Système de gestion de réseau : Livre blanc sur les pratiques recommandées

Contenu

Introduction

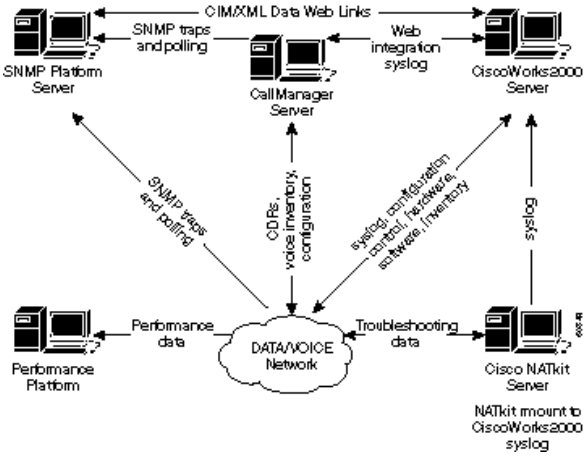
Le modèle de gestion de réseau de l'organisation internationale de normalisation (ISO) définit cinq zones fonctionnelles de gestion de réseau. Ce document couvre tous les domaines fonctionnels. Le but global de ce document est de fournir des recommandations pratiques concernant chaque domaine fonctionnel afin d'augmenter l'efficacité globale des outils de gestion et des pratiques en cours. Il fournit également des directives de conception pour la future mise en oeuvre des outils et technologies de gestion de réseau.

Gestion de réseau CSNA

Les domaines fonctionnels du model de Gestion de réseau OIN cinq sont répertoriés ci-dessous.

- Gestion de défaut — Détectez, isolez, informez, et corrigez les défauts produits dans le réseau.
- Gestion de la configuration — Aspects de configuration des périphériques de réseau tels que la Gestion de fichier de configuration, la gestion des stocks, et la gestion de logiciel.
- Gestion des performances — Moniteur et aspects des performances de mesure divers de sorte que la performance globale puisse être mise à jour à un taux acceptable.
- Gestion de la sécurité — Fournissez l'accès aux périphériques de réseau et les ressources de l'entreprise aux personnes autorisées.
- Gestion comptable — Les informations d'utilisation des ressources de réseau.

Le diagramme suivant affiche qu'une architecture de référence que Cisco Systems croit devrait être la solution minimale pour gérer un réseau de données. Cette architecture inclut un serveur Cisco CallManager pour ceux qui prévoient de gérer la Voix sur le Protocole Internet (VoIP) : Le diagramme affiche comment vous intègreriez le serveur CallManager dans la topologie NMS.



L'architecture de Gestion de réseau inclut ce qui suit :

- Plate-forme de Protocole SNMP (Simple Network Management Protocol) pour la Gestion de défaut
- Plate-forme de supervision des performances pour la Gestion des performances et tendre à long terme
- Serveur CiscoWorks2000 pour la gestion de la configuration, la collecte de Syslog, et la gestion des inventaires matériels et logiciels

Quelques Plateformes SNMP peuvent directement partager des données avec le serveur CiscoWorks2000 utilisant des méthodes communes de modèle de l'information/langage d'extensible markup (CIM/XML). La CIM est un modèle de données commun d'un schéma indépendant du type d'implémentation pour décrire les informations de Gestion globales dans un réseau/environnement d'entreprise. La CIM est composée d'une spécification et d'un schéma. La spécification définit les détails pour l'intégration avec d'autres modèles de gestion tels que le MIB SNMP ou les fichiers de bureau de l'information de Gestion de Task Force de Gestion (DMTF MIFs), alors que le schéma fournit les descriptions modèles réelles.

Le XML est un langage de balisage utilisé pour représenter des données structurées en forme textuelle. Un but spécifique de XML était de garder la majeure partie de l'alimentation descriptive du SGML tout en enlevant autant de la complexité comme possible. Le XML est semblable dans le concept au HTML, mais tandis que le HTML est utilisé pour donner les informations graphiques au sujet d'un document, le XML est utilisé pour représenter des données structurées dans un document.

Les clients des Services avancés de Cisco incluraient également le serveur de NATkit de Cisco pour la surveillance et le dépannage proactifs supplémentaires. Le serveur de NATkit aurait un accès de disque monté à distance (rmount) ou de Protocole FTP (File Transfer Protocol) aux données résidant sur le serveur CiscoWorks2000.

Le chapitre de fondements de Gestion de réseau de la *présentation générale de la technologie d'interconnexion de réseaux* fournit plus de vue d'ensemble détaillée concernant des fondements de Gestion de réseau.

Gestion de défaut

L'objectif de la gestion de pannes est de le détecter, se connecter, informent des utilisateurs de, et (dans la mesure du possible) réparez automatiquement les problèmes de réseau pour continuer le réseau s'exécuter efficacement. Puisque les défauts peuvent entraîner le temps d'arrêt ou la dégradation inacceptable de réseau, la Gestion de défaut est peut-être le plus largement mise en application des éléments de Gestion de réseau OIN.

Plateformes de Gestion de réseau

Une plate-forme de Gestion de réseau déployée à l'entreprise gère une infrastructure qui se compose des éléments de réseau multifournisseur. La plate-forme reçoit et les événements de processus des éléments de réseau dans le réseau. Des événements des serveurs et d'autres ressources essentielles peuvent également être expédiés à une plate-forme d'administration. Les fonctions généralement disponibles suivantes sont incluses dans une plate-forme d'administration standard :

- Détection de réseau
- Mappage de topologie des éléments de réseau
- Gestionnaire d'événement
- Collecteur et grapher de données de performance
- Navigateur de données de gestion

Des Plateformes de Gestion de réseau peuvent être visualisées comme console principale pour des exploitations réseau en détectant des défauts dans l'infrastructure. La capacité de détecter des problèmes rapidement dans n'importe quel réseau est essentielle. Le personnel d'exploitations réseau peut compter sur une carte graphique du réseau pour afficher les états opérationnels d'éléments de réseau essentiels tels que des Routeurs et des Commutateurs.

Les Plateformes de Gestion de réseau un tel HP OpenView, Computer Associates Unicenter, et Sun Solstice peuvent exécuter une détection des périphériques de réseau. Chaque périphérique de réseau est représenté par un élément graphique sur la console de la plate-forme d'administration. Les différentes couleurs sur les éléments graphiques représentent les états opérationnels de périphérique réseau en cours. Des périphériques de réseau peuvent être configurés pour envoyer des notifications, appelées les déroutements SNMP, aux Plateformes de Gestion de réseau. Lors de

recevoir les notifications, l'élément graphique représentant le périphérique de réseau change à un couleur différent selon la sévérité de la notification reçue. La notification, habituellement appelée un événement, est placée dans un fichier journal. Il est particulièrement important que les fichiers du Management Information Base de Cisco les plus en cours (MIB) soient chargés sur la plate-forme SNMP pour s'assurer que les diverses alertes des périphériques de Cisco sont interprétées correctement.

Cisco édite les fichiers MIB pour gérer de divers périphériques de réseau. Les fichiers MIB de Cisco se trouvent sur le site Web de cisco.com, et incluent les informations suivantes :

- Fichiers MIB édités dans le format SNMPv1
- Fichiers MIB édités dans le format SNMPv2
- Déroutements pris en charge SNMP sur des périphériques de Cisco
- OID pour des objets MIB SNMP de courant de Cisco

Un certain nombre de Plateformes de Gestion de réseau sont capables de gérer les sites géographiquement distribués de multiple. Ceci est accompli en permutant des données d'administration entre les consoles de gestion aux sites distants avec une station de Gestion au site principal. L'avantage principal d'une architecture distribuée est qu'il réduit le trafic d'administration, de ce fait, fournissant plus d'utilisation efficace de la bande passante. Une architecture distribuée permet également au personnel pour gérer localement leurs réseaux des sites distants avec des systèmes.

Une amélioration récente aux plates-formes d'administration est la capacité à distance aux éléments de réseau de gestion utilisant une interface web. Cette amélioration élimine le besoin du logiciel client spécifique sur des postes de travail individuel d'accéder à une plate-forme d'administration.

