Livre blanc sur les pratiques recommandées en matière de processus de référence

Table des matières

[Introduction](#)
[Ligne De Base](#)
[Qu'est-ce qu'une planification initiale ?](#)
[Pourquoi une planification initiale ?](#)
[Objectif De Base](#)
[Organigramme de base](#)
[Procédure De Base](#)
[Étape 1 : Compiler un inventaire du matériel, des logiciels et de la configuration](#)
[Étape 2 : Vérifiez que la MIB SNMP est prise en charge dans le routeur](#)
[Étape 3 : Interroger et enregistrer un objet MIB SNMP spécifique à partir du routeur](#)
[Étape 4 : Analyser les données pour déterminer les seuils](#)
[Étape 5 : Résolution des problèmes immédiats identifiés](#)
[Étape 6 : Surveillance du seuil de test](#)
[Étape 7 : Implémenter la surveillance des seuils via SNMP ou RMON](#)
[Bases MIB supplémentaires](#)
[MIB de routeur](#)
[MIB des commutateurs Catalyst](#)
[MIB de liaison série](#)
[Commandes de configuration d'alarme et d'événement RMON](#)
[Alarmes](#)
[Événements](#)
[Mise en œuvre d’alarmes et d’événements RMON](#)
[Informations connexes](#)

Introduction

Ce document décrit des concepts et des procédures d'établissement des références pour les réseaux hautement disponibles. Il inclut des facteurs de succès capital pour la création de bases du réseau et le seuillage pour aider à évaluer le succès. Il fournit également le détail significatif pour des processus de spécification de base et de seuil et la mise en oeuvre qui suivent les indications de pratique recommandée identifiées par l'équipe de service de haute disponibilité de Cisco (HAS).

Ce document vous guide pas à pas dans le processus de planification initiale. Certains produits NMS (Network Management System) actuels peuvent vous aider à automatiser ce processus. Toutefois, le processus de planification initiale reste le même, que vous utilisiez des outils automatisés ou manuels. Si vous utilisez ces produits NMS, vous devez ajuster les paramètres de

seuil par défaut pour votre environnement réseau unique. Il est important d'avoir un processus pour choisir intelligemment ces seuils afin qu'ils soient significatifs et corrects.

Ligne De Base

Qu'est-ce qu'une planification initiale ?

Une ligne de base est un processus permettant d'étudier le réseau à intervalles réguliers afin de s'assurer qu'il fonctionne comme prévu. Il s'agit de plus d'un rapport détaillant l'état du réseau à un moment donné. En suivant le processus de planification initiale, vous pouvez obtenir les informations suivantes :

- Obtenir des informations précieuses sur l'état du matériel et des logiciels
- Déterminer l'utilisation actuelle des ressources réseau
- Prendre des décisions précises concernant les seuils d'alarme réseau
- Identifier les problèmes réseau actuels
- Prévoir les problèmes futurs

Le schéma suivant illustre une autre façon d'examiner la ligne de base.

La ligne rouge, le point d'interruption du réseau, est le point auquel le réseau se rompt, déterminé par la connaissance des performances matérielles et logicielles. La ligne verte, la charge réseau, est la progression naturelle de la charge sur le réseau à mesure que de nouvelles applications sont ajoutées, et d'autres facteurs de ce type.

L'objectif d'une ligne de base est de déterminer :

- Emplacement de votre réseau sur la ligne verte
- Vitesse à laquelle la charge réseau augmente
- Espérons prédire à quel moment les deux vont se croiser

En effectuant régulièrement une planification initiale, vous pouvez connaître l'état actuel et extrapoler le moment où les défaillances se produiront, puis vous préparer à ces défaillances à l'avance. Cela vous aide également à prendre des décisions plus avisées sur le moment, l'endroit et la manière de dépenser l'argent du budget pour les mises à niveau du réseau.

Pourquoi une planification initiale ?

Un processus de référence vous aide à identifier et à planifier correctement les problèmes critiques de limitation des ressources sur le réseau. Ces problèmes peuvent être décrits comme des ressources de plan de contrôle ou des ressources de plan de données. Les ressources du plan de contrôle sont propres à la plate-forme et aux modules spécifiques du périphérique et peuvent être affectées par un certain nombre de problèmes, notamment :

- Utilisation des données
- Fonctionnalités activées
- Conception réseau

Les ressources du plan de contrôle incluent des paramètres tels que :

- Utilisation du processeur
- Utilisation de la mémoire
- Utilisation du tampon

Les ressources du plan de données sont affectées uniquement par le type et la quantité de trafic et incluent l'utilisation de la liaison et l'utilisation du fond de panier. En basant l'utilisation des ressources sur les zones critiques, vous pouvez éviter de graves problèmes de performances, ou pire, une panne du réseau.

Avec l'introduction d'applications sensibles à la latence, telles que la voix et la vidéo, la planification initiale est plus importante que jamais. Les applications traditionnelles TCP/IP (Transmission Control Protocol/Internet Protocol) sont pardonnantes et permettent un certain délai. La voix et la vidéo sont basées sur le protocole UDP (User Datagram Protocol) et ne permettent pas les retransmissions ou l'encombrement du réseau.

En raison de la nouvelle combinaison d'applications, la planification initiale vous aide à comprendre les problèmes d'utilisation des ressources du plan de contrôle et du plan de données et à planifier de manière proactive les modifications et les mises à niveau pour garantir une réussite continue.

