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.

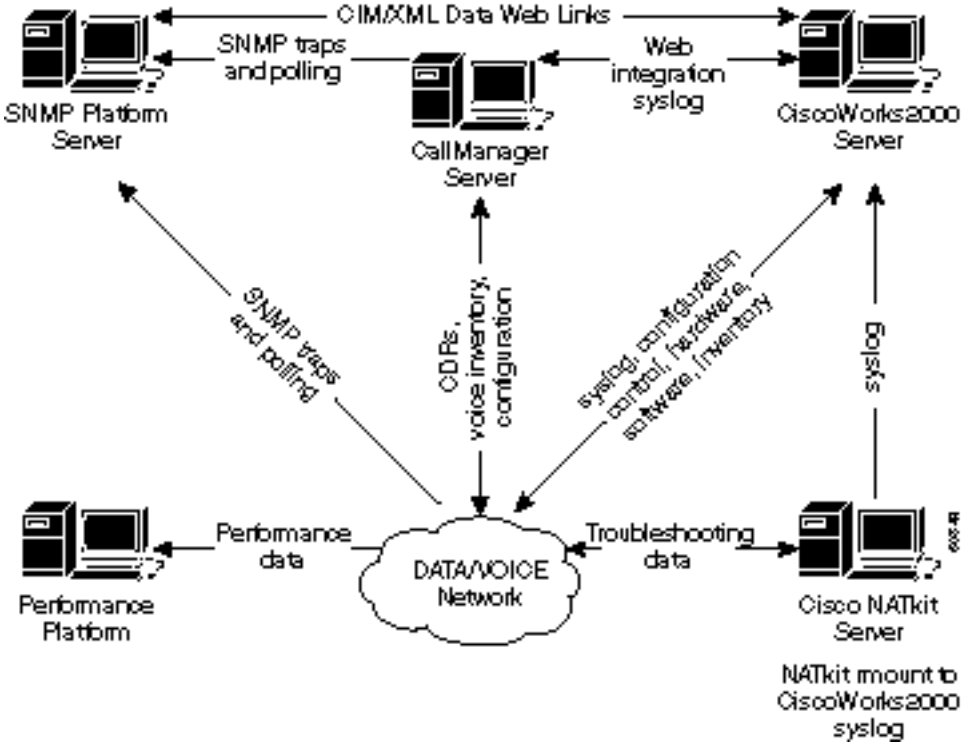
Gestion de réseau CSNA

Les cinq domaines de fonctionnalité du modèle de gestion de réseau de l’ISO se trouvent ci-dessous.

- Gestion des défaillances : détection, isolation, signalement et correction des défaillances

détectées sur le réseau.
- Gestion de la configuration : aspects de configuration des périphériques réseau comme la gestion des fichiers de configuration, la gestion du parc et la gestion des logiciels.
- Gestion des performances : surveillance et mesure des différents aspects de la performance afin que la performance globale puisse être maintenue à un niveau acceptable.
- Gestion de la sécurité : fournir un accès aux périphériques réseau et aux ressources de l'entreprise aux personnes autorisées.
- Gestion de la comptabilité : données sur l'utilisation des ressources du réseau.

Le schéma suivant montre une architecture de référence qui, selon Cisco Systems, devrait être la solution minimale pour la gestion d'un réseau de données. Cette architecture comprend un serveur Cisco CallManager pour la gestion de la voix sur IP (VoIP) : Le schéma montre comment intégrer le serveur CallManager dans la topologie du système de gestion de réseau.



L'architecture de gestion de réseau comprend les éléments suivants :

- Plateforme du protocole SNMP (Simple Network Management Protocol) pour la gestion des défaillances
- Plateforme de surveillance des performances pour la gestion et les tendances à long terme des performances
- Serveur CiscoWorks2000 pour la gestion de la configuration, la collecte des journaux système et la gestion du parc matériel et logiciel

Certaines plateformes du protocole SNMP peuvent partager directement des données avec le serveur CiscoWorks2000 à l'aide de méthodes CIM/XML (Common Information Model/eXtensible Markup Language). CIM est un modèle de données unifié d'un schéma de mise en œuvre neutre pour décrire les données de gestion générales dans un environnement réseau et d'entreprise. Le modèle CIM se compose d'une spécification et d'un schéma. La spécification définit les détails de l'intégration avec d'autres modèles de gestion, bases d'informations de gestion (MIB) SNMP ou les fichiers d'informations de gestion (MIF) de DMTF, tandis que le schéma fournit les descriptions réelles du modèle.

XML est un langage de balisage utilisé pour la représentation de données structurées sous forme

textuelle. Un objectif spécifique du langage XML consistait à conserver le plus de puissance possible du langage SGML, tout en le simplifiant au maximum. Le langage XML est similaire au langage HTML, mais alors que le langage HTML sert à transmettre des informations graphiques sur un document, le langage XML sert plutôt la représentation de données structurées dans un document.

Les clients des services avancés de Cisco incluront également le serveur NATkit de Cisco pour ajouter de la surveillance et du dépannage proactifs. Le serveur NATkit disposera d'un accès par disque monté à distance (rmount) ou par protocole de transfert de fichier (FTP) aux données se trouvant sur le serveur CiscoWorks2000.

Le chapitre Notions de base de la gestion de réseau du document *Présentation de la technologie Internetworking fournit une vue d'ensemble plus détaillée des notions de base de la gestion de réseau.*

Gestion des défaillances

L'objectif de la gestion des défaillances est de détecter, de consigner, d'informer les utilisateurs et (dans la mesure du possible) de résoudre automatiquement les problèmes de réseau pour que le réseau fonctionne efficacement. Comme les défaillances peuvent entraîner du temps d'arrêt ou une dégradation inacceptable du réseau, la gestion des défaillances est peut-être l'élément de gestion de réseau de l'ISO le plus largement mis en œuvre.

Plateformes de gestion de réseau

Une plateforme de gestion de réseau déployée dans l'entreprise gère une infrastructure composée d'éléments de réseau de différents fournisseurs. La plateforme reçoit et traite les événements des composants du réseau. Les événements provenant des serveurs et d'autres ressources critiques peuvent également être transmis à une plateforme de gestion. Les fonctions suivantes, généralement offertes, sont comprises dans une plateforme de gestion standard :

- Découverte de réseaux
- Cartographie topologique des composants du réseau
- Gestionnaire d'événements
- Collecteur et graphiques de données de performance
- Navigateur de données de gestion

Les plateformes de gestion de réseau peuvent être considérées comme la console principale pour l'exploitation du réseau servant à la détection des défaillances dans l'infrastructure. Il est essentiel de pouvoir détecter rapidement les problèmes dans tout réseau. Le personnel d'exploitation du réseau peut se baser sur une carte de réseau graphique pour afficher les états de fonctionnement des composants critiques du réseau, comme les routeurs et les commutateurs.

Les plateformes de gestion de réseau comme HP OpenView, Computer Associates Unicenter et SUN Solstice peuvent effectuer la détection des périphériques réseau. Chaque périphérique réseau est représenté par un élément graphique sur la console de la plateforme de gestion. Les différentes couleurs des éléments graphiques correspondent à l'état de fonctionnement actuel des périphériques réseau. Les périphériques réseau peuvent être configurés pour envoyer des notifications, appelées des interruptions SNMP, aux plateformes de gestion de réseau. Lors de la réception des notifications, l'élément graphique représentant le périphérique réseau passe à une couleur différente selon la gravité de la notification reçue. La notification, généralement appelée événement, est consignée dans un fichier journal. Il est particulièrement important que les fichiers

de la base d'informations de gestion (MIB) de Cisco les plus récents soient chargés sur la plateforme SNMP pour s'assurer que les diverses alertes provenant des périphériques Cisco sont interprétées correctement.

