White paper de práticas recomendadas do processo de linha de base

Contents

Introdução

Este documento descreve os conceitos fundamentais e os procedimentos para redes de alta disponibilidade. Inclui fatores críticos ao sucesso para a de sucessão crítica para que a avaliação comparativa e o limite de rede ajude a avaliar o sucesso. Ele também fornece detalhes significativos processos para de linha de base e limites e a implementação que segue as diretrizes de práticas recomendadas identificadas pela equipe da Cisco de High Availability Services (HAS).

Este documento fornece instruções passo a passo sobre o processo de criação de linha de base. Alguns produtos de sistema de gerenciamento de rede (NMS) atuais podem ajudar a automatizar esse processo. No entanto, o processo de linha de base permanece o mesmo, independentemente de você usar ferramentas manuais ou automatizadas. Se você usar esses

produtos NMS, deverá ajustar as configurações de limite padrão para seu ambiente de rede exclusivo. É importante ter um processo para escolher inteligentemente esses limites, para que sejam significativos e corretos.

Linha de base

O que é uma linha de base?

Uma linha de base é um processo para estudar a rede em intervalos regulares para garantir que a rede esteja funcionando como projetado. É mais do que um único relatório detalhando a integridade da rede em um determinado momento. Seguindo o processo de linha de base, você pode obter as seguintes informações:

- Obter informações valiosas sobre a integridade do hardware e do software
- Determinar a utilização atual dos recursos de rede
- Tomar decisões precisas sobre limites de alarmes de rede
- Identificar os problemas de rede atuais
- Prever problemas futuros

Outra maneira de examinar a linha de base é ilustrada no diagrama a seguir.

A linha vermelha, o ponto de ruptura de rede, é o ponto em que a rede será interrompida, o que é determinado pelo conhecimento do desempenho do hardware e do software. A linha verde, a carga da rede, é a progressão natural de carga na rede à medida que novos aplicativos são adicionados e outros fatores.

A finalidade de uma linha de base é determinar:

- Onde sua rede está na linha verde
- Quão rápido a carga da rede está aumentando
- Esperamos prever em que momento os dois se cruzarão

Executando uma linha de base regularmente, você pode descobrir o estado atual e extrapolar quando as falhas ocorrerão e preparar-se para elas com antecedência. Isso também o ajuda a tomar decisões mais informadas sobre quando, onde e como gastar o dinheiro do orçamento em atualizações de rede.

Por que uma linha de base?

Um processo de linha de base ajuda a identificar e planejar adequadamente problemas críticos de limitação de recursos na rede. Esses problemas podem ser descritos como recursos do plano de controle ou recursos do plano de dados. Os recursos do plano de controle são exclusivos da plataforma e dos módulos específicos dentro do dispositivo e podem ser afetados por vários

problemas, incluindo:

- Utilização de dados
- Recursos habilitados
- Projeto de rede

Os recursos do plano de controle incluem parâmetros como:

- Utilização da CPU
- Utilização de memória
- Utilização de buffer

Os recursos do plano de dados são afetados somente pelo tipo e quantidade de tráfego e incluem a utilização do link e do painel traseiro. Ao fazer a linha de base da utilização de recursos para áreas críticas, você pode evitar problemas sérios de desempenho ou, pior, uma queda da rede.

Com a introdução de aplicativos sensíveis à latência, como de voz e vídeo, uma avaliação comparativa se faz mais imprescindível do que nunca. As aplicações do Protocolo de Controle de Transmissão Tradicional/Protocolo Internet (TCP/IP) perdoam e permitem uma certa quantidade de atraso. Voz e vídeo são baseados no User Datagram Protocol (UDP) e não permitem retransmissões ou congestionamento de rede.

Devido à nova combinação de aplicativos, a linha de base ajuda você a entender os problemas de utilização de recursos do plano de controle e do plano de dados e a planejar proativamente alterações e atualizações para garantir o sucesso contínuo.

As redes de dados existem há muitos anos. Até recentemente, manter as redes em execução era um processo bastante complacente, com alguma margem de erro. Com a aceitação cada vez maior de aplicativos sensíveis à latência, como VoIP (Voice over IP, Voz sobre IP) o trabalho de funcionamento da rede está cada vez mais difícil e exige mais precisão. Para ser mais preciso e fornecer a um administrador de rede uma base sólida sobre a qual gerenciar a rede, é importante ter alguma ideia de como a rede está sendo executada. Para fazer isso, você deve percorrer um processo chamado linha de base.

