HOW TO MONITOR WINDOWS SERVICES USING THE QA SNMP MONITOR

When configuring ipMonitor to monitor Windows Services, there may be instances when the Service Monitor cannot be used. For example, if:

- RPC connectivity is not allowed.
- RPC connectivity is not working properly.
- A Credential to represent the administrative account cannot be used.

On such occasions, you can use the QA SNMP Monitor to monitor Windows services. There are a number of advantages to this setup:

- The QA SNMP Monitor is relatively easy to configure.
- This setup will work on a stand-alone system as well as across non-trusted domains, provided SNMP connectivity exists between both systems.
- This setup results in a non-intrusive, low network overhead monitoring process.

Before you begin

Step 1:

Before creating a QA SNMP Monitor to implement the example outlined in this tutorial, ensure that the Windows SNMP service has been configured and enabled on the remote systems.

If the SNMP Service has not been installed:

1. Click **Start**, **Control Panel**, **Add or Remove Programs**, and then **Add/Remove Windows Components.**
2. In **Components**, click **Management and Monitoring Tools** and then click **Details**.
3. Select the **Simple Network Management Protocol** check box, and then click **OK**.
4. Click **Next.**

Step 2:

You must also download and install the ipMonitor SNMP Assistant. More information on the SNMP Assistant can be found in the SNMP Center section of the ipMonitor Support Portal.

Top

AVAILABLE RESOURCES

Click the XML icon to download resources designed to be used with this tutorial. The XML file includes one preconfigured Monitor.

Top

© 2005 ipMonitor Corporation. All rights reserved.

SAMPLE MONITOR SETTINGS

Monitor Name	**QA-SNMP:: server name:: Server service**
Monitor Type	QA SNMP Monitor
SNMP Object Type	svSvcName
OID	1.3.6.1.4.1.77.1.2.3.1.1.6.83.101.114.118.101.114
Returns	The name of the network service.
Monitoring Condition	**Pass if the returned result includes the word 'server'** Monitor failure indicates that the service is not running.

Note: The imported Monitor is initially disabled. This allows you to make changes to the default settings before the Monitors are enabled to go live in a production environment. Once the Monitors are imported, the following settings will need to be verified (and if necessary, modified) for each Monitor:

- IP Address / Domain Name
- UDP Port
- Community

To learn more about modifying the above parameters, please refer to the 'Configuring the QA SNMP Monitor' section of this tutorial.

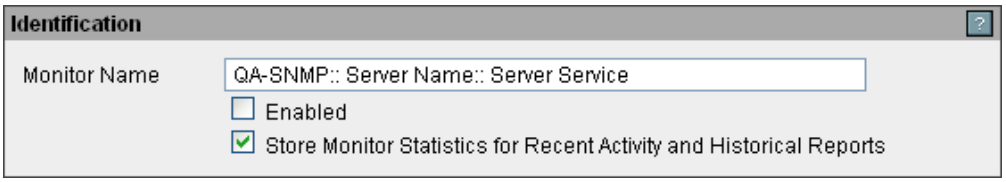
> **TIP**
>
> For detailed instructions regarding importing XML files into your ipMonitor installation, please refer to the tutorial entitled "How to Import and Export Configuration Settings".

Top

CONFIGURING THE QA SNMP MONITOR

For the purposes of this tutorial, we'll be referring to the preconfigured Monitor included in the XML resource download. Alternatively, you can create a new Monitor by clicking the **Monitors** menu option and then selecting **Add a Monitor**. Choose the **SNMP - QA** Monitor from the list provided.

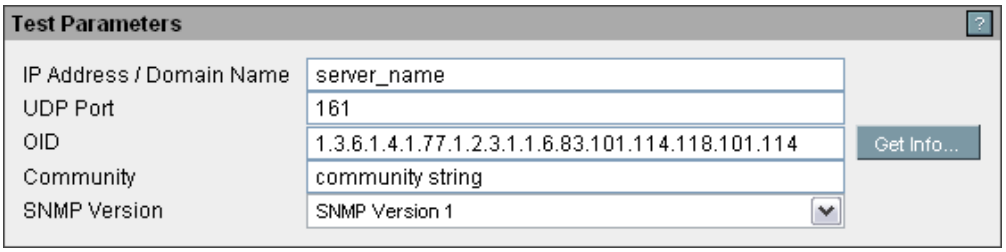
Identification



1. Enter a unique, descriptive name for the Monitor in the **Name** field.
2. Check the **Enabled** checkbox.
3. Choose whether you want the Monitor to **Store Statistics for Recent Activity and Historical Reports**.

