White paper sulle best practice per i processi di base

Sommario

Introduzione

In questo documento vengono descritti i concetti e le procedure di base per le reti a disponibilità elevata. Include fattori di successo critici per l'utilizzo della rete come base e soglia per valutare il successo. Fornisce inoltre dettagli significativi per i processi di base e di soglia e per l'implementazione che seguono le linee guida delle best practice identificate dal team HAS (High Availability Services) di Cisco.

In questo documento viene illustrato in modo dettagliato il processo di creazione della baseline. Alcuni prodotti NMS (Network Management System) attuali possono aiutare ad automatizzare questo processo, tuttavia, il processo di base rimane lo stesso indipendentemente dal fatto che si utilizzino strumenti automatizzati o manuali. Se si utilizzano questi prodotti NMS, è necessario modificare le impostazioni di soglia predefinite per l'ambiente di rete specifico. È importante disporre di un processo per scegliere in modo intelligente tali soglie in modo che siano significative e corrette.

Previsione

Definizione di baseline

Una linea di base è un processo per lo studio della rete a intervalli regolari al fine di garantire che la rete funzioni come previsto. Si tratta di più di un singolo rapporto che descrive dettagliatamente lo stato della

rete in un determinato momento. Seguendo il processo di baseline, è possibile ottenere le seguenti informazioni:

- Ottenere informazioni importanti sullo stato dell'hardware e del software
- Determinare l'utilizzo corrente delle risorse di rete
- Prendere decisioni accurate sulle soglie degli allarmi di rete
- Identificazione dei problemi di rete correnti
- Prevedere i problemi futuri

Nel diagramma seguente è illustrato un altro modo di esaminare la linea di base.

La linea rossa, il punto di interruzione della rete, è il punto in cui la rete si interrompe, che viene determinato dalla conoscenza delle prestazioni dell'hardware e del software. La linea verde, il carico di rete, rappresenta la progressione naturale del carico sulla rete man mano che vengono aggiunte nuove applicazioni e altri fattori di questo tipo.

Lo scopo di una baseline è determinare:

- Posizione della rete sulla linea verde
- Velocità di aumento del carico di rete
- Speriamo di prevedere in che momento i due si interseceranno

Eseguendo una baseline a intervalli regolari, è possibile individuare lo stato corrente *ed* estrapolare eventuali errori e prepararli in anticipo. Questo consente anche di prendere decisioni più informate su quando, dove e come spendere i soldi del budget per gli aggiornamenti della rete.

Perché una baseline?

Un processo di previsione consente di identificare e pianificare correttamente i problemi critici di limitazione delle risorse nella rete. Questi problemi possono essere descritti come risorse del piano di controllo o risorse del piano dati. Le risorse Control Plane sono specifiche della piattaforma e dei moduli all'interno del dispositivo e possono essere interessate da diversi problemi, tra cui:

- Utilizzo dei dati
- Funzionalità attivate
- Progettazione della rete

Le risorse Control Plane includono parametri quali:

- Utilizzo CPU
- Utilizzo della memoria

- Utilizzo buffer

Le risorse del piano dati sono influenzate solo dal tipo e dalla quantità di traffico e includono l'utilizzo del collegamento e del backplane. Basando l'utilizzo delle risorse per le aree critiche, è possibile evitare gravi problemi di prestazioni o, peggio ancora, un collasso della rete.

Con l'introduzione di applicazioni sensibili alla latenza, quali voce e video, è ora più importante che mai baselining. Le applicazioni TCP/IP (Transmission Control Protocol/Internet Protocol) tradizionali perdono e consentono un certo ritardo. Voce e video sono basati sul protocollo UDP (User Datagram Protocol) e non consentono ritrasmissioni o congestione della rete.

Grazie alla nuova combinazione di applicazioni, la definizione della baseline consente di comprendere i problemi di utilizzo delle risorse sia del control plane che del data plane, nonché di pianificare in modo proattivo le modifiche e gli aggiornamenti per garantire il successo continuo.

Le reti di dati esistono da molti anni. Fino a poco tempo fa, mantenere le reti in funzione era un processo abbastanza perdonante, con un certo margine di errore. Con la crescente accettazione di applicazioni sensibili alla latenza, come VoIP (Voice over IP), il lavoro di gestione della rete sta diventando sempre più difficile e richiede maggiore precisione. Per essere più precisi e fornire a un amministratore di rete una solida base su cui gestire la rete, è importante avere un'idea di come la rete è in funzione. A tale scopo, è necessario eseguire un processo denominato previsione.

Obiettivo di base

L'obiettivo di una base di riferimento è:

1. Determinare lo stato corrente dei dispositivi di rete
2. Confrontare tale stato con le linee guida sulle prestazioni standard
3. Impostare le soglie per avvisare l'utente quando lo stato supera tali linee guida

A causa della grande quantità di dati e del tempo necessario per analizzarli, è innanzitutto necessario limitare l'ambito di una baseline per semplificare l'apprendimento del processo. Il punto di partenza più logico, e a volte il più vantaggioso, è il nucleo della rete. Questa parte della rete è in genere la più piccola e richiede la massima stabilità.

Per semplicità, questo documento spiega come basare un importantissimo Simple Network Management Protocol Management Information Base (SNMP MIB): cpmCPUTotal5min. cpmCPUTotal5min è la media decrescente di cinque minuti di un'unità di elaborazione centrale (CPU) di un router Cisco ed è un indicatore delle prestazioni del control plane. La linea di base verrà eseguita su un router Cisco serie 7000.

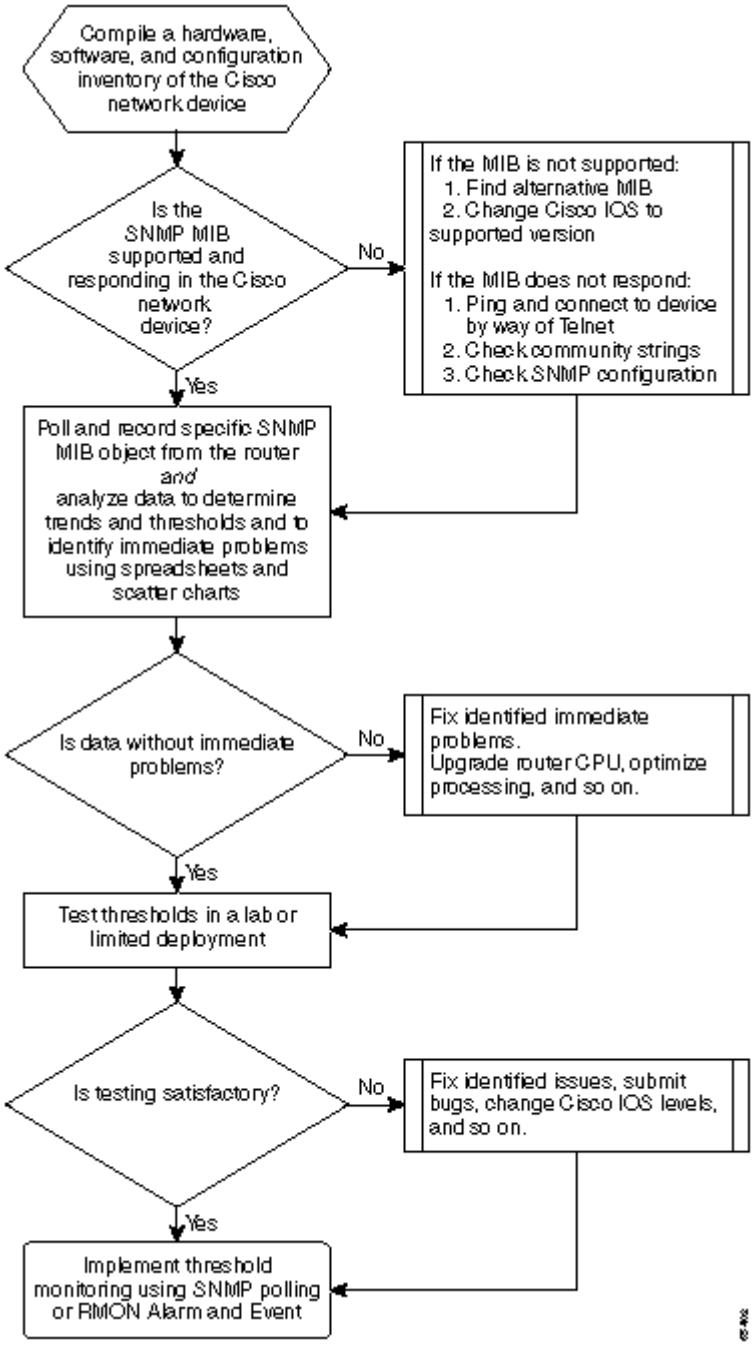
Una volta appreso il processo, è possibile applicarlo a qualsiasi dato disponibile nel vasto database SNMP disponibile nella maggior parte dei dispositivi Cisco, ad esempio:

- Utilizzo di ISDN (Integrated Services Digital Network)
- Perdita di celle nella modalità di trasferimento asincrono (ATM)
- Memoria di sistema libera

Diagramma di flusso della baseline principale

Il diagramma di flusso seguente mostra i passaggi di base del processo della baseline di base. Sebbene siano

disponibili prodotti e strumenti per eseguire alcuni di questi passaggi, tendono ad avere lacune in termini di flessibilità o facilità d'uso. Anche se si prevede di utilizzare gli strumenti del sistema di gestione della rete (NMS, Network Management System) per eseguire l'associazione alla baseline, si tratta comunque di un buon esercizio di analisi del processo e di comprensione del funzionamento reale della rete. Questo processo può anche togliere un po' di mistero dal funzionamento di alcuni strumenti NMS, poiché la maggior parte degli strumenti fa essenzialmente le stesse cose.



