Service Response Monitor

User Guide

Release 5.8.2

ca technologies

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products:

- CA eHealth®
- CA Embedded Entitlements Manager (CA EEM)
- CA IT Asset Manager (CA ITAM)
- CA IT Client Manager (CA ITCM)
- CA Network and Systems Management (CA NSM)
- CA Patch Manager
- CA Server Automation
- CA Service Desk Manager (CA SDM)
- CA Spectrum®
- CA SystemEDGE
- CA Systems Performance for Infrastructure Managers
- CA Virtual Assurance for Infrastructure Managers
- CA Software Delivery

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction

This section contains the following topics:

Scope

This guide explains how to install, configure, and use the CA Virtual Assurance Service Response Monitoring Application Insight Module (SRM AIM).

The guide describes step-by-step test configurations of the AIM.

Audience

This guide is intended for administrators who install, configure, and use CA Virtual Assurance to manage virtual environments. It assumes that you are familiar with the operating systems used in your environment, virtualization technologies, and SNMP.

Related Publications

The CA Virtual Assurance documentation consists of the following deliverables:

Administration Guide

Explores how to administer and use CA Virtual Assurance to manage virtual resources in your environment.

Installation Guide

Contains brief architecture information, various installation methods, post-installation configuration information, and Getting Started instructions.

Online Help

Provides window details and procedural descriptions for using the CA Virtual Assurance user interface.

Reference Guide

Provides detailed information about AutoShell, CLI commands, and MIB attributes.

Performance Metrics Reference

Describes the performance metrics that are available for monitoring the systems performance of the supported platforms.

Release Notes

Provides information about operating system support, system requirements, published fixes, international support, known issues, and the documentation roadmap.

Service Response Monitoring User Guide

Provides installation and configuration details of SRM.

SystemEDGE User Guide

Provides installation and configuration details of SystemEDGE.

SystemEDGE Release Notes

Provides information about operating system support, system requirements, and features.

Conventions

This guide uses the following conventions:

Case-Sensitivity

All names of classes, commands, directives, environment parameters, functions, and properties mentioned in this guide are case-sensitive and you must spell them exactly as shown. System command and environment variable names *may* be case-sensitive, depending on your operating system's requirements.

Cross-References

References to information in other guides or in other sections in this guide appear in the following format:

Guide Name

Indicates the name of another guide.

"Chapter Name"

Indicates the name of a chapter in this or another guide.

Synonyms

Terms such as attribute, object, object identifier (OID) are synonymous to the term 'variable' in this document.

Syntax

Syntax and user input use the following form:

Italic

Indicates a variable name or placeholder for which you must supply an actual value.

{a|b}

Indicates a choice of mandatory operands, a or b.

[ ] or [[ ]]

Indicates optional operands.

Syntax Example

The following example uses these conventions:

`modify -t ZONE [-m` *`zoneserver`*`] -p` *`psetname`* `{-min` *`mincpu`*`|-max` *`maxcpu`*`} pset -session` *`ssh`*

The operands -min and -max are mandatory, but you can only use one of them depending on what you want to define, the minimum number of CPUs in the processor set or the maximum number. The operand -m is not required for this command to function. All other parts of the command must be entered as shown.

Installation Path

Install_Path used in path statements indicates the directory in which CA Virtual Assurance or components of CA Virtual Assurance are installed.

Defaults:

- Windows x86: C:\Program Files\CA
- Windows x64: C:\CA, C:\Program Files (x86)\CA, or C:\Program Files\CA
- UNIX, Linux: /opt/CA

Chapter 2: Functional Characteristics

This section contains the following topics:

Overview

The following list provides an overview about the functional characteristics of SRM.

State management

SRM fully supports the state object model of SystemEDGE. You can configure thresholds and severity for associated metrics in the configuration file.

File-based configuration, Policy configuration

You can configure SRM through Policy Configuration in CA Virtual Assurance. The Policy Configuration is file-based and provides the following warm start features:

- Supports warm start triggered by SystemEDGE when a new SRM control file is delivered.
- Allows SRM to suspend execution and reconfigure itself on-the-fly when a new configuration file is delivered.

Note: See the CA Virtual Assurance Online Help for details on how to perform Policy Configuration.

Remote deployment

All required componts to run SRM (SRM AIM, Advanced Encryption, SystemEDGE) can remotely be deployed and installed from the CA Virtual Assurance manager. See also Appendix Installation.

Legacy compatibility

SRM accepts and collects all data metrics gathered by SRM Version 2.0 or 2.1 release. SRM can use the configuration files of version 2.x. See also Appendix Installation in this guide.

Log file customization

SRM lets you configure the name, size, and number of log files.

Named tests

SRM supports tests configured with a test name that can be used for identification.

Performance optimization

Performance metrics supply real-time performance information about the functionality of the SRM AIM. You can monitor the health of the SRM AIM, either manually or through SystemEDGE. You can tune the configuration information to get the best response from SRM.

Run once

SRM supports that a test can run on request only, not through the poll interval scheduler.

SNMP-based configuration

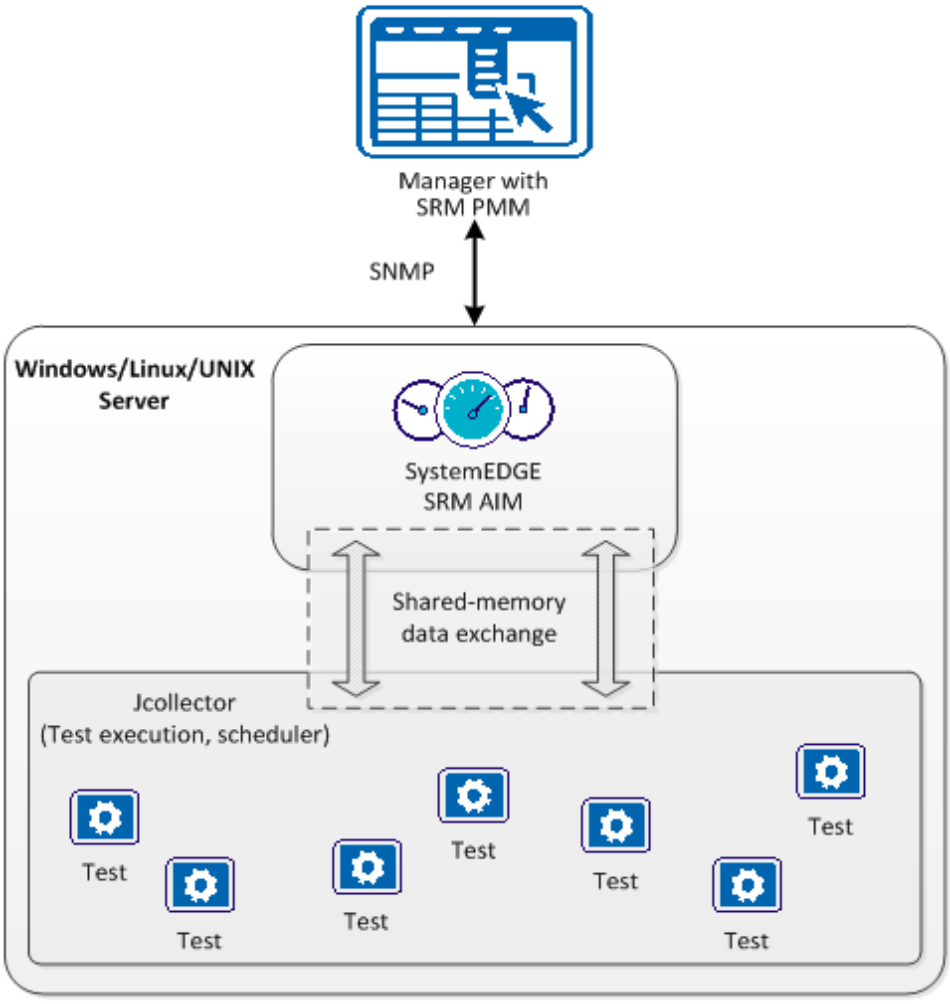
SRM supports IPv6 and SNMPv3 within its tests.

Architecture

The Service Response Monitoring Application Insight Module (SRM AIM) is a functional extension (plug-in) for SystemEDGE Version 5.0. SRM retrieves the responsiveness of a logical or physical service that runs on the local or on a remote system. SRM is Java-based and multi-threaded and handles multiple test configurations across multiple servers. SRM executes preconfigured or custom tests to measure the elapsed time and throughput of execution.

The following diagram illustrates these relationships.

Interaction Between Service Response Monitoring Components



The svcrsp.cf configuration file contains the test specifications. The SRM AIM reads this configuration file and makes the test specifications available in the shared memory segment. The SRM Jcollector component reads each test configuration from the shared memory. Jcollector executes the tests, collects the results of this timing process, and propagates the results to the SRM AIM. SystemEDGE sends these results and associated status information to CA Virtual Assurance.

Test Table Information

Useful state management of SRM requires the capability to monitor specific metrics and specify the severity of the associated monitors.

The SRM test table stores the following information:

Test Instance Name

(Optional) Specifies the Test Instance Name for the test. This name is used for state manager object information, resource instance information for performance data collection, and as an alternative to the random integer *index* as a primary key for tests which can change depending upon the templates delivered. It is optimal to have a non-NULL Test Name, but is mandatory only for file-based configuration when the configuration file has a version equal or greater than 3.0. SRM retains legacy support.

Note: This value is only writable during creation of the test. You cannot modify it afterwards, because it acts as a primary key for the table.

Service Context Info

Specifies a location to store any information a manager likes to store, such as UUID's, flags, antecedent properties of this test object, and so on. SRM does not directly use this information for any functionality, but delivers this information as part of any manager notification. The manager, however, can use this information to direct results of this test to the appropriate monitored device. For example, a DNS test can be associated with the actual DNS device instead of the machine running the DNS test.

Test Class Name

(Optional) Specifies the Test Class Name for the test. This name is used for state manager object information, resource instance information for performance data collection, and for object information of monitors that are created upon the test.

Note: This value is only writable during creation of the test. You cannot modify it afterwards, because it acts as a primary key for the table.

Log Level

Specifies the log level for the code executing the test. The global SRM log level is used if this parameter has no value or if the value is invalid. Possible values are:

-1 - no logging

0 - log fatal level messages

1 - log also critical level messages

2 - log also warning level messages

3 - log also information level messages

4 - log also debug level messages

5 - log also debug1 level messages

6 - log also debug2 level messages

7 - log also debug3 level messages

Note: If high logging is enabled for HTTP monitors, the CPU usage can spike up. Setting low or medium log levels is recommended except for extreme circumstances.

Flags

(Optional) Specifies the following flags:

Default flag

Specifies the “best practices” solution.

0x0001 [cube_collect]

Indicates if this test collects data for historical performance analysis to support Unicenter NSM Systems Performance reporting and analytics. If this flag is set SRM adds emphistory entries enabled for cube collection to monitor the SRM fixed set of metrics for this test. By default the entries are not added.For more information about emphistory, see the *SystemEDGE User Guide*.

0x0100 [run_once]

Indicates that this test only runs on request. It is not controlled by the poll interval scheduler.

The SystemEDGE monitor table contains monitors for SRM tests. The SystemEDGE monitor creation process supports the creation of SRM monitors through an SE-OID-helper functionality. This helper requires that the SE Class, Instance and Attribute are filled with TestType, TestInstance and TestMetric, for example, Class=Http, Instance=MyHomePage, Attribute=Overall Response Time. The helper detects the corresponding metric OID, inserts it into the SystemEDGE monitor OID attribute, and creates a monitor.

Note: For further information, see the *SystemEDGE User Guide*.

File Encryption

SRM can encrypt the configuration file as a whole or just individual sensitive values.

The encryption of the entire file is possible only if SystemEDGE is in managed mode. If at configuration or reconfiguration time, svcrsp receives the input configuration file encrypted, it also encrypts the modified configuration file. Any subsequent changes maintain the file encrypted.

The partial encryption is always present. The test password parameter is always encrypted when written to the svcrsp.cf file.

The details of the encryption mechanism are handled by SystemEDGE. SRM has no access to encryption or decryption keys. SRM always uses the decrypt function of SystemEDGE to access the configuration file, regardless the file is encrypted or not.

Control File Processing

When you add tests to the configuration file, consider the following procedure.

To add tests to the configuration file

1. Stop SystemEDGE agent to edit the svcrsp.cf file.
2. Add tests with status active or notInService to the svcrsp.cf file.
3. Store the file and start SystemEDGE.

At this stage SystemEDGE and SRM perform the following steps:

1. SRM parses the svcrsp.cf file and initializes itself.
2. If any critical error is encountered (like invalid java path), the configuration fails and SystemEDGE disables the AIM.
3. If any test configuration is invalid or the test status is different from active or notInService, SRM does not create the test and removes it from the configuration file.
4. SRM passes the tests to the Jcollector process that starts the tests.
5. SRM updates the test results each 30 seconds.

You can change most of the test parameters through SNMP while the tests are running (except: name, class, and so on).

Reserve Rows in Availability Table

Use this feature to allow the coexistence of locally added tests with SNMP manager added tests.

A SNMP manager or user should follow these steps to add a new test through SNMP:

1. Get the first unused test index: svcRspUnusedIndex SNMP variable from the svcrsp.asn1 MIB.
2. Use this index to create a new test.

Use the reserved_range global parameter to ensure that the svcRspUnusedIndex never returns an index that is intended for a test added through other means.

Performance Metrics

The Performance Metrics Group supplies a counter which is incremented whenever the scheduled tests did not complete in the allotted time. Another counter measures how many times the tests have run. Tracking these counters over time would provide a good indication whether the SRM configuration needs to be adjusted. Performance metrics supply real-time performance information about the functionality of the SRM AIM. You can monitor the health of the SRM AIM, either manually or through SystemEDGE. You can tune the configuration information to get the best response from SRM.

svcRspPrfReset

Specifies an enumerated integer (1 = ok , 2 = reset) allowing the end user to reset ALL performance counters for this AIM. When a reset (2) is set, all counters are set to zero (0) and this entry is set back to ok (1).

svcRspPrfRuns

Indicates the total number of execution intervals completed since the AIM was started or the counters reset.

svcRspPrfLateRuns

Indicates the total number of execution intervadls that have been late since the AIM was started or the counters reset.

svcRspPrfConsLate

Indicates the number of last successive intervals that were delayed. This should be 1 or 0, a number greater than 1 signifies systematic delays. svcRspPrfConsLate will be incremented with the difference between the current value of late_exec_runs and the one read at the previous SystemEDGE interval (maximum 1), and reset to 0 on the first update on which the difference is 0.

Example: Applying the File I/O Test to SRM AIM

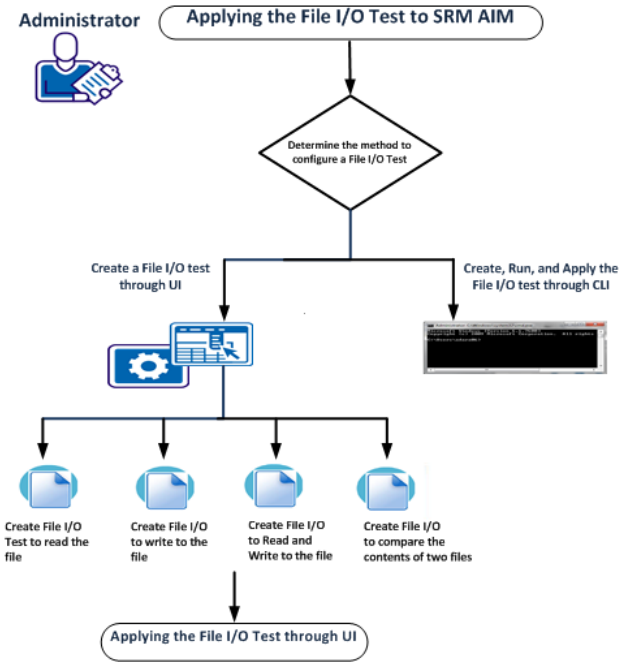
As a CA Virtual Assurance Administrator, your responsibilities include installing, maintaining, deploying, and configuring the Service Response Monitoring Application Insight Module (SRM AIM). The SRM AIM runs preconfigured or custom tests to measure execution elapsed time and throughput.

CA Virtual Assurance can help automate these activities by first creating and applying the File I/O Test to SRM AIM. The File I/O test monitors the amount of time required to perform an operation on an NFS or SMB file system.

File I/O Test on SRM AIM retrieves the responsiveness of a logical or physical service that runs on a local or remote system. Each sample test runs every 30 seconds and times out after 10 seconds when the operation is not successful. Statistics for response and availability are calculated over 120-second intervals. Based on the results, the administrator monitors and manages the health of the virtual network.

Important: SRM AIM runs as the root user, a File I/O test could write to the /etc/passwd or boot.ini file and cripple a system. Use caution when creating and enabling these tests. A sample test file exists in /sysedge/plugins/svcrsp directory.

The scenario walks you through the process of applying the File I/O test to SRM AIM:



Select one of the following methods to configure a file I/O test:

- Create a File I/O Test through UI (see page 21)
- Create, Run and Apply a File I/O Test through CLI (see page 31)

When you create the File I/O test through UI, you need to apply it through the user interface separately.

- Apply the File I/O Test through UI (see page 29)

Determine the Method to Configure a File I/O Test

Create File I/O test to define a set of monitors, configuration preferences, and other settings that control how the agent runs and what it monitors.

You can create the File I/O test through the user interface or command-line interface (CLI).

- **User Interface**—Helps you specify each option, provides a short description, and displays default values.
- **Command-Line Interface**—Lets you configure and apply the File I/O test in unattended and silent mode.

Create a File I/O Test through UI

You can create the following operations for the File I/O test from the Test Monitor toolbar. The File I/O test monitors the amount of time required to perform one of the following operations on an NFS or SMB file system:

- Create a File I/O Test to Read the File (see page 21)
- Create a File I/O Test to Write to the File (see page 23)
- Create a File I/O Test to Read and Write to the File (see page 25)
- Create File I/O Test to Compare the Contents of Two Files (see page 27)

Create a File I/O Test to Read the File

This example creates a test that monitors the amount of time to read the content of file located at F:\Test\testfile.bin.

Follow these steps:

1. Click + (New) on the Test toolbar.

   The New test pane appears.

2. Enter suitable values in the following fields.

   Test Name

   Specifies a valid test name

   Example: Fileio Read Operation

   Description

   Specifies the description of the test

   Example: Performing a read operation for testfile.bin.

   Test Class

   (Optional) Specifies a valid test class

   Example: File IO R

   Test Interval

   Specifies the interval period of the test

   Default: 30

   Test Timeout

   Specifies the interval period of the test

   Default: 10

   Test Type

   Specifies the test type

   Example: File I/O

   File Operations

   Specifies the available operations for the test

   Example: Read

   Destination Filename

   Specifies the path of destination filename

   Example: F:\Test\testFile.bin

   User Name

   Specifies the user name

   Example: FIOTestUser

3. Accept defaults values for other fields.
4. Click Save Test

   The test is saved and appears in the Available Policies page.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=11
type=fileio
desc="Performing a read operation for testfile.bin."
destination=F:\Test\testFile.bin
args="op=r"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="Fileio Read Operation"
class=""
context=""
flags="1"
loglevel=3
}
```

When you apply the File I/O test, the svcrsp.cf file is executed.

For information about the errors returned by File I/O tests, see File I/O Test Error Codes.

Create a File I/O Test to Write to the File

This example reads the C:\sysedge\bin\saFileIOTest.bin file and then writes the contents to F:\Test\WTest.bin.

Follow these steps:

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.

2. Enter suitable values in the following fields.

Test Name

Specifies a valid test name

Example: Fileio Write Operation

Description

Specifies the description of the test

Example: Performing a write operation for WTest.bin.

Test Class

(Optional) Specifies a valid test class

Example: File IO W

Test Interval

Specifies the interval period of the test

Default: 30

Test Timeout

Specifies the interval period of the test

Default: 10

Test Type

Specifies the test type

Example: File I/O

File Operations

Specifies the available operations for the test

Example: Write

Source Filename

Specifies the path of source filename

Example: C:\sysedge\bin\saFileIOTest.bin

Destination Filename

Specifies the path of destination filename

Example: F:\Test\WTest.bin

User Name

Specifies the user name

Example: FIOTestUser

3. Accept defaults for the other values.
4. Click Save Test
   The test is saved and appears in the Available Policies page.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=22
type=fileio
desc="Performing a write operation for WTest.bin."
destination=F:\Test\WTest.bin
args="op=w&local=C:\sysedge\bin\saFileIOTest.bin"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="Write Operation"
class=""
context=""
flags="1"
loglevel=3
}
```

When you apply the File I/O test, the svcrsp.cf file is executed.

For information about the errors returned by File I/O tests, see File I/O Test Error Codes.

Create a File I/O Test to Read and Write to the File

This example reads the C:\sysedge\bin\saFileIOTest.bin file, writes the contents to F:\Test\RWTest.bin, and then reads F:\Test\WTest.bin.

Follow these steps:

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.

2. Enter suitable values in the following fields.

Test Name

Specifies a valid test name

Example: fileio

Description

Specifies the description of the test

Example: Performing a read/write operation for RWTest.bin.

Test Class

(Optional) Specifies a valid test class

Example: File IO RW

Test Interval

Specifies the interval period of the test

Default: 30

Test Timeout

Specifies the interval period of the test

Default: 10

Test Type

Specifies the test type

Example: File I/O

File Operations

Specifies the available operations for the test

Example: Read/Write

Source Filename

Specifies the path of source filename

Example: C:\sysedge\bin\saFileIOTest.bin

Destination Filename

Specifies the path of destination filename

Example: F:\Test\RWTest.bin

User Name

Specifies the user name

Example: FIOTestUser

3. Accept defaults for the other values.
4. Click Save Test
   The test is saved and appears in the Available Policies page.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=33
type=fileio
desc="Performing a read/write operation for RWTest.bin."
destination=F:\Test\RWTest.bin
args="op=rw&local=C:\sysedge\bin\saFileIOTest.bin"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="Read-Write Operation"
class=""
context=""
flags="1"
loglevel=3
}
```

When you apply the File I/O test, the svcrsp.cf file is executed.

For information about the errors returned by File I/O tests, see File I/O Test Error Codes.

Create File I/O Test to Compare the Contents of Two Files

This example reads the C:\sysedge\bin\saFileIOTest.bin file and reads the F:\Test\CompTest.bin file, and compares their contents.

Follow these steps:

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.

2. Enter suitable valuesp in the following fields.

Test Name

Specifies a valid test name

Example: fileio

Description

Specifies the description of the test

Example: Comparing files

Test Class

(Optional) Specifies a valid test class

Example: File IO Comp

Test Interval

Specifies the interval period of the test

Default: 30

Test Timeout

Specifies the interval period of the test

Default: 10

Test Type

Specifies the test type

Example: File I/O

File Operations

Specifies the available operations for the test

Example: Compare

Source Filename

Specifies the path of source filename

Example: C:\sysedge\bin\saFileIOTest.bin

Destination Filename

Specifies the path of destination filename

Example: F:\Test\CompTest.bin

User Name

Specifies the user name

Example: FIOTestUser

3. Accept defaults for the other values.
4. Click Save Test
   The test is saved and appears in the Available Policies page.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=44
type=fileio
desc="Comparing files."
destination=F:\Test\CompTest.bin
args="op=cmp&local=C:\sysedge\bin\saFileIOTest.bin"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="File Compare"
class=""
context=""
flags="1"
loglevel=3
}
```

When you apply the File I/O test, the svcrsp.cf file is executed.

For information about the errors returned by File I/O tests, see File I/O Test Error Codes.

Apply the File I/O Test through UI

After you create File I/O test using user interface, you apply it to machines across the enterprise. CA Virtual Assurance applies the compiled configuration file containing all settings to all specified agent machines. The new policy is implemented after an automatic agent warm start.

Follow these steps:

1. Click Policy.

   The Policy page appears.
2. Open the Configuration pane, expand Policies, and then select Service Response.

   The Available Policies page appears.
3. Select the policy in the Available Policies table.

   The Summary page for the policy appears with the list of policies

4. Select the File I/O policy.

   File I/O policy details appear in the right pane.

5. Click Action and select Apply.

   Tabs appear for selecting machines on which to apply the policy. The Update machines running this policy tab lets you apply the policy to machines that are already running the policy. The Apply to Machines not running this Policy tab lets you apply the policy to machines that have no policy or using a different policy.

6. (Optional) Do *one* of the following from the Update machines running this policy tab:

   - Select Update all machines using this policy to deploy the policy on all machines currently running it. This option is useful if you have made File I/O test changes that you want to apply globally.
   - Select Update selected groups of machines to update only machines that meet any of the following criteria:
     - Run an out-of-date version of the policy
     - Use a policy that has exceptions
     - Run a current version of the policy

     Select any of these options. Policy exceptions occur when a user applies a point configuration change to an agent that is not represented in the applied policy.
   - Select Advanced and then manually select machines in the Select Machines pane that you want to reapply the policy to.

7. Click Apply Policy.

   The policy application is initiated.

8. (Optional) Select Advanced and then select the machines that you want to reapply the policy to in the Select Machines pane.

You can also reapply the policy to system when one of the following occurs:

- You updated the policy.
- You received notice that the configuration on an agent machine has changed.

