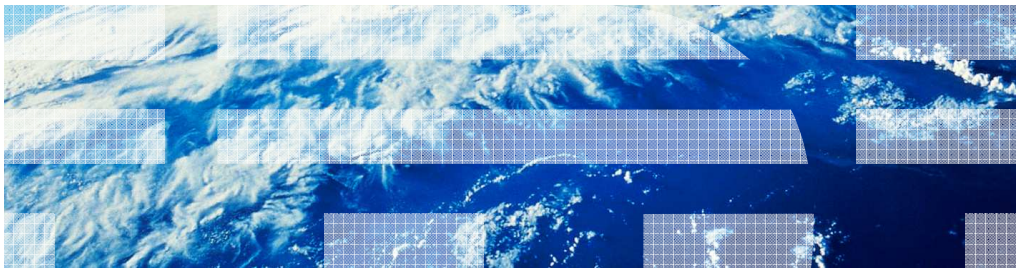
IBM WebSphere DataPower XC10 V2.0

SNMP support



This presentation will discuss the Simple Network Management Protocol support in WebSphere DataPower XC10 V2.0.

Table of contents

- SNMP overview
- SNMP support in WebSphere DataPower XC10 V2.0
- Summary

This presentation will discuss support for the Simple Network Management Protocol (SNMP) in WebSphere DataPower XC10 V2.0. The presentation will first cover the overview of SNMP followed by it's support in the DataPower XC10 appliance.

Section

SNMP overview

This section will cover the SNMP overview.

SNMP

- Simple Network Management Protocol is a UDP-based network protocol
- With SNMP you can monitor hardware devices on the network for scenarios that require administration
- Common devices managed by SNMP include
  - Computer hosts
  - Routers
  - Switches
  - IP telephones
  - Printers

Simple Network Management Protocol is commonly known as SNMP. SNMP is a UDP-based network protocol that is commonly used to communicate with hardware devices on a computer network. SNMP provides a mechanism for monitoring hardware devices, and altering their configurations by requesting information from a service running on the hardware called an agent, and sending the agent requests to alter the hardware's configuration. Hardware devices that are commonly monitored and managed using SNMP include computer hosts, routers, switches, IP telephones, and network printers. Using an SNMP client to communicate with the hardware's SNMP agent, information about the current state of the hardware can be determined. Based on this information, requests can be sent to the device using SNMP to alter it's configuration.

Basic SNMP components

- Managed device
- Agent (software service running as a daemon on the managed device)
- Network management system (commonly referred to as NMS)
  - Read-only or read-write access to managed device
  - Gathers information from the managed device and can send settings to alter the managed devices configuration if granted read-write access
  - SNMP client to interface with managed device's agent
- Managed device is monitored by one or more network management systems
  - Executes applications to monitor and control the managed device

The **three basic components** of an SNMP scenario are: a hardware device to be managed, a service that runs on the device, and a network management system.

The service that runs on the hardware to be managed using SNMP is called an agent. The agent commonly runs as a daemon on the device, constantly listening for requests. When the agent receives an SNMP request from a client, it returns information requested about the state of the hardware. One example of a commonly requested piece of information for a computer system is its hard drive capacity. SNMP clients can request the capacity of the hardware to determine how close the managed device is to having a full hard drive.

A network management system consists of one or more computers on the network that access information about the hardware using the managed device's agent, and make adjustments to the device, using SNMP, based on that information. In order to make adjustments to the hardware device's configuration the SNMP client must be granted read-write access by the hardware's SNMP agent. If a client has read-only access, it will only be allowed to receive information about the hardware's state and is not granted permission to change it's configuration using SNMP. SNMP client applications can be developed to monitor a device's configuration, and automatically send requests to make adjustments to the hardware based on it's monitored data.