Objetivo da linha de base

O objetivo de uma linha de base é:

1. Determinar o status atual dos dispositivos de rede
2. Compare esse status com as diretrizes de desempenho padrão
3. Defina limiares que alertem você quando o status exceder essas diretrizes.

Devido à grande quantidade de dados e ao tempo necessário para analisá-los, você deve primeiro limitar o escopo de uma linha de base para facilitar o aprendizado do processo. O local

mais lógico e, às vezes, mas vantajoso para começar é o centro da rede. Essa parte da rede é geralmente a menor e requer a maior estabilidade.

Por uma questão de simplicidade, este documento explica como estabelecer uma base muito importante para a base de informações de gerenciamento de protocolo de gerenciamento de rede simples (SNMP MIB): cpmCPUTotal5min. cpmCPUTotal5min é a média decadente de cinco minutos da unidade central de processamento (CPU) de um roteador Cisco e é um indicador de desempenho do plano de controle. A linha de base será executada em um Cisco 7000 Series Router.

Depois de conhecer o processo, você pode aplicá-lo a qualquer dado disponível no vasto banco de dados SNMP, que está disponível na maioria dos dispositivos Cisco, tais como:

- Uso de Integrated Services Digital Network (ISDN)
- Perda de célula do Modo de Transferência Assíncrono (ATM - Asynchronous Transfer Mode)
- Memória livre do sistema

Fluxograma da linha de base central

O seguinte fluxograma mostra as etapas básicas do principal processo de linha de base. Embora os produtos e as ferramentas estejam disponíveis para executar algumas dessas etapas para você, eles tendem a apresentar lacunas em termos de flexibilidade ou facilidade de uso. Mesmo que você planeje usar as ferramentas do sistema de gerenciamento de rede (NMS) para realizar a linha de base, este ainda é um bom exercício para estudar o processo e entender como a sua rede realmente funciona. Esse processo pode ser também o mistério de como algumas ferramentas NMS funcionam uma vez que a maioria das ferramentas faz essencialmente as mesmas coisas.

Procedimento de linha de base

Etapa 1: Compilar um inventário de hardware, software e configuração

É extremamente importante que você compile um inventário de hardware, software e configuração por vários motivos. Primeiro, as MIBs Cisco SNMP são, em alguns casos, específicas para a versão do Cisco IOS que você está executando. Alguns objetos MIB são substituídos por novos e, às vezes, são completamente eliminados. O inventário de hardware é muito importante depois que os dados são coletados, pois os limiares que você precisa configurar após a linha de base inicial são, com freqüência, baseados no tipo de CPU, na quantidade de memória etc. dos dispositivos Cisco. O inventário de configuração também é importante para certificar-se de que você conhece as configurações atuais: Você pode querer alterar as configurações do dispositivo após sua linha de base para ajustar os buffers e assim por diante.

A maneira mais eficaz de fazer com que isto seja parte da linha de base de uma rede Cisco é usar o CiscoWorks2000 Resource Manager Essentials (Essentials). Se esse software estiver

instalado corretamente na rede, o Essentials deve ter os inventários atuais de todos os dispositivos em seu banco de dados. Basta observar os estoques para ver se existem problemas.

A tabela a seguir é um exemplo de relatório de inventário do software Cisco Router Class, exportado do Essentials e, em seguida, editado no Microsoft Excel. A partir deste inventário, observe que você precisa usar dados da MIB de SNMP e Identificadores de objeto (OIDs) encontrados nas versões 12.0x e 12.1x do Cisco IOS.

