Embedded Management and Cisco IOS Embedded Event Manager

Last updated: November 2011

Q. What is embedded management?

A. The term "embedded management" is used to describe the software subsystems within Cisco IOS® Software that help manage, monitor, and automate actions within a router or switch running Cisco IOS Software.

Q. What is unique about embedded management and Cisco IOS Software Embedded Event Manager (EEM) in particular?

A. Traditionally, network management happens from outside the network looking in. Embedded management and EEM add a new dimension. It is management from within the network and within the device itself.

Q. What benefit do I get from EEM?

A. EEM is a generic, onboard automation platform that can be used in a wide range of scenarios such as automatic fault detection and alerting, automated diagnostics and troubleshooting, zero-touch deployment, automatic device configuration, and feature customization. The major benefit comes from the fact that users can easily insert custom logic into network devices without having to upgrade the Cisco IOS Software image. The flexibility and extensibility brought by EEM allow customers to effectively reduce operational expenses and protect their long-term investment on network infrastructures enabled by Cisco IOS technologies.

Q. I already have a network management system. Do I need EEM?

A. EEM is effectively turning a traditionally dumb box into an intelligent collaborative component in the overall network management system. External Network Management Systems (NMSs) play significant roles in fault management, configuration management, capacity planning, provisioning, and data collection. The embedded intelligence built on top of EEM can be used in conjunction with NMSs to provide reliable, scalable, and distributed solutions in networks of different sizes. For example, there could be instances where some problem cuts off communication to an external management system, leaving it unable to manage the device. Or it might be difficult to achieve the desired polling rate for many managed devices from a central system. In this case, distributing part of the management burden to the device itself might be a better solution.

Q. I have a small business network with very little network management. Should I care about EEM?

A. Because EEM is included as part of the Cisco IOS Software image and runs on the routers and switches themselves, you can use this platform to build some very simple data collection and device management capabilities inside the box without incurring additional cost for an external NMS.

Q. This is starting to sound interesting. Basically, how does EEM work?

A. EEM consists of three main components: event detectors, the event manager server, and the policy director. These are software components in the Cisco IOS Software. The event detectors do just that: detect when certain events occur within Cisco IOS Software and notify the event manager server. The policy director registers with the event manager server to receive events and implements policy actions. The policies are either system policies that come with Cisco IOS Software or user policies defined by you. After being registered, the policy's actions are carried out whenever the event of interest occurs. The event manager

server is responsible for keeping track of which policies are registered to which events. It is also responsible for multievent correlation, notifies the appropriate policy engine to execute a policy, keeps track of event and script history, and performs policy scheduling.

Q. What are some examples of events?
A. For example, you might have a policy run when a particular syslog message occurs. Or a policy could run when an interface fails. Or a policy could run when CPU utilization reaches some specified threshold. There are many examples using the available event detectors.

Q. How many different event detectors are there?
A. There are currently 23 event detectors and more to come in future Cisco IOS Software releases.

Q. How are EEM policies defined?
A. User policies are defined by you, the customer. There are two types of user policies: applet policies and Tcl policies. They are registered using configuration Command-Line Interface (CLI) commands. See more about each of them in later questions.

Q. Can an EEM policy send a Simple Network Management Protocol (SNMP) trap?
A. Yes. The MIB that defines the trap or inform is CISCO-EMBEDDED-EVENT-MGR-MIB.my and can be retrieved from Cisco.com. Starting with EEM 3.0, you can also generate a custom trap from your EEM policies.

EEM Availability

Q. Is EEM available now?
A. Yes. It is available for many Cisco® products. It is in Cisco IOS Software mainline, "T," "S," and "SX/SY" software trains. Please see Cisco IOS Software Feature Navigator for more information. Similar functionalities are also present on IOS-XR and NX-OS products.

Q. Are there different versions of EEM?
A. Yes. EEM version 1.0 was introduced in Cisco IOS Software Releases 12.0(26)S and 12.3(4)T. Later versions of EEM have been made available in Cisco IOS Software Releases 12.2SX, 12.2SR, 12.2SB, 12.4, and 12.4T, 12.2SG, 12.2SE, and Cisco IOS XE. The latest version at the time this was prepared was EEM version 4.0.

Q. Where can I get more details about the different EEM versions?
A. Please refer to the EEM user guides posted at http://www.cisco.com/go/eem.

EEM Applet Policies

Q. What is an applet policy?
A. An applet policy is a fairly simple policy defined using the Cisco configuration CLI. In EEM 3.0, we introduced control structure in applet policy support so that users can define more sophisticated logic with it. With EEM 4.0, IOS Shell (IOS.sh) based policies can be configured inline and stored as part of running configuration providing even more flexibility.