Cisco publie les fichiers MIB pour la gestion de divers périphériques réseau. Les fichiers MIB de Cisco se trouvent sur le site Web cisco.com et contiennent les renseignements suivants :

- Fichiers MIB publiés dans le format SNMPv1
- Fichiers MIB publiés dans le format SNMPv2
- Interruptions SNMP prises en charge par les périphériques Cisco
- Identifiants d'objets pour les objets MIB SNMP actuels de Cisco

Un certain nombre de plateformes de gestion de réseau sont capables de gérer plusieurs sites distribués géographiquement. Pour ce faire, les données de gestion sont échangées entre les consoles de gestion des sites à distance et une station de gestion au site principal. Le principal avantage d'une architecture distribuée est qu'elle réduit le trafic de gestion, ce qui permet d'optimiser l'utilisation de la bande passante. Une architecture distribuée permet également au personnel de gérer localement les réseaux à partir des sites à distance avec des systèmes.

Une récente amélioration des plateformes de gestion est la capacité à gérer à distance les composants du réseau à l'aide d'une interface Web. Cette amélioration élimine la nécessité d'un logiciel client spécial sur chaque station utilisateur pour pouvoir accéder à une plateforme de gestion.

Une entreprise a généralement différents composants de réseau. Toutefois, chaque périphérique nécessite habituellement des systèmes de gestion des composants propres au fournisseur afin de gérer efficacement les composants du réseau. Par conséquent, il se peut que plusieurs stations de gestion interrogent les composants du réseau pour obtenir les mêmes informations. Les données collectées par les différents systèmes sont stockées dans des bases de données distinctes, ce qui engendre des frais d'administration pour les utilisateurs. Cette limite a poussé les fournisseurs de réseaux et de logiciels à adopter des normes comme l'architecture pour un intermédiaire commun dans les requêtes d'objet (CORBA) et la productique (CIM) pour faciliter l'échange de données de gestion entre les plateformes de gestion et les systèmes de gestion des composants. Avec les fournisseurs qui adoptent des normes relatives au développement de systèmes de gestion, les utilisateurs peuvent s'attendre à une interopérabilité et à des économies de coûts pour le déploiement et la gestion de l'infrastructure.

L'architecture CORBA définit un système qui assure l'interopérabilité entre les objets d'un environnement distribué hétérogène de manière transparente pour le programmeur. Sa conception repose sur le modèle d'objet du Object Management Group (OMG).

Dépannage de l'infrastructure

Les serveurs TFTP (Trivial File Transfer Protocol) et de journal système (syslog) sont des composants essentiels d'une infrastructure de dépannage en matière d'exploitation de réseau. Le serveur TFTP sert principalement à stocker les fichiers de configuration et les images logicielles des périphériques réseau. Les routeurs et les commutateurs sont capables d'envoyer des messages de journal système à un serveur syslog. Les messages facilitent la fonction de dépannage lorsque des problèmes surviennent. Le personnel de soutien de Cisco a parfois besoin des messages du journal système pour effectuer une analyse de cause première.

La fonction de collecte distribuée de journaux système des Resource Management Essentials (Essentials) de CiscoWorks2000 permet de déployer plusieurs stations de collecte UNIX ou NT

sur des sites à distance afin d'effectuer la collecte et le filtrage des messages. Les filtres peuvent spécifier quels messages de journal système seront transmis au serveur Essentials principal. Le principal avantage de la mise en œuvre de la collecte distribuée est la réduction du nombre de messages envoyés aux serveurs syslog principaux.

Détection des défaillances et notifications

L'objectif de la gestion des défaillances est de détecter, d'isoler, de signaler et de corriger les défaillances détectées sur le réseau. Les périphériques réseau peuvent alerter les stations de gestion lorsqu'une défaillance survient sur les systèmes. Un système de gestion des défaillances efficace est composé de plusieurs sous-systèmes. La détection des défaillances est effectuée lorsque les périphériques envoient des messages d'interruption SNMP, des interrogations SNMP, des seuils de surveillance à distance (RMON) et des messages de journal système. Un système de gestion informe l'utilisateur final lorsqu'une défaillance est signalée et que des mesures correctives peuvent être prises.

Les interruptions doivent être activées de manière cohérente sur les périphériques réseau. Les interruptions supplémentaires sont prises en charge avec les nouvelles versions du logiciel Cisco IOS pour les routeurs et les commutateurs. Il est important de vérifier et de mettre à jour le fichier de configuration pour s'assurer que les interruptions sont décodées correctement. Un examen périodique des interruptions configurées avec l'équipe des services d'assurance de réseau (ANS) de Cisco assurera la détection efficace des défaillances dans le réseau.

Le tableau suivant répertorie les interruptions CISCO-STACK-MIB prises en charge par les commutateurs de réseau local (LAN) Cisco Catalyst. Ces interruptions peuvent également servir à surveiller les conditions de défaillance sur ces commutateurs.

Alerte	Description
module Up	L'entité d'agent a détecté que l'objet **moduleStatus de cette base MIB est passé à l'état ok(2) pour l'un de ses modules.**
module Down	L'entité d'agent a détecté que l'objet *moduleStatus de cette base MIB est passé à un état autre que* **ok(2) pour l'un de ses modules.**
chassis AlarmOn	L'entité de l'agent a détecté que l'objet *chassisTempAlarm*, **chassisMinorAlarm** ou *chassisMajorAlarm de cette base MIB est passé à l'état* **on(2).** Une interruption *chassisMajorAlarm signifie que l'une des conditions suivantes est vraie :* • panne de tension • défaillance simultanée de la température et du ventilateur • défaillance complète de l'alimentation (deux modules sur deux, ou un sur un) • défaillance de la mémoire morte effaçable et programmable électriquement (EEPROM) • défaillance de la mémoire vive non volatile (NVRAM)

	• défaillance de la communication MCP • état NMP inconnu Une interruption chassisMajorAlarm signifie que l'une des conditions suivantes est vraie : • alarme de température • défaillance de ventilateur • défaillance partielle de l'alimentation (un module sur deux) • modules d'alimentation de types incompatibles
chassisAlarmOff	L'entité de l'agent a détecté que l'objet *chassisTempAlarm*, **chassisMinorAlarm** ou *chassisMajorAlarm de cette base MIB est passé à l'état* **off(1).**

Les interruptions de surveillance des environnements (envmon) sont définies dans l'interruption CISCO-ENVMON-MIB. L'interruption envmon envoie des notifications relatives à la surveillance des environnements d'entreprise de Cisco lorsqu'un seuil d'environnement est dépassé. Lorsque l'interruption envmon est utilisée, un type d'interruption d'environnement spécifique peut être activé, ou tous les types d'interruption du système de surveillance des environnements peuvent être acceptés. Si aucune option n'est spécifiée, tous les types d'environnement sont activés. Ce peut être l'une ou plusieurs des valeurs suivantes :

- tension − un message ciscoEnvMonVoltageNotification est envoyé si la tension mesurée à un point de test donné est en dehors de l'intervalle normal du point de test (par exemple, à l'étape de l'avertissement, de l'état critique ou de l'arrêt).
- arrêt − un message ciscoEnvMonShutdownNotification est envoyé si la surveillance des environnements détecte qu'un point de test atteint un état critique et qu'il est sur le point de lancer un arrêt.
- alimentation − un message ciscoEnvMonRedundantSupplyNotification est envoyé en cas de défaillance du module d'alimentation redondante (le cas échéant).
- ventilateur − un message ciscoEnvMonFanNotification est envoyé en cas de défaillance de l'un des ventilateurs du bloc de ventilation (le cas échéant).
- température − un message ciscoEnvMonTemperatureNotification est envoyé si la température mesurée à un point de test donné est en dehors de l'intervalle normal du point de test (par exemple, à l'étape de l'avertissement, de l'état critique ou de l'arrêt).

