NetIQ® AppManager® for Nortel™ BCMx

Management Guide

February 2011

Legal Notice

NetIQ AppManager is covered by United States Patent No(s): 05829001, 05986653, 05999178, 06078324, 06397359, 06408335.

Contents

About this Book and the Library

The NetIQ AppManager product (AppManager) is a comprehensive solution for managing, diagnosing, and analyzing performance, availability, and health for a broad spectrum of operating environments, applications, services, and server hardware.

AppManager provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager, administrative staff can monitor computer and application resources, check for potential problems, initiate responsive actions, automate routine tasks, and gather performance data for real-time and historical reporting and analysis.

Intended Audience

This guide provides information for individuals responsible for installing an AppManager module and monitoring specific applications with AppManager.

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

Provides complete information about AppManager pre-installation requirements and step-by-step installation procedures for all AppManager components.

User Guide for AppManager Control Center

Provides complete information about managing groups of computers, including running jobs, responding to events, creating reports, and working with Control Center. A separate guide is available for the AppManager Operator Console.

Administrator Guide for AppManager

Provides information about maintaining an AppManager management site, managing security, using scripts to handle AppManager tasks, and leveraging advanced configuration options.

Upgrade and Migration Guide for AppManager

Provides complete information about how to upgrade from a previous version of AppManager.

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

The AppManager library is available in Adobe Acrobat (PDF) format from the NetIQ Web site: www.netiq.com/support/am/extended/documentation/default.asp?version=AMDocumentation.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and CD-ROM titles • Variable names and values • Emphasized words
`Fixed Font`	• File and folder names • Commands and code examples • Text you must type • Text (output) displayed in the command-line interface
Brackets, such as *[value*]	• Optional parameters of a command
Braces, such as {*value}*	• Required parameters of a command
Logical OR, such as *value1*|*value2*	• Exclusive parameters. Choose one parameter.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measureable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

Chapter 1
Introducing AppManager for Nortel BCMx

This chapter introduces AppManager for Nortel Business Communications Manager (Nortel BCMx), providing a brief overview of the module's architecture and describing how you can use AppManager to better monitor vital BCM resources.

Please note that in this document, the term *BCMx* refers to the AppManager module, and the term *BCM* refers to all supported versions of BCM. If a discussion relates only to a specific supported version, the appropriate version number is used to reference the BCM model or software in question.

Features and Benefits

AppManager is designed to help you gain easy access to BCM data, and to help you analyze and manage that data. The AppManager for Nortel BCMx solution minimizes the cost of maintaining BCM services and functions, aids in capacity planning, and can prevent downtime.

With AppManager for Nortel BCMx, administrators gain access to a new set of tools they can leverage to gather a wide range of diagnostic and management data, which can help prevent outages and keep things running smoothly.

AppManager for Nortel BCMx includes Knowledge Scripts for creating jobs that monitor the health, availability, and performance of key BCM features. These scripts allow you to monitor and manage crucial services at a depth unparalleled by any other solution. Each Knowledge Script can be configured to raise an event, collect data for reporting, and perform automated problem management when an event occurs.

The following are just a few of the features and benefits of monitoring Nortel BCM with AppManager:

- BCMs and associated components are discovered with a single discovery job
- Knowledge Scripts collect data for all monitored BCMs and associated components:
  - System health, including CPU, memory, disk space, and temperature
  - BCM availability
  - BCM link utilization for LAN links
  - BCM QoS log entries for MOS estimates for several codecs: G.711a, G.711u, G.723.1 (5.3 and 6.3 kbps), G.729, and G.729A
  - Hunt group usage, including abandoned calls
  - Nortel BCM alarms
- Limited support for SRG (Survivable Remote Gateway) mode and local mode with the Alarms, CallByCallLimits, ChassisUsage, HealthCheck, HuntGroupUsage, InterfaceHealth, LinkUtilization, PSTNFallback, SystemUpTime, and SystemUsage Knowledge Scripts

Counting AppManager Licenses

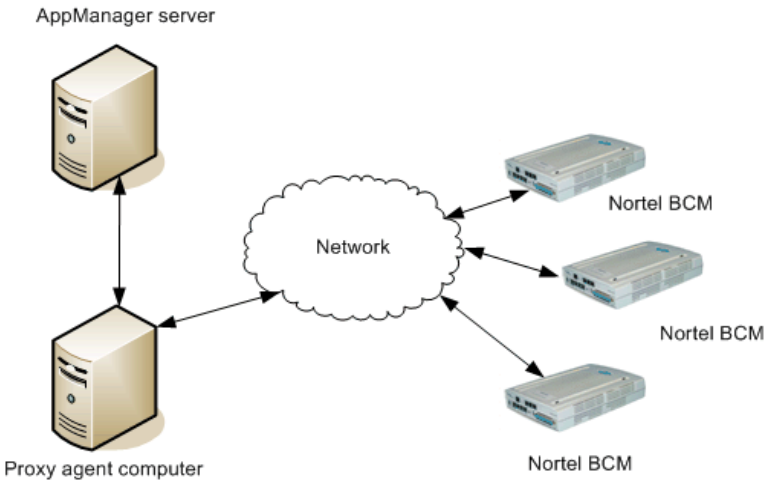
AppManager for Nortel BCMx consumes one AppManager license per phone registered to a BCM.

Proxy Architecture

With AppManager proxy architecture support for Nortel BCM, the AppManager agent does not need to be installed on every device that you want to monitor.

Within the proxy architecture, the AppManager for Nortel BCMx managed object (`qNortelBCMx.dll`) is installed on the managed client (agent) computer. When you run a Knowledge Script job, the BCMx managed object runs on the managed client and sends messages to and from BCM devices (using CIM/XML) for which you have designated the managed client computer as the proxy.

The following drawing shows the relationship between Nortel BCM devices and the AppManager server and proxy agent computers.



Scalability Considerations

Only one computer should act as a proxy for any given Nortel BCM device. One computer should be the proxy for no more than 100 Nortel BCM devices. Of course, this number is only a recommendation and can vary based on the capabilities of your proxy computer.

As you scale up your Nortel BCM environment, consider the following:

- The HealthCheck Knowledge Script requires extensive use of the proxy computer's processing capacity. Because this script is a member of the NortelBCMx Recommended Knowledge Script Group (KSG), running it may affect the performance of other recommended scripts that are running at the same time.
- The LogicalDiskSpace Knowledge Script is a member of the NortelBCMx Recommended KSG, which allows you to run all recommended scripts at one time. However, there are limits on the number of Logical Disk objects on which the LogicalDiskSpace script can run. If you run the Recommended KSG on more objects than the LogicalDiskSpace script allows, you will receive an error message indicating that the number of target objects has exceeded its limit. If you receive this error message, remove the LogicalDiskSpace script from the KSG. Then run LogicalDiskSpace alone on fewer Logical Disk objects.

Chapter 2
Installing AppManager for Nortel BCMx

This chapter provides installation instructions and describes system requirements for AppManager for Nortel BCMx.

This chapter assumes you have AppManager installed. For more information about installing AppManager or about AppManager system requirements, see the *Installation Guide for AppManager*, which is available on the NetIQ Web site or in the `\Documentation` folder of the AppManager installation kit.

System Requirements

AppManager for NortelBCMx has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB), console, and proxy agent computer	At minimum, 7.0 Support for Windows Server 2008 requires hotfix 71704, or the most recent AppManager Windows Agent hotfix. For more information, see the AppManager Suite Hotfixes Web page.
Nortel BCM software installed on the BCM hardware you want to monitor	4.0 on BCM 200, 400, or 1000 1.0, 5.0 on BCM 450 1.0, 3.0, 5.0 on BCM 50 (firmware releases 1.00.2.04.j through 3.0), including versions 50a (with an ADSL router) and 50e (with an Ethernet router)
Nortel BCM patch installed on the BCM hardware you want to monitor	BCM.R400.032-PSM installed on BCM software version 4.0. NetIQ does not guarantee the CPU and memory data returned by the SystemUsage Knowledge Script if patch BCM.R400.032-PSM is not installed.
Microsoft operating system installed on the proxy agent computer	One of the following: • 32-bit Windows 2000 • 32- or 64-bit Windows Server 2003 • 32- or 64-bit Windows Server 2008 • Windows Server 2008 R2

For the latest information about supported software versions and the availability of module updates, visit the AppManager Supported Products page at www.netiq.com/support/am/supportedproducts/default.asp. If you encounter problems using this module with a later version of your application, contact NetIQ Technical Support.

For more information about system requirements for the AppManager agent, repository, and management server, see the *Installation Guide for AppManager*.

Installing the Module

The setup program automatically identifies and updates all relevant AppManager components on a computer. Therefore, run the setup program only once on any computer. The pre-installation check also runs automatically when you launch the setup program.