Nome de dispositivo	Tipo de roteador	Versão	Versão de 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	I	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 o Essentials não estiver instalado na rede, você poderá usar a ferramenta de linha de comando UNIX snmpwalk de uma estação de trabalho UNIX para encontrar a versão do IOS. Isso é mostrado no seguinte exemplo: Se não tiver certeza de como esse comando funciona, digite man snmpwalk no prompt do UNIX para obter mais informações. A versão IOS será importante quando a escolha de qual MIB OIDs para a linha de base começar, porque os objetos dependem do IOS. Observe também que, conhecendo o tipo de roteador, você poderá determinar posteriormente quais devem ser os limites para CPU, buffers e assim por diante.

```
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
```

Etapa 2: Verifique se o SNMP MIB é suportado no roteador

Agora que você tem um inventário do dispositivo que deseja pesquisar para sua linha de base, você pode começar a escolher os OIDs específicos que deseja pesquisar. Isso poupa muita frustração se você verificar, antecipadamente, que os dados que deseja realmente estão lá. O objeto MIB cpmCPUTotal5min está em CISCO-PROCESS-MIB.

Para descobrir para qual OID você deseja efetuar a apuração, é necessária uma tabela de conversão disponível no site de CCO da Cisco. Para acessar este site em um navegador da Web, vá para a página MIBs da Cisco e clique no link OIDs.

Para acessar esse site da Web de um servidor FTP, digite ftp://ftp.cisco.com/pub/mibs/oid/. Nesse site, você pode fazer o download do MIB específico que foi decodificado e classificado pelos números OID.

O exemplo a seguir é extraído da tabela CISCO-PROCESS-MIB.oid. Este exemplo mostra que o OID para o MIB cpmCPUTotal5min é .1.3.6.1.4.1.9.9.109.1.1.1.1.5.

Observação: não se esqueça de adicionar um "." ao início do OID ou você receberá um erro quando tentar pesquisá-lo. Talvez você precise também adicionar ".1" no final da OID para instanciá-la. Isso informa ao dispositivo a instância do OID que você está procurando. Em alguns casos, os OIDs têm mais de uma instância de um tipo específico de dados, como quando um roteador tem várias CPUs.

<#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"
```

Há duas maneiras comuns de pesquisar o OID da MIB para garantir que ele esteja disponível e funcionando. É uma boa ideia fazer isso antes de iniciar a coleta de dados em massa, para que você não perca tempo pesquisando algo que não esteja lá e acabe com um banco de dados vazio. Uma maneira de fazer isso é usar um caminhador MIB de sua plataforma NMS, como o HP OpenView Network Node Manager (NNM) ou o CiscoWorks Windows, e inserir o OID que deseja verificar.

A seguir está um exemplo do HP OpenView SNMP MIB walker.

Outra maneira fácil de pesquisar o MIB OID é usar o comando UNIX snmpwalk como mostrado no exemplo a seguir.

```
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
```

Nos dois exemplos, o MIB retornou um valor de 0, o que significa que, para esse ciclo de polling, a utilização média da CPU foi de 0%. Se você tiver dificuldade para fazer com que o dispositivo responda com os dados corretos, tente fazer ping no dispositivo e acessar o dispositivo por meio de Telnet. Se o problema persistir, verifique a configuração do SNMP e as strings de comunidade do SNMP. Talvez seja necessário encontrar uma MIB alternativa ou outra versão do IOS para fazer isso funcionar.

Etapa 3: Sondar e registrar o objeto SNMP MIB específico do roteador

Há várias maneiras de pesquisar objetos MIB e registrar a saída. Produtos prontos, produtos shareware, scripts e ferramentas de fornecedores estão disponíveis. Todas as ferramentas de front-end usam o processo get do SNMP para obter as informações. As principais diferenças estão na flexibilidade da configuração e na maneira na qual os dados são registrados em um banco de dados. Novamente, examine a MIB do processador para ver como esses vários métodos funcionam.

Agora que você sabe que o OID é suportado no roteador, você precisa decidir com que frequência sondá-lo e como registrá-lo. A Cisco recomenda que a MIB da CPU seja interrogada em intervalos de cinco minutos. Um intervalo menor aumentaria a carga na rede ou no dispositivo e, como o valor MIB é uma média de cinco minutos, não seria útil pesquisá-lo com mais frequência do que o valor médio. Geralmente, também é recomendável que o polling de linha de base tenha pelo menos um período de duas semanas para que você possa analisar pelo menos dois ciclos comerciais semanais na rede.

As telas a seguir mostram como adicionar objetos MIB ao HP OpenView Network Node Manager version 6.1. Na tela principal, selecione Options > Data Collection & Thresholds.

Em seguida, selecione Edit > Add > MIB Objects.

No menu, adicione a string OID e clique em Apply. Agora você introduziu o objeto MIB na plataforma HP OpenView para que ele possa ser interrogado.

Em seguida, você deve informar ao HP OpenView qual roteador deve ser consultado para este OID.

No menu Coleta de dados, selecione Editar > Adicionar > Coleções MIB.

No campo Source (Origem), insira o nome DNS (Domain Naming System) ou o endereço IP do roteador a ser interrogado.

Selecione Store (Armazenamento), No Thresholds (Sem Limites) na lista Set Collection Mode (Definir Modo de Coleta).

Defina Polling Interval (Intervalo de pesquisa) como 5m para intervalos de cinco minutos.

Clique em Apply.

Você deve selecionar File > Save para que as alterações entrem em vigor.

Para verificar se a coleção está configurada corretamente, realce a linha de resumo da coleção para o roteador e selecione Actions > Test SNMP. Isso verifica se a série de comunidade está correta e interrogará todas as instâncias do OID.

Clique em Fechar e deixe a coleta ser executada por uma semana. No final do período semanal, extraia os dados para análise.

Os dados serão analisados mais facilmente se você copiá-los parcialmente para um arquivo ASCII e importá-los para uma ferramenta de planilha, como o Microsoft Excel. Para fazer isso com o HP OpenView NNM, você pode usar a ferramenta de linha de comando snmpColDump. Cada coleção configurada é gravada em um arquivo no diretório /var/opt/OV/share/databases/snmpCollect/.

Extraia os dados para um arquivo ASCII chamado testfile com o seguinte comando:

```
<#root>

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

testfile
```

Observação: cpmCPUTotal5min.1 é o arquivo de banco de dados que o HP OpenView NNM criou quando a pesquisa do OID começou.

O arquivo de teste gerado é semelhante ao do exemplo a seguir.

```
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/……
```

Depois que a saída do arquivo de teste estiver na estação UNIX, você poderá transferi-la para o PC utilizando o FTP (Protocolo de Transferência de Arquivos).

Também é possível coletar os dados usando seus próprios scripts. Para fazer isso, execute um snmpget para o OID da CPU a cada cinco minutos e despeje os resultados em um arquivo .csv.

Etapa 4: Analisar dados para determinar limites

Agora que você tem alguns dados, pode começar a analisá-los. Essa fase da linha de base determina as configurações de limiar que podem ser usadas e que são uma medida precisa do desempenho ou da falha e que não irão disparar muitos alarmes quando você ativar o monitoramento de limiares. Uma das maneiras mais fáceis de fazer isso é importar os dados para uma planilha como as do Microsoft Excel e esboçar um gráfico disperso. Esse método torna muito fácil ver quantas vezes um determinado dispositivo teria criado um alerta de exceção se você estivesse monitorando-o para um determinado limite. Não é aconselhável ativar limites sem fazer uma linha de base, pois isso pode criar tempestades de alertas de dispositivos que excederam o limite escolhido.

Para importar o arquivo de teste para uma planilha do Excel, abra o Excel, selecione Arquivo > Abrir e selecione o arquivo de dados.

O aplicativo Excel, então, orienta você durante toda a importação do arquivo.

Quando concluído, o arquivo importado deve ser semelhante à tela a seguir.

Um gráfico de dispersão permite que você visualize mais facilmente como várias configurações de limite funcionariam na rede.

Para criar um gráfico de dispersão, realce a coluna C no arquivo importado e, em seguida, clique no ícone Chart Wizard. Depois, siga as etapas do Wizard de Gráfico para criar um gráfico de dispersão.

No Assistente de gráfico etapa 1, como mostrado abaixo, selecione a guia Tipos padrão e selecione o tipo de gráfico XY (Dispersão). Em seguida, clique em Avançar.

Na etapa 2 do Assistente de Gráfico, conforme mostrado abaixo, selecione a guia Intervalo de Dados e selecione o intervalo de dados e a opção Colunas. Clique em Next.

Na etapa 3 do Assistente de Gráfico, conforme mostrado abaixo, insira o título do gráfico e os

valores dos eixos X e Y e clique em Avançar.

No Assistente de Gráfico etapa 4, selecione se deseja que o gráfico de dispersão em uma nova página ou como um objeto na página existente.

Clique em Concluir para colocar o gráfico no local desejado.

What If? Análise

Não é possível usar o gráfico de dispersão na análise. No entanto, antes de continuar, você precisa fazer as seguintes perguntas:

- O que o fornecedor (no exemplo, o fornecedor é a Cisco) recomenda como um limiar desta variável de MIB?

  Em geral, a Cisco recomenda que um roteador de núcleo não exceda 60% de utilização média da CPU. Sessenta por cento foi escolhido porque um roteador precisa de alguma sobrecarga caso tenha problemas ou a rede tenha algumas falhas. A Cisco estima que um roteador de núcleo precise de aproximadamente 40% de sobrecarga de CPU caso um protocolo de roteamento precise recalcular ou reconvergir. Essas porcentagens variam com base nos protocolos que você usa e na topologia e estabilidade da rede.

- O que acontece se eu usar 60 por cento como configuração de limiar?