Les réseaux de données existent depuis de nombreuses années. Jusqu’à récemment, le maintien du fonctionnement des réseaux était un processus relativement indulgent, avec une certaine marge d’erreur. Avec l'acceptation croissante des applications sensibles à la latence, telles que la voix sur IP (VoIP), le travail d'exécution du réseau devient de plus en plus difficile et nécessite plus de précision. Afin d’être plus précis et de fournir à un administrateur réseau une base solide sur laquelle gérer le réseau, il est important d’avoir une idée de la façon dont le réseau fonctionne. Pour ce faire, vous devez passer par un processus appelé planification initiale.

Objectif De Base

L'objectif d'une ligne de base est de :

1. Déterminer l'état actuel des périphériques réseau
2. Comparer cet état aux directives de performances standard
3. Définissez des seuils pour vous avertir lorsque l'état dépasse ces consignes

En raison de la quantité importante de données et du temps nécessaire à leur analyse, vous devez d'abord limiter la portée d'une planification initiale pour faciliter l'apprentissage du

processus. Le point de départ le plus logique, et parfois le plus avantageux, est le coeur du réseau. Cette partie du réseau est généralement la plus petite et nécessite la plus grande stabilité.

Dans un souci de simplicité, ce document explique comment établir une base de référence pour une base d'informations SNMP MIB (Simple Network Management Protocol Management Information Base) très importante : cpmCPUTotal5min. cpmCPUTotal5min est la moyenne décroissante sur cinq minutes de l'unité centrale (UC) d'un routeur Cisco. Il s'agit d'un indicateur de performance du plan de contrôle. La ligne de base sera exécutée sur un routeur de la gamme Cisco 7000.

Une fois que vous avez appris le processus, vous pouvez l'appliquer à toutes les données disponibles dans la vaste base de données SNMP qui est disponible dans la plupart des périphériques Cisco, tels que :

- Utilisation du réseau numérique à intégration de services (RNIS)
- Perte de cellules en mode ATM (Asynchronous Transfer Mode)
- Mémoire système disponible

Organigramme de base

L'organigramme suivant présente les étapes de base du processus de planification initiale. Bien que des produits et des outils soient disponibles pour effectuer certaines de ces étapes pour vous, ils ont tendance à présenter des lacunes en termes de flexibilité ou de facilité d'utilisation. Même si vous prévoyez d'utiliser les outils NMS (Network Management System) pour effectuer la planification initiale, il s'agit d'un bon exercice pour étudier le processus et comprendre le fonctionnement réel de votre réseau. Ce processus peut également résoudre le mystère du fonctionnement de certains outils NMS, car la plupart des outils font essentiellement la même chose.

Procédure De Base

Étape 1 : Compiler un inventaire du matériel, des logiciels et de la configuration

Il est extrêmement important de dresser un inventaire du matériel, des logiciels et de la configuration pour plusieurs raisons. Premièrement, les MIB SNMP Cisco sont, dans certains cas, spécifiques à la version de Cisco IOS que vous exécutez. Certains objets MIB sont remplacés par de nouveaux ou sont, parfois, complètement éliminés. L'inventaire matériel est le plus important après la collecte des données, car les seuils que vous devez définir après la ligne de base initiale sont souvent basés sur le type de processeur, la quantité de mémoire, etc., sur les périphériques Cisco. L'inventaire des configurations est également important pour vous assurer de connaître les configurations actuelles : Vous pouvez modifier les configurations des périphériques après votre ligne de base pour régler les tampons, etc.

La façon la plus efficace de réaliser cette partie de la ligne de base d’un réseau Cisco est avec CiscoWorks2000 Resource Manager Essentials (Essentials). Si ce logiciel est correctement

installé sur le réseau, Essentials doit disposer des inventaires actuels de tous les périphériques dans sa base de données. Il suffit de regarder les inventaires pour voir s'il y a des problèmes.

Le tableau suivant est un exemple de rapport d'inventaire logiciel Cisco Router Class exporté depuis Essentials, puis modifié dans Microsoft Excel. À partir de cet inventaire, notez que vous devez utiliser les données MIB SNMP et les identificateurs d'objet (OID) trouvés dans les versions 12.0x et 12.1x de Cisco IOS.

Nom du périphérique	Type de routeur	Version	Version du logiciel
field-2500a.embu-mlab.cisco.com	Cisco 2511	L	12.1(1)
qdm-7200.embu-mlab.cisco.com	Cisco 7204	B	12.1(1)E
voip-3640.embu-mlab.cisco.com	Cisco 3640	0x00	12.0(3c)
wan-1700a.embu-mlab.cisco.com	Cisco 1720	0x101	12.1(4)
wan-2500a.embu-mlab.cisco.com	Cisco 2514	L	12.0(1)
wan-3600a.embu-mlab.cisco.com	Cisco 3640	0x00	12.1(3)
wan-7200a.embu-mlab.cisco.com	Cisco 7204	B	12.1(1)E
172.16.71.80	Cisco 7204	B	12.0(5 T)

Si Essentials n'est pas installé sur le réseau, vous pouvez utiliser l'outil de ligne de commande UNIX snmpwalk à partir d'une station de travail UNIX pour rechercher la version de l'IOS. Ceci est illustré dans l'exemple suivant. Si vous n'êtes pas sûr du fonctionnement de cette commande, tapez man snmpwalk à l'invite UNIX pour plus d'informations. La version de l'IOS est importante dans lorsque vous commencez à choisir les OID de MIB à la ligne de base, car les objets de MIB dépendent de l'IOS. Notez également qu'en connaissant le type de routeur, vous pourrez déterminer ultérieurement quels seuils doivent être définis pour le processeur, les tampons, etc.

```
nsahpov6% snmpwalk -v1 -c private 172.16.71.80 system
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-JS-M), Version 12.0(5)T, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 23-Jul-2001 23:02 by kpma
system.sysObjectID.0 : OBJECT IDENTIFIER:
.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.cisco7204
```

Étape 2 : Vérifiez que la MIB SNMP est prise en charge dans le routeur

Maintenant que vous disposez d'un inventaire de l'appareil que vous souhaitez interroger pour votre ligne de base, vous pouvez commencer à choisir les OID spécifiques que vous souhaitez interroger. Cela vous évite beaucoup de frustration si vous vérifiez à l'avance que les données que vous voulez sont bien là. L'objet cpmCPUTotal5min MIB se trouve dans la base de données CISCO-PROCESS-MIB.