La détection des défaillances et la surveillance des composants du réseau peuvent être étendues du niveau de l'appareil aux niveaux du protocole et de l'interface. Pour un environnement réseau, la surveillance des défaillances peut comprendre le réseau local virtuel (VLAN), le mode de transfert asynchrone (ATM), les indications sur les défaillances sur les interfaces physiques, etc. Il est possible de mettre en œuvre la gestion des défaillances au niveau du protocole à l'aide d'un système de gestion des composants comme CiscoWorks2000 Campus Manager. L'application TrafficDirector de Campus Manager sert principalement à effectuer la gestion des commutateurs à l'aide de la prise en charge de mini-RMON sur les commutateurs Catalyst.

Avec un nombre croissant de composants réseau et la complexité des problèmes de réseau, un système de gestion des événements capable de mettre en corrélation les différents événements réseau (journal système, interruption, fichiers journaux) peut être envisagé. L'architecture sous-tendant un système de gestion des événements est comparable à un système de gestionnaire de gestionnaires (MOM). Un système de gestion des événements bien conçu permet au personnel

du centre d'exploitation de réseau (NOC) d'être proactif et efficace pour détecter et diagnostiquer les problèmes de réseau. La hiérarchisation et la suppression des événements permettent au personnel d'exploitation de réseau de se concentrer sur des événements de réseau critiques, d'analyser plusieurs systèmes de gestion des événements, notamment Cisco Info Center, et de mener une analyse de faisabilité afin d'explorer complètement les fonctionnalités de ces systèmes. Pour obtenir de plus amples renseignements, visitez le Cisco Info Center.

Surveillance proactive des défaillances et notifications

Les événements et alarmes RMON sont deux groupes définis dans la spécification RMON. En règle générale, une station de gestion effectue des interrogations sur les périphériques réseau pour connaître l'état ou la valeur de certaines variables. Par exemple, une station de gestion interroge un routeur pour en connaître l'utilisation de l'unité centrale (CPU) et générer un événement quand la valeur atteint un seuil paramétré. Cette méthode gaspille la bande passante du réseau et peut également manquer l'atteinte réelle du seuil dépendant de l'intervalle d'interrogation.

Avec les alarmes et les événements RMON, un périphérique réseau est configuré pour surveiller lui-même les seuils d'augmentation et de baisse. À un intervalle de temps prédéfini, le périphérique réseau utilise un échantillon d'une variable et le compare aux seuils. Une interruption SNMP peut être envoyée à une station de gestion si la valeur réelle passe au-dessus ou en deçà des seuils configurés. Les groupes d'alertes et d'événements RMON fournissent une méthode proactive pour gérer les périphériques réseau critiques.

Cisco Systems recommande la mise en œuvre d'alarmes et d'événements RMON sur les périphériques réseau critiques. Les variables surveillées peuvent comprendre l'utilisation du CPU, des défaillances de tampon, des abandons d'entrée ou de sortie, ou de toute variable de type entier. À partir de la version 11.1(1) du logiciel Cisco IOS, toutes les images de routeur prennent en charge les groupes d'alarmes et d'événements RMON.

Pour obtenir des informations détaillées sur la mise en œuvre d'alarmes et d'événements RMON, consultez la section Mise en œuvre d'alarmes et d'événements 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. RMON utilise ce qu'on appelle un *compartiment pour stocker les historiques et les statistiques sur l'agent RMON (le commutateur dans ce cas).* La taille du compartiment est définie sur la sonde RMON (périphérique SwitchProbe) ou sur l'application RMON (outil TrafficDirector), puis envoyée au commutateur pour la définir.

Environ 450 Ko d'espace de code sont nécessaires pour prendre en charge le mini-RMON (par exemple, quatre groupes RMON : statistiques, historique, alarmes, et événements). La mémoire dynamique requise pour RMON varie en fonction de la configuration de l'exécution.

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

Définition du groupe R	Espace de DRAM utilisé	Notes

MON		
Statistiques	140 octets par port Ethernet/Fast Ethernet commuté	Par port
Historique	3,6 Ko pour 50 compartiments *	Chaque compartiment supplémentaire utilise 56 octets
Alarmes et événements	2,6 Ko par alarme et ses entrées d'événements	Par alarme par port

RMON utilise ce qu'on appelle un *compartiment pour stocker les historiques et les statistiques sur l'agent RMON (comme un commutateur).*

Mise en œuvre d'alarmes et d'événements RMON

En intégrant RMON à une solution de gestion des défaillances, un utilisateur peut surveiller le réseau de manière proactive avant qu'un problème potentiel ne se produise. Par exemple, si le nombre de paquets de diffusion reçus augmente considérablement, cela peut entraîner une augmentation de l'utilisation de CPU. En mettant en œuvre les alarmes et les événements RMON, un utilisateur peut configurer un seuil pour surveiller le nombre de paquets de diffusion reçus et alerter la plateforme SNMP par une interruption SNMP si le seuil configuré est atteint. Les alarmes et les événements RMON éliminent le nombre excessif d'interrogations normalement effectuées par la plateforme SNMP pour atteindre le même objectif.

Deux méthodes sont disponibles pour configurer les alarmes et événements RMON :

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

Les exemples de procédures ci-dessous expliquent comment définir un seuil pour surveiller le nombre de paquets de diffusion reçus sur une interface. Le même compteur est utilisé dans ces procédures, comme le montre l'**exemple de la commande show interface à la fin de la présente section.**

Exemple avec l'interface de ligne de commande

Pour mettre en œuvre les alarmes et les événements RMON à l'aide de l'interface CLI, suivez les étapes suivantes :

1. Trouvez l'index d'interface associé à l'interface Ethernet 0 en parcourant la base 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. Récupérez l'OID associé au champ CLI à surveiller. Dans cet exemple, l'OID pour « broadcasts » est 1.3.6.1.2.1.2.2.1.12. Les OID Cisco pour les variables spécifiques à la base MIB sont disponibles sur le site Web cisco.com.
3. Définissez les paramètres suivants pour configurer les seuils et les événements.seuils d'augmentation et de baissetype d'échantillonnage (absolu ou delta)intervalle d'échantillonnagemesure à prendre lorsqu'un seuil est atteintPour cet exemple, un seuil est

configuré pour surveiller le nombre de paquets de diffusion reçus sur l'interface Ethernet 0. Une interruption sera générée si le nombre de paquets de diffusion reçus est supérieur à 500 entre des échantillons pris à 60 secondes d'intervalle. Le seuil sera réactivé lorsque le nombre de diffusions d'entrée n'augmente pas entre deux échantillons.**Remarque :** Pour obtenir des informations détaillées sur ces paramètres de commande, consultez la documentation CCO (Cisco Connection Online) pour obtenir des commandes d'alarme et d'événement RMON pour votre version Cisco IOS particulière.