You can install the module in one of the following ways:

- Run the module setup program, `AM70-NortelBCMx-7.x.x.0.msi`, which you downloaded from the Web. Save the module setup files on the distribution computer, and then delete the older versions of the module setup files. For more information about the distribution computer, see the *Installation Guide for AppManager.*
- Use Control Center to install the module on the remote computer where an agent is installed. Ensure you check in the installation package, which is the `.XML` file included with the module setup program. For more information about the `.XML` file, see the *AppManager for NortelBCMx Readme*. For more information about deploying modules on agent computers, see the *Control Center User Guide for AppManager.*

To install the module:

1. Run the module setup program on all repository computers to install the Knowledge Scripts and reports. For repositories running in a clustered environment, run the setup program on the node that currently owns the cluster resource.
2. Install the module on each proxy agent computer. Use one of the following methods:
   - Run the module setup program.
   - Use Control Center Console to deploy the installation package.

   Note
   No other AppManager module should be installed on the proxy agent computer.
3. Run the module setup program on all Operator Console and Control Center computers to install the Help.
4. Configure the user name and password for the BCM devices into AppManager Security Manager. For more information, see "Configuring the BCM User Name and Password" on page 8.
5. *If you have not already discovered Nortel BCMx resources*, run the Discovery_NortelBCMx Knowledge Script on the proxy agent computers where you installed the module.

After the installation has completed, you can find a record of problems encountered in the `NortelBCMx_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\<ServerName>` folder.

Verifying Your Installed Module

To verify installation on many computers, run the ReportAM_CompVersion Knowledge Script. Ensure you discover a report-enabled agent before running this script. For more information, see the Help for the script.

To verify installation on one or only a few computers, use the Operator Console.

To verify your installed module with the Operator Console:

1. In the TreeView pane, select the computer for which you want to verify your installed module.
2. From the TreeView menu, select **Properties**. On the System tab, the System information pane displays the version numbers for all modules installed on the computer.
3. Verify that the version number from the *AppManager for Nortel BCMx Readme* matches the version number shown in the System information pane.

Upgrading Knowledge Script Jobs

This release of AppManager for Nortel BCMx may contain updated Knowledge Scripts. You can push the changes for updated scripts to running Knowledge Script jobs in one of the following ways:

- Use the AMAdmin_UpgradeJobs Knowledge Script.
- Use the Properties Propagation feature.

Running AMAdmin_UpgradeJobs

The AMAdmin_UpgradeJobs Knowledge Script can push changes to running Knowledge Script jobs. Your AppManager repository (`QDB`) must be at version 7.0 or later. In addition, the repository computer must have hotfix 72040 installed, or the most recent AppManager Repository hotfix. To download the hotfix, see the AppManager Suite Hotfixes Web page.

Upgrading jobs to use the most recent script version allows the jobs to take advantage of the latest script logic while maintaining existing parameter values for the job.

For more information, see the Help for the AMAdmin_UpgradeJobs Knowledge Script.

Propagating Knowledge Script Changes

You can propagate script changes to jobs that are running and to Knowledge Script Groups, including recommended Knowledge Script Groups and renamed Knowledge Scripts.

Before propagating script changes, verify that the script parameters are set to your specifications. Customized script parameters may have reverted to default parameters during the installation of the module. New parameters may need to be set appropriately for your environment or application.

You can choose to propagate only properties (specified in the Schedule and Values tabs), only the script (which is the logic of the Knowledge Script), or both. Unless you know specifically that changes affect only the script logic, you should propagate both properties and the script.

For more information about propagating Knowledge Script changes, see the "Running Monitoring Jobs" chapter of the *Operator Console User Guide for AppManager*.

Propagating Changes to Ad Hoc Jobs

You can propagate the properties and the logic (script) of a Knowledge Script to ad hoc jobs started by that Knowledge Script. Corresponding jobs are stopped and restarted with the Knowledge Script changes.

To propagate changes to ad hoc Knowledge Script jobs:

1. In the Knowledge Script view, select the Knowledge Script for which you want to propagate changes.
2. Click **Properties Propagation > Ad Hoc Jobs**.
3. Select the components of the Knowledge Script that you want to propagate to associated ad hoc jobs:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, such as schedule, monitoring values, actions, and advanced options.

Propagating Changes to Knowledge Script Groups

You can propagate the properties and logic (script) of a Knowledge Script to corresponding Knowledge Script Group members.

After you propagate script changes to Knowledge Script Group members, you can propagate the updated Knowledge Script Group members to associated running jobs. For more information, see "Propagating Changes to Ad Hoc Jobs" on page 8.

To propagate Knowledge Script changes to Knowledge Script Groups:

1. In the Knowledge Script view, select the Knowledge Script Group for which you want to propagate changes.
2. On the KS menu, select **Properties propagation > Ad Hoc Jobs**.
3. ***If you want to exclude a Knowledge Script member from properties propagation***, deselect that member from the list in the Properties Propagation dialog box.
4. Select the components of the Knowledge Script that you want to propagate to associated Knowledge Script Groups:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, including the schedule, actions, and Advanced properties.

5. Click **OK**. Any monitoring jobs started by a Knowledge Script Group member are restarted with the job properties of the Knowledge Script Group member.

Configuring the BCM User Name and Password

AppManager cannot communicate with Nortel BCM devices unless it has permission to do so. You can grant that permission by configuring the appropriate user name and password into AppManager Security Manager.

Configure Security Manager *before* you run Discovery_NortelBCMx. Without knowing the user name and password, the discovery process cannot locate your BCM devices.

If you need to create a new user for the BCM, see the "Security Policies and Accounts and Privileges" chapter of the *Administration Guide* for your BCM device.

On the Custom tab in Security Manager, complete the following fields:

Field	Description
Label	`NortelBCMx`
Sub-label	`default`
Value 1	Case-sensitive user name
Value 2	Case-sensitive password
Extended application support	Encrypts the user name and password in Security Manager. Do not leave this option unselected.

Scheduling BCM Maintenance

Use the AMAdmin_SchedMaint Knowledge Script to specify a maintenance period for a BCM device. During the maintenance period, regularly scheduled AppManager jobs can be prevented from running. Set the maintenance periods to coincide with those times that you are performing scheduled backups of your BCM device.

You can specify the type of Knowledge Scripts you want to block by Knowledge Script category, or prevent all jobs from running on a server (because of expected downtime, for example).

For more information about setting up AMAdmin_SchedMaint, see the Help for the script.

For more information about performing backups of your BCM device, see the *Administration Guide* for your BCM device.

Troubleshooting Missing Data Points

AppManager for NortelBCMx sends consolidated requests to the Nortel BCM device in order to efficiently collect the data used by all NortelBCMx Knowledge Scripts (except Alarms and Discovery). AppManager sends these requests 30 seconds before a Knowledge Script begins each iteration. This 30-second data-collection offset allows enough time for AppManager to execute the query before a Knowledge Script requires the data.

If you notice that data points are missing from a job's data stream, it may be that 30 seconds is not enough time for AppManager to execute all of the queries you need, most likely because you are running several scripts on the same schedule.

