

Création de scripts sur les routeurs : Embedded Event Manager

1. Introduction

Le réseau est devenu une composante critique de l'infrastructure IT de toute entreprise. Le support des applications métiers, des communications unifiées et la convergence des services amènent des impératifs de plus en plus forts de haute disponibilité.

Cette haute disponibilité concerne, entre autres, la disponibilité des équipements eux-mêmes. Cisco a développé et rendu disponible un certain nombre d'innovations au service de la disponibilité de ces équipements permettant d'offrir une intelligence embarquée afin d'améliorer la détection d'événements et leur prise en charge par l'équipement.

Ce document a pour objectif d'introduire une de ces innovations majeures : Embedded Event Manager (EEM).

2. Présentation de EEM

Cisco IOS Embedded Event Manager (EEM) est une technologie puissante de gestion des équipements et des systèmes intégrés à la plate-forme logicielle Cisco IOS.

EEM permet aux administrateurs réseaux de développer et d'exécuter des scripts pour automatiser les tâches, réaliser des améliorations mineures et créer des solutions de rechange. Grâce à EEM, les événements sont étudiés du point de vue de l'équipement et les actions interviennent sans qu'il soit nécessaire de disposer d'une connectivité externe.

EEM de fait apporte de nombreux avantages dans l'administration et la gestion quotidienne du réseau en permettant d'automatiser un certain nombre de tâches et d'être plus réactif, l'équipement pouvant détecter lui-même une anomalie et remontant une alerte de façon autonome.

Afin d'illustrer ces avantages, voici quelques exemples d'utilisation de la technologie EEM :

- Sauvegarde automatique de la configuration sur un serveur FTP dès que la configuration de l'équipement est sauvegardée localement par un 'write memory'.
- Notification par le biais d'un message syslog de sévérité haute et/ou d'un email que la mémoire libre du système passe au dessous d'un seuil ou si le nombre de routes dans la table de routage atteint un seuil proche des limites du système, etc.
- Contrôler la modification des configurations à certaines heures de la journée, voire l'interdire complètement, par exemple, entre 8h et 18h.
- Augmentation de la sévérité du message syslog si un port critique tombe (par exemple le port permettant la connexion Internet de l'Entreprise, ou la connexion vers d'autres filiales)
- Notification email si une carte ou un module est retiré ou inséré.

- Activation de diagnostics locaux (par GOLD) et notification suite à l'apparition d'un événement.
- Automatiser la configuration : par exemple un téléphone est connecté sur un port d'accès, le switch le détecte et applique automatiquement la configuration adaptée sur ce port (segmentation voix/données sur différents vlan, application de la QoS...)
- Etc.