SNMP agents

- An SNMP agent on a managed device exposes status information as variables
  - Various data can be made available about the device using SNMP for example:
    - System name
    - Free memory
    - Processor usage
    - Uptime
- SNMP agent can also accept requests from clients to perform 'active' administration
  - Modify managed devices configuration
- Agent status information and active administration commands are defined in "MIB" files

The SNMP agent provides information to SNMP clients, and makes adjustments to the hardware device's configuration based on requests it receives from those clients. Agents can provide a wide variety of data about the hardware device. The information that an agent has available to send to an SNMP client is defined in a management information base, or MIB file. SNMP clients will use the agent's MIB file to see what requests it can make, and what information it can gather from the agent. It will also use the agent's MIB files to see what requests it can make to alter the hardware's configuration.

SNMP MIB files

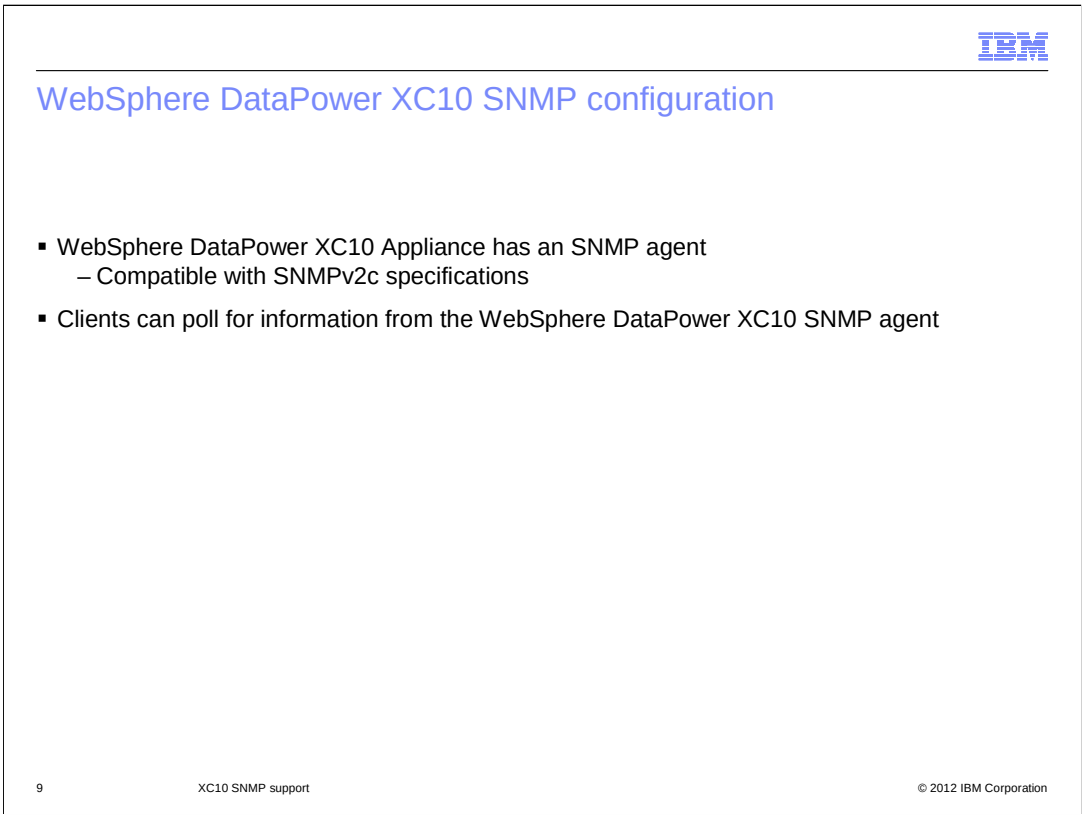
- MIB
  - Management Information Base
  - Defines variables that can be read or set on the managed device using SNMP
    - Information about the managed device that can be polled for using SNMP clients
    - Active management settings that can be set or changed to alter the device configuration using SNMP

An SNMP management information base file (MIB) contains variables that can be read or set on the managed device using SNMP. Clients get a copy of the hardware agent's MIB files, and use them to access data and send requests to change the hardware's configuration using SNMP requests. MIB files are flat text files.

Section

SNMP in WebSphere DataPower XC10 V2.0

This next section will look at SNMP in DataPower XC10 version 2.



