession Element Configuration
1 - RADSVR Application Configuration
2 - S1IS Application Configuration
3 - RESMON Application Configuration
4 - NPM Application Configuration
5 - PSE Application Configuration
6 - OMPUSH Application Configuration
X - exit
select -

```

- 8** Enter the number next to the 'S1IS Application Configuration' option in the menu.

*Example response*



## S1IS Application Configuration

```

1 - LIST_TOKEN_VALUES (List the current session and
idle times set in Sun One.)
2 - TOKEN_ADMIN (Change the token idle and session
expiry time)
X - exit
select -

```

| If you want to              | Do      |
|-----------------------------|---------|
| view the current SSO values | step 9  |
| configure SSO values        | step 10 |

- 9** Enter the number next to the 'LIST\_TOKEN\_VALUES' option in the menu.

*Example response*

```

=== Executing "LIST_TOKEN_VALUES"
30 # Idle time of the token
365 # Session time of the token
=== "LIST_TOKEN_VALUES" completed successfully

```

| If you                                 | Do                                |
|----------------------------------------|-----------------------------------|
| want to re-configure SSO values        | step 10                           |
| do not want to re-configure SSO values | you have completed this procedure |

- 10** Enter the number next to the 'TOKEN\_ADMIN' option in the menu.

*Example response*

```

=== Executing "TOKEN_ADMIN"
Enter the new Token Idle Time:

```

- 11** When prompted, enter the desired value for the idle time of the SSO token, which is the time the token can remain idle before it becomes invalid. The default value is 30 minutes.

```

Enter the new Token Session Time:

```

*Example response*

- 12** When prompted, enter the desired value for the duration of the SSO token id, which is the time the token id can be used before it expires. The default value is 525600 minutes (365 days).

*Example response*

```

Enter the new Token Idle Time:60
Enter the new Token Session Time: 182
Success 0: Successfully completed.
NOTE: Operation succeeded.

```

```
=== "TOKEN_ADMIN" completed successfully
```

- 13** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

---

**—End—**

---

## Mapping of IEMS devices to authorization domains

The following table lists the authorization domain that devices in IEMS use. For a description of user groups, see ["Setting up local user accounts on an SPFS-Based Server"](#) (page 338)

When assigning users to secondary user groups, use the tables that follow, which provide a mapping between commands and secondary user groups. The list of the available tables is as follows:

- ["MGC and MG user groups"](#) (page 487)
- ["TRK user groups"](#) (page 491)
- ["EMS user groups"](#) (page 492)
- ["LN user groups"](#) (page 495)
- ["SEC user groups"](#) (page 496)

For mapping of CEM user groups to IEMS user group mappings, see ["Security group mapping between IEMS and CEM"](#) (page 497).

### MGC and MG user groups

| Command                                            | User group                 |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
|----------------------------------------------------|----------------------------|--------------------------------------|-----------------------|----------------------------|-----------------------|-----------------------|---------------------------------|------------------|-----------------------|------------------|
|                                                    | m<br>g<br>c<br>a<br>d<br>m | m<br>g<br>c<br>s<br>p<br>r<br>o<br>v | m<br>g<br>c<br>r<br>w | m<br>g<br>c<br>m<br>t<br>c | m<br>g<br>c<br>r<br>o | m<br>g<br>a<br>d<br>m | m<br>g<br>s<br>p<br>r<br>o<br>v | m<br>g<br>r<br>w | m<br>g<br>m<br>t<br>c | m<br>g<br>r<br>o |
| <b>CS 2000 Core</b>                                |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch MAPCI Session                               | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>GWC (GWC network element)</b>                   |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| GWC Unit Manager                                   | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Launch Command Line                                | x                          |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch TMM (see <a href="#">Note 1</a> )           | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Launch LMM (see <a href="#">Note 2</a> )           | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Launch CS 2000 tools (see <a href="#">Note 3</a> ) | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>MG 9000 network element</b>                     |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Update Radius Secret (see <a href="#">Note 4</a> ) |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |

| Command                                                                                                  | User group                 |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
|----------------------------------------------------------------------------------------------------------|----------------------------|--------------------------------------|-----------------------|----------------------------|-----------------------|-----------------------|---------------------------------|------------------|-----------------------|------------------|
|                                                                                                          | m<br>g<br>c<br>a<br>d<br>m | m<br>g<br>c<br>s<br>p<br>r<br>o<br>v | m<br>g<br>c<br>r<br>w | m<br>g<br>c<br>m<br>t<br>c | m<br>g<br>c<br>r<br>o | m<br>g<br>a<br>d<br>m | m<br>g<br>s<br>p<br>r<br>o<br>v | m<br>g<br>r<br>w | m<br>g<br>m<br>t<br>c | m<br>g<br>r<br>o |
| <b>SAM21</b>                                                                                             |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch SCU subnet                                                                                        | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Launch SCU manager                                                                                       | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>GWC-CARD / CICMEM-CARD/ CICM-CARD / 3PC-CARD /HLR-CARD / MC-CARD /USP-CARD / KDC-CARD /SAM21-UNIT</b> |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch SAM21 Card View                                                                                   | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>UAS network element</b>                                                                               |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Command Line                                                                                             | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>NE-USP / USP</b>                                                                                      |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch USP Manager                                                                                       | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Command Line                                                                                             | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>ERS 8600</b>                                                                                          |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| ERS 8600 Device Manager (Launch)                                                                         | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| ERS 8600 Device Manager (Configure)                                                                      | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Command Line                                                                                             | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Update Radius Secret (see <a href="#">Note 4</a> )                                                       | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>Media Server 2000</b>                                                                                 |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Configure MS2000 Automated INI Backup                                                                    |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| Config and Maintenance Tool                                                                              |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| <b>MG 3200</b>                                                                                           |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Configure MG 3200 Automated INI Backup                                                                   |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| Launch Configuration GUI                                                                                 |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| IPSec and IKE Config Tool                                                                                |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| <b>STORM</b>                                                                                             |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch Command Line                                                                                      | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Launch STORM Manager                                                                                     | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>SSTrunks NE and Units</b>                                                                             |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch Session Server                                                                                    | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |

| Command                                            | User group                 |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
|----------------------------------------------------|----------------------------|--------------------------------------|-----------------------|----------------------------|-----------------------|-----------------------|---------------------------------|------------------|-----------------------|------------------|
|                                                    | m<br>g<br>c<br>a<br>d<br>m | m<br>g<br>c<br>s<br>p<br>r<br>o<br>v | m<br>g<br>c<br>r<br>w | m<br>g<br>c<br>m<br>t<br>c | m<br>g<br>c<br>r<br>o | m<br>g<br>a<br>d<br>m | m<br>g<br>s<br>p<br>r<br>o<br>v | m<br>g<br>r<br>w | m<br>g<br>m<br>t<br>c | m<br>g<br>r<br>o |
| Command Line                                       | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>Media Application Server</b>                    |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| MAS Manager (P) (Configure)                        |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| MAS Manager (P) (Launch)                           |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| <b>CALL-AGENT-CORE</b>                             |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch MAPCI Session                               | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>CALL-AGENT-PLAT</b>                             |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Call Agent Platform Command Line                   | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>NE-CICM / CICM-Node</b>                         |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch CICM Manager                                | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>Media Gateway 7480/15000</b>                    |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Client-Server IP provisioning                      | x                          | x                                    | x                     | x                          | x                     | x                     | x                               | x                | x                     | x                |
| MDM Manager GUI                                    | x                          | x                                    | x                     | x                          | x                     | x                     | x                               | x                | x                     | x                |
| Legacy MDM tools                                   | x                          | x                                    | x                     | x                          | x                     | x                     | x                               | x                | x                     | x                |
| Command Line                                       | x                          | x                                    | x                     | x                          | x                     | x                     | x                               | x                | x                     | x                |
| Update Radius secret (see <a href="#">Note 4</a> ) | x                          | x                                    | x                     | x                          | x                     | x                     | x                               | x                | x                     | x                |
| <b>Media Gateway 20000</b>                         |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Client-Server IP provisioning                      | x                          | x                                    | x                     | x                          | x                     | x                     | x                               | x                | x                     | x                |
| MDM Manager GUI                                    | x                          | x                                    | x                     | x                          | x                     | x                     | x                               | x                | x                     | x                |
| Legacy MDM tools                                   | x                          | x                                    | x                     | x                          | x                     | x                     | x                               | x                | x                     | x                |
| Command Line                                       | x                          | x                                    | x                     | x                          | x                     | x                     | x                               | x                | x                     | x                |
| <b>MSS - Unknown</b>                               |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Client-Server IP Provisioning                      | x                          | x                                    | x                     | x                          | x                     | x                     | x                               | x                | x                     | x                |
| MDM Manager GUI                                    | x                          | x                                    | x                     | x                          | x                     | x                     | x                               | x                | x                     | x                |
| Command Line                                       | x                          | x                                    | x                     | x                          | x                     | x                     | x                               | x                | x                     | x                |
| <b>APPLN-APS</b>                                   |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| APS Manager (CMT)                                  | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| APS Audio Configuration Tool                       | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |

| Command                                                     | User group                 |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
|-------------------------------------------------------------|----------------------------|--------------------------------------|-----------------------|----------------------------|-----------------------|-----------------------|---------------------------------|------------------|-----------------------|------------------|
|                                                             | m<br>g<br>c<br>a<br>d<br>m | m<br>g<br>c<br>s<br>p<br>r<br>o<br>v | m<br>g<br>c<br>r<br>w | m<br>g<br>c<br>m<br>t<br>c | m<br>g<br>c<br>r<br>o | m<br>g<br>a<br>d<br>m | m<br>g<br>s<br>p<br>r<br>o<br>v | m<br>g<br>r<br>w | m<br>g<br>m<br>t<br>c | m<br>g<br>r<br>o |
| <b>MTX / MSC / HLR / TRI</b>                                |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch CEM (see <a href="#">Note 5</a> )                    |                            |                                      |                       |                            | x                     |                       |                                 |                  |                       |                  |
| <b>IMS/CSE / Media Portal</b>                               |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch MCP System Management Console                        |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| Command Line                                                |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| Launch MCS Client (P) (Configure)                           |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| Launch MCS Client (P) (Launch)                              |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| <b>APPLN-OSSGate</b>                                        |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| APPLN-OSSGate                                               |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| Launch OSSGate                                              |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| Launch BPT Servlet                                          |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| Launch BPT Command Line                                     |                            |                                      |                       |                            |                       | x                     | x                               | x                | x                     | x                |
| <b>MCS Manager for MCS/CSE and Media Portal</b>             |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch MCS Client (P) (Configure)                           | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Launch MCS Client (P) (Launch)                              | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Launch MCP System Management Console                        | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Launch Command Line                                         | x                          |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| <b>MCS Manager for SSLines (see <a href="#">Note 6</a>)</b> |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| MCP System Manager Console                                  | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Configure Session Mgr Platform Command Line (Launch)        | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Session and System Manager Command Line (Launch)            | x                          |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Configure Provisioning Clients                              | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| MCP Provisioning Client (Launch)                            | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <b>MCS SM Unit / FPM-UNIT</b>                               |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| MCP System Manager Console                                  | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Command Line                                                | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |

| Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | User group                 |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|--------------------------------------|-----------------------|----------------------------|-----------------------|-----------------------|---------------------------------|------------------|-----------------------|------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | m<br>g<br>c<br>a<br>d<br>m | m<br>g<br>c<br>s<br>p<br>r<br>o<br>v | m<br>g<br>c<br>r<br>w | m<br>g<br>c<br>m<br>t<br>c | m<br>g<br>c<br>r<br>o | m<br>g<br>a<br>d<br>m | m<br>g<br>s<br>p<br>r<br>o<br>v | m<br>g<br>r<br>w | m<br>g<br>m<br>t<br>c | m<br>g<br>r<br>o |
| <b>EMS-FPM-Mgr</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |
| Launch MCP System Management Console                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| Command Line                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | x                          | x                                    | x                     | x                          | x                     |                       |                                 |                  |                       |                  |
| <p><b>Note 1:</b> To launch TMM on the GWC network element, the user must be associated with an MGC user group and a TRK user group.</p> <p><b>Note 2:</b> To launch LMM on the GWC network element, the user must be associated with an MGC user group and an LN user group.</p> <p><b>Note 3:</b> To launch CS 2000 tools on a GWC network, the user must be associated with an MGC user group and an EMS user group.</p> <p><b>Note 4:</b> To update Radius secret also requires SECADM* privileges.</p> <p><b>Note 5:</b> To launch CEM requires MGCRO. Only MGCRO can launch CEM. MGC* cannot launch CEM.</p> <p><b>Note 6:</b> Members of ems* and mgc* can launch the MCS Manager in read-only mode. Members of emsadm and emsrw only have configuration or read-write privileges.</p> |                            |                                      |                       |                            |                       |                       |                                 |                  |                       |                  |

### TRK user groups

| Command | User group            |                  |                  |                  |                  |
|---------|-----------------------|------------------|------------------|------------------|------------------|
|         | t<br>r<br>k<br>a<br>s | t<br>r<br>k<br>s | t<br>r<br>k<br>r | t<br>r<br>k<br>m | t<br>r<br>k<br>r |

|                                                                                                                                 | d<br>m | p<br>r<br>o<br>v | w | t<br>c | o |
|---------------------------------------------------------------------------------------------------------------------------------|--------|------------------|---|--------|---|
| <b>GWC (GWC network element)</b>                                                                                                |        |                  |   |        |   |
| Launch TMM (see Note)                                                                                                           | x      | x                | x | x      | x |
| <b>APPLN-TMM</b>                                                                                                                |        |                  |   |        |   |
| Trunk Maintenance Manager                                                                                                       | x      | x                | x | x      | x |
| <b>APPLN-OSSGate</b>                                                                                                            |        |                  |   |        |   |
| Launch OSSGate                                                                                                                  | x      | x                | x | x      | x |
| Launch BPT Servlet                                                                                                              | x      | x                | x | x      | x |
| <b>Note:</b> To launch TMM on the GWC network element, the user must be associated with an MGC user group and a TRK user group. |        |                  |   |        |   |

**EMS user groups**

| Command                                            | User group                 |                                      |                       |                            |                       |
|----------------------------------------------------|----------------------------|--------------------------------------|-----------------------|----------------------------|-----------------------|
|                                                    | e<br>m<br>s<br>a<br>d<br>m | e<br>m<br>s<br>s<br>p<br>r<br>o<br>v | e<br>m<br>s<br>r<br>w | e<br>m<br>s<br>m<br>t<br>c | e<br>m<br>s<br>r<br>o |
| <b>EMS-APS-Mgr (APS Manager)</b>                   |                            |                                      |                       |                            |                       |
| APS Manager                                        | x                          | x                                    | x                     | x                          | x                     |
| <b>CS 2000 Manager (EMS-CS2K-Mgr)</b>              |                            |                                      |                       |                            |                       |
| Launch Core Manager Maintenance                    | x                          | x                                    | x                     | x                          | x                     |
| Launch MAPCI session                               | x                          | x                                    | x                     | x                          | x                     |
| Update Radius Secret (see <a href="#">Note 1</a> ) | x                          | x                                    | x                     | x                          | x                     |
| <b>EMS-GWC-Mgr (GWC Manager)</b>                   |                            |                                      |                       |                            |                       |
| GWC Manager (CMT)                                  | x                          | x                                    | x                     | x                          | x                     |
| GWC Manager Network View                           | x                          | x                                    | x                     | x                          | x                     |
| <b>MG 3200 Manager</b>                             |                            |                                      |                       |                            |                       |
| IPSec and IKE Configuration tool                   | x                          | x                                    | x                     | x                          | x                     |
| <b>MG 9000 Manager</b>                             |                            |                                      |                       |                            |                       |
| MG 9000 Manager                                    | x                          | x                                    | x                     | x                          | x                     |



| Command                                                     | User group                 |                                      |                       |                            |                       |
|-------------------------------------------------------------|----------------------------|--------------------------------------|-----------------------|----------------------------|-----------------------|
|                                                             | e<br>m<br>s<br>a<br>d<br>m | e<br>m<br>s<br>s<br>p<br>r<br>o<br>v | e<br>m<br>s<br>r<br>w | e<br>m<br>s<br>m<br>t<br>c | e<br>m<br>s<br>r<br>o |
| IPSec Tool                                                  | x                          | x                                    | x                     | x                          | x                     |
| <b>EMS-SAM21-Mgr</b>                                        |                            |                                      |                       |                            |                       |
| SAM21 Manager GUI                                           | x                          | x                                    | x                     | x                          | x                     |
| <b>EMS-UAS-Mgr (UAS Manager)</b>                            |                            |                                      |                       |                            |                       |
| UAS Manager (CMT)                                           | x                          | x                                    | x                     | x                          | x                     |
| <b>CICM Manager (EMS-CICM-Mgr/CICM-Mgr-Node)</b>            |                            |                                      |                       |                            |                       |
| Launch CICM Manager                                         | x                          | x                                    | x                     | x                          | x                     |
| Launch Command Line                                         | x                          | x                                    | x                     | x                          | x                     |
| <b>MCS Manager for MCS/CSE and Media Portal</b>             |                            |                                      |                       |                            |                       |
| Launch MCS Client (P) (Configure)                           | x                          | x                                    | x                     | x                          | x                     |
| Launch MCS Client (P) (Launch)                              | x                          | x                                    | x                     | x                          | x                     |
| Launch MCP System Management Console                        |                            |                                      |                       |                            |                       |
| <b>MCS Manager for SSLines (see <a href="#">Note 2</a>)</b> |                            |                                      |                       |                            |                       |
| MCP System Manager Console                                  | x                          | x                                    | x                     | x                          | x                     |
| Configure Session Mgr Platform Command Line (Launch)        | x                          | x                                    | x                     | x                          | x                     |
| Session and System Manager Command Line (Launch)            | x                          | x                                    | x                     | x                          | x                     |
| Configure Provisioning Clients                              | x                          | x                                    | x                     | x                          | x                     |
| MCP Provisioning Client (Launch)                            | x                          | x                                    | x                     | x                          | x                     |
| <b>MCS SM Unit / FPM-UNIT</b>                               |                            |                                      |                       |                            |                       |
| MCP System Manager Console                                  | x                          | x                                    | x                     | x                          | x                     |
| Command Line                                                | x                          | x                                    | x                     | x                          | x                     |
| <b>EMS-FPM-Mgr</b>                                          |                            |                                      |                       |                            |                       |
| Launch MCP System Management Console                        | x                          | x                                    | x                     | x                          | x                     |
| Command Line                                                | x                          | x                                    | x                     | x                          | x                     |
| <b>MDM-Mgr-UNIT</b>                                         |                            |                                      |                       |                            |                       |
| Update Radius secret (see <a href="#">Note 1</a> )          | x                          | x                                    | x                     | x                          | x                     |
| <b>EMS-MDM-Mgr</b>                                          |                            |                                      |                       |                            |                       |
| Client-Server IP provisioning                               | x                          | x                                    | x                     | x                          | x                     |

| Command                                            | User group                 |                                      |                       |                            |                       |
|----------------------------------------------------|----------------------------|--------------------------------------|-----------------------|----------------------------|-----------------------|
|                                                    | e<br>m<br>s<br>a<br>d<br>m | e<br>m<br>s<br>s<br>p<br>r<br>o<br>v | e<br>m<br>s<br>r<br>w | e<br>m<br>s<br>m<br>t<br>c | e<br>m<br>s<br>r<br>o |
| MDM Manager GUI                                    | x                          | x                                    | x                     | x                          | x                     |
| Legacy MDM Tools                                   | x                          | x                                    | x                     | x                          | x                     |
| Change MDM Centralized Account                     | x                          | x                                    | x                     | x                          | x                     |
| Command Line                                       | x                          | x                                    | x                     | x                          | x                     |
| Partition NEs                                      | x                          | x                                    | x                     | x                          | x                     |
| MDM Operator Client GUI                            | x                          | x                                    | x                     | x                          | x                     |
| Update Radius secret (see <a href="#">Note 1</a> ) | x                          | x                                    | x                     | x                          | x                     |
| <b>PLAT-SPFS</b>                                   |                            |                                      |                       |                            |                       |
| Command Line                                       | x                          | x                                    | x                     | x                          | x                     |
| Servman Applications Status                        | x                          | x                                    | x                     | x                          | x                     |
| Swact Cluster                                      | x                          |                                      | x                     |                            |                       |
| Restart SPFS                                       | x                          |                                      | x                     |                            |                       |
| Update Radius secret (see <a href="#">Note 1</a> ) | x                          | x                                    | x                     | x                          | x                     |
| <b>SPFS-UNIT</b>                                   |                            |                                      |                       |                            |                       |
| Command Line                                       | x                          | x                                    | x                     | x                          | x                     |
| Servman Applications Status                        | x                          | x                                    | x                     | x                          | x                     |
| Swact Cluster                                      | x                          | x                                    | x                     | x                          | x                     |
| Restart SPFS                                       | x                          | x                                    | x                     | x                          | x                     |
| <b>PLAT-SDM</b>                                    |                            |                                      |                       |                            |                       |
| Command Line                                       | x                          | x                                    | x                     | x                          | x                     |
| Update Radius secret (see <a href="#">Note 1</a> ) | x                          | x                                    | x                     | x                          | x                     |
| <b>PLAT-MDM</b>                                    |                            |                                      |                       |                            |                       |
| Command Line                                       | x                          | x                                    | x                     | x                          | x                     |
| Update Radius secret (see <a href="#">Note 1</a> ) | x                          | x                                    | x                     | x                          | x                     |
| <b>APPLN-QOS</b>                                   |                            |                                      |                       |                            |                       |
| Launch Command Line                                | x                          | x                                    | x                     | x                          | x                     |
| <b>APPLN-NPM</b>                                   |                            |                                      |                       |                            |                       |

| Command                                                                                                                                                                                                                                                   | User group |          |      |        |        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------|------|--------|--------|
|                                                                                                                                                                                                                                                           | emsadm     | emssprov | emsw | emsmtc | emsmro |
| Command Line                                                                                                                                                                                                                                              | x          | x        | x    | x      | x      |
| <b>Note 1:</b> To update Radius secret, the user also requires SECADM* privileges.<br><b>Note 2:</b> Members of ems* and mgc* can launch the MCS Manager in read-only mode. Members of emsadm and emsrw only have configuration or read-write privileges. |            |          |      |        |        |

### LN user groups

| Command                                                                                                                         | User group |         |      |       |      |
|---------------------------------------------------------------------------------------------------------------------------------|------------|---------|------|-------|------|
|                                                                                                                                 | lnadm      | lnsprov | lnrw | lnmtc | lnro |
| <b>GWC (GWC NE)</b>                                                                                                             |            |         |      |       |      |
| Launch LMM (see Note)                                                                                                           | x          | x       | x    | x     | x    |
| <b>APPLN-LMM</b>                                                                                                                |            |         |      |       |      |
| Line Maintenance Manager                                                                                                        | x          | x       | x    | x     | x    |
| <b>APPLN-OSSGate</b>                                                                                                            |            |         |      |       |      |
| Launch OSSGate                                                                                                                  | x          | x       | x    | x     | x    |
| Launch BPT Servlet                                                                                                              | x          | x       | x    | x     | x    |
| Launch BPT Command Line                                                                                                         | x          | x       | x    | x     | x    |
| <b>Note:</b> To launch LMM on the GWC network element, the user must be associated with an MGC user group and an LN user group. |            |         |      |       |      |

## SEC user groups

| Command                                                     | User group                 |                                      |                       |                            |                       |
|-------------------------------------------------------------|----------------------------|--------------------------------------|-----------------------|----------------------------|-----------------------|
|                                                             | s<br>e<br>c<br>a<br>d<br>m | s<br>e<br>c<br>s<br>p<br>r<br>o<br>v | s<br>e<br>c<br>r<br>w | s<br>e<br>c<br>m<br>t<br>c | s<br>e<br>c<br>r<br>o |
| <b>CS2k Manager (EMS-CS2K-Mgr)</b>                          |                            |                                      |                       |                            |                       |
| Update Radius Secret (also requires EMS* privileges)        | x                          |                                      |                       |                            |                       |
| <b>MG 9000 NE</b>                                           |                            |                                      |                       |                            |                       |
| Update Radius Secret (also requires MG* privileges)         | x                          |                                      |                       |                            |                       |
| <b>ERS 8600</b>                                             |                            |                                      |                       |                            |                       |
| Update Radius Secret (also requires MGC* privileges)        | x                          |                                      |                       |                            |                       |
| <b>MDM-Mgr-UNIT</b>                                         |                            |                                      |                       |                            |                       |
| Update Radius Secret (also requires EMS* privileges)        | x                          |                                      |                       |                            |                       |
| <b>EMS-MDM-Mgr</b>                                          |                            |                                      |                       |                            |                       |
| Update Radius Secret (also requires EMS* privileges)        | x                          |                                      |                       |                            |                       |
| <b>Media Gateway 7480/15000</b>                             |                            |                                      |                       |                            |                       |
| Update Radius Secret (also requires MGC* or MG* privileges) | x                          |                                      |                       |                            |                       |
| <b>PLAT-SPFS</b>                                            |                            |                                      |                       |                            |                       |
| Update Radius Secret (also requires EMS* privileges)        | x                          |                                      |                       |                            |                       |
| <b>PLAT-MDM</b>                                             |                            |                                      |                       |                            |                       |
| Update Radius Secret (also requires EMS* privileges)        | x                          |                                      |                       |                            |                       |

## Security group mapping between IEMS and CEM

The following table lists the CEM user group or client function to the user group mapping. For more information about CEM user groups, see *CEM Administration and Security*, 411-8111-942.

### CEM client function to user group mapping

| User groups / client function                        | User group           |                |               |                    |               |                |
|------------------------------------------------------|----------------------|----------------|---------------|--------------------|---------------|----------------|
|                                                      | m<br>gcs<br>pro<br>v | m<br>gc<br>mtc | m<br>gcr<br>o | e<br>ms<br>ad<br>m | e<br>ms<br>rw | e<br>ms<br>mtc |
| PMUser (can set thresholds on EMS)                   |                      |                |               |                    | X             |                |
| FMUser (can clear/acknowledge alarms on EMS)         |                      |                |               |                    |               | X              |
| CMUser (can provision network elements)              | X                    |                |               |                    |               |                |
| CTUser (can perform call trace on a network element) |                      | X              |               |                    |               |                |
| CEMAdminUser (can change user groups on EMS)         |                      |                |               | X                  |               |                |
| Observer (Read only)                                 |                      |                | X             |                    |               |                |

## Security Token Administration GUI overview

IEMS Security Token Administration GUI can be used to:

- view user session (or token) information
- terminate user sessions

IEMS Security Token Administration GUI displays all of the user sessions that are available to the Identity Server and displays the expiration time for each session. See "[List of valid tokens window](#)" (page 498).

IEMS Security Token Administration GUI displays the following:

- the user sessions that are available
- the amount of time (minutes) remaining for a user session
- the maximum time (minutes) before the session expires after which the user session must re authenticate to regain access
- the time (minutes) that have expired while the user session is idle
- the maximum time (minutes) that a user session can remain idle

For details on how to log in to the IEMS Security Token Administration GUI, see "[Launching the IEMS Security Token Administration GUI](#)" (page 499).

### List of valid tokens window

#### List of valid tokens

|                          | Type  | User    | Idle Time | Max Idle Time | Time Left | Max Session Time |
|--------------------------|-------|---------|-----------|---------------|-----------|------------------|
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525592    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525593    | 525600           |
| <input type="checkbox"/> | TTL   | amadmin | 0         | 5             | 525589    | 525600           |
| <input type="checkbox"/> | 2-use | user1   | 0         | 5             | 525599    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525592    | 525600           |
| <input type="checkbox"/> | 2-use | user1   | 0         | 5             | 525598    | 525600           |
| <input type="checkbox"/> | TTL   | user1   | 2         | 5             | 525595    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 1         | 5             | 525592    | 525600           |
| <input type="checkbox"/> | 2-use | user1   | 0         | 5             | 525599    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525593    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525592    | 525600           |

# 

### 

Use this procedure to launch the IEMS Security Token Administration GUI.

### 

To perform this procedure, the user account you are using to log into the IEMS Security Token Administration GUI must be set up on the IEMS server and have secadm or emsadm administration privileges.

To verify that the user account is set up, see the procedure for Listing all groups and users in the *IEMS Administration and Security* (NN10336-611) document.

### 

| Step | Action |
|------|--------|
|------|--------|

**At a web browser**

- Launch the IEMS Security Token Administration GUI using a URL in the format of:  
  
`https://hostname:8443/tokenadmin`  
*The Token Management window is displayed.*
- Enter your user name in the User Name field.
- Enter your password in the Password field.
- Click **Login**.  
  
*The List of valid tokens window opens as follows:*

|           |        |  |        |
|-----------|--------|--|--------|
| Terminate | Logout |  | Filter |
|-----------|--------|--|--------|

**List of valid tokens**

|                          | Type  | User    | Idle Time | Max Idle Time | Time Left | Max Session Time |
|--------------------------|-------|---------|-----------|---------------|-----------|------------------|
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525592    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525593    | 525600           |
| <input type="checkbox"/> | TTL   | amadmin | 0         | 5             | 525589    | 525600           |
| <input type="checkbox"/> | 2-use | user1   | 0         | 5             | 525599    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525592    | 525600           |
| <input type="checkbox"/> | 2-use | user1   | 0         | 5             | 525598    | 525600           |
| <input type="checkbox"/> | TTL   | user1   | 2         | 5             | 525595    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 1         | 5             | 525592    | 525600           |
| <input type="checkbox"/> | 2-use | user1   | 0         | 5             | 525599    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525593    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525592    | 525600           |

5 You have completed this procedure.

—End—



## Viewing a user session

### Application

Use this procedure to view one user session or a range of sessions that are available to the Identity Server.

### Prerequisites

You require a user account with administration privileges to perform this task.

### Action

| Step | Action |
|------|--------|
|------|--------|

#### *At the IEMS Security Token Administration GUI*

- 1 Log in to the IEMS Security Token Administration GUI.
  - a. Open the Token Management window. See "[Launching the IEMS Security Token Administration GUI](#)" (page 499).
  - b. Enter your user name in the User Name field.
  - c. Enter your password in the Password field.
  - d. Click **Login**.

*The List of valid tokens window opens.*

|           |        |   |        |
|-----------|--------|---|--------|
| Terminate | Logout | * | Filter |
|-----------|--------|---|--------|

| List of valid tokens     |       |         |           |               |           |                  |
|--------------------------|-------|---------|-----------|---------------|-----------|------------------|
|                          | Type  | User    | Idle Time | Max Idle Time | Time Left | Max Session Time |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525592    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525593    | 525600           |
| <input type="checkbox"/> | TTL   | amadmin | 0         | 5             | 525589    | 525600           |
| <input type="checkbox"/> | 2-use | user1   | 0         | 5             | 525599    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525592    | 525600           |
| <input type="checkbox"/> | 2-use | user1   | 0         | 5             | 525598    | 525600           |
| <input type="checkbox"/> | TTL   | user1   | 2         | 5             | 525595    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 1         | 5             | 525592    | 525600           |
| <input type="checkbox"/> | 2-use | user1   | 0         | 5             | 525599    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525593    | 525600           |
| <input type="checkbox"/> | 3-use | amadmin | 0         | 5             | 525592    | 525600           |

- 2 Enter a string in the Filter field.

**Note:** You can enter any character in the Filter field, including a meta-character (\*).

**Example**

To list all users whose names start with am, enter am\*.

To list all users whose names end with min, enter \*min.

To list all users whose names contain ad, enter \*ad\*.

- 3 Click **Filter** to refresh the List of valid tokens window and view the list of valid tokens using the value in the Filter field.
- 4 You have completed this procedure.

---

—End—

---



**3** Click **Terminate**.

*The List of valid tokens window is updated with the list of valid tokens.*

**4** You have completed this procedure.

---

**—End—**

---

---

## Health Monitors overview

---

If the Central Security Server's framework components fail, no security clients can access security services provided by the IEMS Central Security Server. Smart health monitors are provided to ensure the crucial security components are not dead or hung. In such situations, the failed components will be automatically restarted. There are three health monitors included on the IEMS server:

- Sun Identity Server health monitor
- Radius Server health monitor
- PAM login servlet health monitor

The health monitors are automatically started by the system after the monitored process starts and are disabled when the monitored process is stopped.

### Sun Identity Server health monitor

The identity server health monitor checks the health of the Sun Identity Server with the following three tests:

- Attempts to login with the user 'unknown'. This user should not be in the system and the login should fail with the proper return values from the server to indicate the server is still functioning.
- Performs a policy check with a system user. The policy test should succeed and indicate that the system user was able to login and perform the policy check.
- Confirms that the nsswitch configuration of the server works and the group 'secadm' can be retrieved through a query to nsswitch.

When any test fails, a customer log, EMSS 314, is generated and the health monitor restarts the Identity Server process group automatically. For details of this log, see *Carrier VoIP Fault Management Logs Reference*, NN10275-909.

### Radius Server health monitor

The Radius Server attempts to log in through the Radius Server using an invalid user name and password. The Radius Server should reply to a client with a message to indicate that the login failed. When the test fails, a customer log, EMSS 313, is generated. The Radius Server health monitor restarts the RADSVR process group automatically. For details of this log, see *Carrier VoIP Fault Management Logs Reference*, NN10275-909.

## PAM Login Servlet health monitor

The PAM login servlet health monitor attempts to retrieve the following URL:

`https://<hostname>:8443/pamlogin/servlet/pamlogin?ReqType=Unknown`

If this fails, the health monitor attempts to retrieve the following URL, which does not use SSL:

`http://<hostname>:8443/pamlogin/servlet/pamlogin?ReqType=Unknown`

After verifying that the WEBSERVICES process group is running, a customer log, EMSS 315, is generated to indicate the PAM login servlet was unhealthy and that WEBSERVICES is being restarted. For details of this log, see *Carrier VoIP Fault Management Logs Reference*, NN10275-909.

# Changing the authentication mechanism between UNIX and DCE

## Application

Use one of the following procedures to change the authentication mechanism between UNIX and Distributed Computing Environment (DCE) on a Server Platform Foundation Software (SPFS)-based server:

- "Switching from UNIX to DCE for authentication" (page 507)
- "Switching from DCE to UNIX for authentication" (page 510)

The default authentication mechanism is UNIX.

## Prerequisites

To perform this procedure, you need to have the root user ID and password for the SPFS-based server, and administrative privileges for the DCE server.

## Action

Perform the following steps to complete this procedure.

### Switching from UNIX to DCE for authentication

| Step                       | Action                                                                                                                                                                                                                                                    |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>At your workstation</i> |                                                                                                                                                                                                                                                           |
| 1                          | Log in to the server by typing<br><code>&gt; telnet &lt;server&gt;</code><br>and pressing the Enter key.<br>where<br><code>server</code> is the IP address or host name of the SPFS-based server on which you want to change the authentication mechanism |
| 2                          | When prompted, enter your user ID and password.                                                                                                                                                                                                           |
| 3                          | Change to the root user by typing<br><code>\$ su -</code><br>and pressing the Enter key.                                                                                                                                                                  |
| 4                          | When prompted, enter the root password.                                                                                                                                                                                                                   |
| 5                          | Disable the Name Service Cache daemon as follows: <ol style="list-style-type: none"> <li>Stop the Name Service Cache daemon</li> </ol>                                                                                                                    |