  Se você desenhar uma linha no gráfico de dispersão horizontalmente em 60, verá que nenhum dos pontos de dados excede 60% de utilização da CPU. Portanto, um limiar de 60 definido nas estações do sistema de gerenciamento de rede (NMS) não terá um alarme de limiar ativado durante o período de interrogação. Uma porcentagem de 60 é aceitável para este roteador. No entanto, observe no gráfico de dispersão que alguns dos pontos de dados estão próximos de 60. Seria bom saber quando um roteador está se aproximando do limite de 60% para que você possa saber antecipadamente que a CPU está se aproximando de 60% e ter um plano sobre o que fazer quando chegar a esse ponto.

- E se eu definir o limite para 50 por cento?

  Estima-se que esse roteador tenha atingido 50% de utilização quatro vezes durante esse ciclo de pesquisa e teria gerado um alarme de limite a cada vez. Esse processo se torna mais importante quando você observa grupos de roteadores para ver o que as diferentes configurações de limiar fariam. Por exemplo, "E se eu definir o limite de 50% para toda a rede central?" Perceba que é muito difícil escolher somente um número.

Análise de "e se" do limite da CPU

Uma estratégia que você pode usar para tornar isso mais fácil é a metodologia de limiar Ready, Set, Go. Essa metodologia utiliza três números limiares sucessivos.

- Pronto—o limite definido como um preditor de quais dispositivos provavelmente precisarão de atenção no futuro

- Defina—o limiar que é usado como um indicador de antecipação, que o alerta quando iniciar o planejamento de um reparo, reconfiguração ou atualização
- Ir — o limite que você e/ou o fornecedor acreditam ser uma condição de falha e requer alguma ação para repará-la; neste exemplo, é de 60%

A tabela a seguir mostra a estratégia de Pronto, Configurar, Continuar.

Limite	Ação	Resultado
45 por cento	Investigar mais	Lista de opções para planos de ação
50 por cento	Formular plano de ação	Lista de etapas no plano de ação
60%	Implementar plano de ação	O roteador não excede mais os limiares. Voltar ao modo Pronto

A metodologia Ready, Set, Go muda o gráfico de linha de base original discutido anteriormente. O diagrama a seguir mostra o gráfico alterado da linha de base. Se você puder identificar os outros pontos de interseção no gráfico, agora terá mais tempo para planejar e reagir do que antes.

Observe que, nesse processo, a atenção está focada nas exceções na rede e não está preocupada com outros dispositivos. Supõe-se que, enquanto os dispositivos estiverem abaixo dos limites, eles estarão bem.

Se você pensar nessas etapas desde o início, estará bem preparado para manter a rede íntegra. A execução desse tipo de planejamento também é extremamente útil para o planejamento de orçamento. Se você souber quais são os seus cinco roteadores go principais, os roteadores do conjunto do meio e os roteadores ready inferiores, poderá planejar facilmente quanto orçamento será necessário para atualizações com base nos tipos de roteadores que eles são e nas opções do seu plano de ação. A mesma estratégia pode ser usada para enlaces de rede de longa distância (WAN) ou qualquer outro OID MIB.

Etapa 5: Corrija os problemas imediatos identificados

Esta é uma das etapas mais fáceis do processo de linha de base. Depois de identificados os dispositivos que excedem o limiar de ida, crie um plano de ação para recolocar esses dispositivos sob o limiar.

Você pode abrir um caso no Centro de assistência técnica (TAC) da Cisco ou entrar em contato com seu engenheiro de sistemas para obter as opções disponíveis. Você não deve supor que voltar a colocar as coisas abaixo do limite vai lhe custar dinheiro. Alguns problemas de CPU podem ser resolvidos alterando a configuração para garantir que todos os processos sejam executados da maneira mais eficiente. Por exemplo, algumas Listas de Controle de Acesso (ACLs) podem fazer com que a CPU de um roteador fique muito alta devido ao caminho que os pacotes percorrem pelo roteador. Em alguns casos, você pode implementar a switching do