3. Architecture de EEM

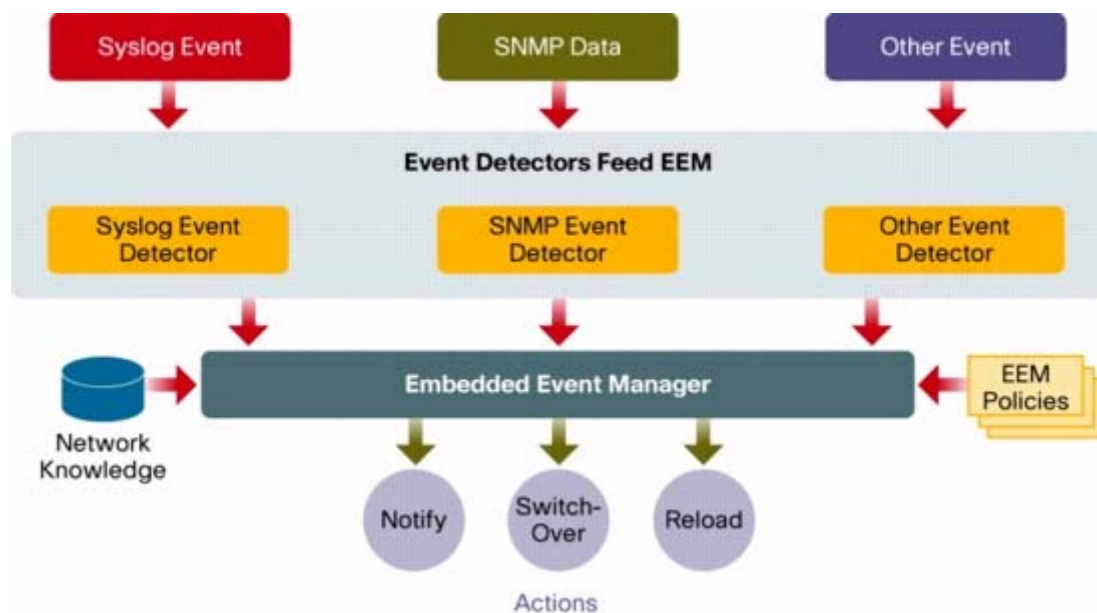
a. Vue générale

Afin de mieux comprendre l'étendue des possibilités, il est important de bien visualiser l'architecture d'EEM.

Cette architecture contient 3 composants :

- Event Detectors/Détecteurs. Un certain nombre de détecteurs sont disponibles permettant d'identifier le ou les événements qui déclencheront la prise en charge par EEM : événement syslog, information d'une MIB SNMP, envoi d'une commande CLI, etc.
- Policy Engines : création de politiques EEM qui seront appliquées après la phase de détection. Il existe deux méthodes de créations de politique EEM : CLI applet ou scripting.
- Actions à mener. La politique EEM définira pour chaque événement les actions à mener : envoi d'un email, syslog, basculement sur une carte/module de backup, redémarrage de l'équipement, commande CLI, etc.

L'architecture générale d'EEM est présentée sur la figure suivante :



Les politiques EEM créées peuvent aller du plus simple : un événement déclenche une action, ou augmenter en complexité : si un ou plusieurs événements sont détectés, vérification d'autres paramètres avant d'effectuer une ou plusieurs actions.

Des variables d'environnement pourront également être créées et utilisées dans les politiques EEM.

b. Les détecteurs

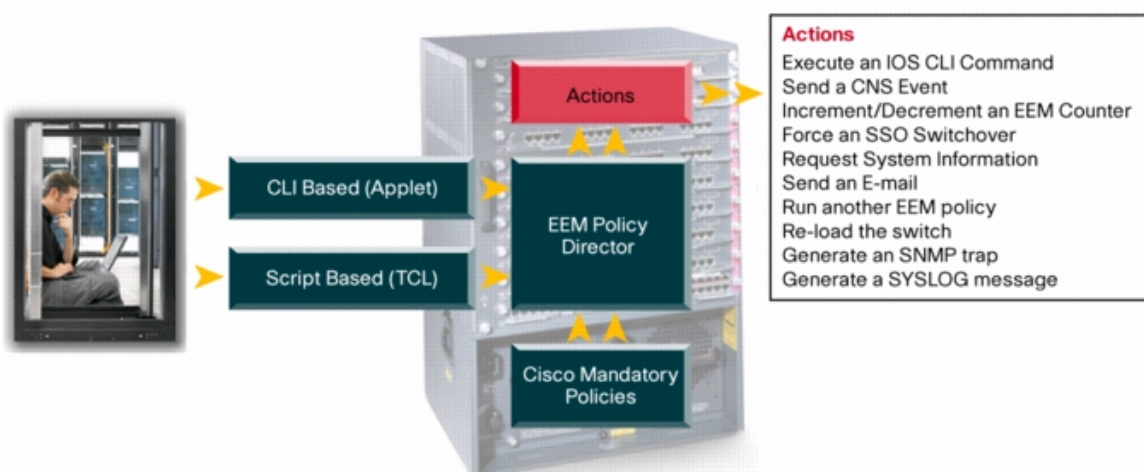
Plus d'une dizaine de détecteurs sont disponibles à ce jour, leur nombre augmentant régulièrement avec les évolutions logicielles des produits.