Procedura prevista

Fase 1: compilare un inventario di hardware, software e configurazione

È estremamente importante compilare un inventario di hardware, software e configurazione per diversi motivi. In primo luogo, i MIB Cisco SNMP sono, in alcuni casi, specifici della versione Cisco IOS in esecuzione. Alcuni oggetti MIB vengono sostituiti con nuovi oggetti o vengono, a volte, completamente eliminati. L'inventario dell'hardware è il più importante dopo la raccolta dei dati, in quanto le soglie da

impostare dopo la baseline iniziale sono spesso basate sul tipo di CPU, sulla quantità di memoria e così via, sui dispositivi Cisco. L'inventario delle configurazioni è importante anche per assicurarsi di conoscere le configurazioni correnti: è possibile modificare le configurazioni dei dispositivi dopo la baseline per ottimizzare i buffer e così via.

Il modo più efficiente per fare questa parte della linea di base per una rete Cisco è con CiscoWorks 2000 Resource Manager Essentials (Essentials). Se il software è installato correttamente nella rete, Essentials deve avere gli inventari correnti di tutti i dispositivi nel proprio database. Basta guardare gli inventari per vedere se ci sono problemi.

La tabella seguente è un esempio di report di inventario del software Cisco Router Class esportato da Essentials e quindi modificato in Microsoft Excel. Da questo inventario, è necessario usare i dati MIB SNMP e gli OID (Object Identifier) trovati nelle versioni 12.0x e 12.1x di Cisco IOS.

Nome dispositivo	Tipo di router	Version	Versione del software
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)

Se Essentials non è installato in rete, è possibile utilizzare lo strumento da riga di comando UNIX **snmpwalk** da una workstation UNIX per trovare la versione IOS. come illustrato nell'esempio seguente. Se non si è certi del funzionamento del comando, digitare **man snmpwalk** al prompt di UNIX per ulteriori informazioni. La versione IOS è importante in quando si inizia a scegliere gli OID MIB da baseline, poiché gli oggetti MIB sono dipendenti da IOS. Inoltre, conoscendo il tipo di router, è possibile determinare in un secondo momento le soglie per la CPU, i buffer e così via.

```
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
```

Passaggio 2: Verificare che il MIB SNMP sia supportato nel router

Ora che si dispone di un inventario del dispositivo su cui si desidera eseguire il polling per la baseline, è possibile iniziare a scegliere gli OID specifici su cui eseguire il polling. Risparmia un sacco di frustrazione se si verifica, in anticipo, che i dati che si desidera sono effettivamente lì. L'oggetto MIB cpmCPUTotal5min si trova in CISCO-PROCESS-MIB.

Per trovare l'OID di cui si desidera eseguire il polling, è necessaria una tabella di conversione disponibile sul sito Web CCO di Cisco. Per accedere a questo sito Web da un browser, andare alla pagina MIB Cisco e fare clic sul collegamento OIDs.

Per accedere al sito Web da un server FTP, digitare **ftp://ftp.cisco.com/pub/mibs/oid/**. Da questo sito è possibile scaricare il MIB specifico che è stato decodificato e ordinato in base ai numeri OID.

L'esempio seguente viene estratto dalla tabella CISCO-PROCESS-MIB.oid. Nell'esempio viene mostrato che l'OID per il MIB **cpmCPUTotal5min** è .1.3.6.1.4.1.9.9.109.1.1.1.1.5.

Nota: non dimenticare di aggiungere un "." all'inizio dell'OID. In caso contrario, verrà visualizzato un messaggio di errore quando si tenta di eseguire il polling. Per creare un'istanza dell'OID, è inoltre necessario aggiungere ".1" alla fine dell'OID. Indica al dispositivo l'istanza dell'OID che si sta cercando. In alcuni casi, gli OID dispongono di più istanze di un particolare tipo di dati, ad esempio quando un router dispone di più CPU.

<#root>

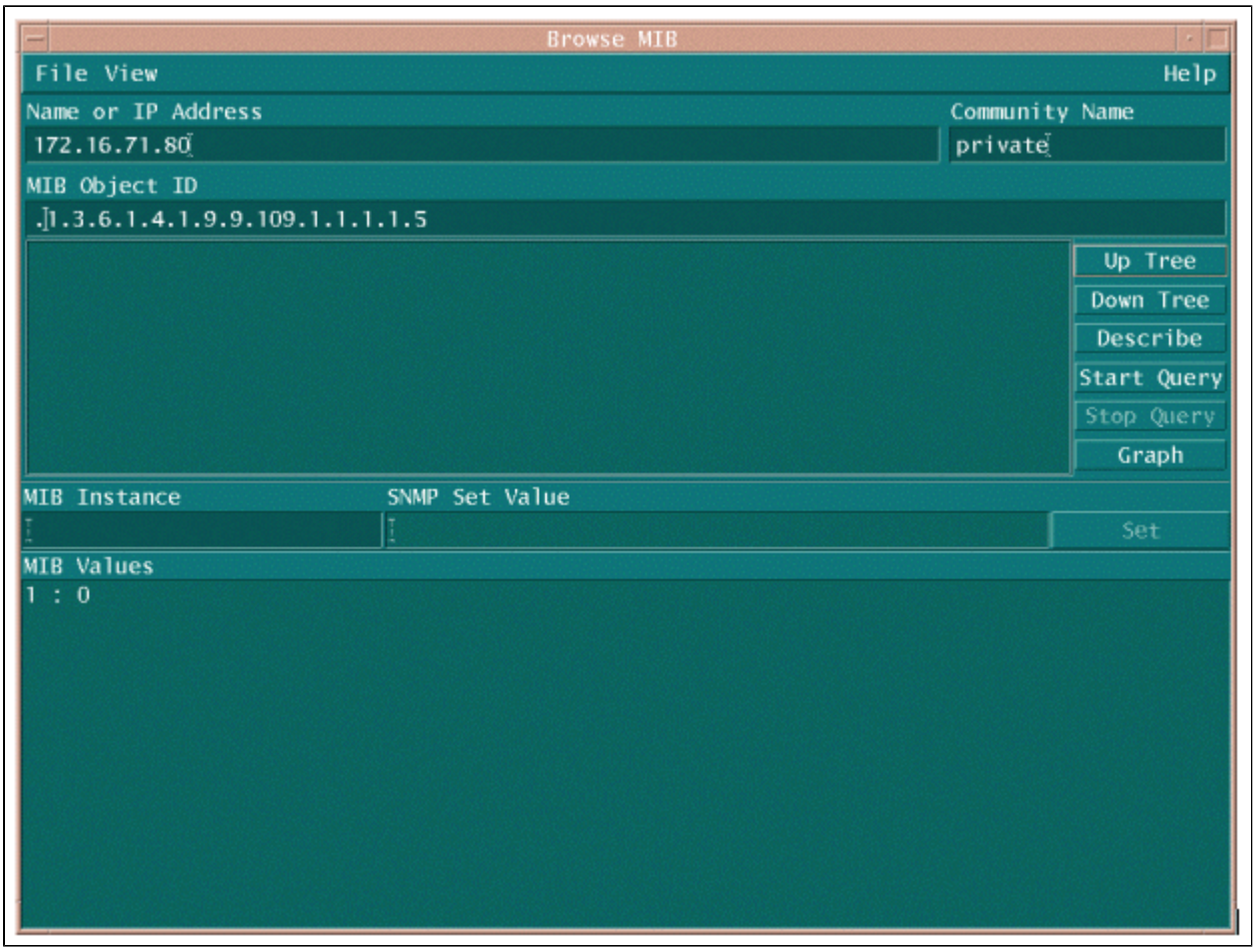
```
ftp://ftp.cisco.com/pub/mibs/oid/CISCO-PROCESS-MIB.oid
### THIS FILE WAS GENERATED BY MIB2SCHEMA
"org" "1.3"
"dod" "1.3.6"
"internet" "1.3.6.1"
"directory" "1.3.6.1.1"
"mgmt" "1.3.6.1.2"
"experimental" "1.3.6.1.3"
"private" "1.3.6.1.4"
"enterprises" "1.3.6.1.4.1"
"cisco" "1.3.6.1.4.1.9"
"ciscoMgmt" "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"
```

Esistono due metodi comuni per eseguire il polling dell'OID MIB per verificare che sia disponibile e funzioni correttamente. È consigliabile eseguire questa operazione prima di avviare la raccolta di massa dei dati, in modo da non sprecare tempo a eseguire il polling di un elemento non presente e finire con un

database vuoto. A tale scopo, è possibile utilizzare MIB walker della piattaforma NMS, ad esempio HP OpenView Network Node Manager (NNM) o CiscoWorks Windows, e immettere l'OID che si desidera controllare.

Di seguito è riportato un esempio di HP OpenView SNMP MIB walker.