WebSphere DataPower XC10 V2.0 has a configurable SNMP agent. The SNMP agent supports SNMPv2c specifications. SNMP clients can connect to WebSphere DataPower XC10 and poll for information using WebSphere DataPower XC10 V2.0's SNMP MIB files. WebSphere DataPower XC10's SNMP agent runs on the appliance as a daemon. System administrators can download the XC10 MIB files from the appliance console and use them to configure a network management system to monitor the WebSphere DataPower XC10 appliance.

WebSphere DataPower XC10 SNMP monitoring

- WebSphere DataPower XC10 SNMP agent can be configured in the appliance console
  - New menu item located under the Appliance tab
    - **Appliance → SNMP Monitoring**

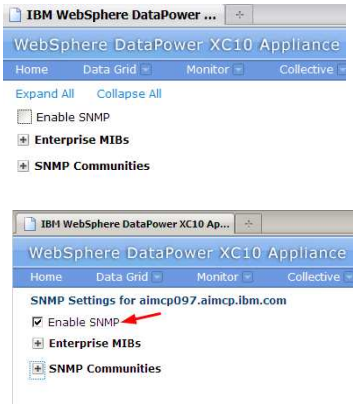
Simple Network Monitoring Protocol (SNMP) monitoring is **not enabled** for the IBM WebSphere DataPower XC10 Appliance by default. SNMP monitoring can be enabled for your IBM WebSphere DataPower XC10 Appliance. This is done by downloading the management information base files (MIBs) provided on the appliance to specify the SNMP data available to the SNMP client.

You must be assigned the Appliance administration permission to perform monitoring and an SNMP client must be configured.

In the WebSphere DataPower XC10 appliance console, a new menu item is available under the appliance tab. Clicking on this menu will take you to the SNMP configuration page.

WebSphere DataPower XC10 SNMP agent configuration

- SNMP configuration options available
  - Enable/disable the SNMP agent
  - Download MIB files for the WebSphere DataPower XC10 SNMP implementation
  - Configure SNMP communities



On the SNMP monitoring configuration page there are three main sections for the configuration of WebSphere DataPower XC10's SNMP agent. From this page, you can enable the SNMP agent. By default, it's disabled. When you click the enable check box the SNMP agent is started. You can also download the agent's MIB files. The last section allows you to create or delete SNMP communities.

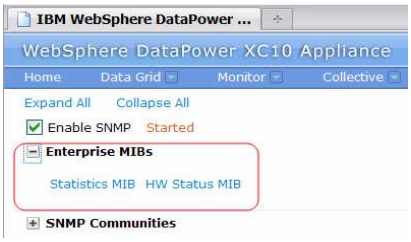
Section

MIBs

This section will discuss WebSphere DataPower XC10 SNMP MIB files.

MIBs downloads

- Download WebSphere DataPower XC10 MIB files
- Use the MIB files with your SNMP client applications
  - Poll for status
- Two MIB files available
  - Statistic MIB
  - Hardware status MIB



WebSphere DataPower XC10's SNMP Management Information Base (MIB) files can be downloaded from this monitoring configuration page. The Enterprise MIB files describe what functions and data are available from the embedded SNMP agent so that your client can appropriately access them. The client can issue SNMP GET, GET-NEXT and GET-BULK commands. You can download the MIB files and import them into your client to access data beyond the base MIB-II data definitions. Expand Enterprise MIBs, and click the name of the MIB file you want to download.

The two available MIB files are **Statistics** and **Hardware Status MIBs**. Statistics MIB includes information that is similar to the statistics that you can see with user interface monitoring functionality. The MIB also includes statistics for container servers. Hardware Status MIB includes information about the state of the hardware, including temperatures, date and time.

Section

Community configuration

This next section will discuss community configuration.