Une entreprise typique est composée de différents éléments de réseau. Cependant, chaque périphérique exige normalement des systèmes de gestion des éléments de constructeur-particularité afin de gérer efficacement les éléments de réseau. Par conséquent, les stations en double de Gestion peuvent voter des éléments de réseau pour les mêmes informations. Les données collectées par des autres systèmes sont enregistrées dans les bases de données distinctes, créant le temps système de gestion pour des utilisateurs. Cette limite a incité le réseau et les fournisseurs de logiciels à adopter des normes telles que l'architecture CORBA (CORBA) et la fabrication intégrée par ordinateur (CIM) pour faciliter l'échange des données d'administration entre les plates-formes d'administration et les systèmes de gestion des éléments. Avec des constructeurs adoptant des normes à l'étude le développement de système de gestion, les utilisateurs peuvent s'attendre l'Interopérabilité et à des économies de coûts en déployant et en gérant l'infrastructure.

CORBA spécifie un système qui fournit l'Interopérabilité entre les objets dans un hétérogène, l'environnement distribué et en quelque sorte qui est transparent au programmeur. Sa conception est basée sur le modèle objet du groupe de Gestion d'objet (OMG).

Dépannage de l'infrastructure

Le Protocole TFTP (Trivial File Transfer Protocol) et les serveurs de log système (Syslog) sont les composants cruciaux d'une infrastructure de dépannage en fonctionnement les exploitations réseau. Le serveur TFTP est utilisé principalement pour enregistrer des fichiers de configuration et des images logicielles pour des périphériques de réseau. Les Routeurs et les Commutateurs sont capables d'envoyer des messages du journal système à un serveur de Syslog. Les messages facilitent la fonction de dépannage quand des problèmes sont produits. De temps en temps, le personnel d'assistance technique de Cisco a besoin des messages de Syslog pour exécuter l'analyse de cause principale.

La fonction distribuée de collecte de Syslog d'essentiel de la gestion des ressources CiscoWorks2000 (essentiel) permet pour le déploiement des plusieurs des stations de collecte UNIX ou de NT aux sites distants pour exécuter la collecte des messages et le filtrage. Les filtres peuvent spécifier que des messages de Syslog seront expédié au serveur principal d'essentiel. Un avantage principal de mettre en application la collecte distribuée est la réduction de messages expédiés aux serveurs principaux de Syslog.

Détection des pannes et notification

L'objectif de la gestion de pannes est de détecter, isoler, informer, et corriger des défauts produits dans le réseau. Les périphériques de réseau sont capables d'alerter des stations de Gestion quand un défaut se produit sur les systèmes. Un système de gestion de pannes efficace se compose de plusieurs sous-systèmes. La détection des pannes fait quand les périphériques envoient des messages de déroutement SNMP, l'interrogation SNMP, des seuils de Surveillance à distance (RMON), et des messages de Syslog. Des alertes système d'une Gestion l'utilisateur final quand un défaut est signalé et des actions correctives peuvent être prises.

Des déroutements devraient être activés uniformément sur des périphériques de réseau. Des déroutements supplémentaires sont pris en charge avec de nouvelles versions logicielles de Cisco IOS pour des Routeurs et des Commutateurs. Il est important de vérifier et mettre le fichier de configuration à jour pour assurer décoder approprié des déroutements. Un examen périodique des déroutements configurés avec l'équipe de services réseau assurée par Cisco (RÉP.) assurera la détection des pannes efficace dans le réseau.

Le tableau suivant présente les déroutements CISCO-STACK-MIB par lesquels sont pris en charge, et peut être utilisé pour surveiller des conditions de panne en fonction, des Commutateurs de réseau local de Cisco Catalyst (RÉSEAU LOCAL).

Déroutement	Description
moduleUp	L'entité agent l'a détecté que l'objet de **moduleStatus** dans ce MIB transitioned **ok(2) à l'**état pour un de ses modules.
moduleDown	L'entité agent l'a détecté que l'objet de *moduleStatus* dans ce MIB transitioned hors **ok(2) de l'**état pour un de ses modules.

chassisAlarmOn	L'entité agent l'a détecté que le *chassisTempAlarm*, le *chassisMinorAlarm*, ou l'objet de *chassisMajorAlarm* dans ce MIB transitioned **on(2) à l'**état. *Un chassisMajorAlarm* indique qu'une des conditions suivantes existe : • Toute panne de tension • La température et panne de ventilation simultanées • Cent pour cent de panne de bloc d'alimentation (deux sur deux, ou une sur un) • Électriquement panne de l'EPROM (EEPROM) • Panne non-volatile de la RAM (NVRAM) • Panne de communication MCP • Inconnu d'état NMP Un chassisMinorAlarm indique qu'une des conditions suivantes existe : • Alarme de la température • Panne de ventilation • Panne partielle d'alimentation électrique (une sur deux) • Deux blocs d'alimentation de type incompatible
chassisAlarmOff	L'entité agent l'a détecté que le *chassisTempAlarm*, le *chassisMinorAlarm*, ou l'objet de *chassisMajorAlarm* dans ce MIB transitioned **off(1) à l'**état.

Des déroutements de superviseur d'environnement (envmon) sont définis dans le déroutement CISCO-ENVMON-MIB. Le déroutement d'envmon envoie des notifications de superviseur d'environnement de spécifique à l'entreprise de Cisco quand un seuil d'environnement est dépassé. Quand l'envmon est utilisé, un type environnemental spécifique de déroutement peut être activé, ou tous les types de déroutement du système de superviseur d'environnement peuvent être reçus. Si aucune option n'est spécifiée, tous les types environnementaux sont activés. Il peut être un ou plusieurs des valeurs suivantes :

- tension — Un ciscoEnvMonVoltageNotification est envoyé si la tension mesurée à un point test de mesure donné est en dehors de la plage normale pour le point test de mesure (comme est à l'étape d'avertissement, essentielle, ou d'arrêt).
- arrêt — Un ciscoEnvMonShutdownNotification est envoyé si le superviseur d'environnement le détecte qu'un point test de mesure atteint un état essentiel et est sur le point d'initier un arrêt.
- approvisionnement — Un ciscoEnvMonRedundantSupplyNotification est envoyé si le bloc d'alimentation redondant (où extant) échoue.
- thermoventilateur — Un ciscoEnvMonFanNotification est envoyé si des n'importe quels des thermoventilateurs dans la baie de thermoventilateur (où extant) échouent.
- la température — Un ciscoEnvMonTemperatureNotification est envoyé si la température mesurée à un point test de mesure indiqué est en dehors de la plage normale pour le point test de mesure (comme est à l'étape d'avertissement, essentielle, ou d'arrêt).

La détection des pannes et la surveillance des éléments de réseau peuvent être développées du niveau de périphérique au protocole et aux niveaux d'interface. Pour un environnement de réseau, la surveillance de défaut peut inclure le réseau local virtuel (VLAN), Mode de transfert asynchrone (ATM), des indications de défaut sur des interfaces physiques, et ainsi de suite. L'implémentation de la gestion de pannes au niveau protocole est disponible à l'aide d'un système de gestion des éléments tel que le Campus Manager CiscoWorks2000. L'application TrafficDirector dans le Campus Manager se concentre sur la gestion de la commutation utilisant le support de mini-RMON sur des Commutateurs de Catalyst.

Avec un nombre croissant d'éléments et de complexité des problèmes de réseau de réseau, un système de gestion d'événement qui est capable de corréler différents événements réseau (Syslog, déroutement, fichiers journal) peut être considéré. Cette architecture derrière un système de gestion d'événement est comparable à un gestionnaire de système de gestionnaires (MAMAN). Un système bien conçu de gestion d'événement permet au personnel dans le Network Operations Center (centre d'exploitation du réseau) pour être proactif et efficace en détectant et en diagnostiquant des problèmes de réseau. L'attribution des priorités d'événements et la suppression permettent au personnel chargé des opérations de réseau pour se concentrer sur des événements réseau essentiels, pour étudier plusieurs systèmes de gestion d'événement comprenant le Cisco Information Center, et pour réaliser une analyse de faisabilité pour explorer entièrement les capacités de tels systèmes. Pour obtenir plus d'informations, allez au Cisco Information Center.