Un altro modo semplice per eseguire il polling dell'OID MIB consiste nell'utilizzare il comando UNIX **snmpwalk**, come illustrato nell'esempio seguente.

```
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.cpmCPUTo
```

In entrambi gli esempi, il MIB ha restituito il valore 0, il che significa che per quel ciclo di polling la CPU ha restituito un utilizzo medio dello 0%. In caso di problemi nell'ottenere la risposta del dispositivo con i dati corretti, provare a eseguire il ping del dispositivo e ad accedere al dispositivo tramite Telnet. Se il problema persiste, controllare la configurazione SNMP e le stringhe della community SNMP. Per eseguire questa operazione, potrebbe essere necessario trovare un MIB alternativo o un'altra versione di IOS.

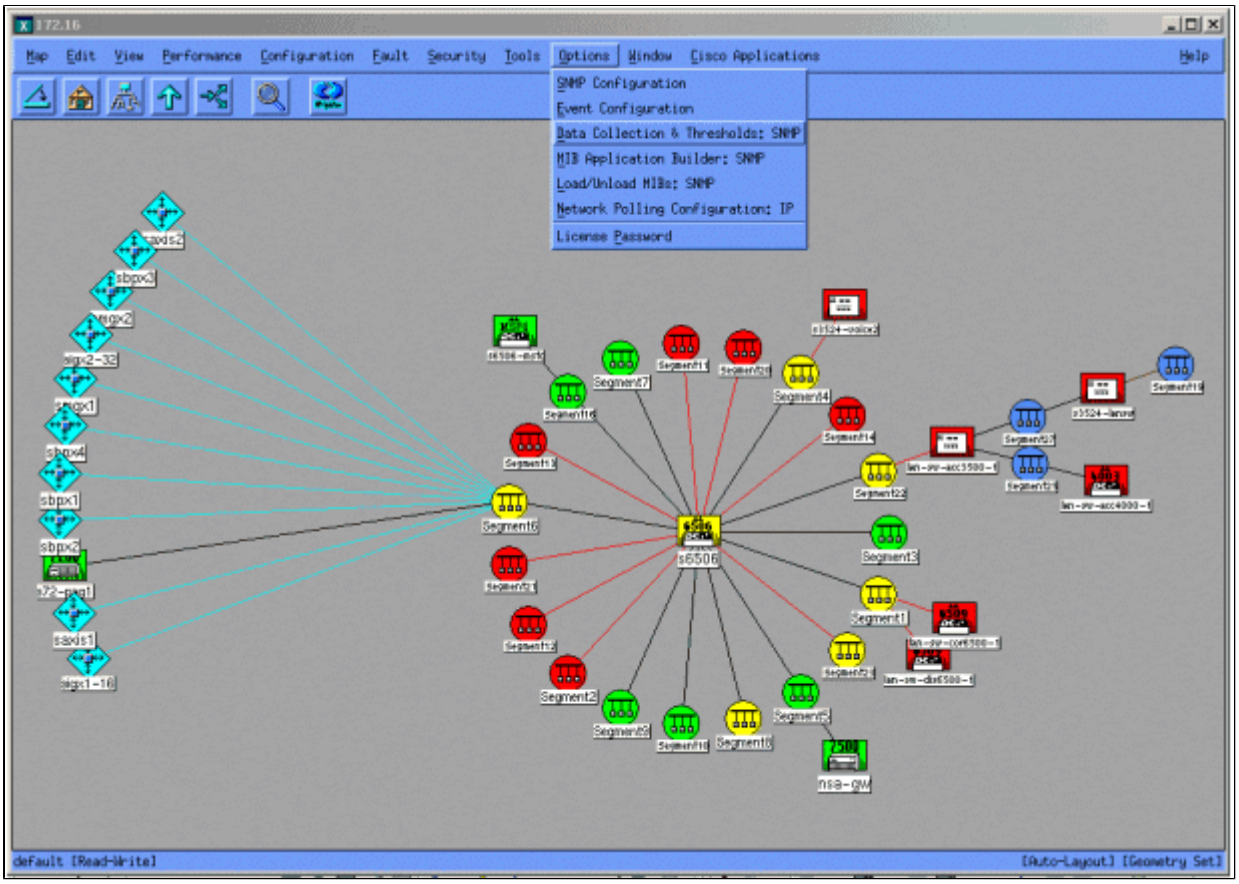
Passaggio 3: Eseguire il polling e registrare un oggetto MIB SNMP specifico dal router

Esistono diversi modi per eseguire il polling degli oggetti MIB e registrare l'output. Sono disponibili prodotti in commercio, prodotti shareware, script e strumenti dei fornitori. Tutti gli strumenti front-end

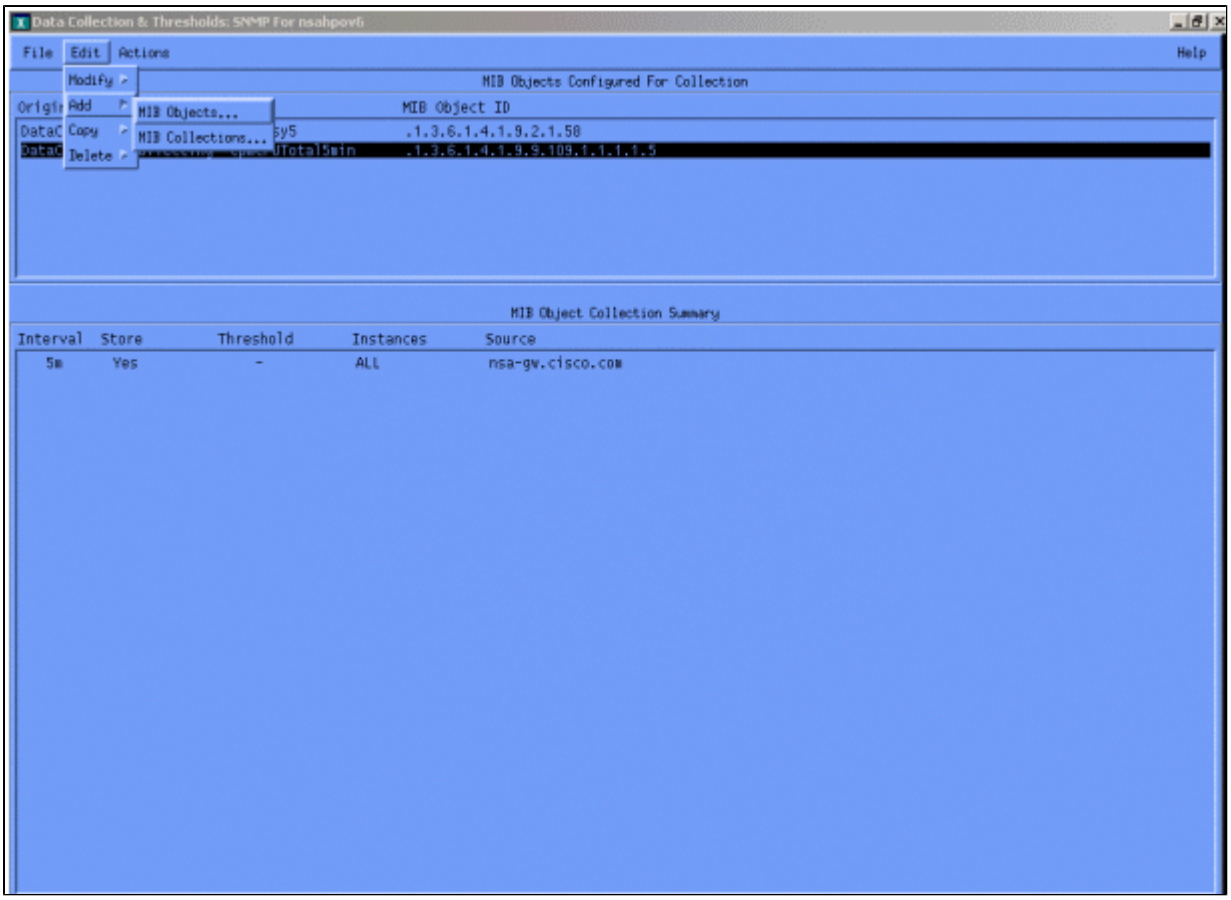
utilizzano il processo SNMP **get** per ottenere le informazioni. Le differenze principali riguardano la flessibilità della configurazione e il modo in cui i dati vengono registrati in un database. Di nuovo, guardate il MIB del processore per vedere come funzionano questi vari metodi.

Ora che si è certi che l'OID è supportato nel router, è necessario decidere la frequenza di polling e di registrazione. Cisco consiglia di eseguire il polling del MIB della CPU a intervalli di cinque minuti. Un intervallo più basso aumenterebbe il carico sulla rete o sul dispositivo e, poiché il valore MIB è una media di cinque minuti, non sarebbe utile eseguire il polling più spesso del valore medio. È inoltre consigliabile che il polling di base abbia un periodo di almeno due settimane, in modo da poter analizzare almeno due cicli aziendali settimanali sulla rete.

