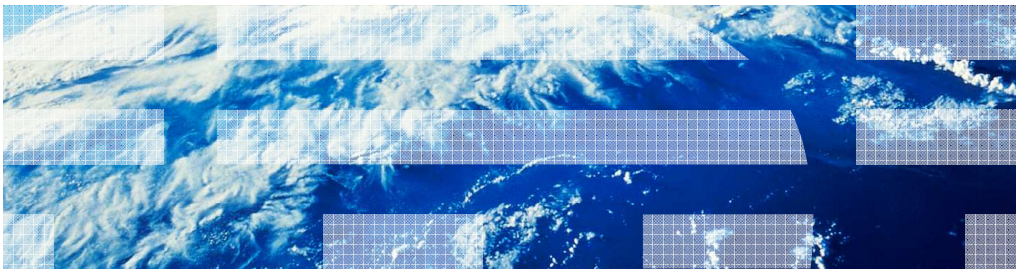
IBM WebSphere CloudBurst Appliance V2.0

SNMP management



This presentation will discuss the Simple Network Management Protocol support in WebSphere CloudBurst™ V2.0.

Agenda

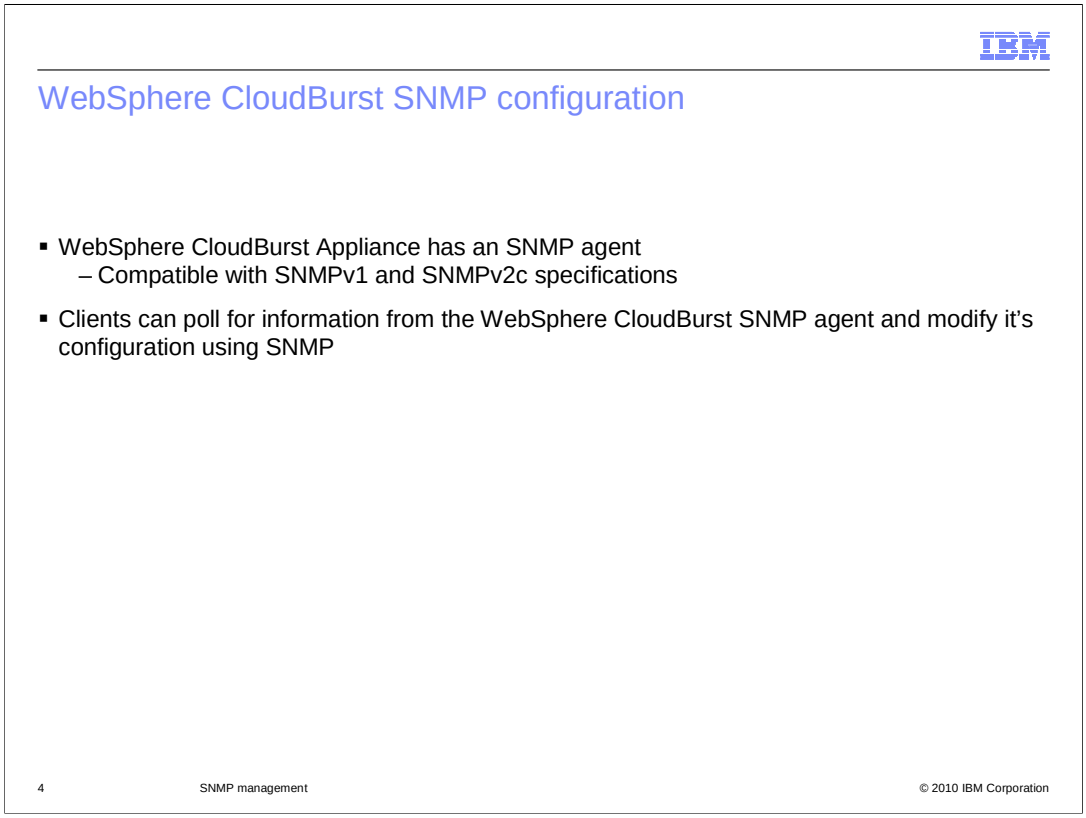
- SNMP Overview
- Community configuration
- MIBS
- Trap subscriptions
- SNMP clients
- Examples
- Summary

This presentation will discuss support for the Simple Network Management Protocol in WebSphere CloudBurst V2.0.

