EMC® Smarts®
IP Availability Manager Extension for NAS

7.0

User's Guide

300-004-106
A01

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Copyright © 2005–2006 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com

All other trademarks used herein are the property of their respective owners.

Contents

Preface v

Chapter 1 Introduction

An introduction to network-attached storage 1-2
Overview of the IP Availability Manager Extension for NAS 1-2
EMC Celerra devices 1-3
NetApps filer 1-4
EMC Smarts IP NAS Solution Architecture 1-5
Monitoring and analysis 1-6
Monitoring 1-6
Analysis 1-6
Notifications 1-6
Impacts 1-7

Chapter 2 Installation and Startup

Overview 2-2
Map display functionality for NAS devices 2-2
Installing and Starting the HTTPS Adapter Service 2-3

Chapter 3 Discovery of NAS Devices

NAS IP discovery features 3-2
ICMP and SNMP probes 3-2
HTTPS/XML discovery probe 3-2
NAS post processing 3-2
Configuring Celerra devices for NAS Extension functionality 3-3
Configuring Control Station and Data Mover IP addresses 3-3
Configuring Control Station user names and passwords 3-3
Configuring IP Availability Manager for NAS autodiscovery 3-4

Chapter 4 NAS IP Elements

Overview 4-2
NASChassis 4-3
Host 4-3
FileServer 4-3
Attributes for FileServer 4-3

Chapter 5 NAS Failure Scenarios

Scenario 1: External IP network cable linking to NAS device fails 5-2
Scenario 2: Connectivity loss on the Control Station external interface 5-3
Scenario 3: Network Server fails due to a power supply failure 5-4

Chapter 6 Viewing NAS Notifications, Maps, and Containment

Viewing NAS notifications 6-2
Opening a notification properties dialog box 6-2
NAS device notification properties 6-2
Viewing NAS service topology in maps 6-3
Opening a topology map 6-3
NAS device topology map graphical representations 6-3
NAS device map types 6-4
Viewing NAS containment 6-8
Opening a NAS device containment dialog 6-8
NAS containment dialog 6-8

Appendix A Glossary and Terminology Matrix

EMC Smarts glossary A-2
Terminology matrix A-5

Appendix B Certified NAS Devices

Appendix C Availability Manager Notifications

Default subscribed events C-2
Notifications generated C-4

Index i-1

Preface

This document provides detailed information about the EMC Smarts IP Availability Manager Extension for NAS (NAS Extension). With the NAS Extension, IP Availability Manager (Availability Manager) discovers, monitors and diagnoses IP connectivity problems that occur with network-attached storage (NAS) devices. IP Availability Manager is a component of the EMC Smarts IP Management Suite.

With the NAS Extension, IP Availability Manager discovers and models network-attached storage devices as IP devices. Supported systems include EMC Celerra systems, and Network Appliance (NetApp) systems. IP Availability Manager Extension for NAS establishes relationships between these storage components and IP network components, identifies IP-related failures, diagnoses root cause problems, and calculates impacts of failures of both the NAS components and the IP network components.

Intended Audience

This document is intended to be read by operators of data centers and network operations centers monitoring the relevant IP networks, and administrators of storage devices, applications, databases, and networks.

Prerequisites

Before performing the procedures in this document, install EMC Smarts 7.0 IP Availability Manager and the EMC Smarts 7.0 Service Assurance Manager.

For more information, see the *EMC Smarts IP Management Suite Installation Guide*, the *EMC Smarts IP Management Suite Migration Guide*, and the *EMC Smarts Service Assurance Management Suite Installation Guide*.

Note: To support NAS Extension management functionality, the Celerra Control Station must support XHMP service and have HTTPS enabled. (See "Installing and Starting the HTTPS Adapter Service" on page 2-3.)

EMC Smarts IP Management Suite installation directory

In this document, the term BASEDIR represents the location where EMC Smarts software is installed.

- For UNIX, this location is: /opt/InCharge*<n>*/*<productsuite>*.
- For Windows, this location is: C:\InCharge*<n>**<productsuite>*.

The <n> represents the EMC Smarts software platform version number. The <productsuite> represents the EMC Smarts product suite to which the product

belongs. For example, on UNIX operating systems, EMC Smarts IP Availability Manager is, by default, installed to: /opt/InCharge7/IP/smarts. On Windows operating systems, this product is, by default, installed to: C:\InCharge7\IP\smarts. This location is referred to as BASEDIR/smarts.

Optionally, you can specify the root of BASEDIR to be something other than /opt/InCharge7 (on UNIX) or C:\InCharge7 (on Windows), but you cannot change the <productsuite> location under the root directory.

For more information about the directory structure of EMC Smarts software, refer to the *EMC Smarts System Administration Guide*.

EMC Smarts IP Management Suite products

The EMC Smarts IP Management Suite includes the following products:

- EMC Smarts IP Availability Manager
- EMC Smarts IP Discovery Manager
- EMC Smarts IP Performance Manager
- EMC Smarts IP Server Performance Manager
- EMC Smarts Adapter for HP OpenView NNM
- EMC Smarts Adapter for IBM/Tivoli NetView

Related documentation

In addition to this document, EMC Corporation provides a Help system for command line programs as well as product documentation.

Help for command line programs

Descriptions of command line programs are available as HTML pages. The index.html file, which provides an index to the various commands, is located in the BASEDIR/smarts/doc/html/usage directory.

EMC Smarts documentation

Readers of this guide may find the following related documentation helpful. It can be found in the BASEDIR/smarts/doc/pdf directory.

Note: These documents are updated periodically. Electronic versions of the updated manuals are available on the Powerlink website: `http://Powerlink.EMC.com`.

- *EMC Smarts Documentation Catalog*
- *EMC Smarts System Administration Guide*
- *EMC Smarts ICIM Reference*
- *EMC Smarts Common Information Model Infrastructure Models Chart*
- *EMC Smarts Common Information Model Application/Business Models Chart*
- *EMC Smarts ASL Reference Guide*
- *EMC Smarts Perl Reference Guide*
- *EMC Smarts Dynamic Modeling Tutorial*
- *EMC Smarts MODEL Reference Guide*

EMC Smarts IP Management Suite documentation

The following EMC Smarts documents are relevant to users of the IP Management product suite:

- *EMC Smarts IP Management Suite Installation Guide*
- *EMC Smarts IP Management Suite Deployment Guide*
- *EMC Smarts IP Management Suite Configuration Guide*
- *EMC Smarts IP Management Suite Discovery Guide*
- *EMC Smarts IP Availability Manager User's Guide*
- *EMC Smarts IP Performance Manager and Server Performance Manager User's Guide*
- *EMC Smarts IP Adapters User's Guide*
- *EMC Smarts IP Availability Manager Extension for IPv6 User's Guide*
- *EMC Smarts IP Availability Manager Extension for NAS User's Guide*
- *EMC Smarts Quick Start Guide*

Refer to the *EMC Smarts Documentation Catalog* for documentation resources provided with other EMC Smarts product suites.

Suggestions for searching PDF files

You may search across multiple PDF files using the Adobe Acrobat Reader software.

1. If the documentation is not accessible to all users of the EMC Smarts product suite, copy the contents of the *BASEDIR/smarts/doc/pdf d*irectory to a central location, such as a shared drive on your LAN, that operators and others may view.
2. To search throughout the documentation library, open the Acrobat Reader software.
   1. Choose **Edit** > **Search**, and enter a word or phrase.
   2. In the **Where would you like to search** option, select **All PDF Documents in** and type the pathname of the location where the PDF documents reside.

If you have more than one EMC Smarts product suite installed, you can set up cross-product document searches by copying files from the BASEDIR/smarts/doc/pdf directory for each product suite into this common documentation directory path.

Conventions used in this guide

EMC uses the following conventions for notes and cautions.

Note: A note presents information that is important, but not hazard-related.

IMPORTANT

An important notice contains information essential to the operation of the software.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

Typographical conventions

EMC uses the following conventions in this guide:

Normal font	In running text: • Interface elements (for example, button names, dialog box names) outside of procedures • Items that the user selects outside of procedures • Java classes and interface names • Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, filenames, functions, menu names, utilities • Pathnames, URLs, filenames, directory names, computer names, links, groups, service keys, file systems, environment variables (for example, command line and text), notifications
Bold	In procedures: • Names of dialog boxes, buttons, icons, menus, fields, and maps • Selections from the user interface, including menu items, and field entries • Key names • Window names • Code examples • Commands • User interface tabs
Italic	Used for: • Full publications titles referenced in text In procedures: • Directory paths • Filenames • Scripts • Important/unique words • URLs • Utilities • Variables
`Courier`	Used for: • System output • User entry
< >	Angle brackets used to enclose parameter or variable values supplied by the user.
[ ]	Square brackets used to indicate optional values.
|	Vertical bar used to indicate alternate selections. The bar means “or”.
{ }	Braces used to indicate content that you must specify (that is, x or y or z).
...	Ellipses used to indicate nonessential information omitted from the example.
%	Used to indicate a C shell prompt.
#	Used to indicate a C shell superuser prompt.
▼▲	Used to indicate a command is wrapped over one or more lines. The command must be typed as one line.

Pathname conventions

Directory pathnames are shown with forward slashes (/). Users of the Windows operating systems should substitute back slashes (\) for forward slashes.

Graphical conventions

If there are figures illustrating consoles in this document, they represent the consoles as they appear in Windows. Under UNIX, the consoles appear with slight differences.

For example, in views that display items in a tree hierarchy such as the Topology Browser, a plus sign displays for Windows and an open circle displays for UNIX.