Surveillance et notification de défaut anticipé

L'alarme et l'événement de RMON sont deux groupes définis dans la spécification de RMON. Normalement, une station de Gestion exécute l'interrogation sur des périphériques de réseau pour déterminer le statut ou la valeur de certaines variables. Par exemple, une station de Gestion vote un routeur pour découvrir l'utilisation de l'unité centrale (CPU) et pour générer un événement quand la valeur frappe des portées un seuil configuré. Cette méthode gaspille la bande passante de réseau et peut également manquer le seuil réel selon l'intervalle de sondage.

Avec l'alarme et les événements de RMON, un périphérique de réseau est configuré pour se surveiller pour la montée et les seuils de chute. À un intervalle de temps de prédéfinis, la volonté de périphérique de réseau prélève un échantillon d'une variable et le compare contre les seuils. Un déroutement SNMP peut être envoyé à une station de Gestion si la valeur réelle dépasse ou tombe au-dessous des seuils configurés. L'alarme et les groupes d'événements de RMON fournissent une méthode par anticipation de gérer les périphériques essentiels de réseau.

Cisco Systems recommande mettre en application l'alarme et l'événement de RMON sur les périphériques essentiels de réseau. Les variables

surveillées peuvent inclure l'utilisation du processeur, les défaillances de la mémoire tampon, les baisses d'entrée/sortie, ou toutes les variables des types d'entier. Commençant par le Logiciel Cisco IOS version 11.1(1), toutes les images de routeur prennent en charge l'alarme et les groupes d'événements de RMON.

Pour des informations détaillées sur l'alarme et l'implémentation d'événement de RMON, référez-vous à la section d'alarme et d'implémentation d'événement de RMON.

Contraintes de mémoire de RMON

L'utilisation mémoire de RMON est constante à travers toutes les plates-formes de commutation concernant les statistiques, les historiques, les alarmes, et les événements. Le RMON utilise ce qui s'appelle une *position* pour enregistrer des historiques et des statistiques sur l'agent RMON (qui est le commutateur dans ce cas). La taille de position est définie sur la sonde RMON (périphérique SwitchProbe) ou l'application RMON (outil de TrafficDirector), puis envoyée au commutateur à placer.

Approximativement 450 K de l'espace de code est nécessaire pour prendre en charge le mini-RMON (par exemple, quatre groupes RMON : statistiques, historique, alarmes, et événements). La configuration requise en mémoire dynamique pour le RMON varie parce qu'elle dépend de la configuration d'exécution.

Le tableau suivant définit les informations d'utilisation de la mémoire RMON à l'exécution pour chaque groupe de mini-RMON.

Définition de groupe RMON	L'espace de mémoire vive dynamique utilisé	Notes
Statistiques	140 octets par Ethernets commutés/port Fast Ethernet	Par port
Historique	3.6 K pour 50 positions *	Chaque position supplémentaire utilise 56 octets
Alarme et événement	2.6 K par alarme et ses entrées d'événement correspondantes	Par alarme par port

*RMON utilise ce qui s'appelle une *position* pour enregistrer des historiques et des statistiques sur l'agent RMON (tel qu'un commutateur).

Alarme et implémentation d'événement de RMON

En incorporant le RMON en tant qu'élément d'une solution de Gestion de défaut, un utilisateur peut surveillent proactivement le réseau avant qu'un problème potentiel se pose. Par exemple, si le nombre de paquets d'émission reçus augmente de manière significative, il peut entraîner une augmentation de l'utilisation du processeur. En mettant en application l'alarme et l'événement de RMON, un utilisateur peut installer un seuil pour surveiller le nombre de paquets d'émission reçus et pour alerter la plate-forme SNMP à l'aide d'un déroutement SNMP si le seuil configuré est atteint. Les alarmes et les événements de RMON éliminent le vote excessif normalement exécuté par la plate-forme SNMP pour accomplir le même but.

Deux méthodes sont fournies par ce que pour configurer le RMON alarment et événement :

- Interface de ligne de commande (CLI)
- SNMP SET

Les procédures suivantes d'échantillon affichent comment placer un seuil pour surveiller le nombre de paquets d'émission reçus sur une interface. Le même compteur est utilisé dans ces procédures comme est affiché dans l'exemple de commande d'interface d' **exposition** à la fin de cette section.

Exemple d'interface de ligne de commande

Pour implémenter l'alarme et l'événement de RMON utilisant l'interface CLI, exécutez les étapes suivantes :

1. Trouvez l'index d'interface associé avec des Ethernet 0 en marchant le MIB ifTable.

```
interfaces.ifTable.ifEntry.ifDescr.1 = "Ethernet0"
interfaces.ifTable.ifEntry.ifDescr.2 = "Ethernet1"
interfaces.ifTable.ifEntry.ifDescr.3 = "FastEthernet0"
interfaces.ifTable.ifEntry.ifDescr.4 = "Fddi0"
```

2. Obtenez l'OID associé avec le champ CLI à surveiller. Pour cet exemple, l'OID pour des « émissions » est 1.3.6.1.2.1.2.2.1.12. Cisco OID pour des variables MIB spécifiques sont fourni par le site Web cisco.com.

3. Déterminez les paramètres suivants pour installer des seuils et des événements.

    - augmentation et seuils de chute
    - échantillonnant le type (absolu ou delta)

- intervalle d'échantillonnage
- action quand le seuil est atteint

Afin de cet exemple, un seuil est installé pour surveiller le nombre de paquets d'émission reçus sur des Ethernet 0. Un déroutement sera généré si le nombre de paquets d'émission reçus est plus grand que 500 entre les 60-deuxièmes échantillons. Le seuil sera réactivé quand le nombre d'émissions d'entrée n'augmente pas entre les échantillons prélevés.

Remarque: Pour détaillé au sujet de ces paramètres de commande, vérifiez la documentation du Cisco Connection Online (CCO) pour des commandes d'alarme et d'événement de RMON pour votre version particulière de Cisco IOS.

4. Spécifiez le déroutement envoyé (événement de RMON) quand le seuil est atteint utilisant les commandes suivantes CLI (les commandes Cisco IOS sont affichées en gras) :

   High Broadcast de description de passerelle déroutée de l'événement 1 de rmon « sur le propriétaire Cisco des Ethernets 0"

   l'émission normale de description de log de l'événement 2 de rmon « a reçu sur le propriétaire Cisco des Ethernets 0"

5. Spécifiez les seuils et les paramètres appropriés (alarme de RMON) utilisant les commandes suivantes CLI :

   seuil montant 500 1 du delta ifEntry.12.1 60 de l'alarme 1 de rmon

   propriétaire 2 Cisco du seuil de chute 0

6. Employez le SNMP pour voter ces tables pour vérifier que les entrées eventTable ont été faites sur le périphérique.

```
rmon.event.eventTable.eventEntry.eventIndex.1 = 1

rmon.event.eventTable.eventEntry.eventIndex.2 = 2

rmon.event.eventTable.eventEntry.eventDescription.1 =
"High Broadcast on Ethernet 0"

rmon.event.eventTable.eventEntry.eventDescription.2 =
"normal broadcast received on ethernet 0"

rmon.event.eventTable.eventEntry.eventType.1 = snmp-trap(3)

rmon.event.eventTable.eventEntry.eventType.2 = log(2)

rmon.event.eventTable.eventEntry.eventCommunity.1 = "gateway"

rmon.event.eventTable.eventEntry.eventCommunity.2 = ""

rmon.event.eventTable.eventEntry.eventLastTimeSent.1 =
Timeticks: (0) 0:00:00

rmon.event.eventTable.eventEntry.eventLastTimeSent.2 =
Timeticks: (0) 0:00:00

rmon.event.eventTable.eventEntry.eventOwner.1 = "cisco"

rmon.event.eventTable.eventEntry.eventOwner.2 = "cisco"

rmon.event.eventTable.eventEntry.eventStatus.1 = valid(1)

rmon.event.eventTable.eventEntry.eventStatus.2 = valid(1)
```

