Cisco IOS Embedded Event Manager Version 2.4 Expanded Capabilities and New Interfaces

Last updated: August 2008

Abstract

This document details new features available with the release of Cisco IOS® Embedded Event Manager (EEM) version 2.4.

Features introduced include:

- Multiple Event Detection—For onboard event correlation
- Remote Program Control (RPC) Event Detector—A new external interface to invoke policies
- SNMP Proxy Event Detector—Another new interface to trigger events from neighboring equipment
- Script Policy Refresh—Introduces a new pull model for managing policies
- Interface Counter Event Detector Enhancement—Improves usability
- Bytecode Support
- General Usability Improvements

Introduction

Cisco IOS Embedded Event Manager (EEM) is a powerful tool integrated with Cisco IOS Software for monitoring and management from within the device itself. EEM offers the ability to monitor software subsystems and take informational, corrective, or any desired action when the monitored events occur or when a threshold is reached. Capturing the state of the router during such situations can be invaluable in taking immediate recovery actions and gathering information to perform root-cause analysis. Network availability is also improved if automatic recovery actions are performed without the need to fully reboot the routing device. Cisco IOS EEM is extremely versatile, allowing an operator to perform many actions, including but not limited to:

- Automation of standard configurations
- Information gathering for diagnosing events
- Real time monitoring and action based on events seen on the router

For more information on Cisco IOS Embedded Event Manager (EEM) capabilities, go to http://www.cisco.com/go/eem.

Multiple Event Detection

In previous EEM versions, actions occur based on a single event. In other words, policies only support a single event specification. EEM 2.4 enhances the function to allow much more control by being able to correlate multiple events to trigger actions. Up to 6 event statements can be used in an applet and up to 8 events can be used in a Tcl script, with support for Boolean functions. This capability provides a unique capability to assist in troubleshooting complex issues with multiple

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

dependencies, as well as more robust methods of configuring and monitoring devices by correlating events together. For example, you may want to monitor both the number of routes and the available memory on a system and take an action if either of the two exceeds a certain threshold.

Events are differentiated and referenced through the addition of **tag**, **trigger** and **correlate** keywords. The following example shows an applet which will detect if all three of the following events occur within an hour:

- A particular syslog message
- An SNMP counter crosses a threshold
- BGP CPU utilization is over 30% for 10 minutes

```
event manager applet example
   event tag e1 syslog pattern "syslog_message"
   event tag e2 snmp oid 1.2.3.4 get-type exact entry-op gt entry-val
1000 poll-interval 10
   event tag e3 ioswdsysmon sub1 cpu-proc taskname "BGP" op gt val 30
triggerperiod 600
   trigger occurs 1 period 360
      correlate event e1 and event e2 and event e3
      action 01.0 syslog msg "All three events occurred in an hour."
```

Another example of multiple event detection shows how a router can detect DHCP changes on an interface and report the new IP address to an email address:

```
event manager applet getIP
  event tag restart syslog pattern “LINEPROTO-5-UPDOWN:.*FastEthernet0
.*state to up”
  event tag periodic timer watchdog time 86400
  trigger
   correlate event restart or event periodic
  action 1.0 cli command “show int Fa0 | inc Internet address is”
  action 2.0 mail to user@cisco.com from user@cisco.com server
smtp.cisco.com subject “IP address info” body “IP address is:
$_cli_result”
```

The previous example policy will detect when interface FastEthernet0 has come up by watching for the appropriate syslog message. The policy will also run every 24 hours (assuming the DHCP lease expires every 24 hours). When the policy runs, it will email the results of the CLI command, "show int Fa0 | inc Internet address is” to the specified user.

Similar event differentiators have been added to the Tcl syntax to support multiple event detection.

```
::cisco::eem::event_register_xxx tag 1 ...
       ::cisco::eem::event_register_yyy tag 2 ...
        ::cisco::eem::trigger {
              ::cisco::eem::correlate event 1 and event 2
              ::cisco::eem::attribute tag 1 occurs 1
              ::cisco::eem::attribute tag 2 occurs 1
        } [occurs <occurs-val>] [period <period-val>] \
              [period-start <period-start-val>] [delay <delay-val>]
```

EEM 2.4 adds two new event detectors, both of which allow the invocation of an EEM policy from outside the router or switch. This ability allows vast flexibility to create robust services based upon events beyond network infrastructure devices. For example, if a router is attached to a UPS and power is lost, the UPS could report to the router how much time it can provide power and the router can take action to gracefully shutdown if the power is not restored within a certain period. One method uses SOAP messages over SSHv2 and the other uses SNMP. Be sure to follow proper configuration guidelines to maintain the highest level of security and authentication.