Section

Overview

This section will discuss SNMP support in WebSphere CloudBurst V2.0.



WebSphere CloudBurst V2.0 has a configurable SNMP agent. The SNMP agent supports SNMPv1 and SNMPv2c specifications. SNMP clients can connect to WebSphere CloudBurst and poll for information using WebSphere CloudBurst V2.0's SNMP MIB files. WebSphere CloudBurst's SNMP agent runs on the appliance as a daemon. The port number is configurable, and system administrators that configure a network management system to monitor WebSphere CloudBurst can access the MIB files from the administrative console. The administrative console and the command line interface can be used to configure the SNMP options for the WebSphere CloudBurst agent.

WebSphere CloudBurst SNMP agent

- WebSphere CloudBurst SNMP agent can be configured in the administrative console UI
  - New menu item located under the Appliance tab
    - Appliance > Monitoring

In the WebSphere CloudBurst administrative console, a new menu item is available under the appliance tab. This link titled monitoring, takes WebSphere CloudBurst administrators to the SNMP configuration page.

WebSphere CloudBurst SNMP agent configuration

- SNMP configuration options available
  - Enable/disable the SNMP agent
  - Configure the agent port number
  - Configure SNMPv2c communities
  - Download MIB files for the WebSphere CloudBurst SNMP implementation
  - Edit trap subscriptions
  - Configure trap subscribers

On the monitoring configuration page of the administrative console there are four main sections for the configuration of WebSphere CloudBurst's SNMP agent. You can enable or disable the SNMP agent, and configure the port that the agent is available on. You can configure SNMPv2c communities, download the agent's MIB files, configure the events for trap subscriptions, and configure client trap subscribers.

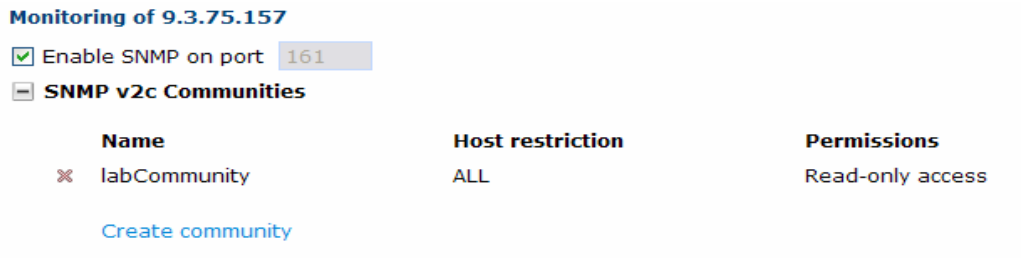
Section

Community configuration

This section will discuss community configuration.

WebSphere CloudBurst SNMPv2c communities

- Add and remove SNMPv2c communities
- Set community access
  - Read-only
  - Read-write
- Restrict host name access to WebSphere CloudBurst SNMP agent



When an SNMP client accesses information from the managed device's agent using SNMP, 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. Communities are configured as read-only or read-write access, and can include a host restriction. SNMP clients must know which community to use to monitor WebSphere CloudBurst activities. The host name or IP address of the client machine must be configured in the community settings of the WebSphere CloudBurst SNMP agent.

Section

MIBS

This section will discuss the WebSphere CloudBurst SNMP MIB files.