7. Employez le SNMP pour voter ces tables pour vérifier que les entrées alarmTable ont été placées.

```
rmon.alarm.alarmTable.alarmEntry.alarmIndex.1 = 1

rmon.alarm.alarmTable.alarmEntry.alarmInterval.1 = 60

rmon.alarm.alarmTable.alarmEntry.alarmVariable.1 = OID:
interfaces.ifTable.ifEntry.ifInNUcastPkts.2

rmon.alarm.alarmTable.alarmEntry.alarmSampleType.1 = absoluteValue(1)

rmon.alarm.alarmTable.alarmEntry.alarmValue.1 = 170183

rmon.alarm.alarmTable.alarmEntry.alarmStartupAlarm.1 =
risingOrFallingAlarm(3)

rmon.alarm.alarmTable.alarmEntry.alarmRisingThreshold.1 = 500

rmon.alarm.alarmTable.alarmEntry.alarmFallingThreshold.1 = 0

rmon.alarm.alarmTable.alarmEntry.alarmRisingEventIndex.1 = 1
```

```
rmon.alarm.alarmTable.alarmEntry.alarmFallingEventIndex.1 = 2

rmon.alarm.alarmTable.alarmEntry.alarmOwner.1 = "cisco"

rmon.alarm.alarmTable.alarmEntry.alarmStatus.1 = valid(1)
```

Exemple de SNMP SET

Afin d'implémenter l'alarme et l'événement de RMON avec l'exécution de SNMP SET, terminez-vous ces étapes :

1. Spécifiez le déroutement envoyé (événement de RMON) quand le seuil est atteint utilisant les exécutions de SNMP SET suivantes :

```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.2.1
 octetstring "High Broadcast on Ethernet 0"
 eventDescription.1 : DISPLAY STRING- (ascii): High Broadcast on Ethernet 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.3.1
 integer 3 eventType.1 : INTEGER: SNMP-trap

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.4.1 octetstring "gateway"
 eventCommunity.1 : OCTET STRING- (ASCII): gateway

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.6.1
 octetstring "cisco" eventOwner.1 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.7.1 integer 1
 eventStatus.1 : INTEGER: valid
```

2. Spécifiez les seuils et les paramètres appropriés (alarme de RMON) utilisant les exécutions de SNMP SET suivantes :

```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.2.2
 octetstring "normal broadcast received on ethernet 0"
 eventDescription.2 : DISPLAY STRING- (ASCII): normal broadcast
 received on ethernet 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.3.2 integer 2
 eventType.2 : INTEGER: log

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.6.2 octetstring "cisco"
 eventOwner.2 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.7.2 integer 1
 eventStatus.2 : INTEGER: valid
```

3. Votez ces tables pour vérifier que les entrées eventTable ont été faites sur le périphérique.

```
% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.9.1

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.2.1 integer 60
 alarmInterval.1 : INTEGER: 60

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.3.1
objectidentifier .1.3.6.1.2.1.2.2.1.12.2
 alarmVariable.1 : OBJECT IDENTIFIER:
.iso.org.dod.internet.mgmt.mib2.interfaces.ifTable
 ifEntry.ifInNUcastPkts.2

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.4.1 integer 2

alarmSampleType.1 : INTEGER: deltaValue

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.7.1 integer 500
 alarmRisingThreshold.1 : INTEGER: 500

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.8.1 integer 0
 alarmFallingThreshold.1 : INTEGER: 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.9.1 integer 1
 alarmRisingEventIndex.1 : INTEGER: 1

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.10.1 integer 2
 alarmFallingEventIndex.1 : INTEGER: 2

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.11.1 octetstring
"cisco"
 alarmOwner.1 : OCTET STRING- (ASCII): cisco
```

```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.12.1 integer 1
 alarmStatus.1 : INTEGER: valid
```

4. Votez ces tables pour vérifier que les entrées alarmTable ont été placées.

```
% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.3.1
```

show interface

Cet exemple est un résultat de la **commande d'interface d'exposition**.