Once you apply the test, each sample test runs every 30 seconds and times out after 10 seconds when the operation is not successful. Statistics for response and availability are calculated over 120-second intervals.

Based on these results, the administrator monitors and manages the health of the virtual network.

Create, Run and Apply a File I/O Test through CLI

You can use the CLI commands to create and automate SRM AIM and run actions based on the results. You can add svcwatch command to create and apply the File I/O test to SRM AIM on the specified host.

This command has the following format:

svcwatch [-h| -p| -v| -u| -n| -a| -A| -x| -X| -m| -t| -d| -f] -o add *index descr* fileio *destination*
username password args interval samples timeout winsiz tos limit flags name class contextInfo logLevel

The svcwatch command uses the following parameters:

-h *hostname* | -h *ipAddr*

(Optional) Specifies the CA SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the CA SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-o add *testparams*

Adds a new test to SRM AIM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

fileio

Specifies the File IO service type.

destination

Specifies the remote file to test.

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Ampersands (&) concatenate and delimit multiple arguments. The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

op=r – Reads the file.

op=w – Writes to a test file located on a remote file system, and then deletes the test file.

op=rw – Writes to a test file on a remote file system, reads the test file, and then deletes the test file.

op=cmp – Reads in one file and then another, and compares their contents.

local=*path* – The local path and file name to use for write, read/write, and compare operations.

domain=*domain* – The domain of the user logging in to the server (Windows only).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example: Compare the Contents of Two Files

This example creates and applies the file I/O test to compare the content of two files:

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360744 "FILEIO-TEST" fileio
"F:\Test\CompTest.bin" "" "" "op=cmp&local=C:\sysedge\bin\saFileIOTest.bin" 30 1 10
120 0 0 0x100 "FILEIO-TEST" "" ""
```

For information about the errors returned by File I/O tests, see File I/O Test Error Codes.

Once you apply the test, each sample test runs every 30 seconds and times out after 10 seconds when the operation is not successful. Statistics for response and availability are calculated over 120-second intervals.

Based on these results, the administrator monitors and manages the health of the virtual network.

File I/O Test Error Codes

The following table defines File I/O error codes returned by File I/O tests. The errors display in the Error Code column on the Test Monitor and Test Profile Monitor pages.

Error Code	Description
1	General error. For more information, refer to any of the following error logs: ■ *%SystemRoot%**windows**system32**sysedge.log* (Windows systems) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	Access to the local file is denied. This error indicates that the user name and password you are using do not have the correct permissions. You can specify a different user name and password on the Modify Test page.
3	Access to the remote file is denied. This error indicates that the user name and password you are using do not have the correct permissions. You can specify a different user name and password on the Modify Test page.
4	Local file is not found.
5	Remote file is not found.
6	The path argument points to the file in the local directory. The source file should be in a local directory, and the destination file should be on a remote file system. You can change the source and destination file names on the Modify Test page.
7	Read of local file failed. The source file true if and only if the file specified by this abstract pathname exists and read by the application; false otherwise.
8	Read of remote file failed.
9	Creation of remote file failed.
10	Write to remote file failed.

Error Code	Description
11	Invalid or no output from external command.
12	Delete of remote file failed.
13	File Comparison failed.
14	Failed to execute file_io_helper.jar.
15	Failed to write a log msg.

Chapter 3: Configuration

This section contains the following topics:

Edit the Control File

You can configure SRM options by adding, deleting, or modifying entries in the SRM configuration file (svcrsp.cf). For example, you may need to change the number of active threads at some point and can do this easily by editing svcrsp.cf. Be sure to stop the SystemEDGE before editing the configuration file and then restart it.

When the SystemEDGE starts (and the SRM AIM is configured to load), the agent reads the svcrsp.cf file to determine the configuration. If you are an advanced user who is very familiar with SystemEDGE and SRM, you can use the svcrsp.cf file to specify the services that you want the agent to measure. If you are configuring several systems to measure services throughout an enterprise, you can create a single svcrsp.cf file and deploy that file to all of your systems.

As an alternative to editing svcrsp.cf manually, you can use the svcwatch utility to update the svcrsp.cf file dynamically. For more information, see SRM CLI Commands.

To edit svcrsp.cf manually

1. Stop the SystemEDGE on the system on which you want to edit the file:
   - For UNIX systems, log in as root and enter the following at the command line, depending on your system:

     Solaris and Linux:
     `/etc/init.d/sysedge stop`

     HP-UX:
     `/sbin/init.d/sysedge stop`

     AIX:
     `/etc/rc.d/sysedge stop`
   - For Windows systems, use the SystemEDGE Control Panel to stop SystemEDGE.

     Note: For information about the name and location of the SystemEDGE startup script for your operating system, see the *SystemEDGE User Guide*.
2. Open the svcrsp.cf file for editing. The default locations of svcrsp.cf are as follows:
   - Solaris, HP-UX, AIX, Linux: /opt/CA/SystemEDGE/plugins/svcrsp
   - Windows: drive:\Program Files\CA\SystemEDGE\plugins\svcrsp
3. Restart the SystemEDGE agent as follows:
   - For UNIX systems, enter the following at the command line, depending on your system:

     Solaris and Linux:
     `/etc/init.d/sysedge start`

     HP-UX:
     `/sbin/init.d/sysedge start`

     AIX:
     `/etc/rc.d/sysedge start`
   - For Windows systems, use the SystemEDGE Control Panel to start SystemEDGE.

Configuration File Format

The SRM configuration file consists of a series of entries that are delimited by braces ({ }). Each field within an entry is keyword dependent (but *not* order dependent). You can ignore optional fields. The format for an entry is as follows:

```
{
index=
type=
desc=" "
dest=" "
args=" "
username=" "
encoded=yes
password=" "
interval=
samples=
timeout=
window=
tos=
limit=
status=
name=
class=
context=
flags=
loglevel=
}
```

Note: If you want to edit the password field manually, you must first specify encoded=no. You can then type in the password in plain text. After you change the password, reset the encoded field to yes, and then restart SystemEDGE. SRM encodes the password to mask it, but the password is neither encrypted nor secure.

Sample Entries

For sample svcrsp.cf entries for each test type, see the example sections for the following services:

- Active Directory
- Custom
- DHCP
- DNS
- FILE I/O
- FTP
- HTTP

- HTTPS
- IMAP
- LDAP
- MAPI
- NIS
- NNTP
- PING
- POP3
- Round-Trip Email
- SMTP
- SNMP
- SQL Query
- TCP Connect
- TFTP
- Virtual User (Windows only)

For a list of keywords for each test, see Keywords for Tests (see page 131).

Global Parameters Block

The global parameters block in the configuration file provides the following parameters:

type=global

Specifies the global section in the configuration file.

loglevel={-1 | 0 | 1 | 2 | ... | 7}

Specifies the log level for the SRM AIM.

-1: Logs no messages

0: Logs fatal level messages

1: Logs also critical level messages

2: Logs also warning level messages

3: Logs also information level messages

4: Logs also debug level messages

5: Logs also debug1 level messages

6: Logs also debug2 level messages

7: Logs also debug3 level messages

Default: 2

logfile=*filename*

Specifies the log file name in the svcrsp data path.

Default: jcollector

lognum=*number*

Specifies the number of the log files. For a log file number equal to 1 (default), the log file name is jcollector.log. For a log file number greater than 1, the log files are: jcollector0.log, jcollector1.log, and so on.

Default: 1

logsize=*size*

Specifies the maximum size of the log file (in kilobytes). A value of 0 specifies an unlimited size.

Default: 1024

maxthreads=*number*

Specifies the maximum number of threads that Jcollector uses to perform tests (one test per thread).

Default: 10

javabin=*path*

Specifies the location of the java executable relative to the SystemEDGE installation directory.

Default: ./jre/bin/java

javaclasspath=*classpath*

Specifies extra classes to load. If a classpath is set, this parameter overrides the CLASSPATH environment variable.

Default: ""

no_collector

SystemEDGE does not start Jcollector. To enable this parameter, remove the comment sign (#).

Important! Use no_collector for debugging purposes only. The parameter effectively disables the SRM execution.

Default: disabled

allow_scripts

Allows execution of external scripts. To enable this parameter, remove the comment sign (#).

Default: disabled

allow_fileio

Allows execution of file IO tests. To enable this parameter, remove the comment sign (#).

Default: disabled

allow_untrusted_ssl_certificates

Allows SSL tests to work with sites that do not have trusted SSL certificates. To enable this parameter, remove the comment sign (#).

Default: disabled

disable_dns_cache

Prevents JRE from caching DNS names. To enable this parameter, remove the comment sign (#).

Default: disabled

allow_snmp_pwd

Allows SRM to provide the password in clear text via SNMP get requests. To enable this parameter, remove the comment sign (#).

Default: disabled

hide_security_flags

Prevents the svcRspSecurityFlags OID from revealing security settings. To enable this parameter, remove the comment sign (#).

Default: disabled

preferIPV6_NoTOS (for HP-UX Java only)

The socket.setTrafficClass() is not supported when utilizing the IPV6 stack. Hence, the IPV4 stack is used to retain standard TOS functionality per default. To enable the IPV6 stack (and thereby disable TOS functionality from all tests), uncomment the parameter.

Note: For all other platforms, this line should remain commented out.

Default: disabled

shmkey=*integer*

Specifies the shared memory access key.

Important! Do not use this parameter unless there is a conflict with an existing installed program.

Default: 3131

reserved_range *start_index end_index*

Specifies a reserved range of test indexes.

Default: None

Example

```
{
  type=global
  loglevel=4
  maxthreads=100
  #javabin=<Java executable path>
  javaclasspath=
  #no_collector
  #allow_scripts
  #allow_fileio
  #allow_untrusted_ssl_certificates
  #disable_dns_cache
  #allow_snmp_pwd
  #hide_security_flags
  #preferIPV6_NoTOS
  #shmkey=<integer>
  #reserved_range <start_index> <end_index>
}
```

Test Definition Parameters Block

The test definition parameters block in the configuration file provides the following parameters:

type=*testtype*

Specifies the test type. For example HTTP, FTP, LDAP, and so on. See the chapter Test Management in this guide for a complete list of test types.

index=*integer*

Specifies a unique number to identify the test. This number is the index of the corresponding service response time table entry.

name=*string*

(Optional) Specifies a test instance name, used for state manager object information, resource instance information for performance data collection, and as an alternative to the random integer index as a primary key for tests (which can change depending upon the templates delivered). This value is only written during creation of the test.

class=*string*

(Optional) Specifies a class name, used for state manager object information, resource instance information for performance data collection, and as an alternative to the random integer index as a primary key for tests (which can change depending upon the templates delivered). This value is only written during creation of the test.

context=*string*

(Optional) Specifies a holder based on the configuration of the test. This holder is a location for a manager to store any information, such as UUIDs, flags, antecedents for the test object, and so on. SRM notifies the manager, but does not directly use this information for any functionality.

desc=*string*

(Optional) Specifies a meaningful description of the test.

Limits: 4096 characters

dest=*string*

Specifies the target of the test. For example, URL, server name, script, and so on.

user=*string*

Specifies the user name if the test requires a login to run the test.

pass=*string*

Specifies the password if the test requires a login to run the test. The password is encrypted by default. In this case, bit 4 of svcRspSecurityFlags is set to 1. If the password is unencrypted, bit 4 of svcRspSecurityFlags is set to 0.

args=*string*

(Optional) Specifies service-specific arguments used for measuring purposes.

Limits: 256 characters

Example service arguments are:

dns: *dns-server hostname*

http: *URL* [*proxy-server*] [*username:user password:pass*]

https: *URL* [*proxy-server*] [*username:user password:pass*]

ftp: *ftp-server username passwd*

pop3: *pop3-server username passwd*

nntp: *nntp-server*

smtp: *smtp-server*

ping: *system-name packetsize*

tcpconnect: *system-name port*

custom: *not used*

encoded={yes | no}

Specifies password encryption. When set to *no* SRM encrypts the password and changes the value to *yes*.

interval=*integer*

(Optional) Specifies the time interval between queries to the service.

Default: 60

samples=*integer*

(Optional) Specifies the number of samples taken at each query interval. For example, if this value is set to three and interval=60, then SRM performs three sample transactions after every 60-second interval.

Default: 1

timeout=*integer*

(Optional) Specifies the value (in seconds) after which service response time measurement timeout for this particular service measurement.

Default: 10

window=*integer*

(Optional) Specifies the period (in seconds) over which response time statistics (mean, availability, and so on) for the particular service are calculated.

Default: 300

tos=*integer*

(Optional) Specifies an 8-bit TOS header in the IP header for each test (IP Type of Service or Differentiated Services Code). The parameter does not enforce any particular RFC standard for the value of this field. You decide an appropriate value.

Default: 0

limit=*integer*

(Optional) Specifies the response limit, used as a boundary for throwing exceptions.

Default: 0

monitor=*monName, mon_index*

(Optional) Specifies the associated monitoring template (threshold) for that test.

The monName variable is equal to the monName parameter value of the monitoring template. The monIndex variable is a unique value for the table entry and the index of the monitor in SystemEDGE's monitor table.

status={active | notInService}

(Optional) Specifies the status of this entry. This variable is equivalent in semantics to the SNMPv2 SMI RowStatus convention (see RFC 1443).

active(1): Available for usage.

notInService(2): Disables usage of the row.

Default: notInService

flags=*hex_value*

(Optional) Test configuration flags:

0x0001 [cube_collect]: Enables the collection of test metrics for this test.

0x0100 [run_once]: Specifies this test is only run on request, not through the poll interval scheduler.

Default: 0x0

loglevel={-1 | 0 | 1 | 2 | ... | 7}

(Optional) Specifies the log level for the SRM AIM. See also Global Parameters Block.

-1: Logs no messages

0: Logs fatal level messages

1: Logs also critical level messages

2: Logs also warning level messages

3: Logs also information level messages

4: Logs also debug level messages

5: Logs also debug1 level messages

6: Logs also debug2 level messages

7: Logs also debug3 level messages

Default: global log level

Example

```
{
  index=25
  type=http
  desc="www.ca.com Http"
  dest="http://www.ca.com"
  encoded="yes"
  password=""
  args="max_depth=3&content_dl=yes&content_err=no"
  interval=30
  samples=1
  timeout=20
  window=300
  tos=0
  limit=0
  status=active
  name="www.ca.com-http"
  class=""
  context=""
  loglevel=1
  flags="1"
  monitor=TotalMeanCritical9000,2511
  monitor=TotalMeanWarning5000,2510
}
```

```
{
  type=monitor
  monName="TotalMeanCritical9000"
  monSeverity=critical
  monAttribute=svcRspTableTotalMean
  monThreshold=9000
  monOperator=gt
}
{
  type=monitor
  monName="TotalMeanWarning5000"
  monSeverity=warning
  monAttribute=svcRspTableTotalMean
  monThreshold=5000
  monOperator=gt
}
```

Monitor Template Definition Parameters Block

The monitor template definition parameters block in the configuration file provides the following parameters:

type=monitor

Specifies the monitor type of the parameters block.

monName=*string*

Specifies the name of the monitor.

monSeverity=*string*

(Optional) Specifies the severity to use for the SystemEDGE object state model. The value none excludes this monitor entry from the object state model. Possible values are:

none

ok

warning

minor

major

critical

fatal

Default: none

monAttribute=*string*

Specifies the attribute that is monitored. Possible attributes are:

svcRspTableNumSamples—Shows the total number of samples taken since this row was initialized.

svcRspTableTotalLastSample—Shows the total response time (in milliseconds) of the last sample.

svcRspTableTotalMin—Shows The minimum total response time sample value over the statistics window.

svcRspTableTotalMax—Shows the maximum total response time sample value over the statistics window.

svcRspTableTotalMean—Shows the mean total response time sample value over the statistics window.

svcRspTableTotalVariance—Shows the variance of the total response time values over the statistics window * 1000. SRM returns a variance value of 1.337 as 1337. The variance is calculated based on seconds.

svcRspTableTotalAvailability—Indicates the availability of this service. This is calculated as the number of successful service queries divided by the number of service queries over the statistics window. A service query is successful if it succeeds within the timeout value specified for this entry.

svcRspTableNameLastSample—Shows the name lookup (DNS) time (in milliseconds) of the last sample.

svcRspTableNameMin—Shows the minimum name lookup time sample value over the statistics window.

svcRspTableNameMax—Shows the maximum name lookup time sample value over the statistics window.

svcRspTableNameMean—Shows the mean name lookup time sample value over the statistics window.

svcRspTableNameVariance—Shows the variance of the name lookup time values over the statistics window.

svcRspTableConnLastSample—Shows the connection time (in milliseconds) of the last sample.

svcRspTableConnMin—Shows the minimum connection time sample value over the statistics window.

svcRspTableConnMax—Shows the maximum connection time sample value over the statistics window.

svcRspTableConnMean—Shows the mean connection time sample value over the statistics window.

svcRspTableConnVariance—Shows the variance of the connection time values over the statistics window.

svcRspTableTranLastSample—Shows the transaction time (in milliseconds) of the last sample.

svcRspTableTranMin—Shows the minimum transaction time sample value over the statistics window.

svcRspTableTranMax—Shows the maximum transaction time sample value over the statistics window.

svcRspTableTranMean—Shows the mean transaction time sample value over the statistics window.

svcRspTableTranVariance—Shows the variance of the transaction time values over the statistics window.

svcRspTableBytesInLastSample—Shows the number of bytes received in the last sample.

svcRspTableBytesOutLastSample—Shows the number of bytes sent in the last sample.

svcRspTableTotalBytesIn—Shows the total number of bytes received since SRM was started. This counter eventually wraps.

svcRspTableTotalBytesOut—Shows the total number of bytes sent since SRM was started. This counter eventually wraps.

svcRspTableThroughput—Shows the throughput, calculated over the statistics window, in bytes/sec. The BytesInLastSample and BytesOutLastSample are added for each sample. This number for each sample is summed up, and divided by the number of seconds in the sample.

monThreshold=*integer*

Specifies the threshold value against which SystemEDGE compares the current value of the monitored attribute.

monOperator={nop | gt | lt | ge | le | eq | ne}

Compares the current attribute value to the threshold value. The operator nop only tracks the current value and does not compare it to the threshold. Possible values are:

nop (no operation)

gt (greater than)

lt (less than)

ge (greater than or equal to)

le (less than or equal to)

eq (equal to)

ne (not equal to)

Default: no operation

Example

This example specifies a warning and a critical threshold at 500 and 900 milliseconds for the mean total response time sample value over the statistics window.

```
{
  type=monitor
  monName="TotalMeanCritical900"
  monSeverity=critical
  monAttribute=svcRspTableTotalMean
  monThreshold=900
  monOperator=gt
}
{
  type=monitor
  monName="TotalMeanWarning500"
  monSeverity=warning
  monAttribute=svcRspTableTotalMean
  monThreshold=500
  monOperator=gt
}
```

Sample Configuration File

An example for a configuration file:

```
{
  type=global

 # Log Level of the SRM/SA AIM and of any test without a specific log level (default
is 2)
 # -1 - off, 0 - fatal, 1 - critical, 2 - warning, 3 - info, 4 - debug, ..., 7 - debug3
   loglevel=2

 # Log file name (default jcollector.log)
   logfile="jcollector.log"

# Log file number (default 1 only one log file, a greater number will cycle through
#<number> log files
# the files will be named <name><id>, e.g. if default name is used: jcollector0.log,
#jcollector1.log ..etc.)
   lognum=1

# Log file size limit in kilobytes (default 1024, 0 means no limit)
   logsize=10240
```

```
# Number of threads the jcollector should use to perform tests
   maxthreads=10

# Location of the Java executable
 #javabin=<Java executable file name incl. path, relative to the SystemEDGE inst.
dir.>

# Extra classes to load; overrides CLASSPATH in environment if defined
   #javaclasspath=<a non-standard classpath>

# Uncomment in order to sysedge does not start jcollector
   #no_collector

# Uncomment to allow execution of external scripts
    #allow_scripts

# Uncomment to allow execution of fileIO tests.
    #allow_fileio

# Uncomment if you want the test password to be provided as clear text to the SNMP
Get    # requests
    #allow_snmp_pwd

# Uncomment to allow SSL tests to work with sites that do not have
# trusted SSL certificates.
    #allow_untrusted_ssl_certificates

# Uncomment to prevent JRE from caching DNS names forever
    #disable_dns_cache

# Uncomment to prevent the svcRspSecurityFlags OID from revealing
# security settings
    #hide_security_flags
```

```
# For current HP/UX Java, socket.setTrafficClass() is not supported
# when utilizing the IPV6 stack. As a default, the IPV4 stack will
# be used to retain standard TOS functionality as in past SA
# releases.  To enable the IPV6 stack (and thereby disable TOS
# functionality from all SA tests), please uncomment the following line.
# (For all other platforms, this line should remain commented out.)
#
    #preferIPV6_NoTOS

# Shared memory access key, the default value is 3131
    #shmkey=<an integer number>

# Reserved range of test indexes, by default there is none
    reserved_range 20 2000
}

{
  index=22
  type=dns
  desc="Test DNS Lookup for http://ca.com_dns"
  dest="130.119.24.108"
  encoded="yes"
  password="gJnvpNczJKjubcMzOJ/h+tvbBnX="
  args="hostname=abc.ca.com"
  interval=300
  samples=1
  timeout=10
  window=86400
  tos=0
  limit=0
  status=notInService
  name="192.168.24.108 Dns"
  class=""
  context="context"
  loglevel=1
  flags="0x100"
  monitor=TotalMeanCritical9,1011
  monitor=TotalMeanWarning5,1010
}
```

```
{
  index=25
  type=http
  desc="www.ca.com Http"
  dest="http://www.ca.com"
  encoded="yes"
  password=""
  args="max_depth=3&content_dl=yes&content_err=no"
  interval=30
  samples=1
  timeout=20
  window=300
  tos=0
  limit=0
  status=active
  name="www.ca.com-http"
  class=""
  context=""
  loglevel=1
  flags="0x1"
  monitor=TotalMeanCritical9000,2511
  monitor=TotalMeanWarning5000,2510
}

{
  type=monitor
  monName="TotalMeanCritical9000"
  monSeverity=critical
  monAttribute=svcRspTableTotalMean
  monThreshold=9000
  monOperator=gt
}

{
  type=monitor
  monName="TotalMeanWarning5000"
  monSeverity=warning
  monAttribute=svcRspTableTotalMean
  monThreshold=5000
  monOperator=gt
}
```

```
{
  type=monitor
  monName="TotalMeanCritical900"
  monSeverity=critical
  monAttribute=svcRspTableTotalMean
  monThreshold=900
  monOperator=gt
}

{
  type=monitor
  monName="TotalMeanWarning500"
  monSeverity=warning
  monAttribute=svcRspTableTotalMean
  monThreshold=500
  monOperator=gt
}

{
  type=monitor
  monName="TotalMeanFatal10"
  monSeverity=fatal
  monAttribute=svcRspTableTotalMean
  monThreshold=10
  monOperator=gt
}

{
  type=monitor
  monName="TotalMeanCritical9"
  monSeverity=critical
  monAttribute=svcRspTableTotalMean
  monThreshold=9
  monOperator=gt
}

