Release Notes

VPFM 2.0
Visualization Performance and Fault Manager

Document Number: **NN48014-400**

Document Version: **02.04**

Date: **June 2009**

NORTEL

Copyright © 2004–2009 Nortel Networks, All Rights Reserved

Trademarks

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

NØRTEL

Contents

Chapter 1
How to get help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

*   download software, documentation, and product bulletins
*   search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
*   sign up for automatic notification of new software and documentation for Nortel equipment
*   open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

http://www.nortel.com/callus

Getting Help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Chapter 2
Visualization Fault and Performance Manager

This chapter provides operational notes for the Visualization Performance and Fault Manager 2.0 release.

The purpose of this document is to describe specific situations in which the VPFM can experience difficulties, and to provide work-around solutions to mitigate the issue, or minimize the possibility of it occurring. Topics in this document include:

- "Operational notes" on page 7
- "Limitations" on page 7

Operational notes

This section provides operational notes for the VPFM 2.0 release.

Installation

When you install VPFM 2.0, you must uninstall any previous installation of VPFM before you begin.

Limitations

The following table lists the limitations for VPFM 2.0.

Table 1   Limitations

CR number	Description
Q01920599	Sometimes when there is no traffic between Alteon switches, the links between them may not get discovered.
Q01928829	Under certain circumstances, links do not appear with the BCM 222 after performing a network discovery.
Q01957639	For ERS 8600, the message and summary information are not correct for the following traps: mplsXCUp mplsXCDown are not correct
Q01957940	Some IP phones do not get discovered as IP phones, even if they are registered with the Signaling Server. They sometimes are discovered as end nodes instead.
Q01964662	When doing a rediscovery on campuses consisting of Secure Routers connected by Frame Relay WAN links, one of the Secure Routers is not visible. Prior to the rediscovery, all routers were discovered. Discovery constraints employed are WAN, VPN crawl, and DNS lookup.

Table 1   Limitations

CR number	Description
Q01970740	Links between Managed Hosts and switches are not discovered under these circumstances: If Router's ARP cache does not provide the MAC address of the host or it is not found until after the device is discovered, it won't be associated with the device early enough to do the linking.
Q01994165	For ERS 8600, the following trends are not available: mplsTunnelConfigured mplsTunnelActive
Q02019344	Event correlation is not available for the following traps in the ERS8600 device: rcnMsdpEstablished rcnMsdpBackwardTransition traceRoutePathChange traceRouteTestFailed traceRouteTestCompleted msdpEstablished msdpBackwardTransition
Q02028096	Garbage characters on the Menu Tree (Network Browser: Layer 2 perspective) for CES-1100 Device family.
Q02028782	Invalid Trend "Percent IO Memory Uses" appears as an option for the following Device Families: ERS 1600 ERS 8300 ERS 8600 WSS NAS
Q02030584	On a Windows 2008 platform, if the VPFM server receives traps at a rate of 300traps/sec or more, the VPFM service might hang. **Workaround:** Restart the Nortel VPFM service.
Q02034465	When uninstalling a VPFM primary server it doesn't warn the user about the credentials and license services that are also uninstalled; this can cause a distributed solution not to work anymore.
Q0203453	For ES 325-425 and ERS 4500 the following trend does not work: s5EnMsTopNmmCurNum
Q02037371	Some Nortel Call Pilots are discovered as End Nodes.
Q02039380	When pointing to CS1K installed as primary UCM server, VPFM link is not created under the Navigation Tree of the UCM Home Page.
Q02039567	Under certain circumstances, links do not appear with Cisco and Nortel devices, after performing a network discovery.
Q02039971	There is no Help button for Monitoring Overrides. **Workaround:** Refer to the VPFM Configuration guide (NN48014-500)

Chapter 3
UCM Common Services

This guide lists the release notes associated with the UCM Common Services.

This chapter provides the following information:

Operational notes

This section provides operational notes for the UCM Common Services. It provides information on the following topics:

Installation

- English is the only language supported.

- Installation locations of the product and common services are greyed out. They can only be changed by clicking the 'Choose' button.

- If MySQL is already existing in the system and running, it needs to be stopped so that the Nortel UCM MySQL can be installed.

- Ports in the 1-1023 range (other than 80 and 443 for HTTP/HTTPS) should not be used. These are TCP/UDP ports that are used by a variety of applications : FTP (20,21), Telnet 23, SNMP 161 and so on. Choosing them may result in applications not working and other conflicts.

- Information about type of server:

— Primary Security Server - Security Administration is installed.

— Member Security Server - Security Administration not installed, redirected to primary server.

— Backup Security Server - Takes over the function of primary in case of primary server failure.

— Central Server - Device Credentials and License Module are installed.

• Check the host file entries on Linux (/etc/hosts) and Windows (C:\Windows\System32\Drivers\etc\hosts). Correct format of Fully-Qualified Domain Name (FQDN):

127.0.0.1   localhost
102.54.94.97   rhino.acme.com   rhino

Note: The value of FQDN mapped in hosts file will appear as default on Windows, and if it is DNS resolvable, also on Linux. Otherwise, the FQDN will have to be inserted manually. When multiple networks interfaces are active, the FQDN must be inserted manually. An eventual default value is not guaranteed to be the desired one. In member or backup mode installation, the hosts file should have entry for primary server. In non-central mode installation, the hosts file should have entry for central server.