*Ethernets 0 d'***interface d'exposition de** gateway>

```
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0000.0c38.1669 (bia 0000.0c38.1669)
Description: NMS workstation LAN
Internet address is 172.16.97.132/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 27 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 1 packets/sec
21337627 packets input, 3263376846 bytes, 0 no buffer

Received 7731303 broadcasts
, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
17328035 packets output, 2824522759 bytes, 0 underruns
174 output errors, 44368 collisions, 4 interface resets
0 babbles, 0 late collision, 104772 deferred
174 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Gestion de la configuration

L'objectif de la gestion de la configuration est de surveiller le réseau et l'information de configuration système de sorte que les effets sur l'exploitation réseau de diverses versions des éléments de matériel et de logiciel puissent être dépistés et gérés.

Standards de configuration

Avec un nombre croissant de périphériques de réseau déployés, il est essentiel de pouvoir identifier exactement l'emplacement d'un périphérique de réseau. Cette information d'emplacement devrait fournir à une description détaillée signicative à ceux chargées acheminer des ressources quand un problème de réseau se pose. Pour accélérer une résolution si un problème de réseau se pose, assurez-vous pour avoir l'information de contact disponible de la personne ou du service chargé des périphériques. L'information de contact devrait inclure le numéro de téléphone et le nom de la personne ou du service.

Nommer des conventions pour des périphériques de réseau, à partir du nom du périphérique à l'interface individuelle, devrait être prévu et mis en application en tant qu'élément du standard de configuration. Une convention nommante bien définie procure au personnel de fournir des problèmes de réseau de pour le dépannage des informations précises. La convention nommante pour des périphériques peut utiliser la situation géographique, nom de construction, plancher, et ainsi de suite. Pour l'interface nommant la convention, il peut inclure le segment auquel un port est connecté, nom de hub se connectant, et ainsi de suite. Sur des interfaces série, il devrait inclure la bande passante réelle, le nombre de l'identifiant de connexion de liaison de données locale (DLCI) (si Relais de trames), la destination, et l'ID ou les informations de circuit fournies par le transporteur.

Gestion de fichier de configuration

Quand vous ajoutez de nouvelles commandes de configuration sur les besoins de périphériques réseau existants, vous devez vérifier les commandes pour l'intégrité avant que l'implémentation réelle ait lieu. Un périphérique incorrectement configuré de réseau peut exercer un effet désastreux sur la connexion réseau et la représentation. Des paramètres de commande de configuration doivent être vérifiés pour éviter des non-concordances ou des questions d'incompatibilité. Il est recommandé de programmer un examen complet des configurations avec des ingénieurs de Cisco de façon régulière.

A entièrement - les essentiel CiscoWorks2000 fonctionnels tient compte de sauvegarder des fichiers de configuration sur des Routeurs et des commutateurs Cisco Catalyst automatiquement. La fonctionnalité de sécurité des essentiel peut être utilisée pour exécuter l'authentification sur des modifications de configuration. Un journal d'audit de modification est disponible pour dépister des modifications et le nom d'utilisateur des

personnes émettant des modifications. Pour des modifications de configuration sur de plusieurs périphériques, deux options sont disponibles : le NetConfig basé sur le WEB dans la version en cours des essentiel CiscoWorks2000 ou du script de **cwconfig**. Des fichiers de configuration peuvent être téléchargés et téléchargés utilisant les essentiel CiscoWorks2000 utilisant les prédéfinis ou les modèles définis par l'utilisateur.

Ces fonctions peuvent être accomplies avec les outils de gestion de la configuration dans les essentiel CiscoWorks2000 :

- Poussez les fichiers de configuration des archives de configuration d'essentiel à un périphérique ou à des périphériques de multiple
- Tirez la configuration du périphérique aux archives d'essentiel
- Extrayez la configuration la plus récente des archives et écrivez-la à un fichier
- Importez la configuration à partir d'un fichier et poussez la configuration aux périphériques
- Comparez les deux dernières configurations dans les archives d'essentiel
- Supprimez les configurations plus anciennes qu'une date spécifiée ou une version des archives
- Copiez la configuration de démarrage sur la configuration en cours

Gestion des stocks

La fonction de détection de la plupart des Plateformes de Gestion de réseau est destinée pour fournir une liste dynamique des périphériques trouvés dans le réseau. Des engines de détection comme ceux mises en application dans des Plateformes de Gestion de réseau devraient être utilisées.

Une base de données d'inventaire fournit les informations de configuration détaillées sur des périphériques de réseau. Les informations communes incluent des modèles de matériel, des modules installés, des images logicielles, des niveaux de microcode, et ainsi de suite. Toutes ces informations sont cruciales en se terminant des tâches telles que la maintenance logicielle et matérielle. La liste à jour des périphériques de réseau collectés par le processus de découverte peut être utilisée comme liste principale pour collecter des informations d'inventaire utilisant le SNMP ou le script. Une liste de périphériques peut être importée du Campus Manager CiscoWorks2000 dans la base de données d'inventaire des essentiel CiscoWorks2000 pour obtenir un inventaire à jour des commutateurs Cisco Catalyst.

Gestion de logiciel

Une mise à jour réussie des images de Cisco IOS sur des périphériques de réseau exige une analyse détaillée des conditions requises telles que la mémoire, ROM de démarrage, niveau de microcode, et ainsi de suite. Les conditions requises sont normalement documentées et disponibles sur le site Web de Cisco sous forme de notes de mise à jour et de guides d'installation. Le processus d'améliorer le Cisco IOS courant d'un périphérique de réseau inclut télécharger une image correcte de CCO, sauvegardant l'image en cours, la vérification de toutes les configurations matérielles requises sont rencontrés, et puis le chargement de la nouvelle image dans le périphérique.

La fenêtre de mise à jour pour se terminer la maintenance de périphérique est assez limitée pour quelques organismes. Dans un environnement de grand réseau avec des ressources limitées, il pourrait être nécessaire de programmer et automatiser des mises à niveau de logiciel après des heures de travail. La procédure peut être terminée utilisant le langage de script comme prévoient ou une application écrite spécifiquement pour effectuer une telle tâche.

Des changements au logiciel des périphériques de réseau tels que des images et des versions de microcode de Cisco IOS devraient être dépistés pour aider à la phase d'analyse où une autre maintenance logicielle est exigée. Avec un rapport de historique des modifications facilement disponible, la personne exécutant la mise à jour peut réduire le risque de charger des images incompatibles ou le microcode dans des périphériques de réseau.

Gestion des performances

Accord de niveau de service

Un accord de niveau de service (SLA) est un contrat écrit entre un fournisseur de services et leurs clients au niveau de performance prévu des services réseau. SLA se compose des mesures convenues entre le fournisseur et ses clients. La valeur définie pour les mesures doit être réaliste, signicative, et mesurable pour les deux interlocuteurs.

La diverse statistique d'interface peut être collectée des périphériques de réseau pour mesurer le niveau de performance. Ces des statistiques peuvent être incluses comme mesures à SLA. Les statistiques telles que des pertes de file d'attente d'entrée, les pertes de file d'attente de sortie, et les paquets ignorés sont utiles pour diagnostiquer des problèmes relatifs aux performances.

Au niveau de périphérique, les métriques de performances peuvent inclure l'utilisation du processeur, l'allocation de mémoire tampon (grands mémoire tampon, tampon moyen, coups manqués, rapport de hit), et l'allocation de mémoire. La représentation de certains protocoles réseau est directement liée à la disponibilité de la mémoire tampon dans des périphériques de réseau. Les statistiques niveau du périphérique de mesure de représentation sont essentielles en optimisant les performances du protocole de haut niveau.

Les périphériques de réseau tels que des Routeurs prennent en charge de divers protocoles de couche plus élevée tels que le groupe de travail de Data-Link Switching (DLSW), artère distante de source pont (RSRB), AppleTalk, et ainsi de suite. Des statistiques de représentation des Technologies de réseau d'étendu (WAN) comprenant le Relais de trames, l'atmosphère, l'Integrated Services Digital Network (le RNIS), et d'autres peuvent être surveillées et collectées.

Supervision des performances, mesure, et enregistrement

Différentes métriques de performances à l'interface, au périphérique, et aux niveaux de protocole devraient être collectées de façon régulière utilisant le SNMP. Le moteur de sondage dans un système d'administration de réseaux peut être utilisé pour la collecte des informations. La plupart des systèmes d'administration de réseaux sont capables de collecter, d'enregistrer, et de présenter des données du sondage.