{
  type=monitor
  monName="TotalMeanWarning5"
  monSeverity=warning
  monAttribute=(null)
  monThreshold=5
  monOperator=gt
}
```

Chapter 4: Test Management

This section contains the following topics:

Create Tests

You can create SystemEDGE policy to define a set of monitors, configuration preferences, and other settings that control how the agent runs and what it monitors. After you create SRM tests, you can group them and associate profiles with agents and agent sets.

See also Policy Configuration in the *Online Help* and *Administration Guide.*

Follow these steps:

1. Click Resources.
2. Open the Configuration pane, expand Policies, and click Service Response.

   The Service Response page appears. You can create a new policy or use the existing default policy if appropriate.
3. Click + (New) on the Available Policies toolbar.

   The New Service Response Monitoring Policy dialog appears.
4. Enter appropriate values and click OK.

   CA Virtual Assurance loads the new policy.
5. Click the Test tab.

   The Test Monitors pane opens.
6. Click + (New) on the Test Monitors toolbar.

   The fields to specify a test appear.
7. Specify a unique name for the test in the Test Name field. The name must be 64 characters or less. Test names are case-sensitive.
8. (Optional) Specify a description and a class for the test in the Description field. The description identifies the test for the user. It must be 4096 characters or less.
9. Specify the interval (in seconds) between tests in the Test Interval field. The interval must be a multiple of 30 seconds. Use this option for tuning the performance of your tests.

10. In the Test Timeout field, specify the time (in seconds) after which the test should time out. Select a number that is less than the interval but greater than the amount of time that the test requires to execute.
11. Set the polling interval by selecting one of the following from the Polling Interval list:
    - Normal
    - Off
    - Slow
12. Select the type of test you want to create from the Test Type list:
    - Active Directory (Windows only)
    - Custom
    - DHCP
    - DNS
    - FILE I/O
    - FTP
    - HTTP
    - HTTPS
    - IMAP
    - LDAP
    - MAPI (Windows only)
    - NIS
    - NNTP
    - PING
    - POP3
    - Round-Trip Email
    - SMTP
    - SNMP
    - SQL Query
    - TCP Connect
    - TFTP
    - Virtual User (Windows only)

13. Set the options for your test in the Test Options field. Options vary by test type. For details about the setting options for each test, refer to the specific page for that test type.

    Note: The options that you set on this page apply to all paths that SRM creates for this test. When you modify these options, the changes affect every path. If you want to modify an option for only one path or only select paths (but not all paths that use this test), you must create a copy of the test, modify the options you want to change, and then associate the new test with the agents to which you want to apply the changes.

14. To set advanced options, select Advanced in the Common Options area.

15. Use the Test Index Override field to control the order in which tests run or to standardize an index for the same test running on multiple machines.

    The SystemEDGE agent usually runs tests in a multi-threaded environment, so several tests run simultaneously. In cases where you want to run tests in sequence and to control the order in which they run, set the thread count to 1 to ensure that only one test runs at a time. Then assign an index value to each test that you want to order. The range of index override values is from 1000000 to 1009999. Priority goes to the lowest index number.

    Note: When using this option, it is good practice to leave some unassigned indexes between tests. This makes it easier to modify the order of tests or add a new test into an existing sequence without having to change the index for all of your tests.

16. In the Samples Per Interval field, specify the number of test transactions to perform at each interval.

In the Statistics Window field, specify the time (in seconds) over which SRM calculates the response time and availability statistics for this test. This value should be a multiple of 30. Ensure that the Statistics Window setting is greater than the Test Interval and preferably a multiple of that value. For example, a Test Interval of 60 and a Statistics Window setting of 300.

1. In the Total Response Limit field, specify the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

2. In the TOS/DSCP field, specify the IP Type of Service (TOS) or Differentiated Services Code Point (DSCP) value if your router is configured to use one of them. If you specify a TOS or DSCP value, the first test sets the value so that subsequent operations will already have it set. See also: RFC 1349.

3. Complete the required entries and click Save Template.

   The new test is saved.

Note: When you are specifying pathnames, be sure to use the correct type of slashes for the operating system on which the test will run. That is, use forward slashes (/) when you specify directories for UNIX systems and backslashes (\) when you specify directories for Windows systems.

Options and Arguments

An option is a property that is common to all tests. In contrast, an argument is a property that is typical for one particular test.

Options

Options are common properties to all the tests. They denote common functions that you can apply to all tests.

Arguments

Arguments are specific properties of a certain test. However, some tests use similar/same arguments; for example, http, https, pop3, round-trip email. They denote functions that you can apply to a specific test.

Active Directory Tests

The Active Directory test monitors the amount of time required to connect to the Active Directory service on a Windows system, perform a standard user name/password authentication, and then perform a user-defined query.

Options and Arguments

Active Directory tests require the following specific options and arguments:

- **Active Directory Server** – The name of the Active Directory server that you are testing.

  Note: As of Service Availability r2.1 IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.
- **Active Directory Domain** – The domain in which the Active Directory server is located.
- **User Name** – A valid user name for the Active Directory server.
- **Password** – A password for the user name specified above. SRM stores the password in encrypded format.
- **Query** – The query to perform, using the LDAP query language.
- **Filter** – (Optional) A term on which to filter the results of your query.

You specify these options and arguments when you create or modify tests.

Examples

This section includes examples for monitoring the amount of time to connect to local and remote Active Directory servers.

Example 1: Testing a Local Active Directory Server

Use this example to create a test that monitors the amount of time to connect to the local Active Directory server named ADTest, authenticate the user name adUser and the encoded password, and then query for the term Registered Users on the mylab.com site.

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select Active Directory.
3. In the Description field, specify ad_local.
4. In the Test Name field, specify Local Active Directory Test.
5. In the Test Interval field, specify 30.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 120.
9. In the Active Directory Server field, specify ADTEST.
10. In the Active Directory Domain field, specify mylab.com.
11. In the User Name field, specify ADUser.
12. In the Password field, specify ADPass.
13. In the Query field, specify cn=Registered,cn=Users,dc=mylab,dc=com.
14. In the Filter field, specify cn=*.
15. Accept defaults for all other fields.
16. Click Save Test.

When you commit the changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=23
type=adir
desc="ad_local"
dest="ADTEST"
username="ADUser"
encoded=yes
password="bXVyaWM="
args="domain=mylab.com&query=cn=Registered,cn=Users,dc=mylab,dc=com&filter=cn=*"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="Local Active Directory Test"
class=""
context=""
flags="1"
loglevel=1
}
```

Example 2: Testing a Remote Active Directory Server

Use this example to create a test that monitors the amount of time to connect to the remote Active Directory server at 10.0.0.234, authenticate the user name RemoteUser and the encoded password, and then query for the term Guest Users on the testlab.com site.

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.

2. From the Test Type list, select Active Directory.
3. In the Description field, specify ad_remote.
4. In the Test Name field, specify Remote Active Directory Test.
5. In the Test Interval field, specify 30.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 120.
9. In the Active Directory Server field, specify 10.0.0.234.

10. In the Active Directory Domain field, specify Test.com.
11. In the User Name field, specify RemoteUser.
12. In the Password field, specify ADPass.
13. In the Query field, specify cn=Guest,cn=Users,dc=testlab,dc=com.
14. In the Filter field, specify cn=*.
15. Click Save Test.

When you commit the changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=24
type=adir
desc="ad_remote"
dest="10.0.0.234"
username="RemoteUser"
encoded=yes
password="bXVyaWMe"
args="domain=test.com&query=cn=Guest,cn=Users,dc=testlab,dc=com&filter=cn=*"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="Remote Active Directory Test"
class=""
context=""
flags="1"
loglevel=2
}
```

For information about errors you may encounter when running Active Directory tests, see Active Directory Test Error Codes (see page 274).

Custom Tests

The Custom test provides the ability to use scripts or programs to perform custom tests.

Options and Arguments

Custom tests require the following specific option or argument:

- **Script path (dest)** – The name of the script or program that you want to use to perform a custom test. This field contains the full script path and arguments. SRM expects that the script or program resides on a local or mounted file system.

You specify this option or argument when you create or modify tests.

Example

Use this example to create a test that monitors a custom service through a script or program. The entry instructs the agent to test a custom service once every 30 seconds, and to wait up to 20 seconds for a successful response. The agent calculates statistics over the last 3600 seconds (1 hour).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select Custom.
3. In the Test Name field, specify Custom_test.
4. In the Description field, specify Test custom service.
5. In the Script path field, specify c:\@work\projects\shortcuts\custom_test.exe.
6. In the Test Interval field, specify 30.
7. In the Test Timeout field, specify 20.
8. In the Samples Per Interval field, specify 1.
9. In the Statistics Window field, specify 3600.
10. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=123
type=CUSTOM
desc="Test custom service"
dest="c:\@work\projects\shortcuts\custom_test.exe"
interval=30
samples=1
timeout=20
window=3600
tos=0
limit=0
status=active
name="Custom_test"
class="Custom_class"
context="Custom_context"
flags="0x0"
loglevel=3
}
```

DHCP Tests

The DHCP test monitors the amount of time required to send a DHCP request and receive a response.

Note: Run DHCP tests only for systems that are statically configured and are not running a DHCP client. These tests require an open socket on port 68 to listen for requests. If another process (such as a DHCP client) is already listening on port 68, the test will fail.

Options and Arguments

DHCP tests require only the following options and arguments:

DHCP Server – The hostname or IP address of the DHCP server to test. Specify this argument when you create or modify tests.

Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0:0:0:0:0:0:10.0.00.0].

Example

Use this example to create a test that monitors the amount of time that is required to send a DHCP request to the DHCP server and receive a response.

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select DHCP.
3. In the Description field, specify dhcp_resp.
4. In the Test Name field, specify Test DHCP Service.
5. In the Test Interval field, specify 300.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 86400.
9. In the DHCP Server field, specify 192.174.12.89.
10. Accept defaults for all other fields.
11. Click Save Test

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=31
type=dhcp
desc="dhcp_resp"
dest="192.174.12.89"
args=""
interval=120
samples=1
timeout=100
window=300
tos=0
limit=0
status=active
name="Test DHCP Service"
class=""
context=""
flags="1"
loglevel=2
}
```

For information about errors you may encounter when running DHCP tests, see DHCP Test Error Codes (see page 274).

DNS Tests

The DNS test monitors the amount of time required to resolve an IP address for a specified server.

Options and Arguments

DNS tests require the following specific options and arguments:

- **DNS Server** – The name of the local DNS server that you are testing.
- **Hostname To Resolve** – The hostname you want to resolve for the DNS server.

You specify these options and arguments when you create or modify tests.

Example

Use this example to create a test that monitors the amount of time that is required to resolve the IP address for http://www.ca.com using the name server at 192.168.0.0. (In your environment, use the IP address of your local DNS server.) The entry instructs the agent to test the service once every 300 seconds (5 minutes), and to wait up to 10 seconds for a successful response. The agent calculates statistics over the last 86,400 seconds (1 day).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select DNS.
3. In the Description field, specify ca.com_dns.
4. In the Test Name field, specify Test DNS lookup.
5. In the Test Interval field, specify 300.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 86400.
9. In the DNS Server field, specify the IP address of your local DNS server (such as 192.168.0.0).
10. In the Hostname To Resolve field, specify http://jimp.ca.com.
11. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=10
type=dns
desc="Test DNS Lookup for http://ca.com_dns"
dest="192.168.0.0"
args="hostname=jimp.ca.com"
interval=300
samples=1
timeout=10
window=86400
tos=0
limit=0
status=active
name="Test DNS Lookup"
class=""
context=""
flags="1"
loglevel=2
}
```

For information about errors you may encounter when running DNS tests, see DNS Test Error Codes (see page 274).

File I/O Tests

The File I/O test monitors the amount of time required to perform one of the following operations on an NFS or SMB file system:

- Reading a file
- Writing to a file
- Writing to a file and then reading it
- Comparing two files

File I/O tests are turned off by default. Enable SRM to run File I/O tests by editing the svcrsp.cf file to uncomment the "allow_fileio" line by removing the preceding pound sign (#). For instructions on editing the svcrsp.cf file, refer to Edit the svcrsp.cf File Manually.

You can create File I/O tests and associate them with agents before you modify the svcrsp.cf file to enable them. However, the tests are created in the "Not Ready" state on the agent and cannot be changed to the active state (able to run) until you enable the File I/O tests as just described. This configuration file directive "allow_fileio" exists as a security measure. Because SRM runs as the root user, a File I/O test could write to the /etc/passwd or boot.ini file and cripple a system. Use caution when enabling and creating these tests.

The size of the file you are testing can affect the performance of the test. A sample test file exists in the *drive*:/sysedge/plugins/svcrsp directory.

Options and Arguments

File I/O tests require the following test-specific options and arguments:

- **File Operation** – The type of operation to perform; one of the following:
  - **Read** – Reads a test file. The file must exist on a local or remote mounted file system. You specify the path to the file to read in the Destination Filename field.
  - **Write** – Writes the contents of a local file to a test file on a remote file system and then deletes the test file. You specify the path to the source file in the Source Filename field and the path to the test file in the Destination Filename field. The source file must exist, and the destination file must not exist.
  - **Read/Write** – Writes the contents of a local file to a test file on a remote file system, reads the test file, compares the test file to the original file, and then deletes the test file. You specify the path to the source file in the Source Filename field and the path to the test file in the Destination Filename field. The source file must exist, and the destination file must not exist.
  - **Compare** – Reads in one file and then another and compares their contents. If the contents do not match, the test fails. You specify the source file and destination file in the Source Filename and Destination Filename fields. Both files must exist.

  Note: If you are testing a *local* file operation (such as from and to c:\), it is not necessary to specify host/login info. Host/login information is only needed for connecting to remote machines.
- **Destination Filename** – The complete path and file name to the local or remote test file. For the write and read/write operations, this file must not exist before the test creates it. For the read and compare operations, it must exist before the test runs.

  Note: When you are specifying pathnames, be sure to use the correct type of slashes for the operating system on which the test will run. That is, use forward slashes (/) when you specify directories for tests that you intend to run on UNIX systems and backslashes (\) when you specify directories for tests that you intend to run on Windows.

  In addition, the files you specify must exist on a *mounted* file system. The SystemEDGE agent and SRM do not mount file systems.
- **User Name (Windows only)** – A valid user name for this FTP server.
- **Password (Windows only)** – The password for the specified user name. SRM stores the password in encrypted form.

  Note: You retype the password in the Verify Password field to verify that you have entered it correctly.
- **Domain (Windows only)** – The domain of the user logging in to the server.

Specify these options and arguments when you create or modify tests.

Examples

This section includes examples for the read, write, read/write, and compare operations. Each sample test runs every 30 seconds and times out after 10 seconds if the operation is not successful. Statistics for response and availability are calculated over 120-second intervals.

Example 1: Reading a File

This example creates a test that monitors the amount of time to read the file located at F:\Test\testfile.bin.

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select File I/O.
3. In the Description field, specify testfile.bin.
4. In the Test Name field, specify Read Operation.
5. In the Test Interval field, specify 30.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 120.
9. In the File Operation field, select Read.
10. In the Destination Filename field, specify F:\Test\testfile.bin.
11. Accept defaults for the other values.
12. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=11
type=fileio
desc="Performing a read operation for testfile.bin."
destination=F:\Test\testFile.bin
args="op=r"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="Read Operation"
class=""
context=""
flags="1"
loglevel=3
}
```

Example 2: Writing a File

This example reads the C:\sysedge\bin\saFileIOTest.bin file and then writes the contents to F:\Test\WTest.bin.

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select File I/O.
3. In the Description field, specify WTest.bin.
4. In the Test Name field, specify Write Operation.
5. In the Test Interval field, specify 30.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 120.
9. In the File Operation field, select Write.
10. In the Destination Filename field, specify F:\Test\WTest.bin.
11. In the Source Filename field, specify C:\sysedge\bin\saFileIOTest.bin.

12. Accept defaults for the other values.
13. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=22
type=fileio
desc="Performing a write operation for WTest.bin."
destination=F:\Test\WTest.bin
args="op=w&local=C:\sysedge\bin\saFileIOTest.bin"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="Write Operation"
class=""
context=""
flags="1"
loglevel=3
}
```

Example 3: Writing and Reading a File

This example reads the C:\sysedge\bin\saFileIOTest.bin file, writes the contents to F:\Test\RWTest.bin, and then reads F:\Test\WTest.bin.

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select File I/O.
3. In the Description field, specify RWTest.bin.
4. In the Test Name field, specify Read-Write Operation.
5. In the Test Interval field, specify 30.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 120.
9. In the File Operation field, select Read/Write.
10. In the Destination Filename field, specify F:\Test\RWTest.bin.

11. In the Source Filename field, specify C:\sysedge\bin\saFileIOTest.bin.
12. Accept defaults for the other values.
13. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=33
type=fileio
desc="Performing a read/write operation for RWTest.bin."
destination=F:\Test\RWTest.bin
args="op=rw&local=C:\sysedge\bin\saFileIOTest.bin"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="Read-Write Operation"
class=""
context=""
flags="1"
loglevel=3
}
```

Example 4: Comparing Two Files

This example reads the C:\sysedge\bin\saFileIOTest.bin file, reads the F:\Test\CompTest.bin file, and compares their contents.

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select File I/O.
3. In the Description field, specify CompTest.
4. In the Test Name field, specify File Compare.
5. In the Test Interval field, specify 30.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 120.
9. In the File Operation field, select Compare.

10. In the Destination Filename field, specify F:\Test\CompTest.bin.
11. In the Source Filename field, specify C:\sysedge\bin\saFileIOTest.bin.
12. Accept defaults for the other values.
13. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=44
type=fileio
desc="Comparing files."
destination=F:\Test\CompTest.bin
args="op=cmp&local=C:\sysedge\bin\saFileIOTest.bin"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="File Compare"
class=""
context=""
flags="1"
loglevel=3
}
```

For information about errors you may encounter when running File I/O tests, see File I/O Test Error Codes (see page 274).

FTP Tests

The FTP test monitors the amount of time required to log in and test the specified FTP server.

Options and Arguments

FTP tests require the following specific options and arguments:

- **FTP Operation**. The type of FTP operation to test. Select either Login-only, Get, or Put. If you select Login-only, specify the name of the FTP Server, a valid port number (default is 21), username and password. This test logs in using the specified username and password and then logs out.

  If you select Get, specify the name of the FTP Server, a valid port number (default is 21), username, password and a Remote File name (the path to the file to be read). This test logs in and reads the specified file (but does not perform a write operation), then logs out.
  If you select Put, specify the name of the FTP Server, a valid port number (default is 21), username, password, and the name of the Local File to be written to the FTP Server. This test logs in and writes the specified file out to the FTP Server, then logs out. If the remote directory does not have writer permission, the test will fail.

- **FTP Server**. The hostname of the FTP server that you are testing.

  Note: As of Service Availability r2.1 IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

- **FTP Port**. (Optional) The port on which the FTP service is running if it is running on a port other than 21 (the default).

- **User Name**. A valid user name for this FTP server.

- **Password**. The password for the specified user name. SRM stores the password in encrypted form.

  Note: You retype the password in the Verify Password field to verify that you have entered it correctly.

You specify these options and arguments when you create or modify tests.

Example

Use this example to create a test that monitors the amount of time required to log in and test the status of the FTP service at ftpstage.ca.com. This example tests the server once every 3600 seconds (1 hour) and waits up to 10 seconds for a successful response. It calculates response time and availability statistics over the last 604,800 seconds (1 week).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.

2. In the Test Name field, specify FTP Test.

3. In the Description field, specify ftptest
4. In the Test Interval field, specify 3600.
5. In the Test Timeout field, specify 10.
6. In the Samples Per Interval field, specify 1.
7. In the Statistics Window field, specify 604800.
8. In the FTP Operation field, specify Login-only.
9. In the FTP Server field, specify ftpstage.mydomain.com.
10. Accept the default value in the FTP Port field.
11. In the User Name field, specify ftpuser.
12. In the Password field, specify ftp123.
13. Accept defaults for all other fields.
14. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=289
type=ftp
desc="ftptest"
dest=ftpstage.mydomain.com:21
username="ftpuser"
encoded=yes
password="bmh12cy"
args="op=login"
interval=3600
samples=1
timeout=10
window=604800
tos=0
limit=0
status=active
name="FTP-Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running FTP tests, see FTP Test Error Codes (see page 274).

HTTP Tests

The HTTP test monitors the amount of time required to log in and test a website. You can test sites directly or use a proxy. This test supports the ability to search for regular expressions on a web page and to specify the number of nested levels you want the HTTP test to traverse during a test.

SRM uses HTTP 1.1 by default for all HTTP requests. It does handle HTTP 1.0 responses.

Options and Arguments

HTTP tests require the following specific options and arguments:

- **URL To Test**. The hostname of the system to test.

  Note: As of Service Availability r2.1 IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

- **URL User Name**. (Optional) A user name for the site you are trying to access if the site requires Web authentication.
- **URL Password**. (Optional) A password for the user name you specified if the site requires Web authentication. SRM stores the password in encrypted form.
- **Frame Depth**. (Optional) The number of levels the test should traverse when downloading nested frames. (The HTTP test downloads all frames, images, external scripts, and applets during the page download so that the measurement reflects the user's experience when downloading a Web page.) The default value is 3.
- **Text Match**. (Optional) A regular expression or text string that you want SRM to match on the pages you test. The number of matches displays in the Results Field column on the Monitor page for the agent.
- **Min Matches**. (Optional) The minimum number of times that SRM must find the search expression (default is 1). If the search expression is not found at least as many times as you specify in this field, the test will fail (Availability=0). If this field is set to zero and the agent does not find the search expression, the Availability measurement is not affected.
- **Download Content**. Checking this box downloads all images, frames, scripts, and applets, with the core HTML code from the proxy site.
- **Fail on Content Errors**. Checking this box specifies that any errors encountered while downloading images, frames, scripts, and applets cause the test to fail.
- **Use Proxy**. Check this box to use a proxy server for the website being tested. If this box is unchecked the following proxy options do not display.
- **Proxy Server**. The hostname (the name or IP address) of the proxy server to use if the system from which you are testing does not have direct Internet access.

- **Proxy Port**. (Optional) The port to use on the proxy server. The default is 80.
- **Proxy User Name**. (Optional) A valid username to be authenticated on the specified proxy server.
- **Proxy Password**. (Optional) The password for the specified user name. SRM stores the password in encrypted form.

Specify these options and arguments when you create or modify tests.

Notes:

- You retype the password in the Verify Proxy Password field to verify that you have entered it correctly.
- HTTP Test supports the HTTP Basic authentication scheme and NTLM authentication. For more information consult documentation on your web server.

Examples

This section includes examples for testing web server response.

Example 1: Testing Web Server Response

Use this example to create a test that monitors the amount of time required to access the main web page at http://www.ca.com. This example tests the server once every 60 seconds and waits up to 20 seconds for a successful response. It calculates response time and availability statistics over the last 300 seconds (5 minutes).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select HTTP.
3. In the Description field, specify ca_web.
4. In the Test Name field, specify ca.com test.
5. In the Test Interval field, specify 60.
6. In the Test Timeout field, specify 20.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 300.
9. In the URL To Test field, specify http://www.ca.com. You specify the full web address, including http://.
10. Accept defaults for all other fields.
11. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=25
type=http
desc="ca-web"
dest="http://www.ca.com"
args="max_depth=3&content_dl=true&content_err=false"
interval=60
samples=1
timeout=20
window=300
tos=0
limit=0
status=active
name="ca.com test"
class=""
context=""
flags="100"
loglevel=3
}
```

Example 2: Testing Web Server Response through a Proxy

Use this example to create a test that monitors the amount of time required to access the main web page at http://www.weather.com. In this example, the test accesses the weather.com website through a proxy server (myproxy) that is running on port 8080. This example tests the server once every 60 seconds and waits up to 20 seconds for a successful response. It calculates response time and availability statistics over the last 300 seconds (5 minutes).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.

2. From the Test Type list, select HTTP.
3. In the Description field, specify weather.com_proxy.
4. In the Test Name field, specify Proxy Test.
5. In the Test Interval field, specify 60.
6. In the Test Timeout field, specify 20.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 300.
9. In the URL To Test field, specify http://www.weather.com. You specify the full web address, including http://.

10. In the Proxy Server field, specify myproxy.
11. In the Proxy Port field, specify 8080.
12. Accept defaults for all other fields.
13. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=26
type=http
desc="weather.com_proxy"
dest="http://www.weather.com"
args="max_depth=3&content_dl=true&content_err=false&proxy=myproxy:8080"
interval=60
samples=1
timeout=20
window=300
tos=0
status=active
name="Proxy test"
class=""
context=""
flags="100"
loglevel=3
}
```

Example 3: Matching Web Server Content

Use this example to create a test that downloads the web page at http://www.weather.com and searches the content for the regular expression, "cumulus." SRM records the number of times that this expression appears in the Results field for the test. This example tests the server once every 60 seconds and waits up to 20 seconds for a successful response. It calculates response time and availability statistics over the last 300 seconds (5 minutes). You can use a similar example to test content for the HTTPS Tests tests by specifying the HTTPS test type and a secure web server.

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select HTTP.
3. In the Description field, specify weather.com_content.
4. In the Test Name field, specify Test Web Content at http://www.weather.com.
5. In the Test Interval field, specify 60.

6. In the Test Timeout field, specify 20.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 300.
9. In the URL To Test field, specify http://www.weather.com. You specify the full web address, including http://.
10. In the Frame Depth field, accept the default of 3 to search through 3 layers of the site for the search text.
11. In the Text Match field, enter cumulus.
12. Accept defaults for all other fields.
13. Click Save Test.

When you commit your changes of the test, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=27
type=http
desc="weather.com."
dest="http://www.weather.com_content"
args="max_depth=3&search=cumulus&minmatch=1&content_dl=true&content_err=false"
interval=60
samples=1
timeout=20
window=300
tos=0
limit=0
status=active
name="Web server content"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running HTTP tests, see HTTP Test Error Codes (see page 274).

HTTPS Tests

The HTTPS test monitors the amount of time required to log in and test a secure website. You can test sites directly or use a proxy. You can also search for regular expressions on a web page, and you can specify the number of nested levels you want the HTTPS test to traverse during the test.

SRM uses HTTP 1.1 by default for all HTTP requests. It can handle HTTP 1.0 responses.

Options and Arguments

HTTPS tests require the following specific options and arguments:

- **URL To Test**. The hostname of the secure website to test.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. For example, 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

- **User Name**. (Optional) A user name for the site you are testing if it requires web authentication.
- **Password**. (Optional) A password for the user name you specified if the site requires web authentication. SRM stores the password in encrypted form.
- **Frame Depth**. (Optional) The number of levels the test should traverse when downloading nested frames. (The HTTPS test downloads all frames, images, external scripts, and applets during the page download so that the measurement reflects the user's experience when downloading a web page.) The default value is 3.
- **Text Match**. (Optional) A regular expression or text string that you want SRM to match on the pages you test. The number of matches displays in the Results Field column on the Monitor page for the agent.
- **Min Matches**. (Optional) The minimum number of times that SRM must find the search expression (default is 1). If the search expression is not found at least as many times as you specify in this field, the test will fail (Availability=0). If this field is set to zero and the agent does not find the search expression, the Availability measurement is not affected.
- **Download Content**. Checking this box downloads all images, frames, scripts, and applets, with the core HTML code from the proxy site.
- **Fail on Content Errors**. Checking this box specifies that any errors encountered while downloading images, frames, scripts, and applets cause the test to fail.
- **Use Proxy**. Check this box to use a proxy server for the website being tested. If this box is not checked, the following proxy options do not appear on the screen.
- **Proxy Server**. The hostname (the name or IP address) of the proxy server to use if the system from which you are testing does not have direct Internet access
- **Proxy Port**. (Optional) The port to use on the proxy server. The default is 80.
- **Proxy User Name**. (Optional) A valid username to be authenticated on the specified proxy server.
- **Proxy Password**. (Optional) The password for the specified user name. SRM stores the password in encrypted form.