```
/etc/init.d/nscd stop
```

and pressing the Enter key.

b. Move the '/etc/nscd.conf' file to a different location.

- 6 Add 'dce' as another option for the password and group in the '/etc/nsswitch.conf' file.

The entries would look similar to 'passwd: files nis dce' and 'group: files nis dce' after the change.

This enables the group information to come from DCE.

- 7 Enable the DCE naming service server by typing

```
config.dce
```

and pressing the Enter key.

- 8 Enable the DCE PAM (Pluggable Authentication Module) by typing

```
config.dce pam
```

and pressing the Enter key.

- 9 Change the 'sesm' entry in the '/etc/pam.conf' file as 'sesm auth required /usr/lib/security/\$ISA/pam\_dce.so.1 try\_first\_pass'.

- 10 Add users and user groups to DCE as follows:

For details on user groups, refer to procedure Setting up local user accounts on an SSPFS-based server in this document.

a. Log in to DCE using the cell\_admin user ID and password.

b. Add a user to DCE by typing

```
dcecp> user create <userid> -group succssn
-password <password> -organization ossaps-users
-mypwd <cell_admin_password>
```

and pressing the Enter key.

where

**userid** is the user ID of the user you want to add

**password** is the password for the user ID you want to add

**cell\_admin\_password** is the password for cell\_admin

c. Add the necessary user groups in DCE by typing

```
dcecp> group create <groupname>
```

and pressing the Enter key.

where



**groupname**

is each of the following groups:

- trkadm, lnadm, mgcadm, mgadm, emsadm
- trkrw, lnrw, mgcrw, mgrw, emsrw
- trksprov, lnspov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmte, mgmtc, emsmte
- trkro, lnro, mgcro, mgro, emsro

- d. Add the new users to the new groups, one at a time, by typing

```
dcecp> group add <groupname> -member <userid>
```

and pressing the Enter key.

where

**groupname**

is each of the following groups:

- trkadm, lnadm, mgcadm, mgadm, emsadm
- trkrw, lnrw, mgcrw, mgrw, emsrw
- trksprov, lnspov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmte, mgmtc, emsmte
- trkro, lnro, mgcro, mgro, emsro

**userid**

is the user ID of a new user

- e. Verify the user was added by typing

```
dcecp> group list <groupname>
```

and pressing the Enter key.

where

**groupname**

is each of the following groups:

- trkadm, lnadm, mgcadm, mgadm, emsadm
- trkrw, lnrw, mgcrw, mgrw, emsrw
- trksprov, lnspov, mgcsprov, mgsprov, emssprov
- trkmtc, lnmtc, mgcmte, mgmtc, emsmte

- `trkro`, `Inro`, `mgcro`, `mgro`, `emsro`

You have completed this procedure.

When the DCE authentication mechanism is selected, you must use the UNIX `passwd` command with the `-r` option to specify a repository. For example, if you want to change the password for a local UNIX user, the command is "**passwd -r files <userid>**".

---

—End—

---

### Switching from DCE to UNIX for authentication

---

| Step | Action |
|------|--------|
|------|--------|

---

*At your workstation*

- |   |                                                                                                                                                                                                                  |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Log in to the server by typing<br><br><code>&gt; telnet &lt;server&gt;</code><br><br>and pressing the Enter key.<br><br>where<br><br><code>server</code> is the IP address or host name of the SPFS-based server |
| 2 | When prompted, enter your user ID and password.                                                                                                                                                                  |
| 3 | Change to the root user by typing<br><br><code>\$ su - root</code><br><br>and pressing the Enter key.                                                                                                            |
| 4 | When prompted, enter the root password.                                                                                                                                                                          |
| 5 | Change the 'sesm' entry in the '/etc/pam/conf' file as 'sesm auth required /usr/lib/security/\$ISA/pam_unix.so.1'.                                                                                               |
| 6 | Remove 'dce' as another option for the password and group in the '/etc/nsswitch.conf' file.<br><br>The entries would look similar to 'passwd: files nis' and 'group: files nis' after the change.                |
| 7 | Disable the DCE naming service server by typing<br><br><code># /etc/dcesetup unconfig.nssdce</code><br><br>and pressing the Enter key.                                                                           |
| 8 | Enable the Name Service Cache daemon as follows:                                                                                                                                                                 |

- a. Restore the '/etc/nscd.conf' file.
- b. Start the Name Service Cache daemon

# /etc/init.d/nscd start

and pressing the Enter key.

You have completed this procedure.

---

—End—

---

## Setting secure FTP proxy

### Application

In order to have a secure (encrypted) channel of FTP communication between the OSS/FTP clients and network elements, you need to set up SSH port forwarding. Use one of the following procedures to set secure FTP proxy using SSH port forwarding:

- ["Setting up SSH port forwarding on Unix"](#) (page 512)
- ["Setting up SSH port forwarding on Windows"](#) (page 513)

Once set up, SSH port forwarding establishes a port forwarding session from client to server, wherein all data forwarded are encrypted and hence secure.

### Prerequisites

You need to have SSH software.

### Action

Perform the following steps to complete this procedure.

#### Setting up SSH port forwarding on Unix

| Step | Action |
|------|--------|
|------|--------|

##### *At your workstation*

- 1 Install the SSH software.
- 2 Establish a port-forwarding session between your workstation and the SPFS-based server by typing
 

```
ssh -L 9999:<remote-host>:9999 <remote-host>
```

 and pressing the Enter key.
 

The first time you run the above command on your workstation in an attempt to forward data to remote-host, you will receive the following message and prompt:

```
The authenticity of host "remote-Host (1.2.3.4)"
can't be established. RSA key fingerprint is <finger
print information>. Are you sure you want to continue
connecting (yes/no)?
```

SSH is verifying whether the host "remote-host" is a trusted host and whether you want to continue connecting to it.
- 3 When prompted, confirm you want to continue connecting by typing

# **yes**

and pressing the Enter key.

- 4 When prompted, enter your password.

Once your password is verified, a port-forwarding session is established. From this point on, all new sessions connecting to 'localhost:local-port' will be forwarded to 'remote-host:remote-port' in a secure channel.

#### **Example**

You set up SSH port forwarding on machine A with the following command:

```
ssh-L 9999:SSPFS-based host:9999 SSPFS-based host
```

To securely transmit data from machine A to the SPFS-based server, you need to open a window logged into machine A, and type the following command:

```
telnet localhost 9999
```

The telnet connection automatically gets secured between machine A and the SPFS-based server.  
You have completed this procedure.

---

—End—

---

## Setting up SSH port forwarding on Windows

| Step | Action |
|------|--------|
|------|--------|

### *At your workstation*

- 1 Install PuTTY software.
- 2 Launch PuTTY to display the PuTTY Configuration window.
- 3 Configure SSH port forwarding as follows:
  - a. Click Session and complete the following fields:
    - In the Host Name (or IP address) field, enter the host name or IP address of the SPFS-based server.
    - In the Port field, enter 22.
    - Under Protocol: select SSH.
  - b. Click Tunnels and complete the following fields:
    - In the Source port field, enter any local port value, for example 9999.

- In the Destination field, enter <host:port>, where host is the host name of the SPFS-based server, and port is the port number on which the SPFS-based server listens for input (9999 is the standard port on which the SPFS-based server listens for a client connection)
- Select Local, and click Add.
- Click Open.

The first time you attempt to open a session, a PuTTY Security Alert window pops up to verify whether the host you want to connect to is a trusted host and whether you want to continue connecting to it.

4 Confirm you want to connect by clicking Yes in the PuTTY Security Alert window.

5 When prompted, enter your user ID and password.

This port-forwarding session is established.

You can now establish a secure connection between your workstation (client machine) and the SPFS-based server as long as the port-forwarding session you just created exists.

6 Establish a secure connection as follows:

- a. Click the computer icon in the top left-hand corner of the window.
- b. Select New Session... from the pull-down menu.

The PuTTY Configuration window opens.

- c. Click Session and complete the following fields:
  - In the Host Name (or IP address) field, enter *localhost*.
  - In the Port field, enter 9999.
  - Under Protocol:, select Telnet.

A secure session with the SPFS-based server is established.

You have completed this procedure.

---

—End—

---

---

## Modifying login session timeouts on an SPFS-based server

---

### Application

Use this procedure when you want to modify the login session timeouts for the following GUI and CLUI client applications:

- CS 2000 Management Tools GUI
- Network Patch Manager GUI and CLUI
- Line Maintenance Manager GUI
- Gateway Controller Manager GUI
- SAM21 Manager GUI
- Trunk Maintenance Manager GUI
- Batch Configuration Monitor GUI
- OSSGate CLUI
- Batch Provisioning Tool CLUI
- Audio Media Server CLUI
- Integrated Element Management System GUI

You can modify the following login session timeouts:

- user inactivity timeout, which specifies the amount of time a client session can be inactive before the user is required to log in again.
- user termination timeout, which specifies the amount of time a user has to log in again before the user is forced to exit the client session.

Both the user inactivity timeout and the user termination timeout have a default value of 10 minutes. If the default value is acceptable, you do not need to perform this procedure.

You can disable the timeout functionality in its entirety by setting the user inactivity timeout to 0, or only disable the user termination timeout by setting its value to 0.

For HA cluster systems, timeout values are set independently for each side of the cluster. If timeout values have only been changed on the active side of a cluster and a SWACT occurs, the timeout values will take the inactive side settings. To ensure consistent interface performance following a

SWACT, when a default timeout setting is changed on the active side of the cluster, the corresponding setting should also be changed on the inactive side of the cluster.

## Prerequisites

To perform this procedure, you need to have root user privileges.

## Action

Perform the following steps to complete this procedure.

In a two-server configuration, you must perform this procedure on both the active and inactive servers.

| Step | Action |
|------|--------|
|------|--------|

### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server** is the IP address or host name of the SPFS-based server, or the physical IP address of the active or inactive server in a two-server configuration.

- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

- 4 When prompted, enter the root password.

- 5 Access the command line interface by typing

```
cli
```

and pressing the Enter key.

### *Example response*

Command Line Interface

```
1 - View
```

```
2 - Configuration
```

```
3 - Other
```

```
select -
```

- 6 Enter the number next to the "Configuration" option in the menu.



*Example response*

## Configuration

```

1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Application Configuration
4 - CORBA Configuration
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
Select -

```

- 7 Enter the number next to the 'Login Session' option in the menu.

*Example response*

## Login Session

```

1 - login_session_timeout (User Inactivity
 Timeout Configuration)
2 - login_session_termination (User
 Termination Timeout Configuration)
3 - login_session_reauthentication (User
 Reauthentication Disable Timeout
 Configuration)
4 - login_session_server (Login Session Master
 Server Configuration)
5 - telnet_greeting (Telnet Login Greeting)
6 - login_retries (Login Retries Limit)
x - exit
select -

```

- 8 Use the following table to determine your next step.

| If you want to modify the      | Do      |
|--------------------------------|---------|
| user inactivity timeout value  | step 9  |
| user termination timeout value | step 11 |

- 9** Enter the number next to the 'login\_session\_timeout' option in the menu.

*Example response*

```
===Executing "login_session_timeout"
Current value for Session Timeout is:
USER_INACTIVITY_TIMEOUT=10
export USER_INACTIVITY_TIMEOUT
Enter the Login Session Timeout Value in Minutes (0 ->
1440):
```

- 10** When prompted, enter the desired login session timeout value, or press the Enter key to accept the current value.

Specifying a value of 0 disables the timeout functionality in its entirety.

*Example response*

```
Modifying Login Session Timeout.
Done.
```

Proceed to step [11](#) if you want to change the login session termination timeout value, otherwise go to step [13](#).

- 11** Enter the number next to the 'login\_session\_termination' option in the menu.

*Example response*

```
===Executing "login_session_termination"
Current value for Session Timeout is:
USER_INACTIVITY_TIMEOUT=10
export USER_TERMINATION_TIMEOUT
Enter the Logging Session Termination Timeout Value in
Minutes (0 -> 1440):
```

- 12** When prompted, enter the desired login session termination timeout value, or press the Enter key to accept the current value.

*Example response*

```
Modifying Login Session Termination Timeout.
Done.
```

Specifying a value of 0 disables the login session termination timeout.

- 13** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

---

—End—

---

## Configuring Automated Data Backups on an SPFS-Based Server

### Application

Use this procedure to view or change the configuration settings for an automated data backup on a Server Platform Foundation Software (SPFS) based server. The automated backup backs up Oracle and critical data.

#### ATTENTION

Log SSPFS320 is generated when an automated data backup fails. Refer to the *Carrier Voice over IP Fault Management Logs Reference document* (NN10275-909) for log details.

You can also schedule a full system backup that overwrites a previous one on a backup media or copy the last successful Oracle backup to DVD or tape when performing an automated data backup on an SPFS-based server. This functionality is designed for use in dark office' conditions where you need to copy backup data more than once before the backup media is ejected from the server, refer to the procedure *Configuring Dark Office Backups on an SPFS-Based Server*, in *Nortel ATM/IP Solution-level Configuration* (NN10409-500).

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
**server** is the IP address or host name of the SPFS-based server on which you want to configure automated data backups
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su -
```

and pressing the Enter key.

- 4 When prompted, enter the root password.

- 5 Access the command line interface by typing

```
cli
```

and pressing the Enter key.

*Response*

```
Command Line Interface
```

```
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

- 6 Enter the number next to the "Configuration" option in the menu.

*Example response*

```
Configuration
```

```
1 - NTP Configuration
2 - Apache Proxy Configuration
3- OAMP Application Configuration
4- CORBA Configuration
5- IP Configuration
6- DNS Configuration
7- Syslog Configuration
8- Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
Select -
```

- 7 Enter the number next to the "Database Configuration" option in the menu.

*Example response*

```
Database Configuration
```

```
1 - change_db (Change Database Host)
2 - change_orabackup (Configure database
 backup)
```

```
X - exit
select -
```

- 8** Enter the number next to the "change\_orabackup" option in the menu.

*Example response*

```
===Executing "change_orabackup"
Current setting:
Automated Backup Enabled N
Backup Time 6:00 Hours
Enable Automated backup (default: N):
```

- 9** When prompted, enter Y to enable automated backup or press the Enter key to accept the default value (N) to disable automated backup.

*Example response*

```
Set backup hour to: (default: 22):
```

- 10** When prompted, enter the time you want the automated backup to occur, or press the Enter key to accept the default value.

*Example response*

```
New settings:
Automated Backup Enabled Y
Backup Time 22:00 Hours
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

- 11** Commit the changes by typing

```
ok
```

and pressing the Enter key.