Les diverses solutions sont disponibles dans le marché pour satisfaire les besoins de la Gestion des performances des environnements d'entreprise. Ces systèmes sont capables de collecter, d'enregistrer, et de présenter des données des périphériques et des serveurs de réseau. L'interface basée sur le WEB sur la plupart des Produits rend les données de performance accessibles à partir n'importe où dedans de l'entreprise. Certaines des solutions généralement déployées de Gestion des performances incluent :

- InfoVista VistaView
- Vision de service IT SAS
- Trinagy TREND

Une évaluation des Produits ci-dessus déterminera s'ils répondent aux exigences de différents utilisateurs. Quelques constructeurs prennent en charge l'intégration avec des Plateformes de Gestion de réseau et de gestion du système. Par exemple, InfoVista prend en charge l'agent de patrouille BMC pour fournir des statistiques de performances de clé des serveurs d'applications. Chaque produit a un modèle différent et des capacités de tarification avec l'offre de base. Le soutien des caractéristiques de Gestion des performances pour les périphériques de Cisco tels que le NetFlow, le RMON, et le Service Assurance Agent (SAA) de Cisco IOS/journaliste de temps de réponse (RTR/SAA CSAA/RTR) est disponible sur quelques solutions. L'accord a récemment ajouté le soutien des Commutateurs BLÊMES de Cisco qui peuvent être utilisés pour collecter et visualiser des données de performance.

La caractéristique de rapporteur horaire du Logiciel Service Assurance Agent (SAA) /Response CSAA/RTR (RTR) dans le Cisco IOS peut être utilisée pour mesurer le temps de réponse entre les périphériques IP. Un routeur de source configuré avec CSAA configuré est capable de mesurer le temps de réponse à un périphérique IP de destination qui peut être un routeur ou un périphérique IP. Le temps de réponse peut être mesuré entre la source et la destination ou chaque saut le long du chemin. Des déroutements SNMP peuvent être configurés pour alerter des consoles de gestion si le temps de réponse dépasse les seuils de prédéfinis.

Les améliorations récentes au Cisco IOS étend les capacités de CSAA pour mesurer ce qui suit :

- Représentation de service de Protocole HTTP (Hypertext Transfer Protocol)
    - Consultation de Système de noms de domaine (DNS)
    - Le Protocole TCP (Transmission Control Protocol) se connectent
    - Temps de transaction de HTTP
- Écart de délai interpaquets (jitter) du trafic de la voix sur ip (VoIP)
- Le temps de réponse entre l'extrémité se dirige pour un Qualité de service (QoS) spécifique
    - Bits de type de service IP (tos)
- Perte de paquets utilisant les paquets générés par CSAA

Configurer la caractéristique CSAA sur des Routeurs peut faire utilisant l'application de l'Internetwork Performance Monitor de Cisco (IPM). Le CSAA/RTR est encastré dans beaucoup mais non tous les ensembles de caractéristiques du logiciel de Cisco IOS. Une release de la version logicielle de Cisco IOS qui prend en charge CSAA/RTR doit être installée sur le périphérique que l'IPM l'utilise pour recueillir des statistiques de représentation. Pour un résumé des versions de Cisco IOS qui prennent en charge CSAA/RTR/IPM, référez-vous au site Web de forums aux questions IPM.

Les informations complémentaires concernant l'IPM incluent :

- Aperçu d'IPM
- Service Assurance Agent (SAA)

Évaluation de performances et accord

Le trafic d'utilisateur a augmenté sensiblement et a placé un plus très demandé sur des ressources de réseau. Les gestionnaires de réseau ont typiquement un point de vue limité sur les types de trafic s'exécutant dans le réseau. Le profilage d'utilisateur et de trafic de l'application fournit une vue détaillée du trafic dans le réseau. Deux Technologies, des sondes RMON et NetFlow, fournissent la capacité de collecter des profils du trafic.

RMON

Les normes de RMON sont conçues pour être déployées en architecture distribuée où les agents (ou encastré ou dans des sondes autonomes) communiquent avec une station centrale (la console de gestion) par l'intermédiaire du SNMP. La norme de RMON RFC 1757 organise des fonctions de surveillance en neuf groupes pour prendre en charge des topologies d'Ethernets, et ajoute un dixième groupe dans RFC 1513 pour de Sonnerie-seuls paramètres symboliques. La surveillance de lien de Fast Ethernet est fournie dans le cadre de la norme RFC 1757, et la surveillance de sonnerie du Fiber Distributed Data Interface (FDDI) est fournie dans le cadre de RFC 1757 et de RFC 1513.

Les normes naissantes de télésurveillance d'entraînements de spécification de RMON RFC 2021 au delà du Contrôle d'accès au support (MAC) posent au réseau et aux couches application. Cette installation permet à des administrateurs d'analyser et dépanner des applications réseau telles que le trafic web, NetWare, les notes, le courrier électronique, l'accès aux bases de données, le Systèmes de fichiers en réseau (NFS), et d'autres. Des alarmes de RMON, les statistiques, l'historique, et les groupes d'hôte/conversation peuvent maintenant être utilisés proactivement surveillent

et mettent à jour la Disponibilité de réseau basée sur le trafic-le d'application-couche la plupart de trafic critique dans le réseau. RMON2 permet à des administrateurs réseau de continuer leur déploiement d'une solution de supervision standard pour prendre en charge des applications critiques et basées sur un serveur.

Les tableaux suivants présentent les fonctions des groupes RMON.

Groupe RMON (RFC 1757)	Fonction
Statistiques	Compteurs pour des paquets, des octets, des émissions, des erreurs, et des offres sur le segment ou le port.
Historique	Périodiquement échantillonne et enregistre des compteurs de groupe de statistiques pour la récupération postérieure.
Hôtes	Met à jour des statistiques sur chaque périphérique hôte sur le segment ou le port.
Hôte N supérieur	Un rapport du sous-ensemble défini par l'utilisateur des hôtes groupent, trié par un compteur statistique. En renvoyant seulement les résultats, le trafic d'administration est réduit.
Table de trafic	Met à jour des statistiques de conversation entre les hôtes sur le réseau.
Alarmes	Un seuil qui peut être placé sur des variables RMON essentielles pour l'administration proactive.
Événements	Génère des déroutements et des entrées de journal SNMP quand un seuil de groupe d'alarmes est dépassé.
Capture de paquet	Gère des mémoires tampons pour des paquets capturés par le groupe Filtres pour télécharger à la console de gestion.
Token Ring	Station de sonnerie — statistiques détaillées sur l'ordre des stations individuel de sonnerie de stations — un liste de stations dans un certain ordre actuellement sur la configuration de station de sonnerie de sonnerie — configuration et mise en place/suppression par routage de source de station — statistiques sur le routage de source, tel que des comptes de saut, et d'autres

RMON2	Fonction
Répertoire de Protocol	Protocoles pour lesquels l'agent surveille et met à jour des statistiques.
Distribution de Protocol	Statistiques pour chaque protocole.
Network Layer Host	Statistiques pour chaque adresse de couche réseau sur le segment, l'anneau, ou le port.
Tableau des couches réseau	Statistiques de trafic pour des paires d'adresses de couche réseau.
Hôte de la couche applicative	Statistiques par protocole de la couche applicative pour chaque adresse réseau.
Tableau de la couche applicative	Statistiques de trafic par protocole de la couche applicative pour des paires d'adresses de couche réseau.
Historique personnalisable par l'utilisateur	Étend l'historique au delà des statistiques de la couche de liaison RMON1 pour inclure n'importe quelles statistiques de RMON, RMON2, MIB-I, ou MIB-II.
Reproduction d'adresses	liaisons d'adresse de couche de MAC-à-réseau.
Groupe de configuration	Capacités et configurations d'agent.

NetFlow

La fonctionnalité NetFlow de Cisco permet des écoulements de statistiques détaillées du trafic à collecter pour la planification de capacité, la facturation, et les fonctions de dépannage. Le NetFlow peut être configuré sur des interfaces individuelles, fournissant des informations sur le trafic traversant ces interfaces. Les types suivants d'informations font partie des statistiques de trafic détaillées :

- Adresses IP de source et de destination
- Nombres d'interface d'entrée et sortie
- Port et destinations port de source TCP/UDP
- Nombre d'octets et de paquets dans l'écoulement
- Nombres de système autonome d'origine et de destination
- Type de service IP (tos)

Des données de NetFlow recueillies sur des périphériques de réseau sont exportées à un ordinateur de collecteur. Le collecteur remplit des fonctions telles que réduire le volume de données (filtrage et agrégation), de stockage de données hiérarchique, et de gestion du système de fichiers. Cisco fournit des applications de collecteur de NetFlow et d'analyseur de NetFlow pour recueillir et analyser des données des Routeurs et des commutateurs Cisco Catalyst. Il y a également des outils de shareware tels que le cflowd qui peut collecter des enregistrements de Protocole UDP (User Datagram Protocol) de NetFlow de Cisco.

Des données de NetFlow sont transportées utilisant des paquets UDP dans trois formats différents :

- Version 1 — Le format d'origine pris en charge dans le NetFlow initial libère.
- Version 5 — Une amélioration postérieure qui a ajouté des numéros de séquence de l'information et d'écoulement d'Autonomous System de Protocole BGP (Border Gateway Protocol).