Remote Program Control Event Detector

The Remote Program Control Event Detector accepts SOAP over SSHv2 requests to the router or switch which in turn can be used to invoke a defined EEM policy or script. The format of the soap request/reply is as follows:

Request Syntax:

```
<?xml version="1.0"?>
<SOAP:Envelope xmlns:SOAP="http://www.cisco.com/eem.xsd">
<SOAP:Body>
  <run_eemscript>
    <script_name> name of script </script_name>
    <argc> argc value </argc>
    <arglist>
    <l> argv1 value </l>
    <2> argv2 value </l>
          …
    <n> argvn value </n>
    </arglist>
  </run_eemscript>
</SOAP:Body>
</SOAP:Envelope>
```

Reply Syntax:

```
<?xml version="1.0"?>
<SOAP:Envelope xmlns:SOAP="http://www.cisco.com/eem.xsd">
<SOAP:Body>
   <run_eemscript_response>
      <return_code> rc </return_code>
```

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
      <output> output string </output>
   </run_eemscript_response>
</SOAP:Body>
</SOAP:Envelope>
```

A sample Perl API with additional documentation and examples is located at: http://forums.cisco.com/eforum/servlet/EEM?page=eem&fn=script&scriptId=1183

In order to provide the highest level of security, EEM RPC must be run over SSHv2. SSHv2 provides an encrypted session for executing server programs. The following describes basic SSHv2 router configuration:

Configure a user if one has not been created.

```
router (config)#username operator privilege 15 password 0 lab
```

Configure the router to enable ssh

```
router(config)# aaa new-model
router(config)# crypto key generate rsa  usage-keys label sshkeys modulus 768
router(config)# ip ssh version 2
```

Configure the domain name:

```
ip domain-name <somename>
Allow SSH access to the VTY ports:
line vty 0 4
  transport input ssh
```

Connect to the router using ssh to make sure ssh is up and running:

```
ssh -2 -c aes256-cbc -m hmac-sha1-96 user@router
```

The router or switch also needs to be configured to accept RPC commands with the option to restrict access with an access list. By default, RPC commands are not accepted by EEM.

```
router(config)#event manager detector rpc ssh [acl access-list-number]
```

The router or switch can also be configured to limit the number of concurrent rpc sessions allowed with:

```
router(config)#event manager detector rpc max-sessions 5
```

Events require registration to accept RPC events. Use the following Tcl command to allow the rpc message to be run for this script:

```
::cisco::eem::event_register_rpc
```

SNMP Proxy Event Detector

The SNMP proxy event detector allows the router or switch to execute an EEM script on the receipt of an SNMP trap. Tcl scripts and applets use the following syntax to enable this functionality.

Before creating any SNMP notification policies, SNMP proxy support must be enabled by the following global config command:

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
router(config)#snmp-server manager
```

Tcl Syntax:

```
event_register_snmp_notification
    oid <oid-number> oid_val <oid-value> op {gt|ge|eq|ne|lt|le}
    [src_ip_address <ip_address>]
    [dest_ip_address <ip_address>]
```

Applet Syntax:

```
event snmp-notification
    oid <oid-number> oid-val <oid-value> op {gt|ge|eq|ne|lt|le}
    [src-ip-address <ip_address>]
    [dest-ip-address <ip_address>]
```

Applet Example:

Configure an SNMP notification applet to run an EEM Tcl policy if the router receives a SNMP notification on destination address 192.168.1.1 from 10.1.1.1 which contains a varbind of 1.3.6.1.2.1.15.3.1.2.10.1.1.2 (bgpPeerState for peer 10.1.1.2), and the OID's value is less than 6 (in this case, indicating that the BGP peer is no longer established).

```
event manager applet bgp-trap-watch
 event snmp-notification dest-ip-address 192.168.1.1 oid
1.3.6.1.2.1.15.3.1.2.10.1.1.2 op lt oid-val 6 src-ip-address 10.1.1.1
action 1 policy adjust_routes.tcl
```

Security for the SNMP event detector can be achieved by using access-lists to control devices with authority to invoke SNMP triggered EEM scripts. CoPP can also be used to rate limit the overall SNMP traffic to the router. The use of SNMPv3 is also recommended.

Script Policy Refresh

Script Policy Refresh allows the router to automatically update Tcl or Tcl bytecode policy from a pre-determined location. This capability allows greater ease in managing EEM scripts in both development and production environments. Simple commands allow the refresh of one, some or all registered scripts, which can significantly reduce administration tasks when updating EEM policies on any size network.

The following optional config command specifies a default location from which to copy policies:

```
router(config)#event manager directory user repository <url location>
```

A new exec command is used to initiate the script refresh:

```
router#event manager update user policy [name <policy-name> | group
<regular expression>] repository <url-location>
```

Use the event manager update command in exec mode to specify an immediate policy update. Policies can be specified directly by name or through a regular expression pattern string to match a group of policies using the group option. If an error occurs registering a newly downloaded policy, the policy that was previously registered will be left unregistered. All activities will be logged to the cli exec session and syslog.

Example:

```
event manager update user policy name intf_down.tcl repository tftp://2.2.2.2/eempolicy/eem_
```

```
event manager update user policy group “*.tcl”
```

An applet may be used with a crontab to invoke the execution of the update on a periodic basis. In the following example, the cli command to update user policies will be run once a week at midnight on Sunday.

```
event manager applet update
 event timer cron cron-entry "@weekly"
 action 1 cli command "event manager update user policy group *.tcl"
```

Care should be taken to ensure only appropriate persons have access to the script repositories, as the router will provide no additional authentication during the script refresh process.