*Example response*

```
=="change_orabackup" completed successfully
```

**ATTENTION**

If enabled, automated backup will start within the first 45 seconds of the backup hour. If the backup hour is set to the current hour, automated backup will occur 24 hours from the current hour.

- 12** Exit each menu level of the command line interface to eventually return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

---

—End—

---

## Performing the 146 GB disk drive upgrade on a Sun Netra 240 server

### Application

Use this procedure to perform the semi-automated disk upgrade on field-grade Netra 240 servers, to replace the two 72 GB drives with two new 146 GB drives.

### Prerequisites

This procedure has the following prerequisites:

- You know the root password on the server to be upgraded
- You have direct console-access to the server (recommended)
- All mirrors must have full redundancy, in an “Okay” state
- No other significant SPFS maintenance is being performed
- This procedure must only be performed after the platform has been upgraded to SN09U or later.
- The platform being upgraded is a Sun Netra 240 with two existing 72 GB drives installed.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

#### *At the server console*

- 1 Establish a login session to the server to be upgraded, preferably at the system console and log in as the root user. For detailed steps, refer to procedure Logging in to an SPFS-based server.

If the server to be upgraded is part of a cluster, ensure you log in to the active node.

- 2 Navigate to the Disk Drive Upgrade menu within the command line interface as follows:

- a. Access the command line interface by typing
 

```
cli
```

 and pressing the Enter key.

#### *Example response*

```
Command Line Interface
1 - View
2 - Configuration
```



```

3 - Other
X - Exit
select -

```

- b. Enter the number next to the “Configuration” option in the menu.

*Example response*

```

Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - OAMP Configuration
4 - COBRA Configuration
5 - IP Configuration
6 - DNS Configuration
7 - Syslog Configuration
8 - Remote Backup Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Disk Drive Upgrade
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - Exit
select -

```

- c. Enter the number next to the “Security Services Configuration” option in the menu.

*Example response*

```

Disk Drive Upgrade
1 - disk_drive_upgrade_146gb (Perform 146 GB Disk
Drive Upgrade)
x - exit
select -

```

- 3** Enter the number next to the “disk\_drive\_upgrade\_146gb” option in the menu.

A welcome and warning message is displayed, together with the option to continue.

- 4** Enter **y** and press Enter to continue with this upgrade, or accept the default answer of **no** to abort the upgrade.

- 5 A series of steps are performed automatically until further action by the operator is required. The automatic steps (which are displayed to the operator) are:

- Remove the disk from the boot device list
- Detach submirrors on the disk
- Clear submirrors on the disk
- Delete the disk from the meta database
- Unconfigure the disk

A major alarm is raised when these automated processes are run. This is normal and not an indication of an upgrade failure. An example alarm is shown below.

```
Apr 18 13:30:30 cs2k0ptm unix: MAJOR ALARM is set.
SC Alert: MAJOR ALARM is set
Apr 18 13:30:31 cs2k0ptm root:
/opt/resmon/Hardware/disk_check_ksh: Disk or disk
mirroring erros: See system alarms for details. d101:
Concat/Stripe is cleared
```

Once these automatic steps have completed, the user is requested to physically replace the disk.

*Example response*

```
Please replace disk 0 with the new 146 GB disk drive.
The disk to be replaced is labeled "HDD 0" on the
chassis. The blue removal lamp should be lit on the
chassis, adjacent to the disk drive to be removed.
Confirm below when the disk drive has been replaced.
Has the disk drive been replaced? [no] y
```

- 6 Physically replace the drive indicated with the new 146 GB drive. Enter **y** and press Enter to continue.

Further automatic steps now prepare this new drive for use. The user is kept informed as to the progress during the steps:

- Scan for all current system devices
- Configure the disk
- Check the disk is the expected size
- Format the disk
- Add the disk to the meta database
- Initialize submirrors on the disk
- Update disk ID in the meta database
- Attach submirrors to the disk

- Update the boot device list with the disk

- 7 If you were currently upgrading the first hard drive, disk 0, steps 5 and 6 are repeated for the second hard drive, disk 1.
- 8 Upon completion of the second hard drive upgrade, confirmation is displayed.

*Example response*

```
*** Disk drive upgrade procedure has completed
successfully. ***
*** Please take a new full system backup as soon as
possible. ***
```

A log of the upgrade procedure is maintained and stored in the file /var/adm/messages.

- 9 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

- 10 If the server you have upgraded is part of a cluster, proceed to step 11. Otherwise, you have completed this procedure.

- 11 Establish a login session to the inactive server to be upgraded, preferably at the system console and log in as the root user. For detailed steps, refer to procedure Logging in to an SPFS-based server.

Ensure you log on to the inactive node.

- 12 Return the inactive server to the "ok" prompt by typing

```
init 0
```

and pressing the Enter key. Wait until the "ok" prompt is displayed.

- 13 Physically replace both the 72 GB disks on the inactive node with the 146 GB disks.

- 14 Perform a clone to copy all data from the active node to the inactive node. Refer to procedure "Cloning the image of one server in a cluster to the other server".

You have completed this procedure.

---

—End—

---

## Cloning the image of one node in a cluster to the other node

### Application

Use this procedure to clone the image of the active node in a cluster to the inactive node.

### Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password
- you need console access to the Inactive node if this is the first time you clone, if you replaced the Inactive unit or if you executed a reverse restore (switched unit 0 and 1)

#### ATTENTION

Ensure that no provisioning activities are in progress, or are scheduled to take place during this procedure.

### Action

Perform the following steps to complete this procedure.

| Step                                                                                                                                                                                                          | Action                                                                                                                                                                                                                                                    |          |    |                   |        |              |        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----|-------------------|--------|--------------|--------|
| <b>At your workstation</b>                                                                                                                                                                                    |                                                                                                                                                                                                                                                           |          |    |                   |        |              |        |
| 1                                                                                                                                                                                                             | Establish a login session to the Active node using one of the following methods:                                                                                                                                                                          |          |    |                   |        |              |        |
| <table border="1"> <thead> <tr> <th>If using</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>telnet (unsecure)</td> <td>step 2</td> </tr> <tr> <td>ssh (secure)</td> <td>step 7</td> </tr> </tbody> </table> |                                                                                                                                                                                                                                                           | If using | Do | telnet (unsecure) | step 2 | ssh (secure) | step 7 |
| If using                                                                                                                                                                                                      | Do                                                                                                                                                                                                                                                        |          |    |                   |        |              |        |
| telnet (unsecure)                                                                                                                                                                                             | step 2                                                                                                                                                                                                                                                    |          |    |                   |        |              |        |
| ssh (secure)                                                                                                                                                                                                  | step 7                                                                                                                                                                                                                                                    |          |    |                   |        |              |        |
| 2                                                                                                                                                                                                             | Log in to the Active node using telnet (unsecure) by typing<br><code>&gt; telnet &lt;server&gt;</code><br>and pressing the Enter key.<br>where<br><b>server</b> is the cluster IP address, which automatically defaults to the Active node in the cluster |          |    |                   |        |              |        |
| 3                                                                                                                                                                                                             | When prompted, enter your user ID and password.                                                                                                                                                                                                           |          |    |                   |        |              |        |

#### At your workstation

- 1 Establish a login session to the Active node using one of the following methods:

| If using          | Do     |
|-------------------|--------|
| telnet (unsecure) | step 2 |
| ssh (secure)      | step 7 |

- 2 Log in to the Active node using telnet (unsecure) by typing  
`> telnet <server>`  
 and pressing the Enter key.  
 where  
**server** is the cluster IP address, which automatically defaults to the Active node in the cluster
- 3 When prompted, enter your user ID and password.

- 4 Change to the root user by typing  
`$ su - root`  
 and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 Proceed to step 9.
- 7 Log in using ssh (secure) by typing  
`> ssh -l root <server>`  
 and pressing the Enter key.  
 where  
`server` is the cluster IP address, which automatically defaults to the Active node in the cluster  
 If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.
- 8 When prompted, enter the root password.
- 9 Verify the status of replicated disk volumes by typing  
`# udfstat`  
 and pressing the Enter key.

| If all file systems are | Do                                 |
|-------------------------|------------------------------------|
| ACTIVE                  | step 10                            |
| not ACTIVE              | contact your next level of support |

- 10 Determine the server profile. Access the command line interface by typing  
`# cli`  
 and pressing the Enter key.  
*Example response*  
 Command Line Interface  
   1 - View  
   2 - Configuration  
   3 - Other  
   X - exits  
 select -
- 11 Enter the number next to the View option in the menu.  
*Example response*

```

View
 1 - SPFS_soft (Display Software Installation
Level Of SPFS)
 2 - chk_SPFS (Check SPFS Processes)
 3 - sw_conf (The software configuration
of the wrtypyxp)
 4 - cpu_util (Overall CPU utilization)
 5 - cpu_util_proc (CPU utilization by process)
 6 - port_util (I/O port utilization)
 7 - disk_util (Filesystem utilization)
X - exit
select -

```

- 12** Enter the number next to the SPFS\_soft option in the menu.

*Example response*

```

=== Executing "SPFS_soft"
SPFS version: 08.0 Build: 200508421 Server Profile:
cbm850
=== "SPFS_soft" completed successfully

```

- 13** Determine the Server Profile.

| If the Server Profile is | Do                      |
|--------------------------|-------------------------|
| cbm850                   | step <a href="#">28</a> |
| anything else            | step <a href="#">14</a> |

- 14** Verify that all applications on the server are running by typing

```
servquery -status all
```

and pressing the Enter key.

*Example response:*

```

APP NAME STATUS
===== =====
SNMP_POLLER RUNNING
DELEGATE RUNNING
PROP_SRV RUNNING
WEBSERVER RUNNING
DATABASE RUNNING
SAM21EM RUNNING
SESMSservice RUNNING
CORBA RUNNING
ORA_ARCHIVE_ROTATOR RUNNING
OMPUSH RUNNIN
GBOOTP RUNNING
WEBSERVICES RUNNING
ORA_AUTO_BACKUP RUNNING
APS RUNNING

```

NPM

RUNNING

- 15 Use the following table to determine your next step.

| If                                       | Do      |
|------------------------------------------|---------|
| all applications are running             | step 18 |
| one or more applications are not running | step 16 |

- 16 Start each application that is not running by typing

```
servstart <app_name>
```

and pressing the Enter key.

where

**app\_name** is the name of the application that is not in a RUNNING state, for example, SAM21EM

- 17 Use the following table to determine your next step.

| If                                    | Do                                 |
|---------------------------------------|------------------------------------|
| one or more applications do not start | contact your next level of support |
| all applications are running          | step 18                            |

- 18 Use the following table to determine your next step.

| If this server is            | Do      |
|------------------------------|---------|
| running the NPM software     | step 19 |
| not running the NPM software | step 21 |

The Network Patch Manager (NPM) software is running on this server if NPM appeared in the response from step 14.

- 19 Verify the Patching Server Element (PSE) server application is running by typing

```
pse status
```

and pressing the Enter key.

| If PSE is   | Do      |
|-------------|---------|
| running     | step 21 |
| not running | step 20 |

- 20 Start the PSE server application by typing

```
pse start
```

and pressing the Enter key.

| If PSE         | Do                                 |
|----------------|------------------------------------|
| does not start | contact your next level of support |
| starts         | step 21                            |

- 21 Use the following table to determine your next step.

| If this server is                                 | Do      |
|---------------------------------------------------|---------|
| running the CS 2000 Management Tools software     | step 22 |
| not running the CS 2000 Management Tools software | step 28 |

- 22 Verify that the SESMservice application is fully functional by typing

```
ptmctl status
```

and pressing the Enter key.

*Example response:*

```
SESM STATUS

COMPONENT STATUS

Proxy Agent RUNNING
RMI Registry RUNNING
Snmpfactory RUNNING
MI2 Server RUNNING
Current number of SESM processes running: 4 (of 4)
SESM APPLICATION STATUS: All Applications ready
```

- 23 Use the following table to determine your next step.

| If the SESMService is | Do                                 |
|-----------------------|------------------------------------|
| not fully functional  | contact your next level of support |
| fully functional      | step 24                            |

- 24 Deconfigure NDS replication before cloning the node by typing

```
#cp /etc/nsswitch.files /etc/nsswitch.conf
```

and pressing the Enter key.

- 25 Type



```
#cp /etc/pam.conf.orig /etc/pam.conf
```

and press the Enter key.

26 Type

```
#cd /opt/nortel/applications/security/current_slisext
/swmgmt/bin
```

and press the Enter key.

27 Type

```
#./configure_slisext.sh -replica disable
```

and press the Enter key.

28 Use the following table to determine your next step.

| If                                                                                                                                                   | Do      |
|------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| this is the first time you are cloning the unit, or you replaced the unit or executed a reverse restore (i.e. switched unit 0 and unit 1)            | step 29 |
| this is not the first time you are cloning the unit, and you did not replace the unit or execute a reverse restore (i.e. switched unit 0 and unit 1) | step 36 |

29 Use the following table to determine your next step.

| If you                                                | Do      |
|-------------------------------------------------------|---------|
| know the Ethernet address of the Inactive unit        | step 34 |
| do not know the Ethernet address of the Inactive unit | step 30 |

### ***At the console connected to the inactive node***

30 Determine the Ethernet address of the Inactive node. Log in to the inactive node through the console (port A) using the root user ID and password.

Ensure you are on the Inactive server by typing `ubmstat`. If `ClusterIndicatorACT` is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server. The response must display `ClusterIndicatorSTBY`, which indicates you are on the Inactive server.

- 31** Bring the system to the OK prompt by typing  
`# init 0`  
 and pressing the Enter key.
- 32** At the OK prompt, display the Ethernet address of the inactive node by typing  
`OK banner`  
 and pressing the Enter key.

*Example response:*

```
Sun Fire V240, No keyboard
Copyright 1998-2002 Sun Microsystems, Inc. All
rights reserved. OpenBoot 4.8.0.build_04, 2048 MB
memory installed, Serial #52964131. Ethernet address
0:3:ba:28:2b:23, Host ID: 83282b23.
```

Ethernet address formats can vary from machine to machine. The fields in an Ethernet address may contain one alphanumeric character or two alphanumeric characters, both are acceptable formats.

- 33** Record the Ethernet address that is displayed.

***At your workstation (login session to the Active node)***

- 34** Start the cloning process by typing  
`# startb <Ethernet address>`  
 and press the Enter key.  
 where  
**Ethernet address** is the Ethernet address of the Inactive unit
- 35** Proceed to step [37](#)
- 36** Start the cloning process by typing  
`# startb`  
 and press the Enter key.
- 37** Use the following table to determine your next step.

| If the system                                               | Do                      |
|-------------------------------------------------------------|-------------------------|
| prompts you to enter the command "boot net - image"         | step <a href="#">38</a> |
| does not prompt you to enter the command "boot net - image" | step <a href="#">42</a> |

- 38 Connect to the console port of the Inactive node.

| If the console displays | Do      |
|-------------------------|---------|
| the OK prompt           | step 41 |
| the login prompt        | step 39 |

***At the console connected to the inactive node***

- 39 Log in using the root user ID and password.
- 40 Bring the system to the OK prompt by typing  
`# init 0`  
 and pressing the Enter key.
- 41 At the OK prompt, boot the inactive node from the image of the active node by typing  
`OK boot net - image`  
 and press the Enter key.  
 There must be a space between the "-" and "image".

***Example response:***

```
SC Alert: Host System has Reset
Sun Fire V240, No Keyboard
Copyright 1998-2002 Sun Microsystems, Inc. All
rights reserved. OpenBoot 4.8.0.build_04, 2048 MB
memory installed, Serial #52964131. Ethernet address
0:3:ba:28:2b:23, Host ID: 83282b23.
Rebooting with command: boot net - image
.
.
.
SC Alert: Host System has Reset
```

***At your workstation (login session to the Active node)***

- 42 Monitor the progress of the cloning from the active node. Cloning the inactive node takes approximately one hour to complete.

***Example response:***

```
Waiting for network response from unit1-priv0...
received network response from unit1-priv0...
Waiting for unit1-priv0 to clone data...
waiting...1
waiting...2
waiting...3
unit1-priv0 is cloning: /export/d2
.
```

```
.
.
Verifying cluster status of unit1-priv0
waiting for cluster filesystem status to become normal.
Deleted snapshot 0.
Deleted snapshot 1.
Deleted snapshot 2.
Deleted snapshot 3.
d99: Soft Partition is cleared
```

- 43** Once the cloning is complete, wait approximately 5 minutes before you proceed to the next step.

***At your workstation (login session to the Active node)***

- 44** Verify the status of replicated disk volumes by typing

```
udfstat
```

and pressing the Enter key.

| If all file systems are | Do                                 |
|-------------------------|------------------------------------|
| ACTIVE                  | step <a href="#">45</a>            |
| not ACTIVE              | contact your next level of support |

***At your workstation***

- 45** Establish a login session to the Inactive node using one of the following methods:

| If using          | Do                      |
|-------------------|-------------------------|
| telnet (unsecure) | step <a href="#">46</a> |
| ssh (secure)      | step <a href="#">51</a> |

- 46** Log in to the Inactive node using telnet (unsecure) by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server** is the physical IP address of the Inactive node in the cluster

- 47** When prompted, enter your user ID and password.

- 48** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

**49** When prompted, enter the root password.

**50** Proceed to step 53.

**51** Log in to the by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

**server** is the physical IP address of the Inactive node in the cluster

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.

**52** When prompted, enter the root password.

**53** Verify the status of replicated disk volumes by typing

```
udfstat
```

and pressing the Enter key.

| If all file systems are | Do                                 |
|-------------------------|------------------------------------|
| ACTIVE                  | step 54                            |
| not ACTIVE              | contact your next level of support |

### ***At your workstation (login session to the Active node)***

**54** Complete the cloning process by typing

```
finishb
```

and pressing the Enter key.

### ***Sessions on both the Active and Inactive nodes***

**55** Reconfigure NDS replication on both the active and inactive nodes after the cloning process is completed by typing

```
#cp /etc/nsswitch.saml /etc/nsswitch.conf
```

and pressing the Enter key.

**56** Type

```
#cp /etc/pam.conf.is /etc/pam.conf
```

and press the Enter key.

- 57** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

**—End—**

---

## Starting the SESM server application

### Application

Use this procedure to start the Succession Element and Subelement Manager (SESM) server application on the SPFS-based server.

### Prerequisites

None

### Action

Perform the steps that follow to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

***At your workstation***

- 1 Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the ubmstat command.

For detailed steps, refer to procedure "Logging in to an SPFS-based server".

- 2 Verify the status of the SESM server application by typing

```
servman query -status -group SESMService
```

and pressing the Enter key.

| If the response indicates | Do                     |
|---------------------------|------------------------|
| not running               | <a href="#">step 3</a> |
| running                   | <a href="#">step 6</a> |

- 3 Start the SESM server application by typing

```
servstart SESMService
```

and pressing the Enter key.

- 4 Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to start.

- 5 Verify the SESM server application started as follows:

- a. Verify the SESM services started by typing

```
servman query -status -group SESMSERVICE
```

and pressing the Enter key.

*Example response:*

```
CS2K Management Tools are running
```

- b. Verify the SESM applications started by typing

```
ptmctl status
```

and pressing the Enter key.

*Example response:*

```
SESM STATUS -----
 COMPONENT STATUS

Proxy Agent RUNNING
RMI Regisry RUNNING
Snmpfactory RUNNING
MI2 Server RUNNING
Current number of SESM processes running: 4 (of 4)
SESM APPLICATION STATUS: All Applications Ready
```

- 6** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

---

—End—

---



## Starting the SAM21 Manager server application

### Application

Use this procedure to start the SAM21 Manager server application on the SPFS-based server that is hosting the CS 2000 Management Tools.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

*At your workstation*

- 1 Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the `ubmstat` command.

For detailed steps, refer to procedure "Logging in to an SPFS-based server".

- 2 Verify the status of the SAM21 Manager server application by typing  

```
servman query -status -group SAM21EM
```

and pressing the Enter key.

| If SAM21EM is | Do                     |
|---------------|------------------------|
| not running   | <a href="#">step 3</a> |
| running       | <a href="#">step 5</a> |

- 3 Start the SAM21EM server application by typing  

```
servstart SAM21EM
```

and pressing the Enter key.
- 4 Verify the SAM21EM server application started by typing  

```
servman query -status -group SAM21EM
```

and pressing the Enter key.

*Example response:*

```
Executing: /opt/servman/bin/servquery -status - group
SAM21EM
Succession SAM21 Element Manager version: SAM21EM_9
_020_0
Current status of the Succession SAM21 Element Manager:
 SNMP Access Gateway is running.
 SAM21 Element Manager Server is running.
```

- 5** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure

---

**—End—**

---

## Starting the NPM server application

### Application

Use this procedure to start the Network Patch Manager (NPM) server application on a Server Platform Foundation Software (SPFS)-based server.

### Prerequisites

You need root user privileges to perform this procedure, and CORBA must be running in order for the NPM to come up.

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the Active server.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
     **server** is the IP address or host name of the SPFS-based server where the NPM server application resides  
 In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su - root
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.  
 In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the Active server.

- 5 Verify the status of the NPM server application by typing
- ```
# servman query -status -group NPM
```
- and pressing the Enter key.

If the NPM server application is	Do
not running	step 6
running	you have completed this procedure

- 6 Start the NPM server application by typing
- ```
servstart NPM
```
- and pressing the Enter key.
- 7 Verify the NPM server application is running by typing
- ```
# servman query -status -group NPM
```
- and pressing the Enter key.
- You have completed this procedure.

—End—

Performing a backup of APS audio files to tape

Application

Use this procedure to back up APS audio files to a 4mm Digital Audio Tape (DAT).



CAUTION

This procedure only applies to a Sun Netra t1400-type server with a DAT drive. If you have a Sun Netra 240-type server, use procedure ["Performing a backup of APS audio files to CD or DVD"](#) (page 547).

Prerequisites

You need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the audio files.

Action

Perform the following steps to complete this procedure.

Step	Action

At the server

- 1 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) digital audio tape (DAT) tape into the DAT drive on the server where the APS resides.

At the server console

- 2 Log in to the server through the console (port A) using the root user ID and password.
- 3 Rewind the tape by typing

```
# mt -f /dev/rmt/0c rewind
```

and pressing the Enter key.
- 4 Change directories to the root filesystem by typing

```
# cd /
```

and pressing the Enter key.
- 5 Back up the APS audio files by typing

```
# /usr/ntdb/uas/scripts/backup_appl_data.sh
```

and pressing the Enter key.

This command backs up file systems /PROV_data, /audio_files, and /user_audio_files.

- 6 Rewind the backup tape by typing

```
# mt -f /dev/rmt/0c rewind
```

and pressing the Enter key.
- 7 To ensure that the backup was successful, list the content of the tape by typing

```
# tar tvf /dev/rmt/0c | more
```

and pressing the Enter key.
- 8 Eject the backup tape, label it, and move the write-enable tab to the "read-only" position (white or grey tab is moved to the left where it cannot be seen) to prevent the data on the tape from being accidentally over-written. Store the tape for later use.

You have completed this procedure.

—End—

Performing a backup of APS audio files to CD or DVD

Application

Use this procedure to back up APS audio files onto a CD or DVD, or move the backup of audio files to another server if the backup is more than 4 GB.

ATTENTION

This procedure only applies to a Sun Netra 240 server with a CD/DVD drive. Use procedure ["Performing a backup of APS audio files to tape" \(page 545\)](#) for a Sun t1400 server with a DAT drive.

Prerequisites

You need one blank CD-R, DVD-R, CD-RW or DVD-RW to store the data if the data is less than 4 GB. Otherwise, you need a server accessible through FTP with adequate space to hold the data.

The backup utility limits the storage to 4 GB on a DVD-R, or DVD-RW.

If you are using a new CD-RW or DVD-RW, or want to use a used CD-RW or DVD-RW and need to erase the contents, refer to procedure "Preparing a CD-RW or DVD-RW for use" in *ATM/IP Security and Administration document* (NN10402-600)

Action

ATTENTION

In a two-server configuration, execute this procedure on the Active server.

Step	Action

At the server

- 1 Insert a blank CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of the Active server.