Specify these options and arguments when you create or modify tests.

Notes:

- You retype the password in the Verify Proxy Password field to verify that you have entered it correctly.
- HTTP Test only supports the HTTP Basic authentication scheme. For more information consult documentation on your web server.

Untrusted SSL Certificates

HTTPS websites display an SSL certificate when the certificate is invalid (untrusted) or the address by which the website is accessed does not match with the SSL certificate.

To allow untrusted SSL certificates you must uncomment (that is, remove '#') 'allow_untrusted_ssl_certificates' in the svcrsp.cf configuration file.

Example

Use this example to create a test that monitors the amount of time required to access the main web page at the secure website, https://chargeMycredit.com This example tests the server once every 60 seconds and waits up to 20 seconds for a successful response. It calculates response time and availability statistics over the last 300 seconds (5 minutes).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select HTTPS.
3. In the Description field, specify chargeMycredit web.
4. In the Test Name field, specify HTTPS Test.
5. In the Test Interval field, specify 60.
6. In the Test Timeout field, specify 20.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 300.
9. In the URL To Test field, specify https://chargeMycredit.com. You specify the full web address, including https://.
10. In the User Name field, specify creditAcct.
11. In the Password field, specify secret.

12. Accept defaults for all other fields.
13. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=27
type=https
desc="Test secure Web response at https://chargeMycredit.com"
dest="https://chargeMycredit.com"
username="creditAcct"
encoded=yes
password="ibwc3m"
args="max_depth=3&minmatch=1&content_dl=true&content_err=false"
interval=60
samples=1
timeout=20
window=300
tos=0
limit=0
status=active
name="HTTPS-Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running HTTPS tests, see HTTPS Test Error Codes (see page 274).

IMAP Tests

The IMAP test monitors the amount of time required to log into a user account and download messages from the IMAP server. The IMAP protocol enables selective filtering and searching through mailboxes by using the SEARCH command.

Options and Arguments

IMAP tests require the following specific options and arguments:

- **IMAP Server**. The hostname of the IMAP mail server.

  Note: As of Service Availability r2.1 IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

- **IMAP Port**. (Optional) The port on which the IMAP service is running. The default is 143.

- **User Name**. A valid user name for a test IMAP account on this server. Do *not* use an active mailbox; create a test account instead.

- **Password**. A valid password for the user account. SRM stores the password in encrypted form.

- **Download**. Select one of the following:

  - **Download First Message** – This option downloads only the first message for this user account.

  - **Download All Messages** – This option downloads all messages for this user account.

- **Delete Downloaded Messages**. (Optional) Select the check box to delete the messages that were downloaded during the test, or leave it blank to leave the messages on the test system.

  Note: If you use the Download All Messages option and if the download fails, delete some portion of the number of messages in the test mailbox and try the test again.

Specify these options and arguments when you create or modify tests.

Example

Use this example to create a test that downloads all messages for the IMAPuser account at imapserver.yourdomain once every 300 seconds and deletes them after downloading them. The test waits up to 10 seconds for a successful response and calculates response time and availability statistics over the last 7200 seconds (2 hours).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.

2. From the Test Type list, select IMAP.

3. In the Description field, specify IMAP_Test.

4. In the Test Name field, specify Test IMAP Service.

5. In the Test Interval field, specify 300.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 7200.
9. In the IMAP Server field, enter imapserver.yourdomain.
10. In the IMAP Port field, accept the default of 143.
11. In the User Name field, specify IMAPuser@server.domain.
12. In the Password field, specify IMAP123.
13. In the Download field, select Download All Messages.
14. Select Delete Downloaded Messages.
15. Accept defaults for all other fields.
16. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=60
type=imap
desc="IMAP_Test."
dest="imapserver.yourdomain.com:143"
args="download=Download All Messages&delete=true"
username="IMAPuser@server.domain"
encoded=yes
password="c4nrxzw"
interval=300
samples=1
timeout=10
window=7200
tos=0
limit=0
status=active
name="Test IMAP Service"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running IMAP tests, see IMAP Test Error Codes (see page 281).

LDAP Tests

The LDAP test monitors the amount of time required to connect to the LDAP service on a Windows system, perform a standard user name/password authentication, and then perform a user-defined query.

Options and Arguments

LDAP tests require the following specific options and arguments:

- **Domain in which the LDAP Server is located**. The hostname or IP address of the LDAP server that you are testing.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

- **LDAP Domain**. (Optional) The domain in which the LDAP server is located.
- **LDAP Port**. (Optional) The port on which the LDAP service is running. The default is port 389.
- **User Name**. (Optional) A valid user name for the LDAP server.
- **Password**. (Optional) A password for the user name specified. SRM stores the password in encrypted form.
- **Query**. An LDAP query to perform. For information about the LDAP query language, refer to your LDAP documentation.
- **Filter**. (Optional) A parameter on which to filter the results of your query.

Specify these options and arguments when you create or modify tests.

Examples

This section includes examples for monitoring the amount of time to connect to a local LDAP server and a remote LDAP server.

Example 1: Testing a Local LDAP Server

Use this example to create a test that monitors the amount of time to connect to the local LDAP server named arch, authenticate the user name ldapUser and the encoded password, and then query for the term annuity.

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.

2. From the Test Type list, select LDAP.
3. In the Description field, specify ldap_arch.

4. In the Test Name field, specify Local LDAP Test.
5. In the Test Interval field, specify 30.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 120.
9. In the LDAP Server field, specify arch.
10. In the LDAP Domain field, specify TEST.
11. In the User Name field, specify ldapUser.
12. In the Password field, specify ldapPassword.
13. In the Query field, specify cn=annuity,ou=Boston,dc=fleet,dc=com.
14. In the Filter field, specify cn=*.
15. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=11
type=ldap
desc="LDAP-TEST"
dest="arch"
username="ldapUser"
encoded=yes
password="Z28ySGVsbA"
args="query=cn=annuity,ou=Boston,dc=fleet,dc=com&domain=Test&filter=cn=*"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="Local LDAP Test"
class=""
context=""
flags="1"
loglevel=1
}
```

Example 2: Testing a Remote LDAP Server

Use this example to create a test that monitors the amount of time to connect to the remote LDAP server at 10.0.0.123, authenticate the user name ldapRUser and the encoded password, and then query for the term Guest Users.

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select LDAP.
3. In the Description field, specify ldap_remote.
4. In the Test Name field, specify Remote LDAP Test.
5. In the Test Interval field, specify 30.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 120.
9. In the LDAP Server field, specify 10.0.0.123.
10. In the LDAP Domain field, specify Test.
11. In the User Name field, specify ldapRUser.
12. In the Password field, specify ldapRPass.
13. In the Query field, specify cn=Guest,cn=Users,dc=testlab,dc=com.
14. In the Filter field, specify cn=*.
15. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=23
type=ldap
desc="ldap_remote"
dest="10.0.0.123:389"
username="ldapRUser"
encoded=yes
password="bXVyaWM"
args="query=cn=guest,cd=users,dc=testlab,dc=com&domain=Test&filter=cn=*"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="Remote LDAP Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running LDAP tests, see LDAP Test Error Codes (see page 281).

MAPI Tests

The MAPI test monitors the amount of time required to log into a user account and either *send* or *retrieve* mail from a MAPI server.

Note: MAPI is a proprietary Microsoft protocol. The MAPI test uses the Microsoft Extended MAPI protocol. For this reason, MAPI tests must originate from a Windows server that is running Microsoft Exchange or Microsoft Outlook. (Outlook Express is not sufficient because it does not install the correct APIs.) The MAPI test requires the MAPI server to specify a default message store and address book provider.

Options and Arguments

MAPI tests require the following specific options and arguments:

- **Operation**. Select the type of mail test to perform: Send or Retrieve.
- **MAPI Server**. The hostname of the MAPI mail server. This system must be in the same domain as the user you specify in the User Name field. The system from which you run the SRM test must also be in the same domain.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.
- **User Name**. A valid user name for a test MAPI account on the Exchange server. This user must have Log In as a Service privileges on the system on which SRM is installed to authenticate the recipient. Do not use an active user account for this test; create a test account in the same domain as the MAPI server you are testing, and make sure that the account has Log In as a Service privileges.
- **Password**. A valid password for the user account. The password is encrypted.

  Note: You must retype the password in the Verify Password field to verify that you have entered it correctly.
- **User Domain**. The Windows domain where the MAPI user account exists. The system you are testing and the user must be in the same domain.
- **Mail Recipient**. (Send only) The email address of a valid mail recipient know by the mail server.
- **Mail Body Size**. (Send only) The size of the test message to send. The default is 4096 bytes.
- **Download**. (Retrieve only) Select *one* of the following:
  - **Download First Message**. This option downloads only the first message for this user account.
  - **Download All Messages**. This option downloads all messages for this user account.
- **Delete Downloaded Messages**. (Retrieve only - Optional) Select the check box to delete the messages that were downloaded during the test or leave it blank to leave the messages on the test system.

Specify these options and arguments when you create or modify tests.

To specify Log In as a Service privileges

1. Open the Administrative Tools Control Panel.
2. Double-click Local Security Policies, Local Policies, User Rights Assignment.

   A list of policies displays in the right pane.

3. Double-click Log in as a service.

   The Log in as a service dialog appears.

4. Click Add.

   The Select Users or Groups dialog appears.

5. Select the name to which you want to add this policy, click Add, and then click OK.

   Note: The test must run on the same domain to which the user belongs.

Example 1

Use this example to create a test that downloads the first message in the MAPI user account at mapiserver.yourdomain once every 120 seconds and deletes it after downloading it. The test waits up to 10 seconds for a successful response and calculates response time and availability statistics over the last 3600 seconds (1 hour).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.

2. In the Operation field, select Send.
3. From the Test Type list, select MAPI.
4. In the Description field, specify MAPI-Test.
5. In the Test Name field, specify MAPI-Test.
6. In the Test Interval field, specify 120.
7. In the Test Timeout field, specify 10.
8. In the Samples Per Interval field, specify 1.
9. In the Statistics Window field, specify 3600.
10. In the MAPI Server field, enter mapiserver.yourdomain.com.
11. In the User Name field, specify MAPIuser.
12. In the Password field, specify MAPI123.
13. In the Verify Password field, specify MAPI123.
14. In the User Domain field, specify myDomain.
15. In the Mail Recipient field, specify congo@yourdomain.com.
16. Accept the default mail body size (256 bytes).
17. Accept defaults for all other fields.
18. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=71
type=mapi
desc="MAPI-Test"
dest="mapiserver.yourdomain.com"
username="MAPIuser"
encoded=yes
password="xlrpm6v"
args="domain=myDomain&op=send&to=congo@yourdomain.com&size=256"
interval=120
samples=1
timeout=10
window=3600
tos=0
limit=0
status=active
name="MAPI-Test"
class=""
context=""
flags="1"
loglevel=1
}
```

Example 2

Use this example to create a test that retrieves the first message from a known MAPI user account at mapiserver.yourdomain.com once every 120 seconds and deletes it after downloading it. The test waits up to 10 seconds for a successful response and calculates response time and availability statistics over the last 3600 seconds (1 hour).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.

2. In the Operation field, select Retrieve.
3. From the Test Type list, select MAPI.
4. In the Description field, specify MAPI_Retrieve_Test.
5. In the Test Name field, specify MAPI Retrieve Test.
6. In the Test Interval field, specify 120.
7. In the Test Timeout field, specify 10.
8. In the Samples Per Interval field, specify 1.
9. In the Statistics Window field, specify 3600.

10. In the MAPI Server field, enter mapiserver.yourdomain.com.
11. In the User Name field, specify MAPIuser.
12. In the Password field, specify MAPI123.
13. In the Verify Password field, specify MAPI123.
14. In the User Domain field, specify myDomain.
15. Select Delete Downloaded Messages.
16. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=31
type=mapi
desc="MAPI_Retrieve_Test"
dest="mapiserver.yourdomain.com"
username="MAPIuser"
encoded=yes
password="bufwate2"
args="domain=myDomain&op=recv&download=first&delete=yes"
interval=60
samples=1
timeout=30
window=300
tos=0
limit=0
status=active
name="MAPI Retrieve Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running MAPI tests, see MAPI Test Error Codes (see page 281).

NIS/NIS+ Tests

The NIS/NIS+ test monitors the amount of time required to log into the specified NIS or NIS+ server and request a specific map file. You can also choose to download the map file.

Options and Arguments

NIS/NIS+ tests require the following specific options and arguments:

- **NIS Server**. The hostname of the NIS server.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

- **NIS Domain**. The domain on which the map file exists.
- **NIS Map**. The map file to test. The default is the hosts file.
- **Download NIS Map?** Select *one* of the following:
  - **Yes**. This option downloads the map file.
  - **No (Verify Only)**. This option verifies that the map file exists but does not download it.

Specify these options and arguments when you create or modify tests.

Example

Use this example to create a test that downloads the hosts map file from the Test domain at nisserver.yourdomain once every 300 seconds. The test waits up to 20 seconds for a successful response and calculates response time and availability statistics over the last 7200 seconds (2 hours).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select NIS.
3. In the Description field, specify NIS_Test.
4. In the Test Name field, specify NIS-Test.
5. In the Test Interval field, specify 300.
6. In the Test Timeout field, specify 20.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 7200.
9. In the NIS Domain field, enter Test.com.
10. In the NIS Server field, enter nisserver.yourdomain.com.
11. In the NIS Map field, accept the default of hosts.
12. In the Download NIS Map? field, select Yes.

13. Accept defaults for all other fields.
14. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=63
type=nis
desc="NIS-Test"
dest="nisserver.yourdomain"
args="domain=Test.com&map=hosts&download=true"
interval=300
samples=1
timeout=20
window=7200
tos=0
limit=0
status=active
name="NIS-Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running NIS or NIS+ tests, see NIS Test Error Codes (see page 281).

NNTP Tests

The NNTP test monitors the amount of time required to connect to an NNTP server and perform a simple transaction.

Options and Arguments

NNTP tests require the following specific options and arguments:

- **NNTP Server**. The hostname of the news server to test.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

- **NNTP Port**. (Optional) The port on which the NNTP service is running. The default is port 119.

Specify these options and arguments when you create or modify tests.

Example

Use this example to create a test that monitors the amount of time required to connect to the NNTP service at new.yourdomain and to perform a simple transaction. This example tests the server once every 3600 seconds (1 hour) and waits up to 10 seconds for a successful response. It calculates response time and availability statistics over the last 86400 seconds (1 day).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select NNTP.
3. In the Description field, specify NewsTest.
4. In the Test Name field, specify News Test.
5. In the Test Interval field, specify 3600.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 86400.
9. In the NNTP Server field, specify news.yourdomain.com.
10. In the NNTP Port field, accept the default port of 119.
11. Accept defaults for all other fields.
12. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=41
type=nntp
desc="NewsTest"
dest="news.yourdomain.com"
args=" "
interval=3600
samples=1
timeout=10
window=86400
tos=0
limit=0
status=active
name="News Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running NNTP tests, see NNTP Test Error Codes (see page 281).

Ping Tests

The ping test monitors the amount of time required to perform a network-level ping of a server. It enables you to determine whether the system is running and has network connectivity.

Options and Arguments

Ping tests require the following specific options and arguments:

- **Destination**. The hostname of the system to ping.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

- **Payload**. (Optional) The size of the packet sent in the ping. The default packet size is 64 bytes.

Specify these options and arguments when you create or modify tests.

Example

Use this example to create a test that tests the system at server.yourdomain three times every 60 seconds and waits up to 5 seconds for a successful response. It calculates response time and availability statistics over the last 3600 seconds (1 hour).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select Ping.
3. In the Description field, specify server.yourdomain_ping.
4. In the Test Name field, specify Ping Test.
5. In the Test Interval field, specify 60.
6. In the Test Timeout field, specify 5.
7. In the Samples Per Interval field, specify 3.
8. In the Statistics Window field, specify 3600.
9. In the Destination field, specify server.yourdomain.com.
10. In the Payload field, accept the default packet size of 64 bytes.
11. Accept defaults for all other fields.
12. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=45
type=ping
desc="server.yourdomain_Ping"
dest="server.yourdomain.com"
args="payload=64"
interval=60
samples=3
timeout=5
window=3600
tos=0
limit=0
status=active
name="Ping Test"
class=""
context=""
flags="100"
loglevel=2
}
```

For information about errors you may encounter when running Ping tests, see Ping Test Error Codes (see page 281).

POP3 Tests

The POP3 test monitors the amount of time required to log into a user account and download messages from a POP3 server.

Options and Arguments

POP3 tests require the following specific options and arguments:

- **POP3 Server**. The hostname of the POP3 mail server.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

- **POP3 Port**. (Optional) The port on which the POP3 service is running. The default is 110.

- **User Name**. A valid user name for a test POP3 account on this server. Do *not* use an active mailbox; create a test account instead.

- **Password**. A valid password for the user account. SRM stores the password in encrypted form.
- **Download**. Select *one* of the following:
  - **Download First Message**. This option downloads only the first message for this user account.
  - **Download All Messages**. This option downloads all messages for this user account.
- **Delete Downloaded Messages**. (Optional) Select the check box to delete the messages that were downloaded during the test, or leave it blank to leave the messages on the test system.

Specify these options and arguments when you create or modify tests.

Example

Use this example to create a test that downloads all messages for the POPuser account at popserver.yourdomain.com once every 300 seconds and deletes them after downloading them. The test waits up to 10 seconds for a successful response and calculates response time and availability statistics over the last 21600 seconds (6 hours).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select POP3.
3. In the Description field, specify popserver.yourdomain_test.
4. In the Test Name field, specify POP3 Test.
5. In the Test Interval field, specify 300.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 21600.
9. In the POP3 Server field, enter popserver.yourdomain.
10. In the POP3 Port field, specify 8080.
11. In the User Name field, specify POPuser@yourdomain.com.
12. In the Password field, specify POP123.
13. In the Download field, select Download All Messages.
14. Select Delete Downloaded Messages.

15. Accept defaults for all other fields.
16. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=51
type=pop3
desc="popserver.yourdomain_test"
dest="popserver.yourdomain.com:8080"
username="POPuser"
encoded=yes
password="ijl3r2kr"
args="download=all&delete=yes"
interval=300
samples=1
timeout=10
window=21600
tos=0
limit=0
status=active
name="POP3 Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running POP3 tests, see POP3 Test Error Codes (see page 281).

Round-Trip E-Mail Tests

The round-trip e-mail test monitors the amount of time required to send an e-mail through SMTP or MAPI to a POP3, IMAP, or MAPI e-mail system and download the message from that server.

Options and Arguments

Round-trip e-mail tests require the following specific options and arguments:

- **Mail Send Type**. The Roundtrip Email Test supports **SMTP** and **MAPI** protocols. Select one. The fields that appear below this option reflect the type of protocol you select.
- **SMTP|MAPI Server**. The hostname of the SMTP or MAPI mail server, where the e-mail originates.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.
- **SMTP Port**. (Optional.) The port on which the SMTP service is running. The default is 25.
- **SMTP|MAPI Mail Recipient**. The name of the account to which the test sends an e-mail.
- **SMTP|MAPI Mail Body Size**. (Optional.) The size of the test message to send. The default is 4096 bytes.
- **Sender Hostname**. (SMTP only. Optional.) Specify the hostname of the sender (for example, *service_availability@hostname*). The default is the agent hostname.

  Note: As of Service Availability r2.1 IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.
- **SNMP|MAPI User Name**. (Optional for SMTP.) A valid user name for the test mail account that is sending the e-mail. Do not use an active mailbox; create a test account instead so that valid email messages are not deleted in the process of removing test email messages.
- **SNMP|MAPI Password**. A valid password for the test user account. SRM stores the password in encrypted form. (Optional for SMTP.)
- **User Domain**. (MAPI test only.) The domain on which the user account that is sending the e-mail exists.
- **Use SSL/TLS**. (SMTP only.) If the SMTP Server requires SSL/TLS authentication, select this checkbox option to enable Secure Sockets Layer/Transport Layer Security.

- **Mail Retrieval Type**. The type of mail service to use to retrieve the e-mail. Select *one* of the following:
  - **POP3**.
  - **IMAP**.
  - **MAPI**.

    Note: The MAPI test requires the Extended MAPI API. MAPI tests, therefore, must originate from a Windows server that is running either Microsoft Exchange or Microsoft Outlook *(not* Outlook Express. Outlook Express does not include the correct API for this test).
- **POP3|IMAP|MAPI Server**. The hostname of the server to which the mail is sent.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.
- **POP3|IMAP Port**. (Optional.) The port on which the mail service is running. Defaults are 110 for POP3 and 143 for IMAP.
- **User Name**. A valid user name for the test mail account that is receiving the e-mail. Do not use an active mailbox; create a test account instead.
- **Password**. A valid password for the test user account. SRM stores the password in encrypted form.
- **User Domain**. (MAPI test only) The domain on which the user account that is receiving the e-mail exists.
- **Poll Interval**. The interval at which to check the recipient e-mail account for messages. The default is 500 ms.

Note: Run the round-trip e-mail test for a minimum of 5 minutes with one sample at each interval.

Specify these options and arguments when you create or modify tests.

This test matches e-mails by their title and time/date stamp. It creates and deletes a user profile each time it runs, and it always deletes the e-mail and then logs off at the end of the test.

Example

Use this example to create a test that monitors the amount of time required to send a test e-mail of 2000 bytes from the mail server at server.mydomain to an account (you@yourdomain.com) on the mail server server.yourdomain. The test waits up to 5 seconds for a successful response, downloads the message using POP3, and calculates response time and availability statistics over the last 86400 seconds (1 day).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select Round Trip Email.
3. In the Description field, specify RTE_SMTP_POP_Test.
4. In the Test Name field, specify Roundtrip Test.
5. In the Test Interval field, specify 300.
6. In the Test Timeout field, specify 5.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 86400.
9. In the Send Mail Type=SMTP field, specify SMTP.
10. In the SMTP Server field, enter server.mydomain.com.
11. In the SMTP Port field, accept the default of 25.
12. In the Mail Recipient field, specify you@yourdomain.com.
13. In the Sender Hostname field, specify Gold.
14. In the User Name field, specify SMTPuser.
15. In the Password field, specify SMTPpassword.
16. In the Use SSL/TLS field, click the checkbox.
17. In the Mail Body Size field, specify 2000.
18. In the Mail Retrieval Type field, select POP3.
19. In the POP3 Server field, specify server.yourdomain.com.
20. In the POP3 Port field, accept the default of 110.
21. In the User Name field, enter Mailuser.
22. In the Password field, enter Mail123.
23. In the Check Interval field, accept the default of 500 ms.

24. Accept defaults for all other fields.
25. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=70
type=rtemail
desc="RTE_SMTP_POP_Test"
dest="server.mydomain.com:25"
username="RTUser"
encoded=yes
password="zrvr8tx"
args="send_Proto=SMTP&to=you@yourdomain.com&size=2000&shost=gold&
SMTP_SSL=yes&send_user=SMTPuser&send_pass=SMTPpassword&get_Proto=POP&
source=server.yourdomain.com:110&check=500"
interval=300
samples=1
timeout=5
window=86400
tos=0
limit=0
status=active
name="Roundtrip Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running round-trip email tests, see any of the following:

- IMAP, MAPI, and POP3 Test Error Codes (see page 281)
- SMTP Test Error Codes (see page 290)

SMTP Tests

The SMTP test monitors the amount of time required to connect to the SMTP service on a mail server and perform a null transaction. It can provide a baseline for the time required to send an e-mail.

Options and Arguments

Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

SMTP tests require the following specific options and arguments:

- **SMTP Server**. The hostname of the SMTP mail server, where the e-mail originates.
- **SMTP Port**. (Optional) The port on which the SMTP service is running. The default is 25.
- **Mail Recipient**. The e-mail account to which the test sends an e-mail.
- **Mail Body Size**. (Optional) The size of the test message to send. The default is 4096 bytes.
- **Sender Hostname**. The hostname of the sender. The default is the agent hostname.
- **User Name**. A valid user name for SMTP authorization.
- **Password**. A valid password for SMTP authorization. SRM stores the password in encrypted form (Optional for SMTP).

  Note: You must retype the password in the Verify Password field to verify that you have entered it correctly.
- **Use SSL/TLS**. (SMTP only) If the SMTP Server requires SSL/TLS authentication, select this checkbox option to enable Secure Sockets Layer/Transport Layer Security.

Specify these options and arguments when you create or modify tests.

Examples

This section includes examples of tests that monitor the amount of time required to send test emails from the mail server at mailserver.yourdomain to the account you@test.com.

Example 1: Testing email Send Time

Use this example to create a test that monitors the amount of time required to send a test email of 10,000 bytes from the mail server at mailserver.yourdomain to the account you@test.com every 60 seconds. The test waits up to 10 seconds for a successful response and calculates response time and availability statistics over the last 300 seconds (5 minutes).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select SMTP.
3. In the Description field, specify smtp_test.
4. In the Test Name field, specify SMTP Email Send Test.
5. In the Test Interval field, specify 60.
6. In the Test Timeout field, specify 10.

7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 300.
9. In the SMTP Server field, specify mailserver.yourdomain.com.
10. In the SMTP Port field, accept the default of 25.
11. In the Mail Recipient field, specify you@test.com.
12. In the Mail Body Size field, specify 10000.
13. In the Sender Hostname field, specify silver.
14. In the User Name field, specify SMTPuser.
15. In the Password field, specify SMTPpassword.
16. In the Use SSL/TLS field, click the check box.
17. Accept defaults for all other fields.
18. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=80
type=smtp
desc="SMTP_Test"
dest="mailserver.yourdomain.com:25"
"username="SMTPuser"
encoded=yes
password:"c21o6BH12"
args="to=you@test.com&size=10000&shost=silver&SSL=yes"
interval=60
samples=1
timeout=10
window=300
tos=0
limit=0
status=active
name="SMTP Email Send Test"
class=""
context=""
flags="1"
loglevel=1
}
```

Example 2: Testing email Send Time When Sender Host is an IPv6 Address

Use this example to create a test that monitors the amount of time required to send a test e-mail of 10,000 bytes from the mail server at mailserver.yourdomain to the account you@test.com every 60 seconds.

