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

Contenu

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 prend pas à pas par le processus de l'établissement des références. Quelques Produits en cours du système d'administration de réseaux (NMS) peuvent aider à automatiser ce processus, cependant, le processus d'établissement des références demeure le même si vous utilisez les outils automatisés ou manuels. Si vous utilisez ces Produits NMS, vous devez ajuster

les définitions de seuil par défaut pour votre seul environnement de réseau. Il est important d'avoir un processus pour choisir intelligemment seuils de sorte qu'ils soient signicatifs et corrects.

Spécification de base

Quelle est une spécification de base ?

Une spécification de base est un processus pour étudier le réseau à intervalles réguliers pour s'assurer que le réseau fonctionne comme conçu. Il est plus qu'un état simple détaillant les santés du réseau à un certain moment. En suivant le processus de référence, vous pouvez obtenir les informations suivantes :

- Obtenez les données de valeur sur les santés du matériel et du logiciel
- Déterminez l'utilisation en cours des ressources de réseau
- Prenez les décisions précises au sujet des seuils d'alarme réseau
- Identifiez les problèmes de réseau en cours
- Prévoyez les futurs problèmes

Une autre manière de regarder la spécification de base est illustrée dans le diagramme suivant.

La ligne rouge, le point d'arrêt de réseau, est le point auquel le réseau se cassera, qui est déterminé par la connaissance de la façon dont le matériel et le logiciel exécutent. La ligne verte, la charge du réseau, est la progression naturelle du chargement sur le réseau car de nouvelles applications sont ajoutées, et d'autres tels facteurs.

Le but d'une spécification de base est de déterminer :

- Là où votre réseau est sur la ligne verte
- Combien rapide la charge du réseau augmente
- Prévoyez si tout va bien à quel moment les deux intersecteront

En exécutant une spécification de base de façon régulière, vous pouvez découvrir l'état actuel *et* extrapoler quand les pannes se produiront et se prépareront à eux à l'avance. Ceci vous aide également à prendre des décisions plus au courant au sujet de quand, où, et comment dépenser l'argent de budget en mises à jour de réseau.

Pourquoi une spécification de base ?

Un processus de référence vous aide à l'identifier et prévoir correctement pour des questions limite de ressource essentielle dans le réseau. Ces questions peuvent être décrites en tant que des ressources en avion de contrôle ou ressources en plan de données. Les ressources plates en contrôle sont seules à la plate-forme et aux modules spécifiques dans le périphérique et peuvent être affectées par un certain nombre de questions comprenant :

- Utilisation de données
- Caractéristiques activées

- Conception de réseaux

Les ressources plates en contrôle incluent des paramètres comme :

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

Des ressources en plan de données sont affectées seulement par le type et la quantité de trafic et incluent l'utilisation et l'utilisation du fond de panier de lien. Par utilisation de ressource en établissement des références pour des zones critiques, vous pouvez éviter des sérieux problème de performances, ou plus mauvais, un ralentissement des données sur le réseau.

Avec l'introduction des applications sensibles à la latence telles que la Voix et le vidéo, l'établissement des références est maintenant plus important que jamais. Les applications traditionnelles du Transmission Control Protocol/Internet Protocol (TCP/IP) pardonnent et tiennent compte d'un retard. La Voix et le vidéo sont Protocole UDP (User Datagram Protocol) basé et ne tiennent pas compte des retransmissions ou de l'encombrement de réseau.

En raison du nouveau mélange d'applications, l'établissement des références vous aide à comprendre des problèmes d'utilisation des ressources d'avion et de plan de données de contrôle et à prévoir proactivement pour que des modifications et des mises à jour assurent le succès continu.

Les réseaux de données ont été autour depuis de nombreuses années. Jusque récemment, la conservation de s'exécuter de réseaux a été un processus pardonnant assez, avec une certaine marge pour l'erreur. Avec l'acceptation croissante des applications sensibles à la latence telles que la voix sur ip (VoIP), le travail d'exécuter le réseau devient plus dur et exige plus de précision. Afin d'être plus précis et donner à un administrateur réseau une base solide sur laquelle pour gérer le réseau, il est important d'avoir une certaine idée de la façon dont le réseau s'exécute. Pour faire ceci, vous devez passer par un processus appelé une spécification de base.

Objectif de référence

L'objectif d'une spécification de base est à :

1. Déterminez l'état actuel des périphériques de réseau
2. Comparez cet état aux instructions standard de représentation
3. Placez les seuils pour vous alerter quand l'état dépasse ces instructions

En raison d'un grand nombre de données et de durée qu'elle prend pour analyser les données, vous doit d'abord limiter la portée d'une spécification de base pour la faciliter pour apprendre le processus. Le plus logique, et parfois le plus salutaire, endroit pour commencer est avec le coeur du réseau. La présente partie du réseau est habituellement la plus petite et exige la plupart de stabilité.

Dans l'intérêt de la simplicité, ce document explique comment au Management Information Base très important de protocole SNMP de la spécification de base une (MIB SNMP) : cpmCPUTotal5min. cpmCPUTotal5min est la moyenne de décomposition de cinq-minute de l'unité centrale d'un routeur de Cisco (CPU), et est un indicateur de performances d'avion de contrôle. La spécification de base sera exécutée sur un routeur de gamme Cisco 7000.

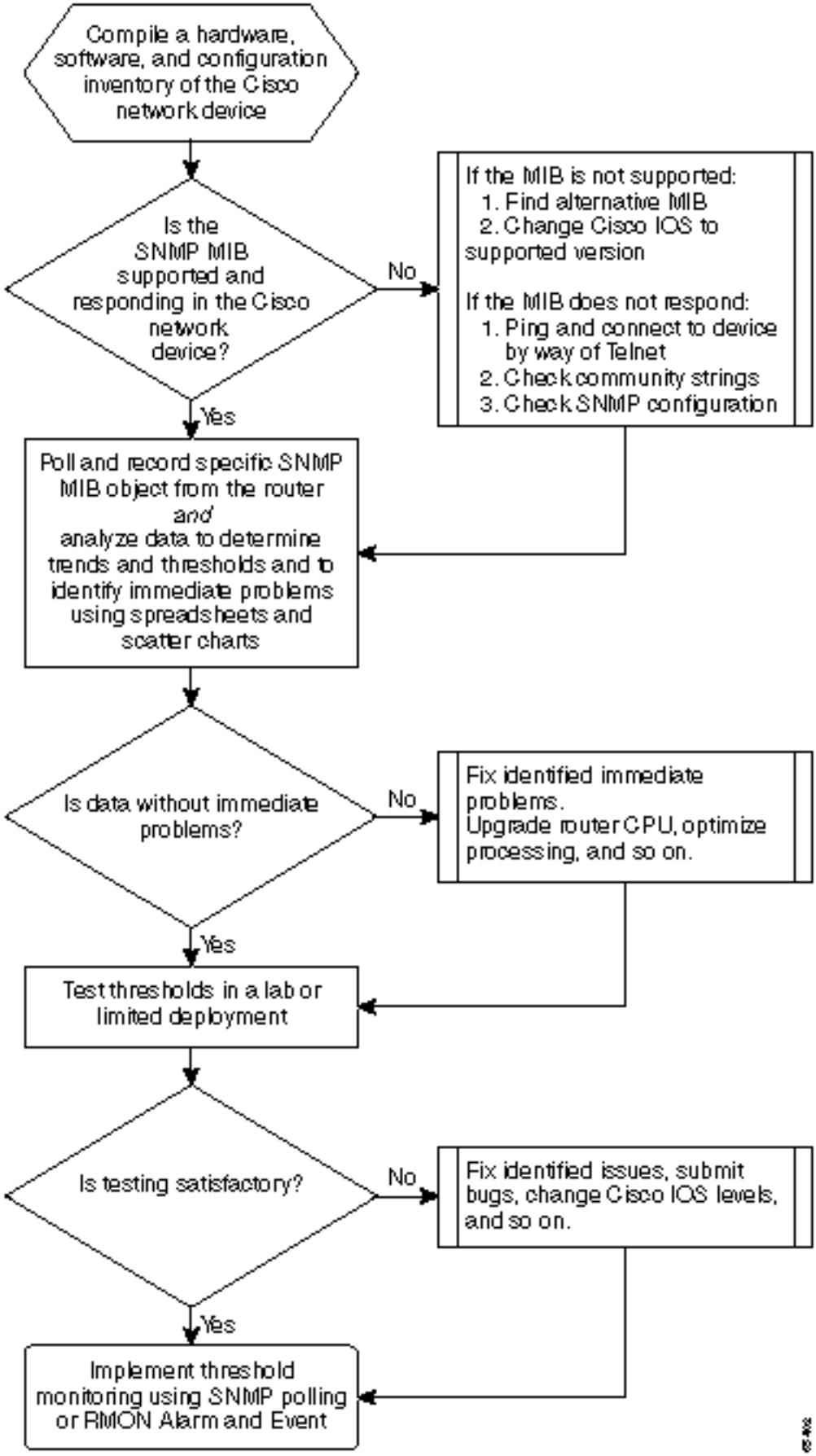
Une fois que vous avez appris le processus, vous pouvez s'appliquer l'à n'importe quelles données disponibles dans la vaste base de données SNMP qui est disponible dans des la plupart

des périphériques de Cisco, comme :

- Utilisation d'Integrated Services Digital Network (le RNIS)
- Perte de cellules de Mode de transfert asynchrone (ATM)
- Mémoire système libre

Organigramme de base

L'organigramme suivant affiche les étapes de base du principal processus de référence. Tandis que les Produits et les outils sont disponibles pour exécuter certaines de ces étapes pour vous, ils tendent à avoir des lacunes dans la flexibilité ou la simplicité d'utilisation. Même si vous prévoyez d'utiliser des outils du système d'administration de réseaux (NMS) pour effectuer l'établissement des références, c'est toujours un bon exercice en étudiant le processus et en comprenant comment votre réseau fonctionne vraiment. Ce processus peut également prendre une partie du mystère hors de la façon dont quelques outils NMS fonctionnent puisque la plupart des outils font essentiellement les mêmes choses.



Procédure de référence

Étape 1 : Compilez un matériel, un logiciel, et un inventaire de configuration

Il est extrêmement important que vous compiliez un inventaire de matériel, de logiciel, et de configuration pour plusieurs raisons. D'abord, le MIB SNMP de Cisco est, dans certains cas, particularité au Cisco IOS libère que vous vous exécutez. Quelques objets MIB sont remplacés par des neufs ou, parfois, sont complètement éliminés. L'inventaire du matériel est le plus important après que les données soient collectées puisque les seuils que vous devez placer après que la spécification de base initiale soient souvent basées sur le type de CPU, quantité de mémoire, et ainsi de suite, sur les périphériques de Cisco. L'inventaire de configuration est également important pour s'assurer que vous connaissez les configurations en cours : Vous pouvez vouloir changer des configurations de périphérique après que votre spécification de base pour accorder des mémoires tampons, et ainsi de suite.