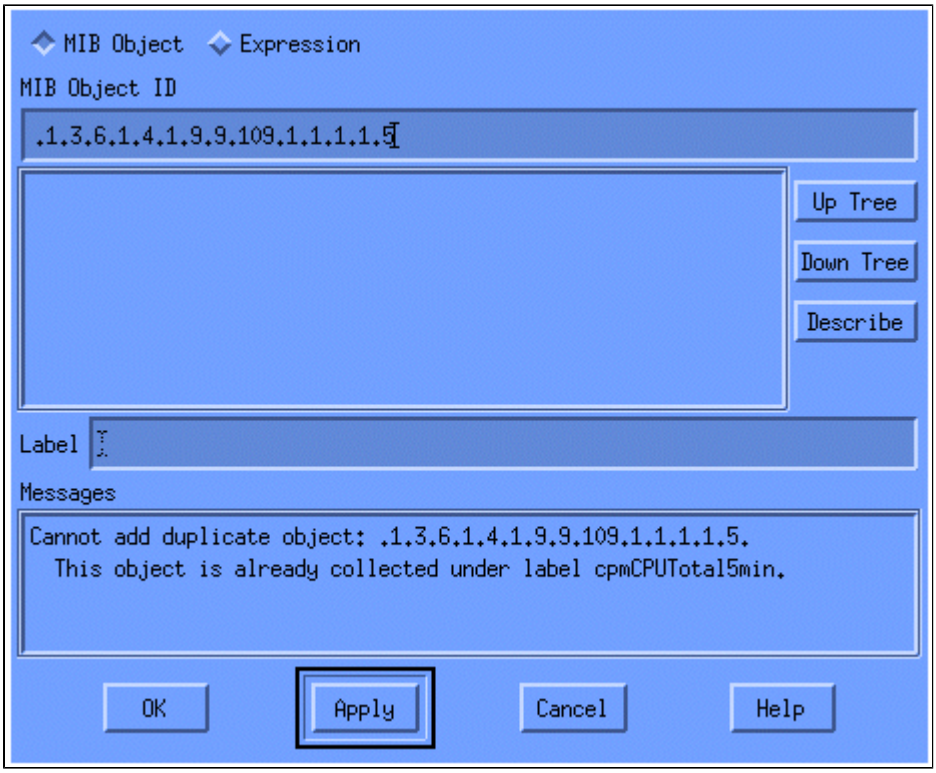
Le seguenti schermate mostrano come aggiungere gli oggetti MIB con HP OpenView Network Node Manager versione 6.1. Dalla schermata principale, selezionare **Opzioni > Raccolta dati e soglie**.



Quindi selezionare **Modifica > Aggiungi > Oggetti MIB**.

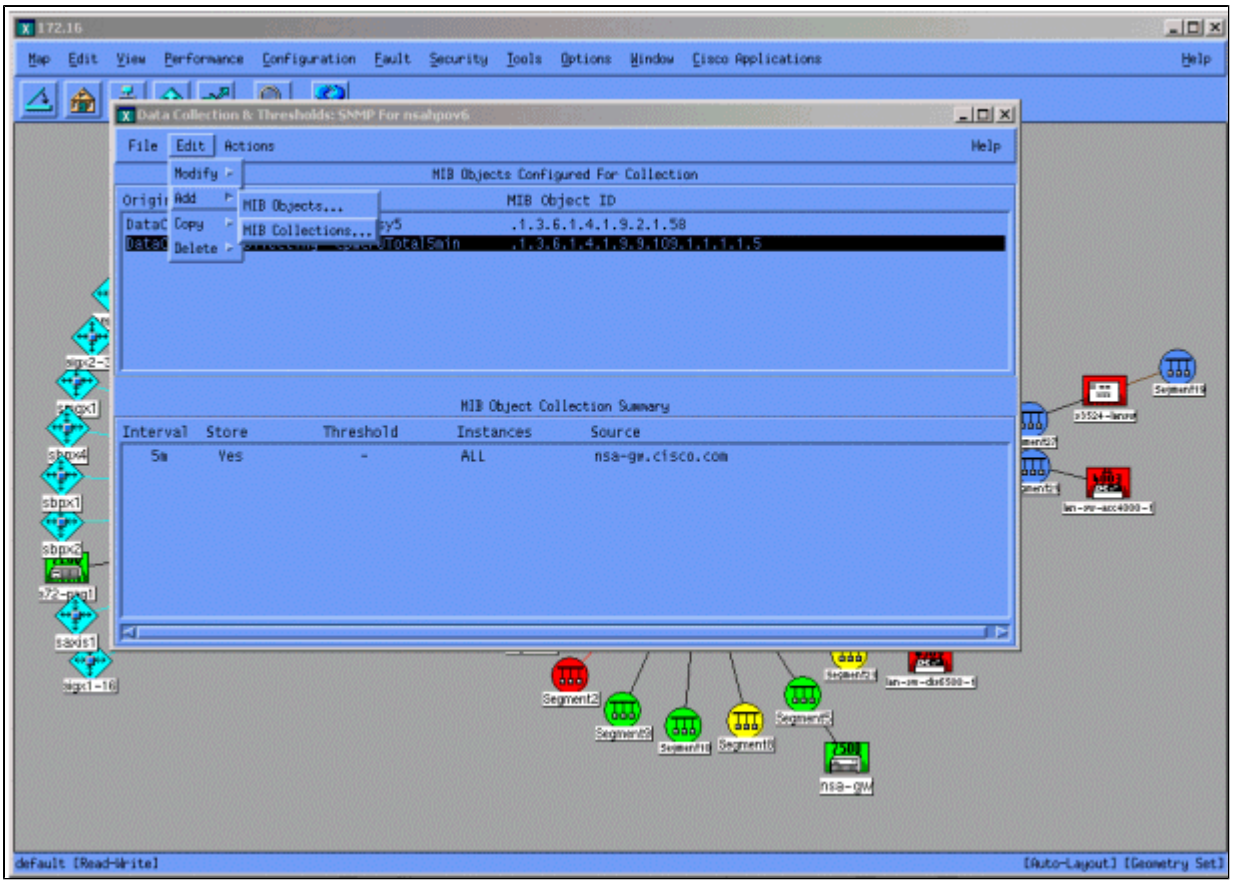


Dal menu, aggiungere la stringa OID e fare clic su **Applica**. A questo punto è stato immesso l'oggetto MIB nella piattaforma HP OpenView in modo che sia possibile eseguirne il polling.



È quindi necessario comunicare ad HP OpenView il router su cui eseguire il polling per questo OID.

Dal menu Raccolta dati, selezionare **Modifica > Aggiungi > Raccolte MIB**.

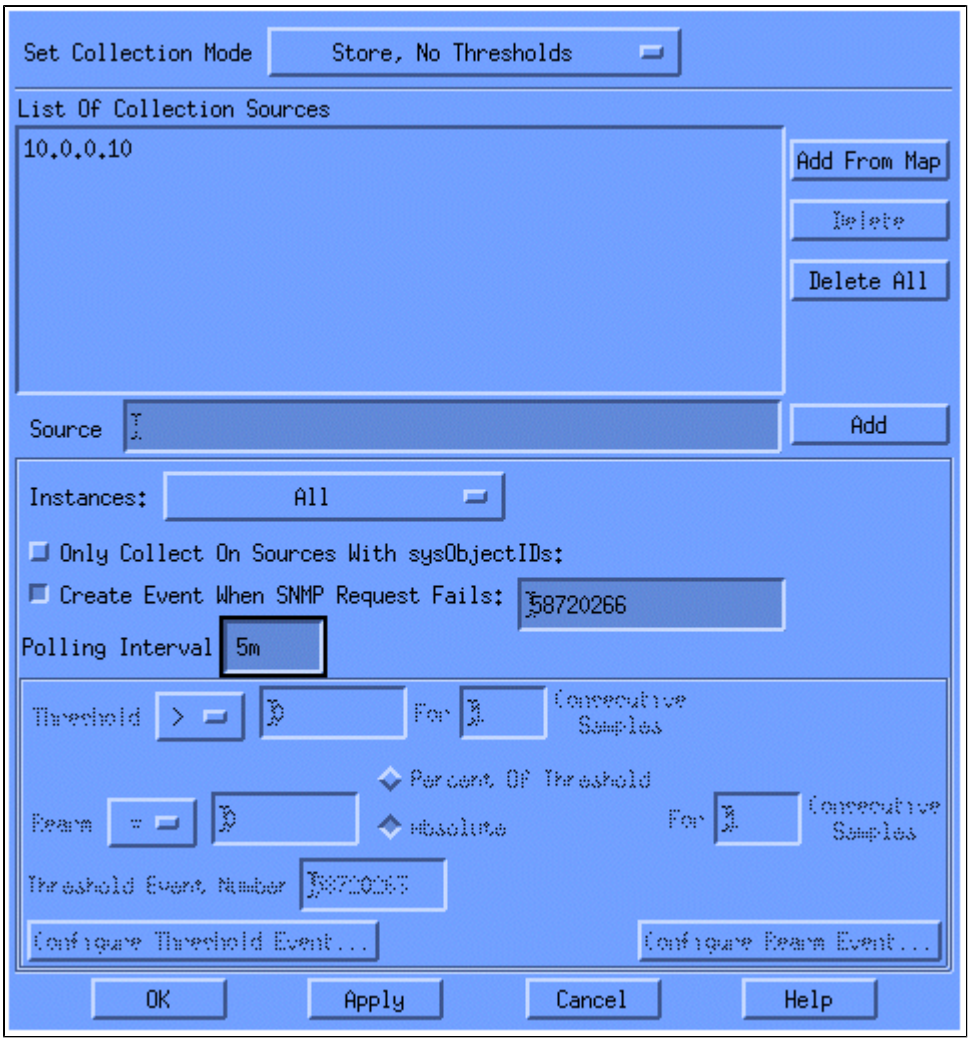


Nel campo Source (Origine), immettere il nome DNS (Domain Naming System) o l'indirizzo IP del router di cui eseguire il polling.

Selezionare **Archivio, Nessuna soglia** dall'elenco Imposta modalità di raccolta.