WebSphere DataPower XC10 SNMP communities

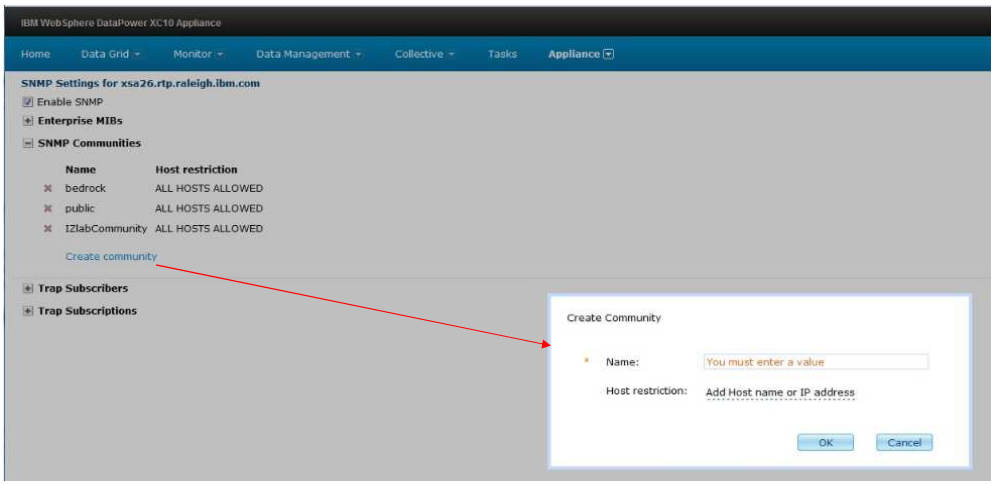
- Add and remove SNMP communities
- Restrict host name access to WebSphere DataPower XC10 SNMP agent

When an SNMP client accesses information from the managed device's agent, it passes the agent credentials as a community name. The community name is equivalent to a username that is used to access information from the managed devices agent. SNMP clients must know which community to use to monitor WebSphere DataPower XC10 activities. Communities can also include a list of host names or IP address's of client machine that are allowed to access the community.

Note that at this time XC10 SNMP communities can only be configured as read-only.

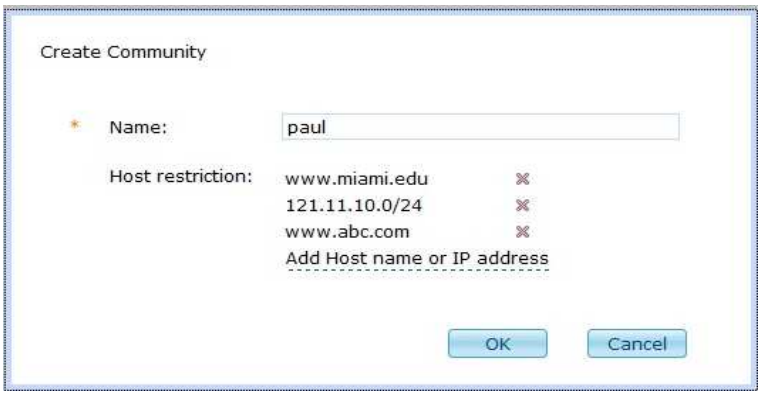
Creating an SNMP community

- Click "**create community**" link



SNMP communities can be created or removed to control the access to the SNMP data available on the appliance. To create an SNMP community, navigate to the Monitoring panel. From the SNMP Monitoring page, expand SNMP Communities. To create a community, click **Create community** on the bottom. Complete the form to describe the SNMP community that you want to create. The **Name** field is the name used to describe an SNMP community.

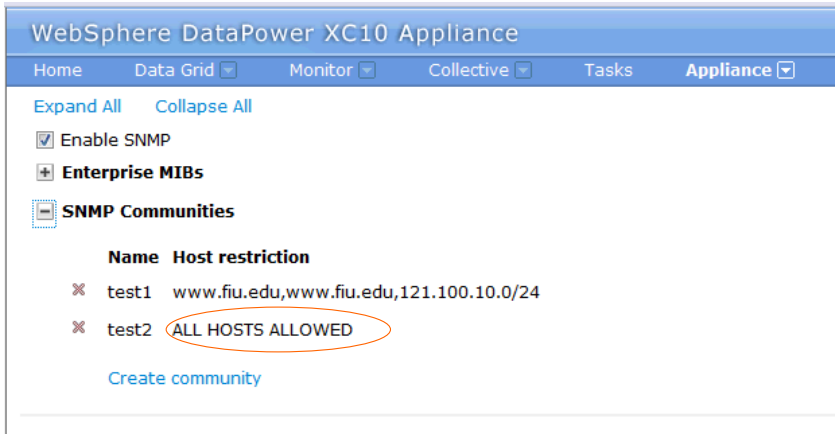
SNMP create community



The **Host restriction** field specifies host names or IP addresses that are allowed to access the community. If a host restriction is included, communication from any other IP address is denied.