- Version 7 — Une amélioration encore postérieure qui a ajouté le soutien de Commutation Netflow du Commutateurs de la gamme Cisco Catalyst 5000 a équipé d'un NetFlow Feature Card (NFFC).

Des versions 2 à 4 et la version 6 n'ont pas été libérées ou ne sont pas prises en charge par FlowCollector. Dans chacune des trois versions, le datagramme se compose d'une en-tête et d'un ou plusieurs flows record.

Le pour en savoir plus, se rapportent au livre blanc de guide de solutions de services Netflow.

Le tableau suivant trace les grandes lignes des versions prises en charge de Cisco IOS pour recueillir des données de NetFlow des Routeurs et des Commutateurs de Catalyst.

Version du logiciel Cisco IOS	Plate-forme matérielle Cisco prise en charge	Versions exportées par NetFlow prises en charge
11.1 CA et 11.1 cc	Cisco 7200, 7500, et RSP7000	V1 et V5
11.2 et 11.2 P	Cisco 7200, 7500, et RSP7000	V1
11.2 P	Module de route switch de Cisco (RSM)	V1
11.3 et 11.3 T	Cisco 7200, 7500, et RSP7000	V1
12.0	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, et RSM	V1 et V5
12.0 T	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX 8800 RPM, et BPX	V1 et V5

	8600	
12.0(3)T et plus tard	Cisco 1600*, 1720, 2500**, 2600, 3600, 4500, 4700, AS5300*, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX8800 RPM, et BPX 8650	V1, V5, et V8
12.0(6)S	Cisco 12000	V1, V5, et V8
	Cisco Catalyst 5000 avec le NetFlow Feature Card *** (NFFC)	V7

* Le soutien de l'exportation de NetFlow V1, V5, et V8 sur des Plateformes de Cisco 1600 et 2500 est visé pour la version du logiciel Cisco IOS 12.0(T). Le soutien de NetFlow de ces Plateformes n'est pas disponible dans la version principale du Cisco IOS 12.0.

** Le soutien du NetFlow V1, V5, et V8 sur la plate-forme AS5300 est visé pour la version du logiciel Cisco IOS 12.06(T).

Le *** MLS et exportation des données de NetFlow est pris en charge dans la version du logiciel de Supervisor Engine de gamme Catalyst 5000 4.1(1) ou plus tard.

Gestion de la sécurité

L'objectif de la gestion de la sécurité est de contrôler l'accès aux ressources de réseau selon les instructions locales de sorte que le réseau ne puisse pas être saboté (intentionnellement ou involontairement). Un sous-système de la gestion de sécurité, par exemple, peut surveiller des utilisateurs ouvrant une session à une ressource de réseau, refusant l'accès à ceux qui écrivent des codes d'accès inapproprié. La Gestion de la sécurité est très un vaste sujet ; donc cette zone du document couvre seulement la Sécurité par rapport au SNMP et au sécurité de base en matière d'accès aux périphériques.

Les informations détaillées sur la sécurité avancée incluent :

- Sécurité croissante sur des réseaux IP
- OpenSystems

Bons débuts d'une mise en œuvre de la gestion de sécurité avec des stratégies de sécurité et des procédures saines en place. Il est important de créer un norme de configuration minimale spécifique à la plate-forme pour tous les Routeurs et Commutateurs qui suivent des meilleures pratiques du secteur pour la Sécurité et la représentation.

Il y a de diverses méthodes de contrôler l'accès sur des Routeurs de Cisco et des Commutateurs de Catalyst. Certaines de ces méthodes incluent :

- Listes de contrôle d'accès (ACL)
- User-id et mots de passe locaux au périphérique
- Système de contrôle d'accès de Terminal Access Controller (TACACS)

TACACS est un protocole de Sécurité standard de l'Internet Engineering Task Force (RFC 1492) qui fonctionne entre les périphériques de client sur un réseau et contre un serveur TACACS. TACACS est un mécanisme d'authentification qui est utilisé pour authentifier l'identité d'un Accès à distance recherchant de périphérique à une base de données privilégiée. Les variations de TACACS incluent TACACS+, l'architecture AAA qui sépare l'authentification, l'autorisation, et les fonctions de traçabilité.

TACACS+ est utilisé par Cisco pour permettre un contrôle plus précis au-dessus de qui peut accéder au périphérique de Cisco en mode non-privilégié et privilégié. De plusieurs serveurs TACACS+ peuvent être configurés pour la tolérance aux pannes. Le TACACS+ étant activé, le routeur et le commutateur incite l'utilisateur pour un nom d'utilisateur et un mot de passe. L'authentification peut être configurée pour le contrôle d'ouverture de connexion ou authentifier des commandes individuelles.

Authentification

L'authentification est le processus d'identifier des utilisateurs, y compris le dialogue de procédure de connexion et de mot de passe, le défi et la réponse, et la prise en charge de messagerie. L'authentification est la manière qu'à un utilisateur est identifié avant d'être permis l'accès au routeur ou au commutateur. Il y a un rapport fondamental entre l'authentification et l'autorisation. Plus d'autorisation favorise un utilisateur reçoit, plus l'authentification devrait être forte.

Autorisation

L'autorisation fournit le contrôle de l'accès à distance, y compris l'autorisation une fois et l'autorisation pour chaque service qui est demandé par l'utilisateur. Sur un routeur de Cisco, la plage de niveau d'autorisation pour des utilisateurs est de 0 à 15 avec 0 étant la plus inférieure et 15 le plus élevé.

Comptabilité

La comptabilité tient compte de collecter et d'envoyer des informations relatives à la sécurité utilisé pour afficher, auditer, et signaler, tel que des identités de l'utilisateur, des temps de début et d'arrêt, et des commandes exécutées. La comptabilité permet à des gestionnaires de réseau de dépister les services que les utilisateurs accèdent à aussi bien que le montant de ressources de réseau qu'ils consomment.

Le tableau suivant présente des commandes d'échantillon de base pour l'usage de TACACS+, d'authentification, d'autorisation, et de la comptabilité sur un routeur de Cisco et un commutateur de Catalyst. Référez-vous au document d'authentification, d'autorisation, et de commandes de traçabilité pour des commandes plus en profondeur.

Commande Cisco IOS	But
Routeur	
aaa new-model	Activez l'authentification, autorisation, expliquant (AAA) comme méthode primaire le contrôle d'accès.
Aaa accounting {*système* | *réseau* | *connexion* | *exécutif* | *niveau commande***} {***arythmique* | *attente-commencement* | *arrêt arrêt***} {***tacacs+* | *rayon***}**	Comptabilité d'enable avec les commandes de configuration globale.
Aaa authentication login default tacacs+	Installez le routeur de sorte que des connexions à n'importe quelle ligne de terminal configurée avec le paramètre de connexion par défaut soient authentifiées avec TACACS+, et échouerez si l'authentification échoue pour une raison quelconque.
Exec default tacacs+ d'autorisation d'AAA aucun	Installez le routeur pour vérifier si on permet à l'l'utilisateur pour exécuter un shell d'EXÉCUTIF en demandant au serveur TACACS+.
IP address de serveur des **tacacs-server host** *tacacs+*	Spécifiez le serveur TACACS+ qui sera utilisé pour l'authentification avec les commandes de configuration globale.
partager-secret de **tacacs-server key**	Spécifiez le secret partagé qui est connu par les serveurs TACACS+ et le routeur de Cisco avec la commande de configuration globale.
Catalyst Switch	
enable de tacacs de set authentication login [*tout* | *console* | *HTTP* | *telnet***] [** *primaire***]**	Authentification de l'enable TACACS+ pour le mode d'ouverture de connexion normal. Employez la console ou les mots clé de telnet pour activer TACACS+ seulement pour des tentatives de port de console ou de connexion de telnet.
*option de repli d'***enable de set authorization exec {***option}***} [** *console* | *telnet* | *chacun des deux***]**	Autorisation d'enable pour le mode d'ouverture de connexion normal. Employez la console ou les mots clé de telnet pour activer l'autorisation seulement pour des tentatives de port de console ou de connexion de telnet.
Partager-secret **principal de set tacacs server**	Spécifiez le secret partagé qui est connu par les serveurs et le commutateur TACACS+.
	Spécifiez le serveur TACACS+ qui sera utilisé

*IP address de serveur de l'***hôte** *tacacs+ de* **set tacacs server**	pour l'authentification avec les commandes de configuration globale.
Enable de set accounting commands {*config* **|** *tous***}** *tacacs* **{***arrêt arrêt***} +**	Comptabilité d'enable des commandes de configuration.

Pour plus d'informations sur la façon configurer l'AAA pour surveiller et contrôler l'accès à l'interface de ligne de commande sur les Commutateurs de RÉSEAU LOCAL d'entreprise de Catalyst, référez-vous à Access de contrôle au commutateur utilisant le document comptable d'authentification, d'autorisation, et.

Sécurité SNMP

Le protocole SNMP peut être utilisé pour apporter des modifications de configuration sur des Routeurs et des Commutateurs de Catalyst semblables à ceux émis du CLI. Des mesures de sécurité appropriées devraient être configurées sur des périphériques de réseau pour empêcher l'accès non autorisé et pour changer par l'intermédiaire du SNMP. Les chaînes de la Communauté devraient suivre les instructions standard de mot de passe pour la longueur, les caractères, et la difficulté de deviner. Il est important de changer les chaînes de la communauté de leurs valeurs par défaut publiques et privées.

On devrait avoir une adresse IP statique et explicitement accorder tous les hôtes de gestion SNMP des juste de transmission SNMP avec le périphérique de réseau par ces prédéfinis par l'adresse IP et la liste de contrôle d'accès (ACL). Le Cisco IOS et le logiciel Cisco Catalyst fournit les fonctionnalités de sécurité qui s'assurent que seulement des stations autorisées de Gestion sont permises pour exécuter des modifications sur des périphériques de réseau.

