

SNMPc Release 7.0

Disaster Recovery Support

Castle Rock Computing

March, 2004

Overview

Communication networks have become an indispensable part of modern enterprises. Employee and customer interaction, technical support, marketing, sales and procurement activities are all highly dependent on an efficient and reliable network infrastructure. With this increasing reliance on data communications, monitoring your network infrastructure has become more important than ever. You can't afford to lose network management capabilities because of a computer power, hardware, or software failure.

This release of SNMPc introduces the important function of a redundant backup server for disaster recovery. By using two SNMPc servers with one designated as a Primary and the other as Backup server you can continue monitoring your network if the Primary system is disabled for any reason. The redundant server feature includes the following important elements:

- Simple and quick setup
- Automatic export of configurations
- Works with multiple remote pollers
- Doesn't repeatedly toggle polling between servers

After a straightforward and quick setup procedure, the Primary SNMPc server will automatically export its configuration files to the Backup server on a scheduled basis. It's important to do this automatically so that the Backup server is always up to date.

When the Backup server detects a failure of the Primary server it will take over all polling of the network, including instructing any remote polling agents to reconnect to the Backup server.

After Backup server takeover, the problem associated with the Primary server must be investigated and resolved by a human operator. To prove stability it may be desirable to run the Primary server in a testing phase for a period of time. For this reason it's important that the Backup server retain its control over polling and not revert automatically to the Primary server as soon as it is running again. Otherwise it is possible for the Primary and Backup servers to repeatedly exchange the network polling role. Reverting control to the Primary server is accomplished with a simple command at the Backup server console.

With the introduction of redundant backup server functionality, SNMPc 7.0 is an important part of your enterprise disaster recovery plan, ensuring uninterrupted network management and monitoring in the face of any unforeseen circumstance.

The remainder of this section introduces other important new functions you can perform with SNMPc 7.0.

Customize TCP Service Polling

Create an unlimited number of custom TCP service polling descriptors with a unique send string and expected reply pattern matching string. Each descriptor can work with different TCP ports or with different applications servers running at the same TCP port.

Monitor up to 16 different custom TCP services for each map object in addition to the connect-only TCP ports of earlier SNMPc versions (Web, Ftp, Sntp, Telnet, User1-4).

Display all TCP service polling information in a single table indexed by the service name. Create web reports for all polled services in a single trend report indexed by service name.

Quickly Manage Event Action Filters

Directly add or change an event action filter using the right-click menus for the selected event log view entry. Removes the need to locate the appropriate trap in the Event Selection tree.

Support event action filters for traps that are not fully defined in compiled mibs. Removes the need to locate and import an exactly matching mib, which simplifies event configuration in the case of mib source errors, new device software versions, and unsupported (legacy) devices.

Enhance User Security

Disable console login after repeated failed login attempts to inhibit programmatic “cracking” of user names and passwords.

Set an expiration period for user passwords, after which time they become disabled and must be changed by the user.

Optionally disable remote login of the Administrator user.

Generate events for login/logout and failed login actions.

Track Map Editing Activities

Generate events when objects are added, removed, or changed by the discovery process or by console users. Shows information about the object, the user and what system address the action came from.

Redundant Backup Server

Operational Procedures

The redundant backup server functionality is mostly implemented externally to the main SNMPc components in a new module named *bkserv.exe*. This module runs on the primary and backup servers and also at any remote poller systems. This module is referenced in the *Config/Software Startup* dialog and is started and stopped along with other SNMPc components.

Each snmpc system performs a different procedure as described in the following sections.

Primary Server

The primary server is responsible only for exporting database files to the backup server.

Database export is done as a side-effect of a file backup operation. Normally you would use scheduled daily backups to ensure that the backup server is always up-to-date. However, after making important changes you can use the *File/Backup* command to activate an immediate export.

The export procedure will start up to several minutes after the local backup is complete. The backed-up database files are compressed and transferred to the Backup server into the directory *bkserv-incoming*.

*Please note that the **trend report samples** database, **exported web reports** and **event log** database are **not exported** to the backup server.*

The primary server generates local events (History Info events) each time it performs a database export to the backup server.