Interface Counter Event Detector—Rate Based Trigger

The interface counter Event Detector (ED) adds the ability for an interface event to be triggered based on a rate of change over a period of time. A rate can be specified both for the entry value and the exit value.

The “event interface” applet CLI command has been modified to accept three new keywords:

```
[entry-type {value | increment | rate}]
[exit-type {value | increment | rate}]
[average-factor <average-factor-value>]
```

Similar commands are added for Tcl scripts:

```
[entry_type {value | increment | rate}]
[exit_type {value | increment | rate}]
[average_factor <average-factor-value>]
```

Applet syntax :

```
[no] event [<ev-label>] interface name <interface-name> parameter <counter-name>
entry-val <entry-val> entry-op {gt|ge|eq|ne|lt|le} [entry-type {value | increment | rate}]
[exit-comb {or | and}]
[exit-val <exit-val> exit-op {gt|ge|eq|ne|lt|le} exit-type {value | increment | rate}]
[exit-time <exit-time-val>]
 poll-interval <poll-int-val>
[average-factor <average-factor-value>]
```

The following is an example of the rate based trigger in action. This applet monitors for errors on an interface. If the rate of change averages to two or more over three 60 second polling cycles, then the interface is reset by doing a shut/no shut. The policy will re-arm after the rate has dropped below 1.

```
event manager applet int-rate-test
 event interface name FastEthernet0/24 parameter input_errors entry-op ge entry-val 2 entry-type rate exit-op lt exit-val 1 exit-type rate average-factor 3 poll-interval 60
 action 1.0 syslog msg "Interface input error rate for $_interface_name is $_interface_value; resetting..."
 action 2.0 cli command "enable"
 action 3.0 cli command "interface $_interface_name"
 action 4.0 cli command "shut"
 action 5.0 cli command "no shut"
 action 6.0 cli command "end"
```

Another example monitors a vlan interface for excessive broad cast packets

```
event manager applet BCAST-CHECK
  event interface name "Vlan100" parameter receive_broadcasts entry-val 3000 entry-op gt entry-type rate poll-interval 60 average-factor 5
  action 1.0 syslog msg "BROADCAST STORM DETECTED"
```

This applet monitors a vlan interface to detect excessive input broadcasts. If the interface receives an average of 3000 broadcast packets per minute over a five minute period, a message will be sent to syslog. The number of broadcast packets received will be checked every 60 seconds, if the average of the 5 most recent values exceeds 3000, the event is triggered.

Bytecode Support

In Cisco IOS Software Release 12.4(20)T, EEM 2.4 introduces Bytecode Language (BCL) support by accepting files with the standard bytecode script extension .tbc. Tcl version 8 defines a BCL and includes a compiler that translates Tcl scripts into BCL. Valid EEM policy file extensions in EEM 2.4 for user and system policies are .tcl (Tcl text files) and .tbc (Tcl bytecode files).

Storing Tcl scripts in bytecode improves the execution speed of the policy because the code is precompiled, creates a smaller policy size, and obscures the policy code. Obfuscation makes it a little more difficult to modify scripts and hides logic to preserve intellectual property rights.

Support for bytecode is being added to provide another option for release of supported and trusted code. Customers should only run well understood, or trusted and supported software on network devices.

To translate a Tcl script to bytecode you can use procomp, part of Free TclPro Compiler, or the Active State Tcl Development Kit. When a Tcl script is compiled using procomp, the code is scrambled and a .tbc file is generated. The bytecode files are platform-independent and can be generated on any operating system on which TclPro is available, including Windows, Linux, and UNIX. Procomp is part of TclPro and available from http://www.tcl.tk/software/tclpro.

General Usability and CLI Improvements

The following ease of use items have been added to EEM 2.4:

Support for passing parameters using the “event manager run” exec command.

```
event manager run tclsrc.tcl <arg1> <arg2>
```

A clear command to kill a Tcl script. In some cases, scripts may be in a loop or some other condition that will not allow the script to complete. Previously, only a device reload would stop the execution of the script.

To clear or kill a policy, use the following command:

```
event manager scheduler clear policy ID
```

Where ID is the job ID found by running the "show event manager policy pending" command. If you want to terminate all running policies, use the command:

```
event manager scheduler clear all
```

The registration substitution enhancement allows for variable use within an event registration line, or for the entire event itself.

```
::cisco::eem::event_register_timer $timeparms
```

```
or
```

```
$registration_line $parms
```

`show event manager` has been enhanced to show multiple events

`show event manager policy pending` now displays a policy Job ID

`show event manager policy events` now displays a policy Job ID and a completion status.

`show event manager history events detailed` now displays a policy Job ID and a completion status.

`show event manager history` traps now displays a policy Job ID for server traps.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Printed in USA C11-492226-00 08/08

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.