La plupart de façon efficace de faire la présente partie de la spécification de base pour un réseau de Cisco est avec le Resource Manager Essentials CiscoWorks2000 (essentiel). Si ce logiciel est installé correctement dans le réseau, les essentiel devraient avoir les inventaires en cours de tous les périphériques dans sa base de données. Vous devez simplement regarder les inventaires pour voir s'il y a des questions.

Le tableau suivant est un exemple d'un état d'inventaire logiciel de classe de routeur de Cisco exporté des essentiel, et alors édité dans Microsoft Excel. De cet inventaire, notez que vous devez utiliser des données MIB SNMP et objecter les identifiants (OID) trouvés dans des releases du Cisco IOS 12.0x et 12.1x.

Nom du périphérique	Type de routeur	Version	Version de logiciel
field-2500a.embu-mlab.cisco.com	Cisco 2511	M	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(5T)

Si des essentiel n'est pas installés dans le réseau, vous pouvez employer le **snmpwalk d'**outil ligne de commande UNIX d'un poste de travail Unix pour trouver la version IOS. Ceci est affiché dans l'exemple suivant. Si vous n'êtes pas sûr comment cette commande fonctionne, tapez le **snmpwalk d'homme au** pour en savoir plus d'invite Unix. La version IOS sera importante dans quand vous commencez choisir qui MIB OID à la spécification de base, puisque les objets MIB sont personne à charge IOS. Notez également qu'en connaissant le type de routeur, vous pouvez plus tard faire des déterminations quant à ce qu'être les seuils devraient pour la CPU, des mémoires tampons, et ainsi de suite.

```
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 le MIB SNMP est pris en charge dans le routeur

Maintenant que vous avez un inventaire du périphérique que vous voulez voter pour votre spécification de base, vous pouvez commencer à choisir la particularité OID vous voulez voter. Il enregistre beaucoup de frustration si vous vérifiez, d'avance, que les données que vous voulez sont réellement là. L'objet MIB cpmCPUTotal5min est dans le CISCO-PROCESS-MIB.

Pour trouver l'OID que vous voulez voter, vous avez besoin d'une table de conversion qui est disponible sur le site Web CCO de Cisco. Pour accéder à ce site Web d'un navigateur Web, aller à Cisco la page du MIB, et cliquer sur les OID joignent.

Pour accéder à ce site Web d'un ftp server, type **ftp://ftp.cisco.com/pub/mibs/oid/**. De ce site, vous pouvez télécharger le MIB de particularité qui a été décodé et trié par des nombres OID.

L'exemple suivant est extrait de la table CISCO-PROCESS-MIB.oid. Cet exemple prouve que l'OID pour le cpmCPUTotal5minMIB est .1.3.6.1.4.1.9.9.109.1.1.1.1.5.

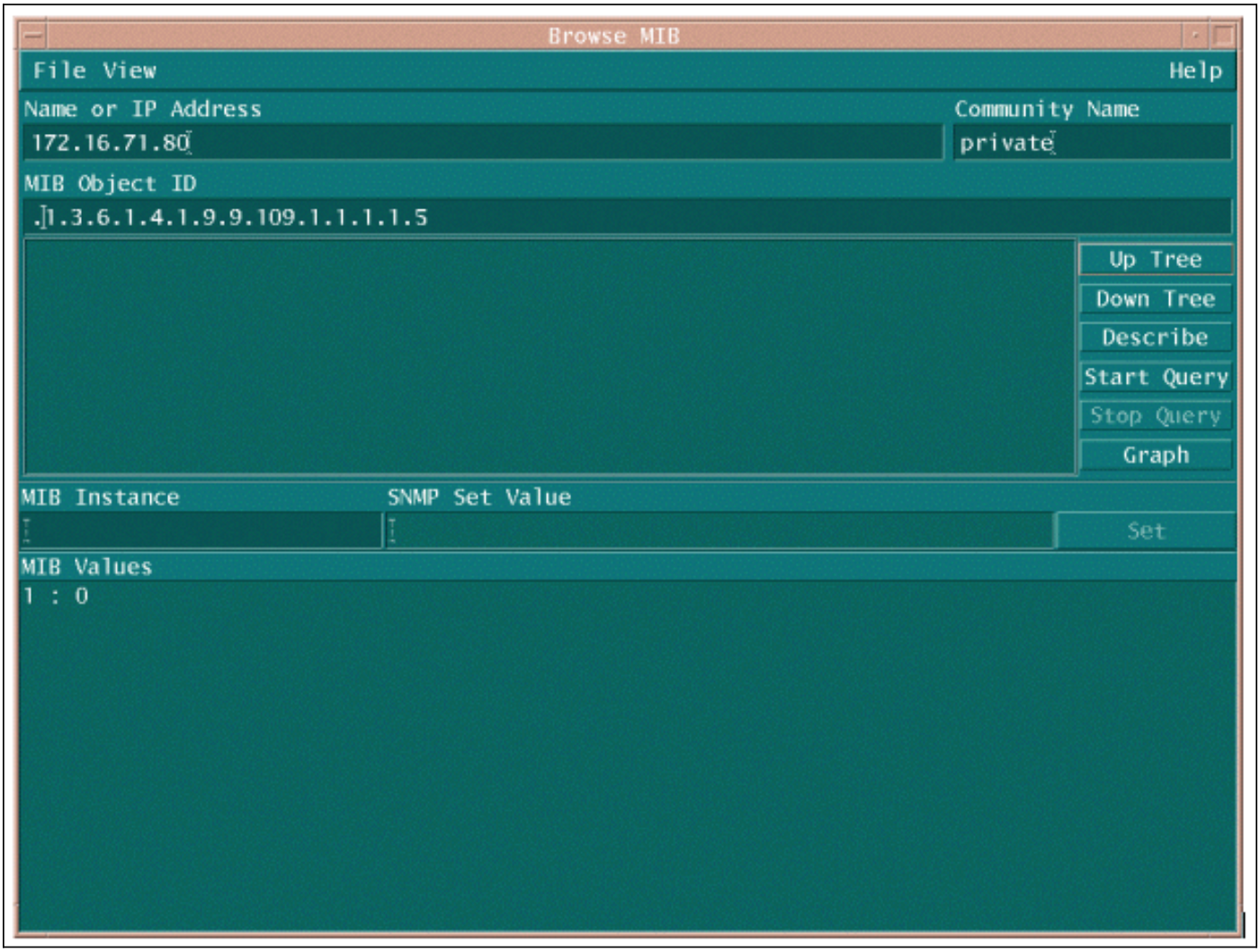
Remarque: N'oubliez pas d'ajouter « . » au début de l'OID ou de vous obtiendra une erreur quand vous essayez de le voter. Vous devez également additionner un ".1" à la fin de l'OID pour l'instancier. Ceci indique au périphérique l'exemple de l'OID que vous recherchez. Dans certains cas, les OID ont plus d'un exemple d'un type de données particulier, comme quand un routeur a de plusieurs CPU.

```
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 y a deux manières courantes de voter le MIB OID pour s'assurer qu'il est disponible et fonctionnement. C'est une bonne idée de faire ceci avant que vous commenciez la collecte des informations en vrac de sorte que vous ne gaspilliez pas l'interrogation de temps quelque chose

qui n'est pas là et finissiez par avec une base de données vide. Une manière de faire ceci est d'utiliser un marcheur MIB de votre plate-forme NMS telle que le gestionnaire de HP OpenView Network Node (NNM), ou des CiscoWorks Windows, et écrit l'OID que vous voulez vérifier.

Ce qui suit est un exemple de marcheur MIB SNMP de HP OpenView.