At your workstation

- 2 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to procedure *Logging in to an SPFS-based server*.

- 3 Change directories to the root file system by typing

```
# cd /
```

 and pressing the Enter key.
- 4 Create a "tar" file of the APS audio files by typing

```
# tar cvf AudioFiles.tar /audio_files /user_audio_files /opt/uas/uas_conf_backup
```

 and pressing the Enter key.
 The above command is entered on one line, and includes a space between each directory.
- 5 Verify the size of the "AudioFiles.tar" file by typing

```
# ls -l AudioFiles.tar
```

 and pressing the Enter key.

If the "AudioFiles.tar" file is	Do
under 4GB	step 6
over 4GB	step 7 only

- 6 Move the "AudioFiles.tar" file onto another server using File Transfer Protocol (FTP).
 Proceed to step 10
- 7 Create a temporary directory by typing

```
# mkdir /tmp/.iso
```

 and pressing the Enter key.
 The directory may already exist.
- 8 Backup the tar file of the APS audio files onto the CD or DVD by typing

```
# /opt/nortel/sspfs/bks/cdwrite AudioFiles.tar
```

 and pressing the Enter key.
- 9 Remove the CD or DVD from the drive, label it, and store it in a safe place.
- 10 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Starting the APS server application

Application

Use this procedure to start the APS server application on the Server Platform Foundation Software (SPFS)-based server where the APS resides.

The APS resides on the same server as the CS 2000 Management Tools software (CS2M).

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the Active server.

Step	Action
At your workstation	
1	Log in to the server by typing <code>> telnet <server></code> and pressing the Enter key. where server is the IP address or host name of the SPFS-based server where the APS resides In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).
2	When prompted, enter your user ID and password.
3	Change to the root user by typing <code>\$ su - root</code> and pressing the Enter key.
4	When prompted, enter the root password.

At your workstation

- 1 Log in to the server by typing
`> telnet <server>`
 and pressing the Enter key.
 where
server is the IP address or host name of the SPFS-based server where the APS resides
 In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing
`$ su - root`
 and pressing the Enter key.
- 4 When prompted, enter the root password.

In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.

- 5 Verify the status of the APS server application by typing

```
# servman query -status -group APS
```

and pressing the Enter key.

If APS server is	Do
not running	Step 6
running	You have completed this procedure.

- 6 Start the APS server application by typing

```
# servstart APS
```

and pressing the Enter key.

- 7 Verify the APS server application started by typing

```
# servman query -status -group APS
```

and pressing the Enter key.

You have completed this procedure.

—End—

Performing a restore of APS audio files from tape

Application

Use this procedure to perform a restore of APS audio files from a backup tape on a Server Platform Foundation Software (SPFS)-based server (Sun t1400) running the SN06.2 or greater release of the SPFS.

ATTENTION

This procedure only applies to a Sun Netra t1400-type server with a DAT drive. If you have a Sun Netra 240-type server, use procedure ["Performing a restore of APS audio files from tape" \(page 552\)](#).

Prerequisites

You need the tape on which you backed up the APS audio files.

Step	Action
At the server	
1	Insert the tape on which you backed up the APS audio files into the DAT drive on the server where the APS resides.
At the server	
2	Log in to the server by typing <pre>> telnet <server></pre> and pressing the Enter key. where server is the IP address or host name of the SPFS-based server on which you are restoring the APS audio files
3	When prompted, enter your user ID and password.
4	Change to the root user by typing <pre>\$ su - root</pre> and pressing the Enter key.
5	When prompted, enter the root password.
6	Change directory to the root file system by typing <pre># cd /</pre> and pressing the Enter key.
7	Restore the audio files to the file system by typing

```
# tar xvf /dev/rmt/0
```

The files are read from tar and placed in the following file systems:
/audio_files and /user_audio_files.

You have completed this procedure.

—End—

Performing a restore of APS audio files from CD

Application

Use this procedure to perform a restore of APS audio files from a backup CD or DVD on a Server Platform Foundation Software (SPFS)-based server (Sun Netra 240) running the SN06.2 or greater release of the SPFS.

ATTENTION

This procedure only applies to a Sun Netra 240-type server with a CD/DVD drive. If you have a Sun Netra t1400-type server, use procedure ["Performing a restore of APS audio files from tape" \(page 552\)](#).

Prerequisites

You need the CD or DVD on which you backed up the APS audio files.

Step	Action
At the server	
1	Insert the CD or DVD on which you backed up the APS audio files into the drive on the server where the APS resides.
At the server	
2	Log in to the server by typing <code>> telnet <server></code> and pressing the Enter key. where <code>server</code> is the IP address or host name of the SPFS-based server on which you are restoring the APS audio files
3	When prompted, enter your user ID and password.
4	Change to the root user by typing <code>\$ su - root</code> and pressing the Enter key.
5	When prompted, enter the root password.
6	Change directory to the root file system by typing <code># cd /</code> and pressing the Enter key.
7	Restore the audio files to the file system by typing

```
# cp /cdrom/cdrom0/* /
```

and pressing the Enter key.

The files are read from cd and placed in the following file systems:
/audio_files and /user_audio_files.

You have completed this procedure.

—End—

Launching CS 2000 Management Tools and NPM Client Applications

Application

Use this procedure to launch any one of the following client applications:

- Trunk Maintenance Manager (TMM)
- CS2000 Management Tools (CMT)
- Line Maintenance Manager (LMM)
- SAM21 Element Manager (SAM21 EM)
- Batch Configuration Monitor (BCM)
- Network Patch Manager (NPM)

ATTENTION

This only applies when the NPM is installed and enabled on the same SPFS-based server as CS 2000 Management Tools.

The NPM also has its own command line user interface (CLUI). Refer to procedure "[Accessing the network patch manager CLUI](#)" (page 567).

This procedure provides the following four methods to launch a CS 2000 Management Tools client application:

1. "[Launch applications from a web browser](#)" (page 558).

ATTENTION

You must use method one to launch an application for the first time.

You cannot use launch methods two through four to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

2. "[Launch applications from the JWS Application Manager](#)" (page 560).
3. "[Launch applications from a desktop icon or Start menu \(Windows only\)](#)" (page 562)
4. "[Launch specific applications using a URL](#)" (page 564).

You can also launch applications from the Integrated Element Management System (IEMS) when the IEMS is present in the office. Refer to document *IEMS Basics* (NN10329-111).

Prerequisites

- Ensure the client workstation meets the minimum requirements. Refer to section "Client workstation requirements" under "CS 2000 Management Tools" in the Basics document for your solution.
-
- Make sure the client workstation meets the minimum requirements.



CAUTION

If you have an ATI Radeon 7000 series graphics card installed on your desktop computer, or an ATI Mobility graphics chip installed in your laptop computer, you can experience the "blue screen of death" in your Windows environment. You can obtain information on this issue at the following website:

<http://developer.java.sun.com/developer/bugPatches/bugs/4713003.html>

A workaround for this issue is to download the latest ATI graphics driver from the following web site:

<http://mirror.ati.com/support/driver.html>

Contact your IT support team if you need assistance.

You need the IP address or host name of the SPFS-based server where the CS 2000 Management Tools are installed, and a valid user name and password to launch an application.

ATTENTION

Users of the CS 2000 Management Tools client applications must belong to the primary user group "succssn" for login access, and to one or more secondary user groups, which specify the operations a user is authorized to perform. If required, refer to procedure "Setting up local user accounts on an SPFS-based server" in *ATM/IP Security and Administration* (NN10402-600)

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2_08 and Java™ Web Start (JWS) version 1.4.2_08 installed to launch the following applications:

- CS 2000 Management Tools
- Line Maintenance Manager
- CS 2000 SAM21 Manager
- Network Patch Manager

Action

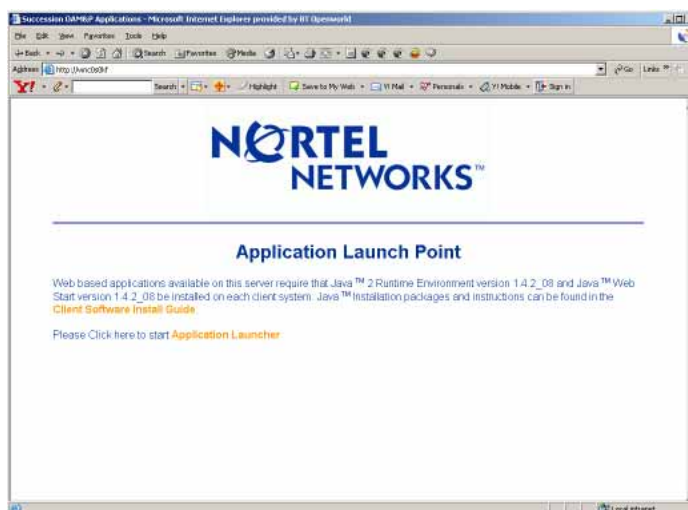
Launch applications from a web browser

Step	Action

At your workstation

- 1 Launch your web browser.
- 2 In the Address field, enter the name or IP address of the SPFS-based server where the CS 2000 Management Tools are installed.

The Application Launch Point page appears.



- 3 Use the following table to determine your next step.

If	Do
you have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 9
you do not have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 4
you do not know which version of JRE and JWS you have	step 4

- 4 Click **Client Software Install Guide** and follow the instructions under How to check version to verify your client setup.

If	Do
you have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 8
you do not have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 5

- 5 Click **Java 2 Runtime Environment Install Guide** under Microsoft Windows or Sun Solaris for system requirements and installation instructions.
- 6 Once you have read through the Java 2 Runtime Environment Install Guide, click **Back** to return to the Client Software Installation page.
- 7 Click **Java 2 Runtime Environment Software Download** under Microsoft Windows or Sun Solaris to download and install the software.

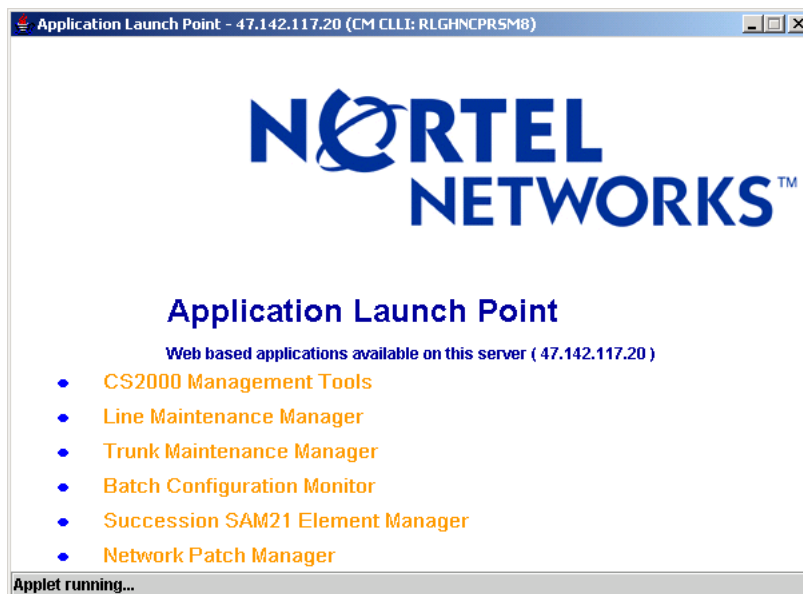
ATTENTION

You must have administrative privileges to install the software on the workstation.

- 8 Click **Back** to return to the Application Launch Point.
- 9 Click **Application Launcher**.
The Login window appears.



- 10 Enter your user name and password, then click **Log In**.
The Application Launch Point, similar to following, appears.



- 11 Click the link for the application you want to launch.
If you delay clicking an application link by 5 minutes or more after you log in, the login window will appear requiring you to log in again.
The interface for the application you launched, is displayed.
- 12 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Launch applications from the JWS Application Manager

Step	Action

At your workstation

1	Launch the Java Web Start Application Manager.

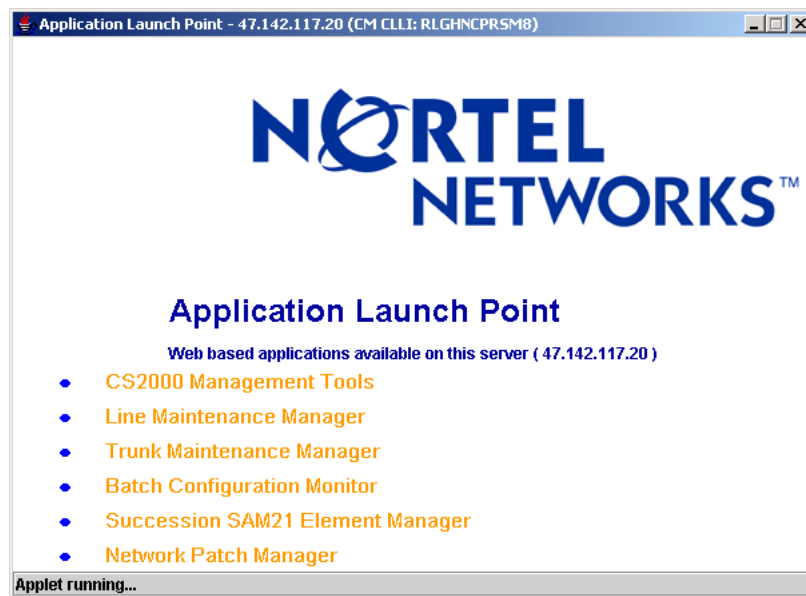


- 2 If you do not see the downloaded applications as shown in the previous figure, then on the View menu click **Downloaded Applications**. Otherwise, skip to the next step.
- 3 Double-click the Application Launch Point you want to access, or select the Application Launch Point and click Start.

The Login window appears.



- 4 Enter your user name and password, then click Log In. The Application Launch Point, similar to following, appears.



- 5 Click the link for the application you want to launch.
The interface for the application you launched, is displayed.
- 6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

ATTENTION

You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

—End—

Launch applications from a desktop icon or Start menu (Windows only)

Step Action

At your workstation

- 1 Use the following table to determine your next step.

If you want to launch an application from ...	Do
... a desktop icon	step 2
... the Start menu	step 4

- 2 To launch a CS 2000 Management Tools client application from a desktop icon, locate the short-cut icon on your desktop, and double-click it to start the application.

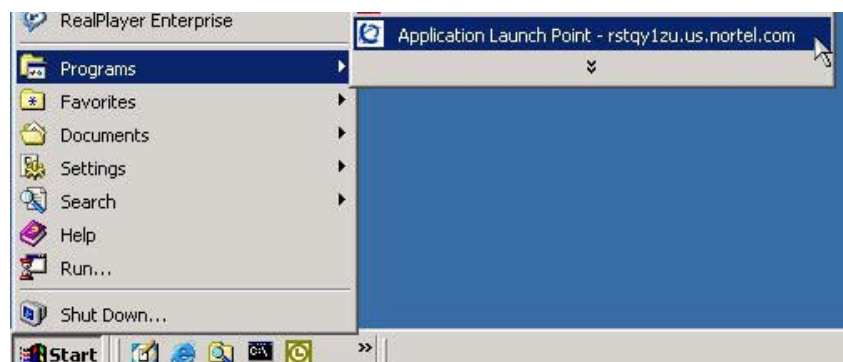
ATTENTION

For short-cut icons to be present on your desktop, you must have the correct settings under the Shortcut Options tab. Access the Shortcut Options tab through File->Preferences in the JWS Application Manager.



The Login window appears.

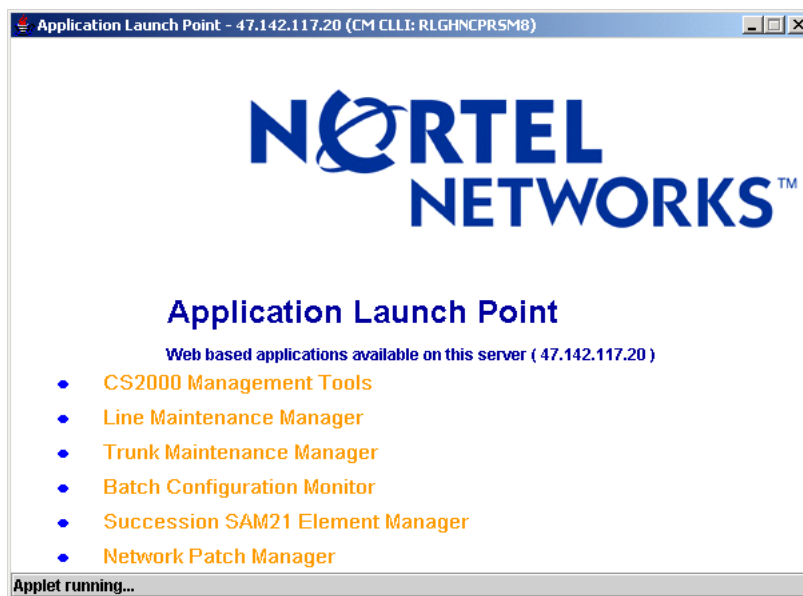
- 3 Proceed to step 5.
- 4 To launch a CS 2000 Management Tools client application from the Start menu, click Start->Programs, then click the CS 2000 Management Tools client application you want to launch.



The Login window appears.

- 5 Enter your user name and password, then click **Log In**.

The Application Launch Point, similar to following, appears.



- 6 Click the link for the application you want to launch.
The interface for the application you launched, is displayed.
- 7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

ATTENTION

You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2_08 and Java™ Web Start (JWS) version 1.4.2_08 installed to launch the applications. If this is the first time you are launching an application, use the first method provided in the "[Launch applications from a web browser](#)" (page 558) procedure.

—End—

Launch specific applications using a URL

Step Action

At your workstation

- 1 Launch your web browser.
- 2 In the Address field, enter one of the following URLs for the application you want to launch:

Application	URL
CS2000 Management Tools	http://<host>:8080/launch/servlet/Launch?app=sesm
Line Maintenance Manager	http://<host>:8080/launch/servlet/Launch?app=Imm
CS2000 SAM21 Manager	http://<host>:8080/launch/servlet/Launch?app=sam21em
Network Patch Manager	http://<host>:8080/launch/servlet/Launch?app=npm

where

host is the host name or IP address of the SPFS-based server where the application resides

The Login window appears.



- 3 Enter your user name and password, then click **Log In**.
The interface for the application you launched, is displayed.
- 4 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Additional information

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and SAM21 Manager) connect to their corresponding server-side application through a Socks proxy.

The Trunk Maintenance Manager (TMM) and Batch Configuration Monitor do not use a Socks proxy.

When you launch a client application that connects through a Socks proxy, you can receive an error message indicating that the Socks connection to the server has failed, the server is down and needs to be rebooted. Once the server has rebooted, you can relaunch the client application.

Accessing the network patch manager CLUI

Application

Use this procedure to access the Network Patch Manager (NPM) command line user interface (CLUI).

You can also access the NPM CLUI from the Integrated Element Management System (IEMS) when the IEMS is present in the office. Refer to *IEMS Basics*, NN10329-111.

The Network Patch Manager also has a graphical user interface (GUI). Refer to procedure "[Launching CS 2000 Management Tools and NPM Client Applications](#)" (page 556) .

Prerequisites

You must have a valid user ID and password to access the NPM interface. In addition, you must be assigned to user group emsadm to perform patching activities using the NPM. If required, refer to procedure "Setting up local user accounts on an SPFS-based server" in *ATM/IP Security and Administration*, NN10402-600.

Action

Perform the following steps to complete this procedure.

Step	Action						
At your workstation							
1	Establish a login session to the server, using one of the following methods:						
<table border="1"> <thead> <tr> <th>If using</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>telnet (unsecure)</td> <td>step 2</td> </tr> <tr> <td>ssh (secure)</td> <td>step 3</td> </tr> </tbody> </table>		If using	Do	telnet (unsecure)	step 2	ssh (secure)	step 3
If using	Do						
telnet (unsecure)	step 2						
ssh (secure)	step 3						
2	Log in to the server using telnet (unsecure) as follows:						
a. Log in to the server by typing <pre>> telnet <server></pre> and pressing the Enter key. where <pre>server</pre> is the IP address or host name of the SPFS-based server							

At your workstation

- Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- Log in to the server using telnet (unsecure) as follows:

- Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server

b. When prompted, enter your user ID and password.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a. Log in to the server by typing

```
> ssh -l <userID> <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter your password.

4 Start the NPM CLUI by typing

```
$ npm
```

and pressing the Enter key.

5 When prompted, enter your user ID and password.

Example response:

```
Entering shell mode: Enter npm' commands, help or quit  
to exit.
```

```
npm>
```

6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Starting the batch provisioning tool

Application

Use this procedure to start the batch provisioning tool.

Prerequisites

You must have a valid user ID and password.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

 and pressing the Enter key.
 where
server is the IP address or host name of the CS 2000 Management Tools server
- 2 When prompted, enter your user ID and password.
- 3 Start the batch provisioning tool by typing

```
$ bpt
```

 and pressing the Enter key.
- 4 When prompted, enter your username and password.

Example response:

```
Login in progress...
You are currently logged in as :  rtps!
=====
Main Menu:
=====
      (1) Execute Batch File
      (2) Display Output
      (3) Display Logs
      (4) Delete Output or Log Files
      (5) Configuration
      (h) Help
      (1) Exit
Selection:  [1/2/3/4/5/h/x:1]
```

You have completed this procedure.

—End—

Connecting to OSSGate

Application

Use this procedure to connect to OSSGate. You can connect to OSSGate with password control turned on or off. When OSSGate password control is turned on, the password will not be echoed on the screen when logging in. To verify or change the status of password control, refer to procedure "Connecting to OSSGate" (page 571).

Prerequisites

You must have a telnet client that supports line mode and can implicitly add a Carriage Return (CR) to any data coming from the OSSGate server.

Action

Perform the following steps to complete this procedure.

Step	Action

From a telnet client

- 1 Connect to the OSSGate by typing

```
> telnet <server> <port_number>
```

where

server is the IP address or host name of the CS 2000 Management Tools server

port_number is the port number (default 10023)

The login prompt will be slightly different depending on whether OSSGate password control is turned on.

- 2 Use the following table to determine your next step:

If the login prompt is	Do
Enter User Name	step 3
Enter username and password	step 5

- 3 When prompted, enter your user name.

Example

```
Enter User Name
```

```
> ossuser
```

- 4 When prompted, enter your password.

Example

```
Enter Password  
> osspassword
```

You have completed this procedure.

- 5** When prompted, enter your username and password separated by a space, and press the Enter key.

Example

```
Enter username and password  
> ossuser osspassword
```

You have completed this procedure.

—End—

Changing modes within OSSGate

Application

Use this procedure to change between the two modes that OSSGate supports: Command Interface (CI) and XML. The default mode is CI for Lines.

Prerequisites

You must be logged in to OSSGate.

Action

Perform the following steps to complete this procedure.

Step	Action

From the OSSGate user interface

- 1 Change to Control mode by pressing the Control key and the B key at the same time (Ctrl+B).

> ^B

and pressing the Enter key.

For some terminal settings, the Ctrl+B character is not displayed on the screen.

- 2 At the prompt, enter the mode to change to by typing

? mode <new_mode>

and pressing the Enter key.

where

new_mode is the mode (ci or xml) to change to

Example

> mode xml

The system responds with a confirmation of the mode change. The following example is for a mode change to XML.

Mode is XML.

You have completed this procedure.

—End—

Stopping the SESM server application

Application

Use this procedure to stop the Succession Element and Subelement Manager (SESM) server application on the CS 2000 Management Tools server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

- 1 Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the `ubmstat` command.

For detailed steps, refer to procedure "Logging in to an SPFS-based server".

- 2 Verify the status of the SESM server application by typing

`# servman query -status -group SESMSservice`

and pressing the Enter key.

If the response indicates	Do
running	step 3
not running	step 6

- 3 Stop the SESM server application by typing

`# servstop SESMSservice`

and pressing the Enter key.
- 4 Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to stop.
- 5 Verify the SESM server application stopped as follows:

- a. Verify the SESM services stopped by typing

```
# servman query -status -group SESMService
```

and pressing the Enter key.

Example response:

```
CS2K Management Tools are not running
```

- b. Verify the SESM applications stopped by typing

```
# ptmctl status
```

and pressing the Enter key.

Example response:

```
SESM STATUS -----
COMPONENT                STATUS
-----
Proxy Agent              NOT RUNNING
RMI Regisry              NOT RUNNING
Snmpfactory              NOT RUNNING
MI2 Server               NOT RUNNING
Current number of SESM processes running:  0 (of 4)
SESM APPLICATION STATUS: No Applications are ready
```

- 6** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Stopping the SAM21 Manager server application

Application

Use this procedure to stop the SAM21 Manager server application on the SPFS-based server that is hosting the CS 2000 Management Tools.

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

Step	Action

At your workstation

- Establish a login session to the server, using one of the following methods

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the `ubmstat` command.

For detailed steps, refer to procedure "Logging in to an SPFS-based server".
- Verify the status of the SAM21 Manager server application by typing
`# servman query -status -group SAM21EM`
and pressing the Enter key.

If SAM21EM is	Do
running	step 3
not running	step 5

- Stop the SAM21EM server application by typing
`# servstop SAM21EM`
and pressing the Enter key.
- Verify the SAM21EM server application stopped by typing
`# servman query -status -group SAM21EM`
and pressing the Enter key.

Example response:

```
Executing: /opt/servman/bin/servquery -status - group
SAM21EM
Succession SAM21 Element Manager version: SAM21EM_9
_020_0
Current status of the Succession SAM21 Element Manager:
    SNMP Access Gateway is not running.
    SAM21 Element Manager Server is not running.
```

- 5 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Stopping the NPM server application

Application

Use this procedure to stop the Network Patch Manager (NPM) server application on a Server Platform Foundation Software (SPFS)-based server.

Prerequisites

You need root user privileges to perform this procedure.

It is recommended that all users exit the NPM CLUI and GUI before stopping the NPM server application.

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the Active server.

Step	Action

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

 and pressing the Enter key.
 where
server is the IP address or host name of the SPFS-based server where the NPM server application resides
 In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.
 In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of

that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.

- 5 Verify the status of the NPM server application by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

If the NPM server application is	Do
running	step 6
not running	you have completed this procedure

- 6 Stop the NPM server application by typing

```
# servstop NPM
```

and pressing the Enter key.

- 7 Verify the NPM server application is no longer running by typing

```
# servman query -status -group NPM
```

and pressing the Enter key.

You have completed this procedure.

—End—

Stopping the APS server application

Application

Use this procedure to stop the APS server application on the Server Platform Foundation Software (SPFS)-based server.

The APS resides on the same server as the CS 2000 Management Tools software (CS2M).

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the Active server.

Step	Action

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

 and pressing the Enter key.
 where
server is the IP address or host name of the SPFS-based server where the APS resides
 In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su - root
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.
 In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of

that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.

- 5 Stop the APS server application by typing

```
# servstop APS
```

and pressing the Enter key.
- 6 Verify the APS server application stopped by typing

```
# servman query -status -group APS
```

and pressing the Enter key.
You have completed this procedure.

—End—

Disconnecting from OSSGate

Application

Use this procedure to disconnect from OSSGate.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
<i>From the OSSGate user interface</i>	
1	Change to Control mode by pressing the Control key and the B key at the same time (Ctrl+B). > ^B and pressing the Enter key. For some terminal settings, the Ctrl+B character is not displayed on the screen.
2	Log out by typing ? logout and pressing the Enter key. You are returned to the input ('>') prompt.
3	Change to Control mode by pressing the Control key and the B key (Ctrl+B) at the same time. > ^B and pressing the Enter key. For some terminal settings, the Ctrl+B character is not displayed on the screen.
4	End the session by typing ? clearconv and pressing the Enter key. You have completed this procedure.
—End—	

Starting and stopping the PM Poller

Application

Use this procedure to start the PM poller on a network element or, stop the PM poller after you have collected the required data on the network element.

Prerequisites

None.

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the Active server.

Step	Action

At your workstation

- 1 Log in to the SPFS-based server by typing

```
> telnet <server>
```

 and pressing the Enter key.
 where
 server is the IP address or host name of the SPFS-based server
 In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su -
```

 and pressing the Enter key.
- 4 When prompted, enter the root password.
 In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the Active server.