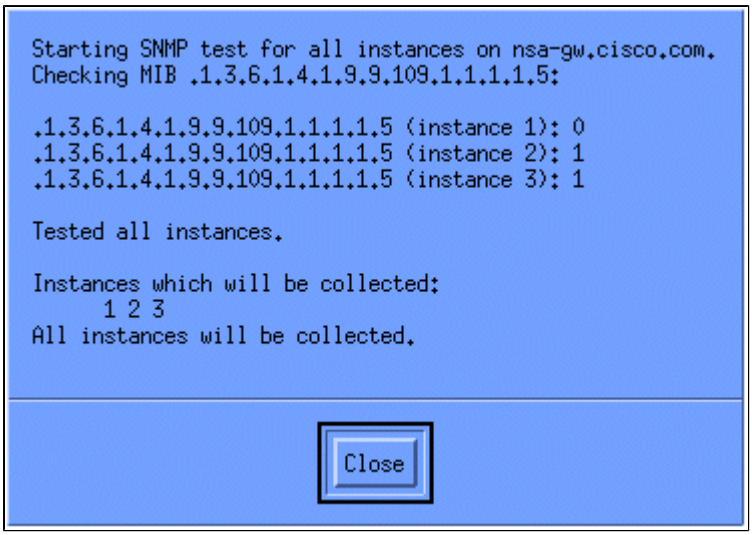
Impostare Intervallo di polling su **5m**, per intervalli di cinque minuti.

Fare clic su **Apply** (Applica).



Per rendere effettive le modifiche, è necessario selezionare **File > Salva**.

Per verificare che la raccolta sia impostata correttamente, evidenziare la riga di riepilogo raccolta per il router e selezionare **Azioni > Test SNMP**. Questo controllo verifica se la stringa della community è corretta ed esegue il polling per tutte le istanze dell'OID.



Fare clic su **Chiudi** e lasciare che l'insieme venga eseguito per una settimana. Al termine del periodo settimanale, estrarre i dati per l'analisi.

L'analisi dei dati risulta più semplice se si esegue il dump in un file ASCII e lo si importa in un foglio di calcolo come Microsoft Excel. A tale scopo, con HP OpenView NNM è possibile utilizzare lo strumento da riga di comando **snmpColDump**. Ogni insieme configurato scrive in un file nella directory /var/opt/OV/share/databases/snmpCollect/.

Estrarre i dati in un file ASCII denominato **testfile** con il comando seguente:

<#root>

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

```
testfile
```

Nota: cpmCPUTotal5min.1 è il file di database creato da HP OpenView NNM all'inizio del polling OID.

Il file di test generato è simile all'esempio seguente.

```
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/â€¦â€¦â€¦
```

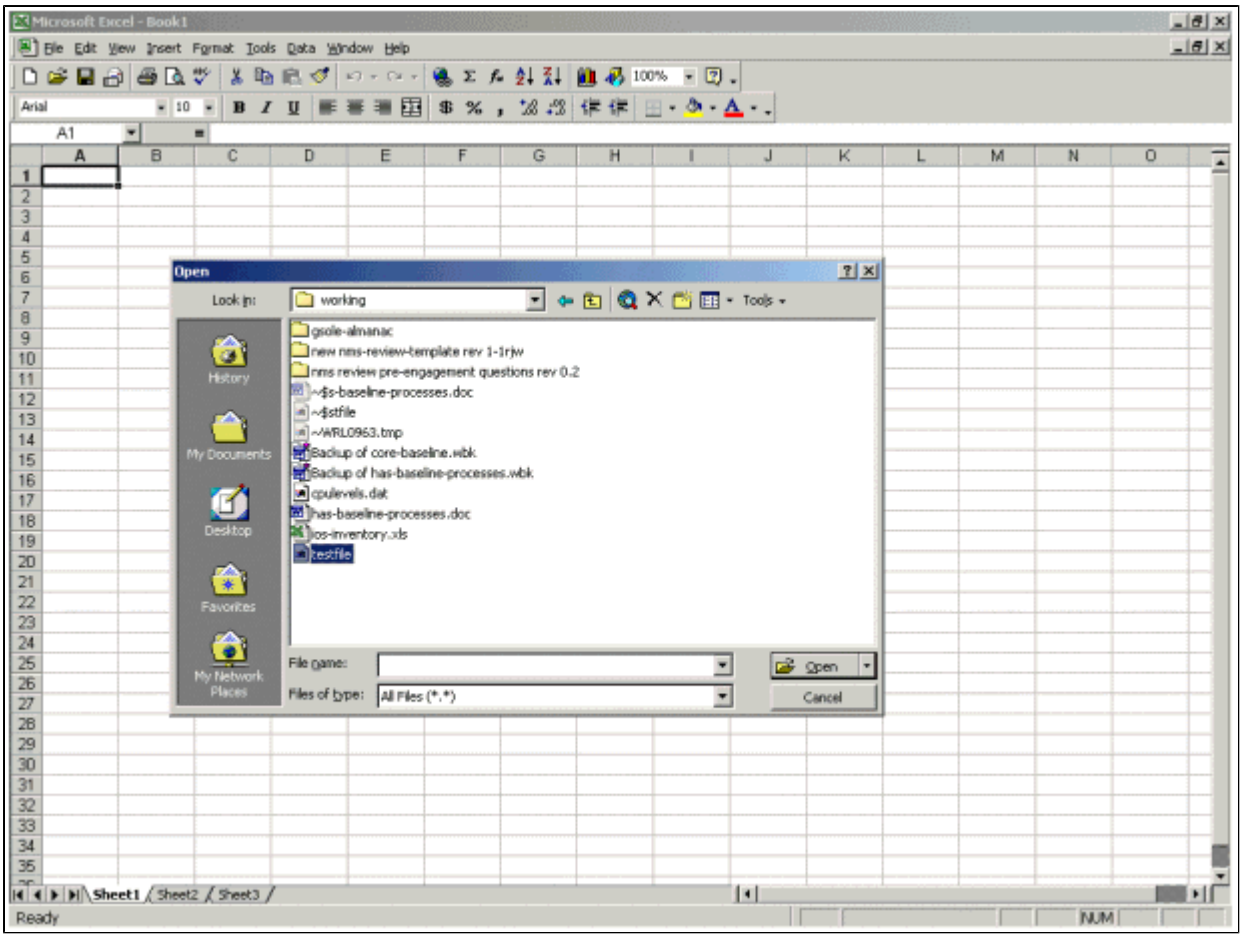
Una volta che l'output del file di test si trova sulla stazione UNIX, è possibile trasferirlo sul PC utilizzando il protocollo FTP (File Transfer Protocol).

È inoltre possibile raccogliere i dati utilizzando script personalizzati. A tale scopo, eseguire uno **snmpget** per l'OID della CPU ogni cinque minuti ed eseguire il dump dei risultati in un file CSV.

Passo 4: Analizzare i dati per determinare le soglie

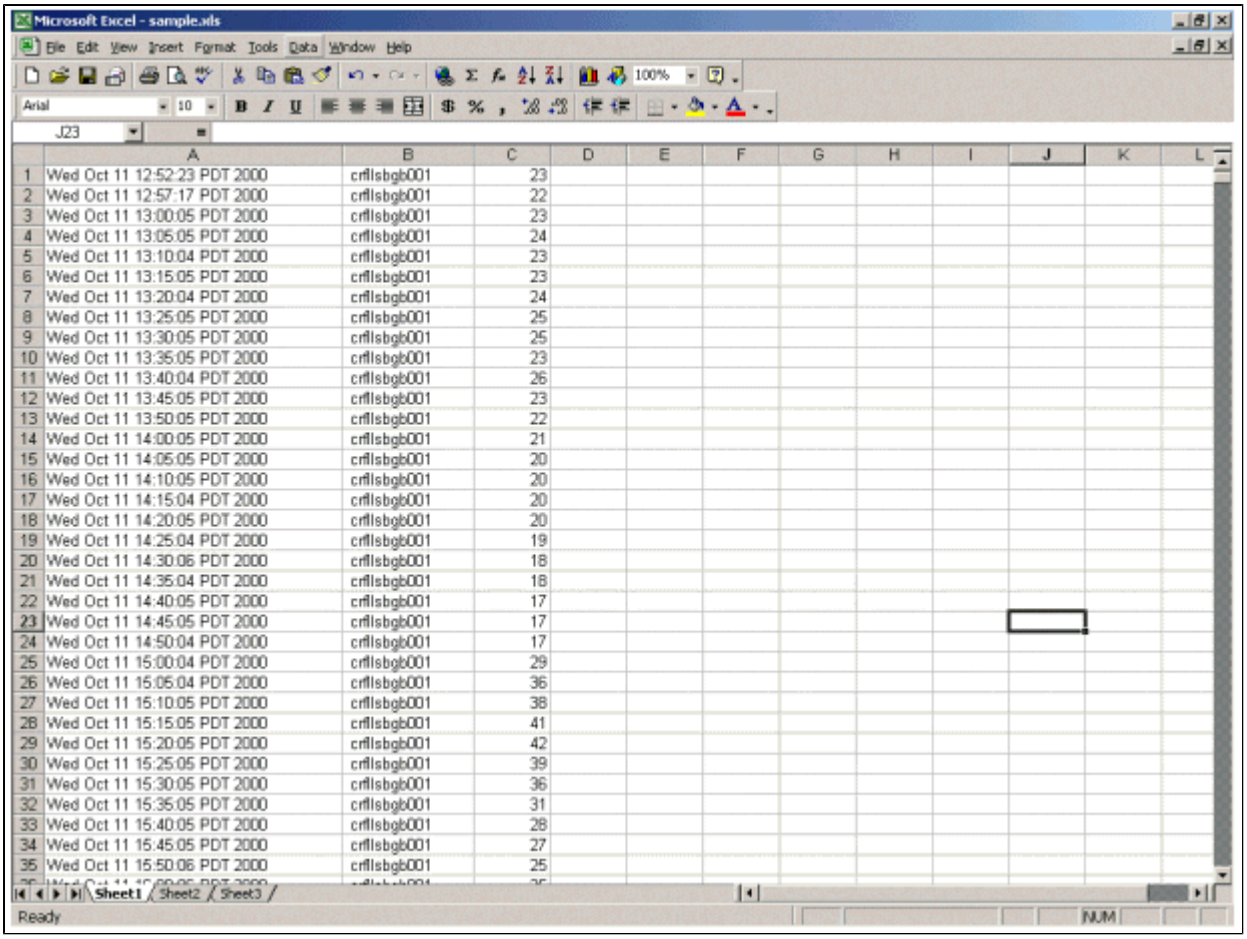
Ora che avete alcuni dati, potete iniziare ad analizzarli. Questa fase della baseline determina le impostazioni di soglia utilizzabili che rappresentano una misura accurata delle prestazioni o degli errori e non attivano troppi allarmi quando si attiva il monitoraggio delle soglie. Uno dei metodi più semplici per eseguire questa operazione consiste nell'importare i dati in un foglio di calcolo come Microsoft Excel e nel tracciare un grafico a dispersione. Questo metodo semplifica notevolmente la visualizzazione del numero di volte in cui un determinato dispositivo avrebbe creato un avviso di eccezione se lo si stesse monitorando per una determinata soglia. Non è consigliabile attivare le soglie senza eseguire una baseline, in quanto ciò potrebbe generare allarmi da dispositivi che hanno superato la soglia scelta.