You can increase the data-collection offset time by changing a Registry setting:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\Appmanager\4.0\NetIQmc\DataRecorder\CollectionOffset
```

In the right pane of the Registry Editor, double-click **NortelBCMx** and change the **Decimal** value from 30 seconds to a larger value that will allow enough time for AppManager to execute the queries for all of the scripts you are running. Keep the value *less* than the shortest interval specified by any Knowledge Script. For example, if one script runs every one minute, but the others run every five minutes, do not change the Registry setting to a value equal to or greater than 60 seconds.

Notes

- Changes to this Registry setting affect the data-collection offset time for *every* NortelBCMx Knowledge Script, except Alarms and Discovery_NortelBCMx.
- If you change a Registry setting, you must restart the NetIQ AppManager Client Resource Monitor service (`netiqmc.exe`) before the new value is in effect.

Chapter 3
NortelBCMx Knowledge Scripts

AppManager for Nortel BCMx provides the following Knowledge Scripts for monitoring Nortel BCM software version 4.0 or later on hardware models 200, 400 and 1000, and Nortel BCM firmware version 1.00.2.04j or greater on hardware model 50, including versions 50a and 50e. From within the Operator Console, select a Knowledge Script on the NortelBCMx tab in the Knowledge Script pane and press **F1** for complete details.

Knowledge Script	What It Does
Alarms	Monitors the Nortel BCMx proxy computer for Nortel BCM alarms.
CallByCallLimits	Monitors the number of incoming and outgoing calls denied because call-by-call limits were exceeded.
ChassisUsage	Monitors the physical chassis of a BCM device.
HealthCheck	Monitors the operational status of BCM services.
HuntGroupUsage	Monitors call statistics for one or more hunt groups.
InterfaceHealth	Monitors the operational status of the interfaces on a network device.
LinkUtilization	Monitors LAN links for utilization and packet errors.
LogicalDiskSpace	Monitors logical disk space usage and availability.
PSTNFallback	Monitors PSTN fallback attempts and failures.
QoSLog	Monitors the MOS estimates for several codecs: G.711a, G.711u, G.723 5.3. kbps, G.723 6.3 kbps, G.729, and G.729A.
SystemUpTime	Monitors the number of seconds that the system has been operational since its last reboot.
SystemUsage	Monitors BCM CPU and memory usage.
UPSHealth	Monitors any attached uninterruptible power supply.
Recommended Knowledge Script Group	Performs essential monitoring of your Nortel BCM environment.
Discovery_NortelBCMx	Discovers the various components of a Nortel BCM installation for software version 4.0 and hardware models 50, 50a, 50e, 200, 400, and 1000.

Alarms

Use this Knowledge Script to monitor the Nortel BCMx proxy computer for Nortel BCM alarms. Nortel BCM devices send alarms to the proxy computer using SNMP traps.

When setting parameters for this script, you are asked to provide a list of alarm identifiers (system messages) that you want to include or exclude from monitoring. Their format consists of a multi-digit alarm number, such as 18 or 10029.

Prerequisites

- Install the Windows SNMP service before running this script. If you installed the service before you installed the Nortel BCMx module that contains this script, you do not need to do anything else. If you installed the service after you installed the Nortel BCMx module, stop and restart the AppManager agent on the proxy agent computer before using this script.
- Configure Nortel BCM devices to send SNMP traps to the proxy agent. For more information, see "Identifying the SNMP Trap Receiver" on page 14.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx

Default Schedule

By default, this script runs on an asynchronous schedule.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Notes for the alarm categories: • If you choose to "Include only" selected alarm identifiers in a category, AppManager will raise events *only* for those identifiers. *AppManager will not raise events for the other identifiers included in the category.* • If you choose to "Exclude" selected alarm identifiers from a category, AppManager will raise events for all alarm identifiers included in the category *except* those that you specifically excluded. • If you accept the default parameter settings, which are "Exclude" and blank (in the *Alarm identifiers* parameter), AppManager will raise events for all identifiers in the category, because you excluded nothing from the category.	
Monitor PVQM alarms?	Select **Yes** to monitor the Nortel BCMx proxy server for alarms in the "PVQM" category. The default is Yes.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers that you specify in the following parameter. By default, AppManager monitors all alarms with PVQM severity in the SNMP trap.

Parameter	How to Set It
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the “PVQM” category. By default, the list contains the 50501, 50504, 50507, and 50510 identifiers.
Monitor critical alarms?	Select **Yes** to monitor the Nortel BCMx proxy server for alarms in the “critical” category. The default is Yes.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. By default, AppManager monitors all alarms with critical severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the “critical” category. The default is an empty list.
Monitor major alarms?	Select **Yes** to monitor the Nortel BCMx proxy server for alarms in the “major” category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. By default, AppManager monitors all alarms with major severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the “major” category. The default is an empty list.
Monitor minor alarms?	Select **Yes** to monitor the Nortel BCMx proxy server for alarms in the “minor” category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. By default, AppManager monitors all alarms with minor severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the “minor” category. The default is an empty list.
Monitor warning alarms?	Select **Yes** to monitor the Nortel BCMx proxy server for alarms in the “warning” category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. By default, AppManager monitors all alarms with warning severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the “warning” category. The default is an empty list.
Monitor info alarms?	Select **Yes** to monitor the Nortel BCMx proxy server for alarms in the “informational” category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. By default, AppManager monitors all alarms with informational severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the “informational” category. The default is an empty list.
Event Severities	
Severity - Critical alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a critical alarm is detected. The default is 10.
Severity - Major alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a major alarm is detected. The default is 15.
Severity - Minor alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a minor alarm is detected. The default is 20.

Parameter	How to Set It
Severity - Warning alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a warning alarm is detected. The default is 25.
Severity - Info alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which an informational alarm is detected. The default is 30.

Identifying the SNMP Trap Receiver

Manually configure Nortel BCM to send SNMP traps to AppManager. Use Element Manager to identify the AppManager proxy computer as an SNMP trap receiver.

To identify the proxy computer as a trap receiver:

1. Log in to Element Manager.
2. On the Administration tab, expand the **General** folder and select **SNMP Trap Destinations**.
3. In the right pane, click **Add**, and then complete the fields as described in the table below:

Field	Instructions
Name	Provide the host name of the proxy agent computer to which you want to send SNMP traps (the computer on which the BCMx module is installed).
Host address	Provide the IP address of the proxy agent computer.
Port	Accept the default: port 162.
SNMP version	Accept the default: v1/v2C.
Community string	Provide the SNMP community string of the proxy agent computer.
User name	Leave this field blank.

4. Click **OK**.

CallByCallLimits

Use this Knowledge Script to monitor incoming and outgoing calls that were denied because call-by-call limits were exceeded. PRI pools that support call-by-call services have maximum and minimum call limits for each service. You can assess the capacity of the PRI call services on your system by monitoring the number of calls that were denied because they exceeded or fell below the limits.

This script raises an event when any monitored value exceeds a threshold that you set.

Call-by-call limits are programmed in Element Manager and are defined as follows:

Limit	Definition
Incoming maximum	The maximum number of calls that can enter the PRI pools for a particular service. Any calls that exceed the maximum will be denied.
Incoming minimum	The minimum number of calls that can enter the PRI pools for a particular service. If the number of calls falls below the minimum, the calls will be denied and the PRI pools will be allocated to a different service.
Outgoing maximum	The maximum number of calls that can exit the PRI pools for a particular service. Any calls that exceed the maximum will be denied.
Outgoing minimum	The minimum number of calls that can exit the PRI pools for a particular service. If the number of calls falls below the minimum, the calls will be denied and the PRI pools will be allocated to a different service.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx_PRIPool

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the CallByCallLimits job fails. The default is 5.
Monitor incoming calls denied after maximum limit exceeded	
Event Notification	

Parameter	How To Set It
Raise event if denied incoming calls exceed threshold?	Select **Yes** to raise an event if the number of denied incoming calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum denied incoming calls	Specify the highest number of incoming calls that can be denied before an event is raised. The default is 0 calls.
Event severity when denied incoming calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of denied incoming calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for incoming calls denied after maximum limit exceeded?	Select **Yes** to collect data about incoming calls that were denied after the maximum limit was exceeded. The default is unselected.
Monitor incoming calls denied after minimum limit not reached	
Event Notification	
Raise event if denied incoming calls exceed threshold?	Select **Yes** to raise an event if the number of denied incoming calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum denied incoming calls	Specify the maximum number of incoming calls that can be denied before an event is raised. The default is 0 calls.
Event severity when denied incoming calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of denied incoming calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for incoming calls denied after minimum limit not reached	Select **Yes** to collect data about incoming calls that were denied after the minimum limit was not reached. The default is unselected.