En voici quelques exemples :

IOS CLI Event Detector	Détection des commandes CLI par expressions régulières
IOS I/F Counter Event Detector	Détection de valeur des compteurs d'interface (dépassement ou passage sous un seuil)
IOS Ressource Threshold Event Detector	Détection de valeurs globales. Ex : utilisation CPU et espace buffer libre
IOS Timer Services Event Detector	Génère un évènement à une heure spécifique du jour ou après un décompte horaire
IOS Watchdog / System event Detector	Détection de conditions relative aux processus IOS ou aux sous-systèmes
Online Insertion and Removal Event Detector	Détection de l'insertion ou retrait d'une carte ou d'un module dans le châssis
Routing Event Detector	Détection d'évènement concernant les protocoles de routage
SNMP Event Detector	Génère un évènement lorsqu'une valeur SNMP atteint un seuil (en augmentation ou diminution)
Syslog Event Detector	Génère un évènement lorsqu'un message syslog correspond à une expression régulière

c. Policy Engines

La création des politiques EEM utilisant ces détecteurs peut se faire de deux façons : par une applet CLI ou un script TCL.



Applet CLI

Cette première méthode de création de politiques EEM permet de configurer l'ensemble des règles en utilisant des commandes CLI IOS.

L'exemple suivant permet de monitorer l'espace mémoire libre de l'équipement et si la valeur de la

MIB correspondante passe en dessous de 512000 octets, un message syslog de niveau « critical » est envoyé et un switchover est effectué.

```
event manager applet memory
  event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op lt entry-val
  512000 poll-interval 10
  action 1.0 syslog priority critical msg "Memory exhausted; current available
  memory is $_snmp_oid_val bytes"
  action 2.0 force-switchover
```

Cet autre permet d'envoyer un message syslog de niveau « emergencies » si l'interface Fast Ethernet 0/0 change d'état.

```
event manager applet fe0trans
  event syslog pattern .*UPDOWN.*FastEthernet0/0.*
  action 1.0 syslog priority emergencies msg "New syslog $_syslog_msg"
```

Les applets CLI n'offrent pas la possibilité de créer des politiques aussi avancées qu'en utilisant du scripting mais permettent simplement et rapidement de créer des politiques EEM sur un équipement.

Script TCL

La deuxième méthode de création de politiques est plus flexible car elle permet d'utiliser des scripts de type TCL. Il devient possible de tirer parti de l'ensemble des avantages du scripting (boucles conditionnelles, scripts hiérarchiques...).

Afin d'illustrer ce propos, voici un exemple de script utilisé pour sauvegarder la configuration de l'équipement dès la sortie de mode de configuration dès que la variable d'environnement «u_cfgSave_on » est positionnée à 1.

```
if $_u_cfgSave_on==1 {
  action_syslog msg "Config save mode set, saving configuration to nvram"
  if [catch {cli_open} result] {
    error $result $errorMsg
  } else {
    array set cli $result
  }
  if [catch {cli_exec $cli(fd) "enable"} result] {
    error $result $errorMsg
  }
  if [catch {cli_write $cli(fd) "copy run start"} result] {
    error $result $errorMsg
  }

  if [catch {cli_read_pattern $cli(fd) "Destination filename"} result] {
    error $result $errorMsg
  }
  if [catch {cli_write $cli(fd) "\n"} result] {
    error $result $errorMsg
  }
  if [catch {cli_read_drain $cli(fd)} result] {
```

```

    error $result $errorInfo
  } else {
    set cmd_output $result
    action_syslog msg "copy command reponse - $cmd_output"
  }
  if [catch {cli_close $cli(fd) $cli(tty_id)} result] {
    error $result $errorInfo
  }
} else {
  action_syslog msg "Config save mode not set, remember to save your
configuration to nvram"
}

```

Actions

En complément des actions démontrées dans les exemples de la section précédente, voici certaines actions pouvant être effectuées dans une politique EEM :

Executer une commande CLI	Envoyer une trap SNMP customisée
Générer un syslog	Envoyer un email ou un e-page
Appeler une autre politique EEM	Incrémenter ou décrémenter un compteur
Forcer un failover vers le superviseur de standby (Catalyst 6500)	Rebooter l'équipement
Appeler un script TCL	...