WebSphere CloudBurst's SNMP MIB files can be downloaded from this monitoring configuration page of the administrative console. Clients that want to interface with the WebSphere CloudBurst SNMP agent will have to download these files and configure them with their SNMP client. Three MIB files are available for the WebSphere CloudBurst appliance's SNMP agent activities. The first is the WebSphere CloudBurst status MIB. This MIB file contains variables that are used to gather information about WebSphere CloudBurst's current state. The WebSphere CloudBurst configuration MIB contains variables that are used to access the management capabilities of WebSphere CloudBurst using SNMP in order to alter it's configuration. The notifications MIB file contains the information necessary for SNMP client trap daemons to receive and work with WebSphere CloudBurst SNMP trap subscriptions.

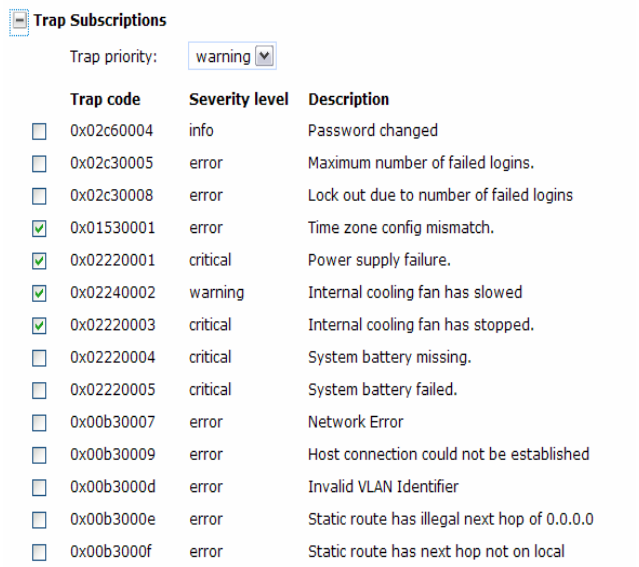
Section

Trap subscriptions

This section will discuss SNMP trap subscriptions.

WebSphere CloudBurst SNMP trap subscriptions

- Trap subscriptions can be configured to send notifications about WebSphere CloudBurst events
  - Set global minimum trap level
  - Enable or disable notification for specific events
  - Each trap has a severity level
    - •Critical
    - •Error
    - •Warning
    - •Notice
    - •Info



SNMP trap subscriptions are supported by WebSphere CloudBurst V2.0. The events that trigger SNMP traps to be sent to clients by the WebSphere CloudBurst SNMP agent can be configured in the trap subscriptions section of the monitoring page. Individual traps can be enabled or disabled. A list of available traps is available under the trap subscriptions section. Each trap that has a check box in the enabled column will trigger a notification to be sent to any clients that are configured as trap subscribers. WebSphere CloudBurst SNMP traps are separated into four severity levels, info, warning, error, and critical. The global minimum trap level can be set on the WebSphere CloudBurst SNMP agent using the dropdown list. Depending on what trap level is specified in the drop down list, any traps that have a lower priority than what is set are not sent to subscribers. For example, if the trap level is set to Warning, Notice and Info level traps are then ignored by the agent and no notifications for those events are sent. Events for Warning, Error, and Critical traps are sent for that configuration.

WebSphere CloudBurst SNMP trap subscribers

- Configure subscribers to trap subscriptions
- Specify client IP address and port
- Configure client access to community
- Set client security version (SNMPv1 or SNMPv2c)

Subscribers to SNMP traps can be configured under the trap subscribers section of the WebSphere CloudBurst administrative console monitoring page. Subscribers to SNMP traps can be added by clicking the create trap subscriber button. In the dialog that opens you can input the SNMP client's information. The IP address, the port the client's trap daemon is listening on, the community the client belongs to, and the SNMP security version must be specified. WebSphere CloudBurst supports SNMPv1 and SNMPv2c security versions. Once clients are registered to receive trap events, events configured in the trap configuration are sent to the client by the WebSphere CloudBurst SNMP agent when they occur.