Monitor outgoing calls denied after maximum limit exceeded	
Event Notification	
Raise event if denied outgoing calls exceed threshold?	Select **Yes** to raise an event if the number of denied outgoing calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum denied outgoing calls	Specify the highest number of outgoing calls that can be denied before an event is raised. The default is 0 calls.
Event severity when denied outgoing calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of denied outgoing calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for outgoing calls denied after maximum limit exceeded?	Select **Yes** to collect data about outgoing calls that were denied after the maximum limit was exceeded. The default is unselected.
Monitor outgoing calls denied after minimum limit not reached	
Event Notification	
Raise event if denied outgoing calls exceed threshold?	Select **Yes** to raise an event if the number of denied outgoing calls exceeds the threshold that you set. The default is Yes.

Parameter	How To Set It
Threshold - Maximum denied outgoing calls	Specify the highest number of outgoing calls that can be denied before an event is raised. The default is 0 calls.
Event severity when denied outgoing calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of denied outgoing calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for outgoing calls denied after minimum limit not reached?	Select **Yes** to collect data about outgoing calls that were denied after the minimum limit was not reached. The default is unselected.

ChassisUsage

Use this Knowledge Script to monitor the physical chassis of a BCM device, including temperature sensors, voltage sensors, and fan speeds. This script raises events for status changes in BCM 200/400 components (running BCM software version 4.0) and for monitored values that exceed or fall below the threshold that you set. In addition, this script generates data streams for the following metrics:

- Remote temperature for BCM 50
- Local temperature
- CPU temperature for BCM 200/400
- Fan 1 and fan 2 speeds for BCM 50
- Power supply voltage levels:
  - v5
  - v+12
  - v-12 for BCM 200/400
  - vcc for BCM 50
  - vccp for BCM 50
  - v3.3 (Standby, One, and Two) for BCM 200/400

Notes

- BCM model 1000 does not support the monitoring of voltage, fan speed, or temperature. This script raises an event if you attempt to monitor any of these chassis components on BCM 1000.
- In this script, the monitoring of fan speeds, temperatures, and voltages is disabled by default. BCM itself will raise an alarm if any of these values is abnormal, and then send the alarm as an SNMP trap to the Alarms script. If you enable the monitoring of fan speeds, temperatures, or voltages, be aware that you may receive duplicate or conflicting alarm and events. For instance, AppManager may raise an event indicating a high temperature based on a threshold that you set, but the BCM does not raise an alarm because the temperature has not yet reached the abnormal level as determined by Nortel.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the ChassisUsage job fails. The default is 5.
The ChassisUsage script monitors status changes only for BCM 200/400 models running BCM software version 4.0. The event message indicates the type of change, such as "The status for local temperature has changed to Above Tolerance" or "The status of fan 1 has changed to Stopped."	
Raise event if local temperature status changes?	Select **Yes** to raise an event if the status of the local temperature changes. The default is unselected.
Event severity when local temperature status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the local temperature has changed. The default is 30.
Raise event if CPU temperature status changes?	Select **Yes** to raise an event if the status of the CPU temperature changes. The default is unselected.
Event severity when CPU temperature status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the CPU temperature has changed. The default is 30.
Raise event if fan 1 status changes?	Select **Yes** to raise an event if the status of fan 1 changes. The default is unselected.
Event severity when fan 1 status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of fan 1 has changed. The default is 30.
Raise event if CPU fan status changes?	Select **Yes** to raise an event if the status of the CPU fan changes. The default is unselected.
Event severity when CPU fan status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the CPU fan has changed. The default is 30.
Raise event if v5 voltage status changes?	Select **Yes** to raise an event if the status of the v5 power supply voltage changes. The default is unselected.
Event severity when v5 voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the v5 power supply voltage has changed. The default is 30.
Raise event if v+12 voltage status changes?	Select **Yes** to raise an event if the status of the v+12 power supply voltage changes. The default is unselected.
Event severity when v+12 voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the v+12 power supply voltage has changed. The default is 30.
Raise event if v-12 voltage status changes?	Select **Yes** to raise an event if the status of the v-12 power supply voltage changes. The default is unselected.
Event severity when v-12 voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the v-12 power supply voltage has changed. The default is 30.
Raise event if v3.3 Standby voltage status changes?	Select **Yes** to raise an event if the status of the v3.3 Standby power supply voltage changes. The default is unselected.
Event severity when v3.3 Standby voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the v3.3 Standby power supply voltage has changed. The default is 30.

Description	How To Set It
Raise event if v3.3 One voltage status changes?	Select **Yes** to raise an event if the status of the v3.3 One power supply voltage changes. The default is unselected.
Event severity when v3.3 One voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the v3.3 One power supply voltage has changed. The default is 30.
Raise event if v3.3 Two voltage status changes?	Select **Yes** to raise an event if the status of the v3.3 Two power supply voltage changes. The default is unselected.
Event severity when v3.3 Two voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the v3.3 Two power supply voltage has changed. The default is 30.
Monitor local temperature	
Event Notification	
Raise event if local temperature exceeds threshold?	Select **Yes** to raise an event if the local temperature exceeds the threshold that you set. The default is unselected.
Threshold - Maximum local temperature	Specify the highest local temperature that can occur before an event is raised. The default is 55º Celsius.
Event severity when local temperature exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the local temperature exceeds the threshold. The default is 10.
Data Collection	
Collect data for local temperature?	Select **Yes** to collect data about local temperature for reports and graphs. The default is unselected.
Monitor remote temperature (BCM 50 only)	
Event Notification	
Raise event if remote temperature exceeds threshold?	Select **Yes** to raise an event if the remote temperature on a BCM 50 exceeds the threshold that you set. The default is unselected.
Threshold - Maximum remote temperature	Specify the highest remote temperature that can occur on a BCM 50 before an event is raised. The default is 55º Celsius.
Event severity when remote temperature exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the remote temperature on a BCM 50 exceeds the threshold. The default is 10.
Data Collection	
Collect data for remote temperature?	Select **Yes** to collect data about remote temperature for reports and graphs. The default is unselected.
Monitor CPU temperature (BCM 200/400 only)	
Event Notification	
Raise event if CPU temperature exceeds threshold?	Select **Yes** to raise an event if the CPU temperature on a BCM 200 or 400 exceeds the threshold that you set. The default is unselected.
Threshold - Maximum CPU temperature	Specify the highest CPU temperature that can occur on a BCM 200 or 400 before an event is raised. The default is 55º Celsius.
Event severity when CPU temperature exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CPU temperature on a BCM 200 or 400 exceeds the threshold. The default is 10.
Data Collection	

Description	How To Set It
Collect data for CPU temperature?	Select **Yes** to collect data about CPU temperature for reports and graphs. The default is unselected.
Monitor fan 1 speed (BCM 50 only)	
Event Notification	
Raise event if fan 1 speed exceeds threshold?	Select **Yes** to raise an event if the speed of fan 1 on a BCM 50 exceeds the threshold that you set. The default is unselected.
Threshold - Maximum fan 1 speed	Specify the highest fan speed that can occur before an event is raised. The default is 10000 RPMs.
Event severity when fan 1 speed exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the fan speed exceeds the threshold. The default is 10.
Data Collection	
Collect data for fan 1 speed?	Select **Yes** to collect data about fan speed for reports and graphs. The default is unselected.
Monitor fan 2 speed (BCM 50 only)	
Event Notification	
Raise event if fan 2 speed exceeds threshold?	Select **Yes** to raise an event if the speed of fan 2 on a BCM 50 exceeds the threshold that you set. The default is unselected.
Threshold - Maximum fan 2 speed	Specify the highest fan speed that can occur before an event is raised. The default is 10000 RPMs.
Event severity when fan 2 speed exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the fan speed exceeds the threshold. The default is 10.
Data Collection	
Collect data for fan 2 speed?	Select **Yes** to collect data about fan speed for reports and graphs. The default is unselected.
Monitor v5 voltage level	
Event Notification	
Raise event if v5 voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the v5 power supply voltage level exceeds or falls below the thresholds that you set. The default is unselected. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is unselected.
Threshold - Maximum v5 voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 5.25 volts.
Event severity when v5 voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum v5 voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 4.75 volts.
Event severity when v5 voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for v5 voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.

Description	How To Set It
Monitor v+12 voltage level	
Event Notification	
Raise event if v+12 voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the v+12 power supply voltage level exceeds or falls below the thresholds that you set. The default is unselected. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is unselected.
Threshold - Maximum v+12 voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 12.6 volts.
Event severity when v+12 voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum v+12 voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 11.4 volts.