Per importare il file di test in un foglio di calcolo di Excel, aprire Excel e selezionare **File > Apri**, quindi selezionare il file di dati.



L'applicazione Excel chiede quindi di eseguire l'importazione del file.

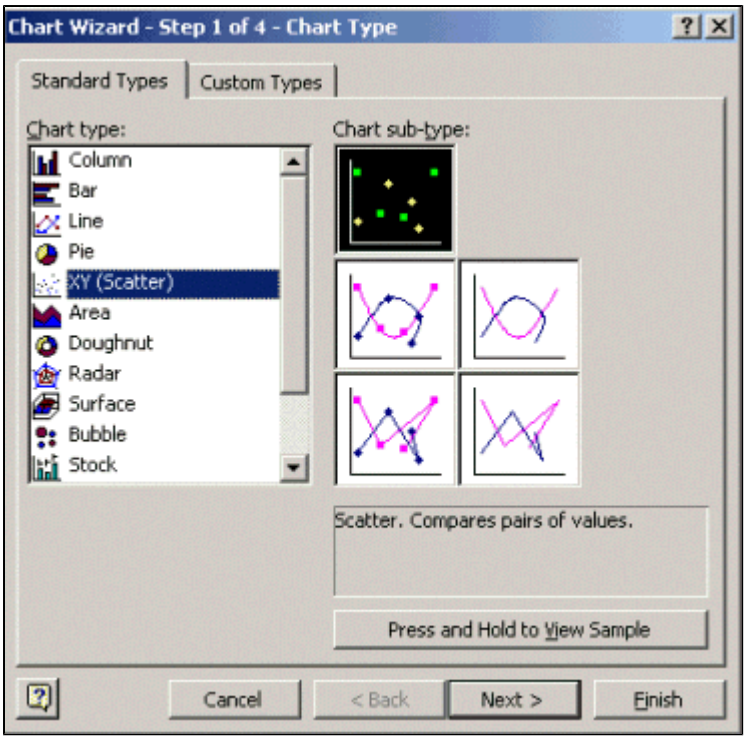
Al termine, il file importato dovrebbe avere un aspetto simile alla seguente schermata.



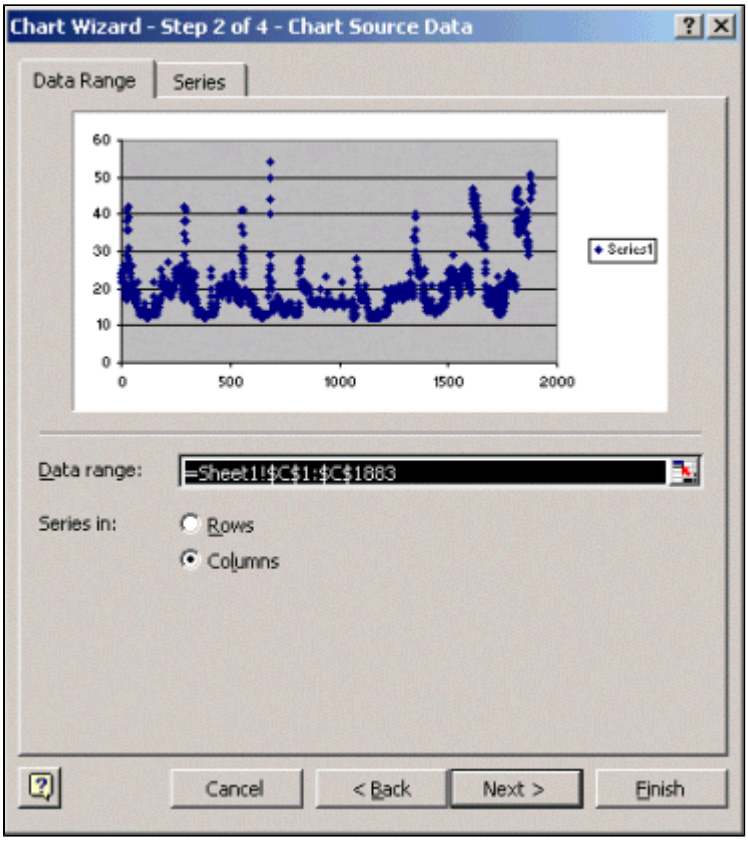
Un grafico a dispersione consente di visualizzare più facilmente il funzionamento delle varie impostazioni di soglia nella rete.

Per creare il grafico a dispersione, evidenziare la colonna C nel file importato, quindi fare clic sull'icona **Creazione guidata Grafico**. Seguire quindi i passaggi della Creazione guidata Grafico per creare un grafico a dispersione.

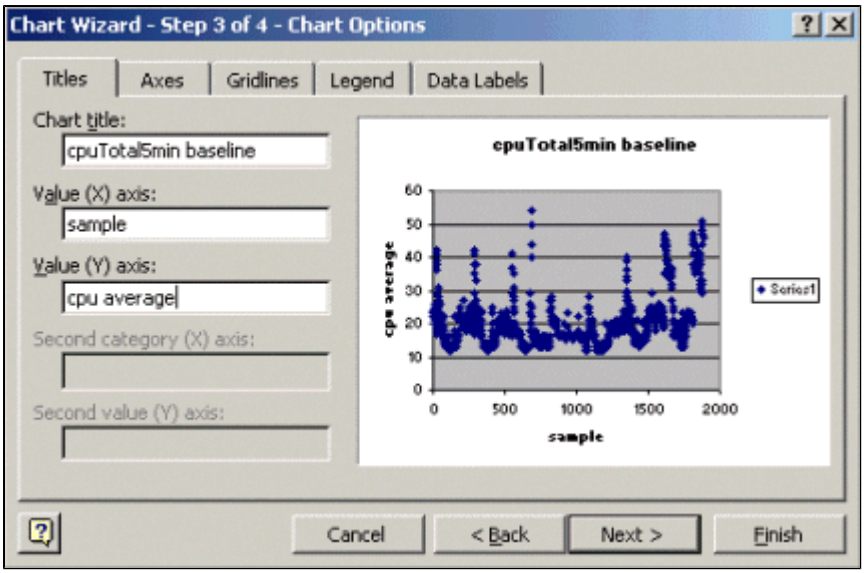
Nel passaggio 1 della Creazione guidata Grafico, come illustrato di seguito, selezionare la scheda **Tipi standard** e selezionare il tipo di grafico a **dispersione (XY)**. Quindi fare clic su **Avanti**.



Nel passaggio 2 della Creazione guidata Grafico, come illustrato di seguito, selezionare la scheda **Intervallo dati** e selezionare l'intervallo di dati e l'opzione **Colonne**. Fare clic su **Next** (Avanti).



Nel passaggio 3 della Creazione guidata Grafico, come illustrato di seguito, immettere il titolo del grafico e i valori degli assi X e Y, quindi fare clic su **Avanti**.



Nel passaggio 4 della Creazione guidata Grafico, scegliere se si desidera che il grafico a dispersione si trovi in una nuova pagina o come oggetto nella pagina esistente.

Fare clic su **Fine** per posizionare il grafico nella posizione desiderata.

"E se?" Analisi

È ora possibile utilizzare il grafico a dispersione per l'analisi. Tuttavia, prima di procedere, è necessario porre le seguenti domande:

- Cosa consiglia il fornitore (in questo esempio il fornitore è Cisco) come soglia per questa variabile MIB?

  In generale, Cisco consiglia di non superare il 60% di utilizzo medio della CPU di un router core. È stato scelto il 60% perché un router ha bisogno di un sovraccarico in caso di problemi o di errori della rete. Cisco stima che un router core abbia bisogno di circa il 40% di sovraccarico della CPU nel caso in cui un protocollo di routing debba ricalcolare o riconvertire. Queste percentuali variano in base ai protocolli utilizzati e alla topologia e stabilità della rete.