Pour trouver l'OID que vous souhaitez interroger, vous devez disposer d'une table de conversion disponible sur le site Web CCO de Cisco. Pour accéder à ce site Web à partir d'un navigateur Web, accédez à la page MIB Cisco, puis cliquez sur le lien OIDs.

Pour accéder à ce site Web à partir d'un serveur FTP, tapez ftp://ftp.cisco.com/pub/mibs/oid/. À partir de ce site, vous pouvez télécharger la MIB spécifique qui a été décodée et triée par numéros d'OID.

L'exemple suivant est extrait de la table CISCO-PROCESS-MIB.oid. Cet exemple montre que l'OID pour la MIB cpmCPUTotal5min est .1.3.6.1.4.1.9.9.109.1.1.1.1.5.

Remarque : n'oubliez pas d'ajouter un "." au début de l'OID ou une erreur s'affiche lorsque vous essayez de l'interroger. Vous devez également ajouter un ".1" à la fin de l'OID pour l'instancier. Cela indique au périphérique l'instance de l'OID que vous recherchez. Dans certains cas, les OID ont plusieurs instances d'un type de données particulier, par exemple lorsqu'un routeur a plusieurs CPU.

<#root>

```
ftp://ftp.cisco.com/pub/mibs/oid/CISCO-PROCESS-MIB.oid
### THIS FILE WAS GENERATED BY MIB2SCHEMA
"org" "1.3"
"dod" "1.3.6"
"internet" "1.3.6.1"
"directory" "1.3.6.1.1"
"mgmt" "1.3.6.1.2"
"experimental" "1.3.6.1.3"
"private" "1.3.6.1.4"
"enterprises" "1.3.6.1.4.1"
"cisco" "1.3.6.1.4.1.9"
"ciscoMgmt" "1.3.6.1.4.1.9.9"
"ciscoProcessMIB" "1.3.6.1.4.1.9.9.109"
"ciscoProcessMIBObjects" "1.3.6.1.4.1.9.9.109.1"
"ciscoProcessMIBNotifications" "1.3.6.1.4.1.9.9.109.2"
"ciscoProcessMIBConformance" "1.3.6.1.4.1.9.9.109.3"
"cpmCPU" "1.3.6.1.4.1.9.9.109.1.1"
"cpmProcess" "1.3.6.1.4.1.9.9.109.1.2"
"cpmCPUTotalTable" "1.3.6.1.4.1.9.9.109.1.1.1"
"cpmCPUTotalEntry" "1.3.6.1.4.1.9.9.109.1.1.1.1"
"cpmCPUTotalIndex" "1.3.6.1.4.1.9.9.109.1.1.1.1.1"
"cpmCPUTotalPhysicalIndex" "1.3.6.1.4.1.9.9.109.1.1.1.1.2"
"cpmCPUTotal5sec" "1.3.6.1.4.1.9.9.109.1.1.1.1.3"
"cpmCPUTotal1min" "1.3.6.1.4.1.9.9.109.1.1.1.1.4"

"cpmCPUTotal5min" "1.3.6.1.4.1.9.9.109.1.1.1.1.5"
```

Il existe deux façons courantes d'interroger l'OID de la MIB pour s'assurer qu'il est disponible et qu'il fonctionne. Il est judicieux de procéder de la sorte avant de commencer la collecte de données en masse, afin de ne pas perdre de temps à interroger un élément qui n'est pas présent et de vous retrouver avec une base de données vide. Pour ce faire, vous pouvez utiliser une fonction de recherche MIB de votre plate-forme NMS, telle que HP OpenView Network Node Manager (NNM) ou CiscoWorks Windows, et saisir l'OID que vous souhaitez vérifier.

L'exemple suivant est un exemple de HP OpenView SNMP MIB walker.

Une autre façon simple d'interroger l'OID de la MIB est d'utiliser la commande UNIX snmpwalk comme indiqué dans l'exemple suivant.

```
nsahpov6% cd /opt/OV/bin
nsahpov6% snmpwalk -v1 -c private 172.16.71.80 .1.3.6.1.4.1.9.9.109.1.1.1.1.5.1

cisco.ciscoMgmt.ciscoProcessMIB.ciscoProcessMIBObjects.cpmCPU.cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUT
```

Dans les deux exemples, la MIB a renvoyé une valeur de 0, ce qui signifie que pour ce cycle d'interrogation, le processeur a utilisé en moyenne 0 %. Si vous rencontrez des difficultés pour que le périphérique réponde avec les données correctes, essayez d'envoyer une requête ping au périphérique et d'accéder au périphérique via Telnet. Si vous rencontrez toujours un problème, vérifiez la configuration SNMP et les chaînes de communauté SNMP. Vous devrez peut-être trouver une autre MIB ou une autre version d'IOS pour que cela fonctionne.