Smarts Manager

Unless otherwise specified, the term Smarts Manager is used to refer to EMC Smarts programs such as Domain Managers, Global Managers, and adapters.

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information — For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Powerlink™ website (registration required) at:

http://Powerlink.EMC.com

Technical support — For technical support, go to EMC Customer Service on Powerlink. To open a service request through Powerlink, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Sales and customer service contacts — For the list of EMC sales locations, please access the EMC home page at:

http://EMC.com/contact

1

Introduction

This chapter introduces the basic hardware and software components of the EMC Smarts IP Availability Manager Extension for NAS. It consists of the following sections:

- An introduction to network-attached storage 1-2
- EMC Celerra devices 1-3
- EMC Smarts IP NAS Solution Architecture 1-5
- Monitoring and analysis 1-6

An introduction to network-attached storage

Network-attached storage along with storage area networks (SANs) are increasingly important as enterprise storage solutions. SANs are optimized for high-volume block-oriented data transfers, while NAS provides storage services for applications that access data at the file level. Network-attached storage systems include centrally managed servers and an operating system that is optimized for fast file access and heterogeneous file sharing over an IP network.

NAS provides facilities for high availability, rapid recovery, data protection, ease-of-management and data backup and recovery. NAS is typically implemented for messaging, development applications, business and regulatory compliance, and general file sharing. NAS is flexible and extensible, allowing for the addition of storage devices to a network, as needed.

A NAS system includes a network server, file servers, and software for configuring and mapping file locations to the network-attached devices. Each NAS device is attached to a local area network (typically, an Ethernet network) and assigned an IP address. The storage system may be a separate backend system connected either logically or physically to the NAS system.

Overview of the IP Availability Manager Extension for NAS

The EMC Smarts IP Availability Manager Extension for NAS (NAS Extension) is applied to an existing IP Availability Manager installation. With the NAS Extension, the Availability Manager discovers and models network-attached storage devices as IP devices. Supported systems include EMC Celerra systems (Data Movers and Control Stations), and Network Appliance (NetApp) Filers.

The Availability Manager uses Codebook Correlation Technology to establish relationships between the IP components of the NAS systems and other IP network components in the environment. The Availability Manager with the NAS Extension identifies IP-related failures, diagnoses root cause problems, and calculates the impacts of failures.

To discover and monitor the NAS topology, the Availability Manager reads configuration information within the Celerra Network Server using the HTTPS Adapter, an XML/HTTPS discovery probe. The EMC Smarts Global Console displays the topology, notifications and maps related to both the IP and NAS elements.

The NAS Extension is implemented through the EMC Smarts IP Availability Manager and Service Assurance Manager.

EMC Celerra devices

A Celerra installation includes the following IP-related devices, as shown in Figure 1-1:

- Celerra Network Server
- Celerra Control Station.
- Celerra Data Movers

Figure 1-1 shows these relationships.

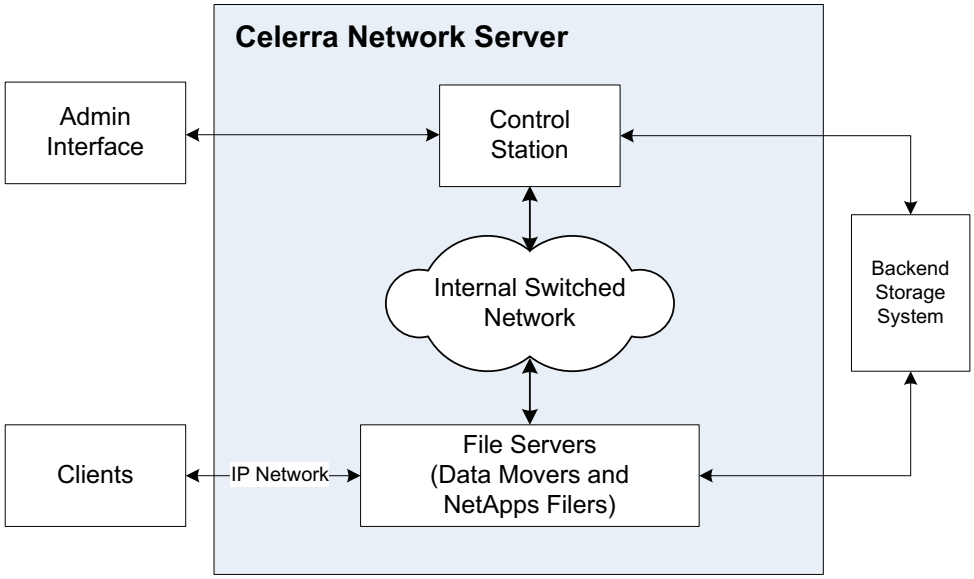

Figure 1-1 NAS Device Relationships

The Control Station includes an IP address that is exposed on the external network. The Data Movers also have IP addresses for external client connectivity.

The Data Movers and Control Station communicate with each other using Ethernet connections over the following supported file access protocols: CIFS, NFS, FTP, TFTP. The Availability Manager does not currently discover or monitor the internal network or the backend storage systems.

Celerra Network Server

The Network Server (not a physical device), is represented by the NASChassis class. A NASChassis is a cabinet that holds one or more Data Movers and one or more Control Stations.

Celerra Control Station

The Control Station, represented by the Host class, is a dedicated management computer that monitors and controls cabinet components and allows access to the full functionality of the Celerra Network Server software. It contains utilities for installing and configuring the Celerra Network Server, maintaining the system, and monitoring system performance. The Control Station runs a set of programs that are collectively referred to as the Control Station software, and an EMC-customized version of Linux as its operating system. The Control Station provides the Celerra Manager, a web interface for Celerra administration.

Celerra Data Mover

The Data Movers, represented by the FileServer class, are the Celerra components that transfer data between the storage system and the network client. A Celerra Network Server can have from 1 to 14 Data Movers.The Data Movers are managed via the Control Station.

A Data Mover can be active (also called primary) or, in a Celerra Network Server model that supports multiple Data Movers, can be a standby for other Data Movers.

Each Data Mover is independent; there is no communication between Data Movers. If a Data Mover fails, the Control Station manages the failover to the standby Data Mover, assuming a standby has been configured.

A Data Mover and the Control Station communicate with each other using both Ethernet and serial connections. A Data Mover communicates with the network using network interface cards (NICs) which may support 10/100/1000Base-T Ethernet or optical Gigabit Ethernet.

A Data Mover communicates with the backend data storage systems using Fibre Channel connections. In the Celerra Clustered Network Server, storage processing is provided by a component of the Data Mover, a Fibre Channel HBA card, that connects to the storage array through a Fibre Channel switch. In the Celerra NS series, storage processing is provided by an auxiliary storage processor enclosure containing two storage processors.

NetApps filer

NetApp filers, also represented by the FileServer class, are the NetApps storage systems. These devices combine file system technology with a proprietary operating system that provides for management as well as optimized storage utilization.

EMC Smarts IP NAS Solution Architecture

The IP NAS solution architecture consists of the following components:

- IP Availability Manager---A Domain Manager that discovers, monitors and analyzes failures in the underlying IP network. With the NAS Extension applied, the Availability Manager discovers and monitors NAS devices, correlates events, diagnoses root-cause problems, and calculates impacts.
- Global Manager---Abstracts and consolidates information from the Domain Managers and de-duplicates notifications.
- Global Console---Provides display capability for notifications, maps, and other graphical information.

Figure 1-2 shows the components and the flow of information for the managed NAS architecture.

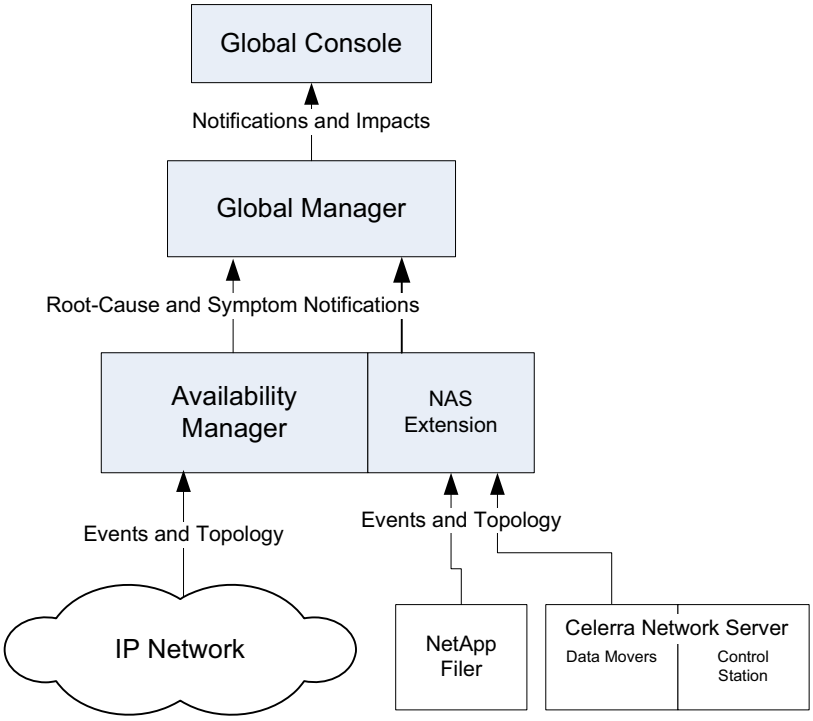

Figure 1-2 Managed NAS Architecture

Monitoring and analysis

Monitoring

To discover the IP configuration of a NAS device, the Availability Manager uses the HTTPS Adapter, which is a process contained within the NAS Extension. This XML-based probe associates the Data Movers with the Network Server via the Control Station.