Q. Can I send an email message using an applet policy?
A. Yes, EEM version 2.1 and later allow this. With EEM 4.0, EEM applet (and Tcl-based) policies can establish secured SMTP connections with public email servers using TLS/SSL. In addition, EEM 4.0 supports custom

SMTP ports, for example, non-default SMTP ports for enhanced security or talking to email servers that use a non-standard SMTP port.

Q. Can I issue a Cisco IOS Software CLI command?
A. Yes.

Q. Can I parse the output from CLI commands and different actions based on the output using applet policies?
A. No. You will probably want to use a Tcl policy for that.

EEM TCL Policies

Q. What is a Tcl policy?
A. It is an EEM policy programmed using the Tcl programming language.

Q. Do you mean to say there is a Tcl interpreter in Cisco IOS Software?
A. Yes, and there has been since Cisco IOS Software Release 12.0. The current version is 8.3.4. It is used by the voice-over-IP (VoIP) subsystems in Cisco IOS Software for Interactive Voice Response (IVR), Embedded Syslog Manager (ESM), and the Cisco IOS Software Tcl shell as well as with EEM.

Q. How do I create Tcl policies?
A. Typically, offline on a PC, using a text editor or programming environment. You would code your policy, then download it (copy it) to the router or switch using Trivial File Transfer Protocol (TFTP) or some other protocol that works, then register it using the EEM configuration CLI commands, then test it. You can also store your policies in a remote server and rely on the EEM policy refresh command to pick up the policy automatically from there.

Q. What if it does not work?
A. There are some debug commands to help you find any error in your policy. You would typically want to try your policy in a test environment before using it in a production network. It might take a few iterations to get it right. Each time you modify your code, transfer it to the router, unregister it, reregister it, and try it. Continue iterating through those steps until you are satisfied, and then deploy your EEM Tcl policy to your production routers.

Q. Is there any management tool to help with managing the Tcl policies? What about CiscoWorks Resource Manager Essentials?
A. CiscoWorks LAN Management Solution (LMS) 3.1 network management system supports the deployment and configuration of EEM policies. There are also powerful third-party tools, such as RuBAN (Run Book Automation) by Davra Networks, a Cisco registered development partner, that you can use to help with reducing manual labor, lowering operational costs, and improving overall operational efficiencies in complete network environments using EEM. For more information about Davra Networks, visit http://www.davranetworks.com or email info@davranetworks.com

Q. Suppose my Tcl script gets in a loop; will it consume all the resources and bring down my router?
A. EEM supports enforcing a threshold on the maximum time policy execution can take, and the default value is 30 seconds. Unless you explicitly remove the control or extend the maximum run-time limit, the system will terminate any policy execution in 30 seconds. In addition, with EEM 4.0, you can limit the maximum amount of system resources EEM policies can consume, block new policy execution when the system is already busy with existing functionalities, as well as, set policy priorities.

Q. Can someone load a virus into the router using this Tcl interpreter or with EEM?

A. No. Not without the enable password for the router. The configuration and registration of any EEM policy is done through the configuration and you must first have authority for that. At registration the policy is read into the router's memory and implemented from there. With EEM 4.0, Tcl-based policies can be registered remotely and securely managed centrally on a server instead of on a router or switch making it harder for someone to load a virus. In addition, with EEM 4.0, 3rd party digital signature support, and policy checksum verification support provide an extra layer of protection against EEM policies that might be forged by an untrusted source.

Q. Where can I learn Tcl and how to use it for EEM?

A. There are many excellent books about Tcl programming. One widely acclaimed title is *Practical Programming in Tcl and Tk* by Brent B. Welch. The programming and use of EEM Tcl extensions are covered in the *Writing Embedded Event Manager Policies* guide (see Cisco IOS Software documentation).

Q. What effect does EEM have on router or switch performance?

A. First, you do not have to use EEM, and all user Tcl policies are completely disabled by the **no event manager directory user policy** command. The effects on performance depend on the number of policies registered and the number of event manager scheduler threads configured. The number of policies that can be registered is limited by the amount of available memory. With EEM 4.0, the maximum amount of system resources EEM policies can consume can be set. EEM 4.0 also allows you to block new policy execution when the system is already busy with existing functionalities.

Q. Can I send an email message from an EEM Tcl policy?

A. Yes. With EEM 4.0, EEM Tcl (and CLI-based applet) policies can establish secured SMTP connections with public email servers using TLS/SSL. In addition, EEM 4.0 supports custom SMTP ports, for example, non-default SMTP ports for enhanced security or talking to email servers that use a non-standard SMTP port.

Q. Can I register Tcl policies that have been compiled using TclPro compiler?

A. Yes.

For More Information

For more information about Cisco IOS Software EEM, visit http://www.cisco.com/go/eem, contact your local account representative, or email askabouteem@external.cisco.com.

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.**

Printed in USA C67-573455-02 11/11