Étape 3 : Interroger et enregistrer un objet MIB SNMP spécifique à partir du routeur

Il existe plusieurs façons d'interroger des objets MIB et d'enregistrer le résultat. Des produits prêts à l'emploi, des logiciels partagés, des scripts et des outils de fournisseurs sont disponibles. Tous les outils frontaux utilisent le processus SNMP get pour obtenir les informations. Les principales différences résident dans la souplesse de la configuration et dans la manière dont les données sont enregistrées dans une base de données. Examinez à nouveau la MIB du processeur pour voir comment ces différentes méthodes fonctionnent.

Maintenant que vous savez que l'OID est pris en charge par le routeur, vous devez décider de la fréquence d'interrogation et d'enregistrement. Cisco recommande d'interroger la base MIB du processeur toutes les cinq minutes. Un intervalle plus faible augmenterait la charge sur le réseau ou le périphérique, et comme la valeur MIB est une moyenne de cinq minutes, il ne serait pas utile de l'interroger plus souvent que la valeur moyenne. Il est également généralement recommandé que l'interrogation de la ligne de base ait au moins une période de deux semaines afin que vous puissiez analyser au moins deux cycles d'activité hebdomadaires sur le réseau.

Les écrans suivants vous montrent comment ajouter des objets MIB avec HP OpenView Network Node Manager version 6.1. Dans l'écran principal, sélectionnez Options > Data Collection & Thresholds.

Sélectionnez ensuite Edit > Add > MIB Objects.

Dans le menu, ajoutez la chaîne OID et cliquez sur Apply. Vous venez d'entrer l'objet MIB dans la plate-forme HP OpenView afin qu'il puisse être interrogé.

Vous devez ensuite indiquer à HP OpenView quel routeur interroger pour cet OID.

Dans le menu Data Collection, sélectionnez Edit > Add > MIB Collections.

Dans le champ Source, saisissez le nom DNS (Domain Naming System) ou l'adresse IP du routeur à interroger.

Sélectionnez Store, No Thresholds dans la liste Set Collection Mode.

Réglez l'intervalle d'interrogation sur 5m, pour des intervalles de cinq minutes.

Cliquez sur Apply.

Vous devez sélectionner File > Save pour que les modifications prennent effet.

Pour vérifier que la collecte est correctement configurée, mettez en surbrillance la ligne récapitulative de collecte pour le routeur et sélectionnez Actions > Test SNMP. Ceci vérifie si la chaîne de communauté est correcte et interroge toutes les instances de l'OID.

Cliquez sur Fermer, et laissez la collection s'exécuter pendant une semaine. À la fin de la période hebdomadaire, extraire les données pour analyse.

Les données sont plus facilement analysées si vous les videz dans un fichier ASCII et que vous les importez dans un tableur tel que Microsoft Excel. Pour ce faire avec HP OpenView NNM, vous pouvez utiliser l'outil de ligne de commande, snmpColDump. Chaque collection configurée écrit dans un fichier du répertoire /var/opt/OV/share/database/snmpCollect/.

Extrayez les données dans un fichier ASCII appelé testfile avec la commande suivante :

<#root>

```
snmpColDump /var/opt/OV/share/databases/snmpCollect/cpmCPUTotal5min.1 >
```

testfile

Remarque : cpmCPUTotal5min.1 est le fichier de base de données créé par HP OpenView NNM au début de l'interrogation OID.

Le fichier de test généré est similaire à l'exemple suivant.

```
03/01/2001 14:09:10 nsa-gw.cisco.com 1
03/01/2001 14:14:10 nsa-gw.cisco.com 1
03/01/2001 14:19:10 nsa-gw.cisco.com 1
03/01/2001 14:24:10 nsa-gw.cisco.com 1
```

```
03/01/2001 14:29:10 nsa-gw.cisco.com 1
03/01/2001 14:34:10 nsa-gw.cisco.com 1
03/01/2001 14:39:10 nsa-gw.cisco.com 1
03/01/2001 14:44:10 nsa-gw.cisco.com 1
03/01/2001 14:49:10 nsa-gw.cisco.com 1
03/01/2001 14:54:10 nsa-gw.cisco.com 1
03/01/2001 14:59:10 nsa-gw.cisco.com 1
03/……
```

Une fois que le fichier de test est sorti sur votre station UNIX, vous pouvez le transférer sur votre PC à l'aide du protocole FTP (File Transfer Protocol).

Vous pouvez également collecter les données à l'aide de vos propres scripts. Pour ce faire, exécutez un snmpget pour l'OID du processeur toutes les cinq minutes et videz les résultats dans un fichier .csv.

Étape 4 : Analyser les données pour déterminer les seuils

Maintenant que vous avez des données, vous pouvez commencer à les analyser. Cette phase de la ligne de base détermine les paramètres de seuil que vous pouvez utiliser pour mesurer précisément les performances ou les pannes et ne déclenchera pas trop d'alarmes lorsque vous activerez la surveillance des seuils. Pour ce faire, l'une des méthodes les plus simples consiste à importer les données dans une feuille de calcul telle que Microsoft Excel et à tracer un graphique en nuages de points. Cette méthode permet de voir très facilement combien de fois un périphérique particulier aurait créé une alerte d'exception si vous la surveilliez pour un certain seuil. Il n'est pas recommandé d'activer les seuils sans effectuer de ligne de base, car cela peut créer des tempêtes d'alerte à partir des périphériques qui ont dépassé le seuil que vous avez choisi.

Pour importer le fichier de test dans une feuille de calcul Excel, ouvrez Excel et sélectionnez Fichier > Ouvrir et sélectionnez votre fichier de données.

L'application Excel vous invite ensuite à importer le fichier.