The sender host is an IPv6 address and the SMTP requires the IPv6 address be embedded in brackets. The IPV6: in [IPV6:address] is not mandatory, but the test will add it at runtime. The test waits up to 10 seconds for a successful response and calculates response time and availability statistics over the last 300 seconds (5 minutes).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select SMTP.
3. In the Description field, specify smtp_test_ipv6.
4. In the Test Name field, specify IPv6 SMTP Email Send Test.
5. In the Test Interval field, specify 60.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 300.
9. In the SMTP Server field, specify mailserver.yourdomain.com.
10. In the SMTP Port field, accept the default of 25.
11. In the Mail Recipient field, specify you@test.com.
12. In the Mail Body Size field, specify 10000.
13. In the Sender Hostname field, specify [IPV6:2000::36:543:2111].
14. In the User Name field, specify SMTPuser.
15. In the Password field, specify SMTPpassword.
16. In the Use SSL/TLS field, click the check box.
17. Accept defaults for all other fields.
18. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=80
type=smtp
desc="SMTP_Test_ipv6"
dest="mailserver.yourdomain.com:25"
"username="SMTPuser"
encoded=yes
password:"c21o6BH12"
args="to=you@test.com&size=10000&shost=[IPV6:2000::36:543:2111]&SSL=yes"
interval=60
samples=1
timeout=10
window=300
tos=0
limit=0
status=active
name="IPv6 SMTP Email Send Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running SMTP tests, see SMTP Test Error Codes (see page 290).

SNMP Tests

The SNMP test monitors the amount of time required to perform an SNMP GET request for a MIB object on a specific agent. It supports only SNMPv1, SNMPv2c, and SNMPv3 operations.

Options and Arguments

SNMP tests require the following specific options and arguments:

- **SNMP Agent**. The hostname or IP address of the system on which the SNMP agent resides.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

- **SNMP Port**. (Optional) The port on which the SNMP service is running. The default is 161.

- **OID**. The object identifier of the MIB object to query. When you query a MIB variable that has an integer value, the value displays in the Results Field column on the Monitor page. This column does not display by default. To set it to display, select Show Configuration Details on the Monitor page, and then select Results Field, and click Update Page.

SNMP Version Options

Select the SNMP version that you want to test with. Available options are SNMPv1, SNMPv2c, and SNMPv3.

SNMPv1 and SNMPv2c tests require the following specific argument:

- **Community String**. The read-only or read-write community string used to contact the agent.

SNMPv3 tests require the following specific arguments:

- **User Name**. SNMPv3 user name configured in SystemEDGE.
- **Security Level**. Permitted level of security in the SNMPv3 Security model. Select NoAuthNoPriv, AuthNoPriv, or AuthPriv:
  - **NoAuthNoPriv**. This indicates that the SNMPv3 user is configured without any authentication and without any encryption (privacy).
  - **AuthNoPriv**. This indicates that the SNMPv3 user is configured with authentication but without any encryption (privacy).
  - **AuthPriv**. This indicates that the SNMPv3 user is configured with both authentication and encryption (privacy).
- **MD5 or SHA**. Select the authentication protocol that the SNMPv3 user is configured with. Applicable for security levels AuthPriv or AuthNoPriv only.
- **Authentication Password**. Enter the authentication password that the SNMPv3 user is configured. Applicable for security levels AuthPriv or AuthNoPriv only.

- **DES or AES or 3DES**. Select the privacy protocol that the SNMPv3 user is configured with. Applicable for security level AuthPriv only.
- **Authentication Privacy**. Enter the privacy password that the SNMPv3 user is configured with. Applicable for security level AuthPriv only.

Specify these options and arguments when you create or modify tests.

Examples

This section includes examples of SNMP version tests that monitor the time required to retrieve MIB object values.

Example 1: SNMPv1 or SNMPv2c Test

Use this example to create a SNMPv1 or SNMPv2c test that monitors the amount of time required to retrieve the value of the MIB object with OID 1.3.6.1.4.1.546.1.1.1.8.0 from the agent on port 5000 of the system at IP address 172.32.6.93. The test performs an SNMP GET for this object every 30 seconds, waits up to 10 seconds for a successful response, and calculates response time and availability statistics over the last 120 seconds (2 minutes).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select SNMP.
3. For Description, specify snmpGet.
4. For Test Name, specify Get value of OID 1.3.6.1.4.1.546.1.1.1.8.0.
5. For Test Interval, specify 30.
6. For Test Timeout, specify 10.
7. For Samples Per Interval, specify 1.
8. For Statistics Window, specify 120.
9. For SNMP Agent, specify 172.32.6.93.
10. For SNMP Port, specify 5000.
11. For Community String, specify public.
12. For OID, specify 1.3.6.1.4.1.546.1.1.1.8.0.
13. Accept defaults for all other fields.
14. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=22
type=snmp
desc="snmpGet"
dest="172.32.6.93:5000"
encoded=yes
password="CHV1JB1"
args="oid=1.3.6.1.4.1.546.1.1.1.8.0"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="Get value of OID 1.3.6.1.4.1.546.1.1.1.8.0"
class=""
context=""
flags="1"
loglevel=1
}
```

Example 2: SNMPv3 Test

Use this example to create a SNMPv3 test that monitors the amount of time required to retrieve the value of the MIB object with OID 1.3.6.1.4.1.546.1.1.1.8.0 from the agent on port 5000 of the system at IP address 172.32.6.93. The test performs an SNMP GET for this object every 30 seconds, waits up to 10 seconds for a successful response, and calculates response time and availability statistics over the last 120 seconds (2 minutes).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.

2. From the Test Type list, select SNMP.
3. For Description, specify snmpv3Get.
4. For Test Name, specify SNMPv3: Get value of OID 1.3.6.1.4.1.546.1.1.1.8.0.
5. For Test Interval, specify 30.
6. For Test Timeout, specify 10.
7. For Samples Per Interval, specify 1.
8. For Statistics Window, specify 120.
9. For SNMP Agent, specify 172.32.6.93.

10. For SNMP Port, specify 5000.
11. For Security Level, select AuthPriv.
12. For User Name, select shades; shades should be a SNMPv3 user that is configured on SystemEDGE.
13. Click SHA for the authentication protocol used by the SNMPv3 user shades.
14. For Authentication Password, specify shapassword.
15. For Verify Password below Authentication Password, specify shapassword.
16. Click DES for the privacy protocol used by the SNMPv3 user shades.
17. For Privacy Password, specify despassword.
18. For Verify Password below Privacy Password, specify despassword.
19. For OID, specify 1.3.6.1.4.1.546.1.1.1.8.0.
20. Accept defaults for all other fields.
21. Click Save Tests.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=23
type=snmp
desc="snmpv3Get"
dest="172.32.6.93:5000"
encoded=yes
password="
c2VjbD0zJnNlY3U9bWQ1ZGVzMiZhdXRdcHI9TUQ1JmF1dGhwdz1wYXNzd29yZCZwcml7cHI6REVTJnBya
XAwdy1wYXNzd29yZA=="
args="oid=1.3.6.1.4.1.546.1.1.1.8.0"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="SNMPv3: Get value of OID 1.3.6.1.4.1.546.1.1.1.8.0"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running SNMP tests, see SNMP Test Error Codes (see page 290).

SQL Query Tests

The SQL Query test monitors the amount of time required to connect to any database that supports JDBC and can execute SQL queries. It supports queries for Oracle, Microsoft SQL Server, and other databases.

Before you begin creating SQL Query tests, verify that the appropriate JDBC driver is available. If necessary, install the JDBC driver files that are specific to the database you are trying to test.

- sqljdbc.jar (JRE Version 1.5 or earlier) or sqljdbc4.jar (JRE Version 1.6 or later) for SQL Server
- ojdbc<XYZ>.jar for Oracle

Copy the JAR files to the jre/lib/ext directory under the SystemEDGE installation directory (for exampl, /opt/SystemEDGE/jre/lib/ext [UNIX] or *drive*:\sysedge\jre\lib\ext [Windows]). To obtain JDBC driver jar files for your database, check the Corporate Web site of the company that distributes the database.

Example to verify the availability of the SQL JDBC driver

1. Change to the *Install_Path*/SystemEDGE/jre/lib/ext directory.
2. Check, if sqljdbc.jar (JRE Version 1.5 or earlier) or sqljdbc4.jar (JRE Version 1.6 or later) is available.

If the SQL JDBC is not available, perform the following steps:

1. Download the SQL JDBC driver from microsoft.com/downloads.
2. Extract the downloaded driver package and copy sqljdbc.jar (JRE Version 1.5 or earlier) or sqljdbc4.jar (JRE Version 1.6 or later) to the *Install_Path*/SystemEDGE/jre/lib/ext directory.
3. Restart SystemEDGE to load the new Java classes.
4. Set up new SQL tests, for example, through Policy Configuration in CA Virtual Assurance. See also the help system from the extracted JDBC package if necessary.

Options and Arguments

SQL Query tests require the following specific options and arguments:

- **Database Type**: Select Oracle, MSSQL, or Other.

  Note: For Oracle and MSSQL, SRM creates a dynamic SQL connect string using a default JDBC driver installed with SRM. For any other JDBC driver that you download, regardless of the database vendor, you must obtain the Java class name of the driver and an appropriate SQL connect string from the vendor and provide specific keywords (see below).

- **SQL Database Server**: The hostname of the SQL database server.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

- **Port**: The port on which the SQL database is running. The default port number appears when you select either Oracle or MSSQL. This field is mandatory.

- **User Name**: A valid user name for the database.

- **Password**: A valid password for the specified user name. SRM stores the password in encrypted form.

- **SQL Driver**: The JDBC driver required to connect to the database. If you select either Oracle or MSSQL as the Database Type, the SQL driver name defaults to the Oracle or MSSQL driver you specified during SRM installation (in which case this field does not appear). To specify a different JDBC driver for Oracle or MSSQL, select Other and complete the required fields. This includes identifying the Java class name of the SQL driver you want to use and the appropriate connect string. Again, the connect string format and the required information varies by vendor. Be sure to obtain that information from the vendor web site or from the vendor's driver documentation.

  Examples:

  ```
  com.microsoft.sqlserver.jdbc.SQLServerDriver
  oracle.jdbc.OracleDriver
  com.mysql.jdbc.Driver
  ```

- **Database Name**: Specify the database instance name. This field is mandatory for Oracle and optional for MSSQL. The driver name and connect string are sufficient for MSSQL (the database instance name is null). This field does not appear if you select Other because you provide that information in an explicit SQL connect string.

- **Query**: An SQL query to perform. For information about the SQL query language, refer to your database documentation.

- **Connect String**: The required SQL connect string for your database. This field appears only if you selected Other as the Database Type, otherwise, SRM builds the connect string based on the information you provide in the required fields in the SRM user interface. If your database driver is other than the default driver for Oracle or MSSQL, you must specify an explicit connect string in this field.

  Note: The format of an SQL connect string varies depending on the database driver from a particular vendor. Refer to your database vendor's web site to obtain the appropriate connect string for your JDBC driver or refer to your JDBC driver documentation.

  The connect string from your database vendor contains a sequence of fields, some of which you can replace with explicit *keywords*, such as a unameValue, pwdValue, hostnameValue, and portValue. When you enter the connect string in the GUI, type in "unameValue" and "pwdValue" and let the agent do the substitution. The vendor-specific connect string should stipulate where in the connect to place the keywords. (SRM does this automatically if you use the default JDBC driver for Oracle or MSSQL.) When an SRM test runs, the following SRM keywords in the connect string get replaced by the values that you specify:

  - The unameValue keyword is replaced by the specified username
  - The pwdValue keyword is replaced by the specified password
  - The hostnameValue keyword is replaced by the specified host name
  - The portValue keyname is replaced by specified port

  Examples:

  ```
  jdbc:oracle:thin:unameValue/pwdValue@hostnameValue:portValue:orcl (connects with orcl)
  jdbc:sqlserver://hostnameValue:portValue;databaseName=vasdb;user=unameValue;password=pwdValue (connects with vasdb)
  jdbc:sqlserver://hostnameValue:portValue;user=unameValue;password=pwdValue (connects with default database)
  jdbc:mysql://hostnameValue:portValue/mydb?user=unameValue&password=pwdValue (connects with mydb)
  ```

Specify these options and arguments when you create or modify tests.

Example 1: Testing an Oracle Database

Use this example to create a test that logs into an Oracle database and performs a query to retrieve the table names from the user tables once every 300 seconds. The test waits up to 10 seconds for a successful response and calculates response time and availability statistics over the last 1800 seconds (30 minutes).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select SQL Query.
3. In the Description field, specify SQLQuery_OracleTest.
4. In the Test Name field, specify Oracle Test.
5. In the Test Interval field, specify 300.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 1800.
9. In the Database Type field, select Oracle.
10. In the SQL Database Server field, specify OracleTest.
11. In the Port field, accept the default: 1521.
12. In the User Name field, specify OracleUser.
13. In the Password field, specify Oracle123.
14. In the Database Name field, specify the name of the database you want to test, for example, MYDB.
15. In the Query field, specify select table_name from user_tables.
16. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=11
type=sql
desc="SQLQuery_OrcaleTest"
dest="OracleTest:1521"
username="OracleUser"
encoded=yes
password="aW1vdXJhdmlldg"
args="query=select table_name from user_tables&dbtype=oracle&dbname=MYDB"
interval=300
samples=1
timeout=10
window=1800
tos=0
limit=0
status=active
name="Oracle Test"
class=""
context=""
flags="1"
loglevel=2
}
```

Example 2: Testing a Microsoft SQL Server Database

Use this example to create a test that logs into a Microsoft SQL database and performs a query to retrieve the table names from the user tables once every 60 seconds. The test waits up to 10 seconds for a successful response and calculates response time and availability statistics over the last 120 seconds.

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.

2. From the Test Type list, select SQL Query.
3. In the Description field, specify SQLQuery_SQLServer.
4. In the Test Name field, specify SQL Test.
5. In the Test Interval field, specify 60.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 120.
9. In the SQL Database Server field, select MSSQL.

10. In the Port field, accept the default: 1433.
11. In the User Name field, specify SQLUser.
12. In the Password field, specify SQL123.
13. In the Database Name field, specify the name of the database you want to test, for example, Northwind.
14. In the Query field, specify select * from categories.
15. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=11
type=sql
desc="SQLQuery.SQLServer"
dest="mySQLServer:1433"
username="SQLUser"
encoded=yes
password="bWnvTRPJhdmll"
args="query=select * from categories"&dbtype=mssql&dbname=Northwind"
interval=60
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="SQL Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running SQL Query tests, see SQL Query Test Error Codes (see page 290).

TCP Connect Tests

The TCP Connect test monitors the amount of time required to connect to a port on a server through TCP. It can help you determine whether the TCP service is running and network connectivity exists.

Options and Arguments

TCP Connect tests require the following specific options and arguments:

- **Destination**. The hostname of the system to which you want to connect.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

- **Port**. The port on which the TCP service is running.

Specify these options and arguments when you create or modify tests.

Example

Use this example to create a test that monitors the amount of time required to connect to port 2049 on the system nfsserver.yourdomain every 60 seconds. The test waits up to 5 seconds for a successful response and calculates response time and availability statistics over the last 600 seconds (10 minutes).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select TCP Connect.
3. In the Description field, specify nfsserver.yourdomain_tcp.
4. In the Test Name field, specify TCP Connection Test.
5. In the Test Interval field, specify 60.
6. In the Test Timeout field, specify 5.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 600.
9. In the Destination field, enter nfsserver.yourdomain.com.
10. In the Port field, specify 2049.
11. Accept defaults for all other fields.
12. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=90
type=tcpconnect
desc="nfsserver.yourdomain_tcp"
args=" "
dest="nfsserver.yourdomain:2049"
interval=60
samples=1
timeout=5
window=600
tos=0
limit=0
status=active
name="TCP Connection Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running TCP Connect tests, see Generic Error Codes (see page 273).

TFTP Tests

The TFTP test monitors the amount of time required to read or write a file using the TFTP protocol.

Options and Arguments

TFTP tests require the following specific options and arguments:

- **TFTP Server**. The hostname of the TFTP server that you are testing. Some TFTP servers may require that you create a writable seed file (stub file) in the TFTP root directory before you perform the Write test. A *stub file* is a file with the same name as the file being written by the TFTP test. If the stub file is not writable, the test will fail.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.

  Note: The agent must have access to the file being written to the TFTP server, either locally or mounted.

- **TFTP Port**. (Optional) The port on which the TFTP service is running. The default is 69.

- **Operation**. The type of operation to perform; one of the following:
  - **Read File –** Reads (attempts to download) a file from the server.
  - **Write File –** Writes a file to a remote file system. Output from TFTP Write tests go to the TFTP root directory. This is a directory configured either before or after installation (of the TFTP server) on Windows. For UNIX systems, it may appear in the system startup configuration file (such as \etc\inetd.conf on Solaris).
- **Filename**. A complete path and file name for the file to *write*. In the case of a *read* operation, you must supply either a complete path or just a file name -- it depends on the requirements of TFTP server you are contacting. You must specify the file or path name on the TFTP server in a manner consistent with the particular server. In most cases, the path is relative to the root of the TFTP directory.

  Note: When you are specifying pathnames, be sure to use the correct type of slashes for the operating system on which the test will run. That is, use forward slashes (/) when you specify directories for tests that you intend to run on UNIX systems and backslashes (\) when you specify directories for tests that you intend to run on Windows systems.

Specify these options and arguments when you create or modify tests.

Example 1: Reading a File with TFTP

Use this example to create a test that monitors the amount of time required to read a file through the TFTP service at tftpserver.yourdomain. This example tests the server once every 30 seconds and waits up to 10 seconds for a successful response. It calculates response time and availability statistics over the last 120 seconds (2 minutes).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select TFTP.
3. In the Description field, specify tftpserver_read.
4. In the Test Name field, specify TFTP Reading File Test.
5. In the Test Interval field, specify 30.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 120.
9. In the TFTP Server field, specify tftpserver.yourdomain.
10. In the TFTP Port field, accept the default of 69.
11. In the Operation field, select Read File.

12. In the Filename field, specify I:\SA\TFTP\get.txt.
13. Accept defaults for all other fields.
14. Click Save Test.

When you perform a commit/sync of the test, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=11
type=tftp
desc="tftpserver.read"
dest="tftpserver@yourdomain.com:69"
args="op=r&path=I:\SA\TFTP\get.txt"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="TFTP Reading File Test"
class=""
context=""
flags="1"
loglevel=1
}
```

Example 2: Writing a File with TFTP

Use this example to create a test that monitors the amount of time required to write a file through the TFTP service at tftpserver.yourdomain. This example tests the server once every 30 seconds and waits up to 10 seconds for a successful response. It calculates response time and availability statistics over the last 120 seconds (2 minutes).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select TFTP.
3. In the Description field, specify tftpserver_write.
4. In the Test Name field, specify TFTP Writing File Test.
5. In the Test Interval field, specify 30.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 120.

9. In the TFTP Server field, specify tftpserver.yourdomain.
10. In the TFTP Port field, accept the default of 69.
11. In the Operation field, select Write File.
12. In the Filename field, specify I:\SA\TFTP\put.txt.
13. Accept defaults for all other fields.
14. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=22
type=tftp
desc="tftpserver_write"
dest="tftpserver.yourdomain.com:69"
args="op=w&path=I:\SA\TFTP\put.txt"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="TFTP Writing File Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running TFTP tests, see TFTP Test Error Codes (see page 290).

Virtual User Tests

The Virtual User test plays back a recorded WinTask script. This test web site enables you to obtain continuous availability and response time data for real user transactions.

Before you create Virtual User tests, you must do the following:

- Verify that SystemEDGE on the target system is able to interact with the desktop.
- Verify that the allow_scripts directive exists in the svcrsp.cf file and that it is not commented out. (Remove the pound sign (#) in front of that line if one exists.)
- Install the WinTask runtime agent and the script you want to run on the system(s) that will run the test.
- Make sure that you have an active (unlocked) desktop open to run scripts.

Consider the following items when you run Virtual User tests:

- You can run Virtual User tests only on Windows systems.
- You cannot run Virtual User tests in a Citrix environment.
- If you are setting up tests for more than one script on the same system, edit the svcrsp.cf file to set maxthreads=1. This setting eliminates the possibility of SRM attempting to run more than one script on the same system simultaneously. You can set this variable during the SRM installation, or by manually editing the svcrsp.cf file.
- If you set a test interval in Advanced options, verify that the Statistics Window setting is greater than the Test Interval and preferably a multiple of that value. For example, a Test Interval of 60 and a Statistics Window setting of 300.

Options and Arguments

Virtual User tests require the following specific options and arguments:

- **Script Path**. The full path and file name to the WinTask executable and the WinTask script that you want to run. Enter the path to the WinTask executable first, followed by a space character and then the path to the script. Be sure to use backslashes (\) when you specify the full path.
- **Target Host**. (Optional) The hostname of the system on which to run the script.

  Note: IPv6 addresses can be used, but they must be embedded in brackets, for example [0aff::230:6eff:fe4b:51db]:8080. Here 0aff::230:6eff:fe4b:51db represents the IPv6 address and 8080 represents the port number.
- **Target Port**. (Optional) The port on the target system where the script can run.

- **Run as User**. (Optional) The user name required to run the script, if the script must run as a specific user.

  Note: The user must be a local user (no domain login) and must have the ability to log in as a service. Set the capability in Windows as follows: Control Panel > Administrative Tools > Local security policy > Local Policies > User Rights assignment > Log in as a service.

- **Password**. (Optional) The password for the user that is running the script. SRM stores the password in encrypted form.

  Note: If you specify values for hostname and port, SRM attempts to connect to the system and port through TCP Connect. If the connections are successful, it attempts to execute the script on the specified system and port. If you do not specify hostname and port, SRM does not provide the DNS name resolution or connect times.

- **Domain**. (Optional) Domain for the user who is running the script.

Specify these options and arguments when you create or modify tests.

Example

Use this example to create a test that monitors the amount of time required to run a script (C:\myScripts\playback_script.rob) on the port 8080 of mySystem every 120 seconds. This script must run as the user myVUser with a password of VUser123. The test waits up to 10 seconds for a successful response and calculates response time and availability statistics over the last 3600 seconds (1 hour).

To create a new test in a policy

1. Click + (New) on the Test Monitors toolbar.

   The New test pane appears.
2. From the Test Type list, select Virtual User.
3. In the Description field, specify vuser_test.
4. In the Test Name field, specify VUser Test.
5. In the Test Interval field, specify 120.
6. In the Test Timeout field, specify 10.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 3600.
9. In the Script Path field, specify C:\wintask\bin\wintask.exe C:\myScripts\playback_script.rob.
10. In the Target Host field, specify mySystem.
11. In the Target Port field, specify 8080.

12. In the Run as User field, specify myVUser.
13. In the Password field, specify VUser123.
14. Accept defaults for all other fields.
15. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=21
type=vuser
desc="vuser_test"
dest="C:\WinTask\bin\taskexec.exe C:\WinTask\Scripts\notepad.rob"
args=""
interval=60
samples=1
timeout=15
window=300
tos=0
limit=0
status=active
name="VUserTest"
class=""
context=""
flags="1"
loglevel=1
}
```

Errors and Availability Measurements

SRM records information about Virtual User test errors in two fields: Results Field and Error Code to help you differentiate between SRM errors and errors that the WinTask application is encountering.

The following table explains how the error codes affect availability measurements. The Results Field provides the value that WinTask returns, and the Error Code field provides the Service Availability error code.

Note: When the Error Code column is 2, the Results Field column displays the error code that was returned by the taskexec.exe application.

Results Field	Error Code	Effect on Availability	Description of Error
0	0	No effect	No errors.
Any number in the range of 300 to 400	2	Negative	SRM could not log in as the user-specified in the Run as User field.