Fonctionnalités de sécurité du routeur

Niveau de privilège SNMP

Cette caractéristique limite les types d'exécutions qu'une station de Gestion peut avoir sur un routeur. Il y a deux types de niveau de privilège sur des Routeurs : En lecture seule (RO) et lecture/écriture (le RW). Le niveau RO permet seulement à une station de Gestion pour questionner les données du routeur. Il ne tient pas compte des commandes de configuration telles que redémarrer un routeur et arrêter des interfaces à exécuter. Seulement le niveau de privilège du RW peut être utilisé pour exécuter de telles exécutions.

Liste de contrôle d'accès SNMP (ACL)

La fonctionnalité d'ACL SNMP peut être utilisée en même temps que la caractéristique de privilège SNMP pour limiter les stations spécifiques de Gestion de demander les informations de Gestion des Routeurs.

Vue SNMP

Cette caractéristique limite les informations spécifiques qui peuvent être récupérées des Routeurs par des stations de Gestion. Il peut être utilisé avec le niveau et les fonctionnalités d'ACL de privilège SNMP pour imposer l'accès restreint aux données par des consoles de gestion. Pour des exemples de configuration de vue SNMP, allez au snmp-server view.

SNMP Version 3

Le SNMP version 3 (SNMPv3) fournit des échanges sécurisés des données d'administration entre les périphériques de réseau et les stations de Gestion. Le cryptage et les fonctions d'authentification dans SNMPv3 assurent la sécurité élevée en transportant des paquets à une console de gestion. SNMPv3 est pris en charge dans le Logiciel Cisco IOS version 12.0(3)T et plus tard. Pour un aperçu technique de SNMPv3, allez à la documentation SNMPv3.

Liste de contrôle d'accès (ACL) sur des interfaces

La fonctionnalité d'ACL fournit des mesures de sécurité en empêchant des attaques telles que l'usurpation d'adresse IP. L'ACL peut être appliqué sur des interfaces en entrée ou en sortie sur des Routeurs.

Caractéristique de sécurité du commutateur de RÉSEAU LOCAL de Catalyst

Liste d'autorisation IP

La caractéristique de liste d'autorisation IP limite le telnet d'arrivée et l'accès SNMP au commutateur des adresses IP non autorisées de source. Des messages de Syslog et les déroutements SNMP sont pris en charge pour informer un système de gestion quand une violation ou un accès non autorisé se produit.

Une combinaison des fonctionnalités de sécurité de Cisco IOS peut être utilisée pour gérer des Routeurs et des Commutateurs de Catalyst. Une stratégie de sécurité doit être établie qui limite le nombre de stations de Gestion capables d'accéder aux Commutateurs et les Routeurs.

Pour plus d'informations sur la façon augmenter la Sécurité sur des réseaux IP, allez à la Sécurité croissante sur des réseaux IP.

Gestion comptable

La gestion comptable est le processus utilisé pour mesurer des paramètres d'utilisation du réseau de sorte que des utilisateurs individuels ou en groupe sur le réseau puissent être réglés convenablement aux fins de la comptabilité ou du chargeback. Semblable à la Gestion des performances, la première étape vers la gestion comptable appropriée est de mesurer l'utilisation des ressources de réseau de la plus haute importance. L'utilisation des ressources réseau peut être mesurée utilisant le NetFlow de Cisco et les caractéristiques d'ip accounting de Cisco. L'analyse des données recueillies par ces méthodes fournit la vue dans les structures d'utilisation en cours.

Un système basé sur l'utilisation de comptabilité et de facturation est une partie essentielle de n'importe quel accord de niveau de service (SLA). Il fournit une méthode pratique de définir des obligations sous SLA et conséquences claires pour le comportement en dehors des termes de SLA.

Les données peuvent être collectées par l'intermédiaire des sondes ou du NetFlow de Cisco. Cisco fournit des applications de collecteur de NetFlow et d'analyseur de NetFlow pour recueillir et analyser des données des Routeurs et des Commutateurs de Catalyst. Des applications de shareware telles que le cflowd sont également utilisées pour recueillir des données de NetFlow. Une mesure actuelle d'utilisation de ressource peut rapporter les informations de facturation, aussi bien que les informations évaluent les ressources équitables et optimales continues. Quelques solutions généralement déployées de gestion comptable incluent :

- Logiciel évident

Lancement de NetFlow et stratégie de collecte des informations

Le NetFlow (flux de réseau) est une technologie de mesure côté entrée qui tient compte de capturer les données exigées pour la planification du réseau, la surveillance, et les applications de traçabilité. Le NetFlow devrait être déployé sur des interfaces de périphérie/routeur d'agrégation pour des fournisseurs de services ou des interfaces de routeur d'accès WAN pour des clients de l'entreprise.

Cisco Systems recommande un déploiement soigneusement prévu de NetFlow avec des services Netflow lancé sur ces derniers les Routeurs stratégiquement localisés. Le NetFlow peut être déployé incrémentalement (interface par l'interface) et stratégiquement (sur les Routeurs bien choisis), plutôt que déployant le NetFlow sur chaque routeur sur le réseau. Le personnel de Cisco travaillera avec des clients pour déterminer sur quels Routeurs et interfaces principaux de clé que le NetFlow devrait être lancé a basées sur les modèles, la topologie du réseau, et l'architecture de la circulation du client.

Les principales considérations de déploiement incluent :

- Des services Netflow devraient ser de doser et d'outil d'accélération des performances de liste d'accès d'une périphérie et ne devraient pas être lancés sur les Routeurs *chauds de* noyau/circuit principal ou les Routeurs s'exécutant très aux débits d'utilisation du CPU élevé.
- Comprenez les exigence de la collecte de données axée sur les applications. Les applications de traçabilité peuvent seulement exiger les informations d'écoulement de routeur d'origine et de fin tandis que les applications de contrôle peuvent exiger une vue de bout en bout (à usage intensif de données) plus complète.
- Comprenez l'incidence de la topologie du réseau et de la stratégie de routage sur la stratégie de collecte d'écoulement. Par exemple, évitez de collecter des écoulements en double par NetFlow de lancement sur les routeurs d'agrégation principaux où le trafic commence ou se termine et pas sur les Routeurs ou les routeurs intermédiaires de circuit principal qui fourniraient des vues en double des mêmes informations d'écoulement.
- Les fournisseurs de services dans l'entreprise de *transporteur de transit* (le trafic de transport ni commençant ni se terminant sur leur réseau) peuvent utiliser des données d'exportation de NetFlow pour les utilisation par les ressources réseau du trafic de transit de mesure pour le comptabilité et de affichage.

Configurez l'ip accounting

La prise en charge de la traçabilité sur IP de Cisco fournit des fonctions de base d'ip accounting. En activant l'ip accounting, les utilisateurs peuvent voir le nombre d'octets et de paquets commutés par le logiciel de Cisco IOS sur une base de source et d'adresse IP de destination. Seulement le trafic IP de transit est mesuré et seulement sur une base sortante. Le trafic généré par le logiciel ou la terminaison en logiciel n'est pas inclus en statistiques de traçabilité. Pour mettre à jour des totaux de comptabilité précis, le logiciel met à jour deux bases de données de traçabilité : un active et une base de données contrôle-aiguë.

La prise en charge de la traçabilité sur IP de Cisco fournit également les informations qui identifient le trafic IP qui échoue des Listes d'accès IP. Identifier les adresses de source IP qui violent des Listes d'accès IP signale des tentatives possibles à l'infraction à la sécurité. Les données indiquent également que des configurations de liste d'accès IP devraient être vérifiées. Pour rendre cette caractéristique disponible aux utilisateurs, l'ip accounting d'enable des violations de liste d'accès utilisant les Access- **violations d'ip accounting** commandent. Les utilisateurs peuvent alors afficher le nombre d'octets et de paquets d'une source unique qui a tenté à l'infraction à la sécurité contre la liste d'accès pour la paire de destination source. Par défaut, l'ip accounting affiche le nombre de paquets qui ont passé des Listes d'accès et a été conduit.

Pour activer l'ip accounting, utilisez une des commandes suivantes pour chaque interface dans le mode de configuration d'interface :

Commande	But
ip accounting	Ip accounting de base d'enable.
violations d'accès d'ip accounting	Activez l'ip accounting avec la capacité d'identifier le trafic IP qui échoue des Listes d'accès IP.

Pour configurer d'autres fonctions d'ip accounting, utilisez un ou plusieurs des commandes suivantes en mode de configuration globale :

Commande	But
*seuil d'***ip accounting-threshold**	Placez le nombre maximal d'écritures à créer.
masque d'IP address d' **ip accounting-list**	L'information de comptabilité de filtre pour des hôtes.
*compte d'***ip accounting-transits**	Contrôlez le nombre d'enregistrements de transit qui seront enregistrés dans la base de données d'ip accounting.

Informations connexes

- **Solutions de Gestion d'entreprise de Cisco, volume I par la presse de Cisco, ISBN 1587050064**
- **Livre blanc Technologies**

Date du fichier PDF généré: 19 mars 2016

http://www.cisco.com/cisco/web/support/CA/fr/109/1093/1093735_NMS_bestpractice.html