After the initial discovery of the NAS IP elements, the Availability Manager continuously monitors the status of these elements by periodically sending ICMP and SNMP polls to the IP devices. For more information, see "Discovery of NAS Devices" on page 3-1. For more information about the full IP discovery process, see the *EMC Smarts IP Management Suite Discovery Guide*.

Analysis

The Availability Manager correlates root cause failures in the underlying IP transport network to problems in the NAS IP elements. For example, the Availability Manager indicates the NAS IP elements that have been impaired or impacted by the failure of a router in the IP transport network.

Notifications

The Availability Manager reports its analysis results to the Global Manager in the following types of notifications: root-cause problem notifications, symptomatic event notifications, and aggregate event notifications.

- Root-cause problem notifications indicate root-cause failures diagnosed by the Availability Manager. Each root-cause problem pinpoints the exact cause of a failure and identifies the managed element where the failure occurred.
- Symptomatic event notifications indicate symptomatic events detected by the Availability Manager. Symptomatic event notifications can also notify events that are not necessarily used for problem analysis but may be of interest to administrators or operators.
- Aggregate event notifications, also known as exceptions, identify high-level elements (such as switches) that are affected by one or more alarms. In an aggregate notification, the alarms for the element may be root-cause problems, symptomatic events, or a combination of root-cause problems and symptomatic events.

Relevant notifications are displayed in the Notification Log Console view of the Global Console. Root-cause failures diagnosed by the Availability Manager display a value of "Yes" for the value of the IsRoot attribute and identify the Availability Manager by its domain name in the Source attribute. Users can double-click a notification to view detailed information about the notification.

For more information, see "NAS IP Elements" on page 4-1. For information about viewing the notifications, see the *EMC Smarts Service Assurance Manager Operator's Guide*.

Impacts

The Availability Manager calculates the Impacts that failures of one managed element may have on other managed elements. Impact information is included in notifications.

2

Installation and Startup

This chapter covers installation and startup issues for the EMC Smarts IP Availability Manager Extension for NAS. Topics in this chapter are:

- Overview 2-2
- Installing and Starting the HTTPS Adapter Service 2-3

Overview

The NAS Extension is installed with the IP Availability Manager. After installation, the Availability Manager can discover NAS devices, and perform root cause and impact analysis on these devices.

Configuring the NAS extension involves the tasks summarized in Table 2-1.

Table 2-1 Steps for Configuring the NAS Extension

Procedure	For more information
If necessary, configure the HTTPS Adapter to support access to the managed Celerra devices.	For information about this requirement, see "Configuring Control Station user names and passwords" on page 3-3.
If necessary, configure external Control Station and Data Mover IP Addresses.	For information about this requirement, see *"Configuring Control Station and Data Mover IP addresses" on page 3-3*, which also refers you to the appropriate EMC documentation, if needed.
Install the HTTPS Adapter as a service and start the service.	"Installing and Starting the HTTPS Adapter Service" on page 2-3.
Start the Availability Manager.	*EMC Smarts IP Management Suite Installation Guide*
Start the Global Manager.	*EMC Smarts Service Assurance Management Suite Installation Guide*. For configuration information, see the *EMC Smarts System Administration Guide*.
Start the Global Console.	*EMC Smarts Service Assurance Management Suite Installation Guide*.

Map display functionality for NAS devices

Service Assurance Manager (SAM) 7.0 installs an enhancement to the map display functionality to show NAS devices.

Installing and Starting the HTTPS Adapter Service

The NAS Extension software includes an adapter process (the HTTPS Adapter), which probes the Celerra devices using the HTTPS/XML probe to obtain internal topology information. While the installation of this adapter is automatic, you must install the service and start it manually. Install the HTTPS Adapter as a service and start the service manually, as described below for UNIX and Windows.

Once started, the HTTPS Adapter registers with the EMC Smarts Broker. For more information about starting services, see the *EMC Smarts System Administration Guide*.

UNIX:
To install the HTTPS Adapter as a service on UNIX, issue the following command:

```
# sm_service install --force --unmanaged --startmode=manual \
'--name=<service_name>' \
'--description=<SMARTS description>' \
'BASEDIR/smarts/bin/sm_adapter_java'
'--name=<HTTPS_Adapter_Name>' \
'--output=<HTTPS_Adapter_Name>.log' \
'-J' \
'nas_probe.jar'
```

where, *<service_name>* is the name registered to the service daemon; You may choose any name you wish for this name; for example, `ic-remote-nas`. When you issue the *sm_service show* command, this name displays.

<SMARTS description> is the description of the service. You may create any description you wish; for example, `SMARTS remote NAS adapter`.

<HTTPS_Adapter_Name> is the name of the HTTPS Adapter, as registered with the EMC Smarts Broker; for example, the default name is `remote-nas`.

You can also specify the Broker and Port, if the Availability Manager with NAS Extension is registered with a Broker and Port other than the default, `localhost:426`. To do this, add the following arguments to the end of the command:

```
--broker=<IP Address or Hostname>:<Port Number>
```

where, *<IP Address or Hostname>* identifies the host on which the Broker is running, and *<Port Number>* identifies which port is used by the Broker. Please note that a colon separates the hostname from the port.

To start the service, issue the following command:

```
# BASEDIR/smarts/bin/sm_service start <service_name>
```

To stop the service, issue the following command:

```
# BASEDIR/smarts/bin/sm_service stop <service_name>
```

WINDOWS:
To install the HTTPS Adapter as a service on Windows, issue the following command on one line:

```
▼sm_service install --force --name=<service_name>
   --description=<SMARTS description>
   --startmode=manual BASEDIR\smarts\bin\sm_adapter_java.exe
   "--name=<HTTPS_Adapter_Name>"
   "--output=<HTTPS_Adapter_Name>.log" "--jar=nas_probe.jar" ▲
```

where, *<service_name>* is the name registered to the service registry; this name must be unique to the registry. You may choose any name you wish for this name so long

as the name has no white spaces. The following is an example, `ic-remote-nas`. When you issue the `sm_service show` command, this name displays.

<SMARTS description> is the description of the service. You may create any description you wish but it is easier to find the service if all EMC Smarts services are grouped together. An example service description is `SMARTS remote NAS adapter`. Service names display alphabetically in the Name column of the Services window located at Control Panel/Administrative Tools, so the example description will follow SMARTS Performance Manager and precede SMARTS Service Assurance Manager.

<HTTPS_Adapter_Name> is the name of the HTTPS Adapter, as registered with the EMC Smarts Broker; for example, the default name is `remote-nas`.

You can also specify the Broker and Port, if the Availability Manager with NAS Extension is registered with a Broker and Port other than the default, `localhost:426`. To do this, add the following arguments to the end of the command:

```
--broker=<IP Address or Hostname>:<Port Number>
```

where, *<IP Address or Hostname>* identifies the host on which the Broker is running, and *<Port Number>* identifies which port is used by the Broker. Please note that a colon separates the hostname from the port.

To start the service, go to the Services window and select the service name, or issue the following command at a command prompt:

```
# BASEDIR\smarts\bin\sm_service start <service_name>
```

To stop the service, go to the Services window and select the service name, or issue the following command:

```
# BASEDIR\smarts\bin\sm_service stop <service_name>
```

3

Discovery of NAS Devices

This chapter describes specialized discovery and post-processing features for NAS IP elements. In addition, it explains how to configure user names and passwords for the HTTPS Adapter to use when accessing certain managed Celerra devices. It contains the following sections:

- NAS IP discovery features 3-2
- Configuring Celerra devices for NAS Extension functionality 3-3
- Configuring IP Availability Manager for NAS autodiscovery 3-4

For information about the IP discovery process in general, see the *EMC Smarts IP Management Suite Discovery Guide*.

NAS IP discovery features

The Availability Manager with the NAS Extension uses standard ICMP (Ping) and SNMP probes to determine device status and containment information. In addition, the NAS Extension uses an HTTPS Adapter to gather configuration information about Celerra Control Station devices, and some post-processing steps to complete the topology creation.

Note that the internal Celerra IP network (the IP network that supports communication between file servers and the control station hosts) is automatically excluded from discovery.

ICMP and SNMP probes

The ICMP probe determines whether a device is operational.

The SNMP probe uses the management, MIB-2, system information to determines the type of device. If the NAS Extension determines that the device is a Control Station, the Availability Manager launches the HTTPS Adapter probe. In addition, if the MIBs are included in the SNMP Agent of the device, the SNMP probe gathers containment information about the device's interfaces and IP address.

HTTPS/XML discovery probe

The HTTPS Adapter gathers information about Celerra devices that is unavailable through the Availability Manager SNMP probes. When the Availability Manager encounters a NAS device during discovery, it launches a probe that queries the Control Station for information such as the associated FileServers, software version, etc.

The HTTPS Adapter probe performs the following tasks:

- Instantiates NASChassis objects (NAS Network Servers)
- Associates FileServer objects (Celerra Data Movers) with the NASChassis object
- Associates Host objects (Control Stations) with the NASChassis object
- Assigns attributes such as software version to the FileServer and NASChassis objects

NAS post processing

Post-processing creates the NAS topology as follows:

- Sets the NASChassis object display name
- Sets the FileServer object display name
- Sets the Host (Control Station) object display name
- Deletes obsolete NASChassis, FileServer and Host (Control Station) objects

In addition, the Availability Manager establishes relationships between these components and the underlying IP network.

The NAS topology is stored in the Repository and displayed on the Global Console via the Topology Browser and various maps. For more information, see "Viewing NAS Notifications, Maps, and Containment" on page 6-1.