Event severity when v+12 voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for v+12 voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.
Monitor v-12 voltage level (BCM 200/400 only)	
Event Notification	
Raise event if v-12 voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the v-12 power supply voltage level exceeds or falls below the thresholds that you set. The default is unselected. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is unselected.
Threshold - Maximum v-12 voltage level	Specify the highest voltage level that can occur before an event is raised. The default is -12.6 volts.
Event severity when v-12 voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum v-12 voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is -11.4 volts.
Event severity when v-12 voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for v-12 voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.
Monitor vcc voltage level (BCM 50 only)	
Event Notification	

Description	How To Set It
Raise event if vcc voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the vcc power supply voltage level exceeds or falls below the thresholds that you set. The default is unselected. vcc refers to voltage from a power supply connected to the collector terminal of a bipolar transistor. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is unselected.
Threshold - Maximum vcc voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 3.4 volts.
Event severity when vcc voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum vcc voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 3.2 volts.
Event severity when vcc voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for vcc voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.
Monitor vccp voltage level (BCM 50 only)	
Event Notification	
Raise event if vccp voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the vccp power supply voltage level exceeds or falls below the thresholds that you set. The default is unselected. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is unselected.
Threshold - Maximum vccp voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 1.442 volts.
Event severity when vccp voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum vccp voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 1.358 volts.
Event severity when vccp voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for vccp voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.
Monitor v3.3 Standby voltage level (BCM 200/400 only)	
Event Notification	
Raise event if v3.3 Standby voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the v3.3 Standby power supply voltage level exceeds or falls below the thresholds that you set. The default is Yes. **Note** You cannot enable an upper or lower threshold unless you check this option.

Description	How To Set It
Upper threshold	Select **Enable** to use an upper threshold value. The default is unselected.
Threshold - Maximum v3.3 Standby voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 3.4 volts.
Event severity when v3.3 Standby voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum v3.3 Standby voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 3.2 volts.
Event severity when v3.3 Standby voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for v3.3 Standby voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.
Monitor v3.3 One voltage level (BCM 200/400 only)	
Event Notification	
Raise event if v3.3 One voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the v3.3 One power supply voltage level exceeds or falls below the thresholds that you set. The default is Yes. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is Unchecked.
Threshold - Maximum v3.3 One voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 3.4 volts.
Event severity when v3.3 One voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum v3.3 One voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 3.2 volts.
Event severity when v3.3 One voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for v3.3 One voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.
Monitor v3.3 Two voltage level (BCM 200/400 only)	
Event Notification	
Raise event if v3.3 Two voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the v3.3 Two power supply voltage level exceeds or falls below the thresholds that you set. The default is Yes. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is Unchecked.
Threshold - Maximum v3.3 Two voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 3.4 volts.

Description	How To Set It
Event severity when v3.3 Two voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is Unchecked.
Threshold - Minimum v3.3 Two voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 3.2 volts.
Event severity when v3.3 Two voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for v3.3 Two voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.

HealthCheck

Use this Knowledge Script to monitor the operational status of Nortel BCM services. A data point of 100 is recorded if the service is running; a data point of 0 is recorded if the service is not running. Possible non-running states include start pending, stopped, stop pending, continue pending, paused, and pause pending.

This script raises an event when a monitored value exceeds a threshold that you set.

It is important to monitor the up-and-down status of vital Nortel BCM services. If any service consumes excessive CPU resources, other services may be adversely affected. Run this script to notify you when a critical service goes down or when the overall percentage of important services drops below the specified threshold. The BCM Reset utility should restart any down service in a timely manner.

Monitored Services

The HealthCheck script monitors the operational status of several BCM services. In addition, the script can be configured to monitor the availability percentage of key services. The following table identifies the services that you can monitor with HealthCheck.

Service Name	Description	Key?
BackupRestoreProviderAgent	CIMOM Provider	
BCM_DataInterfacesProviderAgent	CIMOM Provider	
BCM_DCMProviderAgent	CIMOM Provider	
BCM_DNSProviderAgent	CIMOM Provider	
BCM_Doorphone	CIMOM Provider	
BCM_HostProviderAgent	CIMOM Provider	
BCM_IPMusicProviderAgent	CIMOM Provider	
BCM_ISDNProviderAgent	CIMOM Provider	
BCM_LicenseProviderAgent	CIMOM Provider	
BCM_LogProviderAgent	CIMOM Provider	
BCM_MIB2ProviderAgent	CIMOM Provider	
BCM_ModemDialUpProviderAgent	CIMOM Provider	
BCM_NetLinkMgrProviderAgent	CIMOM Provider	
BCM_NetworkInterfacesProviderAgent	CIMOM Provider	
BCM_PPPoEProviderAgent	CIMOM Provider	
BCM_PSM_ProviderAgent	CIMOM Provider	
BCM_RASProviderAgent	CIMOM Provider	
BCM_RoutingProviderAgent	CIMOM Provider	
BCM_SecurityProviderAgent	CIMOM Provider	
BCM_SNMPProviderAgent	CIMOM Provider	
BCM_SRGProviderAgent	CIMOM Provider	
BCM_TimeServiceProviderAgent	CIMOM Provider	
BCM_TimeZoneSettingProviderAgent	CIMOM Provider	
BCM_WANProviderAgent	CIMOM Provider	

Service Name	Description	Key?
BCM_WebCacheProviderAgent	CIMOM Provider	
BcmAmp	IP Music	
BCMCoreUploadProviderAgent	CIMOM Provider	
BCMInventoryProviderAgent	CIMOM Provider	
BCMPerfMonProviderAgent	CIMOM Provider	
BCMSystemProviderAgent	CIMOM Provider	
BCMUPSProviderAgent	CIMOM Provider	
BCMWebProviderAgent	CIMOM Provider	
btraceserver	Plug-in for Authentication and Routing Management for BT	
CallPilotProviderAgent	CIMOM Provider	
CCRSAppServer	Call Center Reporting Service	Yes
CDRProviderAgent	CIMOM Provider	
CDRService	Call Detail Recording service	
cfsserver	Component Feature service	Yes
core_file_monitor	Core File Monitor	
coreauthservice	CoreTel Authentication Service	
CoreTel	Main Telephony Process	Yes
CoreTelProviderAgent	CIMOM Provider	
crond	CRON Scheduler Daemon	
Cte	Computer Telephony Engine	
ctiserver	Computer Telephony Integration	Yes
DataDebugToolsProviderAgent	CIMOM Provider	
dhcpd	DHCP Server Daemon	Yes
DHCPProviderAgent	CIMOM Provider	
DiaLogger	System Logging Mechanism	
DSCProviderAgent	CIMOM Provider	
EchoServer	Echo Server	
feps	Functional Endpoint Proxy Server	Yes
gated	Router SNMP Subagent	
HGMetricsReporter	Hunt Group Metrics	
HotDesking	used with IP sets	
httpd	http Daemon	
ipppd.ippp0-15	Router/WAN Services	Yes
IPSecProviderAgent	CIMOM Provider	
IpTelProviderAgent	CIMOM Provider	
IVRProviderAgent	CIMOM Provider	
LanCteProviderAgent	CIMOM Provider	

Service Name	Description	Key?
LANProviderAgent	CIMOM Provider	
lms	Line Monitor Server	
LogManagement	Log File Management Service	
mgs	Media Gateway Server	Yes
mmdp	IVR Service	Yes
modemcc	Modem Call Control	Yes
monit	Monitoring Daemon	
mps	IP Telephony - Media Path	Yes
MscService	Media Services Card Service	Yes
Msm	Media Services Manager	Yes
MsmProviderAgent	CIMOM Provider	
NetworkStatisticsProviderAgent	CIMOM Provider	
NnuScheduler	System Scheduler	
owcimomd	Open WBEM CIMOM Server Daemon	Yes
Pdrd	Persistence Data Repository service	Yes
psm	Process Status Monitor service	Yes
qmond	QoS Monitor	
RAIDProviderAgent	CIMOM Provider	
securityservice	Authentication and Authorization	
snmpd	SNMP Server Daemon	
SoftwareUpdateProviderAgent	CIMOM Provider	
srg	Survivable Remote Gateway Service	Yes
srp	IVR Service	Yes
ssba	System Set Based Admin service	Yes
sshd	Secure Shell Daemon	
SyslogListener	Syslog Receiver	
tmwservice	Time service	
ToneSrvr	Tone Server	
utps	UniSTIM Terminal Proxy Server	Yes
voicemail	Voice Mail Process	Yes
Wan	WAN Service	Yes

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx

Default Schedule

The default interval for this script is 12 minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the HealthCheck job fails. The default is 5.
Raise event if services are not available?	Select **Yes** to raise an event if any monitored service is not available. The default is Yes.
Event severity when services are not available	Set the severity level, from 1 to 40, to indicate the importance of an event in which a monitored service is not available. The default is 10.
Monitor Key Service Availability	
Event Notification	
Raise event if key service availability falls below threshold?	Select **Yes** to raise an event if the percentage of key service availability falls below the threshold that you set. The default is Yes.
Threshold - Minimum key service availability	Specify the lowest percentage of key service availability that can occur before an event is raised. The default is 100%.
Event severity when key service availability falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of key service availability falls below the threshold. The default is 10.
Data Collection	
Collect data for key service availability?	Select **Yes** to collect data about key service availability for reports and graphs. The default is unselected.

HuntGroupUsage

Use this Knowledge Script to monitor call statistics for one or more hunt groups: busy percentage, abandoned percentage, average time in queue, and overflow percentage. This script raises an event if any monitored value exceeds the threshold that you set. In addition, this script generates data streams for percentage of abandoned calls, percentage of busy calls, overflow percentage, average time in queue, total calls, and total answers.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx_HuntGroup