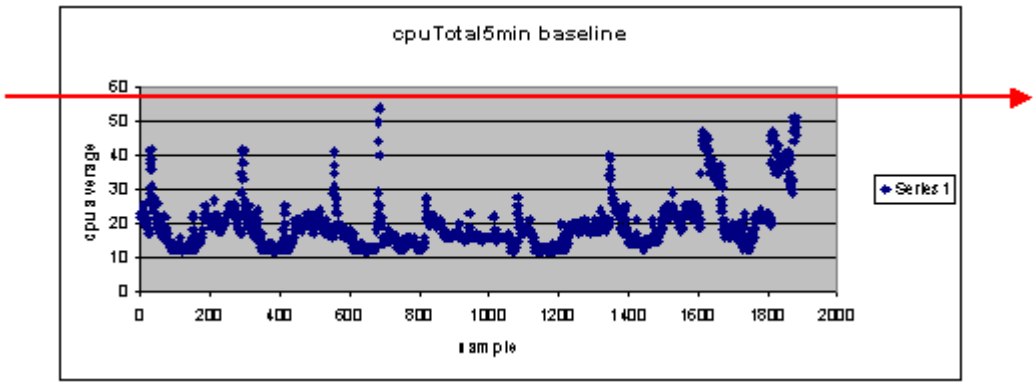
- Cosa succede se si utilizza il 60% come impostazione di soglia?

  Se si traccia una linea sul grafico a dispersione in orizzontale a 60, si noterà che nessuna delle coordinate supera il 60% di utilizzo della CPU. Pertanto, una soglia di 60 punti impostata sulle stazioni del sistema di gestione della rete (NMS) non ha attivato un allarme di soglia durante il periodo di voto. Per questo router è accettabile una percentuale di 60. Tuttavia, nel grafico a dispersione alcune delle coordinate sono vicine a 60. Sarebbe bello sapere quando un router si sta avvicinando alla soglia del 60% in modo da sapere in anticipo che la CPU si sta avvicinando al 60% e avere un piano per cosa fare quando raggiunge quel punto.

- Cosa succede se si imposta la soglia al 50%?

  Si stima che questo router abbia raggiunto il 50% di utilizzo quattro volte durante questo ciclo di polling e avrebbe generato ogni volta un allarme di soglia. Questo processo diventa più importante quando si esaminano *i gruppi di router* per verificare quale sarebbe la funzione delle diverse impostazioni di soglia. Ad esempio, "Cosa succede se si imposta la soglia al 50% per l'intera rete principale?" Vedete, è molto difficile scegliere un solo numero.

Analisi "What If" soglia CPU



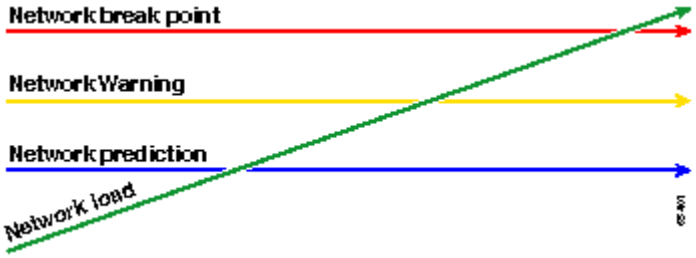
Una strategia che può essere utilizzata per semplificare questa operazione è la metodologia di soglia Pronto, Imposta, Vai. Questa metodologia utilizza tre numeri di soglia in successione.

- Pronto: la soglia impostata come predittore dei dispositivi che richiedono probabilmente attenzione in futuro.
- Imposta: la soglia utilizzata come indicatore anticipato, che avvisa l'utente di iniziare la pianificazione di una riparazione, riconfigurazione o aggiornamento.
- Goâ€”la soglia che tu e/o il fornitore ritenete essere una condizione di errore e che richiede qualche azione per ripararla; in questo esempio è il 60 per cento

Nella tabella seguente viene illustrata la strategia Pronto, Imposta, Vai.

Soglia	Azione	Risultato
45%	Esamina ulteriormente	Elenco delle opzioni per i piani d'azione
50%	Elaborazione piano d'azione	Elenco delle fasi del piano d'azione
60%	Attuazione del piano d'azione	Il router non supera più le soglie. Torna alla modalità Pronto

La metodologia Ready, Set, Go modifica il grafico di base originale descritto in precedenza. Nel diagramma seguente viene illustrato il grafico della linea di base modificata. Se è possibile identificare gli altri punti di intersezione nel grafico, si disporrà ora di più tempo per pianificare e reagire rispetto a prima.



Si noti che in questo processo, l'attenzione è focalizzata sulle eccezioni nella rete e non riguarda altri dispositivi. Si presume che i dispositivi fino a quando rimangono al di sotto delle soglie funzionino correttamente.

Se questi passaggi sono stati studiati fin dall'inizio, si sarà ben preparati per mantenere la rete integra. L'esecuzione di questo tipo di pianificazione è inoltre estremamente utile per la pianificazione del budget. Se si conoscono i primi cinque router **go**, i router **impostati per il** livello intermedio e i router **pronti per il**

livello inferiore, è possibile pianificare facilmente il budget necessario per gli aggiornamenti in base al tipo di router utilizzati e alle opzioni del piano d'azione disponibili. La stessa strategia può essere utilizzata per i collegamenti WAN (Wide Area Network) o qualsiasi altro OID MIB.

Passaggio 5: Risolvere i problemi immediati identificati

Si tratta di una delle parti più semplici del processo di base. Una volta identificati i dispositivi che superano la soglia di **go**, è necessario creare un piano d'azione per riportare tali dispositivi al di sotto della soglia.

È possibile aprire una richiesta con il Technical Assistance Center (TAC) di Cisco o contattare il tecnico di sistema per conoscere le opzioni disponibili. Non devi partire dal presupposto che riportare le cose al di sotto della soglia ti costerà denaro. Alcuni problemi della CPU possono essere risolti modificando la configurazione per garantire che tutti i processi vengano eseguiti nel modo più efficiente possibile. Ad esempio, alcuni Access Control Lists (ACL) possono aumentare notevolmente il numero di CPU di un router a causa del percorso dei pacchetti attraverso il router. In alcuni casi, è possibile implementare la commutazione NetFlow per modificare il percorso di commutazione dei pacchetti e ridurre l'impatto dell'ACL sulla CPU. Qualunque siano i problemi, in questa fase è necessario riportare tutti i router al di sotto della soglia, in modo da poter implementare le soglie in un secondo momento senza il rischio di allagare le stazioni NMS con troppi allarmi di soglia.

Passaggio 6: Monitoraggio soglia test

Questo passo prevede il test delle soglie in laboratorio utilizzando gli strumenti che utilizzerete nella rete di produzione. Esistono due approcci comuni al monitoraggio delle soglie. È necessario scegliere il metodo più appropriato per la rete in uso.

- Metodo di polling e confronto tramite una piattaforma SNMP o un altro strumento di monitoraggio SNMP

  Questo metodo utilizza una maggiore larghezza di banda per il polling del traffico e accetta i cicli di elaborazione sulla piattaforma SNMP.

- Usare le configurazioni di eventi e allarmi RMON (Remote Monitoring) nei router in modo che inviino un allarme solo quando viene superata una soglia

  Questo metodo riduce l'utilizzo della larghezza di banda della rete, ma aumenta anche l'utilizzo della memoria e della CPU sui router.

Implementazione di una soglia tramite SNMP

Per impostare il metodo SNMP utilizzando HP OpenView NNM, selezionare **Opzioni > Raccolta dati e soglie** come durante la configurazione del polling iniziale. Questa volta, tuttavia, selezionare **Archivia, Controlla soglie** invece di Archivia, Nessuna soglia nel menu delle raccolte. Dopo aver impostato la soglia, è possibile aumentare l'utilizzo della CPU sul router inviandogli più ping e/o percorsi SNMP. Potrebbe essere necessario abbassare il valore di soglia se non è possibile forzare la CPU ad un valore sufficientemente alto per innescare la soglia. In ogni caso, dovete assicurarvi che il meccanismo di soglia funzioni.

L'utilizzo di questo metodo è limitato dal fatto che non è possibile implementare più soglie contemporaneamente. Per impostare tre diverse soglie simultanee, sono necessarie tre piattaforme SNMP. Strumenti quali Concord Network Health e Trinagy TREND consentono più soglie per la stessa istanza OID.

Se il sistema è in grado di gestire una sola soglia alla volta, è possibile prendere in considerazione la

strategia Pronto, Imposta, Vai in modalità seriale. In altre parole, quando la soglia **ready** viene raggiunta continuamente, iniziare l'indagine e aumentare la soglia al livello impostato per il dispositivo. Quando il livello **impostato** viene raggiunto continuamente, iniziare a formulare il piano d'azione e aumentare la soglia al livello **go** per quel dispositivo. Una volta raggiunta la soglia di accettazione, implementare il piano d'azione. Ciò dovrebbe funzionare esattamente come il metodo a tre soglie simultanee. La modifica delle impostazioni di soglia della piattaforma SNMP richiede un po' più di tempo.