Lorsque vous avez terminé, le fichier importé doit ressembler à l'écran suivant.

Un graphique à nuages de points vous permet de visualiser plus facilement le fonctionnement des différents paramètres de seuil sur le réseau.

Pour créer le graphique en nuages de points, mettez en surbrillance la colonne C dans le fichier importé, puis cliquez sur l'icône Assistant Graphique. Suivez ensuite les étapes de l'Assistant Graphique pour créer un graphique à nuages de points.

À l'étape 1 de l'Assistant Graphique, comme indiqué ci-dessous, sélectionnez l'onglet Types standard, puis sélectionnez le type de graphique XY (nuage de points). Cliquez ensuite sur Next.

Dans l'étape 2 de l'Assistant Graphique, comme indiqué ci-dessous, sélectionnez l'onglet Plage de données et sélectionnez la plage de données et l'option Colonnes. Cliquez sur Next (Suivant).

À l'étape 3 de l'Assistant Graphique, comme indiqué ci-dessous, entrez le titre du graphique et les valeurs des axes X et Y, puis cliquez sur Suivant.

À l'étape 4 de l'Assistant Graphique, sélectionnez si vous voulez que le graphique en nuages de points apparaisse sur une nouvelle page ou en tant qu'objet dans la page existante.

Cliquez sur Terminer pour placer le graphique à l'emplacement souhaité.

"Et si ?" Analyse

Vous pouvez maintenant utiliser le graphique en nuages de points pour l'analyse. Toutefois, avant de continuer, vous devez vous poser les questions suivantes :

- Que recommande le fournisseur (dans cet exemple, le fournisseur est Cisco) comme seuil pour cette variable MIB ?

  En général, Cisco recommande qu'un routeur principal n'utilise pas plus de 60 % du processeur en moyenne. Soixante pour cent ont été choisis parce qu'un routeur a besoin d'une surcharge en cas de problème ou de défaillance du réseau. Cisco estime qu'un routeur principal a besoin d'environ 40 % de surcharge CPU au cas où un protocole de routage doit recalculer ou reconverger. Ces pourcentages varient en fonction des protocoles utilisés, de la topologie et de la stabilité de votre réseau.

- Que faire si j'utilise 60 % comme paramètre de seuil ?

  Si vous tracez une ligne horizontale de 60 sur le graphique en nuages de points, vous constaterez qu'aucun des points de données ne dépasse 60 % d'utilisation du processeur. Ainsi, un seuil de 60 défini sur vos stations NMS (Network Management System) n'aura pas déclenché d'alarme de seuil pendant la période d'interrogation. Un pourcentage de 60 est acceptable pour ce routeur. Cependant, notez dans le graphique en nuages de points que certains points de données sont proches de 60. Il serait intéressant de savoir quand un routeur approche le seuil de 60 % afin de savoir à l'avance que le processeur approche 60 % et d'avoir un plan pour ce qu'il doit faire lorsqu'il atteint ce point.

- Que faire si je fixe le seuil à 50 % ?

  On estime que ce routeur a atteint 50 % d'utilisation quatre fois au cours de ce cycle d'interrogation et qu'il aurait généré une alarme de seuil à chaque fois. Ce processus devient plus important lorsque vous examinez des groupes de routeurs pour voir ce que les différents paramètres de seuil feraient. Par exemple, « Et si je définissais le seuil à 50 % pour l'ensemble du réseau principal ? » Vous voyez, il est très difficile de choisir un seul numéro.

Analyse de simulation du seuil du processeur

La méthodologie de seuil Prêt, défini et activé est une stratégie que vous pouvez utiliser pour faciliter la tâche. Cette méthodologie utilise trois nombres de seuils successifs.

- Prêt : le seuil que vous définissez comme prédicteur des périphériques qui nécessiteront

probablement une attention particulière à l'avenir

- Set : seuil utilisé comme indicateur précoce, qui vous avertit de commencer à planifier une réparation, une reconfiguration ou une mise à niveau
- Go : le seuil que vous et/ou le fournisseur considérez comme une condition de panne et qui nécessite une action pour la réparer ; dans cet exemple, il est de 60 %

Le tableau suivant présente la stratégie de la stratégie Prêt, défini, activé.

Seuil	Action	Résultat
45 %	Étudier plus en détail	Liste des options pour les plans d'action
50 %	Formuler un plan d'action	Liste des étapes du plan d'action
60 %	Mettre en oeuvre le plan	Le routeur ne dépasse plus les seuils. Revenir au mode Prêt

La méthodologie Ready, Set, Go modifie le graphique de base d'origine évoqué précédemment. Le schéma suivant illustre le graphique de la planification initiale modifiée. Si vous pouvez identifier les autres points d'intersection sur le graphique, vous avez maintenant plus de temps pour planifier et réagir qu'auparavant.

Notez que dans ce processus, l'attention se concentre sur les exceptions dans le réseau et ne se préoccupe pas des autres périphériques. On suppose que tant que les périphériques sont en dessous des seuils, ils fonctionnent correctement.

Si vous avez réfléchi à ces étapes dès le début, vous serez bien préparé pour maintenir le réseau en bonne santé. Ce type de planification est également extrêmement utile pour la planification budgétaire. Si vous connaissez vos cinq routeurs principaux, vos routeurs intermédiaires et vos routeurs inférieurs prêts, vous pouvez facilement planifier le budget dont vous aurez besoin pour les mises à niveau en fonction de leur type et des options de votre plan d'action. La même stratégie peut être utilisée pour les liaisons de réseau étendu (WAN) ou tout autre OID de MIB.