Section

SNMP clients

This section will discuss SNMP clients.

SNMP clients

- WebSphere CloudBurst 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 CloudBurst Appliance can be accessed using SNMP clients that can consume MIB-II data. Common clients that are used to access an 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 CloudBurst 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 CloudBurst.

Section

Examples

This section will discuss examples of using SNMP with WebSphere CloudBurst.

Example 1: monitoring WebSphere CloudBurst information using SNMP

- A network administrator enables monitoring of CloudBurst Appliance with an SNMP monitoring client such as ITCAM
- User views resource utilization statistics over time to understand appliance load trends
  - Processor
  - Memory
  - Network input/output
- Network administrator gains understanding of the appliance's workload

An example of using WebSphere CloudBurst SNMP monitoring support is to monitor system statistics. A comprehensive SNMP monitoring client can connect to WebSphere CloudBurst's SNMP agent to monitor and log system statistics. The network administrator can view resource information such as processor usage, memory load, and network input/output over time to understand WebSphere CloudBurst's load trends.

Example 2: Trap subscription using WebSphere CloudBurst SNMP

- WebSphere CloudBurst SNMP agent configured to send a trap notification when the internal cooling fan stops
- The trap is enabled and the SNMP client subscription is configured
- SNMP client trap daemon is started on the network management system
- The cooling fan on the WebSphere CloudBurst Appliance stops
- The trap is caught by the WebSphere CloudBurst SNMP agent and a notification is sent to the client trap daemon
- The SNMP client trap daemon receives the notification that the internal cooling fan has stopped
- The administrator monitoring the WebSphere CloudBurst appliance using the network management system sees that the fan has stopped and investigates the problem
- The fan is replaced and WebSphere CloudBurst resumes normal function

Another example of interfacing with WebSphere CloudBurst's SNMP agent involves using trap subscriptions. WebSphere CloudBurst Appliance's SNMP trap subscription support can be configured to alert a client when the internal cooling fan stops. A network administrator using an SNMP client can configure a trap daemon to listen for notifications from WebSphere CloudBurst. They can enable the trap on WebSphere CloudBurst to send a notification when the internal cooling fan stops. They can add their client trap daemon as a subscriber to WebSphere CloudBurst's SNMP trap notifications. When the internal cooling fan stops and the trap for that event is enabled, the WebSphere CloudBurst SNMP agent will send a notification to the waiting client trap daemon. The administrator can then be notified by it's SNMP client that an event has occurred, and will know that the internal cooling fan of WebSphere CloudBurst has failed. They can then replace the fan.

Section

Summary

This section will summarize using SNMP with WebSphere CloudBurst.

Summary

- WebSphere CloudBurst appliance has an SNMP agent
- SNMP agent can be enabled or disabled
- SNMPv2c communities can be added, removed, and managed
  - Specify community name
  - Read-only or read-write access
  - Host name restrictions
- Trap subscriptions can be configured to send notifications to listeners using a trap daemon client
- Trap subscribers are configured
  - Specify trap subscriber IP addresses
  - Community affiliation
  - SNMPv1 or SNMPv2c security usage

WebSphere CloudBurst V2.0 has an SNMP agent that can be enabled or disabled. The agent is configurable, and the port number on which it runs can be specified. The WebSphere CloudBurst administrative console has a new monitoring page under the appliance tab. This monitoring configuration page has elements to help configure the SNMP agent settings. SNMPv2c communities can be configured for the agent, specifying the name, read, write, and host name restrictions. Trap notifications for WebSphere CloudBurst events can be enabled or disabled. Clients that want to subscribe to SNMP traps can be configured. Registering the IP, community, and security version for the clients that want to receive trap subscription notifications from the WebSphere CloudBurst SNMP agent enables them to receive traps.

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_CB20_SNMPManagement.ppt

This module is also available in PDF format at: ../CB20_SNMPManagement.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, CloudBurst, Tivoli, 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

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.