Results Field	Error Code	Effect on Availability	Description of Error
Any number between 600,000 and 700,000	61	No effect	Possible error with the WinTask script that is running.
-1	2	Negative	System error.
Any other number	2	Negative	Possible error with the WinTask script that is running.

For information about errors you may encounter when running Virtual User tests, see Virtual User Test Error Codes (see page 290).

Keywords for Tests

All SRM tests use a keyword=value format for arguments that display in the args field. Keyword-value pairs are separated by an ampersand (&) character. For example, the arguments field for a round-trip e-mail test appears similar to the following:

```
send_proto=smtp&to=recipient&size=256&shost=senderhost&smtp_ssl=true
&send_user=sender&send_pass=secret&get_proto=pop3&source=popserver
&source_port=110&check=600
```

When you use the SRM page to add or modify tests, SRM uses the correct keywords automatically. If you are editing the svcrsp.cf file manually or using svcwatch to update the file dynamically, you must use the following keywords.

Test	Keyword	Description
Active Directory	domain	The domain in which the Active Directory server is located.
	query	The query to send to the Active Directory server.
	filter	The server-side result filter.
Custom	No additional arguments	
DHCP	No additional arguments	
DNS	hostname	The host name to look up.
File I/O	local	The local path and file name to use for write, read/write, and compare operations.
	domain	The domain of the user logging into the server (Windows only).

Test	Keyword	Description
	op	One of the following: ■ r – Reads the file. ■ w – Writes the contents of a local reference file to a test file located on a remote file system, and then deletes the test file. ■ rw – Writes the contents of a local reference file to a test file on a remote file system, reads the test file, and then deletes it. ■ cmp – Reads in one file and then another, and compares their contents.
FTP	local	Specifies the name of the file to be written to on the FTP Server.
	remote	Specifies the path of the file to be read.
	op	One of the following: ■ g - (get) Log in and read the specified file (but does not perform a write operation), then log out. ■ p - (put) Log in and write the specified file out to the FTP Server, then log out. If the remote directory does not have writer permission, the test will fail. ■ login (no remote and local keywords) - Log in using the specified username and password and then log out.
HTTP and HTTPS	max_depth	The number of levels the test should traverse when downloading nested frames. (The HTTP and HTTPS tests download all frames, images, external scripts, and applets during the page download so that the measurement reflects the user's experience when downloading a Web page.) The default value is 3.
	proxy	The hostname of the proxy server to use if the system from which you are testing does not have direct Internet access.
	proxyuser	The user name for this proxy.
	proxypass	The password of the proxy user.

Test	Keyword	Description
	content_dl	■ true - Downloads content including scripts, images, applets, and so on. ■ false - Does not download content.
	content_err	■ true - Any errors while downloading cause the test to fail. ■ false - Errors are not considered during download.
	minmatch	Minimum number of times to find the search pattern.
	search	A regular expression you want SRM to match on the pages you test.
IMAP	download	The emails to download; one of the following: ■ Download First Message – Downloads only the first message for this user account. ■ Download All Messages – Downloads all messages for this user account.
	delete	Whether to delete downloaded messages; one of the following: ■ true – Deletes downloaded messages. ■ false – Does not delete downloaded messages.
LDAP	query	Specifies the query to send to the LDAP server.
	domain	Specifies the LDAP domain.
	filter	Specifies the server-side result filter.
MAPI	domain	The Windows domain for the user account.
	op	■ send - Sends the test message. ■ recv - Receives a test message.

Test	Keyword	Description
	download	The emails to download; one of the following: ■ Download First Message – Downloads only the first message for this user account. ■ Download All Messages – Downloads all messages for this user account.
	to	■ Specifies the email recipient of the test message.
	size	■ Specifies the size of the test message in bytes. Default 256
	delete	Whether to delete downloaded messages; one of the following: ■ true – Deletes downloaded messages. ■ false – Does not delete downloaded messages.
NIS	domain	Specifies the domain on which the map file exists.
	map	Specifies the map file to test. Default: host
	download	■ true - Downloads the specified NIS map. ■ false - Does not download the specified map.
File I/O	local	The local path and file name to use for write, read/write, and compare operations.
	domain	The domain of the user logging into the server (Windows only).
NNTP	No additional arguments	
PING	payload	The size of the packet sent in the ping. The default packet size is 64 bytes.
POP3	download	The emails to download; one of the following: ■ Download First Message – Downloads only the first message for this user account. ■ Download All Messages – Downloads all messages for this user account.

Test	Keyword	Description
	delete	Whether to delete downloaded messages; one of the following: ■ true – Deletes downloaded messages. ■ false – Does not delete downloaded messages.
Round-Trip Email	to	The user account who receives the message.
	size	The size of the email to send in bytes. Default 256
	send_proto	The protocol to use for sending mail; one of the following: ■ smtp ■ mapi
	shost	Specifies the host name which sends the message.
	smtp_ssl	■ true - Enables SMTP SSL encryption. ■ false - Disables SMTP SSL encryption.
	send_user	Specifies the name of the sender account.
	send_pass	Specifies the password of the sender.
	sdomain	(MAPI protocol only) The user domain for sending messages with the MAPI protocol.
	get_proto	The protocol to use for receiving mail; one of the following: ■ pop ■ imap ■ mapi
	source	Specifies the host to which the email is sent.
	source_port	Specifies the port number for IMAP or POP3. Defaults: 110 (POP3), 143 (IMAP)
	gdomain	(MAPI protocol only) The user domain for retrieving messages with the MAPI protocol.
	check	Specifies the poll interval in seconds. Default: 600

Test	Keyword	Description
	delete	Whether to delete downloaded messages; one of the following: ■ true – Deletes downloaded messages. ■ false – Does not delete downloaded messages.
SMTP	to	The user account to receive the email.
	size	The size of the email to send in bytes. Default: 256
	shost	Specifies the host name which sends the message.
	ssl	■ true - Enables SMTP SSL encryption. ■ false - Disables SMTP SSL encryption.
SNMP	snmpversion	■ snmp - Specifies SNMPv1/2. ■ snmp3 - Specifies SNMPv3.
	user	Specifies the SNMPv3 user name.
	securitylevel	Specifies the SNMPv3 security level: ■ AuthPriv - Authentication and Privacy ■ NoAuthNoPriv - No Authentication and no Privacy ■ AuthNoPriv - Authentication and no Privacy
	auth_protocol	Specifies the SNMPv3 authentication protocol: ■ MD5 ■ SHA
	auth_password	Specifies the authentication password.
	priv_protocol	Specifies the SNMPv3 privacy protocol: ■ DES ■ AES ■ 3DES
	priv_password	Specifies the privacy password.
	oid	The object identifier of the variable to query.
	community	The community string for reading the variable.

Test	Keyword	Description
SQL Query	query	The query to send to the database.
	qtype	(Optional) The type of the query. Valid values are: ■ query - (Default) The query argument represents a normal query, for example, SELECT. ■ stored - The query argument represents the argument for an EXECUTE query; a stored procedure and arguments. ■ update - The query argument contains an update query, For example, INSERT. This query type returns an integer value: -1, 0, positive integer
	dbtype	Specifies the type of the database: ■ oracle ■ mssql ■ other
	driver	(for 'other' databases) The JDBC driver to use for the query.
	url	(for 'other' databases) The database connect string; varies by database type. For information about connect strings, refer to your database documentation.
	dbname	The name of the database to query. When using "other" as database type, this field does not appear in the user interface. Specify the database name in the connect string instead.
TCP Connect	No additional arguments	
TFTP	path	The path and file name of the file to read or write.
	op	One of the following: ■ r – Reads a file from the server. ■ w – Writes a file to a remote file system.
Virtual User	domain	The domain for the user who is running the script.
	port	The port on which the script is running.
	hostname	The hostname of the destination system; this

Test	Keyword	Description
		value is used for DNS lookup and connection timings.

Using Custom Scripts to Create Tests

You can create a custom script to instruct SRM to perform a custom test on a local system.

Guidelines for Creating Custom Tests

Consider the following when creating custom tests:

- If a custom test returns a value <= 0 for name resolution time, connection time, or transaction time, the test availability is set to 0.
- The unit for times reported by a custom script is milliseconds.
- A successful custom script needs to return integer values only.
- A successful script returns 0 as its exit code. A value other than 0 represents a failed custom script.
- The result code is placed in the results field in the MIB for that test.

Guidelines for Writing the Script

You can write the script as a binary executable or in a scripting language such as UNIX shell or Perl. Custom response modules work very much like SystemEDGE agent extension objects. For more information about SystemEDGE extension objects, see the *SystemEDGE User Guide*. SRM expects the custom script to provide a single line of output with *at least* three values (and up to six values) followed by a line feed.

The script you create must return the following information in this order:

1. DNS resolution time (required)
2. Connection time (required)
3. Transaction time (required)
4. Result code (optional)
5. Bytes in (optional)
6. Bytes out (optional)

SRM calculates throughput based out on the data the script returns for bytes in and bytes out. Therefore, if the script provides bytes in, it must also provide bytes out (and vice versa). Correct output from the script must be one of the following three options:

Option A:

1. DNS resolution time
2. Connection time
3. Transaction time

Option B:

1. DNS resolution time
2. Connection time
3. Transaction time
4. Result code

Option C:

1. DNS resolution time
2. Connection time
3. Transaction time
4. Result code
5. Bytes in
6. Bytes out

Options and Arguments

Custom tests require the following specific option or argument:

Script Path – The full path and file name to the custom script that you want to run.

Note: When you are specifying pathnames, be sure to use the correct type of slashes for the operating system on which the test runs, that is, use forward slashes (/) when you specify directories for tests that you intend to run on UNIX systems and backslashes (\) when you specify directories for tests that you intend to run on Windows systems.

When you specify the timeout value for Custom tests, ensure that it provides enough time to allow the script to execute. If the script does not have enough time to execute, SRM will terminate it, and if the script does not clean up its own child processes, those processes continue to run, which could eventually cause the system to hang.

You specify this option or argument when you create or modify tests.

Example

Use this example to create a test that monitors the amount of time that is required to run the script located in /local/bin/custom_Test.pl. The entry instructs the agent to test the service once every 120 seconds (2 minutes), and to wait up to 20 seconds for a successful response. The agent calculates statistics over the last 3600 seconds (6 hours).

Do the following on the Create a new Test page

1. Select Advanced next to Common Options.
2. From the Test Type list, select Custom.
3. In the Test Name field, specify custom_Test.pl.
4. In the Description field, specify Test Custom Service.
5. In the Test Interval field, specify 120.
6. In the Test Timeout field, specify 20.
7. In the Samples Per Interval field, specify 1.
8. In the Statistics Window field, specify 3600.
9. In the Script Path field, specify /local/bin/custom_Test.pl.
10. Click Save Test.

When you commit your changes, SRM adds an entry similar to the following to the svcrsp.cf file:

```
{
index=99
type=custom
desc="Test custom service"
dest="/local/bin/custom_Test.pl"
interval=120
samples=1
timeout=20
window=3600
tos=0
limit=0
status=active
name="Custom Service Test"
class=""
context=""
flags="1"
loglevel=1
}
```

For information about errors you may encounter when running custom tests, see Custom Test Error Codes (see page 274).

Appendix A: Service Response Monitor CLI Commands

You can use the CLI commands to script and automate CA Service Response Monitor and run actions based on the command results.

This section contains the following topics:

svcwatch add adir Command--Add an Active Directory Test

The svcwatch add adir command adds an Active Directory test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr adir destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

adir

Specifies the Active Directory service type.

destination

Specifies the domain controller for the test.

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

domain=*domain* - The domain in which the Active Directory server is located.

query=*query* - The query to send to the Active Directory server.

filter=*filter* - The server-side result filter.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding an Active Directory test:

```
svcwatch -p 161 -c admin -o add 1360740 "AD-TEST" adir "DC.com" "ADUser"
"bXVyaWM=" "domain=mylab.com&query=cn=Registered,cn=Users,dc=mylab,
dc=com&filter=cn=*" 30 3 30 60 0 0 0x100 "AD-TEST" "ClassName"
"ContextName" 7
```

More Information

Keywords for Tests (see page 131)

svcwatch add custom Command--Add a Custom Test

The svcwatch add custom command adds a custom test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr custom destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

custom

Specifies the Custom service type.

destination

Specifies the path of the script.

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

No arguments available for the Custom service type. An empty string in quotes "" specifies no arguments.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131)

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding a custom test:

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360741 "CUSTOM-TEST" custom
"c:\scripts\custom-test.bat" "" "" "" 30 3 30 60 0 0 0x100 "Custom-TEST"
"ClassName" "ContextName" 7
```

More Information

Keywords for Tests (see page 131)

svcwatch add dhcp Command--Add a DHCP Test

The svcwatch add dhcp command adds a DHCP test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr dhcp destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

dhcp

Specifies the DHCP service type.

destination

Specifies the host name or IP address of the DHCP server to test.

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

No arguments available for the DHCP service type. An empty string in quotes "" specifies no arguments.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding a DHCP test:

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360742 "DHCP-TEST" dhcp
"dhcpservername" "" "" "" 30 3 30 60 0 0 0x100 "DHCP-TEST" "ClassName"
"ContextName" 7
```

More Information

Keywords for Tests (see page 131)

svcwatch add dns Command--Add a DNS Test

The svcwatch add dns command adds a DNS test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr dns destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

dns

Specifies the DNS service type.

destination

Specifies the DNS server for the test.

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service argument. The argument is a pair of a parameter and a value (hostname=*host*) which is enclosed in quotes.

hostname=*host* - The host name to look up.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding a DNS test:

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360743 "DNS-TEST"
dns "mydnsserver" "" "" "hostname=testhost" 30 3 30 60 0 0 0x100
"DNS-Test" "ClassName" "ContextName" 7
```

More Information

Keywords for Tests (see page 131)

svcwatch add fileio Command--Add a File IO Test

The svcwatch add fileio command adds a file IO test to SRM on the specified host.

This command has the following format:

svcwatch [-h| -p| -v| -u| -n| -a| -A| -x| -X| -m| -t| -d| -f] -o add *index descr* fileio *destination username password args interval samples timeout winsiz tos limit flags name class contextInfo logLevel*

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

fileio

Specifies the File IO service type.

destination

Specifies the remote file to test.

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

op=r - Reads the file.

op=w - Writes the contents of a local reference file to a test file located on a remote file system, and then deletes the test file.

op=rw - Writes the contents of a local reference file to a test file on a remote file system, reads the test file, and then deletes the test file.

op=cmp - Reads in one file and then another, and compares their contents.

local=*path* - The local path and file name to use for write, read/write, and compare operations.

domain=*domain* - The domain of the user logging in to the server (Windows only).

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding a file I/O test:

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360744 "FILEIO-TEST"
fileio "F:\Test\CompTest.bin" "" "" "op=cmp&local=C:\sysedge\bin\saFileIOTest.bin"
30 1 10 120 0 0 0x100 "FILEIO-TEST" "" ""
```

More Information

Keywords for Tests (see page 131)

svcwatch add ftp Command--Add an FTP Test

The svcwatch add ftp command adds an FTP test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr ftp destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

ftp

Specifies the FTP service type.

destination

Specifies the FTP server for the test.

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

op=g (get) - Log in and read the specified file (but does not perform a write operation), then log out.

op=p (put) - Log in and write the specified file out to the FTP Server, then log out. If the remote directory does not have writer permission, the test fails.

op=login - Log in using the specified username and password and then log out.

remote=*path* - Specifies the path of the file to read.

local=*path* - Specifies the name of the file to write to on the FTP Server.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding an ftp test:

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360745 "FTP-TEST"
ftp "ftpstage.mydomain.com:21" "ftpuser" "ftp123" "op=login" 3600 1
10 604800 0 0 0x100 "FTP-TEST" "" "" 1
```

More Information

Keywords for Tests (see page 131)

svcwatch add http | https Command--Add an HTTP or HTTPS Test

The svcwatch add http | https command adds an HTTP or HTTPS test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr {http|https} destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

http | https

Specifies the HTTP or HTTPS service type.

destination

Specifies the web server for the test.

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

max_depth=*number* - The number of levels the test traverses when downloading nested frames (HTTP and HTTPS tests download all frames, images, external scripts, and applets during page download so that the measurement reflects the user experience when downloading a page).

Default: 3

search=*pattern* - A regular expression you want SRM to match on the pages you test.

minmatch=*number* - Minimum number of times to find the search pattern.

content_dl=true|false - Download content including scripts, images, applets, and so on.

content_err=true|false - Any errors while downloading cause the test to fail.

proxy=*proxy* - The hostname of the proxy server to use if the system from which you are testing does not have direct internet access.

proxyuser=*puser* - The user name for this proxy.

proxypass=*ppass* - The password of the proxy user.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding an https test:

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360746 "HTTPS-TEST"
https "https://chargeMycredit.com" "creditAcct" "secret"
"max_depth=3&minmatch=1&content_dl=true&content_err=false" 60 1 20
300 0 0 0x100 "HTTPS-TEST" "" ""
```

More Information

Keywords for Tests (see page 131)

svcwatch add imap Command--Add an IMAP Test

The svcwatch add imap command adds an IMAP test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr imap destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

imap

Specifies the IMAP service type.

destination

Specifies the IMAP server and port for the test (*server*:*port*). Default port: 143

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

download=Download First Message - Downloads only the first message for this user account.

download=Download All Messages - Downloads all messages for this user account.

delete=true - Deletes downloaded messages.

delete=false - Does not delete downloaded messages.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding an IMAP test:

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360747 "IMAP-TEST"
imap "imapserver.yourdomain.com:143" "IMAPuser@server.domain" "IMAP123"
"download=Download All Messages&delete=true" 300 1 10 7200 0 0 0x100
"IMAP-TEST" "" ""
```

More Information

Keywords for Tests (see page 131)

svcwatch add ldap Command--Add an LDAP Test

The svcwatch add ldap command adds an LDAP test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr ldap destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

ldap

Specifies the LDAP service type.

destination

Specifies the LDAP server and port for the test (*server:port*). Default port: 389

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

query=*query* - Specifies the query to send to the LDAP server.

domain=*domain* - Specifies the LDAP domain.

filter=*filter* - Specifies the server-side result filter.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding an LDAP test:

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360748 "LDAP-TEST"
ldap "arch" "ldapUser" "ldapPassword" "query=cn=annuity,ou=Boston,
dc=fleet,dc=com&domain=Test&filter=cn=*" 30 1 10 120 0 0 0x100
"LDAP-TEST" "" ""
```

More Information

Keywords for Tests (see page 131)

svcwatch add mapi Command--Add a MAPI Test

The svcwatch add mapi command adds a MAPI test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr mapi destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

mapi

Specifies the MAPI service type.

destination

Specifies the MAPI server for the test.

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

domain=*domain* - The Windows domain for the user account.

op=send - Sends the test message.

op=recv - Receives a test message.

download=Download First Message - Downloads only the first message for this user account.

download=Download All Messages - Downloads all messages for this user account.

to=*recipient* - Specifies the email recipient of the test message.

size=*number of bytes* - Specifies the size of the test message in bytes. Default 256

delete=true - Deletes downloaded messages.

delete=false - Does not delete downloaded messages.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding a MAPI test:

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360749"MAPI-TEST"
mapi "mapiserver.yourdomain.com" "MAPIuser" "MAPI123" "domain=myDomain
&op=send&to=congo@yourdomain.com&size=256" 120 1 10 3600 0 0 0x100
"MAPI-TEST" "" ""
```

More Information

Keywords for Tests (see page 131)

svcwatch add nis Command--Add a NIS Test

The svcwatch add nis command adds an NIS test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr nis destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

nis

Specifies the NIS service type.

destination

Specifies the NIS server for the test.

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

domain=domain - Specifies the domain on which the map file exists.

map=map - Specifies the map file to test. Default: hosts

download=true|false - Specifies whether to download the NIS map.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding an NIS test:

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360750 "NIS-TEST"
nis "nisserver.yourdomain" "" "" "domain=Test.com&map=hosts&download=true"
300 1 20 7200 0 0 0x100 "NIS-TEST" "" ""
```

More Information

Keywords for Tests (see page 131)

svcwatch add nntp Command--Add an NNTP Test

The svcwatch add nntp command adds an NNTP test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr nntp destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

nntp

Specifies the NNTP service type.

destination

Specifies the NNTP server and port for the test (*server*:*port*). Default port: 119

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

No arguments available for the NNTP service type. An empty string in quotes "" specifies no arguments.

Note: For details of the particular arguments for each service type, see Keywords for Test Arguments (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding an NNTP test:

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360751 "NNTP-TEST" nntp
"nntpservername:119" "" "" "" 30 3 30 60 0 0 0x100 "TestNNTP" "ClassName"
"ContextName" 7
```

More Information

Keywords for Tests (see page 131)

svcwatch add ping Command--Add a PING Test

The svcwatch add ping command adds a PING test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr ping destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

ping

Specifies the PING service type.

destination

Specifies the target computer for the test.

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service argument. The argument is a pair of a parameter and a value (payload=*number of bytes*) which is enclosed in quotes.

payload=*number of bytes* - The size of the packet sent in the ping. The default packet size is 64 bytes.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding a ping test:

```
svcwatch -h localhost -p 161 -c admin -o add 1360752 "TEST" ping "127.0.0.1"
"" "" "payload=1000" 30 3 30 60 0 0 0x100 "TestPING" "ClassName" "ContextName" 7
```

More Information

Keywords for Tests (see page 131)

svcwatch add pop3 Command--Add a POP3 Test

The svcwatch add pop3 command adds a POP3 test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr pop3 destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

pop3

Specifies the POP3 service type.

destination

Specifies the POP3 server and port (*server:port*) for the test. Default port: 110

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

download=Download First Message - Downloads only the first message for this user account.

download=Download All Messages - Downloads all messages for this user account.

delete=true - Deletes downloaded messages.

delete=false - Does not delete downloaded messages.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding a POP3 test:

```
svcwatch -h localhost -p 161 -c doublesecret -o add 1360753 "POP3-TEST"
pop3 "mypop3server:110" "pop3user" "pop3pass" "download=Download First Message
&delete=true" 30 3 30 60 0 0 0x100 "TestPOP3" "ClassName" "ContextName" 7
```

More Information

Keywords for Tests (see page 131)

svcwatch add rtemail Command--Add a Round Trip Email Test

The svcwatch add rtemail command adds a round-trip email test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr rtemail destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

rtemail

Specifies the round-trip email service type.

destination

Specifies the SMTP or MAPI server for the test (*smtpserver*:*port*). Default SMTP port: 25

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

send_proto=smtp|mapi - Specifies the sending protocol.

to=*recipient* - Specifies the name of the email recipient.

size=*number of bytes* - Specifies the size of the test message in bytes. Default 256

shost=*senderhost* - Specifies the host name which sends the message.

smtp_ssl=true|false - Specifies whether SMTP SSL encryption is enabled.

send_user=*suser* - Specifies the name of the sender account.

send_pass=*spass* - Specifies the password of the sender.

sdomain=*domain* - (MAPI only) Specifies the domain the sender belongs to.

get_proto=pop3|imap|mapi - Specifies the receiving protocol.

source=*targethost* - Specifies the host to which the email is sent.

source_port=*port* - Port number for IMAP or POP3. Defaults: 110 (POP3), 143 (IMAP)

gdomain=*domain* - (MAPI only) Specifies the domain the receiver belongs to.

check=*poll interval* - Specifies the poll interval in seconds. Default: 600

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding a round-trip email test:

```
svcwatch -p 161 -c admin -o add 1360754 "RT-EMAIL TEST" rtemail
"mysmtp.com:25" "smtpuser" "zrvr8tx" "send_proto=smtp&to=recipient
&size=256&shost=senderhost&smtp_ssl=true&send_user=sender&send_pass=secret
&get_proto=pop3&source=popserver&source_port=110&check=600"
30 3 30 60 0 0 0x100 "TestRTEMAIL" "ClassName" "ContextName" 7
```

More Information

Keywords for Tests (see page 131)

svcwatch add smtp Command--Add an SMTP Test

The svcwatch add smtp command adds an SMTP test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr smtp destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

smtp

Specifies the SMTP service type.

destination

Specifies the SMTP server and port (*server*:*port*) for the test. Default port: 25

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

to=*recipient* - Specifies the name of the email recipient.

size=*number of bytes* - Specifies the size of the test message in bytes. Default 256

shost=*senderhost* - Specifies the host name which sends the message.

ssl=true|false - Specifies whether SMTP SSL encryption is enabled.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding an SMTP test:

```
svcwatch -p 161 -c admin -o add 1360755 "SMTP TEST" smtp "mysmtp.com:25"
"smtpuser" "zrvr9tx" "to=recipient&size=256&shost=senderhost&smtp_ssl=true"
30 3 30 60 0 0 0x100 "TestSMTP" "ClassName" "ContextName" 7
```

More Information

Keywords for Tests (see page 131)

svcwatch add snmp Command--Add an SNMP Test

The svcwatch add snmp command adds an SNMP test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr snmp destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

snmp

Specifies the SNMP service type.

destination

Specifies the SNMP agent host and port (*server*:*port*) for the test. Default SNMP port: 161

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

snmpversion=snmp|snmp3 - Specifies SNMPv1/2 or SNMPv3.

user=*user name* - Specifies the SNMPv3 user name.

securitylevel=AuthPriv|NoAuthNoPriv|AuthNoPriv - Specifies the SNMPv3 security level

auth_protocol=MD5|SHA - Specifies the SNMPv3 authentication protocol.

auth_password=*password* - Specifies the authentication password.

priv_protocol=DES|AES|3DES - Specifies the SNMPv3 privacy protocol.

priv_password=*password* - Specifies the privacy password.

oid=*oid* - The object identifier of the variable to query.

community=*string* - The community string for reading the variable.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Examples

Adding an SNMPv1 test:

```
svcwatch -p 161 -c admin -o add 1360757 "SNMP TEST" snmp "myhost:161" "" ""
"snmpversion=snmp&oid=1.3.6.1.4.1.546.1.1.7.8.27.0&community=admin" 30 3 30
60 0 0 0x100 "TestSNMP" "" "" 7
```

Adding an SNMPv3 test:

```
svcwatch -p 161 -c admin -o add 1360756 "SNMP3 TEST" snmp "myhost:161" "" ""
"snmpversion=snmp3&user=admin&securitylevel=AuthPriv&auth_protocol=MD5
&auth_password=XP1abcTZ&oid=1.3.6.1.4.1.546.1.1.7.8.27.0&community=topsecret"
30 3 30 60 0 0 0x100 "TestSNMP3" "" "" 7
```

More Information

Keywords for Tests (see page 131)

svcwatch add sql Command--Add an SQL Test

The svcwatch add sql command adds a SQL test to SRM on the specified host. For details and prerequisites, see SQL Query Tests (see page 117) in this guide.

This command has the following format:

```
svcwatch [options] -o add index descr sql destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

sql

Specifies the SQL service type.

destination

Specifies the database server and port (*server*:*port*) for the test. Default ports: 1433 (SQL Server), 1521 (Oracle)

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

query=*query* - Specifies the SQL query.

qtype=query|stored|update - (Optional) Specifies the query type (Default: query)

dbtype=oracle|mssql|other - Specifies the database type.

dbname=*name* - (oracle and mssql only) Specifies the database name. When you select "other", specify the database name in the connect string.

driver=driver - (other only) The JDBC driver to use for the query.

url=*string* - (other only) The database connect string; varies by database type. For information about connect strings, refer to your database documentation.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Examples

Adding a SQL server test:

```
svcwatch -p 161 -c admin -o add 1360758 "TestSqlServer" sql
"192.168.100.100:1433" "sa" "AdminLvl1" "query=select * from
vas_system&dbtype=mssql&dbname=vasdb" 30 3 30 60 0 0 0x100
"TestSQL" "" ""
```

Adding a SQL server JDBC driver test:

```
svcwatch -p 161 -c admin -o add 1360761 "TestSqlServerJDBCDriver"
sql "192.168.100.100:1433" "sa" "AdminLvl1" "query=select * from
my_system&dbtype=other&driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
&url=jdbc:sqlserver://hostnameValue:portValue;databaseName=vasdb;
user=unameValue;password=pwdValue" 30 3 30 60 0 0 0x100
"TestSqlServerJDBCDriver" "" ""
```

Adding an Oracle test:

```
svcwatch -p 161 -c admin -o add 1360759 "TestOracle" sql
"192.168.101.101:1521" "joe" "AdminLvl1" "query=select * from big_system
&dbtype=oracle&dbname=bigdb" 30 3 30 60 0 0 0x100 "TestOracle" "" ""
```

Adding an Oracle JDBC Thin Driver test:

```
svcwatch -p 161 -c admin -o add 1360762 "TestOracleJDBCThinDriver" sql
"192.168.101.101:1521" "joe" "AdminLvl1" "query=select table_name from
user_tables&dbtype=other&driver=oracle.jdbc.OracleDriver
&url=jdbc:oracle:thin:unameValue/pwdValue@hostnameValue:portValue:orcl"
30 3 30 60 0 0 0x100 "TestOracleThin" "" ""
```

More Information

SQL Query Tests (see page 117)
Keywords for Tests (see page 131)

svcwatch add tcpconnect Command--Add a TCP Connect Test

The svcwatch add tcpconnect command adds a TCP Connect test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr tcpconnect destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

tcpconnect

Specifies the TCP Connect service type.

destination

Specifies the remote host and port (*server*:*port*) for the test.

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

No arguments available for the DHCP service type. An empty string in quotes "" specifies no arguments.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding a TCP connect test:

```
svcwatch -p 161 -c admin -o add 1360763 "Test" tcpconnect
"192.168.90.10:1433" "" "" "" 60 5 30 60 0 0 0X100
"Testtcpconnect" "" "" 1
```

Here, as host is not specified, default is localhost. The port number is 161. 'add' adds new test to SRM. The unique svcRspTable index number is 2013."Test" is the description of this test. tcpconnect specifies TCP Connect service type. The details of remote host and port tested is 192.168.90.10:1433.

The two empty strings in quotes ("") specify no user name and password used for authentication. "" specifies no arguments available for tcpconnect service type. The test interval is specified as 60 seconds. The number of samples tested per interval is 5. The timeout is 30 seconds. The statistics window size is 60 seconds. 0 (zero) specifies a normal service (and not IP Type of Service or Differentiated Services)

0 (zero) specifies the acceptable performance limit (or threshold) for the total response time of this test. This test is executed on request only (run once) with flag set to 0x100. Specifies the unique name per service type as Testtcpconnect. Specifies no class name, and context information in "". This test is executed with log level as critical with '1'.

More Information

Keywords for Tests (see page 131)

svcwatch add tftp Command--Add a TFTP Test

The svcwatch add tftp command adds a TFTP test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr tftp destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

tftp

Specifies the TFTP service type.

destination

Specifies the TFTP server and port (*server*:*port*) for the test. Default port: 69

username

Specifies the user name for authentication in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

op=r - Reads a file from the server.

op=w - Writes a file to a remote file system.

path=*path* - The path and file name of the file to read or write.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding a TFTP test:

```
svcwatch -p 161 -c admin -o add 1360764 "Test" tftp "192.168.120.10:69"
"" "" "op=r&path=I:\SA\TFTP\get.txt" 60 3 30 60 0 0 0X100 "Testtftp"
"" "" 0
```

More Information

Keywords for Tests (see page 131)

svcwatch add vuser Command--Add a Virtual User Test

The svcwatch add vuser command adds a Virtual User test to SRM on the specified host.

This command has the following format:

```
svcwatch [options] -o add index descr vuser destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

The add command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o add *testparams*

Adds a new test to SRM.

testparams

Specifies the parameters for the new test.

index

Specifies the svcRspTable index.

descr

Specifies the description of the test in quotes. An empty string in quotes "" specifies no description.

vuser

Specifies the Virtual User service type.

destination

Specifies the path of the script for the test.

username

Specifies the user name to run the script in quotes. An empty string in quotes "" specifies no user name.

password

Specifies the password for authentication in quotes. An empty string in quotes "" specifies no password.

args

Specifies the service arguments. Each argument is a pair of a keyword and a value (key=value). Multiple arguments are concatenated and delimited by ampersands (&). The complete arguments string is enclosed in quotes.

General syntax for arguments: "key1=value1[&key2=value2& ...]"

host=*hostname*:*port* - The hostname of the destination system; this value is used for DNS lookup and connection timings. The port on which the script is running.

domain=*domain* - The domain of the user who is running the script.

Note: For details of the particular arguments for each service type, see Keywords for Tests (see page 131).

interval

Specifies the test interval in seconds.

Limits: multiple of 30 seconds

samples

Specifies the samples per interval.

timeout

Specifies the timeout in seconds.

winsiz

Specifies the statistics window size in seconds.

tos

Specifies the IP Type of Service or Differentiated Services Code. Use 0 (zero) for a normal service. See also RFC 1349.

limit

Specifies the acceptable performance limit (or threshold) for the total response time of this test. This value is used in reports.

flags

Specifies the following flags:

0x001 = collect performance cubes

0x100 = execute on request only (run once)

name

Specifies the unique name per service type. An empty string in quotes "" specifies no test name.

class

Specifies the class name. An empty string in quotes "" specifies no class name.

contextInfo

Specifies context information. An empty string in quotes "" specifies no context information.

logLevel

Specifies the log level for the test execution code. Possible values are:

-2 = use SRM-global log level (default)

-1 = do not log

0 = fatal (only the most important messages)

1 = critical

...

7 = debug3 (log all messages)

Example

Adding a virtual user test:

```
svcwatch -h localhost -p 161 -c snmp_admin -o add 1360765 "vUser Test"
vuser "C:\WinTask\bin\taskexec.exe C:\WinTask\Scripts\notepad.rob" ""
"" "" 30 1 10 120 0 0 0x001 "vUserTEST" "ClassName" "ContextName" 7
```

More Information

Keywords for Tests (see page 131)

svcwatch delete Command--Delete a Test

The svcwatch delete command deletes a test on the specified host.

This command has the following format:

```
svcwatch [options] -o delete index
```

The delete command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o delete *index*

Deletes the specified test.

index

Specifies the svcRspTable index used to identify the test to delete.

Example

Delete a test on myremote host:

```
svcwatch -h myremote -p 161 -c admin -o delete 1360739
```

svcwatch list Command--View Test Information

The svcwatch list command lists the available tests on the specified host.

This command has the following format:

```
svcwatch [options] -o list
```

The list command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o list

Lists available tests.

Example

Listing tests on localhost:

```
svcwatch -o list
```

svcwatch setstatus Command--Change the Status of a Test

The svcwatch setstatus command changes the status of a test on the specified host.

This command has the following format:

```
svcwatch [options] -o setstatus index status
```

The setstatus command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o setstatus *index status*

Specifies the new status of a test.

index

Specifies the svcRspTable index used as an identifier of the test.

Note: You overwrite an existing test with a new test, when you use the add command with the index of that test.

status

Specifies the status. Possible values are:

active (1),

notInService (2),

notReady (3),

createAndGo (4),

createAndWait (5),

destroy (6)

Example

Change the status of a test:

```
svcwatch -p 161 -c admin -o setstatus 1360739 2
```

svcwatch version Command--View SRM Version Information

The svcwatch version command displays the version of the SRM AIM on the specified host.

This command has the following format:

```
svcwatch [options] -o version
```

The version command uses the following parameters:

options

Specifies the possible options for this command.

-h *hostname* | -h *ipAddr*

(Optional) Specifies the SystemEDGE host.

Default: localhost

-p *port*

(Optional) Specifies the SystemEDGE SNMP port.

Default: 161

-c *community*

(Optional) Specifies the SNMP community string for SNMP version 1 and 2c.

Default: public

-v *snmpVersion*

(Optional) Specifies the SNMP version. Possible values are:

- 1
- 2c
- 3

Default: 1

-u *secName*

(Optional) Specifies the name of the SNMPv3 secure user.

-u *secLevel*

(Optional) Specifies the level of security for SNMPv3. Possible values are:

- 1 – noAuthNoPriv
- 2 – AuthNoPriv
- 3 – AuthPriv

-n *contextName*

(Optional) Specifies the instance name for a MIBMuxed agent.

-a *authPassword*

(Optional) Identifies the authentication password required when SNMPv3 is selected with security AuthNoPriv or AuthPriv.

-A *authProtocol*

(Optional) Specifies the authentication protocol. Possible values are:

- MD5 – authentication protocol HMAC-MD5
- SHA – authentication protocol HMAC-SHA

Default: MD5

-x *privPassword*

(Optional) Specifies the privacy (encryption) password for SNMPv3 with security level 3 (AuthPriv).

-X *encryptProtocol*

(Optional) Specifies the use of encryption protocol for privacy. Possible values are:

- DES – Data Encryption Standard
- AES – Advanced Encryption Standard using cryptographic keys of 128 bits (AES128)
- 3DES – Triple Data Encryption Standard

-m *FIPSmode*

(Optional) Specifies the FIPS mode. Possible values are:

- 0 – non-FIPS
- 1 – FIPS coexistence
- 2 – FIPS only

Default: 0

-t *timeout*

(Optional) Specifies the SNMP command timeout.

Default: 10 seconds

-d *logLevel*

(Optional) Specifies the log level for SNMP messages. Possible values are:

- 0 – log fatal messages
- 1 – log critical messages
- 2 – log warning messages
- 3 – log information messages
- 4 – log all messages
- 5 – log all messages including debugging messages

Default: 0

-f *logFile*

(Optional) Specifies the name of the logfile.

Default: sysedge_utility.log

-L

(Optional) Detects the current locale of the console and language catalog if available. If a language catalog is not found, the utility falls back to English as a default language.

-o version

Displays the version of the CA SystemEDGE AIM for Service Response Monitoring.

Example

Display the version on myremote host:

```
svcwatch -h myremote -o version
```

Appendix B: Installation

This section contains the following topics:

Installation Through CA Virtual Assurance Setup

When you run the CA Virtual Assurance custom installation, you can select the AIMs which you want to install. The custom installation installs SystemEDGE and all AIMs by default on the manager system.

Remote Deployment

You can install SystemEDGE and AIMs on AIX, HP-UX, Linux, Solaris, or Windows systems from the CA Virtual Assurance Manager through Remote Deployment.

To deploy agents to systems, create a deployment job. Deployment jobs contain the details that are required for CA Virtual Assurance to deliver the deployment packages to the appropriate systems at the appropriate time.

Follow these steps:

1. Select Resources, Deploy.

   The Deployment pane displays the Packages, Templates, and Jobs.

2. Right-click the Jobs folder in the Manage Resource pane and select Create New Job. You can also select the Jobs folder and Click + (New) on the Job Status toolbar.

   The Jobs Setup page appears.

3. Enter a name in the Job Name pane and optionally base the job on an existing template, and click Next.

   The Package Selection page appears.

4. Select a platform and the packages you want to deploy.

5. (Optional) Click the Details tab.

   The Package Wrapper Details dialog appears and lets you edit the package properties in-line. If the package wrappers are in an incomplete or invalid state, and the fields can be modified through in-line editing.

   a. Click Edit and modify the package wrapper properties.

   b. Click Save, and then click OK.

      The package wrapper properties are updated.

6. Click the down arrow to add the package wrappers to the job, and click Next.

   The Machine Selection page appears.

7. Select the systems to deploy to and click Next. If you have many servers in your environment, multiple pages with some entries can be required to list all servers. When you select servers on a page and scroll to the next page, any selections that are made on previous pages remain valid.

   The Machines Selected page appears.

8. Click Set Credentials, set the system credentials that are required to establish a connection and click Next.

   Note: Deployment to Windows target systems using domain credentials must be in the form of DOMAIN\username.

   The Advanced page appears.

9. (Optional) Set the distribution server to manage the deployment. If not set, it is automatically chosen.

10. Select the scheduling options for the job:

    Immediate Delivery

    Starts the job immediately after creating new deployment job. The immediate delivery is the default option.

    Staggered Delivery

    Delivers the packages over a specific time period.

    Scheduled Delivery

    Schedules the deployment for a specific time in the future.

11. (Optional) If a package has previously been successfully deployed to a system using this deployment infrastructure, you can force it to run again.

12. Click Next.

    The Summary page appears.

13. Review the details of the job and click Deploy.

    The deployment job is created.

Note: You can save the job as a template after you create it. A template saves the package and machine selections so that you can easily reuse them for subsequent jobs.

Individual Installation

When you install the SRM AIM on top of SystemEDGE, consider that the SRM AIM depends on Advanced Encryption and SystemEDGE.

Based on these dependencies, the installation sequence is as follows:

1. SystemEDGE Core
2. Advanced Encryption
3. SRM AIM

The installer does not allow any other sequence. For example, when you try to install SRM without Advanced Encryption, it displays an error message and the installation does not start.

Note: See the CA Virtual Assurance Implementation Guide or SystemEDGE User Guide for details about installing SystemEDGE.

To install the SRM AIM on Windows using ca-setup.exe

1. Navigate to the DVD1\Installers\Windows\Agent\SysMan directory. Install the following components in this directory by considering the sequence:
    1. CA_SystemEDGE_Core
    2. CA_SystemEDGE_AdvancedEncryption
    3. CA_SystemEDGE_SRM
2. Change to the appropriate directory, and run the following command:

    ```
    ca-setup
    ```

    Follow the instructions on the screen and complete the installation.

To install the SRM AIM on Linux and UNIX using ca-setup.sh

1. Open a terminal console and change to the DVD2/Installers/*Platform*/Agent/SysMan directory. Install the following components in this directory by considering the sequence:
   1. CA_SystemEDGE_Core
   2. CA_SystemEDGE_AdvancedEncryption
   3. CA_SystemEDGE_SRM
2. Change to the appropriate directory and run the following command:

   ```
   sh ca-setup.sh
   ```

   Follow the instructions on the screen and complete the installation.

During the SRM installation, you can specify the following parameters:

Allow Runnings Scripts

Specifies if you want to allow running custom scripts. These scripts run with superuser privileges.

Default: No (typical installation)

Allow FileIO Tests

Allows running FileIO tests. Because the tests run with superuser privileges, they can access any file on the system when it is enabled.

Default: No (typical installation)

Allows untrusted SSL certificates

Allows HTTPS tests to access sites with invalid certificates (untrusted or when the website does not match the name in the certificate).

Default: No (typical installation)

Miscellaneous

Installs the SRM documentation component.

Default: Yes

Upgrade

All functionality enhancements are specified as *additional* functionality. Their parameters in the configuration file are either populated with default information or allowed to be NULL. The SRM AIM supports upgrade from SRM 2.0 and SRM 2.1 and accepts a version 2.x svcrsp.cf file as appropriate.

Uninstallation on Windows

You can uninstall the SRM AIM from the control panel or from the command line. It case of removing components that were originally installed through Remote Deployment, Idprimer and CAM are not uninstalled.

To uninstall the SRM AIM from the Windows Add or Remove Programs Window

1. Select Start, Settings, Control Panel, Add or Remove Programs.

   The Add or Remove Programs window appears and lists the following components:

   - CA SystemEDGE Core
   - CA SystemEDGE AdvancedEncryption
   - CA SystemEDGE SRM

2. Right-click CA SystemEDGE SRM and select Uninstall.

   A dialog charts the uninstallation process. When the uninstallation completes, the dialog closes.

To uninstall the SRM AIM from the command line

1. Open a command prompt and change to the DVD1\Installers\Windows\Agent\SysMan\CA_SystemEDGE_SRM directory.
2. Run the following command:

   ```
   ca-setup -x
   ```

   A dialog charts the uninstallation process. When the uninstallation completes, the dialog closes.

Uninstallation on Linux or UNIX

You uninstall the SRM AIM from the command line. In case of removing components that were originally installed through Remote Deployment, Idprimer and CAM are not uninstalled.

To uninstall the SRM AIM on UNIX using ca-setup.sh

1. Open a terminal console and log in as root (su).
2. Change to the DVD2/Installers/*<Platform>*/Agent/SysMan/CA_SystemEDGE_SRM directory and run the following command:

   ```
   sh ca-setup.sh -x
   ```

   A dialog charts the uninstallation process. When the uninstallation process completes, the dialog closes.

To uninstall the SRM AIM on UNIX using lsm

1. Open a terminal console and log in as root (su).
2. Run the following command:

   ```
   lsm -e CA_SystemEDGE_SRM
   ```

   Follow the progress of the uninstallation process until it completes.

Appendix C: Error Codes

This section contains the following topics:

Error Codes Overview

This page defines error codes that you may encounter while using SRM. The errors display in the Error Code column on the Test Monitor and Test Profile Monitor pages. Additional information about some of the tests displays in the Results Field column. (To display the Error Code and Results Field columns, click Show Column Config on the Test Monitor page, select Error Code and Results Field, and then click Update Page.)

Windows Systems

On Windows systems, SRM logs errors in the following locations:

- *Install_Path*\SystemEDGE\data\port161\sysedge.log – Agent-side messages
- *Install_Path*\SystemEDGE\data\port161\plugins\svcrsp\jcollector.log – Collector messages, including initialization of all test arguments and outcome of each test execution
- *Install_Path*\SystemEDGE\data\port161\plugins\svcrsp\sarunas.log – Virtual User run-as-user errors

Note: The drive and installation directory depend on the directory in which SRM is installed.

UNIX Systems

On UNIX systems, SRM logs errors in the following locations:

- System log (syslog) files for your platform – Agent-side errors
- *Install_Path/*SystemEDGE/data/port161/svcrsp/jcollector.log – Collector messages , including initialization of all test arguments and outcome of each test execution

jcollector.log file

All test-specific error codes are recorded in the jcollector.log file.

To set the debugging level in this file

1. Stop SystemEDGE.
2. Open the svcrsp.cf file for editing.
3. Uncomment (remove the pound sign (#) in front of) the #collector_debug line, and set the loglevel directive as follows:
   - Specify loglevel=0 for general use.
   - Specify loglevel=1 to view the start and end times for each pass of tests.
   - Specify loglevel=2 to view the start and end time for each individual test.
   - Specify loglevel=3 for debugging.

Note: Use the [#] to locate the portion of debug log that corresponds to the failing test.

CA-specific error codes generally take precedence over the standard numeric codes for the service because the CA-specific codes generally indicate an error in the program. For example, if the HTTP test starts downloading a page, returns a 404 error, and then encounters a file I/O error before the transaction is over, the Error Code field in the SRM table is set to 58 (I/O error during transaction), rather than 404.

Error Code Descriptions

SRM generates the following types of error codes:

- Generic
- Active Directory
- Custom
- DHCP
- DNS
- File I/O
- FTP
- HTTP/HTTPS
- IMAP
- LDAP
- MAPI
- NIS
- NNTP
- Ping
- POP3

- Reconfiguration and Initialization
- SMTP
- SNMP
- SQL Query
- TFTP
- Virtual User
- Results Field

Generic Error Codes

Generic Error Codes

These codes apply to all test types.

Error Code	Description
50	Incorrect or malformed test arguments. To modify the arguments, go to the Test Management page, select the test to modify, and click Modify. For more information, refer to the Help page for the type of test that you are running (such as the File I/O help page).
51	Unknown host. To modify the hostname, go to the Test Management page, select the test to modify, and click Modify. For more information, refer to the Help page for the type of test that you are running.
52	Invalid port. The port you selected may be in use or unavailable on the system you are testing. You can modify the port on the Modify Test page for your test. For more information, refer to the Help page for the type of test that you are running.
53	Error setting socket options (such as TOS). This error may result from invalid permissions for the registry on the target system. Check the system configuration settings.
54	The test timed out. You can set a different timeout value on the Modify Test page for your test. For more information, refer to the Help page for the type of test that you are running.
55	Error creating the socket. This error may result from system configuration problems. Check the system configuration settings on the target system.
56	Error while connecting the socket. This error may result from system configuration problems. Check the system configuration settings on the target system.

Error Code	Description
57	Error while closing the socket. This error may result from system configuration problems. Check the system configuration settings on the target system.
58	I/O error during transaction. This error may result from system configuration problems. Check the system configuration settings on the target system.
59	Error during WSAStartup (Windows only). WSAStartup allows an application to specify the version of the Windows Sockets API that is required and to retrieve details of the specific Windows Sockets implementation. Check the system configuration settings on the target system.
60	The socket was prematurely closed. This error indicates that the target system terminated the connection unexpectedly. Check the system configuration settings on the target system.
61	Bad sample, throwing out results.

A - H Error Codes

Active Directory and LDAP Test Error Codes

Error Code	Description
1	General error. For more information, refer to any of the following error logs: ■ %SystemRoot%\windows\system32\sysedge.log (Windows systems) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	The ldap.jar file may not be installed correctly. Check the target system to ensure that the file exists in the jre/lib/ext directory. If it does not, copy the file to that directory.
3	The domain may be incorrect. Verify that you specified the correct domain for the LDAP server you are testing. You can specify a different domain on the Modify Test page. For more information, refer to LDAP Tests.

Error Code	Description
4	Login failure. Verify that you specified a valid user name and password for the LDAP server you are testing. You can specify a different user name and password on the Modify Test page. For more information, refer to LDAP Tests.
5	The query produced no results. This error may result if you entered an invalid query or if the query does not match any content on the LDAP server. You can specify a different query on the Modify Test page. For more information, refer to LDAP Tests.

Custom Test Error Codes

Error Code	Description
1	Error executing the custom script. Verify that the script exists in the directory you specified on the Modify Test page. You can change the script name and destination on this page, if necessary. For more information, refer to Using Custom Scripts.
2	The custom script returned a bad exit code. This error may indicate that the script does not conform to the guidelines for writing a custom script. Update the script, if necessary.
3	The custom script printed malformed output. This error may indicate that the script does not conform to the guidelines for writing a custom script. Update the script, if necessary.
4	The custom script did not print any output. This error may indicate that the script does not conform to the guidelines for writing a custom script. Update the script, if necessary.
5	An error occurred while reading from the I/O stream. This error may result from system configuration problems. Check the system configuration settings on the target system.

DHCP Test Error Codes

Error Code	Description
1	General error. For more information, refer to any of the following error logs: ■ %SystemRoot%\windows\system32\sysedge.log (Windows systems) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	Cannot bind to a socket. Check the system configuration settings on the target system.
3	Socket timeout on receive. Check the system configuration settings on the target system.

DNS Test Error Codes

Error Code	Description
1	An error occurred while sending the query. Check the network settings and availability for the target system.
2	An error occurred while receiving the response. Check the network settings and availability for the target system.
3	The server indicated that the query was invalid.
4	The server indicated a server error. This error indicates that SRM was able to contact the target system, but that system is experiencing errors. Check the system configuration settings on the target system.
5	The server indicated that the host was not found. This error indicates that SRM was able to contact the target system, but that system is experiencing errors. Check the system configuration settings on the target system.

File I/O Test Error Codes

Error Code	Description
1	General error. For more information, refer to any of the following error logs: ■ *%SystemRoot%**windows**system32**sysedge.log* (Windows systems) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	Access to the local file is denied. This error indicates that the user name and password you are using may not have the correct permissions. You can specify a different user name and password on the Modify Test page. For more information, refer to File I/O Tests.
3	Access to the remote file is denied. This error indicates that the user name and password you are using may not have the correct permissions. You can specify a different user name and password on the Modify Test page. For more information, refer to File I/O Tests.
4	Local file is not found.
5	Remote file is not found.
6	The path argument points to the file in the local directory. The source file should be in a local directory, and the destination file should be on a remote file system. You can change the source and destination file names on the Modify Test page. For more information, refer to File I/O Tests.
7	Read of local file failed. The source file true if and only if the file specified by this abstract pathname exists and can be read by the application; false otherwise
8	Read of remote file failed.
9	Creation of remote file failed.
10	Write to remote file failed.
11	invalid or no output from external command.
12	Delete of remote file failed.
13	File Comparison failed.
14	Failed to execute file_io_helper.jar.
15	Failed to write a log msg.

FTP Test Error Codes

Error Code	Description
421	Service not available; closing control connection. (The service may respond to any command by closing a connection if it knows that it must shut down.) This error indicates that SRM was able to contact the target system, but that system is experiencing errors. Check the system configuration settings on the target system.
425	Cannot open data connection. This error indicates that SRM was able to contact the target system, but that system is experiencing errors. Check the system configuration settings on the target system.
426	Connection closed; transfer aborted. This error indicates that SRM was able to contact the target system, but that system is experiencing errors. Check the system configuration settings on the target system.
450	Requested file action not taken. File unavailable. This error may indicate that the file is in use or is not in the expected location. Verify that the file you are testing exists and is not in use.
451	Requested action aborted. Local error in processing. This error indicates that SRM was able to contact the target system, but that system is experiencing errors. Check the system configuration settings on the target system.
452	Requested action not taken. Insufficient storage space in system. This error indicates that you may need to add more disk space to the FTP server.
500	Syntax error. Command unrecognized. You may receive this error if the command line is too long or you are running non-standard FTP software.
501	Syntax error in parameters or arguments. You may receive this error if you are running a non-standard FTP software.
502	Command not implemented. You may receive this error if you are running a non- standard FTP software.
503	Bad sequence of commands. You may receive this error if you are running a non-standard FTP software.
504	Command not implemented for that parameter. You may receive this error if you are running a non-standard FTP software.
530	User not logged in. Verify that you are using a valid user name and password to perform FTP operations. You can specify a different user name and password on the Modify Test page. For more information, refer to FTP Tests.
532	Need account for storing files. Verify that the user account you are using for the test can store files on the FTP server.

Error Code	Description
550	Requested action not taken. File unavailable. You may receive this error if the file was not found, or if the service has no access to the file.
552	Requested file action aborted. Storage allocation exceeded. Verify that your FTP server has enough storage space for the action you are attempting to perform.
553	Requested action not taken. Illegal file name. Verify that the file you are using the correct file name for the FTP operation that you are attempting to perform.

HTTP/HTTPS Test Error Codes

Error Code	Description
1	The specified URL is invalid. You can specify a different URL on the Modify Test page. For more information, refer to HTTP Tests or HTTPS Tests.
2	The URL has an incorrect protocol: it uses http:// instead of https://. You can specify a different URL on the Modify Test page. For more information, refer to HTTPS Tests.
3	An error occurred while sending the request. This error may indicate that you are using a non-standard HTTP server that SRM does not support.
4	An error occurred while reading the HTTP status code. This error may indicate that you are using a non-standard HTTP server that SRM does not support.
5	An error occurred while retrieving the HTTP headers. This error may indicate that you are using a non-standard HTTP server that SRM does not support.
6	An error occurred while retrieving the HTTP content. This error may indicate that you are using a non-standard HTTP server that SRM does not support.
7	An error occurred while parsing the document. This error may indicate that you are using a non-standard HTTP server that SRM does not support.
8	An invalid maximum depth was specified. You can specify a different depth on the Modify Test page. For more information, refer to HTTP Tests or HTTPS Tests.
20	The host was not found when following a link. This error indicates a problem on the site you are testing.

Error Code	Description
21	The protocol was invalid when following a link. This error indicates a problem on the Web page you are testing.
400	Bad request. This error indicates a problem on the HTTP page you are testing.
401	Unauthorized. This error indicates a problem on the site you are testing.
402	Payment required. This error indicates a problem on the site you are testing.
403	Forbidden. This error indicates a problem on the site you are testing.
404	Not found. This error indicates that the Web page or content you were requesting does not exist in the location that you are looking for it. This error may result from a problem with the Web page you are testing or from an incorrect URL. You can specify a different URL on the Modify Test page. For more information, refer to HTTP Tests or HTTPS Tests.
405	Method not allowed. This error indicates a problem on the site you are testing.
406	Not acceptable. This error indicates a problem on the site you are testing.
407	Proxy authentication required. This error may indicate that the proxy user name or password that you supplied is not correct. Verify that you are using a valid account. You can specify a different user name and password for the proxy server on the Modify Test page. For more information, refer to HTTP Tests or HTTPS Tests.
408	Request timed out. This error indicates a problem on the site you are testing.
409	Conflict. This error indicates a problem on the site you are testing.
410	Gone. This error indicates a problem on the site you are testing.
411	Length required. This error indicates a problem on the site you are testing.
412	Precondition failed. This error indicates a problem on the site you are testing.
413	Request entity too large. This error indicates a problem on the site you are testing.
414	Request URL too large. This error indicates a problem on the site you are testing.
415	Unsupported media type. This error indicates a problem on the site you are testing.
500	Server error. This error indicates a problem on the site you are testing.

Error Code	Description
501	Not implemented. This error indicates a problem on the site you are testing.
502	Bad gateway. This error indicates a problem on the site you are testing.
503	Out of resources. This error indicates a problem on the site you are testing.
504	Gateway timeout. This error indicates a problem on the site you are testing.
505	HTTP version not supported. This error indicates a problem on the site you are testing.

I - R Error Codes

IMAP Test Error Codes

Error Code	Description
10	General error. For more information, refer to any of the following error logs: ■ %SystemRoot%\windows\system32\sysedge.log (Windows systems) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
11	Cannot bind to a socket. This error indicates that the socket on the mail server you are testing is unavailable.
12	Socket timeout on receive. This error indicates that the socket on the mail server you are testing is unavailable.
13	Login failed. This error may indicate a problem with the IMAP mail server, or it may indicate that the user name and password you have configured are incorrect. You can specify a different user name and password on the Modify Test page. For more information, refer to IMAP Tests.
14	Selecting the inbox failed. This error may indicate a problem with the IMAP mail server, or it may indicate that the user name and password you have configured for the account you are testing are incorrect. You can specify a different user name and password on the Modify Test page. For more information, refer to IMAP Tests.

Error Code	Description
15	The inbox is empty. This error indicates that you have not sent mail to your test account, so the test cannot download any emails. Reconfigure your test email account so that it contains email. If you selected Delete All Messages when you configured the test, you must ensure that you are sending more email to the account before the next time you run the test.
16	Reading from the inbox failed. This error may indicate a problem with the IMAP mail server.
17	Message flag change failed. This error indicates that the email did not appear as read or deleted, depending on the operation you were performing. Check the configuration of your IMAP mail server.
18	Message removal failed. This error indicated that the test was not able to delete messages, even though you selected Delete Downloaded Messages on the Modify Test page. Check the configuration of your IMAP mail server.
19	Cannot find message by subject. This error indicates either that the mail server cannot perform filtering or that a message with the subject on which you are searching does not exist. Check your IMAP mail server and the user account.
20	Cannot connect to the server.

MAPI Test Error Codes

Error Code	Description
50	Bad arguments; Internal jcollector error.
200	Bad hostname. DNS lookup failed. This error may indicate that you provided an incorrect MAPI server name when you created the test. You can modify the name on the Modify Test page. For more information, refer to MAPI Tests.
210	MAPI login failed. This error may indicate that you provided an incorrect user name or password when you created the test. You can modify the name on the Modify Test page. For more information, refer to MAPI Tests.
211	MAPI logoff failed. This error may indicate a MAPI server problem.
220	Failed to initialize MAPI. This error may indicate a problem with your MAPI server. Check your server configuration.
221	Failed to open user's Message Store. This error may indicate a problem with your MAPI server. Check your server configuration.

Error Code	Description
222	Failed to open user's Content table. This error may indicate a problem with your MAPI server. Check your server configuration.
223	Failed to open Global Message Store table. This error may indicate a problem with your MAPI server. Check your server configuration.
224	Failed to set search columns. This error may indicate a problem with your MAPI server. Check your server configuration.
225	Query table columns failed. This error may indicate a problem with your MAPI server. Check your server configuration.
226	Unable to get row count. This error may indicate a problem with your MAPI server. Check your server configuration.
227	Unable to find default received folder. This error may indicate a problem with your MAPI server. Check your server configuration.
228	Unable to open folder. This error may indicate a problem with your MAPI server. Check your server configuration.
229	Memory allocation (malloc) failed. Check your server configuration.
230	Message store is NULL. This error may indicate a problem with your MAPI server. Check your server configuration.
231	Unable to reset row position. Check your server configuration.
240	User's mailbox not found. This error may indicate that you provided an incorrect user name or password on the Modify Test page. For more information, refer to MAPI Tests.
241	User has no mail to read. This error may indicate that you did not create mail for the account that is being tested or that you did not send new mail after the test deleted all messages in the account. Verify that you are sending mail to the account that the test can download. For more information, refer to MAPI Tests.
242	Message not found. SRM does not search for specific messages. This error may indicate a problem with your MAPI server. Check your server configuration.
243	Test timed out. You can set a different timeout value on the Modify Test page. For more information, refer to MAPI Tests.
250	Unable to delete mail. This error may indicate a problem with the MAPI server or with the user account permissions. Check your MAPI server settings and user account administration.
260	MAPI profile exists. This error may indicate a problem with your MAPI server. Check your server configuration.

Error Code	Description
261	Unable to create dynamic profile. This error may indicate a problem with your MAPI server. Check your server configuration.
262	Unable to delete dynamic profile. This error may indicate a problem with your MAPI server. Check your server configuration.

NIS Test Error Codes

Error Code	Description
1	General error. For more information, refer to any of the following error logs: ■ %SystemRoot%\windows\system32\sysedge.log (Windows systems) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	The nis.jar file may not be installed in jre/lib/ext. Check the jre/lib/ext directory. If the nis.jar file is not there, copy it to that directory.
3	The domain may not be correct. You can specify a different domain name on the Modify Test page. For more information, refer to NIS Tests.
4	Cannot find the host. This error can indicate that the NIS server you are querying is unavailable, or that the test is using an incorrect server name. You can modify the NIS server name on the Modify Test page. For more information, refer to NIS Tests.
5	The map file name may be incorrect. You can specify a different map file on the Modify Test page. For more information, refer to NIS Tests.

NNTP Test Error Codes

Error Code	Description
400	Service discontinued. This error indicates that the NNTP service was discontinued on this server. Check the server configuration settings.
411	No such news group. SRM does not query specific news groups, so this error indicates a problem that is unrelated to SRM.
412	No newsgroup has been selected. SRM does not query specific news groups, so this error indicates a problem that is unrelated to SRM.

Error Code	Description
420	No current article has been selected. SRM does not query specific news groups, so this error indicates a problem that is unrelated to SRM.
421	No next article in this group. SRM does not query specific news groups, so this error indicates a problem that is unrelated to SRM.
422	No previous article in this group. SRM does not query specific news groups, so this error indicates a problem that is unrelated to SRM.
423	No such article number in this group. SRM does not query specific news groups, so this error indicates a problem that is unrelated to SRM.
430	No such article found. SRM does not query specific news groups, so this error indicates a problem that is unrelated to SRM.
435	Article not wanted; do not send it. SRM does not query specific news groups, so this error indicates a problem that is unrelated to SRM.
436	Transfer failed; try again later. SRM does not transfer data for the NNTP test, so this error indicates a problem that is unrelated to SRM.
437	Article rejected; do not try again. SRM does not query specific news groups, so this error indicates a problem that is unrelated to SRM.
440	Posting not allowed. SRM does not post information for the NNTP test, so this error indicates a problem that is unrelated to SRM.
441	Posting failed. SRM does not post information for the NNTP test, so this error indicates a problem that is unrelated to SRM.
500	Command not recognized. This error may indicate that you are using a non-standard NNTP server that SRM does not support.
501	Command syntax error. This error may indicate that you are using a non-standard NNTP server that SRM does not support.
502	Access restriction, or permission denied. This error may indicate that the NNTP service is not running on the port you specified on the Modify Test page. For more information, refer to NNTP Tests. The error may also indicate that your NNTP server requires a login, which the SRM test does not perform. Check the system settings on your NNTP server.
503	Program fault; command not performed. This error may indicate that you are using a non-standard NNTP server that SRM does not support.

Ping Test Error Codes

Error Code	Description
1	Negative payload. This error indicates that the payload you specified for the ping test is an invalid (negative) number. You can modify this value on the Modify Test page. For more information, refer to Ping Tests.

POP3 Test Error Codes

Error Code	Description
0	The POP3 server returned +OK. This message indicates the query worked. It is informational only.
1	The POP3 server returned -ERR. This error indicates that the query did not work. For more information, refer to any of the following error logs: ■ %SystemRoot%\windows\system32\sysedge.log (Windows systems) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	The POP3 server returned an invalid response. This error indicates that SRM could not recognize the response that the server returned (whether the test succeeded or failed). For more information, refer to any of the following error logs: ■ %SystemRoot%\windows\system32\sysedge.log (Windows systems) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)

Reconfiguration and Initialization Error Codes

Error Code	Description
101	A structural error in the configuration file detected.
102	Value of plugin is not equal to svcrsp.
103	The passed configuration file could not be opened for reading.
104	Value of path is empty.

Error Code	Description
105	Decryption of the configuration file failed.
106	Unspecified error during file processing.
107	Unsupported parameter found.
108	Unexpected value of the mode parameter.
109	The given configuration file does not exist.
110	Launching Jcollector failed.
111	The given Java executable is missing.
112	Value of the parameter is too long. It will be cut during processing.
113	There is no version indication in the configuration file.
114	Unsupported version of the configuration file.
201	Duplicate monitor index found (in the test definition block) .
202	Duplicate monitor template definition name found (in the monitor template definition block).
203 (1)	Invalid value of the parameter monAttribute. Not all attributes are allowed to be monitored.
205 (2)	Invalid value of the parameter monOperator.
206 (3)	Invalid value of the parameter monSeverity.
208	Monitor template name (monName) is missing.
209	Monitor template threshold (monThreshold) is missing.
210	Monitor template operator (monOperator) is missing.
211	Monitor template attribute (monAttribute) is missing.
301	Duplicate test index found.
302	Test interval is lower than the pre-defined minimum. Test interval will be adjusted to the pre-defined minimum.
303	Non-existent monitor template referred from a test.
304	Invalid value of another parameter within test definition.
305	Not allowed value of the parameter “samples”; must be an integer.
306	Not allowed value of the parameter “status”.
307	Not allowed value of the parameter “timeout”; must be an integer, smaller or equal to the value of “interval”.
308	Not allowed value of the parameter “window”; must be an integer.

Error Code	Description
309	Destination attribute missing.
310	Test name missing.
311	Test type missing.
312	Test index missing.
313	Invalid reserved range of test indices.
314	Invalid test index.

(1) A valid value is one of the following:

- svcRspTableNumSamples (11)
- svcRspTableTotalLastSample (12)
- svcRspTableTotalMin (13)
- svcRspTableTotalMax (14)
- svcRspTableTotalMean (15)
- svcRspTableTotalVariance (16)
- svcRspTableTotalAvailability (17)
- svcRspTableNameLastSample (18)
- svcRspTableNameMin (19)
- svcRspTableNameMax (20)
- svcRspTableNameMean (21)
- svcRspTableNameVariance (22)
- svcRspTableConnLastSample (23)
- svcRspTableConnMin (24)
- svcRspTableConnMax (25)
- svcRspTableConnMean (26)
- svcRspTableConnVariance (27)
- svcRspTableTranLastSample (28)
- svcRspTableTranMin (29)
- svcRspTableTranMax (30)
- svcRspTableTranMean (31)
- svcRspTableTranVariance (32)
- svcRspTableBytesInLastSample (33)
- svcRspTableBytesOutLastSample (34)
- svcRspTableTotalBytesIn (35)
- svcRspTableTotalBytesOut (36)
- svcRspTableThroughput (37)

(2) A valid value is one of the following:

- NOP – nop, no operation (1)
- GT – gt, greater than (2)
- LT – lt, less than (3)
- GE – ge, greater or equal to (4)
- LE – le, less or equal to (5)
- EQ – eq, equal (6)
- NE – ne, not equal (7)

(3) A valid value is one of the following:

- NONE – no severity (default), no monitor will be created (1)
- WARNING – Creates a monitor with a severity of warning (3)
- MINOR – Creates a monitor with a severity of minor (4)
- MAJOR – Creates a monitor with a severity of major (5)
- CRITICAL – Creates a monitor with a severity of critical (6)
- FATAL – Creates a monitor with a severity of fatal (7)

S - Z Error Codes

SMTP Test Error Codes

Error Code	Description
3	The SMTP server returned an invalid response. This error indicates that SRM could not recognize the response that the server returned. For more information, refer to any of the following error logs: ■ %SystemRoot%\windows\system32\sysedge.log (Windows systems) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
421	The domain service is not available. Closing the transmission channel. This error indicates that your SMTP server is not running.
432	A password transition is needed. This error indicates a problem with your SMTP server. Check the configuration settings. (SRM does not provide a password or user account for testing the SMTP service.)

Error Code	Description
450	Requested mail action not taken: mailbox unavailable; ATRN request refused. This error indicates that you specified an invalid mail recipient on the Modify Test page. For more information, refer to SMTP Tests.
451	Requested action aborted: local error in processing; Unable to process ATRN request now. This error indicates a problem with your SMTP server. Check the server configuration settings.
452	Requested action not taken: insufficient system storage. This error indicates that your SMTP server does not include enough disk space to store the messages the test is sending. Check the available space and, if necessary, add more, or configure your tests to use a different server.
453	You have no mail. This is an informational message. SRM does not check the mail in an SMTP account.
454	TLS not available temporarily; Encryption is required for the requested authentication mechanism. This error indicates a problem with your SMTP server configuration. SRM does not use authentication for the SMTP test.
458	Unable to queue messages for node. This error indicates a problem with your SMTP server configuration.
459	Node node not allowed: reason. This error indicates a problem with your SMTP server configuration.
500	Command not recognized: command; Syntax error. This error indicates that you are using a non-standard SMTP server that cannot recognize the SRM commands.
501	Syntax error. No parameters allowed. This error indicates that you are using a non-standard SMTP server that cannot recognize the SRM commands.
502	Command not implemented. This error indicates that you are using a non-standard SMTP server that cannot recognize the SRM commands.
503	Bad sequence of commands. This error indicates that you are using a non-standard SMTP server that cannot recognize the SRM commands.
504	Command parameter not implemented. This error indicates that you are using a non-standard SMTP server that cannot recognize the SRM commands.
521	Machine does not accept mail. This error indicates that you specified an invalid mail recipient on the Modify Test page. For more information, refer to SMTP Tests.

Error Code	Description
530	Must issue a STARTTLS command first; Encryption is required for the requested authentication mechanism. This error indicates a problem with your SMTP server configuration. SRM does not use authentication for the SMTP test.
534	The authentication mechanism is too weak. This error indicates a problem with your SMTP server configuration. SRM does not use authentication for the SMTP test.
538	Encryption is required for the requested authentication mechanism. This error indicates a problem with your SMTP server configuration. SRM does not use authentication for the SMTP test.
550	Requested action not taken: mailbox unavailable. This error may indicate that you specified an invalid mail recipient on the Modify Test page. For more information, refer to SMTP Tests.
551	User not local; please try forwardpath. This error may indicate that you specified an invalid mail recipient on the Modify Test page. For more information, refer to SMTP Tests.
552	Requested mail action aborted: exceeded storage allocation. This error may indicate that you need to delete mail from the account of the mail recipient you specified on the Modify Test page. For more information, refer to SMTP Tests.
553	Requested action not taken: mailbox name not allowed. This error indicates that you specified an invalid mail recipient on the Modify Test page. For more information, refer to SMTP Tests.
554	Transaction failed. This error indicates that you specified an invalid mail recipient on the Modify Test page, or that the SMTP server is experiencing difficulties. For more information, refer to SMTP Tests and check your SMTP server configuration.

SNMP Test Error Codes

Error Code	Description
1	Too big.
2	No such name. This error indicates that you specified an incorrect OID on the Modify Test page. For more information, refer to SNMP Tests.
3	Bad value. This error indicates that the object you are querying returned an invalid value. This indicates a problem with the object you are querying.

Error Code	Description
4	Read only. This error indicates that the object you are querying is read-only. This message is informational only. SRM does not attempt to set values for MIB objects.
5	General error. For more information, refer to any of the following error logs: ■ %SystemRoot%\windows\system32\sysedge.log (Windows) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
6	General error. For more information, refer to any of the following error logs: ■ %SystemRoot%\windows\system32\sysedge.log (Windows) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory/*plugins/svcrsp/jcollector.log (UNIX)
7	Cannot bind to a socket. This error may result from invalid permissions for the registry on the target system. Check the system configuration settings.
8	Socket timeout on receive. This error may result from invalid permissions for the registry on the target system. Check the system configuration settings.
9	Cannot create outgoing packet. This error indicates a problem with SRM. For more information, refer to the system log files: %SystemRoot%\windows\system32\sysedge.log (Windows) or syslog files (UNIX).
10	Cannot decode incoming packet. This error indicates a problem with SRM. For more information, refer to the system log files: %SystemRoot%\windows\system32\sysedge.log (Windows) or syslog files (UNIX).

SQL Query Test Error Codes

Error Code	Description
1	General error. For more information, refer to any of the following error logs: ■ %SystemRoot%*windows**system32**sysedge.log* (Windows) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	The JDBC driver may not be installed in jre/lib/ext. Verify that the JDBC driver for your database exists in the jre/lib/ext directory. If not, copy it there.
3	Java SLQ exception occurred. For more information, refer to the jcollector.log file, which is located in the *SystemEDGE-install-directory*\sysedge\plugins\svcrsp (Windows) or *SystemEDGE-install-directory/*plugins/svcrsp directory (UNIX)

TFTP Test Error Codes

Error Code	Description
1	General error. For more information, refer to any of the following error logs: ■ %SystemRoot%\windows\system32\sysedge.log (Windows) or syslog files (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) or *SystemEDGE-install-directory/*plugins/svcrsp/jcollector.log (UNIX)
2	Socket timeout on receive. This error may result from invalid permissions for the registry on the target system. Check the system configuration settings.
3	Operation on TFTP client failed. This error could indicate that you specified an incorrect path to the file you want to read or write on the Modify Test page, or that the configuration on the TFTP server is incorrect. For more information, refer to TFTP Tests, or check your system configuration settings on the TFTP server.

Virtual User Test Error Codes

Error Code	Description
300	Unable to get process token. This error indicates that SRM cannot communicate with the system where the test should run. The problem may be with Service Availability attempt to log in as another user. For more information, refer to any of the following error logs: ■ %SystemRoot%\windows\system32\sysedge.log ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\sarunas.log ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log
301	Unable to adjust token privileges. This error indicates that SRM cannot communicate with the system where the test should run. For more information, refer to any of the following error logs: ■ %SystemRoot%\windows\system32\sysedge.log ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\sarunas.log ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log
302	Unable to log in user. This error indicates that sarunas.exe file is not installed in the *drive*:sysedge\plugins\svcrsp\sarunas.log directory, or that you specified an incorrect user name or password on the Modify Test page. For more information, refer to Virtual User Tests and the *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\sarunas.log file.
303	Unable to give user desktop access. This error indicates that you did not enable SNMP to interact with the desktop. For more information, refer to Enabling the SNMP Service to Interact with the Desktop.
304	Process creation failed. For more information, refer to any of the following error logs: ■ %SystemRoot*%**windows**system32**sysedge.log* ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\sarunas.log ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log

Results Field

The Results Field displays different types of data, depending on the type of test you are running and the information in the Error Codes column. The following table describes the tests that use the Results Field and the type of information that displays in the column for each of those tests.

Test Type	Information that Displays in Results Field Column
Custom	The fourth argument that is returned from the custom test script. (The first three arguments are the DNS resolution time, connection time, and transaction time.)
HTTP and HTTPS	If the test specifies a value for Search Expression, this field provides the number of times that the test matched the search expression on the target page.
Virtual User	If the value of the Error Codes field is 2, this field indicates the exit code that the taskexec.exe application returned.

Index

R

S

T

U

V