Une autre méthode facile de voter le MIB OID est d'utiliser le **snmpwalk de** commande UNIX suivant les indications de 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.
cpmCPUTotal5min.1 : Gauge32: 0
```

Dans les deux exemples, le MIB a renvoyé une valeur de 0, signifiant que pour ce cycle de sondage la CPU a fait la moyenne de 0 pour cent d'utilisation. Si vous avez la difficulté obtenant le périphérique pour répondre avec les données correctes, essayez cingler le périphérique et accéder au périphérique par le telnet. Si vous avez toujours un problème, vérifiez la configuration SNMP et les chaînes de caractères de la communauté SNMP. Vous pouvez devoir trouver un MIB d'alternative ou une version différente d'IOS pour faire ce travail.

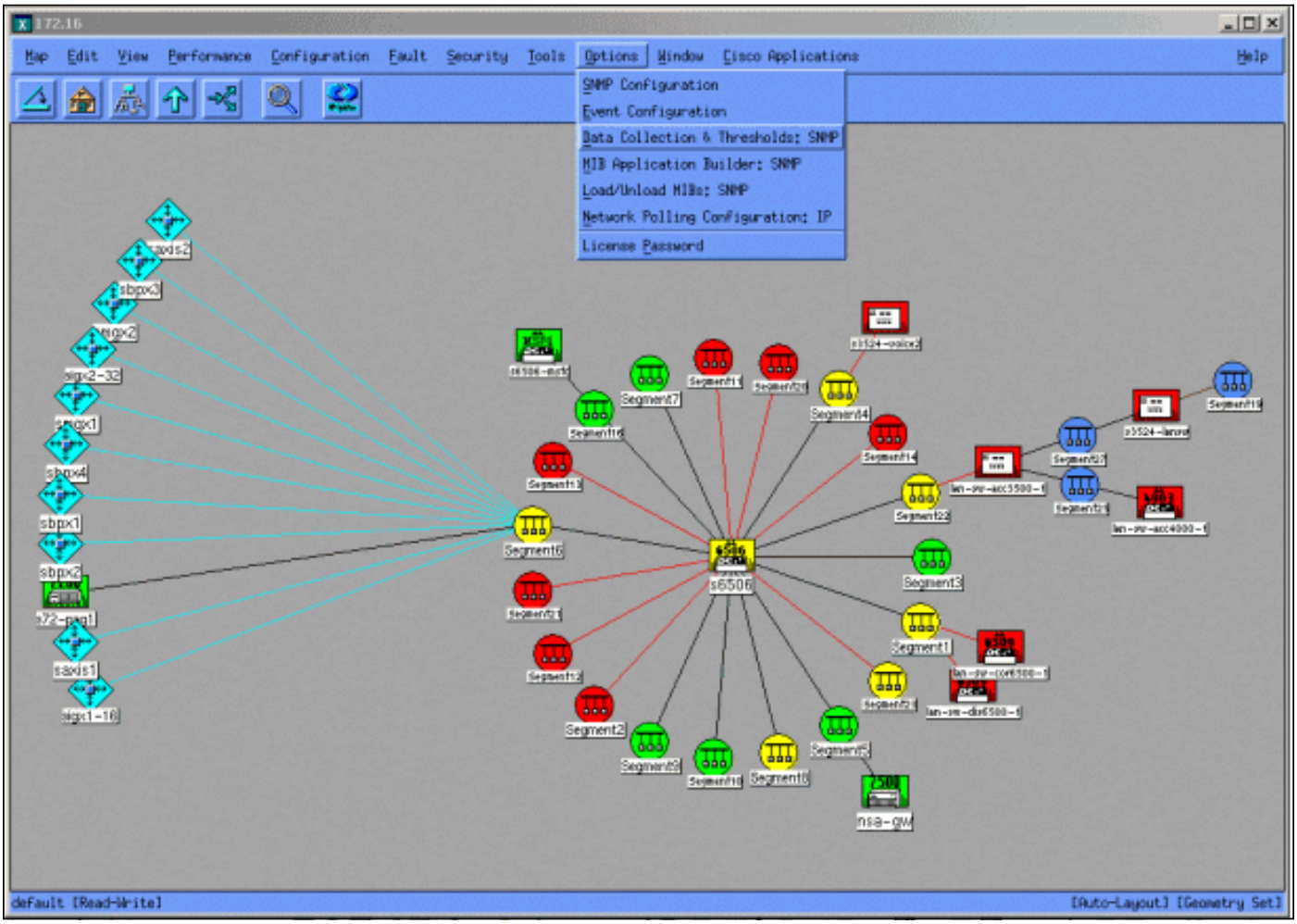
Étape 3 : Objet MIB SNMP de particularité de balayage et d'enregistrement du routeur

Il y a plusieurs manières de voter des objets MIB et d'enregistrer la sortie. Les Produits

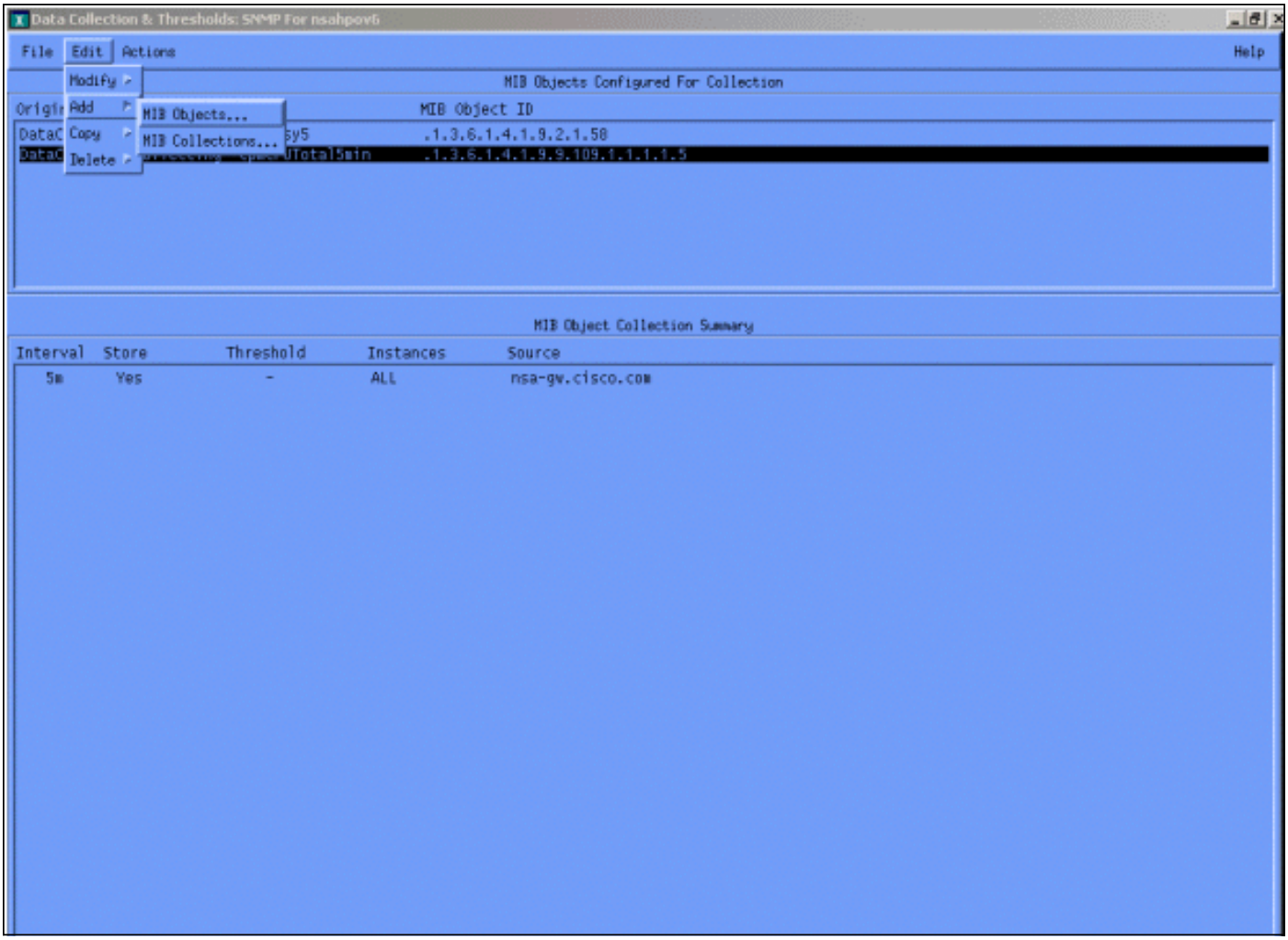
disponibles immédiatement, les Produits de shareware, les scripts, et les outils de constructeur sont disponibles. Tous les outils frontaux emploient le processus de snmp get pour obtenir les informations. Les principales différences sont dans la flexibilité de la configuration et de la manière dans lesquelles les données sont enregistrées dans une base de données. De nouveau, regardez le MIB de processeur pour voir comment ces diverses méthodes fonctionnent.

Maintenant que vous savez l'OID est pris en charge dans le routeur, vous devez décider combien de fois le voter et comment l'enregistrer. Cisco recommande que le MIB CPU soit voté à intervalles de cinq-minute. Un intervalle inférieur augmenterait le chargement sur le réseau ou le périphérique, et puisque la valeur MIB est une moyenne de cinq-minute de toute façon il ne serait pas utile de la voter plus souvent que la valeur ramenée à une moyenne. On le recommande également généralement que l'interrogation de spécification de base aient au moins une période de deux semaines de sorte que vous puissiez analyser au moins des cycles conjoncturels bi-hebdomadaires sur le réseau.

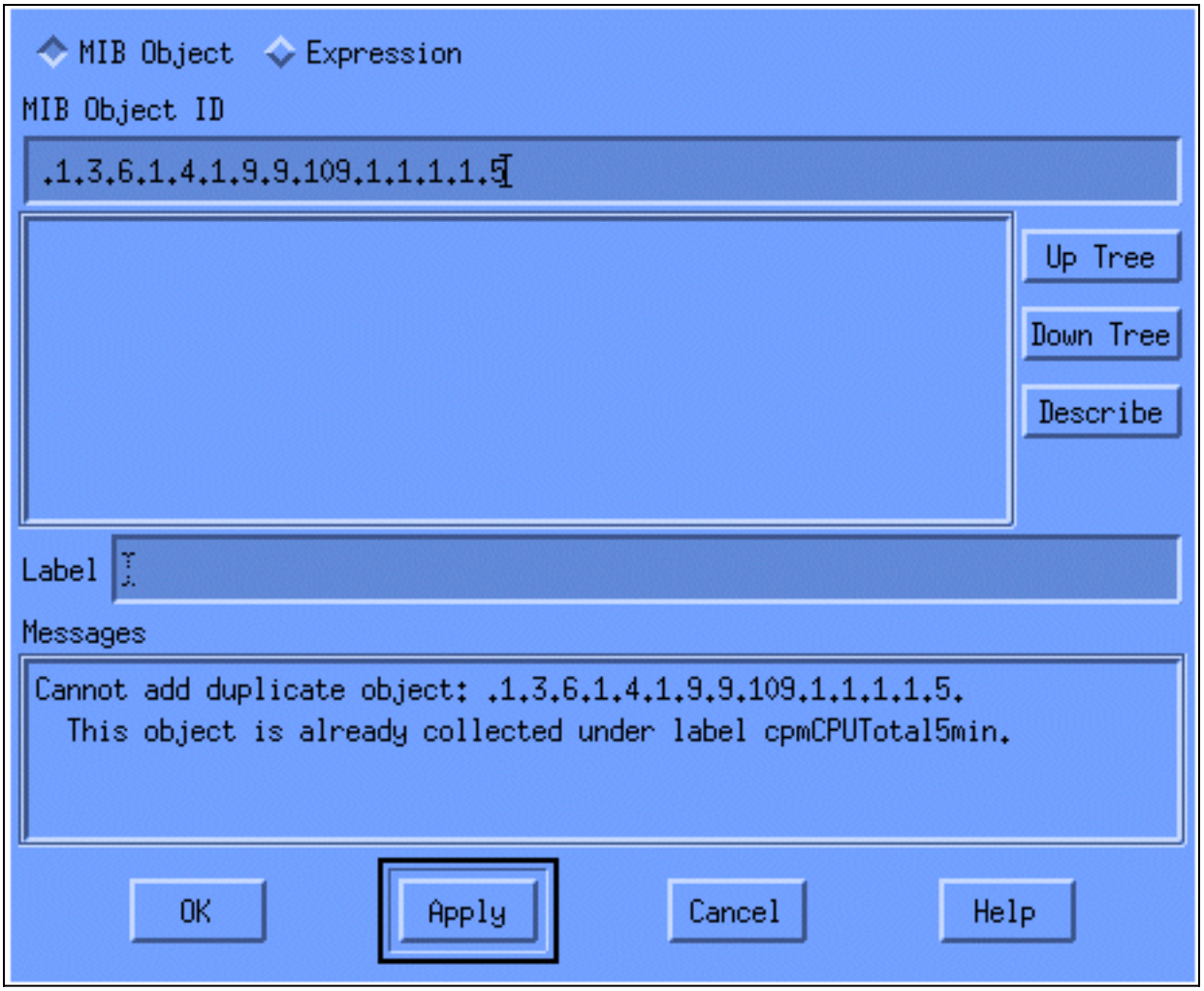
Les écrans suivants t'affichent que comment faire ajoutez les objets MIB avec la version 6.1 de gestionnaire de HP OpenView Network Node. De l'écran principal, des **options** choisies **> de la collecte des informations et seuils**.



Sélectionnez alors **éditent > ajoutent > des objets MIB**.

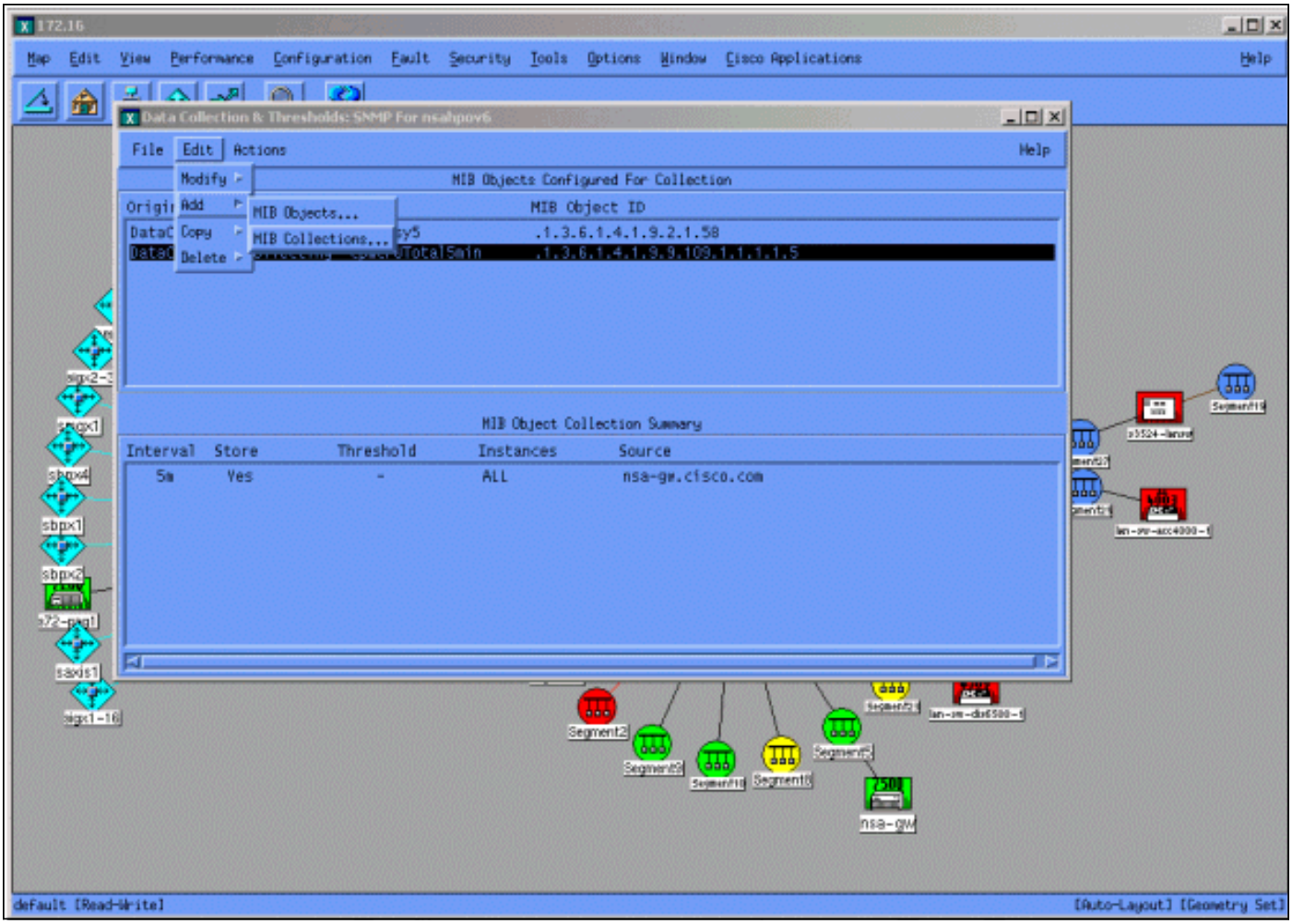


Du menu, ajoutez la chaîne OID et cliquez sur Apply. Vous avez maintenant écrit l'objet MIB dans la plate-forme de HP OpenView de sorte qu'elle puisse être votée.



Vous devez avez ensuite fait le HP OpenView connaître quel routeur à voter pour cet OID.

Du menu de collecte des informations, choisi **éditez > ajoutez > des collectes des bases MIB**.

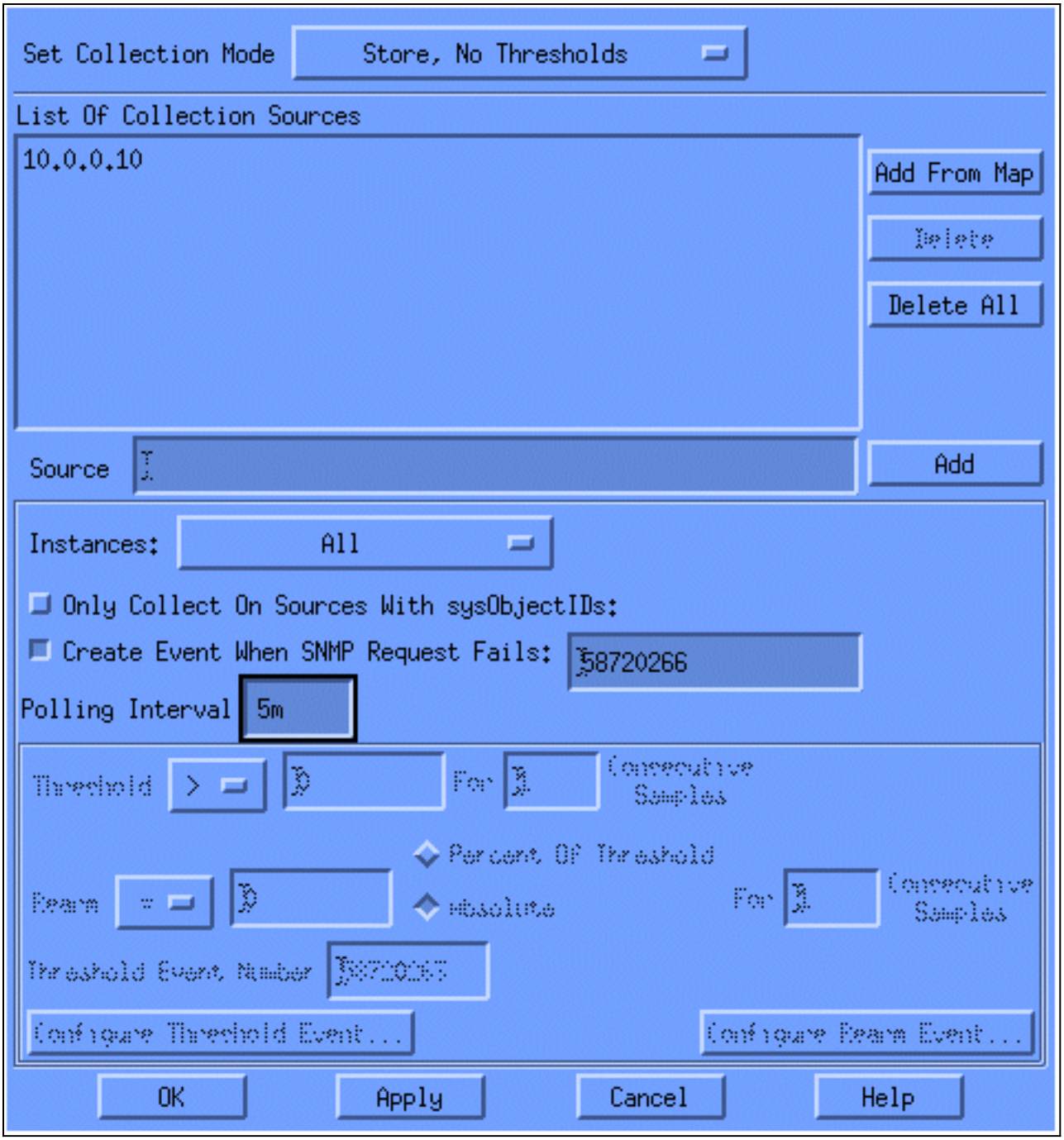


Dans le domaine de source, écrivez le nom de système de noms de domaine (DN) ou l'adresse IP du routeur à voter.

La mémoire choisie**, aucun seuils du** mode de collecte de positionnement les répertorient.

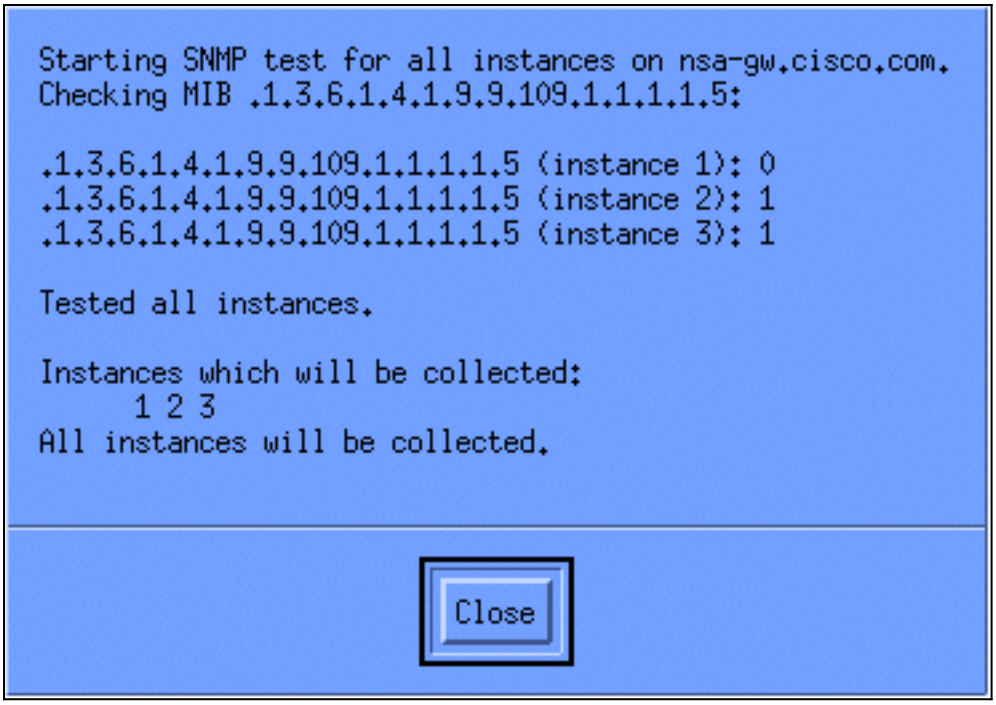
Placez l'intervalle de sondage à **5m**, pour cinq intervalles minute.

Cliquez sur **Apply**.



Vous devez sélectionner le **fichier > la sauvegarde** pour que les modifications prennent l'affect.

Pour vérifier que la collecte est installée correctement, mettez en valeur la ligne récapitulative de collecte pour le routeur et le **SNMP** choisi d'**actions > de test**. Ceci vérifie pour voir si la chaîne de la communauté est correcte et votera pour tous les exemples de l'OID.



La fin de clic, et a permis la collecte de fonctionner pendant une semaine. À la fin de la période hebdomadaire, extrayez les données pour l'analyse.

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

Extrayez les données à un fichier ASCII Appelé **testfile** avec la commande suivante :

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

Remarque: cpmCPUTotal5min.1 est le fichier de base de données qui le HP OpenView NNM créé quand l'interrogation OID a commencé.

Le fichier de test généré ressemble 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/.....
```