Backup Server

The backup server is responsible for loading the exported database files and for monitoring the status of the primary server.

After an export operation has completed, the backup server will automatically perform a *File/Restore* operation from the *bkserv-incoming* directory. If you are using the console you will notice that some windows are closed and others refreshed when this occurs.

You can use the backup server for viewing device snmp information. However if you add or change any map objects, these changes will be lost the next time the exported primary database files are loaded. While the backup server is in the passive (monitoring the primary server) mode it will not poll map objects.

The backup server will poll the primary server at intervals you specify in the *Config/Backup-Restore* dialog. If a poll fails for the specified number of attempts, the backup server will take over polling of map objects by enabling the *Enable Status Polling* and *Enable Service Polling* settings in the *Config/Discovery-Polling Agents* dialog.

Once the backup server is polling map objects it will no longer monitor the primary server. The backup server will not automatically relinquish its polling role when the primary server starts running again. This behavior assures that the polling role does not repeatedly toggle between primary and backup servers in the case where the primary server is failing intermittently.

The backup server generates local events whenever it loads exported database (History Info events), when any polls of the primary server fail (Warning events), and when polling is taken over from the primary server (Error event).

Remote Polling Agent

Remote polling agents are responsible for polling map objects and reporting status changes to the primary or backup server, depending on which server currently has the polling role.

When first started, each remote polling agent will connect to the primary server and acquire the address of the backup server, if any. Thereafter the polling agent will query the backup server at timed intervals to determine if it has taken over the polling role. If so, the polling agent will disconnect from the primary server and connect to the backup server.

If the backup server is polling objects then any remote polling agents will connect only to the backup server and send status change events only to the backup server. Therefore, if both the primary and backup servers are set to poll objects then no status events will go to the primary server from any remote polling agents.

Once connected to the backup server, remote polling agents continue to query the polling state of the server. If the polling state is disabled on the backup server then the polling agents will disconnect and reconnect to the primary server.

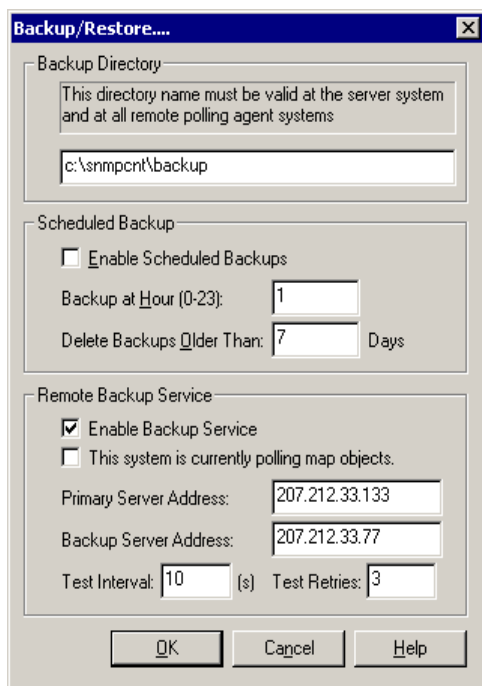
Remote polling agents send events to both the primary and backup server whenever they disconnect and reconnect from one system to another.

System Configuration

The following preconditions must exist before configuring the redundant backup server functionality:

- The password for the *Administrator* and *Remote Poller* users must be the same on both systems.
- There must be an available communication path between both systems and from each system to any remote polling agents you are using.

Use the ***Config/Backup-Restore*** menu to configure redundant backup server functionality on both the primary and backup servers. The following image of this dialog shows the new settings in the *Remote Backup Service* section.