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the HuntGroupUsage job fails. The default is 5.
Monitor Abandoned Percentage	
Event Notification	
Raise event if abandoned percentage exceeds threshold?	Select **Yes** to raise an event if the percentage of abandoned calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum abandoned percentage	Specify the highest percentage of abandoned calls that can occur before an event is raised. The default is 5%.
Event severity when abandoned percentage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of abandoned calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for abandoned percentage?	Select **Yes** to collect data about the percentage of abandoned calls for reports and graphs. The default is unselected.
Monitor Busy Percentage	
Event Notification	

Description	How To Set It
Raise event if busy percentage exceeds threshold?	Select **Yes** to raise an event if the percentage of busy calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy percentage	Specify the highest percentage of busy calls that can occur before an event is raised. The default is 5%.
Event severity when busy percentage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of busy calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for busy percentage?	Select **Yes** to collect data about the percentage of busy calls for reports and graphs. The default is unselected.
Monitor Overflow Percentage	
Event Notification	
Raise event if overflow percentage exceeds threshold?	Select **Yes** to raise an event if the percentage of overflow calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum overflow percentage	Specify the highest percentage of overflow calls that can occur before an event is raised. The default is 25%.
Event severity when overflow percentage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of overflow calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for overflow percentage?	Select **Yes** to collect data about the percentage of overflow calls for reports and graphs. The default is unselected.
Monitor Average Time in Queue	
Event Notification	
Raise event if average time in queue exceeds threshold?	Select **Yes** to raise an event if the average time calls spend in queue exceeds the threshold that you set. The default is Yes.
Threshold - Maximum average time in queue	Specify the longest average time that calls can spend in queue before an event is raised. The default is 45 seconds.
Event severity when average time in queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average time calls spend in queue exceeds the threshold. The default is 10.
Data Collection	
Collect data for average time in queue?	Select **Yes** to collect data about average queue time for reports and graphs. The default is unselected.
Monitor Total Calls	
Data Collection	
Collect data for total calls?	Select **Yes** to collect data about the total number of calls for reports and graphs. The default is unselected.
Monitor Total Answers	
Data Collection	
Collect data for total answers?	Select **Yes** to collect data about the total number of answered calls for reports and graphs. The default is unselected.

InterfaceHealth

Use this Knowledge Script to monitor the operational status of interfaces for a BCM. This script raises an event when interface status changes. In addition, this script generates a data stream for interface availability.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx_LANLink

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the InterfaceHealth job fails. The default is 5.
Raise event if interface goes down?	Select **Yes** to raise an event if interface status changes to “down.” The default is Yes.
Event severity when interface is down	Set the severity level, from 1 to 40, to indicate the importance of an event in which interface status changes to “down.” The default is 5.
Raise event if interface comes up?	Select **Yes** to raise an event if an interface’s status changes to “up.” The default is Yes.
Event severity when interface is up	Set the severity level, from 1 to 40, to indicate the importance of an event in which interface status changes to “up.” The default is 30.
Monitor Interface Availability	
Data Collection	
Collect data for interface availability?	Select **Yes** to collect data about interface availability for reports and graphs. If enabled, data collection returns a value of 100 if the interface is available or a value of 0 if the interface is not available. The default is unselected.

LinkUtilization

Use this Knowledge Script to monitor LAN links on a BCM. This script monitors bandwidth utilization (including inbound and outbound utilization), bytes sent and received (bytes per second since the last polling period), and percentage of packet errors.

This script raises an event when a monitored value exceeds the threshold that you set. In addition, this script generates data streams for bandwidth utilization, packet errors, outbound bandwidth utilization, inbound bandwidth utilization, sent bytes, and received bytes.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

For both modes, this script can monitor packet errors, sent bytes, and received bytes. It cannot monitor bandwidth utilization for either mode.

Resource Object

Nortel_BCMx_LANLink

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the LinkUtilization job fails. The default is 5.
Monitor Bandwidth Utilization	
Event Notification	
Raise event if bandwidth utilization exceeds threshold?	Select **Yes** to raise an event if bandwidth (inbound and outbound) utilization exceeds the threshold that you set. The default is Yes.
Threshold - Maximum bandwidth utilization	Specify the highest percentage of bandwidth utilization that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which bandwidth utilization exceeds the threshold. The default is 10.
Data Collection	
Collect data for bandwidth utilization?	Select **Yes** to collect data about inbound and outbound bandwidth utilization for reports and graphs. The default is unselected.
Monitor Packet Errors	

Description	How To Set It
Event Notification	
Raise event if packet errors exceed threshold?	Select **Yes** to raise an event if the percentage of packet errors exceeds the threshold that you set. The default is Yes. **Hint** When a packet is dropped during a VoIP transmission, a conversation can lose an entire syllable or word. Obviously, data loss can severely impair call quality. Set this parameter to **Yes** to receive immediate notification of packet loss that exceeds the threshold that you set.
Threshold - Maximum packet errors	Specify the highest percentage of packet errors that can occur before an event is raised. The default is 8%.
Event severity when packet errors exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold. The default is 10.
Data Collection	
Collect data for packet errors?	Select **Yes** to collect data about the percentage of packet errors for reports and graphs. The default is unselected.
Monitor Outbound Bandwidth Utilization	
Event Notification	
Raise event if outbound bandwidth utilization exceeds threshold?	Select **Yes** to raise an event if outbound bandwidth utilization exceeds the threshold that you set. The default is Yes.
Threshold - Maximum outbound bandwidth utilization	Specify the highest percentage of outbound bandwidth utilization that can occur before an event is raised. The default is 50%.
Event severity when outbound bandwidth utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which outbound bandwidth utilization exceeds the threshold. The default is 10.
Data Collection	
Collect data for outbound bandwidth utilization?	Select **Yes** to collect data about the percentage of outbound bandwidth utilization for reports and graphs. The default is unselected.
Monitor Inbound Bandwidth Utilization	
Event Notification	
Raise event if inbound bandwidth utilization exceeds threshold?	Select **Yes** to raise an event if inbound bandwidth utilization exceeds the threshold that you set. The default is Yes.
Threshold - Maximum inbound bandwidth utilization	Specify the highest percentage of inbound bandwidth utilization that can occur before an event is raised. The default is 50%.
Event severity when inbound bandwidth utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which inbound bandwidth utilization exceeds the threshold. The default is 10.
Data Collection	
Collect data for inbound bandwidth utilization?	Select **Yes** to collect data about the percentage of inbound bandwidth utilization for reports and graphs. The default is unselected.
Monitor Bytes Sent	
Data Collection	
Collect data for bytes sent?	Select **Yes** to collect data about the number of bytes sent per second for reports and graphs. The default is unselected.

Description	How To Set It
Monitor Bytes Received	
Data Collection	
Collect data for bytes received?	Select **Yes** to collect data about the number of bytes received per second for reports and graphs. The default is unselected.

LogicalDiskSpace

Use this Knowledge Script to monitor logical disk space usage and availability. This script raises an event when any monitored value exceeds a threshold that you set. In addition, this script generates data streams for used disk space and available disk space.

Resource Object

Nortel_BCMx_LogicalDisk

The LogicalDiskSpace Knowledge Script is a member of the NortelBCMx Recommended Knowledge Script Group (KSG), which allows you to run all recommended scripts at one time. However, there are limits on the number of Logical Disk objects on which the LogicalDiskSpace script can run. If you run the KSG on more objects than the LogicalDiskSpace script allows, you will receive an error message indicating that the number of target objects has exceeded its limit. If you receive this error message, remove the LogicalDiskSpace script from the KSG and run LogicalDiskSpace alone on fewer Logical Disk resources.

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the LogicalDiskSpace job fails. The default is 5.
Monitor Used Disk Space	
Event Notification	
Raise event if used disk space exceeds threshold?	Select **Yes** to raise an event if the amount of used disk space exceeds the threshold that you set. The default is Yes.
Threshold - Maximum used disk space	Specify the highest percentage of disk space that can be used before an event is raised. The default is 80%.
Event severity when used disk space exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which used disk space exceeds the threshold. The default is 10.
Data Collection	
Collect data for used disk space?	Select **Yes** to collect data about used disk space for reports and graphs. The default is unselected.
Monitor Available Disk Space	
Event Notification	
Raise event if available disk space falls below threshold?	Select **Yes** to raise an event if available disk space falls below the threshold that you set. The default is Yes.

Description	How To Set It
Threshold - Minimum available disk space	Specify the lowest amount of disk space that can be available before an event is raised. The default is 10 MB.
Event severity when available disk space falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which available disk space falls below the threshold. The default is 10.