Étape 5 : Résolution des problèmes immédiats identifiés

C'est l'une des parties les plus faciles du processus de planification initiale. Une fois que vous avez identifié les périphériques qui dépassent le seuil d'aller, vous devez élaborer un plan d'action pour les ramener sous ce seuil.

Vous pouvez ouvrir un dossier auprès du centre d'assistance technique de Cisco (TAC) ou contacter votre ingénieur système pour connaître les options disponibles. Vous ne devez pas supposer que le fait de ramener les choses sous le seuil vous coûtera de l'argent. Certains problèmes liés au processeur peuvent être résolus en modifiant la configuration afin de garantir que tous les processus s'exécutent de la manière la plus efficace possible. Par exemple, certaines listes de contrôle d'accès (ACL) peuvent faire fonctionner le processeur d'un routeur très haut en

raison du chemin emprunté par les paquets via le routeur. Dans certains cas, vous pouvez implémenter la commutation NetFlow pour modifier le chemin de commutation de paquets et réduire l'impact de la liste de contrôle d'accès sur le processeur. Quels que soient les problèmes, il est nécessaire de ramener tous les routeurs sous le seuil dans cette étape afin que vous puissiez implémenter les seuils plus tard sans risque d'inonder les stations NMS avec trop d'alarmes de seuil.

Étape 6 : Surveillance du seuil de test

Cette étape consiste à tester les seuils dans les travaux pratiques à l'aide des outils que vous utiliserez dans le réseau de production. Il existe deux approches communes pour la surveillance des seuils. Vous devez choisir la méthode la mieux adaptée à votre réseau.

- Méthode d'interrogation et de comparaison utilisant une plate-forme SNMP ou un autre outil de surveillance SNMP

  Cette méthode utilise davantage de bande passante réseau pour interroger le trafic et exécute des cycles de traitement sur votre plate-forme SNMP.

- Utiliser les configurations d'alarmes et d'événements RMON (surveillance à distance) dans les routeurs afin qu'ils envoient une alerte uniquement lorsqu'un seuil est dépassé

  Cette méthode réduit l'utilisation de la bande passante réseau, mais augmente également l'utilisation de la mémoire et du processeur sur les routeurs.

Implémentation d'un seuil via SNMP

Pour configurer la méthode SNMP à l'aide de HP OpenView NNM, sélectionnez Options > Data Collection & Thresholds comme vous l'avez fait lorsque vous avez configuré l'interrogation initiale. Cette fois, cependant, sélectionnez Store, Check Thresholds plutôt que Store, No Thresholds dans le menu collections. Après avoir défini le seuil, vous pouvez augmenter l'utilisation du processeur sur le routeur en lui envoyant plusieurs requêtes ping et/ou plusieurs marches SNMP. Vous devrez peut-être abaisser la valeur de seuil si vous ne pouvez pas forcer le processeur à dépasser le seuil. Dans tous les cas, vous devez vous assurer que le mécanisme de seuil fonctionne.

L'une des limites de cette méthode est que vous ne pouvez pas implémenter plusieurs seuils simultanément. Vous avez besoin de trois plates-formes SNMP pour définir trois seuils simultanés différents. Des outils tels que Concord Network Health et Trinagy TREND permettent plusieurs seuils pour la même instance OID.

Si votre système ne peut gérer qu'un seul seuil à la fois, vous pouvez envisager la stratégie Prêt, défini, activé en série. Autrement dit, lorsque le seuil prêt est atteint continuellement, commencez votre recherche et augmentez le seuil au niveau défini pour ce périphérique. Lorsque le niveau défini est atteint en permanence, commencez à formuler votre plan d'action et augmentez le seuil jusqu'au niveau go pour ce périphérique. Ensuite, lorsque le seuil d'aller est atteint en permanence, mettez en oeuvre votre plan d'action. Cela devrait fonctionner aussi bien que la méthode des trois seuils simultanés. La modification des paramètres de seuil de la plate-forme

SNMP prend simplement un peu plus de temps.

Implémentation d'un seuil à l'aide de RMON Alarm and Event

Grâce aux configurations d'événements et d'alarmes RMON, le routeur peut surveiller lui-même plusieurs seuils. Lorsque le routeur détecte une condition de dépassement de seuil, il envoie une interruption SNMP à la plate-forme SNMP. Un récepteur de déroutement SNMP doit être configuré dans la configuration de votre routeur pour que le déroutement soit transféré. Il existe une corrélation entre une alarme et un événement. L'alarme vérifie l'OID pour le seuil donné. Si le seuil est atteint, le processus d'alarme déclenche le processus d'événement qui peut soit envoyer un message de déroutement SNMP, soit créer une entrée de journal RMON, soit les deux. Pour plus de détails sur cette commande, consultez RMON Alarm and Event Configuration Commands.

Les commandes de configuration de routeur suivantes ont la commande router monitor cpmCPUTotal5min toutes les 300 secondes. Il déclenche l'événement 1 si le processeur dépasse 60 pour cent et déclenche l'événement 2 si le processeur tombe à 40 pour cent. Dans les deux cas, un message de déroutement SNMP est envoyé à la station NMS avec la chaîne privée community.