4. Précisez l'interruption envoyée (événement RMON) lorsque le seuil est atteint à l'aide des commandes CLI suivantes (les commandes de Cisco IOS sont affichées en gras) :**rmon event 1 trap gateway description "Diffusion élevée sur Ethernet 0" owner ciscormon event 2 log description "diffusion normale reçue sur ethernet 0" owner cisco**
5. Précisez les seuils et les paramètres pertinents (alarme RMON) à l'aide des commandes CLI suivantes :**l'alarme RMON 1 ifEntry. 12.1 60 Delta augmentation-seuil 500 1falling-threshold 0 2 owner cisco**
6. Utilisez SNMP pour interroger ces tables afin de 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. Utilisez SNMP pour interroger ces tables afin de vérifier que les entrées alarmTable ont été définies.

```
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 avec les opérations SNMP SET

Pour mettre en œuvre les alarmes et événements RMON avec l'opération SNMP SET, suivez les étapes suivantes :

1. Précisez l'interruption envoyée (événement RMON) lorsque le seuil est atteint à l'aide des opérations 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. Précisez les seuils et les paramètres pertinents (alarme RMON) à l'aide des opérations 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. Interrogez ces tables afin de 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. Interrogez ces tables afin de vérifier que les entrées alarmTable ont été définies.

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

show interface

Cet exemple est le résultat de la commande **show interface.**

gateway> **show interface** ***ethernet 0***

```
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 les informations de configuration du réseau et du système afin que les effets sur l'exploitation du réseau de diverses versions des composants matériels et logiciels puissent faire l'objet d'un suivi et d'une gestion.

Normes de configuration

Avec un nombre croissant de périphériques réseau déployés, il est essentiel de pouvoir déterminer l'emplacement précis d'un périphérique réseau. Ces renseignements relatifs à l'emplacement doivent fournir une description détaillée pour les personnes chargées de la répartition des ressources lorsqu'un problème de réseau se produit. Pour accélérer la résolution d'un problème de réseau, assurez-vous de disposer des coordonnées de la personne ou du service responsable des périphériques. Les coordonnées doivent comprendre le numéro de téléphone et le nom de la personne ou du service.

Les conventions d'appellation des périphériques réseau, allant du nom du périphérique à celui des interfaces individuelles, doivent être planifiées et mises en œuvre dans le cadre de la norme de configuration. Une convention d'appellation bien définie fournit au personnel la possibilité de fournir des renseignements précis lors du dépannage des problèmes de réseau. La convention d'appellation pour les périphériques peut utiliser l'emplacement géographique, le nom du bâtiment, l'étage, etc. Pour la convention d'appellation des interfaces, celle-ci peut comprendre le segment auquel un port est connecté, le nom du concentrateur de connexion, etc. Sur les interfaces en série, elle doit comprendre la bande passante réelle, le numéro d'identificateur de connexion de liaison de données (DLCI) local (si le relayage de trames est utilisé), la destination, et l'identifiant de circuit ou les renseignements fournis par l'opérateur.

Gestion des fichiers de configuration

Lorsque vous ajoutez de nouvelles commandes de configuration aux périphériques réseau existants, vous devez vérifier les commandes pour vous assurer de leur intégrité avant que la mise en œuvre ne soit réellement effectuée. Un périphérique réseau mal configuré peut avoir un effet désastreux sur la connectivité et les performances du réseau. Les paramètres de la commande de configuration doivent être vérifiés afin d'éviter les problèmes de non-concordance ou d'incompatibilité. Il est recommandé de planifier des examens approfondis réguliers des configurations avec les ingénieurs de Cisco.

Un système CiscoWorks2000 Essentials entièrement fonctionnel permet de sauvegarder automatiquement les fichiers de configuration sur commutateurs Cisco Catalyst et les routeurs. La fonction de sécurité d'Essentials peut être utilisée pour effectuer l'authentification sur les modifications de configuration. Un journal de vérification des modifications est disponible pour faire le suivi des modifications et le nom d'utilisateur des personnes qui apportent les modifications. Pour modifier la configuration de plusieurs périphériques, deux options sont disponibles : l'outil en ligne NetConfig dans la version actuelle de CiscoWorks2000 Essentials ou le script **cwconfig.** Les fichiers de configuration peuvent être téléchargés et téléversés à l'aide de CiscoWorks2000 Essentials en utilisant des modèles prédéfinis ou définis par l'utilisateur.

Ces fonctions peuvent être utilisées avec les outils de gestion de la configuration de CiscoWorks2000 Essentials :

- Envoi de fichiers de configuration de l'archive des configurations d'Essentials à un ou plusieurs périphériques
- Envoi de la configuration à partir du périphérique à l'archive d'Essentials
- Extraction de la dernière configuration de l'archive et exportation dans un fichier
- Importation de la configuration à partir d'un fichier et envoi de la configuration aux périphériques
- Comparaison des deux dernières configurations dans l'archive d'Essentials
- Suppression des configurations antérieures à une date ou à une version spécifiée dans l'archive
- Copie de la configuration de démarrage comme configuration exécutée.

Gestion des inventaires

La fonction de découverte de la plupart des plateformes de gestion de réseau vise à fournir une liste dynamique des périphériques présents sur le réseau. Les moteurs de découverte comme ceux mis en œuvre dans les plateformes de gestion de réseau devraient être utilisés.

Une base de données du parc fournit des informations de configuration détaillées sur les périphériques réseau. Les informations courantes incluent les modèles du matériel, les modules installés, les images logicielles, les niveaux de microcode, etc. Tous ces éléments d'information sont essentiels pour effectuer des tâches comme la maintenance logicielle et matérielle. La liste à jour des périphériques réseau collectés par le processus de découverte peut servir comme liste principale pour collecter des informations sur le parc à l'aide du protocole SNMP ou de scripts. Une liste de périphériques peut être importée de CiscoWorks2000 Campus Manager dans la base de données du parc de CiscoWorks2000 Essentials pour obtenir un parc à jour des commutateurs Cisco Catalyst.

Gestion des logiciels

La réussite d'une mise à niveau des images Cisco IOS sur les périphériques réseau nécessite une analyse détaillée des exigences comme la mémoire, la mémoire morte d'amorçage, le niveau de microcode, etc. Les exigences sont généralement documentées et disponibles sur le site Web de Cisco sous la forme de notes de version et de guides d'installation. Le processus de mise à niveau d'un périphérique réseau exécutant Cisco IOS comprend le téléchargement d'une image correcte à partir de CCO, la sauvegarde de l'image actuelle, en vous assurant que toutes les exigences matérielles sont respectées, puis en chargeant la nouvelle image dans le périphérique.

La fenêtre de mise à niveau pour terminer la maintenance des périphériques est assez limitée pour certaines entreprises. Dans un environnement réseau de grande envergure avec des ressources limitées, il peut être nécessaire de planifier et d'automatiser les mises à niveau logicielles après les heures de travail. La procédure peut être exécutée à l'aide d'un langage de script comme Expect ou à l'aide d'une application programmée spécifiquement pour effectuer une telle tâche.