Data Collection	
Collect data for available disk space	Select **Yes** to collect data about available disk space for reports and graphs. The default is unselected.

PSTNFallback

Use this Knowledge Script to monitor the number of PSTN (Public Switched Telephone Network) fallback attempts and failures that have occurred since the last polling period. Attempts are calls that were not able to route through the preferred trunk. Failures are calls that were not able to route through the fallback trunk.

This script raises an event when any monitored value exceeds a threshold that you set. In addition, this script generates data streams for PSTN fallback attempts and failures.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx_TelephonyFolder

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the PSTNFallback job fails. The default is 5.
Monitor PSTN Fallback Attempts	
Event Notification	
Raise event if PSTN fallback attempts exceed threshold?	Select **Yes** to raise an event if the number of fallback attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum PSTN fallback attempts	Specify the highest number of fallback attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when PSTN fallback attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of fallback attempts exceeds the threshold. The default is 20.
Data Collection	
Collect data for PSTN fallback attempts	Select **Yes** to collect data about the number of fallback attempts for reports and graphs. The default is unselected.
Monitor PSTN Fallback Failures	
Event Notification	

Description	How To Set It
Raise event if PSTN fallback failures exceed threshold?	Select **Yes** to raise an event if the number of fallback failures exceeds the threshold that you set. The default is Yes.
Threshold - Maximum PSTN fallback failures	Specify the highest number of fallback failures that can occur before an event is raised. The default is 0 failures.
Event severity when PSTN fallback failures exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of fallback failures exceeds the threshold. The default is 10.
Data Collection	
Collect data for available PSTN fallback failures	Select **Yes** to collect data about the number of fallback failures for reports and graphs. The default is unselected.

QoSLog

Use this Knowledge Script to monitor the MOS estimates for several codecs: G.711a, G.711u, G.723 5.3 kbps, G.723 6.3 kbps, and G.729 and G.729A (in the outgoing call direction only). This script raises an event if any MOS estimate falls below the threshold you set. In addition, this script generates data streams for MOS estimates for each monitored codec.

If you use VoIP trunks, run this script to gather information from the BCM QoS Monitor log in order to verify that QoS between target BCMs is maintaining acceptable MOS. For more information, see "Understanding the Mean Opinion Score" on page 43.

Prerequisite

Enable the QoS Monitor to log MOS scores. For more information, see "Enabling QoS Monitor" on page 42.

Resource Object

Nortel_BCMx_TelephonyFolder

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QOSLog job fails. The default is 5.
Raise event if QoS monitor is not running from device?	Select **Yes** to raise an event if QoS Monitor is not running. The default is Yes. The QoS Monitor must be running in order to log the MOS scores this script monitors.
Event severity when QoS monitor is not running from device	Set the severity level, from 1 to 40, to indicate the importance of an event in which QoS Monitor is not running. The default is 5.
Monitor G.711a MOS	
Event Notification	
Raise event if G.711a MOS falls below threshold?	Select **Yes** to raise an event if the MOS for the G.711a codec falls below the threshold that you set. The default is Yes.
Threshold - Minimum G.711a MOS	Specify the lowest MOS that can occur before an event is raised. The default is 3.60.
Event severity when G.711a MOS falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS falls below the threshold. The default is 5.
Data Collection	

Description	How To Set It
Collect data for G.711a MOS?	Select **Yes** to collect data about G.711a MOS for reports and graphs. The default is unselected.
Monitor G.711u MOS	
Event Notification	
Raise event if G.711u MOS falls below threshold?	Select **Yes** to raise an event if the MOS for the G.711u codec falls below the threshold that you set. The default is Yes.
Threshold - Minimum G.711u MOS	Specify the lowest MOS that can occur before an event is raised. The default is 3.60.
Event severity when G.711u MOS falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS falls below the threshold. The default is 5.
Data Collection	
Collect data for G.711u MOS?	Select **Yes** to collect data about G.711u MOS for reports and graphs. The default is unselected.
Monitor G.723 5.3 kbps MOS	
Event Notification	
Raise event if G.723 5.3 kbps MOS falls below threshold?	Select **Yes** to raise an event if the MOS for the G.723 5.3 kbps codec falls below the threshold that you set. The default is Yes.
Threshold - Minimum G.723 5.3 kbps MOS	Specify the lowest MOS that can occur before an event is raised. The default is 3.60.
Event severity when G.723 5.3 kbps MOS falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS falls below the threshold. The default is 5.
Data Collection	
Collect data for G.723 5.3 kbps MOS?	Select **Yes** to collect data about G.723 5.3 kbps MOS for reports and graphs. The default is unselected.
Monitor G.723 6.3 kbps MOS	
Event Notification	
Raise event if G.723 6.3 kbps MOS falls below threshold?	Select **Yes** to raise an event if the MOS for the G.723 6.3 kbps codec falls below the threshold that you set. The default is Yes.
Threshold - Minimum G.723 6.3 kbps MOS	Specify the lowest MOS that can occur before an event is raised. The default is 3.60.
Event severity when G.723 6.3 kbps MOS falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS falls below the threshold. The default is 5.
Data Collection	
Collect data for G.723 6.3 kbps MOS?	Select **Yes** to collect data about G.723 6.3 kbps MOS for reports and graphs. The default is unselected.
Monitor G.729 MOS	
Event Notification	
Raise event if G.729 MOS falls below threshold?	Select **Yes** to raise an event if the MOS for the G.729 codec falls below the threshold that you set. The default is Yes.
Threshold - Minimum G.729 MOS	Specify the lowest MOS that can occur before an event is raised. The default is 3.60.

Description	How To Set It
Event severity when G.729 MOS falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS falls below the threshold. The default is 5.
Data Collection	
Collect data for G.729 MOS?	Select **Yes** to collect data about G.729 MOS for reports and graphs. The default is unselected.
Monitor G.729A MOS	
Event Notification	
Raise event if G.729A MOS falls below threshold?	Select **Yes** to raise an event if the MOS for the G.729A codec falls below the threshold that you set. The default is Yes.
Threshold - Minimum G.729A MOS	Specify the lowest MOS that can occur before an event is raised. The default is 3.60.
Event severity when G.729A MOS falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS falls below the threshold. The default is 5.
Data Collection	
Collect data for G.729A MOS?	Select **Yes** to collect data about G.729A MOS for reports and graphs. The default is unselected.

Enabling QoS Monitor

If you use VoIP trunks, enable QoS Monitor in BCM before running the QoSLog Knowledge Script.

To enable QoS Monitor:

1. Log in to Element Manager.
2. On the Administration tab, expand **System Metrics** (for BCM 50 devices) or **System Status** (for BCM 4.0 devices), and then select **QoS Monitor**.
3. From the **Monitoring mode** list, select **Enabled in QoS-Monitor mode**.

For more information about VoIP trunks, see the "VoIP trunk gateways" chapter of the *Networking Configuration Guide* for your BCM device. For information about enabling the QoS Monitor, see the *Administration Guide* for your BCM device.

Understanding Codecs

In a VoIP transmission, the codec samples the sound and determines the data rate. A codec converts analog signals to digital (outbound) and digital signals to analog (inbound) for voice transmissions, and compresses (outbound) and decompresses (inbound) the digital information.

If you use VoIP trunks, use the QoSLog Knowledge Script to monitor the Mean Opinion Score (MOS) for six codec types. For more information, see "Understanding the Mean Opinion Score" on page 43.

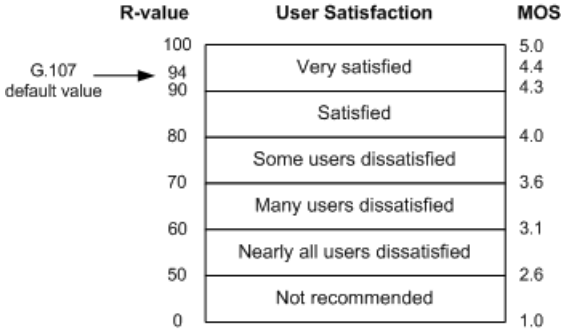
Codec	Description
G.711a	ITU standard for H.323-compliant codecs. Uses the A-law for companding, a popular standard in Europe.
G.711u	ITU standard for H.323-compliant codecs. Uses the U-law for companding, the most frequently used method in North America.

Codec	Description
G.723-5.3 kbps	Dual-rate speech codec for multimedia communications transmitting at 5.3 kbps. Uses the conjugate structure algebraic code excited linear predictive compression (ACELP) algorithm.
G.723-6.3 kbps	Dual-rate speech codec for multimedia communications transmitting at 6.3 kbps. Uses the multipulse maximum likelihood quantization (MPMLQ) compression algorithm.
G.729	High-performing codec that offers compression with high quality.
G.729A	Less-complex version of the G.729 codec. Developed for simultaneous voice and data applications for which the G.729 codec was too complex. Speech quality is virtually indistinguishable between G.729 and G.729A.

Understanding the Mean Opinion Score

The Mean Opinion Score (MOS) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. A modified version of the ITU (International Telecommunications Union) G.107 standard E-model equation is used to calculate the MOS. This algorithm is used to evaluate the quality of a transmission by factoring in the "mouth to ear" characteristics of a speech path.

The E-model is a complex calculation, the output of which is a single score called an R-value that is derived from delays and equipment impairment factors. An R-value can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor). As shown below, an estimated MOS can be calculated directly from an R-value:



SystemUpTime

Use this Knowledge Script to monitor the number of seconds that the BCM has been operational since its last reboot. This script raises an event if the system has rebooted. In addition, this script generates a data stream for system availability.

You want to be informed when your BCM has been rebooted. While a BCM is rebooting, calls are not going through. Knowing that the BCM has been rebooted can help prepare you for calls from disgruntled users whose calls were incomplete.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the SystemUpTime job fails. The default is 5.
Raise event if system has rebooted?	Select **Yes** to raise an event if the BCM has been rebooted. The default is Yes.
Event severity when system has rebooted	Set the severity level, from 1 to 40, to indicate the importance of an event in which the BCM has been rebooted. The default is 10.
Monitor System Up Time	
Data Collection	
Collect data for system up time?	Select **Yes** to collect data about system up time (number of seconds that the BCM has been powered on or since its last reboot) for reports and graphs. The default is unselected.