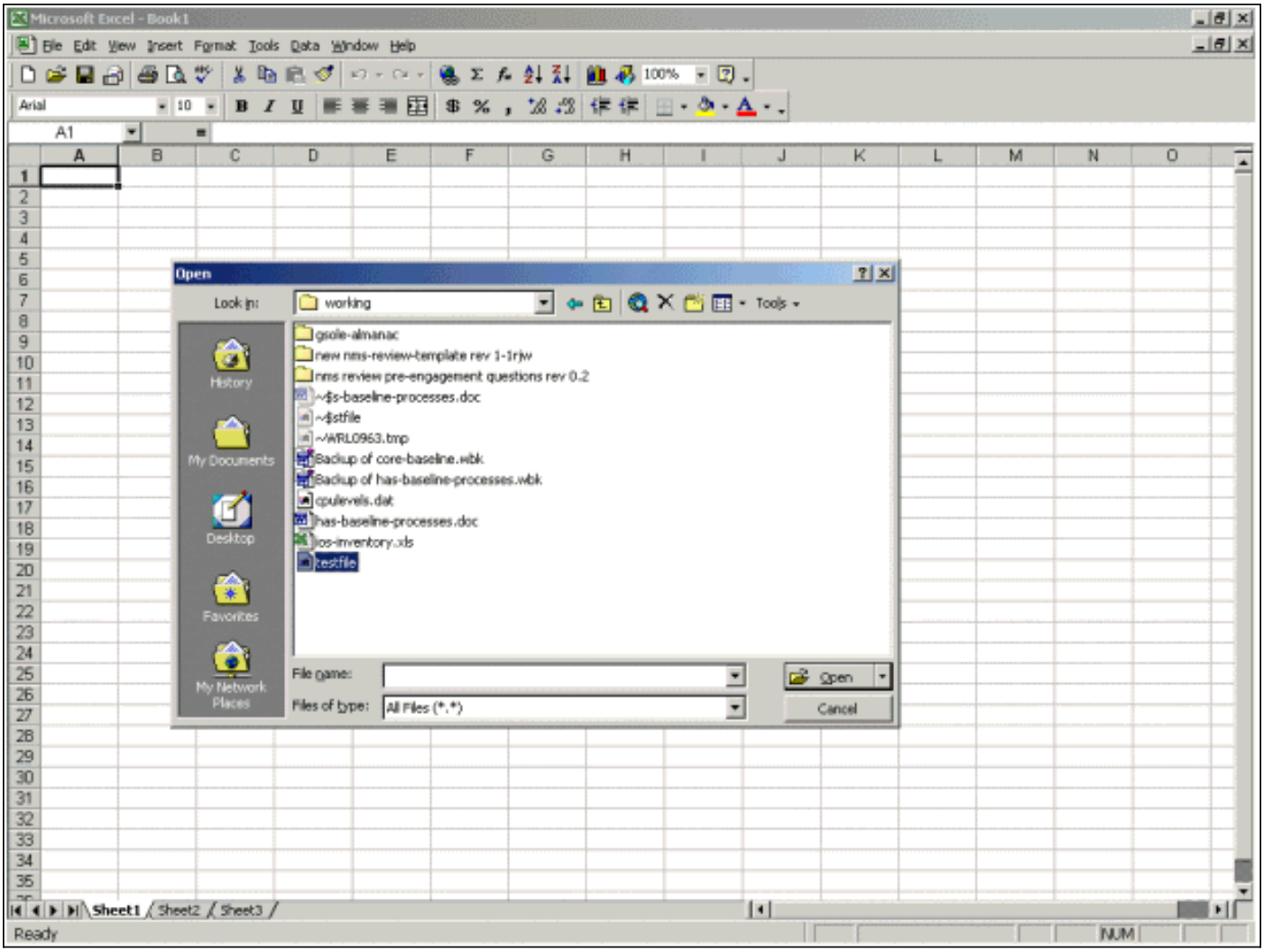
Une fois que la sortie de fichier de test est sur votre station Unix, vous pouvez la transférer vers votre PC utilisant le Protocole FTP (File Transfer Protocol).