When user clicks "Add Host name of IP Address", that area becomes a text box. When user hits "Enter" or clicks outside of the text area the list of entries grow. When user clicks on a red X icon, the corresponding item is removed from the list. When user clicks OK, the dialog goes away, and a new SNMP community will appear, with the entries previously entered appearing as comma-separated values in the "Host restrictions" column in the table.

Host restriction field



If you do not enter anything in the Host Restriction field in the "create" dialog, it will show up in user interface as "ALL HOSTS ALLOWED"

Deleting an SNMP community

To remove an SNMP community, click the red X next to the community you want to remove. Note that communities cannot be modified. If a community has to be modified, then it must be removed and then re-created.

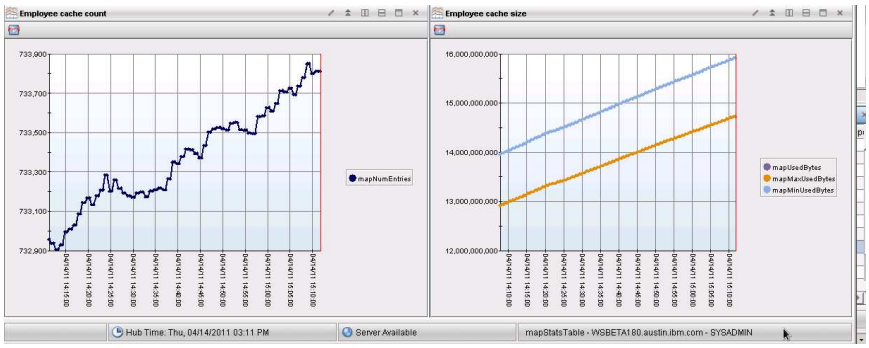
Section

SNMP clients

This section will discuss SNMP clients.

SNMP clients

- WebSphere DataPower XC10 Appliance can be monitored by a network management system using products such as:
  - IBM Tivoli Composite Application Manager (ITCAM)
  - IBM Director
  - HP OpenView
  - Net-SNMP
  - Any monitoring client that can consume MIB-II data



WebSphere DataPower XC10 Appliance can be accessed using any SNMP client that can consume MIB-II data. Common clients that are used to access and monitor managed devices on the network using SNMP include IBM Tivoli Composite Application Manager and IBM Director. Other vendor applications can also be used as SNMP clients to interface with WebSphere DataPower XC10 including HP OpenView. The free SNMP toolkit available from Net-SNMP.org contains a suite of SNMP protocol applications that can be used to monitor WebSphere DataPower XC10.

Section

Summary

This section will summarize SNMP feature in WebSphere DataPower XC10.

Summary

- Simple Network Management Protocol is a UDP-based network protocol
- With SNMP you can monitor hardware devices on the network for scenarios that require administration
- SNMPv2c communities can be added, removed, and managed
  - Specify community name
  - Host name restrictions

To summarize, Simple Network Management Protocol is commonly known as SNMP. SNMP is a UDP-based network protocol that is commonly used to communicate with hardware devices on a computer network. WebSphere DataPower XC10 V2.0 has an SNMP agent that can be enabled or disabled. The WebSphere DataPower XC10 appliance console has a new configuration page under the appliance tab. This SNMP settings configuration page has elements to help configure the SNMP agent settings. SNMPv2c communities can be configured for the agent, specifying the name, and host name restrictions.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_XC10_SNMPSupport.ppt

This module is also available in PDF format at: ../XC10_SNMPSupport.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, DataPower, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.