Configuring Celerra devices for NAS Extension functionality

To support NAS Extension functionality, you may need to configure the following:

- Control Station and Data Mover IP addresses
- Control Station user names and passwords

Configuring Control Station and Data Mover IP addresses

The IP Availability Manager Extension for NAS requires access to the Control Station and Data Mover IP addresses that are exposed on the external network. You configure the IP addresses after the devices are cabled to the network switches.

For information about cabling the Celerra Network Server, see the *Celerra NS500/NS600/NS700/NS704 Integrated Configuration Version 5.4 SETUP GUIDE, P/N 300-002-070 REV A02*. Refer to the Connect Cables section, step 5.

For information about how to configure the external IP addresses once the cables are in place, see the *Configuring and Managing Celerra Networking* and *Configuring and Managing Celerra Network High Availability* technical modules for more information.

Configuring Control Station user names and passwords

When using the HTTPS Adapter, the Availability Manager accesses each Celerra Control Station device. Some Control Station devices may restrict access to configured user names and passwords. If the default user name and password (*nasadmin*) are used, no configuration is required. For information about encryption and other security issues, see the "Securing Access to EMC Smarts Software" section of the *EMC Smarts System Administration Guide*.

Configuring device logins

To configure a login into the Celerra Control Station, issue the following line in the *clientConnect.conf* file:

```
nasUser:<device_id>:<login_id>:<password>
```

Where,

- *<device_id>* is either a device name or its IP address
- *<login_id>* is the user name; default user name is `nasadmin`
- *<password>* is the password; default password is `nasadmin`

Note: If an asterisk is used as a wildcard in the final entry of the first field before the nasUser section, that entry will become the default nasUser value. Thus, if you include asterisks in the *clientConnect.conf* file, you must move the *nasUser* section above these entries. This wildcard priority also holds true for definitions within the *nasUser* section; for example, if you configure logins for more than one Celerra Control Station device, ensure that the first login does not contain a wildcard. For more information on using wildcards, see the *EMC Smarts IP Management Suite Configuration Guide*.

Adding/removing/modifying logins

You can add/remove/modify these entries anytime using the *sm_edit* utility. In the next discovery process, the modified entries will be active. For more information, see the *EMC Smarts System Administration Guide*.

Configuring IP Availability Manager for NAS autodiscovery

Enable autodiscovery and create one or more discovery filters to discover the following types of devices in the managed storage environment:

- Host systems (HostSystems)
- Fibre Channel switches (FCSwitches)
- Celerra Control Stations (NAS_ControlStations)
- Celerra Data Movers (NAS_FileServers)
- NAS clients (NASClient_Hosts)

You create an IP-address discovery filter that has the specific values for your NAS devices in the first, second, and third octet positions, and an asterisk (wildcard character) in the fourth octet position; for example, *172.32.14.**.

The specific values limit the discovery filter to a specific network (in this example, network 172.32.14.0), and the asterisk allows Availability Manager to discover all candidate devices belonging to the 172.32.14.0 network. You create an IP-address discovery filter for each network that you want Availability Manager to sweep for candidate NAS devices.

See the *EMC Smarts IP Management Suite Discovery Guide* for details on creating filters.

4

NAS IP Elements

This chapter describes NAS IP elements and relationships that are specific to NAS IP discovery. It contains the following sections:

- Overview 4-2
- NASChassis 4-3
- Host 4-3
- FileServer 4-3

Overview

The Availability Manager builds a data model of the discovered NAS IP elements in the managed environment. The model represents the discovered elements as instances of the EMC Smarts ICIM classes.

The NAS IP elements are represented by instances of the following ICIM classes:

- NASChassis
- FileServer
- Host (Celerra Control Station)

During the discovery post-processing phase, the Availability Manager creates the relationships and connections between the storage objects: Celerra Data Mover (FileServer object), NAS Network Server (NASChassis object), and Celerra Control Station (Host object).

Note that, in addition, the Availability Manager discovers the Layer 2 and Layer 3 elements and relationships that are described in the *EMC Smarts IP Availability Manager User's Guide*; for example, Cable, Card, Interface.

For more information about the EMC Smarts ICIM classes and the discovery process, see the *EMC Smarts IP Management Suite Discovery Guide*.

NASChassis

A chassis is a physical package that encloses other elements; in this case, the enclosed elements are the Celerra Data Movers and Control Station.

NASChassis is instantiated for each Celerra Network Server (NASChassis object) found during the discovery process.

The NASChassis is related to the FileServer and Host objects through the PackagesSystems relationship. The NASChassis is also related to remote Control Station Host objects through the ConnectedTo relationship. The ConnectedTo relationship reflects inter-Celerra device communication.

Host

A host is a computer such as a workstation or server; in this case it represents the Celerra Control Station.

This class is used to instantiate the Celerra Control Station, which is the Celerra device management element. The Host class also exists in the Availability Manager.

A Host object is related to the NASChassis object through the PackagedIn relationship.

FileServer

A file server (Celerra Data Mover or NetApp Filer) is responsible for central storage and management of data files so that other computers can access the files. File server configurations can vary greatly, from a networked group of storage arrays that includes many disk drives to a virtual entity on a computer host. In a large Celerra network however, a file server may be included in a Celerra Network Server that contains a Control Station, or it might be associated with a remote Control Station on the same IP network, or with a Control Station on a network not monitored by EMC Smarts. There is no concept of Control Station with the NetApp Filer, which includes its own management software.

A FileServer object is related to the NASChassis object by the PackagedIn relationship, and to the IP network through the ConnectedVia relationship.

Attributes for FileServer

Table 4-1 lists key attributes for FileServer.

Table 4-1 Attributes for FileServer

Attribute	Description
InternalName	Unique name for this file server
InetAddr	IP address for accessing this file server
SoftwareVersion	Software version executing in this file server
Slot	Slot in the Chassis that packages this file server
Standby	Name of the file server backing up this file server

5

NAS Failure Scenarios

This chapter describes the following failure scenarios that illustrate Availability Manager functionality for the NAS IP environment:

- Scenario 1: External IP network cable linking to NAS device fails..... 5-2
- Scenario 2: Connectivity loss on the Control Station external interface..... 5-3
- Scenario 3: Network Server fails due to a power supply failure..... 5-4

Scenario 1: External IP network cable linking to NAS device fails

Figure 5-1 shows a scenario where the external connection to a file server fails because a cable is down (#1 in the figure). Because a file server may be equipped with a hot spare and failover may occur automatically, NAS functionality may not be affected. However, the operator needs to know that the cable has failed and which devices may have been affected.

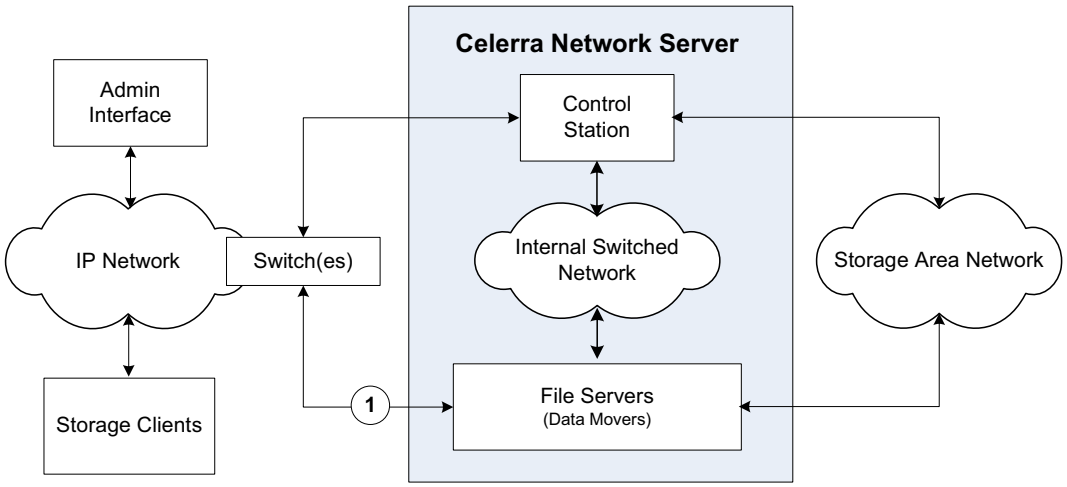

Figure 5-1 External Network Cable Failure to a File Server

In this case, the following notifications may be generated:

- Notifications: Cable Down, IP Network Switch Interface Down, FileServer Unresponsive (in the event that failover does not happen)
- Root Cause: Interface Down
- Impact: FileServer Down

Scenario 2: Connectivity loss on the Control Station external interface

When an external interface to the Control Station fails because of device failure or loss of connectivity to the IP network, the Control Station may fail over to another host. However, the operator needs to know that the interface has failed and which devices may have been affected.

Figure 5-2 shows a scenario where an external interface on the Control Station has failed (#2 in the figure).