Vous pouvez également recueillir les données utilisant vos propres scripts. Pour faire ceci, exécutez un **snmpget** pour la CPU OID toutes les cinq minutes et videz les résultats dans un fichier .csv.

Étape 4 : Analysez les données pour déterminer des seuils

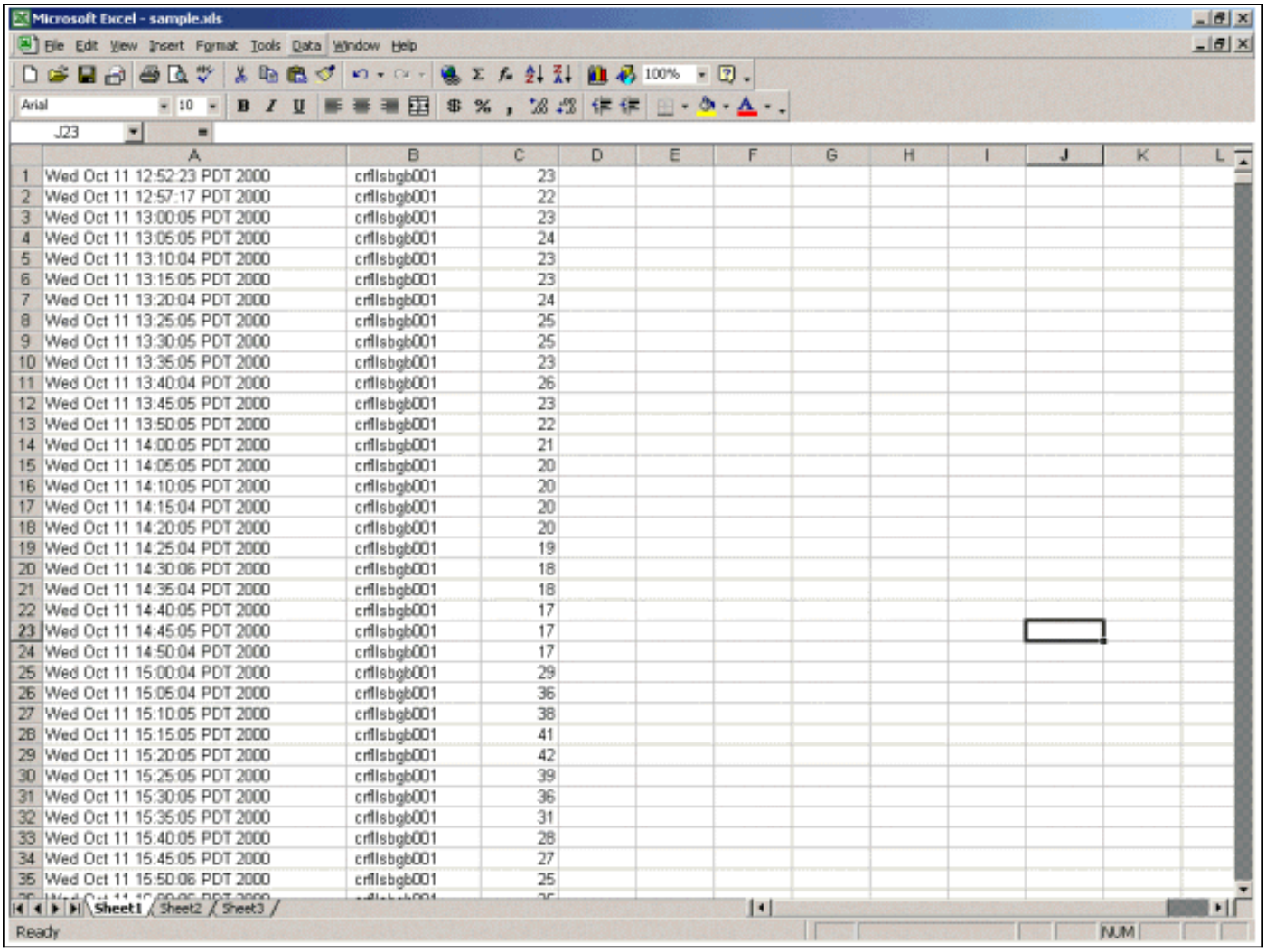
Maintenant que vous avez quelques données, vous pouvez commencer à l'analyser. Cette phase de la spécification de base détermine les définitions de seuil que vous pouvez utiliser qui sont une mesure précise de représentation ou défaut et ne placerez pas outre de trop d'alarmes quand vous activez la surveillance de seuil. Un des moyens les plus simples de faire ceci est d'importer les données dans un tableur tel que Microsoft Excel et de tracer un tableau de dispersion. Cette méthode le rend très facile de voir 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 des seuils sans faire une spécification de base, puisque ceci peut créer les tempêtes vigilantes des périphériques qui ont dépassé le seuil que vous avez choisi.

Pour importer le fichier de test dans un tableur d'Exceler, Exceler ouverts et sélectionner le **fichier > ouvrent** et sélectionnent votre fichier de données.



L'application d'Exceler vous incite alors en important le fichier.