4. Conclusion

La technologie EEM est aujourd'hui disponible sur l'ensemble des plates-formes multiservices ISR et routeurs Cisco ainsi que sur le Catalyst 6500 et le Cisco 7600.

Cisco IOS Embedded Event Manager (EEM)

Pour de plus amples informations (Introduction, Q&A, Livre Blanc) sur Embedded Event Manager, visitez :

http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.html

Cisco IOS Tools for Commercial

Utilisation de plusieurs scripts EEM pour automatiser et diagnostiquer un réseau de petite ou moyenne taille.

Les informations générales :

http://www.cisco.com/en/US/products/ps9421/products_ios_protocol_group_home.html

Un très bon moyen de se familiariser avec EEM au travers d'exemples de scripts : les 20 scripts EEM utilisés avec à chaque fois une vidéo d'explications sur la manière de procéder :

http://www.cisco.com/en/US/products/ps9421/networking_solutions_products_generic_content0900aecd80719ee6.html

Communauté en ligne EEM

Une communauté en ligne de rédaction de scripts pour Cisco IOS Embedded Event Manager vient d'ouvrir appelée Cisco Beyond :

<http://cisco.com/go/ciscobeyond>

Cisco Beyond est une nouvelle communauté de rédaction de scripts avec un système Web convivial de partage de fichiers où clients, partenaires et autres utilisateurs peuvent télécharger et échanger des scripts EEM. Comme les autres communautés en ligne du même type, Cisco Beyond est destinée à tous les publics : les utilisateurs EEM débutants pourront bénéficier des exemples de pratiques optimales tandis que les plus expérimentés y trouveront de nouvelles astuces tout en faisant profiter les autres de leur propre savoir-faire.



Contactez-nous :

www.cisco.fr

0800 907 375

Siège social Mondial

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis

www.cisco.com

Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social France

Cisco Systems France
11 rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France

www.cisco.fr

Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis

www.cisco.com

Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912

www.cisco.com

Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante :

www.cisco.com/go/offices

Afrique du Sud • Allemagne • Arabie saoudite • Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • Colombie • Corée • Costa Rica • Croatie • Danemark • Dubaï, Emirats arabes unis • Ecosse • Espagne • Etats-Unis • Finlande • France Grèce • Hong Kong SAR Hongrie • Inde • Indonésie • Irlande • Israël • Italie • Japon • Luxembourg • Malaisie • Mexique • Nouvelle Zélande • Norvège • Pays-Bas • Pérou Philippines • Pologne • Portugal • Porto Rico • République tchèque • Roumanie • Royaume-Uni • République populaire de Chine • Russie Singapour • Slovaquie • Slovénie • Suède • Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Venezuela • Vietnam • Zimbabwe



Copyright © 2008 Cisco Systems, Inc. Tous droits réservés. CCSP, CCVP, le logo Cisco Square Bridge, Follow Me Browsing et StackWise sont des marques de Cisco Systems, Inc. ; Changing the Way We Work, Live, Play, and Learn, et iQuick Study sont des marques de service de Cisco Systems, Inc. ; et Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, le logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, le logo Cisco Systems, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, le logo iQ, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, le logo Networkers, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient et TransPath sont des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays.

Toutes les autres marques mentionnées dans ce document ou sur le site Web appartiennent à leurs propriétaires respectifs. L'emploi du mot partenaire