Les modifications apportées aux logiciels des périphériques réseau, comme les images de Cisco IOS et les versions de microcode, doivent faire l'objet d'un suivi pour faciliter la phase d'analyse lorsqu'une autre maintenance logicielle est nécessaire. Avec un rapport d'historique des modifications facilement accessible, la personne chargée de la mise à niveau peut limiter le risque de charger des images ou du microcode incompatibles sur des périphériques réseau.

Gestion des performances

Contrat de niveau de service

Un contrat de niveau de service (SLA) est un contrat écrit entre un fournisseur de services et ses clients sur le niveau de performance attendu des services de réseau. Le SLA consiste en des indicateurs convenus entre le fournisseur et ses clients. Les valeurs définies pour les indicateurs doivent être réalistes, significatives et mesurables pour les deux parties.

Il est possible de collecter diverses statistiques sur les interfaces des périphériques réseau pour mesurer le niveau de performance. Ces statistiques peuvent être comprises comme des indicateurs dans le cadre du SLA. Les statistiques comme les abandons de a file d'attente d'entrée, les abandons de la file d'attente de sortie et les paquets ignorés sont utiles pour diagnostiquer les problèmes liés à la performance.

Au niveau du périphérique, les indicateurs de performance peuvent comprendre l'utilisation du CPU, l'attribution de mémoire tampon (grande mémoire tampon, mémoire tampon moyenne, échecs, taux d'attribution) et l'attribution de mémoire. La performance de certains protocoles réseau est directement liée à la disponibilité de la mémoire tampon dans les périphériques réseau. La mesure des statistiques de performance du niveau du périphérique est essentielle pour optimiser la performance des protocoles de niveau supérieur.

Les périphériques réseau comme les routeurs prennent en charge divers protocoles de couche supérieure, comme Data Link Switching Workgroup (DLSW), Remote Source Route Bridging (RSRB), AppleTalk, etc. Les statistiques de performance des technologies de réseau étendu (WAN), notamment le relayage de trames, le mode de transfert asynchrone (ATM), le réseau numérique à intégration de services (ISDN) et d'autres peuvent être surveillées et collectées.

Surveillance, mesure et rapports de performance

Différents indicateurs de performance au niveau de l'interface, du périphérique et du protocole doivent être collectés régulièrement à l'aide du protocole SNMP. Le moteur d'interrogation d'un système de gestion de réseau peut être utilisé pour collecter des données. La plupart des systèmes de gestion de réseau sont capables de collecter, de stocker et de présenter des données recueillies.

Diverses solutions sont offertes sur le marché pour répondre aux besoins de la gestion des performances dans les environnements d'entreprise. Ces systèmes sont capables de collecter, de stocker et de présenter les données des périphériques réseau et des serveurs. L'interface Web de la plupart des produits rend les données de performance accessibles de partout dans l'entreprise. Voici quelques exemples de solutions de gestion des performances souvent déployées :

- VistaView d'InfoVista
- IT Service Vision de SAS
- TREND de Trinagy

Un examen des produits ci-dessus permet de déterminer s'ils répondent aux exigences des différents utilisateurs. Certains fournisseurs prennent en charge l'intégration à des plateformes de gestion de réseau et de gestion de système. Par exemple, InfoVista prend en charge Patrol Agent de BMC pour fournir des statistiques de performance clés des serveurs d'applications. Chaque produit dispose d'un modèle de tarification et de fonctionnalités de l'offre de base différents. La prise en charge des fonctionnalités de gestion de performance pour les périphériques Cisco

comme NetFlow, RMON et l'agent d'assurance de service/compte rendu de temps de réponse de Cisco IOS (RTR/SAA CSAA/RTR) est offerte dans certaines solutions. Concord a récemment ajouté la prise en charge pour les commutateurs de réseau WAN de Cisco qui peut être utilisée pour collecter et afficher les données de performance.

La fonctionnalité d'agent d'assurance de service (SAA)/compte rendu de temps de réponse (RTR) CSAA/RTR dans Cisco IOS peut être utilisée pour mesurer le temps de réponse entre les périphériques IP. Un routeur source configuré avec CSAA 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 pour chaque saut le long du chemin. Les interruptions SNMP peuvent être configurées pour les consoles de gestion des alertes si le temps de réponse dépasse les seuils prédéfinis.

Les récentes améliorations apportées à Cisco IOS étendent les fonctionnalités de CSAA pour mesurer les éléments suivants :

- performance du service du protocole de transfert hypertexte (HTTP)recherche dans le système de noms de domaine (DNS)protocole de contrôle de transmission (TCP)durée de transaction HTTP
- variance de la latence interpaquets (gigue) du trafic de voix sur IP (VoIP)
- temps de réponse entre les points terminaux pour une qualité de service (QoS) précisebits de type de service (ToS) IP
- perte de paquets à l'aide de paquets générés par CSAA

La configuration de la fonctionnalité CSAA sur les routeurs peut être effectuée à l'aide de l'application InterNetwork Performance Monitor (IPM) de Cisco. Le CSAA/RTR est intégré à de nombreux ensembles de fonctionnalités du logiciel Cisco IOS. Une version du logiciel Cisco IOS prenant en charge CSAA/RTR doit être installée sur le périphérique utilisé par IPM pour collecter des statistiques de performance. Pour obtenir un résumé des versions de Cisco IOS prenant en charge CSAA/RTR/IPM, consultez le site Web de la Foire aux questions sur IPM.

Les renseignements supplémentaires sur IPM comprennent :

- la présentation d'IPM
- l'agent d'assurance de service

Analyse et réglage de la performance

Le trafic des utilisateurs a significativement augmenté et exige plus de ressources du réseau. Les gestionnaires de réseau disposent généralement d'une vue limitée des types de trafic qui transitent sur le réseau. Le profile de trafic des utilisateurs et des applications fournit une vue détaillée du trafic du réseau. Deux technologies, NetFlow et les sondes RMON, permettent de collecter des profils de trafic.

RMON

Les normes RMON sont conçues pour être déployées dans une architecture distribuée où les agents (intégrés ou dans des sondes autonomes) communiquent avec une station centrale (la console de gestion) par SNMP. La norme RMON du RFC 1757 organise les fonctions de surveillance en neuf groupes pour prendre en charge les topologies Ethernet et ajoute un dixième groupe dans le RFC 1513 pour les paramètres spécifiques aux réseaux en anneau à jeton. La surveillance des liaisons Fast Ethernet est fournie dans le cadre de la norme RFC 1757, tandis

que la surveillance de l'anneau d'interface de données distribuées sur fibre (FDDI) est fournie dans le cadre des RFC 1757 et 1513.

La spécification RMON émergente de RFC 2021 dirige les normes de surveillance à distance au-delà de la couche de contrôle d'accès au support (MAC) vers les couches réseau et application. Cette configuration permet aux administrateurs d'analyser et de dépanner des applications réseau comme le trafic Web, NetWare, Notes, le courriel, l'accès aux bases de données, le système de gestion de fichiers en réseau (NFS), etc. Les alarmes RMON, les statistiques, l'historique et les groupes d'hôtes et de conversations peuvent désormais être utilisés pour surveiller et gérer de manière proactive la disponibilité du réseau en fonction du trafic de la couche application, le trafic le plus critique du réseau. RMON2 permet aux administrateurs réseau de poursuivre leur déploiement de solutions de surveillance basées sur des normes afin de prendre en charge les applications critiques situées sur un serveur.

Les tableaux suivants répertorient les fonctions des groupes RMON.