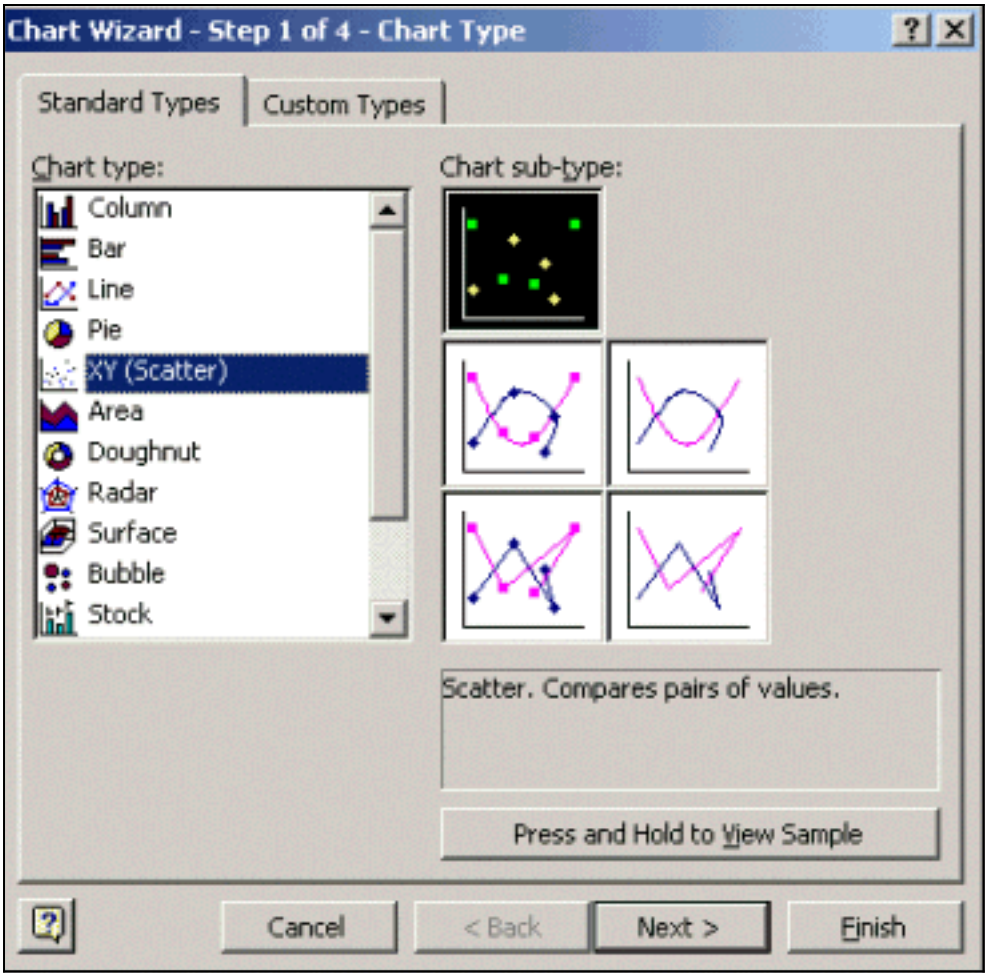
Une fois terminé, le fichier importé devrait sembler semblable à l'écran suivant.



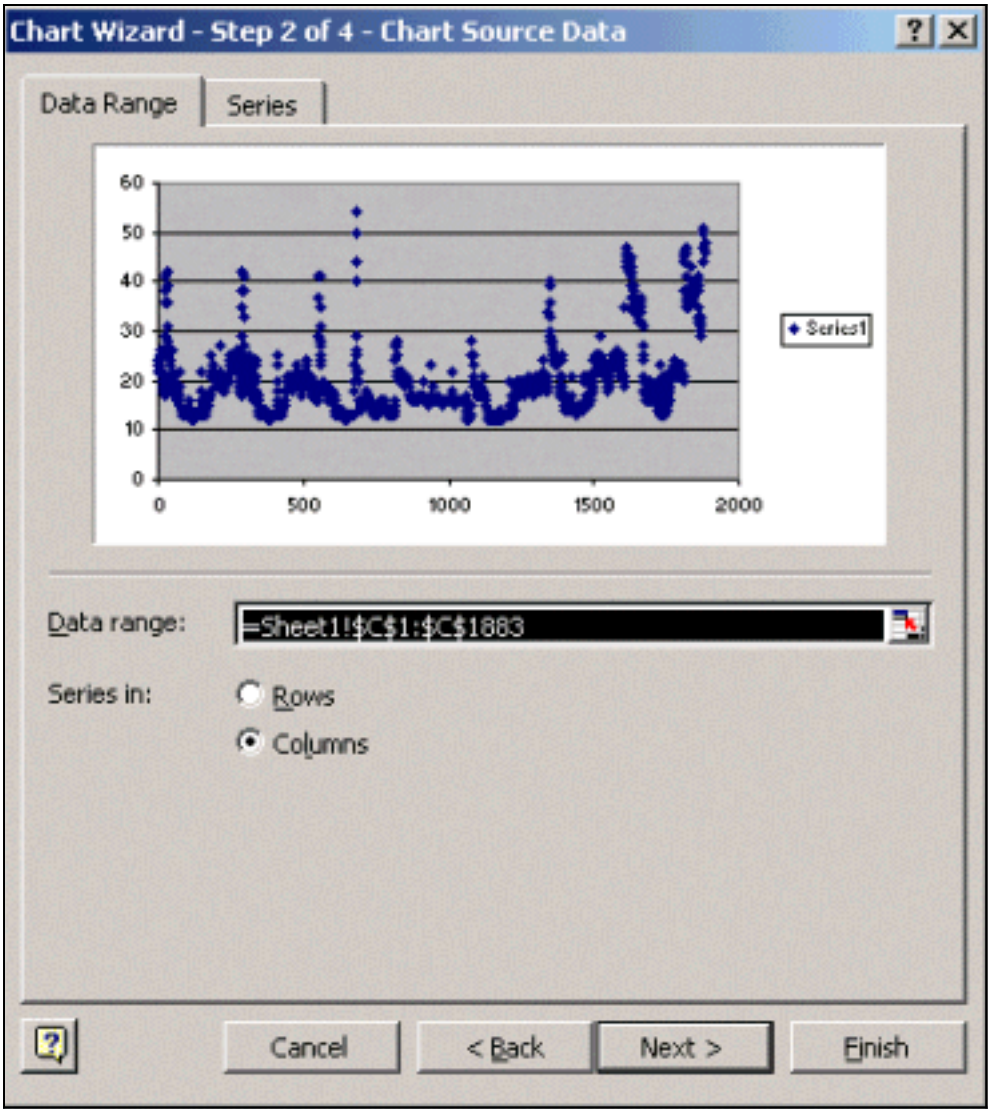
Un tableau de dispersion vous permet à visualisent plus facilement comment les diverses définitions de seuil travailleraient au réseau.

Pour créer le tableau de dispersion, le C de colonne de point culminant dans le fichier importé et puis cliquer sur l'icône d'**Assistant Diagrammes**. Suivez alors les étapes par l'Assistant Diagrammes pour établir un tableau de dispersion.

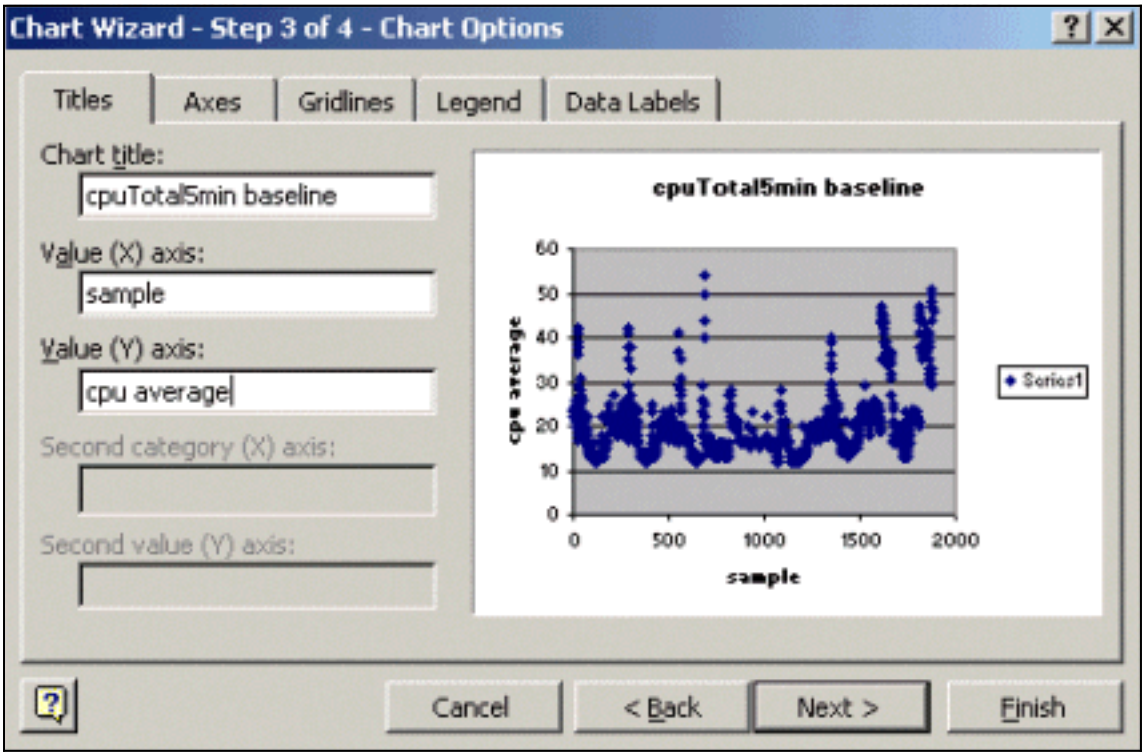
Dans l'étape 1 d'Assistant Diagrammes, comme affiché ci-dessous, sélectionnez l'onglet de **types standards**, et sélectionnez le type **DE X/Y de** tableau **(de dispersion)**. Cliquez ensuite sur **Next**.



Dans l'étape 2 d'Assistant Diagrammes, comme affichés ci-dessous, sélectionnez l'onglet de **plage des données** et sélectionnez la plage des données et l'option de **colonnes**. Cliquez sur **Next** (Suivant).



Dans l'étape 3 d'Assistant Diagrammes, comme affichés ci-dessous, écrivez le titre de tableau et les valeurs X et d'axe des ordonnées, et puis cliquez sur Next.



Dans l'étape 4 d'Assistant Diagrammes, sélectionnez si vous voulez le tableau de dispersion à une nouvelle page ou comme objet dans la page existante.