Pour utiliser la méthode Ready, Set, Go, utilisez toutes les instructions de configuration suivantes.

```
rmon event 1 trap private description "cpu hit60%" owner jharp
rmon event 2 trap private description "cpu recovered" owner jharp
rmon alarm 10 cpmCPUTotalTable.1.5.1 300 absolute rising 60 1 falling 40 2 owner jharp


rmon event 3 trap private description "cpu hit50%" owner jharp
rmon event 4 trap private description "cpu recovered" owner jharp
rmon alarm 20 cpmCPUTotalTable.1.5.1 300 absolute rising 50 3 falling 40 4 owner jharp

rmon event 5 trap private description "cpu hit 45%" owner jharp
rmon event 6 trap private description "cpu recovered" owner jharp
rmon alarm 30 cpmCPUTotalTable.1.5.1 300 absolute rising 45 5 falling 40 6 owner jharp
```

L'exemple suivant montre le résultat de la commande show rmon alarm qui a été configurée par les instructions ci-dessus.

<#root>

```
zack#

sh rmon alarm

Alarm 10 is active, owned by jharp
 Monitors cpmCPUTotalTable.1.5.1 every 300 second(s)
 Taking absolute samples, last value was 0
 Rising threshold is 60, assigned to event
1
 Falling threshold is 40, assigned to event
2
```

```
 On startup enable rising or falling alarm
Alarm 20 is active, owned by jharp
 Monitors cpmCPUTotalTable.1.5.1 every 300 second(s)
 Taking absolute samples, last value was 0
 Rising threshold is 50, assigned to event
3
 Falling threshold is 40, assigned to event
4
 On startup enable rising or falling alarm
Alarm 30 is active, owned by jharp
 Monitors cpmCPUTotalTable.1.5.1 every 300 second(s)
 Taking absolute samples, last value was 0
 Rising threshold is 45, assigned to event
5
 Falling threshold is 40, assigned to event
6
 On startup enable rising or falling alarm
```

L'exemple suivant montre le résultat de la commande show rmon event.

<#root>

zack#

sh rmon event

```
Event 1 is active, owned by jharp
 Description is cpu hit60%
 Event firing causes trap to community
private, last fired 00:00:00
Event 2 is active, owned by jharp
 Description is cpu recovered
 Event firing causes trap to community
private, last fired 02:40:29
Event 3 is active, owned by jharp
 Description is cpu hit50%
 Event firing causes trap to community
private, last fired 00:00:00
Event 4 is active, owned by jharp
 Description is cpu recovered
 Event firing causes trap to community
private, last fired 00:00:00
Event 5 is active, owned by jharp
 Description is cpu hit 45%
 Event firing causes trap to community
private, last fired 00:00:00
Event 6 is active, owned by jharp
 Description is cpu recovered
 Event firing causes trap to community
private, last fired 02:45:47
```

Vous pouvez essayer ces deux méthodes pour déterminer celle qui convient le mieux à votre environnement. Vous pouvez même trouver qu'une combinaison de méthodes fonctionne bien. Dans tous les cas, les tests doivent être effectués dans un environnement de laboratoire pour s'assurer que tout fonctionne correctement. Après avoir effectué les tests en laboratoire, un

déploiement limité sur un petit groupe de routeurs vous permettra de tester le processus d'envoi d'alertes à votre centre d'opérations.

Dans ce cas, vous devrez abaisser les seuils pour tester le processus : Il n'est pas recommandé d'essayer d'augmenter artificiellement le processeur sur un routeur de production. Vous devez également vous assurer que lorsque les alertes arrivent sur les stations NMS du Centre d'exploitation, il existe une politique de remontée pour vous assurer que vous êtes informé lorsque les périphériques dépassent les seuils. Ces configurations ont été testées en laboratoire avec Cisco IOS Version 12.1(7). Si vous rencontrez des problèmes, vous devez contacter les ingénieurs système ou d'ingénierie Cisco pour vérifier si vous avez un bogue dans votre version de l'IOS.

Étape 7 : Implémenter la surveillance des seuils via SNMP ou RMON

Une fois que vous avez testé en profondeur la surveillance des seuils dans les travaux pratiques et dans un déploiement limité, vous êtes prêt à mettre en oeuvre des seuils sur le réseau principal. Vous pouvez maintenant passer systématiquement par ce processus de base pour d'autres variables MIB importantes sur votre réseau, telles que les tampons, la mémoire libre, les erreurs de contrôle de redondance cyclique (CRC), la perte de cellules AMT, etc.

Si vous utilisez des configurations d'événements et d'alarmes RMON, vous pouvez désormais arrêter l'interrogation à partir de votre station NMS. Cela réduit la charge sur votre serveur NMS et la quantité de données d'interrogation sur le réseau. En suivant systématiquement ce processus pour identifier les indicateurs d'intégrité importants du réseau, vous pourriez facilement en arriver au point que l'équipement réseau se surveille lui-même à l'aide de la fonction RMON Alarm and Event.

Bases MIB supplémentaires

Après avoir appris ce processus, vous souhaiterez peut-être étudier d'autres bases MIB à planifier et à surveiller. Les sous-sections suivantes présentent une brève liste de certains OID et des descriptions qui peuvent vous être utiles.

MIB de routeur

Les caractéristiques de mémoire sont très utiles pour déterminer l'état d'un routeur. Un routeur sain doit presque toujours disposer d'un espace tampon pour fonctionner. Si le routeur commence à manquer d'espace tampon, le processeur devra travailler plus dur pour créer de nouveaux tampons et essayer de trouver des tampons pour les paquets entrants et sortants. Une discussion approfondie sur les tampons dépasse le cadre de ce document. Cependant, en règle générale, un routeur sain ne doit manquer que très peu de tampons, voire aucun, et ne doit pas présenter de défaillance de tampon, ou une condition de mémoire libre nulle.