Implementazione di una soglia con l'uso di un evento e di un allarme RMON

Utilizzando le configurazioni degli allarmi e degli eventi RMON, è possibile configurare il monitoraggio del router in modo che utilizzi automaticamente più soglie. Quando il router rileva una condizione di superamento della soglia, invia una trap SNMP alla piattaforma SNMP. Affinché la trap venga inoltrata, è necessario che nella configurazione del router sia impostato un ricevitore di trap SNMP. Esiste una correlazione tra un allarme e un evento. L'allarme controlla l'OID per la soglia specificata. Se viene raggiunta la soglia, il processo di allarme attiva il processo di eventi che può inviare un messaggio trap SNMP, creare una voce del log RMON o entrambi. Per ulteriori informazioni su questo comando, vedere Comandi RMON Alarm e Event Configuration.

I seguenti comandi di configurazione del router dispongono del monitoraggio del router cpmCPUTotal5min ogni 300 secondi. Genererà l'evento 1 se la CPU supera il 60% e l'evento 2 quando la CPU ritorna al 40%. In entrambi i casi, verrà inviato un messaggio trap SNMP alla stazione NMS con la stringa privata della community.

Per utilizzare il metodo Ready, Set, Go, utilizzare tutte le istruzioni di configurazione seguenti.

```
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'esempio che segue mostra l'output del comando **show rmon alarm** configurato dalle istruzioni precedenti.

<#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
```

Nell'esempio seguente viene illustrato l'output del comando **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
```

Provare entrambi i metodi per individuare quello più adatto all'ambiente in uso. È anche possibile che una combinazione di metodi funzioni correttamente. In ogni caso, i test devono essere eseguiti in un ambiente di laboratorio per garantire che tutto funzioni correttamente. Dopo il test in laboratorio, un'installazione limitata su un piccolo gruppo di router consentirà di testare il processo di invio degli avvisi al centro operativo.

In questo caso, è necessario abbassare le soglie per testare il processo: si sconsiglia di provare ad aumentare

artificialmente la CPU su un router di produzione. È inoltre necessario assicurarsi che, quando gli allarmi arrivano nelle stazioni NMS del Centro operativo, vi sia una policy di escalation per essere sicuri di essere informati quando i dispositivi superano le soglie. Queste configurazioni sono state testate in un laboratorio con Cisco IOS versione 12.1(7). In caso di problemi, è consigliabile rivolgersi al team di progettazione Cisco o ai tecnici di sistema per verificare se la versione del sistema operativo in uso contiene un bug.

Passaggio 7: Implementare il monitoraggio delle soglie utilizzando SNMP o RMON

Dopo aver eseguito test approfonditi sul monitoraggio delle soglie in laboratorio e in un'installazione limitata, è possibile implementare le soglie in tutta la rete principale. È ora possibile eseguire sistematicamente questo processo di base per altre variabili MIB importanti sulla rete, quali buffer, memoria libera, errori CRC (Cyclic Redundancy Check), perdita di celle AMT e così via.

Se si utilizzano le configurazioni degli allarmi e degli eventi RMON, è possibile interrompere il polling dalla stazione NMS. In questo modo si riduce il carico sul server NMS e la quantità di dati di polling sulla rete. Eseguendo sistematicamente questo processo per importanti indicatori dello stato della rete, è possibile giungere facilmente al punto in cui le apparecchiature di rete si stanno monitorando da sole utilizzando gli eventi e gli allarmi RMON.

MIB aggiuntivi

Dopo aver appreso questo processo, è possibile esaminare altri MIB per la baseline e il monitoraggio. Nelle sottosezioni seguenti viene presentato un breve elenco di alcuni OID e vengono fornite descrizioni che possono risultare utili.

MIB router

Le caratteristiche della memoria sono molto utili per determinare lo stato di un router. Un router integro deve disporre quasi sempre di spazio di buffer sufficiente per funzionare. Se lo spazio del buffer del router inizia a esaurirsi, la CPU dovrà lavorare più duramente per creare nuovi buffer e cercare buffer per i pacchetti in entrata e in uscita. La trattazione approfondita dei buffer esula tuttavia dalle finalità del presente documento. Tuttavia, in generale, un router integro deve avere pochissimi errori nel buffer e non deve avere errori nel buffer o una condizione di memoria libera pari a zero.

Oggetto	Descrizione	OID
ciscoMemoryPoolFree	Numero di byte del pool di memoria attualmente inutilizzati nel dispositivo gestito	1.3.6.1.4.1.9.9.48.1.1.1.6
CiscoMemoryPoolLargestFree	Numero massimo di byte contigui del pool di memoria attualmente inutilizzati	1.3.6.1.4.1.9.9.48.1.1.1.7
BufferElMiss	Numero di mancati	1.3.6.1.4.1.9.2.1.12

	riscontri dell'elemento del buffer	
errore buffer	Numero di errori di allocazione buffer	1.3.6.1.4.1.9.2.1.46
bufferNoMem	Numero di errori di creazione del buffer dovuti alla mancanza di memoria disponibile	1.3.6.1.4.1.9.2.1.47

MIB switch Catalyst

Oggetto	Descrizione	OID
cpmCPUTotal5min	Percentuale complessiva di CPU occupata nell'ultimo periodo di cinque minuti. Questo oggetto depreca l'oggetto avgBusy5 da OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5
cpmCPUTotal5sec	Percentuale complessiva di CPU occupata nell'ultimo periodo di cinque secondi. Questo oggetto rende obsoleto l'oggetto BUSHper da OLD-CISCO-	1.3.6.1.4.1.9.9.109.1.1.1.3

	SYSTEM-MIB	
sysTraffic	Percentuale di utilizzo della larghezza di banda per l'intervallo di polling precedente	1.3.6.1.4.1.9.5.1.1.8
sysTrafficPeak	Valore massimo del contatore del traffico dall'ultima volta in cui i contatori della porta sono stati azzerati o il sistema è stato avviato	1.3.6.1.4.1.9.5.1.1.19
oraPiccoTrafficoSys	Tempo (in centesimi di secondo) trascorso il quale si è verificato il valore di picco del contatore del traffico	1.3.6.1.4.1.9.5.1.1.20
PortTopNUtilizzazione	Utilizzo della porta nel sistema	1.3.6.1.4.1.9.5.1.20.2.1.4
portTopNBufferOverFlow	Numero di overflow del buffer della porta nel sistema	1.3.6.1.4.1.9.5.1.20.2.1.10

MIB Serial Link

Oggetto	Descrizione	OID
locIfInputQueueDrops	Numero di pacchetti ignorati perché la coda di input	1.3.6.1.4.1.9.2.2.1.1.26

	è piena	
locIfOutputQueueDrops	Numero di pacchetti ignorati perché la coda di output è piena	1.3.6.1.4.1.9.2.2.1.1.27
locIfInCRC	Numero di pacchetti di input con errori di checksum di ridondanza ciclici	1.3.6.1.4.1.9.2.2.1.1.12

Comandi RMON Alarm e Event Configuration

Allarmi

Gli allarmi RMON possono essere configurati con la seguente sintassi:

<#root>

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

Elemento	Descrizione
numero	Il numero di allarme, che è identico all'alarmIndex nella alarmTable nel MIB RMON.
variabile	L'oggetto MIB da monitorare, che si traduce nella alarmVariable utilizzata nella alarmTable del MIB RMON.
intervallo	Il tempo, in secondi, l'allarme monitora la variabile MIB, che è identica all'alarmInterval utilizzato nell'alarmTable del MIB RMON.
delta	Verifica la modifica tra le variabili MIB, che influisce sull'alarmSampleType nell'alarmTable del MIB RMON.
assoluto	Esegue il test diretto di ogni variabile MIB, con effetto sull'alarmSampleType nell'alarmTable del MIB RMON.
valore soglia	Valore in corrispondenza del quale viene attivato l'allarme.
numero-evento	(Facoltativo) Numero dell'evento da attivare quando la soglia di aumento o di diminuzione

	supera il limite. Questo valore è identico a alarmRisingEventIndex o alarmFallingEventIndex nella alarmTable del MIB RMON.
valore soglia	Valore in corrispondenza del quale viene reimpostato l'allarme.
stringa proprietario	(Facoltativo) Specifica un proprietario per l'allarme, che è identico all'alarmOwner nella alarmTable del MIB RMON.

Eventi

Gli eventi RMON possono essere configurati con la seguente sintassi:

<#root>

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

Elemento	Descrizione
numero	Numero di evento assegnato, identico all'eventIndex nell'eventTable nel MIB RMON.
registro	(Facoltativo) Genera una voce del registro RMON quando viene attivato l'evento e imposta il tipo di evento nel MIB RMON su log o log-and-trap.
trap community	(Facoltativo) Stringa della community SNMP utilizzata per questa trap. Configura l'impostazione di eventType nel MIB RMON per questa riga come snmp-trap o log-and-trap. Questo valore è identico a eventCommunityValue in eventTable nel MIB RMON.
stringa di descrizione	(Facoltativo) Specifica una descrizione dell'evento, identica alla descrizione dell'evento nell'oggetto eventTable del MIB RMON.
stringa proprietario	(Facoltativo) Proprietario di questo evento, che è identico a eventOwner nell'eventTable del MIB RMON.

Implementazione di eventi e allarmi RMON

Per informazioni dettagliate sull'implementazione degli allarmi e degli eventi RMON, consultare la sezione Implementazione degli allarmi e degli eventi RMON nel white paper *sulle best practice dei sistemi di gestione della rete*.

Informazioni correlate

- **Documentazione e supporto tecnico - Cisco Systems**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).