The screenshot shows the 'Backup/Restore....' dialog box. It has three main sections: 'Backup Directory', 'Scheduled Backup', and 'Remote Backup Service'. The 'Backup Directory' section has a text box containing 'c:\snmpent\backup'. The 'Scheduled Backup' section has a checkbox for 'Enable Scheduled Backups' which is unchecked, and two text boxes for 'Backup at Hour (0-23):' (value 1) and 'Delete Backups Older Than:' (value 7) Days. The 'Remote Backup Service' section has a checked checkbox for 'Enable Backup Service', an unchecked checkbox for 'This system is currently polling map objects.', and three text boxes: 'Primary Server Address:' (207.212.33.133), 'Backup Server Address:' (207.212.33.77), and 'Test Interval:' (10) (s) 'Test Retries:' (3). At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Use the ***Enable Backup Service*** checkbox to enable or disable database export (primary server) and primary server monitoring (backup server). This check box must be enabled on both systems.

Use the ***This system is currently polling map objects*** checkbox to enable or disable map object status polling at the server you are logged on to. This checkbox is usually enabled at the primary server and disabled at the backup server.

When the backup server determines that the primary is down, it will take over polling of all map devices by automatically setting this checkbox on. Once you have resolved the problem at the primary Server, disable this checkbox at the backup system to revert to the normal state.

Note that the ***This system is currently polling map objects*** checkbox is just a shorthand convenience for the *Enable Status Polling* setting in the *Discovery/Polling Agent* dialog.

Use the ***Primary Server Address*** and ***Backup Server Address*** edit boxes to set the IP address, in dot notation, of the corresponding server systems. These settings must be the same on both systems.

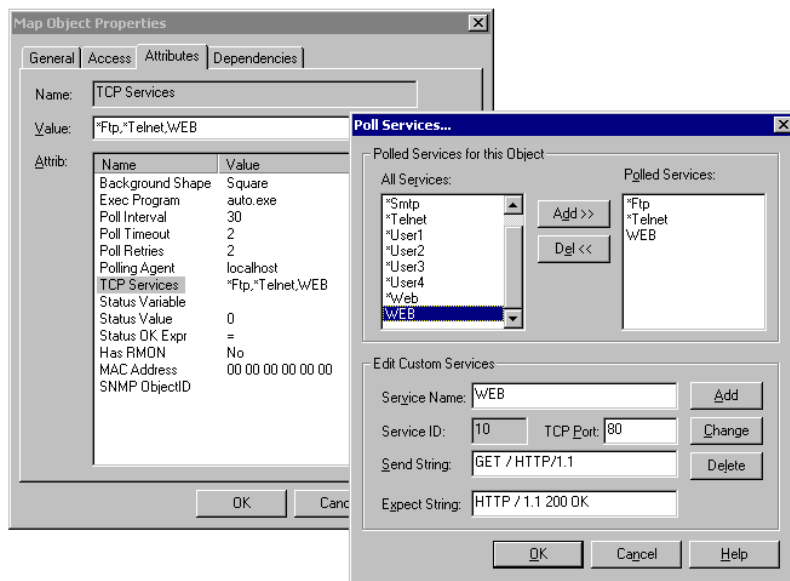
Use the ***Test Interval*** and ***Test Retries*** edit boxes to set the time between checks of the primary server by the backup server and how many times to retry before taking over polling.

Custom TCP Service Polling

Custom TCP Service polling has been introduced to allow more flexible and powerful polling of your application servers. Custom TCP Service polling has the following features:

- You can optionally send a text string to the TCP service and compare the reply to a text pattern (ASCII and “*” characters).
- Each map object can poll up to 16 different Custom TCP Services, along with the 8 connect-only services used in earlier versions of SNMPc (Web, Telnet, Ftp, Smt, User1, User2, User3, User4).
- There is no limit on the total number of Custom TCP Service descriptors that can be created.

Custom TCP Services are set by editing the new *TCP Services* map object attribute. This attribute replaces the multiple *HasSVC* attributes used in earlier versions of SNMPc. Double-clicking on this attribute shows the new *Poll Services* dialog as follows:

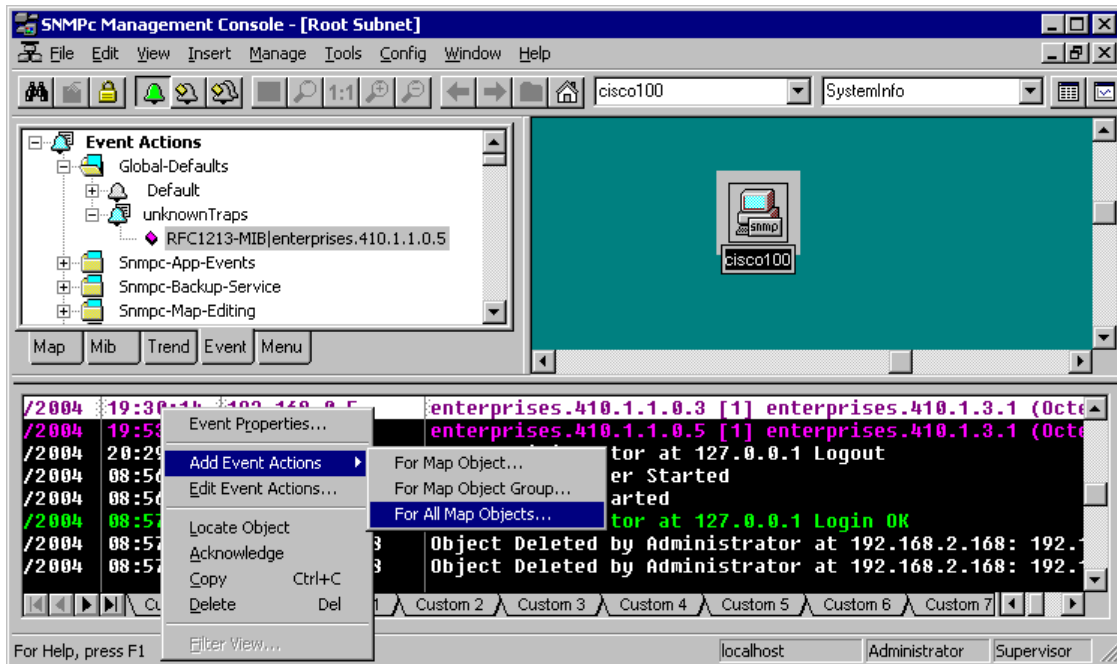


Use the *Poll Services* dialog to add and change Custom TCP Service descriptors and to select which services are polled for the selected map object. For backwards compatibility the connect-only services supported in previous versions of SNMPc are included and shown with a “*” prefix in the service name.

Note: In this release of SNMPc, discovery support for Custom TCP Services has not been added. The discovery agent continues to support only the connect-only services from earlier releases of SNMPc (Web, Ftp, Telnet, Smt, User1-4).

Simplified Editing of Event Filters

New commands have been added to the event view window right-click menu to edit event action filters. The following image shows these new commands and also the new *unknownTraps* trap type that is used to match undefined traps:



Use the *Edit Event Action* command to edit an existing filter that matched the event. Note that the matching filter might be a global one and you might prefer to add a new filter if you want to change actions for a specific node or trap parameters.

Use the one of three *Add Event Actions* commands to create a new matching filter and set the actions. This command will create one of three filter types to match (1) all nodes; (2) the node in the event; or (3) all nodes with the same Group as the node in the event. In most cases you should set additional matching parameters in the Match tab of the Event Filter dialog.

The *Add Event Actions* command tries to add a filter for traps that don't have full definitions compiled in. This feature uses a new generic trap type under the "Global-Defaults" event subtree named "unknownTrap". For better results you may wish to import the correct mibs before adding event action filters so that they are placed in the proper enterprise-specific subtrees.

You can now also set a specific email address in the *Email Action* of the *Event Actions* dialog box. This removes the need to create different users and user groups to support an ad-hoc email recipient.

User Security Enhancements

Maximum Login Attempt Retries

Repeated failed login attempts will lock out further attempts for a particular user name for one minute. This inhibits programmatic guessing of usernames and passwords. The maximum number of attempts is set in the *MaxLoginRetry* setting of the *[SNMPcConfig]* section in *snmpc.ini*. The default is 5 attempts.