- 5 Change to the PM poller directory by typing

```
# cd /opt/nortel/snmp-poller/bin
```

and pressing the Enter key.

- 6 Use the following table to determine your next step.

If you want to	Do
start the PM poller	step 7
stop the PM poller	step 9

- 7 Start the PM poller as follows:

- a. Start the PM poller by typing

```
# servstart SNMP_POLLER
```

and pressing the Enter key.

- b. Verify the PM poller started by typing

```
# servman query -status -group SNMP_POLLER
```

and pressing the Enter key.

Example response:

```
owner:    root
pids:    23853
```

- 8 Use the following table to determine your next step.

If you want to	Do
leave the PM poller running	you have completed this procedure
stop the PM poller	step 9

- 9 Stop the PM poller as follows:

- a. Stop the PM poller by typing

```
# servstop SNMP_POLLER
```

and pressing the Enter key.

Example response

```
SNMP_POLLER stopped
```

- b. Verify the PM poller stopped by typing

```
# servman query -status -group SNMP_POLLER
```

and pressing the Enter key.

Example response

```
pmfadm: "snmpp" No such <nametag> registered  
The poller process is not running.
```

You have completed this procedure.

—End—

View and Modify the QoS Collection Application properties

Application

Use this procedure to view and modify the configuration details for the QoS Collector Application (QCA) on the SPFS-based server. For modification of QoS Collector Application configuration use the procedures [step 7](#) and [step 8](#) under, “Modifying QoS Collector Application properties” to reflect the changes on both the units of the HA server.

QCA is applicable to AAL2 solutions starting with SN09U.

In a two-server configuration, you must perform this procedure on both the active and inactive servers.

Prerequisites

You need the root user ID and password to log in to the server where the QCA software resides.

For the Modify procedure, the `qca.properties` must be modified on an inactive unit and a `swact` needs to be done to reflect the modifications.

Action

Step	Action

At your workstation

- 1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- 2 Log in to the server using telnet (unsecure) as follows:
 - a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where

server is the hostname or IP address of the server

- b. When prompted, enter your user ID and password.
- c. Change to the root user by typing

```
$ su -
```

and pressing the Enter key.
- d. When prompted, enter the root password.

Proceed to [step 4](#).

3 Log in using ssh (secure) as follows:

- a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the hostname or IP address of the server

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

- b. When prompted, enter the root password.

For the modify procedure, verify that you have logged into the inactive cluster.

4 Edit the QCA properties file by typing

```
# vi /opt/nortel/qca/properties/qca.properties
```

and pressing the Enter key.

Example response

```

# QCA Properties file
# The QCA will have to be restarted for changes in the properties
# file to be reflected in the application's operation.

# port name to start application on.
# Default is 20000
portNumber=20001

# The maximum size of a file, in MBytes, before it is closed
# Range is 1 to 100
# Default is 1
MaxFileSize=10

# The maximum time, in minutes, a file can be open before it is
# closed
# Range is 1 to 240
# Default is 15
MaxFileTime=10

# How long, in days, the files are kept before deleting
# Range 1 to 30.
# Default is 5
RetainFileTime=3

# Hour of the day that the directory structure is recycled
# Range 0 (12:00 AM) to 23 (11:00 PM) Do NOT specify minutes.
# Default is 0
recycleToD=14

# File Extension used in the QCA output file name.
# Default is xml
fileExt=xml

# Node name to be used in the QCA output file name.
# Default in QCA.
nodeName=CS2K1

# 'true' or 'false' value indicating whether the output file
# should be compressed when closed. Default is true.
closedFileCompression=true

# 'true' or 'false' value indicating whether the file should be
# compressed at the first directory recycle
# Note: If closedFileCompression is true the value of the
# oldFileCompression property is negated as the files will have
# already been compressed. Default is true.
oldFileCompression=true

```

- 5 Save and exit the session by typing

:wq

and pressing the Enter key.

- 6 The view procedure is complete. .
To modify go to [step 7](#).

Modify QoS Collector Application properties

- 7** Perform a swact on the active cluster unit such that modified qca.properties is picked up in the inactive unit:

- a. Change to the root user on active unit by typing

```
$ su -
```

and pressing the Enter key.

- b. When prompted, enter the root password.

- c. Execute the following command

```
# init 6
```

and pressing the Enter key.

and pressing the Enter key.

- 8** On newly active unit

- a. change to the root user by typing

```
$ su -
```

and pressing the Enter key.

- b. When prompted, enter the root password.

- c. Type the following command to synchronize the qca.properties file from newly active unit to inactive unit.

```
/opt/nortel/sspfs/Scripts/syncfiles /opt/nortel/qca/  
properties/qca.properties
```

- 9** You have completed this procedure.

—End—

Starting and stopping the QoS Collector Application

Application

Use this procedure to start or stop the QoS Collector Application (QCA) on the Server Platform Foundation Software (SPFS)-based server.

The QCA is installed on the same SPFS-based server as the CS 2000 Management Tools software (CS2M), but a second instance of QCA may also be installed on a separate SPFS-based server.

You need to stop and restart the QCA after you performed procedure "Configuring the QoS Collector Application" in the Configuration Management document.

QCA is not applicable to AAL2 solutions.

If QCA functionality is not desired at the site, then the QCA application need not be installed during the CS2M installation/upgrade. Starting in SN09U, CS2M installation/upgrade prompts users as to whether or not the QCA package is to be installed. For older releases, QCA has to be uninstalled manually at the sites where QCA is not desired. Refer to the procedure Installing and Uninstalling the QoS Collector Application.

Prerequisites

None

Action

Step	Action

At your workstation

- 1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	Step 2
ssh (secure)	Step 3

- 2 Log in to the server using telnet (unsecure) as follows:
 - a. Log into the server by typing


```
> telnet <server>
```

 and pressing the Enter key.

where

server is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration, where the QCA you want to start or stop resides

- b. When prompted, enter your user ID and password.
- c. Change to the root user by typing

```
$ su -root
```

and pressing the Enter key.

- d. When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing **ubmstat**. If **ClusterIndicatorSTBY** is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display **ClusterIndicatorAct**, which indicates you are on the active server.

Proceed to step 4

3 Log in using ssh (secure) as follows:

- a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration.

If this is the first time you are logging in using ssh, the system will request you confirm to continue connecting. Enter **yes** at the prompt.

- b. When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing **ubmstat**. If **ClusterIndicatorSTBY** is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through ssh using the physical IP address of the other unit. The response must display **ClusterIndicatorAct**, which indicates you are on the active server.

4 Verify the status of QCA by typing

```
# servman query -status -group QCA
```

and pressing the Enter key.

Example response when QCA is running:

A QCA instance is registered with PMFADN as QCA and running on the portNumber=20000

Example response when QCA is not running:

A QCA instance is not registered with PMFADN as QCA

- 5 Use the following table to determine your next step.

If you want to	Do
start QCA	step 6
stop QCA	step 7

- 6 Start QCA by typing

```
# /opt/nortel/qca/qca_server
```

and pressing the Enter key.

Example response

Registering QCA with servman.

Attempting to register QCA as Qca with PMFADM. Have you checked the qca.properties file? Are you sure you want to continue [no or yes]

At the prompt, enter yes to confirm you wish to continue.

Example response

Registration as Qca was ok. QCA started.

QCA has been started with the following properties...

MaxFileSize=5

(Supported values are 1 to 100)

MaxFileTime=15

(Supported values are 1 to 240)

recycleToD=0

(Supported values are 0 to 23)

portNumber=20000

(Supported values are 20000 to 20004)

RetainFileTime=5

(Supported values are 1 to 30)

fileExt=xml

(Supported value is an alphanumeric character string)

nodeName=QCA

(Supported value is an alphanumeric character string)

closedFileCompression=true

```
(Supported values are 'true' and 'false')
oldFileCompression=true
(Supported values are 'true' and 'false')
Please check /var/log/customerlog if any of the above
properties does not fall within the range of supported
values.
```

Proceed to step 8

7 Stop QCA by typing

```
# /opt/nortel/qca/stop_qca
```

and pressing the Enter key.

Example response

```
Are you sure you want to stop the QCA? Have you checked
the port number in qca.properties? [no or yes]
```

At the prompt, enter **yes** to confirm you wish to continue.

Example response

```
De-registering QCA from servman
Attempting to unregister QCA as Qca from FMFADM.
Attempting to stop local QCA on port : 20000
```

QCA stopped successfully.

8 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Installing and Uninstalling the QoS Collector Application

Application

The QCA application package is bundled in the CS2M package along with SAM21EM and SESM packages. QCA installation comes as a part of the CS2M install procedure. However, in cases where QCA packages need to be installed or uninstalled separately, use the following manual procedure to install or uninstall the QoS Collector Application.

Prerequisites

QoS Collector Application must be stopped before uninstalling the application.

To stop the QoS Collection Application, refer to procedure Starting and stopping the QoS Collector Application.

Action

Perform the following steps to complete this procedure.

Step	Action						
<i>At your workstation</i>							
1	Establish a login session to the server, using one of the following methods:						
<table border="1"> <thead> <tr> <th>If using</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>telnet (unsecure)</td> <td>step 2</td> </tr> <tr> <td>ssh (secure)</td> <td>step 3</td> </tr> </tbody> </table>		If using	Do	telnet (unsecure)	step 2	ssh (secure)	step 3
If using	Do						
telnet (unsecure)	step 2						
ssh (secure)	step 3						
2	Log in to the server using telnet (unsecure) as follows:						
a. Log in to the server by typing: <pre>> telnet <server></pre> and pressing the Enter key where <i>server</i> is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration.							
b. When prompted, enter your user ID and password.							

At your workstation

- Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- Log in to the server using telnet (unsecure) as follows:

- Log in to the server by typing:

```
> telnet <server>
```

and pressing the Enter key

where

server

is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration.

- When prompted, enter your user ID and password.

- c. Change to the root user by typing

```
$ su -root
```

and pressing the Enter key

- d. When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

- e. Proceed to step 4

3 Log into the server using SSH (secure) as follows:

- a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key

where

server

is the IP address or host name of the server, or the physical IP address of the active server in a two-server configuration.

If this is the first time you are logging in using `ssh`, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

- b. When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

4 Verify the status of QCA by typing:

```
# servman query -status -group QCA
```

and pressing the Enter key

Example response when QCA is running

A QCA instance is registered with PMFADN as Qca and running on the portNumber=20000

Example response when QCA is not running

A QCA instance is not registered with PMFADM as Qca

Example response when QCA is not installed

QCA

=====

Group not registered

a. Enter the number next to the “Configuration” option in the menu.

5 Use the following table to determine your next step.

If you want to	Do
Uninstall QCA	step 6
Install QCA	step 7

6 Uninstall QCA by typing:

```
# pkgrm NTQCA
```

and pressing the Enter key

The QoS Collector Application must be stopped before uninstalling the application.

Example response

The following package is currently installed:

```
NTQCA      Succession QoS Collector Application
           (sparc) QCA_9_108_0
```

Do you want to remove this package? [y,n,?,q]

At the prompt, enter **y** to confirm you wish to continue. The QCA package is uninstalled and the progress is displayed. The uninstallation is complete when the following line is displayed:

Removal of <NTQCA> was successful.

Proceed to step 8.

7 Install QCA by typing:

```
# pkgadd -d QCA_9_108_0.pkg
```

and pressing the Enter key.

Confirm that the result of step 4 indicates the QCA application is not installed.

Example response

The following package are available:
 1 NTQCA Succession QoS Collector Application
 (sparc) QCA_9_108_0
 Select package(s) you wish to process (or 'all' to
 process all packages). (default: all) [?,??,q]:

At the prompt, enter **all** to confirm you wish to continue.

Example response

```
Processing package instance <NTQCA> from </QCA_9_108
.0.pkg>
Succession QoS Collector Application (sparc)
QCA_9_108_0
Nortel Networks
## Executing checkinstall script. Using </opt> as the
package base directory.
## Processing package information.
## Processing system information. 1 package pathname
is already properly installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.
This package contains scripts which will be executed
with super-user permission during the process of
installing this package.
Do you want to continue with the installation of
<NTQCA> [y,n,?]
```

At the prompt, enter **y** to confirm you wish to continue. The QCA package is installed and the progress is displayed. The installation is complete when the following line is displayed:

Installation of <NTQCA> was successful.

- 8 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

If the QCA application was installed using this procedure, it must be manually started. Refer to the procedure "Starting and stopping the QoS Collector Application".

—End—

Clearing the JWS Cache on a Client Workstation

Application

Use this procedure to clear the Java™ Web Start (JWS) cache on a client workstation.

The JWS cache on a client workstation needs to be cleared after an HTTPS certificate is installed on an existing Sun server that was not previously using a certificate. Clearing the cache allows you to properly launch the CS 2000 Management Tools client applications from your workstation.

Prerequisites

None

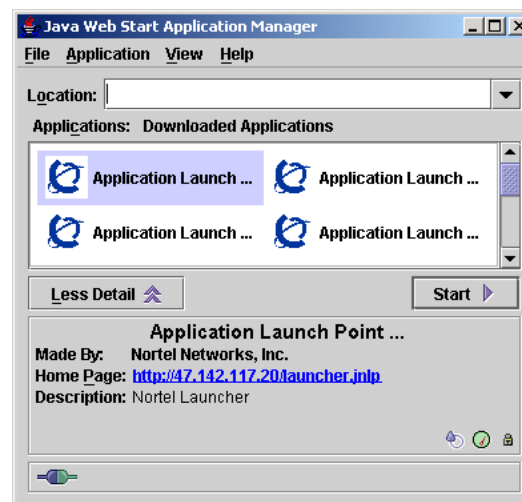
Action

Perform the following steps to complete this procedure.

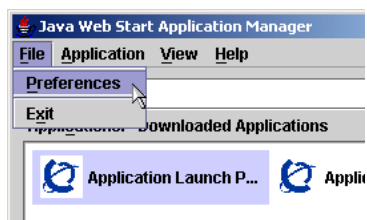
Step	Action

At your workstation

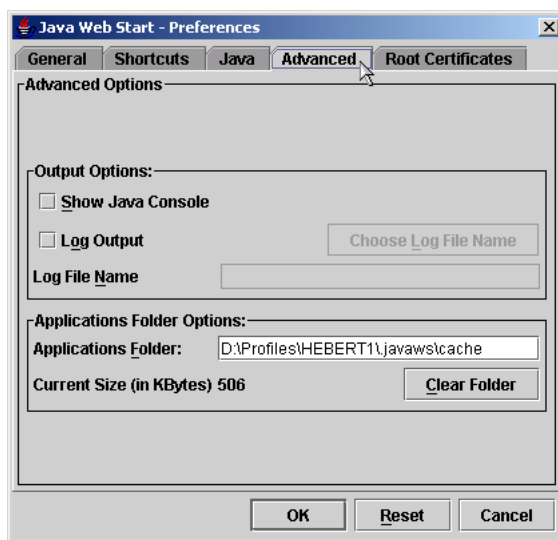
- 1 Access the Java Web Start Application Manager.



- 2 Click **File->Preferences** to access the Preferences window.



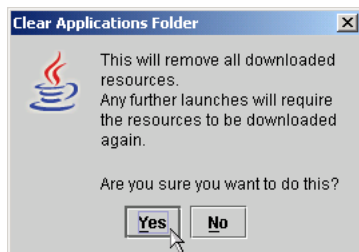
- 3 Click the **Advanced** tab to access the Advanced window.



- 4 Click **Clear Folder** to clear the cache.



- 5 Click **Yes** to confirm you want to clear the cache (remove all downloaded resources).



- 6 Click **OK** to close the Preferences window.
- 7 Exit the Java Web Start Application Manager.

You have completed this procedure.

—End—

Starting the OMPUSH server application

Application

Use this procedure to start the OMPUSH server application.

The OMPUSH server application is automatically started with SPFS.

Prerequisites

The Server Platform Foundation Software (SPFS) must be at release (I)SN06.2 or higher.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server is the IP address or host name of the SPFS-based server
- 2 When prompted, enter your user ID and password.
- 3 Determine the status of the OMPUSH server application by typing

```
$ ompush_ctl -status
```

and pressing the Enter key.

If the OMPUSH server application	Do
is not running	step 4
is running	you have completed this procedure

- 4 Start the OMPUSH server application by typing

```
$ ompush_ctl -start
```

and pressing the Enter key.

Example response:

```
Tue May 22 19:13:38 2003: start ompush command.
```

The OMPUSH start command was sent.

You have completed this procedure.

—End—

Stopping the OMPUSH server application

Application

Use this procedure to stop the OMPUSH server application.

Prerequisites

The Server Platform Foundation Software (SPFS) must be at release (I)SN06.2 or higher.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

- 1 Log in to the server by typing

```
> telnet <server>
```

 and pressing the Enter key.
 where
 server is the IP address or host name of the SPFS-based server
- 2 When prompted, enter your user ID and password.
- 3 Determine the status of the OMPUSH server application by typing

```
$ ompush_ctl -status
```

 and pressing the Enter key.

If the OMPUSH server application	Do
is running	step 4
is not running	you have completed this procedure

- 4 Stop the OMPUSH server application by typing

```
$ ompush_ctl -stop
```

 and pressing the Enter key.

Example response:

```
Tue May 22 19:13:38 2003: start ompush command.
The OMPUSH stop command was sent.
```

You have completed this procedure.

—End—

Cleaning up old data in the NPM database

Application

Use this procedure to clean up the old data in the Network Patch Manager (NPM) database following an upgrade.

ATTENTION

This procedure includes stopping and starting the NPM, which has the NPM re-discover the patches on the system when the NPM is brought back into service. This can take up to one hour depending on office configuration. Therefore, ensure patching tasks are not planned or scheduled in the timeframe you want to perform this procedure.

ATTENTION

This procedure purges any user-defined reports, tasks, sets, plans and alarms, disables any enabled plans such as AUTOAPPLY and AUTORESTART, releases any patches or devices on hold, and unconfigures the Patch File Receipt System (PFRS). Therefore, you will need to re-define any user-defined reports, tasks, sets, plans, and alarms, re-enable any plans such as AUTOAPPLY and AUTORESTART, place any desired patches or devices on hold, and re-configure PFRS following this procedure.

Prerequisites

You must have root user privileges to perform this procedure.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

- 1 Generate and save a patchlist report using the NPM CLUI or GUI.
The patchlist report may be useful in the event the apply time information is required at a later time.

If using the	Do
CLUI	step 2
GUI	step 14

- 2 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server

For detailed steps, refer to "Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM" (page 49)

- 3 Change directory to /data/npm by typing:

```
# cd /data/npm
```

 and pressing the Enter key
- 4 Determine if a tmp directory exists in the npm directory by typing:

```
# ls -l
```

 and pressing the Enter key.
- 5 Use the following table to determine your next step

If	Do
a tmp directory exists	step 7
otherwise	step 6

- 6 Create a tmp directory by typing

```
# mkdir tmp
```

 and pressing the Enter key
- 7 Change directory to the tmp directory by typing:

```
# cd tmp
```

 and pressing the Enter key.
- 8 Generate the patchlist report by typing

```
# npm q patchlist output <filename>.list
```

 and pressing the Enter key.
 where
filename is the name you want to give to the patchlist report

```
npm q patchlist output aug032004.list
```

 Example response
 Enter the NPM Succession user id and password.
 Login
- 9 When prompted, enter the NPM user ID

Example response

```
password
```

- 10** When prompted, enter the NPM user password.

Example response

```
Redirecting output to:  aug032004.list
System retrieved...
patchid, category, hold, spapp, stattime,
status, deviceid
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03
08:21:09.540, VA, NCOS8_1_7_OC3_0_1_10
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02
14:35:34.538, A, NCOS8_1_7_OC3_0_1_11
Redirecting output to standard I/O
```

- 11** Display the file by typing

```
$ ls
```

and pressing the Enter key.

Example response

```
aug032004.list
local.login
local.cshrc
local.profile
```

- 12** If required, display the contents of the file by typing:

```
# cat <filename> |more
```

and pressing the Enter key.

where

filename is the name you gave to the patchlist report file

```
cat aug032004.list
```

Example response

```
System retrieved...
patchid, category, hold, spapp, stattime,
status, deviceid
SCO00UBU, GEN, FALSE, FALSE, 2004-08-03
08:21:09.540, VA, NCOS8_1_7_OC3_0_1_10
SCO00UBU, GEN, FALSE, FALSE, 2004-08-02
14:35:34.538, A, NCOS8_1_7_OC3_0_1_11
```

- 13** Proceed to [step 25](#)

Access the NPM GUI. If required, refer to procedure.

- 14** Access the NPM GUI.

For detailed steps, refer to "[Launching CS 2000 Management Tools and NPM Client Applications](#) " (page 556)

At the NPM GUI

- 15 On the **Tasks** menu, click **Reports...**
- 16 Click the **Report List** tab to display the list of defined reports.
- 17 Click on **PATCHLIST**, and then click **Execute** to generate the PATCHLIST report.
The Reports Results window is displayed.
- 18 Click **Save**, to save the results of the PATCHLIST report and specify the filename and location to save the report.
The Save window is displayed.
- 19 Enter a name for the saved report in the File name field and then click **Save**
- 20 Click **Close** to close the Reports Results window.
- 21 Click **Close** to close the Reports window.
- 22 On the Edit menu, Click **Preferences**.
- 23 Click on the **System Preferences** tab.
Copy and paste the data on display including that in the Delete Patches from the Drop Box after Retrieval checkbox

At your workstation

- 24 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server.