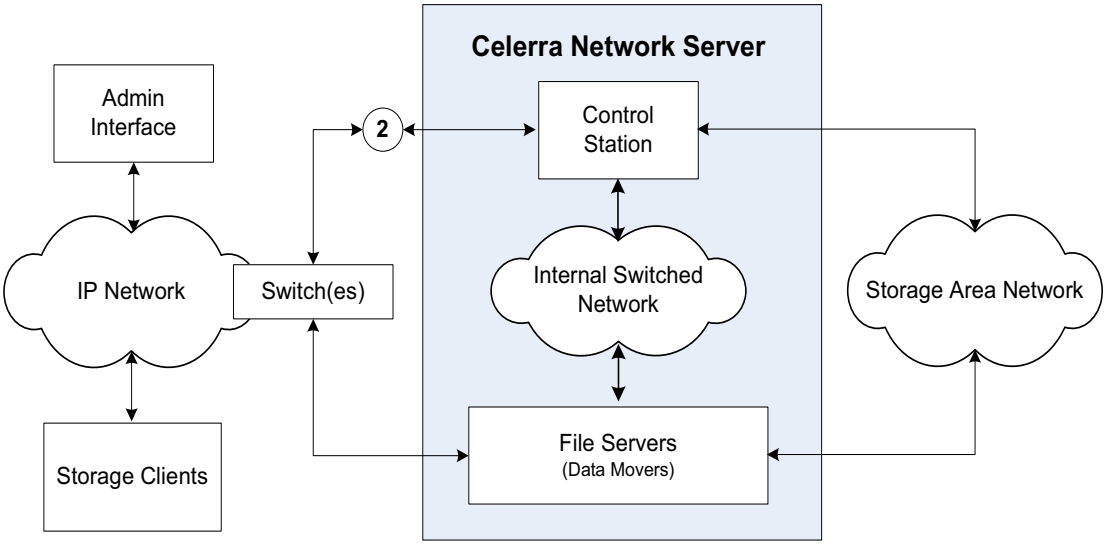

Figure 5-2 External Network Cable Failure to a Control Station

In this case, the following notifications are generated:

- Notifications: Host (Control Station) Unresponsive
- Root Cause: Interface Down
- Impact: Host (Control Station) Unresponsive

Scenario 3: Network Server fails due to a power supply failure

In the event that the power supply to the Network Server is interrupted, for example, because a circuit breaker is tripped, all of the systems packaged within the Network Server will fail.

Figure 5-3 shows a scenario where the Network Server is powered off (#3 in the figure).

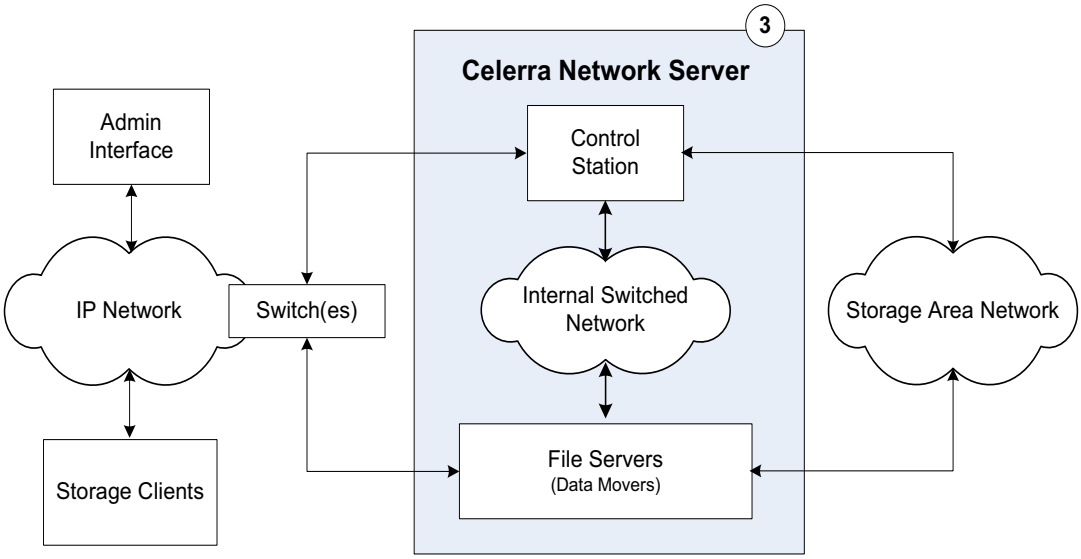

Figure 5-3 Power Failure on the Network Server

In this case, the following notifications are generated:

- Notifications: NASChassis Down, Host Unresponsive, FileServer Unresponsive
- Root Cause: NASChassis Down
- Impacts: FileServer Unresponsive, Host Unresponsive

6

Viewing NAS Notifications, Maps, and Containment

This chapter describes using the Global Console to view NAS IP device notifications, topology maps, and containment information for the NAS devices. It contains the following sections:

- Viewing NAS notifications 6-2
- Viewing NAS service topology in maps 6-3
- Viewing NAS containment 6-8

For general instructions on viewing notifications, maps, and containment information, see the *EMC Smarts Service Assurance Manager Operator's Guide*. For information about the NAS topology elements discovered and the events notified by the Availability Manager, see "NAS IP Elements" on page 4-1.

Viewing NAS notifications

You view the notifications, maps, and containment information by attaching the Global Console to the Global Manager. The Availability Manager reports NAS device notifications to the Global Manager. You can then view the notifications through the attached Global Console in two basic ways:

- As table entries in a Notification Log Console view
- As color-coded severity icons in a Map Console view

Opening a notification properties dialog box

To obtain detailed information about an individual NAS device notification, you can use any of the following common methods to open the Notification Properties dialog box:

- Double-click a NAS device notification in the Notification Log Console.
- Select a NAS device notification in the Notification Log Console and click the **Properties** toolbar button.
- Right-click a selected NAS device notification and select ***Properties*** in the pop-up menu.
- Double-click a NAS device map icon affected by active events.

NAS device notification properties

Figure 6-1 shows an example of the detailed information displayed in the Notification Properties dialog box for a FileServer Down notification.

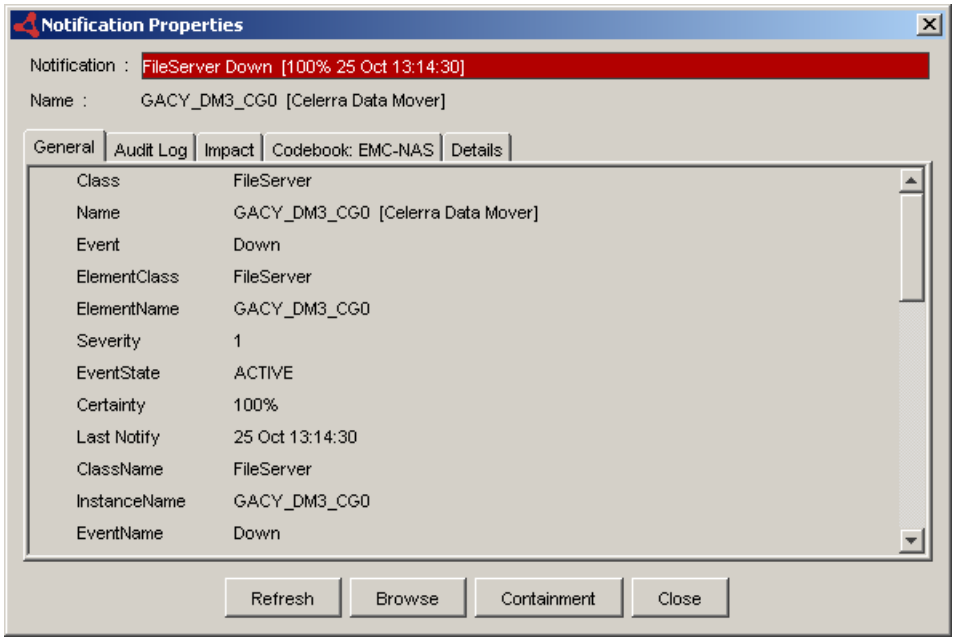

Figure 6-1 Notification Properties Dialog Box Showing FileServer Down

Viewing NAS service topology in maps

The Availability Manager sends NAS device topology—instances of the NASChassis, Host and FileServer classes—to the Global Manager along with the standard IP topology.

The Global Console presents the topology information in a variety of dynamically updated formats that show the status of the NAS device and network elements and their many relationships. One of those formats is the topology map, which is a graphical representation of the topology.

Viewing topology maps is an easy and quick way to learn more about the source, impact, and cause of NAS device notifications. You view the NAS device topology maps using the Map Console view of the Global Console.

Opening a topology map

You can use any of the following common methods to open a NAS device topology map:

- Open the Map Console by selecting the Show Map option from any opened console attached to the Global Manager. For example, in the Notification Log Console, click a NAS device notification and then select ***Event > Show Map***, or right-click the notification and then select ***Show Map*** in the pop-up menu. In the Topology Browser Console, right-click a NAS device element and select ***Show Map*** in the pop-up menu.
- Open the Map Console from the Global Console by selecting ***File > New > Map Console***. In the Topology tab of the Map Console, click NAS element to display a map for the element, or right-click the NAS element and select a map type from the pop-up menu.
- In an opened Topology map, right-click NAS device element map icon and select a map type from the pop-up menu.

Table 6-1 shows which maps are available for which NAS classes and their default map views.

Table 6-1 Storage Map Availability

	Storage Map Views			
Storage Class Name	**SAN Connectivity**	**NAS Connectivity**	**Physical Connectivity**	**Default Map View**
FileServer	X	X	X	Physical Connectivity
Host (NAS Control Station)	X		X	Physical Connectivity
NASChassis		X		NAS Connectivity

NAS device topology map graphical representations

NAS device Topology maps contain FileServer and Host (Control Station) elements, along with their relationships and connections. In a map display, a *node* is a graphical representation of an element, and an *edge* is a graphical representation of a relationship or connection between elements.

Table 6-2 identifies and describes the default node icon for FileServer that may appear in a NAS topology map. In the Map Console, you can also select ***Map > Map Legend*** to see a similar list.

