HOW TO: Configure the Simple Network Management Protocol (SNMP) Service in Windows Server 2003

Article ID: 324263 - View products that this article applies to.

This article was previously published under Q324263

SUMMARY

This step-by-step article describes how to configure the Simple Network Management Protocol (SNMP) Service in Windows Server 2003. This article describes how to configure SNMP agent properties, SNMP traps, and SNMP security.

The SNMP Service, when configured for an agent, generates trap messages that are sent to a trap destination, if any specific events occur. For example, you can configure the SNMP service to send a trap when it receives a request for information that does not contain the correct community name and does not match an accepted host name for the service.

How to Configure SNMP Agent Information

To configure SNMP agent information:

1. Click **Start**, point to **Control Panel**, point to **Administrative Tools**, and then click **Computer Management**.
2. In the console tree, expand **Services and Applications**, and then click **Services**.
3. In the right pane, double-click **SNMP Service**.
4. Click the **Agent** tab.
5. Type the name of the user or administrator of the computer in the **Contact** box, and then type the physical location of the computer or contact in the **Location** box.

   These comments are treated as text and are optional.
6. Under **Service**, click to select the check boxes next to the services that are provided by your computer. Service options are:

   - **Physical**: Specifies whether the computer manages physical devices, such as a hard disk partition.
   - **Applications**: Specifies whether the computer uses any programs that send data by using TCP/IP.
   - **Datalink and subnetwork**: Specifies whether this computer manages a TCP/IP subnetwork or datalink, such as a bridge.
   - **Internet**: Specifies whether this computer acts as an IP gateway (router).
   - **End-to-end**: Specifies whether this computer acts as an IP host.

7. Click **OK**.

NOTE: If you have installed additional TCP/IP network devices, such as a switch or a router, see Request for Comments (RFC) 1213 for additional information. To view RFC 1213, visit the following Internet Engineering Task Force (IETF) Web site:

http://www.ietf.org/rfc/rfc1213.txt (http://www.ietf.org/rfc/rfc1213.txt)

Microsoft provides third-party contact information to help you find technical support. This contact information may change without notice. Microsoft does not guarantee the accuracy of this third-party contact information.

How to Configure SNMP Communities and Traps

To configure traps:

1. Click **Start**, point to **Control Panel**, point to **Administrative Tools**, and then click **Computer Management**.
2. In the console tree, expand **Services and Applications**, and then click **Services**.
3. In the right pane, double-click **SNMP Service**.
4. Click the **Traps** tab.
5. In the **Community name** box, type the case-sensitive community name to which this computer will send trap messages, and then click **Add to list**.
6. Under **Trap destinations**, click **Add**.
7. In the **Host name, IP or IPX address** box, type the name, IP or IPX address of the host, and then click **Add**.

   The host name or address appears in the **Trap destinations** list.
8. Repeat steps 5 through 7 to add the communities and trap destinations that you want.
9. Click **OK**.

How to Configure SNMP Security

To configure SNMP security for a community:

1. Click **Start**, point to **Control Panel**, point to **Administrative Tools**, and then click **Computer Management**.
2. In the console tree, expand **Services and Applications**, and then click **Services**.
3. In the right pane, double-click **SNMP Service**.
4. Click the **Security** tab.
5. Click to select the **Send authentication trap** check box (if it is not already selected) if you want a trap message sent whenever authentication fails.
6. Under **Accepted community names**, click **Add**.
7. To specify how the host processes SNMP requests from the selected community, click the permission level that you want in the **Community Rights** box.
8. In the **Community Name** box, type the case-sensitive community name that you want, and then click **Add**.
9. Specify whether or not to accept SNMP packets from a host. To do so, do one of the following:

9. Specify whether or not to accept SNMP packets from a host. To do so, do one of the following:
    - To accept SNMP requests from any host on the network, regardless of identity, click **Accept SNMP packets from any host**.
    - To limit the acceptance of SNMP packets, click **Accept SNMP packets from these hosts**, click **Add**, and then type the appropriate host name, IP or IPX address in the **Host name, IP or IPX address** box.
10. Click **Add**.
11. Click **OK**.

IMPORTANT: If you remove all of the community names, including the default name "Public", SNMP does not respond to any community names that are presented.

REFERENCES

For additional information about how to configure network security for the SNMP service, click the following article number to view the article in the Microsoft Knowledge Base:

324261 (http://support.microsoft.com/kb/324261/EN-US/) Configure Network Security for the SNMP Service in Windows Server 2003

Properties

Article ID: 324263 - Last Review: October 30, 2006 - Revision: 4.3

APPLIES TO

- Microsoft Windows Server 2003, Standard Edition (32-bit x86)
- Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
- Microsoft Windows Server 2003, Enterprise x64 Edition
- Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
- Microsoft Windows Server 2003, 64-Bit Datacenter Edition
- Microsoft Windows Server 2003, Web Edition

Keywords: kbnetwork kbenv kbhowto kbhowtomaster kbnetwork KB324263