© 2005 ipMonitor Corporation. All rights reserved.

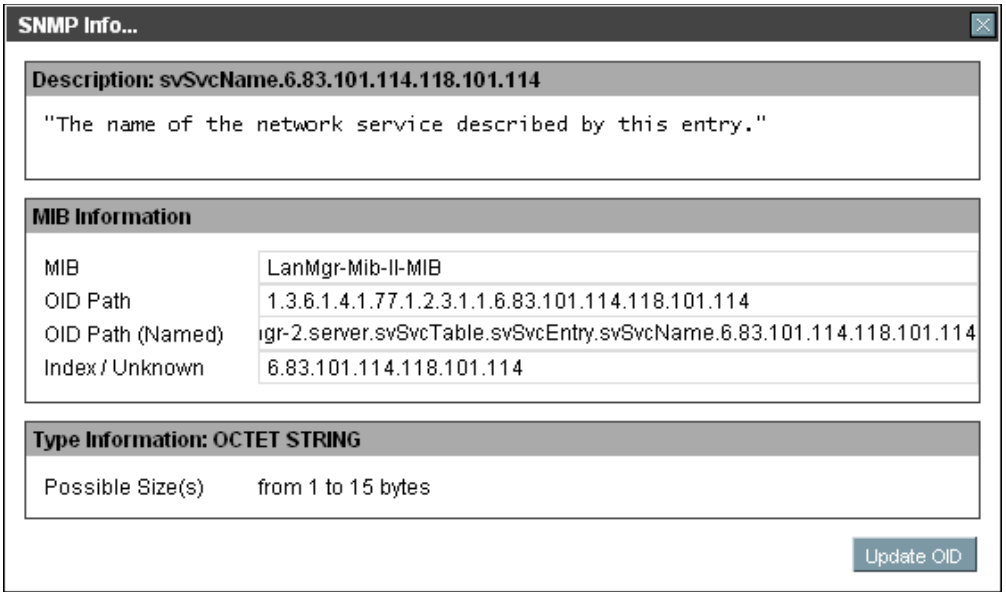
Test Parameters



4. Specify the **location** of the Server service
5. If needed, specify a different **UDP Port** number for the SNMP Service. By default, the standard Port number used for SNMP communication (Port 161) is already entered.
6. If you are using the preconfigured Monitor, the appropriate OID for the monitoring task is already entered. Otherwise, you will need to specify an OID path in the **OID** field. For assistance with this step, please refer to the section of this tutorial titled 'Choosing an Appropriate OID for the Monitoring Task'.
7. Enter the SNMP **Community** string that allows ipMonitor to communicate with the SNMP Service.

Analysis of Test Results

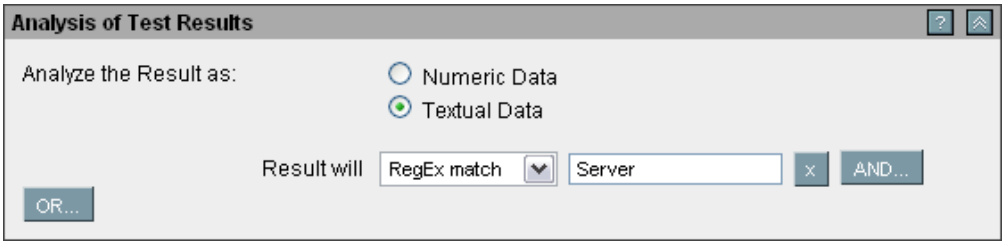
The following example uses the **Analysis of Test Results** settings configured for the Monitor provided in the XML resource download.



© 2005 ipMonitor Corporation. All rights reserved.

Analysis of Test Results

The type of data supported by the selected OID determines the possible methods of analysis using the QA SNMP Monitor.



1. In order to return the desired value (the name of the network service), the QA SNMP Monitor is configured to analyze the result as **Textual Data**.
2. The expected **result is determined to be a RegEx match for the word 'Server'**, ensuring that the Monitor will pass if the RegEx match is returned.

> **TIP**
>
> By default, the Timing intervals for each parameter are set to 300 seconds. If needed, adjust these defaults to meet your specific monitoring environment's requirements until the optimum settings are reached.