Groupe RMON (RFC 1757)	Fonction
Statistiques	Compteurs pour les paquets, les octets, les diffusions, les erreurs et les offres sur le segment ou le port.
Historique	Échantillonne et enregistre régulièrement les compteurs du groupe de statistiques pour les récupérer ultérieurement.
Hôtes	Conserve les statistiques sur chaque périphérique hôte sur le segment ou le port.
Premiers N hôtes	Rapport de sous-ensemble défini par l'utilisateur du groupe d'hôtes, trié en fonction d'un compteur statistique. En renvoyant uniquement les résultats, le trafic de gestion est réduit.
Matrice de trafic	Conserve les statistiques de conversation entre les hôtes sur le réseau.
Alarmes	Seuil pouvant être défini sur des variables RMON critiques pour une gestion proactive.
Événements	Génère des interruptions et des entrées de journal SNMP en cas de dépassement d'un seuil du groupe d'alarmes.
Capture de paquets	Gère les mémoires tampons pour les paquets capturés par le groupe de filtre pour être chargés dans la console de gestion.
Token Ring	Station d'anneau : statistiques détaillées sur chaque station. Ordre de station d'anneau : une liste ordonnée de stations actuellement dans l'anneau. Configuration de la station d'anneau : configuration et insertion/suppression par station. Routage source : statistiques sur le

	routage source, comme le nombre de sauts et d'autres.

RMON2	Fonction
Répertoire de protocoles	Les protocoles utilisés par l'agent pour surveiller et gérer les statistiques.
Distribution de protocoles	Les statistiques pour chaque protocole.
Hôte de couche réseau	Les statistiques pour chaque adresse de couche réseau sur le segment, l'anneau ou le port.
Matrice de la couche réseau	Les statistiques de trafic pour les paires d'adresses de couche réseau.
Hôte de la couche application	Les statistiques par protocole de couche application pour chaque adresse réseau.
Matrice de la couche application	Les statistiques de trafic par protocole de couche application pour les paires d'adresses de couche réseau.
Historique définissable par l'utilisateur	Étend l'historique au-delà des statistiques de couche liaison RMON1 pour intégrer les statistiques de RMON, RMON2, MIB-I et MIB-II.
Mise en correspondance d'adresses	Les correspondances d'adresses des couches MAC et réseau.
Groupe de configuration	Les fonctionnalités et les configurations de l'agent.

Netflow

La fonctionnalité Cisco NetFlow permet de collecter les statistiques détaillées des flux de trafic aux fins de planification de capacité, de facturation et de dépannage. NetFlow peut être configuré sur des interfaces individuelles pour fournir des informations sur le trafic qui transite par ces interfaces. Les types d'informations suivants font partie des statistiques détaillées sur le trafic :

- Adresses IP de source et de destination
- Numéros d'interface d'entrée et de sortie
- Port source et ports de destination TCP/UDP
- Nombre d'octets et de paquets dans le flux
- Numéros de systèmes autonomes sources et de destination
- Type de service (ToS) IP

Les données NetFlow collectées sur les périphériques réseau sont exportées vers un collecteur. Le collecteur exécute des fonctions comme la réduction du volume de données (par filtrage et agrégation), le stockage hiérarchique des données et la gestion du système de fichiers. Cisco

offre les applications NetFlow Collector et NetFlow Analyzer pour collecter et analyser les données des routeurs et des commutateurs Cisco Catalyst. Il existe également des outils partagiciels, comme cflowd, qui peuvent collecter des enregistrements de protocole de datagramme utilisateur (UDP) de Cisco NetFlow.

Les données de NetFlow sont transportées à l'aide de paquets UDP dans trois formats différents :

- Version 1 — Le format d'origine pris en charge dans les versions initiales de NetFlow.
- Version 5 — Une amélioration ultérieure qui a ajouté les informations sur le système autonome du protocole de passerelle frontière (BGP) et les numéros de séquence des flux.
- Version 7 — Une amélioration encore plus récente qui a ajouté la prise en charge de la commutation NetFlow pour les commutateurs de la gamme Cisco Catalyst 5000 équipés d'une carte de fonctionnalité NetFlow (NFFC).

Les versions 2 à 4 et la version 6 n'ont pas été publiées ou ne sont pas prises en charge par FlowCollector. Dans les trois versions, le datagramme est composé d'un en-tête et d'un ou de plusieurs enregistrements de flux.

Pour en savoir plus, consultez le document technique Guide des solutions pour les services NetFlow.

Le tableau suivant présente les versions de Cisco IOS prises en charge pour la collection des données NetFlow à partir de routeurs et de commutateurs Catalyst.

Modification de la version du logiciel Cisco IOS	Plateformes matérielles Cisco prises en charge	Versions exportées de 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 commutation de routage (RSM) de Cisco	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 8600	V1 et v5
12.0(3)T et versions	Cisco 1600*, 1720, 2500**, 2600, 3600,	V1, V5 et V8

ultérieures	4500, 4700, AS5300*, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX8800 RPM et BPX 8650	
12.0(6)S	Cisco 12000	V1, V5 et V8
—	Cisco Catalyst 5000 avec carte de fonctionnalité NetFlow (NFFC)***	V7

* La prise en charge des versions 1, 5 et 8 de l'exportation NetFlow sur les plateformes Cisco 1600 et 2500 est destinée à la version 12.0(T) du logiciel Cisco IOS. La prise en charge de NetFlow pour ces plateformes n'est pas disponible dans la version principale 12.0 de Cisco IOS.

* La prise en charge des versions 1, 5 et 8 de NetFlow sur la plateforme AS5300 est destinée à la version 12.06(T) du logiciel Cisco IOS.

*** L'exportation de données NetFlow et MLS est prise en charge dans la version 4.1(1) et les versions ultérieures du logiciel de moteur de supervision de la gamme Catalyst 5000.

Gestion de la sécurité

L'objectif de la gestion de la sécurité est de contrôler l'accès aux ressources du réseau conformément aux directives locales afin que le réseau ne puisse pas être saboté (intentionnellement ou non). Un sous-système de gestion de la sécurité peut, par exemple, surveiller les utilisateurs qui se connectent à une ressource réseau, en refusant l'accès à ceux qui entrent des codes d'accès incorrects. La gestion de la sécurité est un sujet très vaste, c'est pourquoi cette section du document ne traite que la sécurité relative au protocole SNMP et la base de la sécurité des accès aux périphériques.

Des informations détaillées sur la sécurité avancée comprennent :

- Renforcement de la sécurité sur les réseaux IP
- OpenSystems

Une bonne mise en œuvre de la gestion de la sécurité commence par la mise en place d'efficaces politiques et procédures de sécurité. Il est important de créer une norme de configuration minimale spécifique à la plateforme pour tous les routeurs et les commutateurs qui suivent les pratiques exemplaires de l'industrie en matière de sécurité et de performance.

Il existe différentes méthodes de contrôle d'accès sur les routeurs Cisco et les commutateurs Catalyst. Certaines de ces méthodes sont les suivantes :

- les listes de contrôle d'accès (ACL)
- des identifiants d'utilisateur et mots de passe locaux pour le périphérique
- le protocole TACACS (Terminal Access Controller Access-Control System)

TACACS est un protocole de sécurité normalisé (RFC 1492) de l'IETF (Internet Engineering Task Force) qui s'exécute entre les périphériques clients d'un réseau et un serveur TACACS. TACACS est un mécanisme d'authentification qui permet d'authentifier l'identité d'un périphérique qui

cherche à accéder à distance à une base de données privilégiée. Les variantes de TACACS comprennent le protocole TACACS+, l'architecture AAA qui sépare les fonctions d'authentification, d'autorisation et de comptabilité.