• Add the server IPs(primary/member/backup) to hosts file on Linux (/etc/hosts) and Windows (C:\Windows\System32\Drivers\etc\hosts).

• High availability is not supported for Device Credentials and Licensing modules. Single Sign-on supports high availability. If a server having Device Credentials and Licensing modules is down/uninstaller/removed all other nodes refering to the server will not have access to Device Credentials and Licensing modules.

• If a primary server is restarted backup and member servers also need to be restarted. Order of restart should be primary, backup, member.

• On IE7 after login if you see a blank page https://your-fqdn.com/securityserver/UI/blank . Got to Tools > Security > Click "Restore all zones to default level"

• FQDN needs to have minimum 2 dots.

• When pointing to a CS1k as primary:

a) The first product (EPM,NRM/VPFM/IPFM) pointing to CS1k primary needs to be a member. If its absolutely necessary to install the product in backup mode the destination xml files under JBOSS_HOMEserver\default\deploy-hasingleton\jms\clusteredDestinations need to be copied manually to the primary

b) Q02038117 : If there was/is any product(EPM,NRM/VPFM/IPFM) using CS1k as primary the CS1k jboss needs to be restarted before installing the new product.

Security

• The default SSO token timeout is 120 minutes, regardless of whether there are user activities or not on a session. Additionally, The default idle timeout is 30 minutes, this is affected by user activities.

- The Active Session list in quantum administration page will list all the sessions that are not logged out and are within the application timeout limit.
- Application certificate is the server-side certificate created at installation time and there is 'client.truststore' file corresponding to it (for client-side calls) in the UCM installation folder. At any time users should not change the application's default certificate. Trying to change the application certificate might break some of the security functionalities. (Q01917319)
- IE7 will warn about the Certificate as the product certificate is not verified by the third party certificate authority(CA). User can avoid this warning by changing the IE setting in the advanced tab(Q01921773).
- Firefox issue: Some times we see a error in firefox "Your certificate contains the same serial number as another certificate issued by the certificate authority. Please get a new certificate containing a unique serial number. (Error code: sec_error_reused_issuer_and_serial)" This happens when the browser is not clearing the cached certificates. Closing the browser might not help. Kill the firefox process and restart the browser. To get the process id "ps -ef | grep firefox" .
- Registration of member/backup to primary is automated. But deregistration after a member/ backup is uninstall is manual. User need to remove the uninstalled member/backup from the elements table via the Security Administration screens.
- When using localhost or IP address in the browser address bar to access UCM page, user will be taken to a login page with a link 'Go to central login for Single Sign-On', clicking the link will switch the url in the address bar to FQDN. Note: Always use FQDN to access UCM page, single-sign-on is only supported on FQDN.

Backup and restore

- Backup and restore can only be run by users in 'Administrators' group (in Windows) or 'root' group (in Linux).
- Stopping backup or restore in the middle of the process (for example by pressing Ctrl-C) is not a supported scenario. The database and system state wont be guaranteed to be stable if this is done. To reduce possibility of users doing this, a warning message will be displayed at the beginning of backup and restore process.
- Restore of users and roles is not supported.
- Restoring will only append the backed up data to the database. Any updates/changes between Backup Restore operation will remain.
- Restoring Device Credentials will replace existing data.

Device and server credentials

- Spaces are not allowed in the device credential ranges.

License

- A known drawback of MacroVision license is that for the Linux platform the user can only use the MAC address associated with the eth0 interface of the server. MAC addresses associated with any other interface would deem the application unlicensed.

- Q02038117 : Export functionality: Selecting multiple rows of same product name might cause unexpected error. By selecting a product row, application exports all the licenses of the product name on all the connected UCM hosts(primary/member/backup).

User interface

- The login warning banner contains "[company name]" instead of a value.To modify it, go to Security Administration -> Security -> Policies. Then click on "Edit" for Security Settings. See ECC-318

Known issues

The following table lists the known issues and workarounds for UCM Common Services.

Table 2   Known issues and workarounds

Issue	Description
IPv6	Problem observed when starting JBoss on Linux. At startup, JBoss is trying to bind an IPv6 IP and it fails. The result is that JBoss is not correctly started.
	This is happening due to a known bug from JDK 1.5 that was solved in JDK 6. Here is the JIRA issue for this problem:
	http://jira.jboss.com/jira/browse/JGRP-47
	Workaround: Add the following option in JBoss startup script (until the switch to JDK 1.6):
	Djava.net.preferIPv4Stack=true
	See the JBoss wiki for more information about this issue, at the following location:
	http://wiki.jboss.org/wiki/IPv6
	This issue and workaround only apply to hybrid boxes (having both IPv4 and IPv6 support). There is no workaround for pure IPv6 boxes.

Limitations

The following table lists the limitations for UCM Common Services.

Table 3   Limitations

CR Number	Description
Q02038860	Cannot add a IPv6 Address Range in Device and Server Credentials.