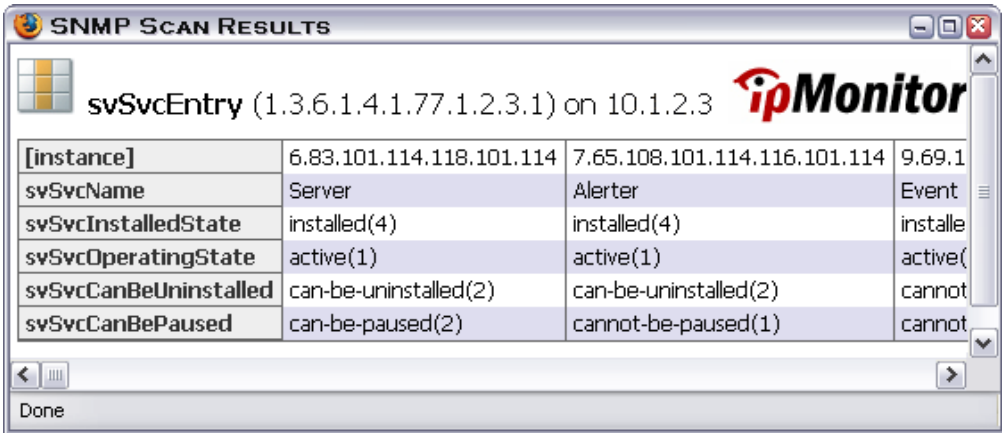
Top

CHOOSING AN APPROPRIATE OID FOR THE MONITORING TASK

When the SNMP Service is enabled on the system, the "lanmanager" SNMP branch is made available. This branch provides access to the Services running on the system. The OID that refers to the Services table is:

1.3.6.1.4.1.77.1.2.3.1.1

You will need to locate the suffix OID that must be used with the Service that requires monitoring. In order to do so, you can use the SNMP Assistant tool. Once the SNMP Assistant is installed on the ipMonitor 7 host, you can use it to run an "SNMP walk" command against the remote system that you want to monitor. The SNMP Assistant will walk the Service name table and list the OIDs for the Services in a browser window.



Simply copy the suffix OID and append it to the initial branch OID.

© 2005 ipMonitor Corporation. All rights reserved.

Example

As shown in the above instructions for configuring a QA SNMP Monitor, the Server Service has the following OID:

.6.83.101.114.118.101.114

Thus, the complete OID is:

1.3.6.1.4.1.77.1.2.3.1.6.83.101.114.118.101.114

The table below contains suffix OIDs for common Services.

Service Name	Suffix OID
Server	.6.83.101.114.118.101.114
Net Logon	.9.78.101.116.32.76.111.103.111.110
DNS Client	.10.68.78.83.32.67.108.105.101.110.116
DHCP Client	.11.68.72.67.80.32.67.108.105.101.110.116
Workstation	.11.87.111.114.107.115.116.97.116.105.111.110
Automatic Updates	.17.65.117.116.111.109.97.116.105.99.32.85.112.100.97.116.101.115
IIS Admin Service	.17.73.73.83.32.65.100.109.105.110.32.83.101.114.118.105.99.101
Terminal Services	.17.84.101.114.109.105.110.97.108.32.83.101.114.118.105.99.101.115
FTP Publishing Service	.22.70.84.80.32.80.117.98.108.105.115.104.105.110.103.32.83.101.114.118.105.99.101
Remote Procedure Call (RPC)	.27.82.101.109.111.116.101.32.80.114.111.99.101.100.117.114.101.32.67.97.108.108.32.40.82.80.67.41
World Wide Web Publishing Service	.33.87.111.114.108.100.32.87.105.100.101.32.87.101.98.32.80.117.98.108.105.115.104.105.110.103.32.83.101.114.118.105.99.101
Windows Management Instrumentation	.34.87.105.110.100.111.119.115.32.77.97.110.97.103.101.109.101.110.116.32.73.110.115.116.114.117.109.101.110.116.97.116.105.111.110
Windows Firewall/Internet Connection Sharing (ICS)	.50.87.105.110.100.111.119.115.32.70.105.114.101.119.97.108.108.47.73.110.116.101.114.110.101.116.32.67.111.110.110.101.99.116.105.111.110.32.83.104.97.114.105.110.103.32.40.73.67.83.41

Top

ADDITIONAL INFORMATION

For more information regarding the QA SNMP Monitor, refer to the **Monitors** section of ipMonitor's Context-Sensitive Help system, and then select **Monitor Types**, followed by **QA SNMP**. The Context-Sensitive Help can be accessed by clicking the **Help** link located in the top right corner of ipMonitor's Administration web interface.

© 2005 ipMonitor Corporation. All rights reserved.