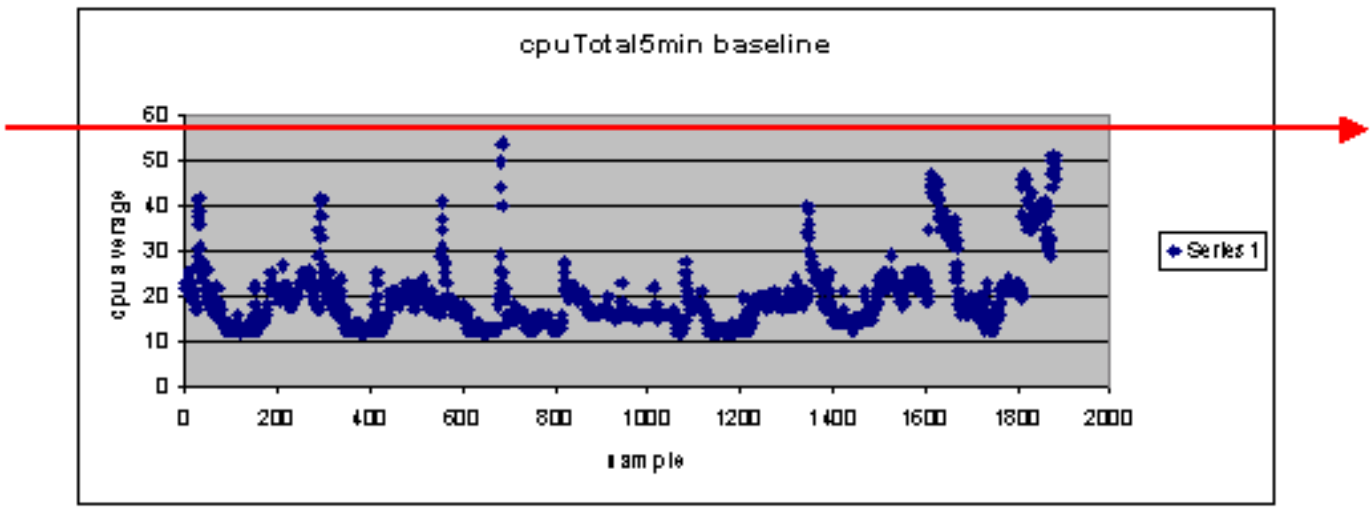
Cliquez sur Finish pour placer le tableau dans votre emplacement désiré.

« Ce qui si ? » Analyse

Vous pouvez maintenant utiliser le tableau de dispersion pour l'analyse. Cependant, avant de commencer, vous devez poser les questions suivantes :

- Queest-ce que le constructeur (dans cet exemple le constructeur est-il Cisco) recommande comme seuil pour cette variable MIB ?Généralement Cisco recommande qu'un principal routeur ne dépasse pas 60 pour cent d'utilisation du processeur moyenne. Soixante pour cent ont été choisis parce qu'un routeur a besoin du temps système au cas où il éprouverait le problème ou le réseau a quelques pannes. Cisco estime qu'un principal routeur a besoin de la CPU d'approximativement 40 pour cent supplémentaire au cas où un protocole de routage devrait recalculer ou reconverge. Ces pourcentages varient basé sur les protocoles vous utiliser-et la topologie et la stabilité de votre réseau.
- Ce qui si j'utilise 60 pour cent comme définition de seuil ?Si vous tracez une ligne à travers le tableau de dispersion horizontalement à 60, vous verrez qu'aucun des points d'informations ne dépasse 60 pour cent d'utilisation du processeur. Ainsi un seuil du positionnement 60 sur vos stations du système d'administration de réseaux (NMS) n'aura pas placé outre d'une alarme de seuil au cours de la période d'interrogation. Un pourcentage de 60 est acceptable pour ce routeur. Cependant, avis dans le tableau de dispersion que certains des points d'informations sont proches de 60. Il ferait beau de connaître quand un routeur s'approche du seuil de 60 pour cent ainsi vous pouvez savoir d'avance que la CPU approche 60 pour cent et avoir un plan pour que ce que fasse quand elle atteint ce point.
- Ce qui si je plaçais le seuil à 50 pour cent ?On l'estime que ce routeur a atteint 50 pour cent d'utilisation quatre fois pendant ce cycle de sondage et aurait généré une alarme de seuil chaque fois. Ce processus devient plus important quand vous regardez des *groupes de Routeurs* pour voir ce que les différentes définitions de seuil feraient. Par exemple, « ce qui si je plaçais le seuil à 50 pour cent pour le principal réseau entier ? » Vous voyez, il est très difficile de choisir juste un nombre.

Seuil CPU « ce qui si » analyse



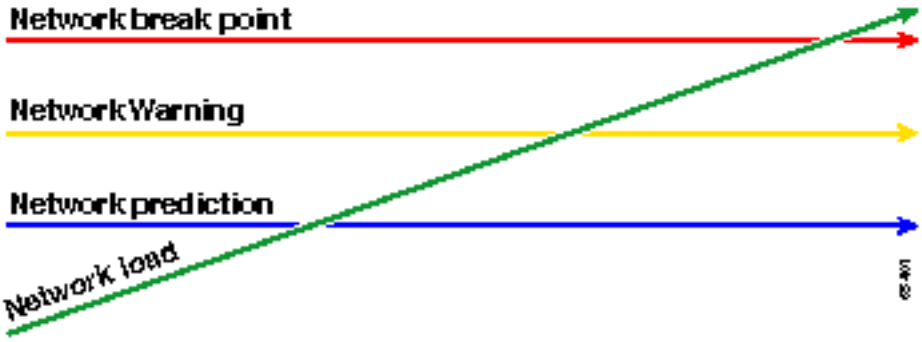
Une stratégie que vous pouvez employer pour faire ce plus facile est la prête, positionnement, vont la méthodologie de seuil. Cette méthodologie utilise trois nombres de seuil en succession.

- Prêt — le seuil que vous placez en tant que predictor de quels périphériques auront besoin vraisemblablement d'attention à l'avenir
- Positionnement — le seuil qui est utilisé comme indicateur tôt, qui vous alerte pour commencer la planification pour une réparation, reconfiguration, ou mise à jour
- Allez — le seuil que vous et/ou le constructeur croyez est une condition de panne et exige une certaine action de la réparer ; dans cet exemple c'est de 60 pour cent

Le tableau suivant affiche la stratégie du prêt, positionnement, vont la stratégie.

Seuil	Action	Résultat
45 pour cent	Étudiez plus plus loin	Liste d'options pour des plans d'action
50 pour cent	Formulez le plan d'action	Liste d'étapes dans le plan d'action
60 pour cent	Plan d'action de mise en place	Le routeur ne dépasse plus des seuils. De nouveau au mode prêt

Les prêts, positionnement, disparaissent la méthodologie changent le diagramme de référence d'origine discuté plus tôt. Le diagramme suivant affiche le diagramme de référence changé. Si vous pouvez identifier les autres points d'intersection sur le tableau, vous avez maintenant plus de temps pour prévoir et réagir que vous avez fait avant.



Notez que dans ce processus, l'attention est concentrée sur les exceptions dans le réseau et n'est pas concernée par d'autres périphériques. On le suppose que tant que les périphériques sont au-dessous des seuils, ils sont bien.

Si vous avez ces étapes pensées du début, vous serez bien préparé pour maintenir le réseau sain. Exécuter ce type de planification est également extrêmement utile pour la planification de budget. Si vous connaissez ce que vos cinq principaux **disparaissent des** Routeurs, vos Routeurs moyens de **positionnement**, et vos Routeurs **prêts** inférieurs sont, vous pouvez facilement prévoir sur de combien de budget vous aurez besoin pour des mises à jour basées sur ce qu'un peu des Routeurs qu'ils sont et ce que vos options de plan d'action sont. La même stratégie peut être utilisée pour les liens ou n'importe quel autre MIB OID de réseau d'étendu (WAN).

Étape 5 : Problèmes immédiats identifiés par difficulté

C'est l'une des parties plus faciles du processus de référence. Une fois que vous avez identifié quels périphériques dépassent le seuil d'**aller**, vous devriez faire un plan d'action pour obtenir le seuil de dessous arrière de ces périphériques.

Vous pouvez ouvrir une valise avec le centre d'assistance technique de Cisco (TAC) ou contacter votre technicien système pour des options disponibles. Vous ne devriez pas supposer que cela obtenir des choses de retour sous le seuil coûtera t'à argent. Quelques questions CPU peuvent être résolues en changeant la configuration pour s'assurer que tous les processus s'exécutent de la plupart de façon efficace. Par exemple, un certain Listes de contrôle d'accès (ACL) peut faire une CPU de routeur exécuter en raison très élevé du chemin les paquets pour prendre par le routeur. Dans certains cas, vous pouvez implémenter la Commutation Netflow pour changer le chemin de commutation par paquets et pour réduire l'incidence de l'ACL sur la CPU. Celui qui les questions soient, il est nécessaire d'obtenir tout le seuil de dessous arrière de Routeurs dans cette étape ainsi vous pouvez implémenter les seuils plus tard sans risque d'inonder les stations NMS avec trop d'alarmes de seuil.

Étape 6 : Surveillance de seuil de test

Cette étape implique de tester les seuils dans le laboratoire utilisant les outils que vous utiliserez dans le réseau de production. Il y a deux approches communes à surveiller des seuils. Vous devez décider quelle méthode est la meilleure pour votre réseau.

- Votez et comparez la méthode utilisant une plate-forme SNMP ou tout autre outil de surveillance SNMPCette méthode utilise plus de bande passante de réseau pour le trafic de vote et prend des cycles de traitement sur votre plate-forme SNMP.
- L'alarme et les configurations d'événement de Surveillance à distance (RMON) d'utilisation dans les Routeurs ainsi eux envoient une alerte seulement quand un seuil est dépasséCette méthode réduit l'utilisation de la bande passante de réseau mais augmente également la mémoire et l'utilisation du processeur sur les Routeurs.

Mise en oeuvre d'un seuil utilisant le SNMP

Pour installer la méthode SNMP utilisant le HP OpenView NNM, les **options** choisies **> la collecte des informations et seuils** comme le faisiez vous quand vous avez installé l'interrogation initiale. Cette fois, cependant, **mémoire** choisie**, seuils de contrôle** plutôt que la mémoire, aucun seuils dans le menu de collections. Après que vous installiez le seuil, vous pouvez soulever l'utilisation du processeur sur le routeur en lui envoyant de plusieurs pings et/ou plusieurs inspections SNMP. Vous pouvez devoir diminuer la valeur seuil si vous ne pouvez pas forcer assez la haute CPU pour se déclencher le seuil. En tous cas, vous devriez s'assurer que le mécanisme de seuil fonctionne.