NetFlow para alterar o caminho de switching do pacote e reduzir o impacto da ACL na CPU. Independentemente dos problemas, é necessário retornar todos os roteadores abaixo desse limiar nessa etapa para que você consiga implementar esses limiares mais tarde sem o risco de inundar as estações NMS com muitos alarmes de limiar.

Etapa 6: Testar o monitoramento do limite

Esta etapa envolve o teste de thresholds no laboratório usando as ferramentas que você utilizará na rede de produção. Há duas abordagens comuns para monitorar thresholds. Você deve decidir qual método é melhor para sua rede.

- Método de sondagem e comparação usando uma plataforma SNMP ou outra ferramenta de monitoramento SNMP

  Esse método usa mais largura de banda de rede para o tráfego de polling e utiliza ciclos de processamento na plataforma SNMP.

- Use as configurações de alarmes e eventos de Monitorização remota (RMON) nos roteadores, de modo que eles enviem um alerta somente quando for ultrapassado um limiar

  Este método reduz o uso de largura de banda da rede, mas também aumenta a utilização de memória e de CPU nos roteadores.

Implementando um limite usando SNMP

Para configurar o método SNMP usando o HP OpenView NNM, selecione Options > Data Collection & Thresholds como você fez ao configurar a pesquisa inicial. Dessa vez, selecione no menu de coleções Store, Check Thresholds rather than Store, No Thresholds no menu de coleções. Depois de configurar o limite, você pode aumentar a utilização da CPU no roteador enviando vários pings e/ou várias caminhadas SNMP. Pode ser necessário reduzir o valor de limiar se não for possível forçar a CPU a um valor alto o suficiente para ultrapassar o limiar. De qualquer forma, você deve garantir que o mecanismo de limiar esteja funcionando.

Uma das limitações da utilização desse método é que você não pode implementar simultaneamente múltiplos limiares. São necessárias três plataformas SNMP para configurar três limiares simultâneos diferentes. Ferramentas como Concord Network Health e Trinagy TREND permitem vários limites para a mesma instância do OID.

Se o seu sistema pode lidar com apenas um limite por vez, você pode considerar a estratégia Pronto, Configurar, Ir em série. Ou seja, quando o limite de prontidão for atingido continuamente, inicie a sua investigação e aumente o limite para o nível definido desse dispositivo. Quando o nível definido é alcançado continuamente, comece a formular seu plano de ação e aumente o limite do nível de atividade para aquele dispositivo. Em seguida, quando o limiar de partida for alcançado continuamente, implemente seu plano de ação. Isso deve funcionar tão bem quanto os três métodos de limiar simultâneos. Basta um pouco mais de tempo para alterar as configurações de limite da plataforma SNMP.

Implementando um Limite usando Alarme e Evento RMON

Usando o alarme RMON e as configurações de eventos, você pode fazer com que o roteador se monitore para vários limiares. Quando o roteador detecta uma condição acima do limiar, ele envia uma armadilha de SNMP à plataforma SNMP. É necessário ter um receptor de desvio de SNMP configurado em sua configuração do roteador para a armadilha ser encaminhada. Há uma correlação entre um alarme e um evento. O alarme verifica o OID para o limite fornecido. Se o limite for atingido, o processo de alarme acionará o processo de evento que pode enviar uma mensagem de interceptação SNMP, criar uma entrada de log RMON ou ambos. Para obter mais detalhes sobre esse comando, consulte Comandos de configuração de alarme e evento RMON.

Os comandos de configuração de roteador a seguir fazem com que o roteador monitore o cpmCPUTotal5min a cada 300 segundos. Acionará o evento 1 se a CPU exceder 60% e acionará o evento 2 quando a CPU voltar para 40%. Em ambos os casos, uma mensagem de interceptação (trapping) SNMP será enviada à estação NMS com a sequência de caracteres privada da comunidade.

Para utilizar método Ready, Set, Go, utilize todas as seguintes instruções de configuração:

```
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
```

O seguinte exemplo mostra a saída do comando show rmon alarm que foi configurada pelas seguintes declarações.

<#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
```

O exemplo a seguir mostra a saída do 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
```

Você pode experimentar os dois métodos para ver qual é o método que melhor se adapta ao seu ambiente. Você pode até descobrir que uma combinação de métodos funciona adequadamente. De qualquer forma, os testes devem ser feitos em um ambiente de laboratório para garantir que tudo funcione corretamente. Depois de testar no laboratório, uma implantação limitada em um pequeno grupo de roteadores permitirá que você teste o processo de envio de alertas para o seu Centro de Operações.

Nesse caso, você terá que reduzir os limites para testar o processo: não é recomendável tentar aumentar artificialmente a CPU em um roteador de produção. Você também deve garantir que, quando os alertas forem enviados às estações NMS no Centro de Operações, haverá uma política de escalação para garantir que você será informado quando os dispositivos excederem os limiares. Essas configurações foram testadas em laboratório com um Cisco IOS Versão 12.1(7). Se você encontrar algum problema, verifique com os engenheiros ou engenheiros de sistemas da Cisco se há algum bug na versão do IOS.

Etapa 7: Implementar a monitoração de limiar usando SNMP ou RMON

Após ter testado totalmente o monitoramento de limiar no laboratório e em uma versão limitada, você estará pronto para implementar limiares em toda a rede principal. Agora você pode seguir esse processo de linha de base sistematicamente para obter outras variáveis MIB importantes na rede, como os buffers, a memória livre, os erros de verificação de redundância cíclica (CRC), a perda de células AMT e outras.

Se você usar as configurações de alarme e evento RMON, agora poderá parar o polling a partir de sua estação NMS. Isso reduzirá a carga no servidor NMS e diminuirá a quantidade de dados de chamadas seletivas na rede. Passando sistematicamente por esse processo para indicadores importantes de integridade da rede, você poderia facilmente chegar ao ponto em que o equipamento de rede está monitorando a si mesmo usando o Alarme e o Evento RMON.

MIBs adicionais

Depois de aprender esse processo, talvez você queira investigar outras MIBs para estabelecer a linha de base e monitorar. As subseções a seguir apresentam uma lista resumida de alguns OIDs e descrições úteis.

MIBs do roteador

As características da memória são muito úteis para determinar a integridade de um roteador. Um roteador em bom estado deve quase sempre ter espaço disponível no buffer para trabalhar. Se o roteador começar a ficar sem espaço de buffer, a CPU terá que trabalhar mais para criar novos buffers e tentar encontrar buffers para pacotes de entrada e de saída. Uma discussão aprofundada sobre buffers está além do escopo deste documento. No entanto, como regra geral, um roteador saudável deve ter poucos, se houver, erros de buffer e não deve ter nenhuma falha de buffer ou uma condição de memória livre zero.

Objeto	Descrição	OID
ciscoMemoryPoolFree	O número de bytes do pool de memória atualmente não utilizados	1.3.6.1.4.1.9.9.48.1.1.1.6

	no dispositivo gerenciado.	
ciscoMemoryPoolLargestFree	O maior número de bytes contíguos do pool de memória que não estão sendo usados no momento	1.3.6.1.4.1.9.9.48.1.1.1.7
bufferSenhorita	O número de elementos de buffer está ausente	1.3.6.1.4.1.9.2.1.12
bufferFail	O número de falhas de alocação de buffer	1.3.6.1.4.1.9.2.1.46
bufferNoMem	O número de buffers gera falhas devido à ausência de memória livre	1.3.6.1.4.1.9.2.1.47

MIBs de Switch Catalyst

Objeto	Descrição	OID