SystemUsage

Use this Knowledge Script to monitor the total CPU usage and memory usage for the BCM. This script raises an event when any monitored value exceeds a threshold that you set. In addition, this script generates data streams for CPU usage and memory usage.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the SystemUsage job fails. The default is 5.
Monitor CPU Usage	
Event Notification	
Raise event if CPU usage exceeds threshold?	Select **Yes** to raise an event if CPU usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum CPU usage	Specify the highest CPU usage that can occur before an event is raised. The default is 80%.
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 10.
Data Collection	
Collect data for CPU usage?	Select **Yes** to collect data about CPU usage for reports and graphs. The default is unselected.
Monitor Memory Usage	
Event Notification	
Raise event if memory usage exceeds threshold?	Select **Yes** to raise an event if memory usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum memory usage	Specify the highest memory usage that can occur before an event is raised. The default is 80%.
Event severity when memory usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. The default is 10.

Description	How To Set It
Data Collection	
Collect data for memory usage?	Select **Yes** to collect data about memory usage for reports and graphs. The default is unselected.

UPSHealth

Use this Knowledge Script to monitor an attached uninterruptible power supply (UPS) for changes in operational status, load status, temperature status, and output and input voltage statuses, as well as temperature, load, and output and input voltage.

By warning you of changes to UPS status, this script can help you prevent outages that affect your users.

This script raises an event if a monitored status changes or if a monitored value exceeds a threshold that you set. In addition, this script generates data streams for UPS temperature, UPS load, UPS output voltage, and UPS input voltage.

Resource Object

Nortel_BCMx_UPS

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the UPSHealth job fails. The default is 5.
Raise event if UPS operational status changes?	Select **Yes** to raise an event if the UPS operational status changes. The default is unselected.
Event severity when UPS operational status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UPS operational status changes. The default is 30.
Raise event if UPS temperature status changes?	Select **Yes** to raise an event if the UPS temperature status changes. The default is unselected.
Event severity when UPS temperature status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UPS temperature status changes. The default is 30.
Raise event if UPS load status changes?	Select **Yes** to raise an event if the UPS load status changes. The default is unselected.
Event severity when UPS load status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UPS load status changes. The default is 30.
Raise event if UPS output voltage status changes?	Select **Yes** to raise an event if the UPS output voltage status changes. The default is unselected.
Event severity when UPS output voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UPS output voltage status changes. The default is 30.

Description	How To Set It
Raise event if UPS input voltage status changes?	Select **Yes** to raise an event if the UPS input voltage status changes. The default is unselected.
Event severity when UPS input voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UPS input voltage status changes. The default is 30.
Monitor Temperature	
Event Notification	
Raise event if temperature exceeds threshold?	Select **Yes** to raise an event if the UPS temperature exceeds the threshold that you set. The default is Yes.
Threshold - Maximum temperature	Specify the temperature that can occur before an event is raised. The default is 55º Celsius.
Event severity when temperature exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the temperature exceeds the threshold. The default is 10.
Data Collection	
Collect data for temperature?	Select **Yes** to collect data about temperature for reports and graphs. The default is unselected.
Monitor Load	
Event Notification	
Raise event if load exceeds threshold?	Select **Yes** to raise an event if the UPS load exceeds the threshold that you set. The default is unselected.
Threshold - Maximum load	Specify the highest percentage of load that can occur before an event is raised. The default is 80%.
Event severity when load exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which load exceeds the threshold. The default is 10.
Data Collection	
Collect data for load?	Select **Yes** to collect data about load for reports and graphs. The default is unselected.
Monitor Output Voltage	
Event Notification	
Raise event if output voltage exceeds or falls below threshold?	Select **Yes** to raise an event if the output voltage level exceeds or falls below the thresholds that you set. The default is unselected.
Upper threshold	Select **Enable** to use an upper threshold value. The default is Enable.
Threshold - Maximum output voltage	Specify the highest output voltage that can occur before an event is raised. The default is 130 volts.
Event severity when output voltage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which output voltage exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is Enable.
Threshold - Minimum output voltage	Specify the lowest output voltage that can occur before an event is raised. The default is 100 volts.
Event severity when output voltage falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which output voltage falls below the threshold. The default is 10.
Data Collection	

Description	How To Set It
Collect data for output voltage?	Select **Yes** to collect data about output voltage for reports and graphs. The default is unselected.
Monitor Input Voltage	
Event Notification	
Raise event if input voltage exceeds or falls below threshold?	Select **Yes** to raise an event if the input voltage level exceeds or falls below the thresholds that you set. The default is unselected.
Upper threshold	Select **Enable** to use an upper threshold value. The default is Enable.
Threshold - Maximum input voltage	Specify the highest input voltage that can occur before an event is raised. The default is 130 volts.
Event severity when input voltage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which input voltage exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is Enable.
Threshold - Minimum input voltage	Specify the lowest input voltage that can occur before an event is raised. The default is 100 volts.
Event severity when input voltage falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which input voltage falls below the threshold. The default is 10.
Data Collection	
Collect data for input voltage?	Select **Yes** to collect data about input voltage for reports and graphs. The default is unselected.

Recommended Knowledge Script Group

The following Knowledge Scripts in the AppManager for Nortel BCMx module are members of the NortelBCMx recommended Knowledge Script Group (KSG).

- Alarms (Configure your Nortel BCM to send SNMP traps to AppManager before using this script. For more information, see "Identifying the SNMP Trap Receiver" on page 14).
- ChassisUsage
- HealthCheck
- InterfaceHealth
- LogicalDiskSpace
- SystemUpTime
- SystemUsage

You can find the NortelBCMx KSG on the RECOMMENDED tab of the Knowledge Script pane of the Operator Console.

All the scripts in the KSG have their parameters set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab, and then run the NortelBCMx group on a Nortel BCMx resource.

Run the KSG from the Master view, not the NortelBCMx view. In order to use the Discovery_NortelBCMx Knowledge Script in a monitoring policy, the view must include root objects, which are not visible in the NortelBCMx view.

The NortelBCMx KSG enables a "best practices" usage of AppManager for monitoring your Nortel BCM environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView. For more information, see "About Policy-Based Monitoring" in the AppManager Help.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the NortelBCMx tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the NortelBCMx tab are not affected.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the NortelBCMx KSG and want to restore it to its original form, you can reinstall AppManager for Nortel BCMX on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\NortelBCMx` directory.

Discovery_NortelBCMx

Use this Knowledge Script to discover resource and configuration information for Nortel BCM software version 4.0 and hardware models 50, 50a, 50e, 200, 400, and 1000.

AppManager for Nortel BCMx provides limited support for Survivable Remote Gateway (SRG) mode and local mode with the Alarms, CallByCallLimits, ChassisUsage, HealthCheck, HuntGroupUsage, InterfaceHealth, LinkUtilization, PSTNFallback, SystemUpTime, and SystemUsage Knowledge Scripts. For more information, see the Help for those scripts.

Prerequisite

Configure your BCM user name and password into AppManager Security Manager. The discovery process will fail if it cannot access this vital information. For more information, see "Configuring the BCM User Name and Password" on page 8.

Resource Object

NT_MachineFolder

Default Schedule

By default, this script runs once a week on Sunday at 3 A.M.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the Discovery_NortelBCMx job fails. The default is 5.
Raise event if discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **Yes** to raise an event when the job succeeds. The default is unselected.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Raise event if discovery fails?	Select **Yes** to raise an event if discovery fails to find Nortel BCMx resources. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails to find Nortel BCMx resources. The default is 5.
Raise event if Nortel BCMx agent not installed?	Select **Yes** to raise an event if the Nortel BCMx managed object is not installed. The default is Yes.
Event severity when Nortel BCMx agent not installed	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the Nortel BCMx managed object is not installed. The default is 15.
Discover Nortel BCMx Devices	

Parameter	How To Set It
List of Nortel BCMx devices	Use this parameter if you have only a few Nortel BCM devices to discover. Type a list of the devices for which you want to discover resources. Use a comma to separate the names or IP addresses in the list. For example: `10.0.1.1,10.0.4.1`
List of Nortel BCMx device ranges	Use this parameter if you have only a few ranges of Nortel BCM devices to discover. Type a list of IP address ranges (up to 256 addresses) of the devices for which you want to discover resources. Only numbers, dashes, periods, and commas are allowed in the list. Use dashes to define a range. For example: `10.0.1.1-10.0.1.50,10.0.4.51-10.0.4.100`
Full path to file with list of Nortel BCMx devices	Instead of typing each Nortel BCM device separately, you can use this parameter to specify the full path to a file on the agent computer that contains a device name on each line of the file.