Objet	Description	OID
PoolMémoireCiscoGratuit	Nombre d'octets du	1.3.6.1.4.1.9.9.48.1.1.1.6

	pool de mémoire actuellement inutilisés sur le périphérique géré	
PoolMémoireCiscoPlusGratuit	Le plus grand nombre d'octets contigus du pool de mémoire actuellement inutilisés	1.3.6.1.4.1.9.9.48.1.1.1.7
bufferElMiss	Nombre d'éléments de mémoire tampon manquants	1.3.6.1.4.1.9.2.1.12
bufferFail	Nombre d'échecs d'allocation de mémoire tampon	1.3.6.1.4.1.9.2.1.46
bufferNoMem	Nombre d'échecs de création de mémoire tampon dus à l'absence de mémoire libre	1.3.6.1.4.1.9.2.1.47

MIB des commutateurs Catalyst

Objet	Description	OID
cpmCPUTotal5min	Pourcentage global d'occupation du processeur au cours de la dernière	1.3.6.1.4.1.9.9.109.1.1.1.5

	période de cinq minutes. Cet objet désapprouve l'objet avgBusy5 de l'ancienne base MIB CISCO-SYSTEM	
cpmCPUTotal5s	Pourcentage global d'occupation du processeur au cours de la dernière période de cinq secondes. Cet objet rend obsolète l'objet busyPer de l'OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.3
TraficSystème	Pourcentage d'utilisation de la bande passante pour l'intervalle d'interrogation précédent	1.3.6.1.4.1.9.5.1.1.8
SysTrafficPeak	Valeur de la mesure du trafic maximal depuis la dernière fois que les compteurs de ports ont été effacés ou que le système a démarré	1.3.6.1.4.1.9.5.1.1.19
TempsPointeTraficSys	Temps (en	1.3.6.1.4.1.9.5.1.1.20

	centièmes de seconde) écoulé depuis l'apparition de la valeur du compteur de trafic de pointe	
portTopNUtilisation	Utilisation du port dans le système	1.3.6.1.4.1.9.5.1.20.2.1.4
portTopNBufferOverFlow	Nombre de débordements de mémoire tampon du port dans le système	1.3.6.1.4.1.9.5.1.20.2.1.10

MIB de liaison série

Objet	Description	OID
locIfInputQueueDrops	Nombre de paquets abandonnés parce que la file d'attente d'entrée était pleine	1.3.6.1.4.1.9.2.2.1.1.26
locIfOutputQueueDrops	Nombre de paquets abandonnés parce que la file d'attente de sortie était pleine	1.3.6.1.4.1.9.2.2.1.1.27
locIfInCRC	Nombre de paquets d'entrée présentant des erreurs de somme de contrôle de redondance	1.3.6.1.4.1.9.2.2.1.1.12

	cyclique	

Commandes de configuration d'alarme et d'événement RMON

Alarmes

Les alarmes RMON peuvent être configurées avec la syntaxe suivante :

<#root>

```
rmon alarm number variable interval {delta | absolute} rising-threshold value
           [event-number] falling-threshold value [event-number]
           [owner string]
```

Élément	Description
numéro	Numéro d'alarme, identique à l'alarmIndex dans la table alarmTable de la base MIB RMON.
variable	Objet MIB à surveiller, qui se traduit par la valeur alarmVariable utilisée dans la table alarmTable de la base MIB RMON.
intervalle	La durée, en secondes, pendant laquelle l'alarme surveille la variable MIB, qui est identique à l'alarmInterval utilisé dans la alarmTable de la MIB RMON.
delta	Teste la modification entre les variables MIB, qui affecte le alarmSampleType dans la table alarmTable de la base MIB RMON.
absolu	Teste directement chaque variable MIB, ce qui affecte alarmSampleType dans la table alarmTable de la MIB RMON.
valeur de seuil ascendante	Valeur à laquelle l'alarme est déclenchée.
event-number	(Facultatif) Numéro d'événement à déclencher lorsque le seuil ascendant ou descendant dépasse sa limite. Cette valeur est identique à alarmRisingEventIndex ou à alarmFallingEventIndex dans la table alarmTable de la base MIB RMON.

valeur de seuil descendante	Valeur à laquelle l'alarme est réinitialisée.
chaîne propriétaire	(Facultatif) Spécifie un propriétaire pour l'alarme, qui est identique à alarmOwner dans la table alarmTable de la base MIB RMON.

Événements

Les événements RMON peuvent être configurés avec la syntaxe suivante :

<#root>

```
rmon event number [log] [trap community] [description string]
           [owner string]
```

Élément	Description
numéro	Numéro d'événement attribué, identique à eventIndex dans eventTable dans la base MIB RMON.
journal de bord	(Facultatif) Génère une entrée de journal RMON lorsque l'événement est déclenché et définit eventType dans la MIB RMON sur log ou log-and-trap.
communauté piège	(Facultatif) Chaîne de communauté SNMP utilisée pour cette interruption. Configure le paramètre eventType dans la base MIB RMON pour cette ligne en tant que snmp-trap ou log-and-trap. Cette valeur est identique à eventCommunityValue dans eventTable dans la base MIB RMON.
chaîne de description	(Facultatif) Spécifie une description de l'événement, identique à la description de l'événement dans eventTable de la base MIB RMON.
chaîne propriétaire	(Facultatif) Propriétaire de cet événement, identique à eventOwner dans eventTable de la base MIB RMON.

Mise en œuvre d’alarmes et d’événements RMON

Pour obtenir des informations détaillées sur la mise en oeuvre des alarmes et des événements RMON, consultez la section Mise en oeuvre des alarmes et des événements RMON du livre blanc Meilleures pratiques des systèmes de gestion de réseau.

Informations connexes

- Support technique et documentation – Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.