Table 6-2 Default Node for NAS Device Topology Maps

Icon / Visual Indicator	Description
	FileServer, such as Celerra Data Mover or NetApp Filer

Note that your system administrator may replace the standard map nodes with other map nodes that are preferred by your organization. In that case, use ***Map > Map Legend*** to see the definitions of your map nodes.

For detailed information about maps, see the *EMC Smarts Service Assurance Manager Operator's Guide*.

NAS Connectivity Map

The NAS Connectivity map shows logical connectivity between NAS FileServer elements and NAS Host elements. No physical connectivity details are included in this map. See Figure 6-4 on page 6-7 for an example.

The initial layout of a NAS Connectivity map depends on the element that you select to launch the map. The edge marked with a + (plus) sign indicates that the edge can be expanded to show hidden MountPoints.

Selecting a NAS element results in an initial layout that centers around the selected element (also known as the map's focal object) and shows the relationships to all elements within one hop of the selected element. Expanding the expandable nodes and edges reveals additional relationships and elements and eventually ends in a fully expanded map.

NAS device map types

The following Availability Manager map types show NAS devices.

- Physical Connectivity
- IP Network Connectivity
- NAS Connectivity
- SAN Connectivity

Figure 6-2 shows a Physical Connectivity map for a NAS FileServer. In this map, the FileServer (123DM2NFS, a Celerra Data Mover) is displayed with a major alert.

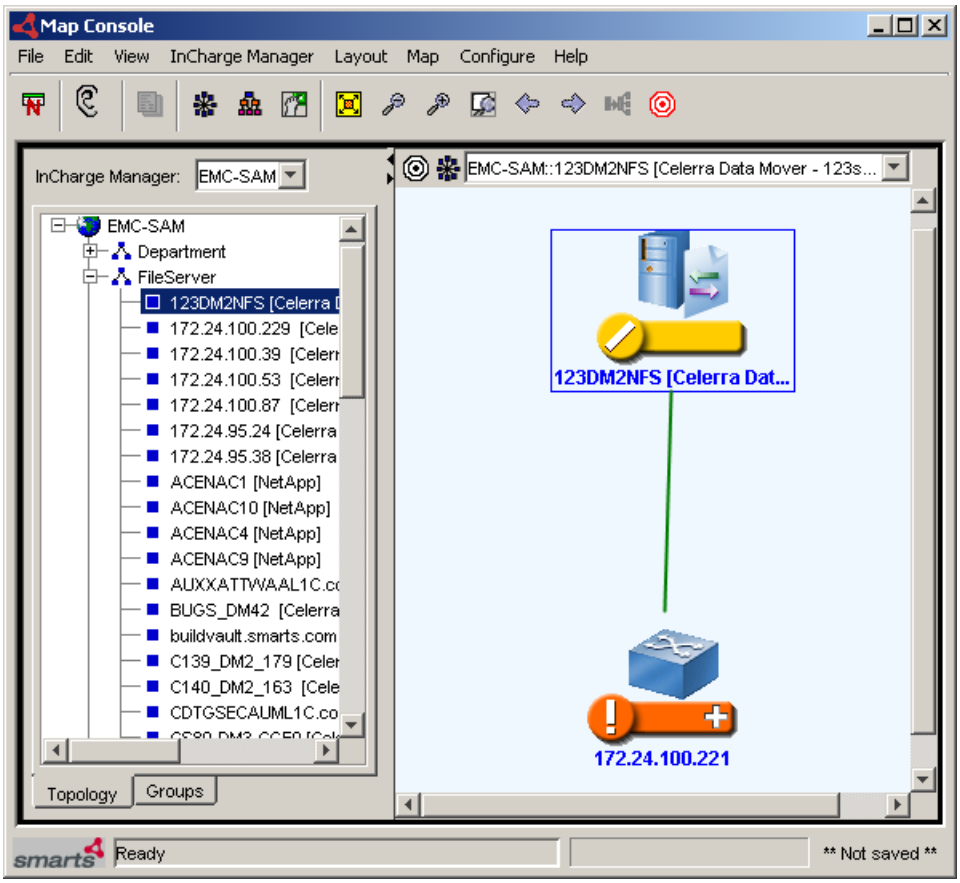

Figure 6-2 **Physical Connectivity Map with a NAS FileServer**

Figure 6-3 shows an IPNetwork Connectivity map with the same FileServer.

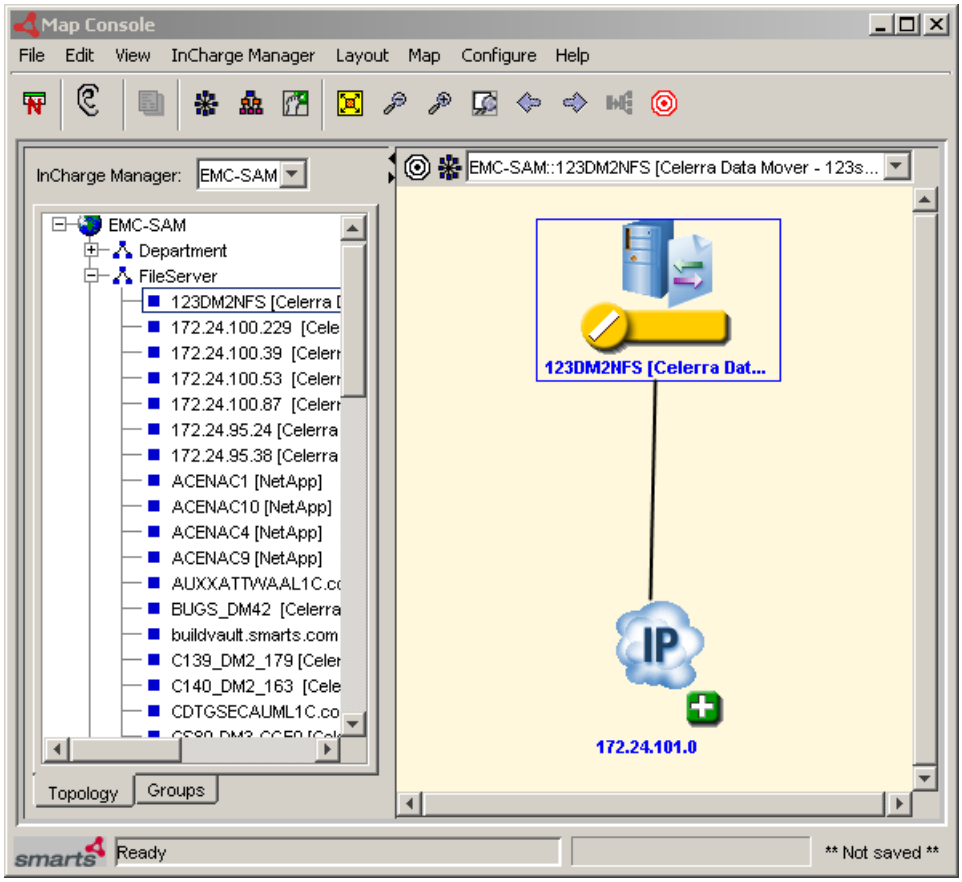

Figure 6-3 IP Network Connectivity Map with a NAS FileServer

Figure 6-4 shows an NAS Connectivity map with a FileServer named server_2.

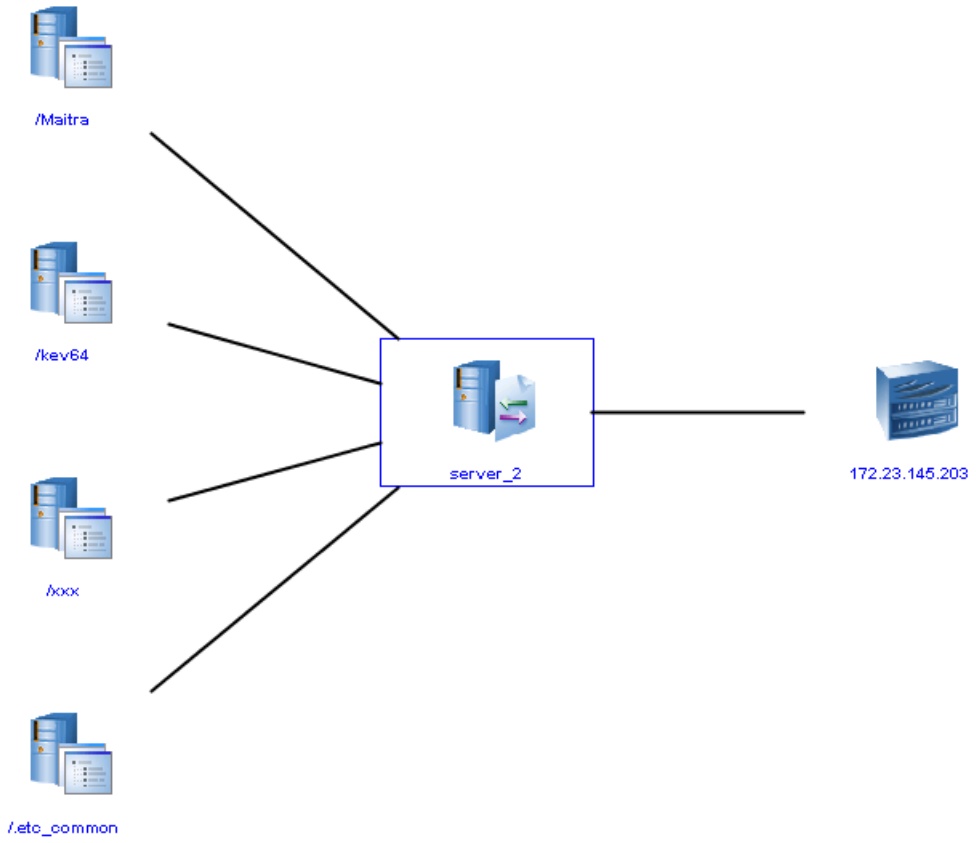

Figure 6-4 NAS Connectivity Map with a NAS FileServer

Figure 6-5 shows an SANConnectivity map with FileServer server_2.