Le protocole TACACS+ est utilisé par Cisco pour permettre un contrôle plus précis des personnes autorisées à accéder au périphérique Cisco en mode non privilégié et privilégié. Plusieurs serveurs TACACS+ peuvent être configurés pour la tolérance aux défaillances. Lorsque TACACS+ est activé, le routeur et le commutateur demandent à l'utilisateur d'entrer un nom d'utilisateur et un mot de passe. L'authentification peut être configurée pour le contrôle des connexions ou pour authentifier des commandes individuelles.

Authentification

L'authentification est le processus d'identification des utilisateurs, notamment la prise en charge du dialogue de connexion et de mot de passe, de la réponse d'identification et de la messagerie. L'authentification désigne la manière dont un utilisateur est identifié avant d'être autorisé à accéder au routeur ou au commutateur. Il existe une relation fondamentale entre l'authentification et l'autorisation. Plus de privilèges d'autorisation reçus par un utilisateur, plus l'authentification devrait être renforcée.

Autorisation

L'autorisation permet de contrôler l'accès à distance, notamment l'autorisation ponctuelle et l'autorisation pour chaque service demandé par l'utilisateur. Sur un routeur Cisco, la plage de niveaux d'autorisation pour les utilisateurs est comprise entre 0 et 15, 0 étant le niveau le plus bas et 15 le plus élevé.

Gestion de comptes

La comptabilité permet la collecte et l'envoi des informations de sécurité utilisées pour la facturation, la vérification et la création de rapports, comme les identités des utilisateurs, les heures de début et d'arrêt et les commandes exécutées. La comptabilité permet aux gestionnaires de réseau de faire le suivi des services auxquels les utilisateurs accèdent, ainsi que la quantité de ressources réseau qu'ils consomment.

Le tableau suivant contient des exemples de commandes de base pour l'utilisation de TACACS+, de l'authentification, de l'autorisation et de la comptabilité sur un routeur Cisco et un commutateur Catalyst. Consultez le document sur les Commandes d'authentification, d'autorisation et de comptabilité pour obtenir plus de détails sur les commandes.

Commande Cisco IOS	Objectif
Routeur	
aaa new-model	Active l'authentification, l'autorisation, la comptabilité (AAA) comme méthode principale pour le contrôle d'accès.
AAA accounting {*system* | *réseau* | *connexion* | *exec* | *niveau de*	Active la fonction de comptabilité avec les commandes de configuration globale.

commande} {*start-stop	wait-start	stop-only*} {*tacacs+	radius*}	
aaa authentication login default tacacs+	Configure le routeur pour que les connexions aux lignes de terminal configurées avec la connexion par défaut soient authentifiées avec TACACS+ et qu'elles échouent si l'authentification échoue pour une raison quelconque.
aaa authorization exec default tacacs+ none	Configure le routeur pour vérifier si l'utilisateur est autorisé à exécuter un interpréteur de commandes EXEC en demandant au serveur TACACS+.
tacacs-server host *tacacs+ server ip address*	Spécifie le serveur TACACS+ qui sera utilisé pour l'authentification avec les commandes de configuration globale.
tacacs-server key *shared-secret*	Spécifie le secret partagé qui est connu des serveurs TACACS+ et du routeur Cisco à l'aide de la commande de configuration globale.
Catalyst Switch	
set authentication login tacacs enable [*all	console	http	telnet*] [*primaire*]	Active l'authentification TACACS+ pour le mode de connexion normal. Utilisez les mots clés console ou Telnet pour activer TACACS+ uniquement pour les tentatives de connexion au port de console ou à Telnet.
set authorization exec enable {*option} fallback option*} [*console	telnet	les deux*]	Active l'autorisation pour le mode de connexion normal. Utilisez les mots clés console ou Telnet pour activer l'autorisation uniquement pour les tentatives de connexion au port de console ou à Telnet.
set tacacs-server key *shared-secret*	Spécifie le secret partagé connu par les serveurs TACACS+ et le commutateur.
set tacacs-server host *tacacs+ server ip address*	Spécifie le serveur TACACS+ qui sera utilisé pour l'authentification avec les commandes de configuration globale.
set accounting commands enable {*config	all*} {*stop-only*} *tacacs+*	Active la gestion des commandes de configuration.

Pour en savoir plus sur la configuration d'AAA pour surveiller et contrôler l'accès à l'interface de ligne de commande sur les commutateurs de réseau local Catalyst d'enterprises, consultez au document Contrôler l'accès au commutateur grâce à l'authentification, l'autorisation et la comptabilité.

Sécurité du protocole SNMP

Le protocole SNMP peut être utilisé pour effectuer des modifications de configuration sur les routeurs et les commutateurs Catalyst semblables à celles effectuées avec l'interface de ligne de commande. Des mesures de sécurité appropriées doivent être configurées sur les périphériques réseau afin d'empêcher tout accès non autorisé et toute modification par SNMP. Les chaînes de communauté doivent respecter les directives de mot de passe habituelles quant à la longueur, les caractères et la difficulté à deviner. Il est important de modifier les chaînes de communauté de leurs valeurs par défaut publiques et privées.

Tous les hôtes de gestion SNMP doivent avoir une adresse IP statique et se voir accorder des droits de communication SNMP explicites avec le périphérique réseau en fonction de cette adresse IP prédéfinie et de la liste de contrôle d'accès (ACL). Les logiciels Cisco IOS et Cisco Catalyst offrent des fonctionnalités de sécurité qui garantissent que seules les stations de gestion autorisées peuvent effectuer des modifications sur les périphériques réseau.

Fonctionnalités de sécurité du routeur

Niveau de privilège SNMP

Cette fonctionnalité limite les types d'opérations qu'une station de gestion peut exécuter sur un routeur. Il existe deux types de niveaux de privilège sur les routeurs : Lecture seule (RO) et lecture-écriture (RW). Le niveau RO permet uniquement à une station de gestion d'interroger les données du routeur. Il ne permet pas l'exécution de commandes de configuration comme le redémarrage d'un routeur et l'arrêt d'interfaces. Seul le niveau de privilège RW peut être utilisé pour effectuer ces opérations.

Liste de contrôle d'accès (ACL) de SNMP

La fonctionnalité de liste de contrôle d'accès de SNMP peut être utilisée conjointement avec la fonctionnalité de privilège de SNMP pour limiter la demande d'informations de gestion de stations de gestion précises.

Vue SNMP

Cette fonctionnalité limite la récupération d'informations précises des routeurs par les stations de gestion. Elle peut être utilisée avec les fonctionnalités de niveau de privilège SNMP et de liste de contrôle d'accès pour restreindre l'accès aux données par les consoles de gestion. Pour des exemples de configuration de la vue SNMP, allez à la page snmp-server view.

SNMP Version 3

La version 3 du protocole SNMP (SNMPv3) permet des échanges de données de gestion sécurisés entre les périphériques réseau et les stations de gestion. Les fonctionnalités de chiffrement et d'authentification du protocole SNMPv3 offrent une sécurité élevée lors du transport des paquets vers une console de gestion. Le protocole SNMPv3 est pris en charge dans la version 12.0(3)T du logiciel Cisco IOS et ses versions ultérieures. Pour obtenir une présentation

technique du protocole SNMPv3, consultez la documentation sur SNMPv3.