For detailed steps, refer to "[Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM](#) " (page 49)
- 25 Stop the NPM server application by typing:

servstop NPM

and pressing the Enter key.
- 26 Access the command line interface by typing:

cli

and pressing the Enter key.

- 27 Enter the number next to the "Configuration" option in the menu.
- 28 Enter the number next to the "Succession Element Configuration" option in the menu.
- 29 Enter the number next to the "NPM Application Configuration" option in the menu.
- 30 Enter the number next to the "CreateDB" option in the menu.
Allow to complete.
- 31 Exit each menu level of the command line interface to eventually return to the root level by typing:
`select - x`
and pressing the Enter key.
- 32 Start the NPM server application by typing:
and pressing the Enter key.
- 33 If any user-defined reports, tasks, sets, plans, or alarms existed prior to this procedure, redefine them using the corresponding procedure.
 - for reports, use procedure [Defining NPM patching reports](#)
 - for tasks, use procedure [Defining NPM patching tasks](#)
 - for sets, use procedure [Defining NPM patching sets](#)
 - for plans, use procedure [Defining NPM patching plans](#)
 - for alarms, use procedure "Defining alarms using the NPM" in document ATM/IP Fault Management, NN10408-900.
- 34 If any patches or devices were on hold prior to this procedure, place them back on hold using procedure [Setting field values using the NPM](#)
- 35 If any plans such as AUTOAPPLY and AUTORESTART, were enabled prior to this procedure, re-enable them using procedure [Modifying NPM patching plans](#)
- 36 If PFRS was configured prior to this procedure, re-configure it using procedure "Configuring NPM for Automatic Patch File Delivery" in *Nortel Carrier Voice over IP Upgrade and Patches* (NN10440-450).

If any users were logged in to the NPM GUI prior to this procedure, they must exit and launch the GUI again. A reconnect to the NPM server from the GUI is not sufficient to clean up old data showing up in the GUI.

- 37** You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Initializing the NPM database

Application

Use this procedure to initialize the Network Patching Manager (NPM) database.

ATTENTION

This procedure purges any user-defined reports, tasks, sets, plans and alarms, disables any enabled plans such as AUTOAPPLY and AUTORESTART, releases any patches or devices on hold, and unconfigures the Patch File Receipt System (PFRS). Therefore, you will need to re-define any user-defined reports, tasks, sets, plans, and alarms, re-enable any plans such as AUTOAPPLY and AUTORESTART, place any desired patches or devices on hold, and re-configure PFRS following this procedure.

Prerequisites

Only the root user can perform this procedure.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

- Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.
where
server is the IP address or host name of the SPFS-based server where NPM resides
- When prompted, enter your user ID and password.
- Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.
- When prompted, enter the root password.
- Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
```

```
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

- 6** Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
```

```
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Application Configuration
5 - CORBA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Disk Drive Upgrade
16 - Login Session
17 - Location Configuration
18 - Cluster Configuration
19 - Succession Element Configuration
20 - snmp_poller (SNMP Poller Configuration)
21 - backup_config (Backup Configuration)
X - exit
Select -
```

- 7** Enter the number next to the "Succession Element Configuration" option in the menu.

Example response:

```
Succession Element Configuration
```

```
1 - SESM Application Configuration
2 - SAM21EM Application Configuration
3 - NPM Application Configuration
4 - PSE Application Configuration
5 - DDMSProxy Application Configuration
6 - OMPUSH Application Configuration
7 - RESMON Application Configuration
```



```
X - exit
select -
```

- 8 Enter the number next to the "NPM Application Configuration" option in the menu.

Example response

```
NPM Application Configuration
1 - CreateDB (Initialize or re-initialize the NPM
database)
X - exit
select -
```

- 9 Enter the number next to the "CreateDB" option in the menu.

- 10 Exit each menu level of the command line interface to eventually return to the root level, by typing

```
select - x
```

and pressing the Enter key.

- 11 If any user-defined reports, tasks, sets, plans, or alarms existed prior to this procedure, re-define them using the corresponding procedure:

- for reports, refer to procedure "Defining reports using the NPM" in the Carrier Voice Over IP Network Upgrade document, NN10440-450
- for tasks, refer to procedure "Defining a task using the NPM" in the Carrier Voice Over IP Network Upgrade document, NN10440-450
- for sets, refer to procedure "Defining sets using the NPM" in the Carrier Voice Over IP Network Upgrade document, NN10440-450
- for plans, refer to procedure "Defining a plan using the NPM" in the Carrier Voice Over IP Network Upgrade document, NN10440-450
- for alarms, use procedure "Defining alarms using the NPM" in the ATM/IP solution-level Fault Management document, NN10408-900.

- 12 If any patches or devices were on hold prior to this procedure, place them back on hold using procedure "Setting field values using the NPM" in the Carrier Voice Over IP Network Upgrade document, NN10440-450.

- 13 If any plans such as AUTOAPPLY and AUTORESTART, were enabled prior to this procedure, re-enable them using procedure

"Modifying a plan using the NPM" in the Carrier Voice Over IP Network Upgrade document, NN10440-450.

- 14** If PFRS was configured prior to this procedure, re-configure it using procedure "Configuring the NPM for automatic patch file delivery" in the ATM/IP solution-level Configuration document, NN10409-500.

If any users were logged in to the NPM GUI prior to this procedure, they must exit and re-launch the GUI. A re-connect to the NPM server from the GUI is not sufficient to clean up old data showing up in the GUI.

You have completed this procedure.

—End—

Starting the PSE server application on an SPFS-based server

Application

Use this procedure to start the Patching Server Element (PSE) server application on a Server Platform Foundation Software (SPFS)-based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

Step	Action

At your workstation

- 1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- 2 Log in to the server using telnet (unsecure) as follows:
 - a. Log in to the server by typing


```
> telnet <server>
```

 and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server, or the physical IP address of the active server in a two-server configuration
 - b. When prompted, enter your user ID and password.
 - c. Change to the root user by typing


```
$ su -
```

 and pressing the Enter key.

- d. When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step 4.

- 3 Log in using ssh (secure) as follows:

- a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server, or the physical IP address of the active server

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.

- b. When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

- 4 Start the PSE server application by typing

```
# pse start
```

and pressing the Enter key.

- 5 Verify the PSE server application started by typing

```
# pse status
```

and pressing the Enter key.

- 6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Stopping the PSE server application on an SPFS-based server

Application

Use this procedure to stop the Patching Server Element (PSE) server application on a Server Platform Foundation Software (SPFS)-based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

Step	Action						
At your workstation							
1	Establish a login session to the server, using one of the following methods:						
	<table border="1"> <thead> <tr> <th>If using</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>telnet (unsecure)</td> <td>step 2</td> </tr> <tr> <td>ssh (secure)</td> <td>step 3</td> </tr> </tbody> </table>	If using	Do	telnet (unsecure)	step 2	ssh (secure)	step 3
If using	Do						
telnet (unsecure)	step 2						
ssh (secure)	step 3						
2	Log in to the server using telnet (unsecure) as follows: - Log in to the server by typing <code>> telnet <server></code> and pressing the Enter key. where server is the IP address or host name of the SPFS-based server, or the physical IP address of the active server in a two-server configuration - When prompted, enter your user ID and password. - Change to the root user by typing <code>\$ su -</code> and pressing the Enter key.						

At your workstation

- Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

- Log in to the server using telnet (unsecure) as follows:

- Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server, or the physical IP address of the active server in a two-server configuration

- When prompted, enter your user ID and password.
- Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

- d. When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

Proceed to step 4.

- 3 Log in using ssh (secure) as follows:

- a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server, or the physical IP address of the active server

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

- b. When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the active server.

- 4 Stop the PSE server application by typing

```
# pse stop
```

and pressing the Enter key.

- 5 Verify the PSE server application stopped by typing

```
# pse status
```

and pressing the Enter key.

- 6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Viewing patching information for the SPFS

Application

Use this procedure to display the patching status for the Server Platform Foundation Software (SPFS) on the server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

- 1 Log in to the server by typing
`> telnet <server>`
 and pressing the Enter key.
 where
`server` is the IP address or host name of the SPFS-based server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing
`$ su - root`
 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Access the command line interface by typing
`# cli`
 and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

- 6 Enter the number next to the "Other" option in the menu.

Example response

Other

1 - Log Rotation

2 - capt_files (Capture Various SPFS Files/Logs For Debugging Purposes)

3 - sun_explorer (Execute the Sun Explorer Data Gathering Tool)

4 - mount_image (Mount A Generic Iso Image To The SPFS Unit)

5 - umount_image (Un-Mount A Generic Iso Image From the SPFS Unit)

6 - disp_SPFSpatch (Display the patching status of the SPFS unit)

X - exit

select -

- 7 Enter the number next to the 'disp_SPFSpatch' option in the menu.

Example response:

===Executing "disp_SPFSpatch"

SPFS Patch	Installed	Applied

=====

SPFS07MA	Yes	Yes

SPFS07MB	Yes	Yes

=="disp_SPFSpatch" completed successfully

If no SPFS patches are installed, the response will display "No SPFS Patches Installed on This Unit".

- 8 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

select - x

and pressing the Enter key.

You have completed this procedure.

—End—

Performing a SwAct on a SPFS based server

Use this procedure to perform a SwAct (switch of activity) on a SPFS based server.



WARNING

This procedure is service impacting.

Prerequisites

There are no prerequisites.

Procedure steps

Step	Action

At your workstation

- 1 Establish a login session to the server using one of the following methods:

If you are using	Do
telnet	step 2
ssh	step 3

- 2 Log in to the server using telnet as follows:
 - a. Log in to the server by typing:


```
telnet <server>
```

 and pressing the Enter key.

where

server

is a unit IP address.
 - b. When prompted, enter your user ID and password.
 - c. Change to the root user by typing:


```
$ su -
```

 and pressing the Enter key.
 - d. When prompted, enter the root password.

3 Log in using ssh as follows:

a. Log in to the server by typing:

```
> ssh -l root <server>
```

and pressing the Enter key,

where

server

is a unit IP address.

If this is the first time you are logging in using ssh, the system will request that you continue by accepting the SPFS-based server's public key.

Accept the key to continue.

b. When prompted, enter the root password.

4 Ensure you are on the active server by typing

```
# ubmstat
```

and pressing the Enter key.

If the output reads	Go to
ClusterIndicatorACT	step 5
ClusterIndicatorSTBY	step 1, because this is not the active unit and use the IP address of the other unit

5 Initiate the manual failover by typing:

```
# swact
```

and pressing the Enter key.

```
Are you sure you want to initiate a cluster failover?  
[Y/N]
```

6 If it is acceptable to initiate a manual failover, indicate you want the failover to occur by typing:

```
y
```

and pressing the Enter key.

While the SwAct itself only takes a few seconds, it could take several minutes to stop the applications on the other node and then restart them.

If	Then
The cluster failover completed successfully	SwAct has successfully completed and all the applications have been started on the newly active node.
The cluster failover is disabled	Go to step 14

- 7 Verify that the unit is now ClusterIndicatorSTBY by entering the following command:

```
# ubmstat
```

and pressing the Enter key.

If	Then
The unit is now ClusterIndicatorSTBY	Go to step 8
The unit is NOT ClusterIndicatorSTBY	Go to step 14

The following shows an example of the expected response:

```
# ubmstat
Group      State
-----
ClusterIndicatorSTBY
# udstat /audio_files: STANDBY normal UP clean
/data: STANDBY normal UP clean
/data_oradata (/data/oradata): STANDBY normal UP clean
/data_qca (/data/qca): STANDBY normal UP clean
/user_audio_files: STANDBY normal UP clean
#
```

- 8 Verify that all replicated filesystems are now STANDBY and UP by entering the following command:

```
# udstat
```

and pressing the Enter key.

If	Then
All replicated filesystems are now STANDBY	Go to step 9
If replicated filesystems are NOT STANDBY	Go to step 14

The following shows an example of the expected response:

```
# udstat
/data_oradata (/data/oradata): STANDBY repair UP dirty
/data_oradata_arch (/data/oradata/arch): STANDBY
normal UP clean
```

- 9** Use steps 1 to 4 to connect to the other SPFS-based unit which has been made active.

- 10** Verify that this unit is ClusterIndicatorACT by entering the following command:

```
# ubmstat
```

and pressing the Enter key.

If	Then
This unit is ClusterIndicatorACT	Go to step 11
This unit is NOT ClusterIndicatorACT	Go to step 14

- 11** Verify that all replicated filesystems are now ACTIVE and UP by entering the following command:

```
# udstat
```

and pressing the Enter key.

If	Then
all replicated filesystems are now ACTIVE and UP	Go to step 12
all replicated filesystems are NOT ACTIVE and UP	Go to step 14

The following shows an example of the expected response:

```
# udstat
/audio_files: ACTIVE normal UP clean
/data: ACTIVE normal UP clean
/data_oradata (/data/oradata): ACTIVE normal UP clean
/data_qca (/data/qca): ACTIVE normal UP clean
/user_audio_files: ACTIVE normal UP clean
/data_oradata (/data/oradata): ACTIVE normal UP clean
/data_oradata_arch (/data/oradata/arch): ACTIVE normal
UP clean
```

- 12** Check that all applications are RUNNING on the newly active side by entering the following command:

```
# servquery -status all
```

and pressing the Enter key.

All the applications should be **RUNNING**. It may take several minutes for all the applications to come up.

The following shows an example of the expected response:

```
# servquery -status all
APP NAME                STATUS
=====                =====
CINOTIFIER              RUNNING
DATABASE                RUNNING
AUTO_BACKUP_MANAGER     RUNNING
IS                      RUNNING
BACKUP_MANAGER          RUNNING
BOOTP                  RUNNING
WEBSERVER              RUNNING
CORBA                  RUNNING
OMPUSH                 RUNNING
WEBSERVICES            RUNNING
DNSSVR                 RUNNING
DDMSPROXY              RUNNING
ORA_AUTO_BACKUP         RUNNING
DELEGATE               RUNNING
NPM                    RUNNING
ORA_ARCHIVE_ROTATOR     RUNNING
CEM                    RUNNING
PROP_SRV               RUNNING
IEMS                   RUNNING
SNMP_POLLER            RUNNING
RADSVR                 RUNNING
#
```

- 13** Continue executing the **`servquery -status all`** command as needed to check that all applications are **RUNNING** on the newly active side. If the applications come up after a few minutes the procedure is complete. If not, go to [step 14](#).
- 14** The SwAct has failed. Investigate any failures reported and resolve the condition or contact your next level support before re-executing the SwAct procedure.

—End—

Increasing the size of a file system on an SPFS-based server

Application

Use one of the following procedures to increase the size of a file system on a Server Platform Foundation Software (SPFS)-based server:

- "Simplex configuration (one server)" (page 629)
- "High-availability configuration (two servers)" (page 632)

It is recommended you perform this procedure during off-peak hours.

The SPFS creates file systems to best fit the needs of applications. However, it may be necessary to increase the size of a file system.

Not all file systems can be increased. The following table lists the file systems that cannot be increased, and lists examples of those that can be increased.

Not all the file systems that can be increased are listed.

SPFS file systems

Cannot be increased	Can be increased (examples)
/ (root)	/data
/var	/opt/nortel
/opt	/data/oradata
/tmp	/audio_files
	/PROV_data
	/user_audio_files
	/data/qca
	/data/mg9kem/logs

While file systems are being increased, writes to the file system are blocked, and the system activity increases. The greater the size increase of a file system, the greater the impact on performance.

Prerequisites

It is recommended that you back up your file systems and oracle data (if applicable) prior to performing this procedure. Refer to procedures ["Performing a backup of oracle data on an SPFS-based server" \(page 135\)](#) and ["Performing a backup of file systems on an SPFS-based server" \(page 140\)](#) if required.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

Step	Action

At your workstation

- 1 Log in to the server by typing

```
> > telnet < server>
```

 and pressing the Enter key.
 where
server is the IP address or host name of the server
- 2 When prompted, enter your user ID and password. You may log on as root or emsadm.
- 3 Determine the amount of disk utilization by the file systems as follows:

- a. Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
```

```
1 - View
  2 - Configuration
  3 - Other
X - exit
select -
```

- b. Enter the number next to the 'View' option in the menu.

Example response

```
View
```

```
1 - SPFS_soft (Display Software
  Installation Level Of SPFS)
2 - chk_SPFS (Check SPFS Processes)
3 - sw_conf (The software configuration of
```

```

the znc0s0jx)
4 - cpu_util (Overall CPU utilization)
5 - cpu_util_proc (CPU utilization by
process)
6 - port_util (I/O port utilization)
7 - disk_util (Filesystem utilization)
X - exit
select -

```

- c. Enter the number next to the 'disk_util' option in the menu.

Example response

Filesystem	size	used	avail	capacity	Mounted on
/dev/md/dsk/d2	3.9G	1.6G	2.3G	42%	/
/proc	OK	OK	OK	0%	/proc
mnttab	OK	OK	OK	0%	/etc/mnttab
fd	OK	OK	OK	0%	/dev/fd
/dev/md/dsk/d8	2.0G	86M	1.8G	5%	/var
swap	2.5G	160K	2.5G	1%	/var/run
swap	512M	3.8M	508M	1%	/tmp
/dev/md/dsk/d11	4.9G	1.5G	3.4G	32%	/opt
/dev/md/dsk/d21	2.9G	111M	2.8G	4%	/opt/nortel
/dev/md/dsk/d22	5.9G	145M	5.7G	3%	/var/mysql/data
/backup	3.9G	4.0M	3.9G	1%	/backup
/data	2.9G	5.9M	2.9G	1%	/data
/data/oradata	9.8G	2.5G	7.3G	26%	/data/oradata
/data/oradata/arch	968M	12M	956M	2%	/data/oradata/arch
/data/qca	9.8G	10M	9.7G	1%	/data/qca

The 'capacity' column indicates the percentage of disk utilization by the file system, which is specified in the 'Mounted on' column.

- 4 Note the file system you want to increase, as well as its current size (under column 'size').
- 5 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

ATTENTION

Before you proceed with this procedure, ensure the file system you want to increase is full or nearly full and that its content is valid application data. Remove any unneeded files or files generated in error that are taking up disk space.

- 6 Determine the size by which to increase the file system, by subtracting the desired size for the file system based on your specific needs, from its current size (noted in 6).

For example, to determine the size by which to increase the “data/oradata” file system, subtract its current size, 10337 MB from the desired size, for example, 15000 MB. You would increase the size of the “data/oradata” file system by 4662786 KB, or 4663 MB.

- 7 Determine the amount of free disk space that can be allocated to file systems as follows:

- a. Determine the amount of free disk space on your system by typing

```
# /opt/nortel/sspfs/fs/meta.pl free_space
```

and pressing the Enter key.

Divide the resulting number by 2048 to determine the amount of free disk space in megabytes (MB) that can be allocated to existing file systems

If the value is	Do
less than zero (0)	contact Nortel for assistance
more than zero (0)	step b

- b. Use the following table to determine your next step.

If	Do
the value you determined in step 8 (size by which to increase the file system) is greater than the value you obtained in step 9a (amount of free disk space you can allocate to file systems)	contact Nortel for assistance
the value you determined in step 8 (size by which to increase the file system) is less than the value you obtained in step 9 a (amount of free disk space you can allocate to file systems)	step 10

ATTENTION

Once you increase the size of a file system, you cannot decrease it. Therefore, it is strongly recommended that you grow a file system in small increments.

- 8** Increase the size of the file system by typing

```
# fileysys grow -m <mount_point> -s <size>m
```

where

mount_point is the name of the file system you want to increase (noted in step 6)

size is the size in megabytes (m) by which you want to increase the file system (determined in step 8)

Example

```
# fileysys grow -m /data -s 512m
```

The preceding example increases the '/data' file system by 512 megabytes (MB).

You have completed this procedure.

—End—

ATTENTION

During this procedure, the cluster will be running without a standby node. The duration is estimated at approximately one hour.

High-availability configuration (two servers)

Step	Action

At your workstation

- 1** For all users except those using Core and Billing Manager (CBM), start a login session using telnet. For CBM, start a login session connecting to the inactive node using ssh.

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 6

- 2** Log in to the Inactive node by typing
- ```
> telnet <server>
```
- and pressing the Enter key.

where

**server** is the physical IP address of the Inactive node in the cluster

If you use the cluster IP address, you will log in to the Active node. Therefore, ensure you use the physical IP address of the Inactive node to log in.

3 When prompted, enter your user ID and password.

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

Ensure you are on the Inactive server by typing `ubmstat`. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorSTBY*, which indicates you are on the Inactive server.

6 Log in using ssh (secure) as follows:

a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

**server** is the physical IP address of the inactive server

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.

b. When prompted, enter the root password.

#### **At the Inactive node**

7 Verify the cluster indicator to ensure you are logged in to the Inactive node, by typing

```
ubmstat
```

and pressing the Enter key.

| If the system response is | Do     |
|---------------------------|--------|
| ClusterIndicatorSTBY      | step 8 |
| ClusterIndicatorACT       | step 2 |

- 8 Verify the status of file systems on this server by typing

# `udstat`

and pressing the Enter key.

| If the file systems are     | Do                                 |
|-----------------------------|------------------------------------|
| STANDBY normal UP clean     | step 9                             |
| not STANDBY normal UP clean | contact your next level of support |

- 9 Determine the amount of disk utilization by the file systems as follows:

- a. Access the command line interface by typing

# `cli`

and pressing the Enter key.

*Example response*

Command Line Interface

```
1 - View
 2 - Configuration
 3 - Other
X - exit
select -
```

- b. Enter the number next to the 'View' option in the menu.

*Example response*

View

```
1 - SPFS_soft (Display Software
 Installation Level Of SPFS)
2 - chk_SPFS (Check SPFS Processes)
3 - sw_conf (The software configuration of
 the znc0s0jx)
4 - cpu_util (Overall CPU utilization)
5 - cpu_util_proc (CPU utilization by
 process)
6 - port_util (I/O port utilization)
7 - disk_util (Filesystem utilization)
X - exit
select -
```

- c. Enter the number next to the 'disk\_util' option in the menu.

*Example response*

| Filesystem         | size | used | avail | capacity | Mounted on         |
|--------------------|------|------|-------|----------|--------------------|
| /dev/md/dsk/d2     | 3.9G | 1.6G | 2.3G  | 42%      | /                  |
| /proc              | OK   | OK   | OK    | 0%       | /proc              |
| mnttab             | OK   | OK   | OK    | 0%       | /etc/mnttab        |
| fd                 | OK   | OK   | OK    | 0%       | /dev/fd            |
| /dev/md/dsk/d8     | 2.0G | 86M  | 1.8G  | 5%       | /var               |
| swap               | 2.5G | 160K | 2.5G  | 1%       | /var/run           |
| swap               | 512M | 3.8M | 508M  | 1%       | /tmp               |
| /dev/md/dsk/d11    | 4.9G | 1.5G | 3.4G  | 32%      | /opt               |
| /dev/md/dsk/d21    | 2.9G | 111M | 2.8G  | 4%       | /opt/nortel        |
| /dev/md/dsk/d22    | 5.9G | 145M | 5.7G  | 3%       | /var/mysql/data    |
| /backup            | 3.9G | 4.0M | 3.9G  | 1%       | /backup            |
| /data              | 2.9G | 5.9M | 2.9G  | 1%       | /data              |
| /data/oradata      | 9.8G | 2.5G | 7.3G  | 26%      | /data/oradata      |
| /data/oradata/arch | 968M | 12M  | 956M  | 2%       | /data/oradata/arch |
| /data/qca          | 9.8G | 10M  | 9.7G  | 1%       | /data/qca          |

The *capacity* column indicates the percentage of disk utilization by the file system, which is specified in the *Mounted on* column.

- 10** Note the file system you want to increase, as well as its current size (under column 'size').
- 11** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

#### ATTENTION

Before you proceed with this procedure, ensure the file system you want to increase is full or nearly full and that its content is valid application data. Remove any unneeded files or files generated in error that are taking up disk space.

- 12** Determine the size by which to increase the file system, by subtracting the desired size for the file system based on your specific needs, from its current size (noted in 10).

For example, to determine the size by which to increase the 'qca' file system, subtract its current size, 123 MB from the desired size, for example, 256 MB. You would increase the size of the 'qca' file system by 133153 KB, or 133 MB.

- 13** Determine the amount of free disk space that can be allocated to file systems as follows:

- a. Determine the amount of free disk space on your system by typing

```
/opt/nortel/sspfs/fs/meta.pl fs
/opt/nortel/sspfs/fs/meta.pl free_space
/ 5000 - p | dc
```

and pressing the Enter key.