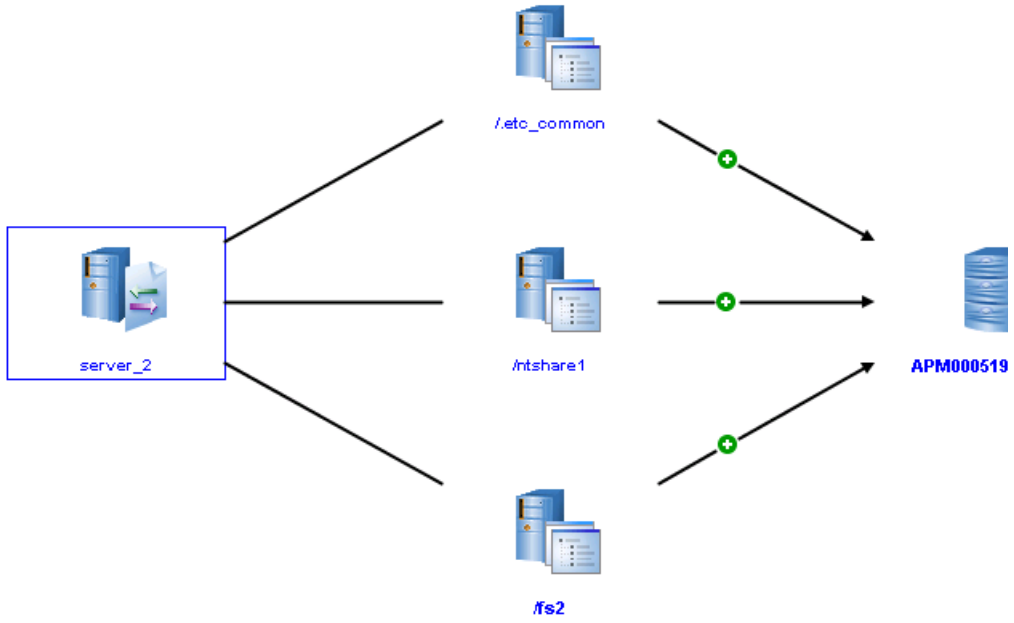

Figure 6-5 SAN Connectivity Map with a NAS FileServer

Viewing NAS containment

The Containment view shows topology information for each type of NAS element. An element's Containment view displays in a dialog box that organizes the information for the element into tab pages and tables.

In a Containment view, different information is available for different types of elements. The containment information is generated by the Availability Manager upon request by the Global Manager.

Opening a NAS device containment dialog

To obtain containment information about an individual NAS device element, you can use any of the following methods to open a Containment dialog for the element:

- In a NAS device map tree, right-click the element and select Containment in the pop-up menu.
- In a NAS device map display, right-click the element and select Containment in the pop-up menu.
- In a Topology Browser Console, right-click the element and select Containment in the pop-up menu.
- In a Notification Log Console, double-click a notification for the element and click the Containment button in the Notification Properties dialog.

NAS containment dialog

Figure 6-6 shows a Containment dialog box for a NASChassis element, showing the associated network cards, adapters, IP addresses, and other information.

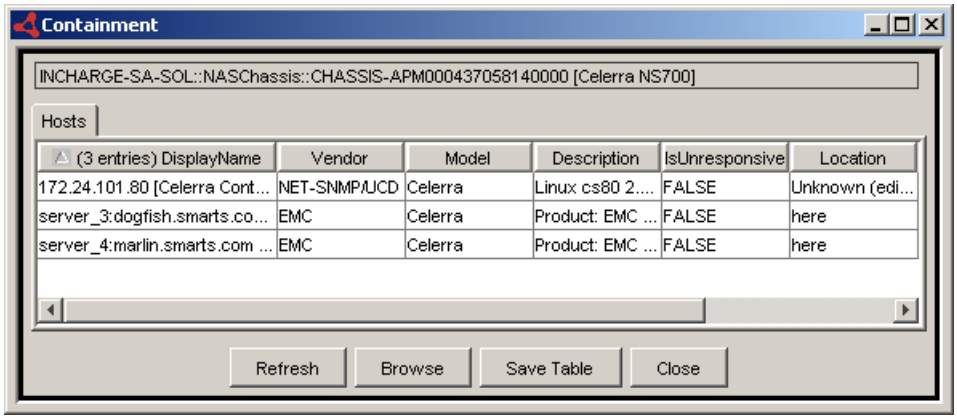

Figure 6-6 NASChassis Containment Dialog—Example

A

Glossary and Terminology Matrix

Some of the terminology used by EMC Smarts documentation may be unfamiliar to EMC Celerra Manager and ControlCenter users. "EMC Smarts glossary" contains EMC Smarts terms used in the IP Availability Manager for NAS Extension documentation. "Terminology matrix" contains a list of terms used in the EMC Smarts NAS Extension documents along with the comparable term for EMC NAS Element Management and/or EMC ControlCenter.

- EMC Smarts glossary A-2
- Terminology matrix A-5

EMC Smarts glossary

Table A-1 lists EMC Smarts terms used in the IP Availability Manager for NAS Extension documentation

Table A-1 Glossary of EMC Smarts Terms Used in NAS Extension Documentation

EMC Smarts Term	EMC Smarts Definition
Adapter	A program that integrates an EMC Smarts Manager with external components. For the NAS Extension, an HTTPS Adapter queries the Celerra Control Station for internal topology information.
Broker	EMC Smarts software that facilitates communications between EMC Smarts Managers and their clients and with other EMC Smarts Managers.
Certification	A label assigned to a network element (system, device, service or application) during the discovery process. The label is based on information that is contained in the *oid2type*.conf* files. Labels include: CERTIFIED---Indicates that the element is discovered using standard mib-2 data and proprietary MIBs. TEMPLATE---Indicates that the OID is recognized by a new entry in *oid2type*.conf*. Note that *oid2type*.conf* is a user-modifiable file with no default entries.
Certification List	Listing of devices that EMC Smarts certifies for management by an EMC Smarts Manager. For a list of Celerra devices certified for the NAS Extension, see "Certified NAS Devices" on page B-1
Codebook	An EMC Smarts data structure that associates problems with the symptoms they cause. This information is used for root-cause and impact analysis using EMC Smarts patented Codebook Correlation Technology™.
Correlation Model	An object-oriented data model that describes the properties of an element, including the characteristic problems of the element, problem symptoms, and symptom propagation patterns to related elements.
Correlator	A general-purpose correlation analysis engine that performs filtering and model processing, along with root-cause and effects analysis. It is driven by three inputs: problem models, topology, and real-time data and events.
Discovery	The process of probing an element to determine its configuration and its relationship to other managed elements, and then instantiating the topology. For the NAS Extension, • The Availability Manager discovers the IP Network elements using ICMP and SNMP probes. • The HTTPS Adapter discovers the components (Data Movers and Control Station) of the Celerra Network Server.
Domain Manager	A generic name for an EMC Smarts software component (such as the Availability Manager), that serves as an analysis engine for a network domain (such as the physical IP network). A Domain Manager includes a Repository of the managed topology and a problem correlation model that monitors network elements, uses correlation technology to pinpoint the root causes of failures, and diagnoses the effects of failures on related elements. Domain Managers report results to the Global Manager for consolidation, and display through the Global Console.
Edge (Map Console display component)	In a map view, an edge represents a connection between two elements. Note that a map edge is not to be confused with a device such as an edge router.

Table A-1 Glossary of EMC Smarts Terms Used in NAS Extension Documentation (continued)

EMC Smarts Term	EMC Smarts Definition
Event	A notable condition that occurs in a network device. The condition may be identified by a message sent from the network element, by a management station polling the element, or by an adapter or third-party software. A Domain Manager uses events, alerts and other data to perform root-cause and impact analysis.
FileServer Element	In the EMC Smarts model for the NAS Extension, the class that represents Data Movers and Filers. In the Global Console for the NAS Extension, a FileServer element is a representation of a Celerra Data Mover or NetApps Filer.
Global Console	A Service Assurance Management Suite component that provides the EMC Smarts graphical user interface (GUI). The Global Console includes the Notification Log, Topology Browser, Map Console, Global Manager Administration Console, Polling and Thresholds Console. (Global Console functionality also available as a Web Console.)
Global Manager	A Service Assurance Management Suite component that manages network elements by obtaining data from distributed Domain Managers. The Global Manager abstracts and consolidates network and system resources, the results of domain-specific root-cause analysis, and the results of domain-specific impact analysis.
Host Element (generic EMC Smarts class for a computer)	In the EMC Smarts model for the NAS Extension, the class that represents the Celerra Control Stations. In the Global Console for the NAS Extension, a Host element is a representation of a Control Station, which is a dedicated management computer that monitors and controls cabinet components and allows access to the full functionality of the Celerra Network Server software.
Icon (Map Console display component)	In a map view for the NAS Extension, an icon represents an entity such as a FileServer or Host element. In the map view, icons are connected by edges.
Impact Analysis	The process of analyzing the effect that root-cause problems have on other elements in the managed system. Impact analysis is performed by Domain Managers, such as the Availability Manager.
Managed Element	An instance of a physical or logical network element that is monitored by a Domain Manager.
Map Console	In the Global Console, the Map Console displays graphical representations of physical and logical topologies including display of managed element icons and edges (connections between elements). Network topology maps for NAS devices include: • Physical Connectivity Map • IP Network Connectivity Map For detailed information about Maps, see the *EMC Smarts Service Assurance Manager Operator's Guide*.
NASChassis Element	In the EMC Smarts model for the NAS Extension, the class that represents the Celerra Network Server. In the Global Console for the NAS Extension, a NASChassis is a representation of a Celerra Network Server, which is the cabinet that contains NAS system elements including a Control Station, Data Movers, and other components that are not monitored by EMC Smarts.
Notification	In the Notification Log of the Global Console, an EMC Smarts message, issued by a Domain Manager, that indicates a problem or other significant event.