Une des limites d'utiliser cette méthode est que vous ne pouvez pas implémenter des plusieurs seuils simultanément. Vous auriez besoin de trois Plateformes SNMP pour placer trois seuils simultanés différents. Les outils tels que des Concord Network Health et le Trinagy TREND permettent des plusieurs seuils pour le même exemple OID.

Si votre système peut seulement manipuler un seuil à la fois, vous pouvez considérer le prêt, positionnement, allez la stratégie de mode séquentielle. C'est-à-dire, quand le seuil **prêt** est atteint continuellement, commencez votre enquête et soulevez le seuil au set level pour ce périphérique. Quand le **set level** est atteint continuellement, commencez à formuler votre plan d'action et à soulever le seuil au niveau d'**aller** pour ce périphérique. Alors quand le seuil d'aller est atteint

continuellement, implémentez votre plan d'action. Ceci devrait fonctionner aussi bien comme méthode simultanée du seuil trois. Cela prend juste un peu plus de temps changeant les définitions de seuil de plate-forme SNMP.

Mise en oeuvre d'un seuil utilisant l'alarme et l'événement de RMON

Utilisant l'alarme et les configurations d'événement de RMON, vous pouvez avoir le moniteur de routeur elle-même pour des plusieurs seuils. Quand le routeur détecte un état de sur-seuil, il envoie un déroutement SNMP à la plate-forme SNMP. Vous devez avoir une installation de récepteur de déroutement SNMP en votre configuration de routeur pour que le déroutement soit expédié. Il y a 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 se déclenche l'event process qui peut l'un ou l'autre envoyer un message de déroutement SNMP, créent une entrée de journal de RMON, ou chacun des deux. Pour plus de détail sur cette commande, voir l'alarme et les commandes de configuration d'événement de RMON.

Les commandes de configuration de routeur suivantes a le moniteur cpmCPUTotal5min de routeur toutes les 300 secondes. Il se déclenchera l'événement 1 si la CPU dépasse 60 pour cent et se déclenchera l'événement 2 quand la CPU retombe à 40 pour cent. Dans des les deux cas, un message de déroutement SNMP sera envoyé à la station NMS avec la chaîne privée de la communauté.

Pour utiliser le prêt, le positionnement, disparaissent la méthode, utilisent toutes les directives 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 affiche la sortie de la commande d'**alarme de show rmon** qui a été configurée par les déclarations ci-dessus.

```
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 affiche la sortie de la commande d'**événement de show rmon**.

```
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 vouloir essayer chacun des deux méthodes pour voir quelle méthode meilleure adapte à votre environnement. Vous pouvez même constater qu'une combinaison des méthodes fonctionne bien. En tous cas, le test devrait être fait dans un environnement de travaux pratiques pour s'assurer que tout fonctionne correctement. Après test dans le laboratoire, un déploiement limité sur un petit groupe de Routeurs te permettra pour tester le processus d'envoyer des alertes à votre centre d'exécutions.

Dans ce cas, vous devrez diminuer les seuils pour tester le processus : Essayer pour soulever artificiellement la CPU sur un routeur de production n'est pas recommandé. Vous devriez également s'assurer que quand les alertes entrent dans les stations NMS au centre d'exécutions, il y a une stratégie de transmission des problèmes pour s'assurer que vous êtes au courant quand les périphériques dépassent des seuils. Ces configurations ont été testées dans un laboratoire avec la version 12.1(7) de Cisco IOS. Si vous rencontrez n'importe quelles questions, vous devriez vérifier avec Cisco machinant ou des techniciens système pour voir si vous avez une bogue dans votre version IOS.

Étape 7 : Surveillance de seuil de mise en place utilisant le SNMP ou le RMON

Une fois que vous avez complètement testé la surveillance de seuil dans le laboratoire, et dans un déploiement limité, vous êtes prêt à implémenter des seuils à travers le principal réseau. Vous pouvez maintenant systématiquement passer par ce processus de référence pour d'autres importantes variables MIB sur votre réseau, tel que des mémoires tampons, mémoire disponible, des erreurs de contrôle de redondance cyclique (CRC), perte de cellules AMT, et ainsi de suite.

Si vous utilisez l'alarme et les configurations d'événement de RMON, vous pouvez maintenant cesser de voter de votre station NMS. Ceci réduira le chargement sur votre serveur NMS et réduira la quantité de données de sondage sur le réseau. En allant systématiquement par ce processus pour des indicateurs de santés de réseau important, vous pourriez facilement être livré au point que l'équipement réseau se surveillent utilisant l'alarme et l'événement de RMON.

MIB supplémentaire

Après que vous ayez appris ce processus, vous pouvez vouloir étudier l'autre MIB à la spécification de base et au moniteur. Les paragraphes suivants présentent une brève liste de quelques OID et descriptions que vous pouvez trouver utile.

MIB de routeur

Les caractéristiques de mémoire sont très utiles en déterminant les santés d'un routeur. Un routeur intègre devrait presque toujours avoir l'espace de mémoire tampon disponible avec lequel pour fonctionner. Si le routeur commence à manquer de l'espace de mémoire tampon, la CPU devra travailler plus dur pour créer de nouvelles mémoires tampons et pour les essayer de trouver des mémoires tampons pour les paquets entrants et sortants. Une discussion approfondie des mémoires tampons est hors de portée de ce document. Cependant, en règle générale, un routeur intègre devrait avoir peu ou pas de coups manqués de mémoire tampon et ne devrait avoir aucune défaillances de la mémoire tampon, ou un état zéro de mémoire disponible.

Objet	Description	OID

ciscoMemoryPool Free	Le nombre d'octets du pool mémoire qui sont actuellement inutilisés sur le périphérique géré	1.3.6.1.4.1.9.9.48.1.1.1.6
ciscoMemoryPool LargestFree	Le plus grand nombre d'octets contigus du pool mémoire qui sont actuellement inutilisés	1.3.6.1.4.1.9.9.48.1.1.1.7
bufferElMiss	Les coups manqués de nombre d'éléments en tampon	1.3.6.1.4.1.9.2.1.12
bufferFail	Le nombre d'échecs d'allocation de la mémoire tampon	1.3.6.1.4.1.9.2.1.46
bufferNoMem	Le nombre de mémoire tampon créent des pannes dues à aucune mémoire disponible	1.3.6.1.4.1.9.2.1.47

MIB de commutateur de Catalyst

Objet	Description	OID
cpmCPUTotal5min	Pourcentage occupé global CPU pendant la dernière période de cinq-minute. Cet objet désapprouve l'objet avgBusy5 de l'OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5
cpmCPUTotal5sec	Pourcentage occupé global CPU pendant la dernière période de cinq secondes. Obsolesces de cet objet l'objet de busyPer de l'OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.3
sysTraffic	Le pourcentage de l'utilisation de bande passante pour l'intervalle de sondage précédent	1.3.6.1.4.1.9.5.1.1.8
sysTrafficPeak	La valeur de mesure du trafic maximal depuis la dernière époque les compteurs de port ont été effacées ou le système a	1.3.6.1.4.1.9.5.1.1.19

	commencé	
sysTrafficPeaktime	Le temps (dans les centièmex d'une seconde) puisque la valeur de mesure du trafic maximal s'est produite	1.3.6.1.4.1.9.5.1.1.20
portTopNUtilization	Utilisation du port dans le système	1.3.6.1.4.1.9.5.1.20.2.1.4
portTopNBufferOverFlow	Le nombre de débordements de 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	Le nombre de paquets relâchés parce que la file d'attente d'entrée était pleine	1.3.6.1.4.1.9.2.2.1.1.26
locIfOutputQueueDrops	Le nombre de paquets relâchés parce que la file d'attente de sortie était pleine	1.3.6.1.4.1.9.2.2.1.1.27
locIfInCRC	Le nombre de paquets en entrée qui ont eu des erreurs cycliques de somme de contrôle de Redondance	1.3.6.1.4.1.9.2.2.1.1.12

Alarme et commandes de configuration d'événement de RMON

Alarmes

Des alarmes de RMON peuvent être configurées avec la syntaxe suivante :

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

Élément	Description
nombre	Le numéro d'alarme, qui est identique à l'alarmIndex dans l'alarmTable dans le MIB RMON.
variable	L'objet MIB à surveiller, qui se traduit en alarmVariable utilisé dans l'alarmTable du MIB RMON.
intervalle	Le temps, en quelques secondes, l'alarme surveille la variable MIB, qui est identique à l'alarmInterval utilisé dans l'alarmTable du MIB

	RMON.
delta	Teste la modification entre les variables MIB, qui affecte l'alarmSampleType dans l'alarmTable du MIB RMON.
absolu	Teste chaque variable MIB directement, qui affecte l'alarmSampleType dans l'alarmTable du MIB RMON.
valeur du seuil montant	La valeur à laquelle l'alarme est déclenchée.
numéro d'événement	(Facultatif) le numéro d'événement à déclencher quand la montée ou le seuil de chute dépasse sa limite. Cette valeur est identique à l'alarmRisingEventIndex ou à l'alarmFallingEventIndex dans l'alarmTable du MIB RMON.
valeur de seuil de chute	La valeur à laquelle l'alarme est remise à l'état initial.
chaîne de caractères du propriétaire	(Facultatif) spécifie un propriétaire pour l'alarme, qui est identique à l'alarmOwner dans l'alarmTable du MIB RMON.

Événements

Des événements de RMON peuvent être configurés avec la syntaxe suivante :

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

Élément	Description
nombre	Numéro d'événement assigné, qui est identique à l'eventIndex dans l'eventTable dans le MIB RMON.
log	(Facultatif) génère une entrée de journal de RMON quand l'événement est déclenché et place l'eventType dans le MIB RMON pour se connecter ou le log-et-déroutement.
le déroutement de	Chaîne de caractères de la communauté SNMP (facultative) utilisée pour ce déroutement. Configure la configuration de l'eventType dans le MIB RMON pour cette ligne comme SNMP-

communauté	déroutement ou log-et-déroutement. Cette valeur est identique à l'eventCommunityValue dans l'eventTable dans le MIB RMON.
chaîne de description	(Facultatif) spécifie une description de l'événement, qui est identique à la description d'événement dans l'eventTable du MIB RMON.
chaîne de caractères du propriétaire	Propriétaire (facultatif) de cet événement, qui est identique à l'eventOwner dans l'eventTable du MIB RMON.

Alarme et implémentation d'événement de RMON

Pour des informations détaillées sur l'alarme et l'implémentation d'événement de RMON, lisez s'il vous plaît la section d'alarme et d'implémentation d'événement de RMON du livre blanc de *pratiques recommandées de systèmes d'administration de réseaux*.

Informations connexes

- Soutien technique et documentation - Cisco Systems