Divide the resulting number by 2048 to determine the amount of free disk space in megabytes (MB) that can be allocated to existing file systems.

| If the value is    | Do                            |
|--------------------|-------------------------------|
| less than zero (0) | contact Nortel for assistance |
| more than zero (0) | step <a href="#">b</a>        |

- b. Use the following table to determine your next step.

| If                                                                                                                                                                                                                               | Do                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| the value you determined in step <a href="#">12</a> (size by which to increase the file system) is greater than the value you obtained in step <a href="#">13 a</a> (amount of free disk space you can allocate to file systems) | contact Nortel for assistance |
| the value you determined in step <a href="#">12</a> (size by which to increase the file system) is less than the value you obtained in step <a href="#">13 a</a> (amount of free disk space you can allocate to file systems)    | step <a href="#">14</a>       |

#### ATTENTION

Once you increase the size of a file system, you cannot decrease it. Therefore, it is strongly recommended that you grow a file system in small increments.

- 14** Increase the size of the desired file system by typing

```
GrowClusteredFileSystem.ksh <mount_point>
<size>m
```

where

**mount\_point** is the name of the file system you want to increase (noted in step [10](#))



**size** is the size in megabytes (m) by which you want to increase the file system (determined in step 12)

**Example**

```
GrowClusteredFileSystem.ksh /data/qca 10m
```

The preceding example increases the '/data/qca' file system by 10 megabytes (MB).

- 15** Verify the status of file systems on the Inactive node by typing

```
udfstat
```

and pressing the Enter key.

| If the file systems are | Do                                                                   |
|-------------------------|----------------------------------------------------------------------|
| STANDBY normal UP clean | <a href="#">step 16</a>                                              |
| otherwise               | repeat step 15 until the file systems are "STANDBY normal UP clean". |

- 16** Reboot the Inactive node by typing

```
init 6
```

and pressing the Enter key.

Wait for the unit to recover before proceeding.

- 17** Perform a swact on the active unit by typing

```
swact
```

and pressing the Enter key.

This action causes a cluster failover and makes the active node inactive, and the inactive node active.

- 18** Log in to the Active node by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server** is the physical IP address of the active node in the cluster.

- 19** When prompted, enter your user ID and password.

- 20** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 21** When prompted, enter the root password.
- Ensure you are on the Active server by typing `ubmstat`. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.
- 22** Verify all applications are running on the active node by typing
- ```
# servquery -status all
```
- and pressing the Enter key.
- Verify all applications are running.
- 23** Verify all replicated file systems are "active up normal" by typing
- ```
udstat
```
- and press the Enter key.
- Ensure all file systems are in the "active up normal" state.
- 24** Clone the other node using procedure "Cloning the image of one server in a cluster to the other server", ensuring you log into the active node.
- You have completed this procedure.

---

—End—

---

## Verifying disk utilization on an SPFS-based server

### Application

Use this procedure to verify disk utilization by the file systems on a Server Platform Foundation Software (SPFS)-based server.

### Prerequisites

You must have root user privileges.

### Action

Perform the following steps to complete this procedure.

| Step | Action |
|------|--------|
|------|--------|

**At your workstation**

- 1 Log in to the server by typing  
`> telnet <server>`  
 and pressing the Enter key.  
 where  
`server` is the IP address or host name of the SPFS-based server
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  
`$ su - root`  
 and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Access the command line interface by typing  
`# cli`  
 and pressing the Enter key.

**Example response**

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exits
select -
```

- 6 Display the current disk capacity utilization as follows:

- a. Enter the number next to the 'View' option in the menu.

*Example response*

View

```

1 - SPFS_soft (Display Software
 Installation Level Of SPFS)
2 - chk_SPFS (Check SPFS Processes)
3 - sw_conf (The software configuration of
 the znc0s0jx)
4 - cpu_util (Overall CPU utilization)
5 - cpu_util_proc (CPU utilization by
 process)
6 - port_util (I/O port utilization)
7 - disk_util (Filesystem utilization)
X - exit
select -

```

- b. Enter the number next to the "disk\_util" option in the menu.

*Example response*

| Filesystem         | size | used | avail | capacity | Mounted on         |
|--------------------|------|------|-------|----------|--------------------|
| /dev/md/dsk/d2     | 3.9G | 1.6G | 2.3G  | 42%      | /                  |
| /proc              | OK   | OK   | OK    | 0%       | /proc              |
| mnttab             | OK   | OK   | OK    | 0%       | /etc/mnttab        |
| fd                 | OK   | OK   | OK    | 0%       | /dev/fd            |
| /dev/md/dsk/d8     | 2.0G | 86M  | 1.8G  | 5%       | /var               |
| swap               | 2.5G | 160K | 2.5G  | 1%       | /var/run           |
| swap               | 512M | 3.8M | 508M  | 1%       | /tmp               |
| /dev/md/dsk/d11    | 4.9G | 1.5G | 3.4G  | 32%      | /opt               |
| /dev/md/dsk/d21    | 2.9G | 111M | 2.8G  | 4%       | /opt/nortel        |
| /dev/md/dsk/d22    | 5.9G | 145M | 5.7G  | 3%       | /var/mysql/data    |
| /backup            | 3.9G | 4.0M | 3.9G  | 1%       | /backup            |
| /data              | 2.9G | 5.9M | 2.9G  | 1%       | /data              |
| /data/oradata      | 9.8G | 2.5G | 7.3G  | 26%      | /data/oradata      |
| /data/oradata/arch | 963M | 12M  | 953M  | 2%       | /data/oradata/arch |
| /data/qca          | 9.8G | 10M  | 9.7G  | 1%       | /data/qca          |

You have completed this procedure.

---

—End—

---

---

# Installing or replacing an HTTPS certificate on an SPFS-based server

---

## Application

Use this procedure to install or replace an HTTPS certificate on a simplex or an HA (high availability) SPFS-based server. An HTTPS certificate enables secure transmission of communications, and is required from (I)SN07 onward.

The steps to create a self-signed certificate are included in this procedure if you choose to use a self-signed certificate (see "[Types of certificates](#)" (page 641)).

## Types of certificates

You can use any one of the following three types of security certificates:

- a certificate granted from a well known certificate authority (CA): used when the server is used in a public way, such as for e-commerce web sites
- a company-generated certificate: used when the server is used internally, and the operating company has its own internal CA
- a self-signed certificate created locally on the server: used when the server is used in a more restricted manner.

When a server with a self-signed certificate is accessed, the browser presents the certificate and asks whether the certificate can be trusted. If the user answers 'yes', the server can be accessed. If the user answers 'no', nothing further will be received from the server.

The certificates differ in the level of trust that needs to be assigned to a server.

## Prerequisites

This procedure has the following prerequisites:

- The domain name service (DNS) must be enabled on the server to allow the security certificate to work, and must be enabled prior to the installation of the certificate. Refer to procedure 'Configuring Domain Name Service' in the .
- If purchasing a certificate from a third-party certificate authority (CA), such as VeriSign, obtain a PEM-encoded X.509 certificate, but without a passcode.

The common name portion of the certificate must match the fully qualified domain name (FQDN) of the server. Nortel recommends the

installation of a unique certificate for each host. A separate file contains the key, and must not have an associated password.

- Make sure all GUI screens are closed before you install the certificate.
- The RSA key for the HTTPS certificate must not have a password.
- The certificate must be created with the fully qualified domain name (FQDN) of the server on which the certificate will be installed.
- Sub-directories 'ssl.crt' and 'ssl.key' must already exist in the '/opt/apache/conf' directory.

## Navigation

- ["Simplex configuration \(one server\)" \(page 642\)](#)
- ["High-availability configuration \(two servers\)" \(page 647\)](#)

## Action

### Simplex configuration (one server)

| Step                                                                                                                                                                                                                                                 | Action                                                                                                                                                                                                                                                                                                                                                                                   |            |    |                                 |        |                                     |        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----|---------------------------------|--------|-------------------------------------|--------|
| <i>At your workstation</i>                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                          |            |    |                                 |        |                                     |        |
| 1                                                                                                                                                                                                                                                    | Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.<br><br>For detailed steps, refer to procedure Logging in to an SPFS-based server.                                                                                                                                                                                            |            |    |                                 |        |                                     |        |
| 2                                                                                                                                                                                                                                                    | Use the following table to determine your next step.                                                                                                                                                                                                                                                                                                                                     |            |    |                                 |        |                                     |        |
| <table border="1"> <thead> <tr> <th>If you are</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>using a self-signed certificate</td> <td>step 3</td> </tr> <tr> <td>not using a self-signed certificate</td> <td>step 4</td> </tr> </tbody> </table> |                                                                                                                                                                                                                                                                                                                                                                                          | If you are | Do | using a self-signed certificate | step 3 | not using a self-signed certificate | step 4 |
| If you are                                                                                                                                                                                                                                           | Do                                                                                                                                                                                                                                                                                                                                                                                       |            |    |                                 |        |                                     |        |
| using a self-signed certificate                                                                                                                                                                                                                      | step 3                                                                                                                                                                                                                                                                                                                                                                                   |            |    |                                 |        |                                     |        |
| not using a self-signed certificate                                                                                                                                                                                                                  | step 4                                                                                                                                                                                                                                                                                                                                                                                   |            |    |                                 |        |                                     |        |
| 3                                                                                                                                                                                                                                                    | Create the self-signed certificate as follows: <ol style="list-style-type: none"> <li>Access the 'conf' directory by typing<br/> <pre># cd /opt/apache/conf</pre> and pressing the Enter key.</li> <li>Generate the key file (server.key) by typing<br/> <pre># /opt/openssl/bin/openssl genrsa -rand /var/log/SPFSlog 1024 &gt; server.key</pre> and pressing the Enter key.</li> </ol> |            |    |                                 |        |                                     |        |

Enter the command on one line with a space between the -rand and /var/log/sspflog entries.

- c. Generate the certificate file (server.crt) by typing

```
/opt/openssl/bin/openssl req -new -key
server.key -x509 -days 3650 -out server.crt
```

and pressing the Enter key.

Enter the command on one line with a space between the -key and server.key entries.

*Example response:*

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank.

For some fields there will be a default value.

If you enter '.', the field will be left blank.

-----

- d. When prompted, enter a two letter code for the country where the server is located.

*Example response:*

Country Name (2 letter code) [AU]:

- e. When prompted, enter the full name of the State or Province where the server is located.

*Example response:*

State or Province Name (full name)

[Some-State]:

- f. When prompted, enter the city where the server is located.

*Example response:*

Locality Name (eg, city) []:

- g. When prompted, enter the name of the company that owns the server.

*Example response:*

Organization Name (eg, company) [Internet Widgits Pty Ltd]:

- h. When prompted, enter the name of the department that owns the server.

*Example response:*

Organizational Unit Name (eg, section) []:

- i. When prompted, enter the fully qualified domain name (FQDN) of the server.

*Example response:*

Common Name (eg, YOUR name []:

Email Address []:

- j. When prompted, enter the email address of the organization that owns the server.

*Example response:*

Email Address []:

- 4 Place the certificate file (server.crt) you obtained in "/opt/apache/conf/ssl.crt".

If directory 'ssl.crt' does not exist, you need to create it.

- 5 Place the key file (server.key) you obtained in '/opt/apache/conf/ssl.key'.

If directory 'ssl.key' does not exist, you need to create it.

- 6 Change the certificate's owner and group by typing

```
chown root:other
/opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

Enter the command on one line with a space between "other" and the directory path.

- 7 Change the key file's owner and group by typing

```
chown root:other
/opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

Enter the command on one line with a space between "other" and the directory path.

- 8 Set the certificate permissions by typing

```
chmod 600 /opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

- 9 Set the key file permissions by typing

```
chmod 600 /opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.



- 10** Restart the WEBSERVER as follows:
- Stop the WEBSERVER by typing  

```
servstop WEBSERVER
```

and pressing the Enter key.
  - Start the WEBSERVER by typing  

```
servstart WEBSERVER
```

and pressing the Enter key.
- 11** Restart the WEBSERVICES as follows:
- Stop the WEBSERVICES by typing  

```
servstop WEBSERVICES
```

and pressing the Enter key.
  - Start the WEBSERVICES by typing  

```
servstart WEBSERVICES
```

and pressing the Enter key.
- 12** Use the following table to determine your next step

| If                             | Do                      |
|--------------------------------|-------------------------|
| The server is hosting the IEMS | step <a href="#">14</a> |
| otherwise                      | step <a href="#">22</a> |

- 13** Stop the IEMS server application by typing  

```
servstop IEMS
```

and pressing the Enter key
- 14** Disable the SSL utility by typing  

```
/opt/nortel/iems/current/bin/SSLUtil.sh Disable
```

and pressing the Enter key.
- 15** Enable the SSL utility by typing  

```
/opt/nortel/iems/current/bin/SSLUtil.sh Enable
```

and pressing the Enter key.
- 16** Start the IEMS server application by typing  

```
servstart IEMS
```

and pressing the Enter key.

- 17** Reconfigure the SunOne IS client environment on the system to use SSL by typing
- ```
# /opt/nortel/applications/security/current_slisext/swm  
ext/swmgmt/bin/configure_slisext.sh -ssl
```
- and pressing the Enter key.
- The above command is entered on one line.
- 18** Restart the WEBSERVER as follows:
- Stop the WEBSERVER by typing
- ```
servstop WEBSERVER
```
- and pressing the Enter key.
- Start the WEBSERVER by typing
- ```
# servstart WEBSERVER
```
- and pressing the Enter key.
- 19** Restart the WEBSERVICES as follows:
- Stop the WEBSERVICES by typing
- ```
servstop WEBSERVICES
```
- and pressing the Enter key.
- Start the WEBSERVICES by typing
- ```
# servstart WEBSERVICES
```
- and pressing the Enter key.
- 20** Restart the Radius server as follows:
- Stop the Radius server by typing
- ```
servstop RADSVR
```
- and pressing the Enter key.
- Start the Radius server by typing
- ```
# servstart RADSVR
```
- and pressing the Enter key.
- 21** If the CS 2000 Management Tools software is installed prior to installing the HTTPS certificate, you need to reconfigure SESM. If required, refer to the procedure "Configuring the SESM server application" in *ATM/IP Configuration Management*, NN10409-500..
- 22** If you installed an HTTPS certificate on an existing SPFS-based server that was not previously using a certificate, users need to clear the JWS cache on their workstation. Clearing the cache allows

users to properly launch the CS 2000 Management Tools client applications. If required, refer to procedure "Clearing the JWS cache on a client workstation" in the ATM/IP Solution-level Configuration Management document, NN10409-500

- 23** You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Action

High-availability configuration (two servers)

Step	Action

At your workstation

- 1** Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

For detailed steps, refer to procedure Logging in to an SPFS-based server.

- 2** Use the following table to determine your next step

If you are	Do
using a self-signed certificate	step 3
otherwise	step 4

- 3** Create the self-signed certificate as follows:

- a. Access the "conf" directory by typing

```
# cd /opt/apache/conf
```

and pressing the Enter key.

- b. Generate the key file (server.key) by typing

```
# /opt/openssl/bin/openssl genrsa -rand
/var/log/SPFSlog 1024 > server.key
```

and pressing the Enter key.

Enter the command on one line with a space between the -rand and /var/log/sspflog entries.

- c. Generate the certificate file (server.crt) by typing

```
# /opt/openssl/bin/openssl req -new -key
server.key -x509 -days 3650 -out server.crt
```

and pressing the Enter key.

Enter the command on one line with a space between the -key and server.key entries.

Example response:

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank.

For some fields there will be a default value.

If you enter '.', the field will be left blank.

- d. When prompted, enter a two letter code for the country where the server is located.

Example response:

Country Name (2 letter code) [AU]:

- e. When prompted, enter the full name of the State or Province where the server is located.

Example response:

State or Province Name (full name)

[Some-State]:

- f. When prompted, enter the city where the server is located.

Example response:

Locality Name (eg, city) []:

- g. When prompted, enter the name of the company that owns the server.

Example response:

Organization Name (eg, company) [Internet Widgits Pty Ltd]:

- h. When prompted, enter the name of the department that owns the server.

Example response:

Organizational Unit Name (eg, section) []:

- i. When prompted, enter the fully qualified domain name (FQDN) of the server.

Example response:

Common Name (eg, YOUR name []):

- j. When prompted, enter the email address of the organization that owns the server.

Example response:

Email Address []:

- 4 Place the certificate file (server.crt) you obtained in '/opt/apache/conf/ssl.crt'.
If directory 'ssl.crt' does not exist, you need to create it.
- 5 Place the key file (server.key) in '/opt/apache/conf/ssl.key'.
If directory 'ssl.key' does not exist, you need to create it.
- 6 Change the certificate's owner and group by typing

```
# chown root:other  
/opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.
Enter the command on one line with a space between "other" and the directory path.
- 7 Change the key file's owner and group by typing

```
# chown root:other  
/opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.
Enter the command on one line with a space between "other" and the directory path.
- 8 Set the certificate permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.
- 9 Set the key file permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.
- 10 Restart the WEBSERVER as follows:
 - a. Stop the WEBSERVER by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.
 - b. Start the WEBSERVER by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.

11 Restart the WEBSERVICES as follows:

- a. Stop the WEBSERVICES by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.

- b. Start the WEBSERVICES by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.

12 Use the following table to determine your next step

If	Do
The server is hosting the IEMS	step 13
otherwise	step 21

13 Stop the IEMS server application by typing

```
# servstop IEMS
```

and pressing the Enter key

14 Disable the SSL utility by typing

```
# /opt/nortel/iems/current/bin/SSLUtil.sh Disable
```

and pressing the Enter key.

15 Enable the SSL utility by typing

```
# /opt/nortel/iems/current/bin/SSLUtil.sh Enable
```

and pressing the Enter key.

16 Start the IEMS server application by typing

```
# servstart IEMS
```

and pressing the Enter key.

17 Reconfigure the SunOne IS client environment on the system to use SSL by typing

```
# /opt/nortel/applications/security/current_slisext/swm  
ext/swmgmt/bin/configure_slisext.sh -ssl
```

and pressing the Enter key.

The above command is entered on one line.

18 Restart the WEBSEVER as follows:

- a. Stop the WEBSERVER by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.
 - b. Start the WEBSERVER by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.
- 19 Restart the WEBSERVICES as follows:
 - a. Stop the WEBSERVICES by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.
 - b. Start the WEBSERVICES by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.
- 20 Restart the Radius server as follows:
 - a. Stop the Radius server by typing

```
# servstop RADSVR
```

and pressing the Enter key.
 - b. Start the Radius server by typing

```
# servstart RADSVR
```

and pressing the Enter key.
- 21 If the CS 2000 Management Tools software is installed prior to installing the HTTPS certificate, you need to reconfigure SESM. If required, refer to the procedure "Configuring the SESM server application" in *ATM/IP Configuration Management*, NN10409-500..
- 22 Clone the image of the node with the HTTPS certificate onto the other node using procedure ["Cloning the image of one node in a cluster to the other node" \(page 528\)](#).
- 23 If you installed an HTTPS certificate on an existing SPFS-based server that was not previously using a certificate, users need to clear the JWS cache on their workstation. Clearing the cache allows users to properly launch the CS 2000 Management Tools client applications. If required, refer to procedure "Clearing the JWS cache on a client workstation" in the *ATM/IP Solution-level Configuration Management* document, NN10409-500

- 24** You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Installing or replacing an HTTPS certificate on a simplex SPFS-based server

Application

Use this procedure to install or replace an HTTPS certificate on a simplex Server Platform Foundation Software (SPFS)-based server. An HTTPS certificate enables secure transmission of communications, and is required from the (I)SN07 release onward.

The steps to create a self-signed certificate are included in this procedure if you choose to use a self-signed certificate (see "[Types of certificates](#)" (page 653)).

Types of certificates

You can use any one of the following three types of security certificates:

- a certificate granted from a well known certificate authority (CA): used when the server is used in a public way, such as for e-commerce web sites
- a company-generated certificate: used when the server is used internally, and the operating company has its own internal CA
- a self-signed certificate created locally on the server: used when the server is used in a more restricted manner.

Note: When a server with a self-signed certificate is accessed, the browser presents the certificate and asks whether the certificate can be trusted. If the user answers 'yes', the server can be accessed. If the user answers 'no', nothing further will be received from the server.

The certificates differ in the level of trust that needs to be assigned to a server.

Prerequisites

This procedure has the following prerequisites:

- The domain name service (DNS) must be enabled on the server to allow the security certificate to work, and must be enabled prior to the installation of the certificate. Refer to procedure 'Configuring Domain Name Service' in the ATM/IP Solution-level Configuration Management document, NN10409-500 .
- If purchasing a certificate from a third-party certificate authority (CA), such as VeriSign, obtain a PEM-encoded X.509 certificate, but without a passcode.

Note: The common name portion of the certificate must match the fully qualified domain name (FQDN) of the server. Nortel recommends the installation of a unique certificate for each host. A separate file contains the key, and must not have an associated password.

- Make sure all GUI screens are closed before you install the certificate.
- The RSA key for the HTTPS certificate must not have a password.
- The certificate must be created with the fully qualified domain name (FQDN) of the server on which the certificate will be installed.
- Sub-directories 'ssl.crt' and 'ssl.key' must already exist in the '/opt/apache/conf' directory.

Action

Simplex configuration (one server)

Step	Action						
At your workstation							
1	Establish a connection to the server through telnet or SSH, and log in using the root user ID and password. For detailed steps, refer to procedure Logging in to an SPFS-based server.						
2	Use the following table to determine your next step.						
<table border="1"> <thead> <tr> <th>If you are</th> <th>Do</th> </tr> </thead> <tbody> <tr> <td>using a self-signed certificate</td> <td>step 3</td> </tr> <tr> <td>not using a self-signed certificate</td> <td>step 4</td> </tr> </tbody> </table>		If you are	Do	using a self-signed certificate	step 3	not using a self-signed certificate	step 4
If you are	Do						
using a self-signed certificate	step 3						
not using a self-signed certificate	step 4						
3	Create the self-signed certificate as follows: - Access the 'conf' directory by typing <pre># cd /opt/apache/conf</pre> and pressing the Enter key. - Generate the key file (server.key) by typing <pre># /opt/openssl/bin/openssl genrsa -rand /var/log/SPFSlog 1024 > server.key</pre> and pressing the Enter key. Note: Enter the command on one line with a space between the -rand and /var/log/sspfslog entries.						

- c. Generate the certificate file (server.crt) by typing

```
# /opt/openssl/bin/openssl req -new -key
server.key -x509 -days 3650 -out server.crt
```

and pressing the Enter key.

Note: Enter the command on one line with a space between the -key and server.key entries.

Example response:

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank.

For some fields there will be a default value.

If you enter '.', the field will be left blank.

- d. When prompted, enter a two letter code for the country where the server is located.

Example response:

Country Name (2 letter code) [AU]:

- e. When prompted, enter the full name of the State or Province where the server is located.

Example response:

State or Province Name (full name)

[Some-State]:

- f. When prompted, enter the city where the server is located.

Example response:

Locality Name (eg, city) []:

- g. When prompted, enter the name of the company that owns the server.

Example response:

Organization Name (eg, company) [Internet Widgits Pty Ltd]:

- h. When prompted, enter the name of the department that owns the server.

Example response:

Organizational Unit Name (eg, section) []:

- i. When prompted, enter the fully qualified domain name (FQDN) of the server.

Example response:

Common Name (eg, YOUR name []):

Email Address []:

- j. When prompted, enter the email address of the organization that owns the server.

Example response:

Email Address []:

- 4 Place the certificate file (server.crt) you obtained in "/opt/apache/conf/ssl.crt".

Note: If directory 'ssl.crt' does not exist, you need to create it.

- 5 Place the key file (server.key) you obtained in '/opt/apache/conf/ssl.key'.

Note: If directory 'ssl.key' does not exist, you need to create it.

- 6 Change the certificate's owner and group by typing

```
# chown root:other  
/opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

Note: Enter the command on one line with a space between "other" and the directory path.

- 7 Change the key file's owner and group by typing

```
# chown root:other  
/opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

Note: Enter the command on one line with a space between "other" and the directory path.

- 8 Set the certificate permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.crt/server.crt
```

and pressing the Enter key.

- 9 Set the key file permissions by typing

```
# chmod 600 /opt/apache/conf/ssl.key/server.key
```

and pressing the Enter key.