Table A-1 Glossary of EMC Smarts Terms Used in NAS Extension Documentation (continued)

EMC Smarts Term	EMC Smarts Definition
Notification Log	In the Global Console, a listing of current notifications, including comprehensive information about the element involved, impact on other elements, root-cause indication, severity, acknowledgment status, escalation information, etc.
Repository	The EMC Smarts in-memory, object-oriented data structure that stores information about the managed elements currently in a network, and the relationships between the elements.
Root-Cause Analysis	The process of analyzing the cause and effect relationships among alarms, alerts, and events in complex systems in order to determine the authentic problem™. Root-cause analysis is performed by Domain Managers.
Topology Browser	In the Global Console, the Topology Browser provides a complete inventory (actual and in representational form) of managed elements in the Repository of a Domain Manager, and the interconnections between those elements. The Topology Browser displays the topology in hierarchical form arranged by classes and instances.

Terminology matrix

Table A-2 lists some comparable terms for the EMC Smarts term used in the EMC Smarts NAS Extension documents, and for EMC NAS Element Management and EMC ControlCenter.

Table A-2 Terminology Matrix for EMC Smarts, EMC NAS Element Management, and EMC ControlCenter Terms

EMC Smarts Term	Comparable EMC NAS Element Management Term	Comparable EMC ControlCenter Term
Broker	N/A	Store
Domain Manager, such as the Availability Manager	Celerra Manager	ControlCenter Infrastructure including ControlCenter Server, Repository, and Stores
Edge (a Map Console term)	N/A	Link In the ControlCenter Console, the Relationship View and Topology View display *links* that represents connections between devices.
Global Console Web Console	N/A	ControlCenter Console and Web Console
Map	N/A	In the ControlCenter Console, the Path Details View and Relationship View
Topology Browser	Celerra Manager user interface	In the ControlCenter Console, the Topology View
Repository	Database	Repository

B

Certified NAS Devices

The following devices are certified for use with the IP Availability Manager Extension for NAS:

- Celerra CNS, NS series, and NSX, with NAS release 4.0 and up.

  Note: To support NAS Extension management functionality, the Celerra Control Station must support XHMP service and have HTTPS enabled.

- NetApp: F700, F800 and F900 series with ONTAP 6.1 – 6.5

C

Availability Manager Notifications

This appendix provides lists of notifications. "Default subscribed events" lists the notifications subscribed to by default. "Notifications generated" lists all events that may be generated by each element.

- Default subscribed events C-2
- Notifications generated C-4

Default subscribed events

Table C-1 lists the default set of events generated by the EMC Smarts IP Availability Manager, including the NAS events, and the class from which they originate, as well as the complete list of the failures, exceptions, root-cause, and symptomatic events that can be reported by IP Availability Manager.

Table C-1 Default Events Subscribed To by IP Availability Manager

Element	Event *(See Key below.)*	Class of Origin
System	Down (r)	ICIM_UnitaryComputerSystem
	Unstable (r)	
	Unresponsive (s)	
	Discovery Error (s)	
Network Adapter	Down (r)	ICIM_NetworkAdapter
	Unstable (r)	
	Disabled (r)	
	Logical Connection Down (r)	
	Backup Activated (s)	NetworkAdapter_Fault
	Exceeded Maximum Uptime (s)	
Connection	Down (r)	ICIM_NetworkDeviceConnection
	Unstable (r)	
Chassis	Down (r)	Chassis
Card	Down (r)	Card
	Switch Over (s)	
Partition	Down (r)	Partition
SNMP Agent	Not Responding (r)	SNMPAgent
VR Agent	Not Responding (r)	VRAgent
Card Redundancy Group	All Components Down (s)	CardRedundancyGroup
	At Risk (s)	
	Reduced Redundancy (s)	
Network Adapter Redundancy Group	All Components Down (s)	NetworkAdapterRedundancyGroup
	At Risk (s)	
	Reduced Redundancy (s)	
Network Connection Redundancy Group	All Components Down (s)	NetworkConnectionRedundancyGroup
	At Risk (s)	
	Reduced Redundancy (s)	

Table C-1 Default Events Subscribed To by IP Availability Manager (continued)

Element	**Event** *(See Key below.)*	**Class of Origin**
System Redundancy Group	All Components Down (s)	SystemRedundancyGroup
	At Risk (s)	
	Reduced Redundancy (s)	
HSRP Group	Switch Over Failed (s)	HSRPGroup
	All Components Down (s)	
	At Risk (s)	
	Reduced Redundancy (s)	
HSRP Endpoint	Switch Over (s)	HSRPEndPoint
Duplicate IP	Duplicate (s)	DuplicateIP
KEY (r) = Root cause (s) = Symptomatic event		

Notifications generated

Table C-2 lists all of the notifications diagnosed by IP Availability Manager.

Table C-2 Notifications Generated By IP Availability Manager

Element	Event	Class of Origin
System	Down	ICIM_UnitaryComputerSystem
	Unstable	
	Discovery Error	
	Might Be Down	
	Unresponsive	
	Connectivity Exception	
	Operational Exception	
Network Adapter	Down	ICIM_NetworkAdapter
	Disabled	
	Logical Connection Down	
	Unstable	NetworkAdapter_Fault
	Backup Activated	
	Exceeded Maximum Uptime	
	Administratively Down	
	Down Or Flapping	
Connections	Down	ICIM_NetworkDeviceConnection
	Unstable	
	Down Or Flapping	
VLAN	Connectivity Exception	VLAN
	Operational Exception	
Chassis	Down	Chassis
Cards	Down	Card
	Operationally Down	
	Switch Over	
Partition	Down	Partition
SNMP Agent	Not Responding	SNMPAgent
	Unresponsive	
	Repeated Restarts	SNMPAgent_Fault

Table C-2 Notifications Generated By IP Availability Manager (continued)

Element	Event	Class of Origin
VR Agent	Not Responding	VRAgent
	Unresponsive	
	Repeated Restarts	VRAgent_Fault
Card Redundancy Group	All Components Down	CardRedundancyGroup
	At Risk	
	Reduced Redundancy	
Network Adapter Redundancy Group	All Components Down	NetworkAdapterRedundancyGroup
	At Risk	
	Reduced Redundancy	
Network Connection Redundancy Group	All Components Down	NetworkConnectionRedundancyGroup
	At Risk	
	Reduced Redundancy	
System Redundancy Group	All Components Down	SystemRedundancyGroup
	At Risk	
	Reduced Redundancy	
HSRP Group	Switch Over Failed	HSRPGroup
	All Components Down	
	At Risk	
	Reduced Redundancy	
HSRP Endpoint	Switch Over	HSRPEndPoint
IP	Down[a]	IP
	Unresponsive[a]	
Duplicate IP	Duplicate	DuplicateIP

a. The IP Availability Manager does not, by default, generate either *IP Down* or *IP Unresponsive* events. These symptomatic events are not required to diagnose any of the root-cause problems reported by IP Availability Manager.

Index

B
BASEDIR v

C
Celerra
    Control Stations v, 1-2
    Data Movers v, 1-2
    Network Server 1-3
Containment dialog
    Opening 6-8
Containment view 6-8
Control Station v, 1-2
Customer support ix

D
Domain Manager
    Containment 6-8

E
Edges
    Table of 6-4
EMC customer service ix
EMC product information ix
EMC technical support ix

G
Global Console 1-2, 1-6, 6-1
    Map Console view 6-2, 6-3
    Notification Log Console view 6-2
    Notification Properties dialog 6-2, 6-8
Global Manager 1-6

H
Help ix
HTTP Adapter
    Installing as a service, Starting 2-3
HTTPS Adapter 2-3

I
Impact notifications 1-7
IPNetwork connectivity map 6-6

M
Map Console
    Icons and indicators 6-4
Maps
    Opening 6-3

N
NAS
    Managed architecture 1-5
NAS Connectivity map 6-7
Network Applications (NetAPPS)
    Filers v, 1-2
Network-attached storage (NAS) 1-2
Nodes
    Table of 6-4
Notification
    Aggregate 1-6
    Symptomatic 1-6
    Root cause
        see Root cause
Notification Log Console 1-6
Notification Properties dialog 6-2, 6-8
    Opening 6-2
Notifications
    Display of 1-6
    Types 1-6

O
Opening a Containment dialog 6-8
Opening a Map 6-3
Opening a Notification Properties dialog 6-2

P
Physical Connectivity map 6-4
Prerequisites v

R
Root-cause problem
    Notification

Root cause 1-6
see Root cause

S

SAN Connectivity map 6-7
Service ix
Service Assurance Manager 1-6
Storage
Network-attached (NAS) 1-2
Storage Area Networks (SAN) 1-2
Symptomatic event 1-6

T

Technical support ix
Topology
Containment 6-8

X

XML/HTTPS discovery probe 1-2