cpmCPUTotal5min	Percentual de ocupação geral da CPU nos últimos cinco minutos. Esse objeto	1.3.6.1.4.1.9.9.109.1.1.1.5

	deprecia o objeto avgBusy5 de OLD-CISCO-SYSTEM-MIB	
cpmCPUTotal5sec	Percentual de ocupação geral da CPU no último período de cinco segundos. Este objeto substitui o objeto busyPer do OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.3
sysTraffic	A porcentagem de utilização da largura de banda do intervalo de eleição anterior	1.3.6.1.4.1.9.5.1.1.8
sysTrafficPeak	Valor do medidor de tráfego de pico desde a última vez que os contadores da porta foram limpos ou o sistema foi iniciado.	1.3.6.1.4.1.9.5.1.1.19
sysTrafficPeaktime	O tempo (em centésimos de segundo)	1.3.6.1.4.1.9.5.1.1.20

	desde que ocorreu o valor do medidor do tráfego de pico	
portTopNUtilization	Utilização da porta no sistema	1.3.6.1.4.1.9.5.1.20.2.1.4
portTopNBufferOverFlow	O número de excessos de buffer da porta no sistema	1.3.6.1.4.1.9.5.1.20.2.1.10

MIBs de enlace serial

Objeto	Descrição	OID
locIfInputQueueDrops	O número de pacotes descartados porque a fila de entrada estava cheia	1.3.6.1.4.1.9.2.2.1.1.26
locIfOutputQueueDrops	O número de pacotes descartados porque a fila de saída estava cheia	1.3.6.1.4.1.9.2.2.1.1.27
locIfInCRC	O número de pacotes de entrada com erros de checksum de redundância cíclica.	1.3.6.1.4.1.9.2.2.1.1.12

Comandos de configuração de alarme e evento RMON

Alarmes

Os alarmes RMON podem ser configurados com a sintaxe a seguir:

<#root>

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

Elemento	Descrição
número	O número do alarme, que é idêntico ao alarmIndex na alarmTable no RMON MIB.
variável	O objeto MIB a ser monitorado, que se converte no alarmVariable usado na alarmTable do RMON MIB.
intervalo	A hora, em segundos, que o alarme monitora a variável MIB, que é idêntica a alarmInterval usado em alarmTable de RMON MIB.
delta	Testa a alteração entre variáveis MIB, que afeta alarmSampleType na alarmTable do RMON MIB.
absoluto	Testa cada variável do MIB diretamente, o que afeta alarmSampleType na alarmTable do RMON MIB.
elevação de valor limiar	O valor no qual o alarme é disparado.
número do evento	(Opcional) O número do evento a ser acionado quando o limite de elevação ou queda exceder seu limite. Este valor é idêntico ao alarmRisingEventIndex ou ao alarmFallingEventIndex na alarmTable do MIB de RMON.
valor de falling-threshold	O valor no qual um alarme é redefinido.
série de proprietário	(Opcional) Especifica um proprietário para o alarme, que é idêntico ao alarmOwner na alarmTable do RMON MIB.

Events

Os eventos RMON podem ser configurados com a seguinte sintaxe:

<#root>

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

Elemento	Descrição
número	O número do evento atribuído, que é idêntico ao eventIndex na eventTable na MIB RMON.
registro	(Opcional) Gera uma entrada de registro RMON quando o evento é disparado e configura a IETF (Internet Engineering Task Force) no MIB de RMON para fazer registrar ou registrar e desviar.
comunidade trap	(Opcional) série de comunidade SNMP usada para esta armadilha. Configura a definição do eventType no MIB RMON para esta linha como snmp-trap ou log-and-trap. Esse valor é idêntico ao eventCommunityValue na eventTable na MIB RMON.
string de descrição	(Opcional) Especifica uma descrição do evento, que é idêntica à descrição na Tabela de Evento do RMON MIB.
série de proprietário	(Opcional) Proprietário desse evento, que é idêntico ao eventOwner na eventTable do MIB de RMON.

Implementação de evento e alarme de RMON

Para obter informações detalhadas sobre a implementação de eventos e alarmes RMON, leia a seção Implementação de eventos e alarmes RMON do white paper Práticas recomendadas de sistemas de gerenciamento de rede.

Informações Relacionadas

- Suporte técnico e documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.