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

La fonctionnalité de liste de contrôle d'accès fournit des mesures de sécurité visant à prévenir les attaques comme la mystification d'adresses IP. La liste de contrôle d'accès peut être appliquée aux interfaces entrantes ou sortantes sur les routeurs.

Fonctionnalité de sécurité du commutateur de réseau local Catalyst

Liste d'autorisation d'adresses IP

La fonctionnalité de liste d'autorisation d'adresses IP limite les accès entrants au commutateur par Telnet et SNMP à partir d'adresses IP source non autorisées. Les messages de journal système et les interruptions SNMP sont pris en charge pour aviser un système de gestion lorsqu'il y a une violation ou un accès non autorisé.

Une combinaison des fonctionnalités de sécurité de Cisco IOS peut être utilisée pour gérer les routeurs et les commutateurs Catalyst. Il est nécessaire de mettre en place une politique de sécurité qui limite le nombre de stations de gestion capables d'accéder aux commutateurs et aux routeurs.

Pour en savoir plus sur l'amélioration de la sécurité sur les réseaux IP, consultez le document Amélioration de la sécurité sur les réseaux IP.

Gestion de la comptabilité

La gestion de comptabilité est le processus utilisé pour mesurer les paramètres d'utilisation du réseau afin que les utilisateurs individuels ou les groupes d'utilisateurs sur le réseau puissent être régis de manière appropriée aux fins de comptabilité ou de remboursement. Comme pour la gestion des performances, la première étape vers une gestion de la comptabilité appropriée consiste à mesurer l'utilisation de toutes les ressources réseau importantes. L'utilisation des ressources réseau peut être mesurée à l'aide de Cisco NetFlow et des fonctionnalités de gestion de la comptabilité IP de Cisco. L'analyse des données obtenues grâce à ces méthodes permet d'obtenir un aperçu des tendances d'utilisation actuelles.

Un système de comptabilité et de facturation basé sur l'utilisation est un élément essentiel de tout contrat de niveau de service (SLA). Il fournit un moyen pratique de définir des obligations dans le cadre d'un SLA et des conséquences claires pour des comportements qui ne font pas partie des conditions du contrat de niveau de service.

Les données peuvent être collectées par des sondes ou par Cisco NetFlow. Cisco offre les applications NetFlow Collector et NetFlow Analyzer pour collecter et analyser les données des routeurs et des commutateurs Catalyst. Des applications de partagiciel comme cflowd sont également utilisées pour collecter les données de NetFlow. Mesurer continuellement l'utilisation des ressources peut générer des informations pour la facturation, ainsi que des informations pour évaluer les ressources justes et optimales. Voici quelques exemples de solutions de gestion de la comptabilité souvent déployées :

- le logiciel Evident

Stratégie d'activation et de collecte des données de NetFlow

NetFlow (flux de réseau) est une technologie de mesure d'entrées qui permet de capturer les données requises pour les applications de planification, de surveillance et de comptabilité du réseau. NetFlow doit être déployé sur les interfaces des routeurs de périphérie et d'agrégation pour les fournisseurs de services ou sur les interfaces de routeur d'accès WAN pour les entreprises clientes.

Cisco Systems recommande un déploiement de NetFlow soigneusement planifié avec activation des services NetFlow sur ces routeurs stratégiquement situés. NetFlow peut être déployé par incréments (interface par interface) et de manière stratégique (sur des routeurs bien choisis), plutôt que d'être sur chaque routeur du réseau. Le personnel Cisco collaborera avec les clients pour déterminer sur quels routeurs et interfaces clés NetFlow doit être activé en fonction des tendances de flux de trafic, de la topologie du réseau et de l'architecture du client.

Les principales considérations relatives au déploiement sont les suivantes :

- Les services NetFlow doivent être utilisés en tant qu'outil d'accélération des performances de la liste de contrôle et de mesures de la périphérie et ne doivent pas être activés sur des routeurs d'infrastructure ou dorsaux *très utilisés* ou des routeurs ayant des taux d'utilisation de CPU très élevés.
- Comprendre les exigences liées à la collecte de données effectuée par des applications. Les applications de comptabilité peuvent ne nécessiter que des informations sur les flux des routeurs de départ et d'arrivée, tandis que les applications de surveillance peuvent nécessiter une vue de bout en bout plus complète (qui est plus exigeante en données).
- Comprendre les effets de la topologie du réseau et de la politique de routage sur la stratégie de collecte des flux. Par exemple, évitez de collecter des flux en double en activant NetFlow sur des routeurs d'agrégation clés d'où le trafic provient ou où il se termine, et non sur les routeurs d'infrastructure ou les routeurs intermédiaires qui fourniraient des vues en double des mêmes informations de flux.
- Les fournisseurs de services dans le domaine du *transport de transit (transportant du trafic dont ni l'origine ni la destination ne se trouve sur leur réseau) peuvent utiliser les données de l'exportation NetFlow pour mesurer l'utilisation des ressources réseau aux fins de comptabilité et de facturation.*

Configuration de la comptabilité IP

La prise en charge de la comptabilité IP de Cisco fournit des fonctionnalités de comptabilité IP de base. En activant la comptabilité IP, les utilisateurs peuvent voir le nombre d'octets et de paquets commutés par le logiciel Cisco IOS par adresse IP d'origine et de destination. Seul le trafic IP de transit est mesuré, et ce uniquement par sortie. Le trafic généré par le logiciel ou dont le logiciel est la destination n'est pas inclus dans les statistiques de la comptabilité. Pour conserver des totaux de comptabilité précis, le logiciel gère deux bases de données de comptabilité : une base de données active et une base de données à points de contrôle.

La prise en charge de la comptabilité IP de Cisco fournit également des informations qui identifient le trafic IP qui a échoué l'authentification par listes d'accès IP. L'identification des adresses IP source qui enfreignent les listes d'accès IP permet le signalement de possibles tentatives de brèches de sécurité. Les données indiquent également si les configurations de la liste d'accès IP doivent être vérifiées. Pour mettre cette fonctionnalité à la disposition des utilisateurs, activez la

comptabilité IP des violations de liste d'accès à l'aide de la commande **ip accounting access-violations.** Les utilisateurs pourront ensuite afficher le nombre d'octets et de paquets provenant d'une source unique qui tente de violer la sécurité en utilisant la liste d'accès de la paire source-destination. Par défaut, la comptabilité IP affiche le nombre de paquets qui ont été authentifiés par des listes d'accès et qui ont été acheminés.

Pour activer la comptabilité IP, utilisez l'une des commandes suivantes pour chaque interface en mode de configuration d'interface :

Commande	Objectif
ip accounting	Active la comptabilité IP de base.
ip accounting access violations	Active la comptabilité IP avec la capacité d'identifier le trafic IP qui échoue l'authentification par des listes d'accès IP.

Pour configurer d'autres fonctionnalités de la comptabilité IP, utilisez une ou plusieurs des commandes suivantes en mode de configuration globale :

Commande	Objectif
ip accounting-threshold *threshold*	Définit le nombre maximal d'entrées de comptabilité à créer.
ip accounting-list *ip-address wildcard*	Filtre les informations de comptabilité des hôtes.
ip accounting-transits *count*	Contrôle le nombre d'enregistrements de transit qui seront stockés dans la base de données de la comptabilité IP.

Reportez-vous aux conventions des conseils techniques Cisco pour connaître les conventions utilisées dans ce document.