- 10 Restart the WEBSERVER as follows:

- a. Stop the WEBSERVER by typing
`# servstop WEBSERVER`
and pressing the Enter key.
 - b. Start the WEBSERVER by typing
`# servstart WEBSERVER`
and pressing the Enter key.
- 11 Restart the WEBSERVICES as follows:
 - a. Stop the WEBSERVICES by typing
`# servstop WEBSERVICES`
and pressing the Enter key.
 - b. Start the WEBSERVICES by typing
`# servstart WEBSERVICES`
and pressing the Enter key.
- 12 Use the following table to determine your next step

If	Do
The server is hosting the IEMS	step 14
otherwise	step 22
- 13 Stop the IEMS server application by typing
`# servstop IEMS`
and pressing the Enter key
- 14 Disable the SSL utility by typing
`# /opt/nortel/iems/current/bin/SSLUtil.sh Disable`
and pressing the Enter key.
- 15 Enable the SSL utility by typing
`# /opt/nortel/iems/current/bin/SSLUtil.sh Enable`
and pressing the Enter key.
- 16 Start the IEMS server application by typing
`# servstart IEMS`
and pressing the Enter key.
- 17 Reconfigure the SunOne IS client environment on the system to use SSL by typing

```
# /opt/nortel/applications/security/current_slisext/swm  
ext/swmgmt/bin/configure_slisext.sh -ssl
```

and pressing the Enter key.

Note: The above command is entered on one line.

18 Restart the WEBSERVER as follows:

- a. Stop the WEBSERVER by typing

```
# servstop WEBSERVER
```

and pressing the Enter key.

- b. Start the WEBSERVER by typing

```
# servstart WEBSERVER
```

and pressing the Enter key.

19 Restart the WEBSERVICES as follows:

- a. Stop the WEBSERVICES by typing

```
# servstop WEBSERVICES
```

and pressing the Enter key.

- b. Start the WEBSERVICES by typing

```
# servstart WEBSERVICES
```

and pressing the Enter key.

20 Restart the Radius server as follows:

- a. Stop the Radius server by typing

```
# servstop RADSVR
```

and pressing the Enter key.

- b. Start the Radius server by typing

```
# servstart RADSVR
```

and pressing the Enter key.

- 21** If the CS 2000 Management Tools software is installed prior to installing the HTTPS certificate, you need to reconfigure SESM. If required, refer to the procedure "Configuring the SESM server application" in *ATM/IP Configuration Management*, NN10409-500..

- 22** If you installed an HTTPS certificate on an existing SPFS-based server that was not previously using a certificate, users need to clear the JWS cache on their workstation. Clearing the cache allows users to properly launch the CS 2000 Management Tools client applications. If required, refer to procedure "Clearing the JWS cache

on a client workstation" in the ATM/IP Solution-level Configuration Management document, NN10409-500

- 23** You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

—End—

Preparing a DVD-RW for use

Application

Use this procedure to verify the DVD-RW is ready for use when using it for the first time, or when you want to erase the contents of a used DVD-RW to use it again.

Prerequisites for Core and Billing Manager 850

All users with non-restricted shell access are authorized to perform this procedure.

You require root-user access, or must be a user in a role group authorized to perform config-admin actions, if an error occurs when ejecting a DVD.

For more information about how to log in to the CBM as an authorized user, how to request non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	<i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611
Requesting non-restricted shell access	<i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611
Displaying actions a role group is authorized to perform	<i>Core and Billing Manager 850 Security and Administration</i> , NN10358-611

Action

Perform the following steps to complete this procedure.

Step	Action

At the server

- 1 Insert the DVD into the drive.

Only rewriteable media can be erased. Verify that the DVD you are attempting to erase is a DVD-RW before inserting it into the drive.

At your workstation

- 2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or hostname of the SPFS-based server

- 3 When prompted, enter your user ID and password.
- 4 Use the following table to determine your next step.

If the DVD is	Do
new	step 5
used	step 6

- 5 Verify the DVD is ready for use by typing
`$ cdrw -l`
 and pressing the Enter key

If the system response	Do
provides the CD device	step 11
indicates "No CD writers found or no media in the drive"	step 6

- 6 Erase the contents of the DVD by typing
`$ cdrw -b all`
 and pressing the Enter key

ATTENTION

Erasing a DVD-RW can take over two hours. You can also use the "fast" and "session" arguments. For more details, refer to the man pages by typing `man cdrw`

- 7 Reinsert the DVD into the drive.
- 8 Verify the DVD is ready for use by typing
`$ cdrw -l`
 and pressing the Enter key

If the system response	Do
provides the CD device	step 11
indicates "No CD writers found or no media in the drive" or "Media in the device is not erasable"	step 9

- 9 Eject the DVD from the drive as follows:
 - a. Ensure you are at the root directory level by typing

```
$ cd /
```

and pressing the Enter key.
 - b. Eject the DVD by typing

```
# eject cdrom
```

and pressing the Enter key.

If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, re-try the "eject cdrom" command.
 - c. Remove the DVD from the drive.
- 10 Obtain another DVD and repeat the process starting with step 4.
- 11 Proceed to use the DVD.

You have completed this procedure.

—End—

Changing the PMGRdaemon password

This procedure enables you to change the Windows Administrator password and the 'Logon' password for the PMGRdaemon service.

ATTENTION

When changing the administrator password for the machine you must also change the 'Logon' password for the PMGRdaemon service.

Step Action

At the Windows desktop interface

- 1 Right click the **"My Computer"** icon on the desktop.
- 2 Select **"Manage"** from the pop-up menu. The Computer Management window opens.
- 3 Under **"System Tools"**, expand the **"Local Users and Groups"** folder.
- 4 Open the **"Users"** folder.
- 5 In the right panel of the Computer Management window, right click the **"Administrator"** icon.
- 6 Select **"Set Password"** from the pop-up menu. The Set Password window opens.
- 7 In the Set Password window, enter the new password in the **"New password"** dialog box.
- 8 Enter the new password in the **"Confirm password"** dialog box.
- 9 Click **"OK"**. The Set Password window closes.
- 10 From the Computer Management window, expand the **"Services and Applications"** folder.
- 11 Open the **"Services"** folder.
- 12 In the right panel of the Computer Management window, right click the **"PMGRdaemon service"** icon and select **"Properties"**.
- 13 When the PMGRdaemon Properties dialog box opens, select the logon tab.
- 14 Make sure the user is set to **'.\Administrator'**.
- 15 Enter the new password.

16 Confirm the new password.

Note: You must log off and back on to the system once you change the passwords.

17 Close all windows and log off and back on to the system.

18 You have completed this procedure.

—End—

ORCA BTX8 and BTX12 TGCP gateway administration overview

The Open Reliable Communication Architecture (ORCA) Broadband Telephony Exchange (BTX) products are VoIP media gateways that provide interworking between a PacketCable managed IP network and the PSTN. You can install and manage an ORCA gateway using the configuration software that is provided with the product (NueraView).

NueraView consists of two integrated products, Nuera Configurator and HP OpenView Network Node Manager. NueraView enables you to:

- set up an ORCA BTX application with the components required to provide network management functions through HP OpenView
- monitor all the ORCA gateways in a network
- recognize fault conditions and isolate the problem to a particular subsystem or network component
- generate performance reports
- define threshold-crossing alerts to detect degrading network performance

For instructions on how to manage the ORCA BTX8 and BTX21 TGCP gateways, refer to vendor-supplied documentation.

How to trace a call on a CS 2000

On a CS 2000, you can trace established intra-office and interoffice calls involving

- TDM circuit-switched technology
- dynamic packet trunks (DPTs) that use SIP-T signaling

Note: Not for DPTs that use BICC signaling.

To trace a call, use the SIPTRACE command. You can use this command in any level of the MAP user interface

The SIPTRACE command can be used to trace E911 calls as well as other calls.

Syntax of the SIPTRACE command

For a TDM call, the syntax of the SIPTRACE command is as follows:

```
SIPTRACE T <TDM-trunk-group> <TDM-trunk-member>
```

where

<TDM-trunk-group> is the common language location identifier (CLLI) of the TDM trunk group.

<TDM-trunk-member> is an integer in the range 0 to 9999

For a call on a DPT, the syntax of the command is as follows:

```
SIPTRACE D '<DPT-SIPT-callid>'
```

where

<DPT-SIPT-callid> is the DPT SIP-T call ID

Note: The DPT SIP-T call ID must be enclosed in single quotation marks, as shown above.

System response

The system response to the SIPTRACE command is as follows:

<input> is currently connected to <output>

Whenever you use a SIP-T callid as input for a SIPTRACE command, the system checks for a possible second trunk termination within the same call server domain. Similarly, if the system finds that a SIP-T callid is the output of a SIPTRACE command, the system checks for a possible second trunk termination within the same call server domain.

For more information, see the following examples.

TDM to line interworking in the CS 2000

In this example, the input is a TDM trunk member. The system response indicates that it is connected to a line.

TDM to line interworking in the CS 2000

```
CI> SIPTRACE T ETSIV1LPA 2

TDM trunk ETSIV1LPA 2 is currently connected to LINE
1158206005
```

SIP-T DPT to line interworking in the CS 2000

In this example, the input is a SIP-T DPT callid. The system response indicates that it is connected to a line. The call scenario is as follows:
Line 1158206005 --> SIP-T --> Line 1158206007.

SIP-T DPT to line interworking in the CS 2000

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT K4SIP1LOOPFR3 callid
0026.4030-10-16-49-02.67@CS2K4_84 is currently connected
to LINE 1158206007
SIP-T DPT KSIP1LOOPFR3 callid
0026.4030-10-16-49-02.67@CS2K4_84 is currently connected
to LINE 1158206005
```

TDM to TDM interworking in the CS 2000

In this example, the input is a TDM trunk member. The system response indicates that it is connected to another TDM trunk member.

TDM to TDM interworking in the CS 2000

```
CI> SIPTRACE T ETSIV1LPB 2

TDM trunk ETSIV1LPB 2 is currently connected to TDM
trunk UKISUPLPA 10
```

TDM to SIP-T DPT interworking in CS 2000

In this example, the input is a TDM trunk member. The system response indicates that it is connected to a SIP-T DPT callid. The call scenario is as follows:

Line 115820607 --> TDM ETSILPA 2 TDM ETSILPB 2 --> SIP-T --> Line 1158206008.

TDM to SIP-T DPT interworking in CS 2000

```
CI> SIPTRACE T ETSIV1LPB 2

TDM trunk ETSIV1LPB 2 is currently connected to
SIP-T DPT K4SIP1LOOPFR3 callid
0026.4030-10-16-49-02.67@CS2K4_84
SIP-T DPT K4SIP1LOOPFR3 callid
0026.4030-10-16-49-02.67@CS2K4_84 is currently connected to
LINE 1158206008
```

SIP-T DPT to TDM interworking in CS 2000

In this example, the input is a SIP-T DPT callid. The system response indicates that it is connected to a TDM trunk member. The call scenario is as follows:

Inter-call Server posted SIP-T --> TDM ETSILPA 2 TDM ETSILPB 2 --> SIP-T --> Line 1158206008.

SIP-T DPT to TDM interworking in CS 2000

```
CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT K1SIP1V1 callid
0026.4030-10-16-49-02.67@CS2K4_84 is currently
connected to TDM trunk ETSIV1LPA 2
SIP-T DPT K1SIP1V1 callid 0026.4030-10-16-49-02.67@CS2K4_84
not associated with any active call
```

Note: In this case, the SIPTRACE command cannot determine the other agent for an inter-call-server SIP-T DPT because another call server is involved. Therefore, the output shows that the SIPTRACE command execution in this call server could not determine the connected agent for the SIP-T leg belonging to another call-server domain. To determine the complete path of the call, the SIPTRACE command must be executed in successive call servers also.

Output TDM trunk member identified as a C7ISL member

In this example, the input is a TDM trunk member. The system response indicates that it is connected to a TDM trunk member that is found to be a member of a C7ISL (ISUP signaling loopback) facility. In this case, the response displays the final agent of the call.

Output TDM trunk member identified as a C7ISL member

```

CI> SIPTRACE T ETSIV1LPB 2

TDM trunk ETSIV1LPB 2 is currently connected to TDM
trunk (C7ISL) ETSIV1LPA 3
TDM trunk (C7ISL) UKISUPLPA 4 is currently connected
to LINE 1158206005

```

Input TDM trunk member identified as a C7ISL member

In this example, the input is a TDM trunk member that is a member of a C7ISL (ISUP signaling loopback) facility. The system response indicates that it is connected to a TDM trunk member.

Input TDM trunk member identified as a C7ISL member

```

CI> SIPTRACE T ETSIV1LPB 2

TDM trunk (C7ISL) ETSIV1LPB 2 is currently connected to
TDM trunk UKISUPLPA 8

```

SIP-T looparound

In this case the system encounters a SIP-T callid as the output of the SIPTRACE command execution. The system then checks for a possible second trunk termination within the same call server domain. The call scenario is as follows:

Line 1158206005 --> SIP-T --> SIP-T (posted) --> Line 1158206007.

SIP-T looparound

```

CI> SIPTRACE D '0026.4030-10-16-49-02.67@CS2K4_84'

SIP-T DPT K1SIP1UK3 callid
0026.4030-10-16-49-02.67@CS2K4_84 is currently
connected to SIP-T DPT K1SIP1V1 callid
0026.4030-10-16-49-02.95@CS2K4_84
SIP-T DPT K2SIP1CZ1 callid
00026.4030-10-16-49-02.95@CS2K4_84 is currently
connected to LINE 1158206005
SIP-T DPT K1SIP1UK3 callid
0026.4030-10-16-49-02.67@CS2K4_84 is currently
connected to LINE 1158206007

```

Note: If the output of the SIPTRACE command involves a SIP-T DPT callid, we cannot predict the sequence in which the output agents will be

displayed in the output. The output sequence depends on the sequence in which the SIP-T GWC returns the DPT terminal IDs.

Using FTP

Application

This procedure is used for the Unix command-line utility file transfer protocol (FTP) to perform the following tasks:

- transfer a file from a remote device, such as a server or another workstation, to your workstation
- transfer a file from your workstation to a remote device, such as a server or another workstation

Prerequisites

This procedure has the following prerequisites:

- You must know the name of the file
- You must know the IP address of the remote device
- You must know how to log in to the remote device, and be in possession of both userid and password
- You must know the name of the directory on your workstation

Action

Perform each of the following procedures as necessary

Transferring a file to your workstation

Step	Action
<i>At your workstation</i>	
1	Open a command prompt window
2	Make sure you are located in the directory that will receive the files. If necessary, use the cd command to change directories
3	Start an FTP session by typing: # ftp <device_ip_address> and pressing the Enter key. where device_ip_address is the IP address of the remote device where the files reside
4	When prompted, enter your user ID and password
5	Change the transfer mode to binary by typing:

At your workstation

- 1 Open a command prompt window
- 2 Make sure you are located in the directory that will receive the files. If necessary, use the cd command to change directories
- 3 Start an FTP session by typing:

ftp <device_ip_address>

and pressing the Enter key.

where

device_ip_address is the IP address of the remote device where the files reside
- 4 When prompted, enter your user ID and password
- 5 Change the transfer mode to binary by typing:

- `ftp> bin`
and pressing the Enter key
- 6 List the directories on the remote device by typing:
`ftp> ls`
and pressing the Enter key
- 7 Locate the directory that contains the files you want to receive. If necessary use the `cd` command to change directories
- 8 List the contents of the directory by typing:
`ftp> ls -l`
and pressing the Enter key
- 9 Locate the file you want to receive
- 10 Copy the file to your workstation by typing:
`ftp> get <file_name>`
and pressing the Enter key.
where
`file_name` is the name of the file
- 11 End the FTP session by typing:
`ftp> bye`
and pressing the Enter key
- 12 List the contents of the directory to ensure the files successfully transferred to your workstation by typing:
`# ls -l`
and pressing the Enter key.
You have completed this procedure.

—End—

Transferring a file from your workstation

Step	Action

At your workstation

1	Make sure you have located the directory that contains the file. If necessary, use the <code>cd</code> command to change directories.

- 2 Open a command prompt window.
- 3 List the contents of the directory by typing:
`ftp> ls -l`
and pressing the Enter key.
- 4 Make sure the directory contains the file you want to copy.
- 5 Start an FTP session by typing:
`# ftp <device_ip_address>`
and pressing the Enter key.
where
`device_ip_address` is the IP address of the remote device.
- 6 When prompted, enter your user ID and password.
- 7 Change the transfer mode to binary by typing:
`ftp> bin`
and pressing the Enter key.
- 8 List the directories on the remote device by typing:
`ftp> ls`
and pressing the Enter key.
- 9 Locate the directory that contains the files. If necessary use the `cd` command to change directories.
- 10 List the contents of the directory by typing:
`ftp> ls -l`
and pressing the Enter key.
- 11 Copy the file to the remote device by typing:
`ftp> put<file_name>`
and pressing the Enter key.
where
`file_name` is the name of the file.
- 12 List the contents of the directory to ensure the files successfully transferred to the device by typing:
`# ls -l`
and pressing the Enter key.

- 13** End the FTP session by typing:
- `ftp> bye`
- and pressing the Enter key.
- You have completed this procedure.

—End—

Appendix A

Mapping of Multiservice Data Manager, Multiservice Switch 15000 and Media Gateway 15000 access privileges to IEMS groups in VoIP networks

In VoIP solutions, IEMS maintains a single set of userids for access to all the MDM workstations and MSS/MG15000 switches in the associated central office. This centralization promotes ease of managing the userids across multiple switches and workstations, and reduces the time to make necessary changes.

IEMS user group mappings

IEMS provides thirty user groups consisting of six device areas with five associated security levels. These user groups are mapped onto the MDM and MSS/MG15000 access privileges.

The six IEMS device areas are:

- In: line services management. This category is not used for MDM or MSS/MG15000 management functions.
- tk: trunk services management. This category is not used for MDM or MSS/MG15000 management functions.
- mgc: media gateway controller management. This category is used for MSS/MG15000 management functions
- gw: gateway management. This category is not used for MSS/MG15000 management functions.
- ems: EMS management. This category is used for MDM functions.
- sec: security management. This category is not used for MDM or MSS/MG15000 management functions.

The five IEMS security areas and how they are used for MSS/MG15000 and MDM management functions are:

- ro (read only) level provides the ability to display surveillance information, but not to alter it.
- rw (read/write) level provides the ability to display surveillance information and to do configuration of MSS/MG15000.
- mtc (maintenance) level provides the ability to configure MSS/MG15000 nodes. Operator Client application access is not supported.
- spro (subscriber provisioning) level is mapped to the system administration impact level for MSS/MG15000 nodes and provides access to MSS/MG15000 administration tools from the Operator Client application.
- adm (administration) level is mapped to the debug impact level for MSS/MG15000 nodes and provides access to all MDM resources except MDP. A special local MDM userid is required to access MDP functionality.

IEMS group mapping for MDM Toolset functionality

Table 1 "IEMS user group mapping for MDM Toolset functions" (page 676) shows the mapping between the IEMS groups and the MDM Toolset functions.

Table 1
IEMS user group mapping for MDM Toolset functions

MDM Toolset functions	IEMS group					MDM local userid
	emsro	emsrw	emsmtc	emsspro	emsadmin	root
Alarm Display: Active	allow	allow	deny	allow	allow	allow
Alarm Help	allow	allow	allow	allow	allow	allow
Command Console	allow	allow	deny	allow	allow	allow
Component Information Viewer	allow	allow	deny	allow	allow	allow
Component Status Display	allow	allow	deny	allow	allow	allow
Data Synchronization Administration	allow	allow	allow	allow	allow	allow
Note: MDP configuration and log viewer commands must be accessed using the MDP administrator userid maintained locally on the MDM workstation.						

MDM Toolset functions	IEMS group					MDM local userid
	emsro	emsrw	emsmtc	emssprov	emsadmin	root
Data Viewer	deny	deny	deny	allow	allow	allow
Disruptive Command Safeguard	deny	deny	deny	deny	allow	allow
Enhanced Multiservice Switch interface controller (EPIC)	deny	allow	deny	allow	allow	allow
General management data router (GMDR) administration	deny	allow	deny	allow	allow	allow
Host group directory server (HGDS) administration	deny	allow	deny	allow	allow	allow
Log Browser	allow	allow	deny	allow	allow	allow
MDM license	deny	allow	deny	allow	deny	allow
MDM release update	deny	allow	deny	allow	allow	allow
MDP configuration	deny	deny	deny	deny	deny	deny
MDP log viewer	deny	deny	deny	deny	deny	deny
MDP data viewer	deny	deny	deny	allow	allow	deny
Memory utilization	allow	allow	allow	allow	allow	allow
Network Activation Tool	deny	allow	deny	allow	allow	allow
MSS Service Data Backup and Restore	deny	deny	allow	deny	allow	allow
Network Model shared memory utilization	allow	allow	allow	allow	allow	allow
Network Status Bar	allow	allow	deny	allow	allow	allow
Network Viewer	allow	allow	deny	allow	allow	allow
Nodal Provisioning	deny	allow	deny	allow	allow	allow
Nodal Provisioning Template	deny	allow	deny	allow	allow	allow
On-line documentation	allow	allow	allow	allow	allow	allow
Operational commands	allow	allow	deny	allow	allow	allow
Note: MDP configuration and log viewer commands must be accessed using the MDP administrator userid maintained locally on the MDM workstation.						

MDM Toolset functions	IEMS group					MDM local userid
	emsro	emsrw	emsmtc	emsspro	emsadmin	root
Password Change	deny	deny	deny	deny	allow	allow
Password encryption	deny	deny	deny	deny	deny	deny
Query Historical Alarms	allow	allow	deny	allow	allow	allow
Quick Start	deny	deny	deny	deny	deny	allow
Server administration	deny	allow	deny	allow	allow	allow
Service selection	allow	allow	deny	allow	allow	allow
Shelf view	allow	allow	deny	allow	allow	allow
Software download	deny	deny	allow	deny	allow	allow
Succession ATM Software Migration	deny	allow	deny	allow	allow	allow
Succession IP Software Migration	deny	allow	deny	allow	allow	allow
System log display	allow	allow	deny	allow	allow	allow
UNIX access	deny	deny	deny	deny	allow	allow
Note: MDP configuration and log viewer commands must be accessed using the MDP administrator userid maintained locally on the MDM workstation.						

IEMS group mappings for MDM Operator Client

Table 2 "IEMS user group mapping for MDM Operator Client tools" (page 678) shows the mapping between the IEMS groups and the tools available through the Operator Client application.

Table 2
IEMS user group mapping for MDM Operator Client tools

MDM Operator Client Resources	IEMS group				
	emsro	emsrw	emsmtc	emsspro	emsadmin
Fault					
Alarm Display	allow	allow	deny	allow	allow
Alarm Help	allow	allow	allow	allow	allow
Net Browser	allow	allow	deny	allow	allow
Network Status Bar	allow	allow	deny	allow	allow
Component Information Viewer	allow	allow	deny	allow	allow

MDM Operator Client Resources	IEMS group				
	emsro	emsrw	emsmtc	emssprov	emsadmin
Shelf View	allow	allow	deny	allow	allow
Configuration					
Nodal Provisioning	deny	deny	deny	allow	allow
Template editor	deny	deny	deny	deny	allow
Performance					
Data Viewer	deny	deny	deny	allow	allow
System Administration					
Service Selection	allow	allow	deny	allow	allow
Log Browser	allow	allow	deny	allow	allow
Security					
Change Password	deny	deny	deny	deny	deny
Utilities					
Operator Commands	deny	allow	deny	allow	allow
Command Console	deny	allow	deny	allow	allow
Telnet	deny	allow	deny	allow	allow
NTPs	allow	allow	allow	allow	allow

IEMS group mappings for MSS/MG15000 functionality

Table 3 "IEMS user group mapping for MSS/MG15000 access privileges" (page 679) shows the mapping between the IEMS groups and the MSS/MG15000 access privileges.

Table 3
IEMS user group mapping for MSS/MG15000 access privileges

MSS/MG15000 UserId attribute	IEMS group				
	mgro	mgrw	mgmtc	mgsprov	mgadmin
Command Scope	network	network	network	network	network
Command Impact	passive	service	configuration	sysadm	debug

680 Appendix A Mapping of Multiservice Data Manager, Multiservice Switch 15000 and Media Gateway 15000 access privileges to IEMS groups in VoIP networks

MSS/MG15000 UserId attribute	IEMS group				
	mgro	mgrw	mgmtc	mgsprov	mgadmin
Customer Identifier	0	0	0	0	0
Allowed Access	FMIP	FMIP	FMIP FTP	FMIP FTP Telnet	FMIP FTP Telnet Local
Allowed Out Access	no	no	no	no	yes
Login Directory	/	/	/	/	/
Time Out Protocol	enabled	enabled	enabled	enabled	enabled

Carrier VoIP

ATM/IP Solution-level Security and Administration

Copyright © 2006, Nortel Networks
All Rights Reserved.

Publication: NN10402-600
Document status: Standard
Document version: 04.04
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose it only to its employees with a need to know, and shall protect it, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.