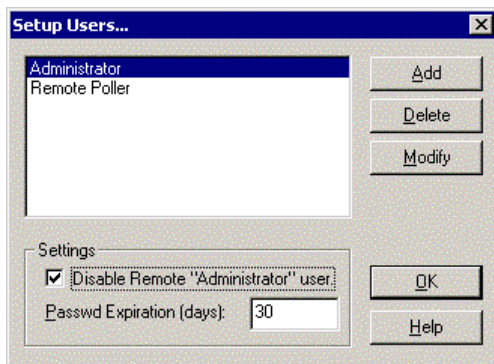
Disabling Remote Administrator User

An option has been added to the “Config/Setup Users” dialog to disable remote login of the Administrator user. Since this user name can not be removed, it is more secure to use it only for login at the server computer. A new admin level user can be created for remote users, in which case an intruder needs to correctly guess both the user name and the password.

Password Expiration

A password expiration feature has been added to the “Config/Setup Users” dialog. This is a global setting for all custom user names. Password expiration is not used for the “Administrator” user, which is another good reason to disable remote login of this user name. After a login action the user is warned of password expiration in each of the seven days prior to expiration. Changing the global expiration days will reset the expiration of all users. Otherwise, the expiration for individual users is reset when the user password changes.

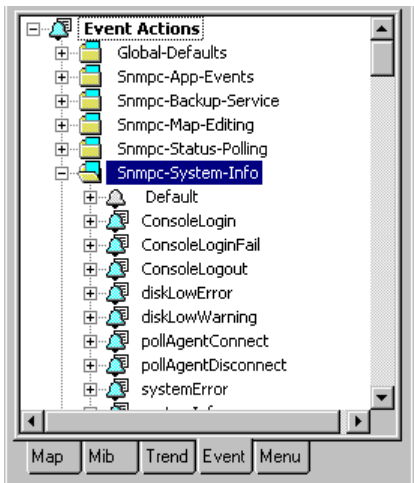
The updated “Setup Users” dialog is shown below:



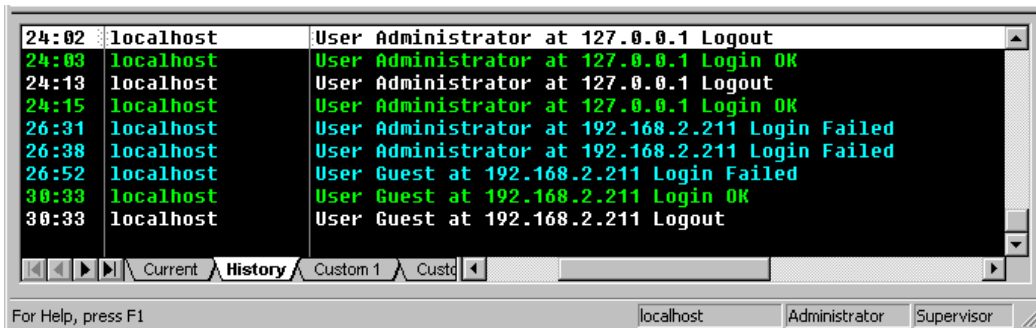
User Login/Logout Events

New events have been added for user login/logout actions. These events include the username, console address, login action and result. Login/Logout events are only generated once for each console computer (first login and last logout).

The following shows the new event filters section for these events:



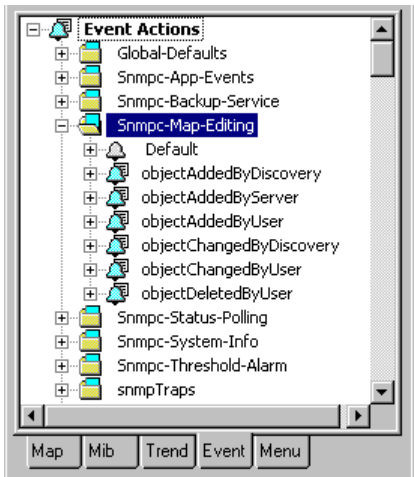
The following image shows an example of some map editing events:



Map Editing Events

New events have been added for map editing actions by the discovery engine or users. These events include the username, console address, object name, type, and map record number for easy correlation with the map or ODBC exported databases.

The following shows the new event filters section (all info events by default) for these events:



The following image shows an example of some map editing events:

