Sistema de gerenciamento de rede: White Paper de práticas recomendadas

ID do Documento: 15114

Atualizado em: julho 11, 2007

Transferência PDF
Imprimir
Feedback

Produtos Relacionados

- Service Assurance Agent (SAA)
- CiscoWorks Resource Manager Essentials
- Alta Disponibilidade
- Protocolo simples de gerenciamento de rede (SNMP)
- Remote Monitoring (RMON)

Índice

Introdução

O modelo de gerenciamento de rede tipo International Organization for Standardization (ISO) define cinco áreas funcionais de gerenciamento de rede. Este documento abrange todas as áreas funcionais. O propósito geral deste documento é fornecer recomendações práticas sobre cada área funcional para aumentar a eficácia geral das ferramentas e das práticas de gerenciamento atuais. Ele também contém diretrizes de design para a futura implementação de tecnologias e ferramentas de gerenciamento de rede.

Gerenciamento de Rede

As cinco áreas funcionais do modelo de gerenciamento de rede ISO estão listadas abaixo.

- Gerenciamento de defeito — Detecte, isole, notifique, e corrija as falhas encontradas na rede.
- Gerenciamento de configuração — Aspectos da configuração dos dispositivos de rede tais como o gerenciamento de arquivo de configuração, a gestão de inventário, e o gerenciamento de software.
- Gerenciamento de desempenho — Monitore e meça vários aspectos do desempenho de modo que o desempenho geral possa ser mantido a nível aceitável.
- Gerenciamento de segurança — Forneça o acesso aos dispositivos de rede e aos recursos corporativos aos indivíduos autorizados.
- Gerenciamento de relatório — Informação de uso de recurso de rede.

O diagrama seguinte mostra uma arquitetura de referência que os Sistemas Cisco acreditam que deverá ser a solução mínima para gerenciamento de uma rede de dados. Esta arquitetura inclui um servidor Cisco CallManager para aqueles que planejam gerenciar VoIP (Voz sobre IP): O diagrama mostra como integrar o servidor CallManager na topologia do NMS.

A arquitetura de gerenciamento da rede inclui o seguinte:

- Plataforma do SNMP (Protocolo simples de gerenciamento de rede) para gerenciamento de falhas
- Plataforma de monitoramento de desempenho para gerenciamento de desempenho a longo prazo e tendências
- Servidor CiscoWorks2000 para gerenciamento de configurações, coleta de syslog e gerenciamento de inventário de hardware e software

Algumas plataformas de SNMP podem diretamente compartilhar de dados com o server do CiscoWorks2000 usando métodos do modelo de informação comum/linguagem de marcação extensível (CIM/XML). CIM é um modelo de dados comum de um esquema de implementação neutra para descrever informações gerais de gerenciamento em um ambiente empresarial/de rede. O CIM é composto de uma especificação e um esquema. A especificação define os detalhes para a integração com outros modelos de gerenciamento tais como o MIBs SNMP ou os arquivos de informação de gerenciamento do Desktop Management Task Force (DMTF MIFs), quando o esquema fornecer as descrições do modelo real.

XML é uma linguagem de marcação, utilizada para representar dados estruturados em forma textual. Um objetivo específico do XML era manter a maior parte do poder descritivo do SGML, retirando ao máximo sua complexidade. XML é semelhante em conceito ao HTML, mas enquanto o HTML é usado para conduzir informações gráficas sobre um documento, o XML é usado para representar dados estruturados em um documento.

Os clientes de serviços avançados da Cisco também incluiriam o servidor NATkit da Cisco para monitoramento proativo adicional e Troubleshooting. O servidor NATkit terá uma rmount (montagem de disco remota) ou um FTP (protocolo de transferência de arquivos) para acesso aos dados localizados no servidor CiscoWorks2000.

O capítulo Fundamentos de gerenciamento de rede da Visão geral sobre a tecnologia de comunicação inter-redes oferece uma visão geral mais detalhada sobre os fundamentos de gerenciamento de rede.

Gerenciamento de falhas

O objetivo do gerenciamento de falha é detectar, para registrar, notifica usuários de, e (na medida do possível) fixe automaticamente problemas de rede para manter a rede ser executado eficazmente. Como as falhas podem causar tempo inativo ou degradação de rede inaceitável, o gerenciamento de falhas talvez seja o elemento de gerenciamento de rede ISO mais largamente implementado.

Plataformas de gerenciamento de rede

Uma plataforma de gerenciamento de rede distribuída na empresa controla uma infraestrutura que consista em elementos de rede de vários fornecedores. A plataforma recebem e os eventos de processos dos elementos de rede na rede. Eventos dos servidores e outros recursos críticos podem também ser encaminhados para uma plataforma de gerenciamento. As seguintes funções geralmente disponíveis são incluídas em uma plataforma de gerenciamento padrão:

- Descoberta da rede
- Mapeamento de topologia dos elementos da rede
- Alimentador de evento
- Coletor e executor de gráfico de dados de desempenho
- Navegador de dados de gerenciamento

Épossível considerar as plataformas de gerenciamento de rede como o console principal para as operações de rede de detecção de defeitos na infra-estrutura. A capacidade para detectar problemas rapidamente em toda a rede é crítica. Os pessoais de operações de rede podem confiar em um mapa de rede gráfica para indicar os estados operacionais do elemento crítico da rede tais como o Roteadores e o Switches.

As plataformas de gerenciamento de rede, como HP OpenView, Computer Associates Unicenter e SUN Solstice, podem executar uma descoberta dos dispositivos da rede. Cada dispositivo de rede é representado por um elemento gráfico no console da plataforma de gerenciamento. Cores diferentes nos elementos gráficos representam o status operacional atual dos dispositivos de rede. Os dispositivos de rede podem ser configurados para enviar as notificações, chamadas SNMP traps, às plataformas de gerenciamento de rede. Após receber as notificações, o elemento gráfico representante do dispositivo de rede muda para uma cor diferente, dependendo da severidade da notificação recebida. A notificação, geralmente chamada de evento, é colocada em um arquivo de registro. É especialmente importante que os arquivos mais recentes da Base de

Informações de Gerenciamento Cisco (MIB) sejam carregados na plataforma SNMP para garantir que os vários alertas dos dispositivos Cisco sejam interpretados corretamente.

A Cisco publica arquivos de MIB para o gerenciamento de vários dispositivos da rede. Os arquivos MIB do Cisco são ficados situados no Web site de cisco.com, e incluem a informação seguinte:

- Arquivos MIB publicados no formato SNMPv1
- Arquivos MIB publicados em formato SNMPv2
- Armadilhas de SNMP suportadas nos dispositivos da Cisco
- OIDs para objetos MIB SNMP atuais Cisco

Uma série de plataformas de gerenciamento de rede são capazes de gerenciar vários locais distribuídos geograficamente. Isto é obtido por meio da troca de dados de gerenciamento entre os consoles de gerenciamento em sites remotos e uma estação de gerenciamento no site principal. As vantagens principal de uma arquitetura distribuída são que reduzem o tráfego de gerenciamento, assim, fornecendo mais uso efetivo de largura de banda. Uma arquitetura distribuída também permite que a equipe gerencie localmente suas redes a partir de locais remotos com sistemas.

Uma melhoria recente às plataformas de gerenciamento é a capacidade remotamente aos elementos de rede de gerenciamento usando uma interface da WEB. Essa melhoria elimina a necessidade de software de cliente especial em estações de usuário individual para acessar uma plataforma de gerenciamento.

Uma empresa típica é formada por diferentes elementos de rede. No entanto, cada dispositivo normalmente exige sistemas de gerenciamento de elemento específico do fornecedor para gerenciar efetivamente os elementos da rede. Por isso, as estações de gerenciamento duplicadas podem estar elegendo elementos de rede para as mesmas informações. Os dados coletados por diferentes sistemas são armazenados em bancos de dados separados, criando carga adicional de administração para os usuários. Essa limitação fez com que os fornecedores de redes de comunicação e de software adotassem padrões como o CORBA e o CIM para facilita o intercâmbio de dados de gerenciamento entre plataformas de gerenciamento e sistemas de gerenciamento de elementos. Com fornecedores adotando padrões em desenvolvimento de sistema de gerenciamento, os usuários poderão contar com interoperabilidade e economia na distribuição e gerenciamento da infra-estrutura.

CORBA especifica um sistema que forneça a Interoperabilidade entre objetos em um heterogêneo, o ambiente distribuído e de um modo que é transparente ao programador. Seu projeto é baseado no modelo de objeto do grupo de gerenciamento de objeto (OMG).

Troubleshooting de Infra-estrutura

O Trivial File Transfer Protocol (TFTP) e os server do log de sistema (Syslog) são componentes cruciais de uma infraestrutura do Troubleshooting nas operações de rede. O servidor TFTP é usado principalmente para armazenar os arquivos de configuração e as imagens de software para os dispositivos de rede. O Roteadores e o Switches são capazes de enviar mensagens de Log de sistema a um servidor de SYSLOG. As mensagens facilitam a função de Troubleshooting quando são encontrados problemas. Ocasionalmente, os pessoais de suporte Cisco precisam os mensagens do syslog de executar a análise da causa raiz.

A função de coleta de syslog distribuída do CiscoWorks2000 Resource Management Essentials (Essentials) permite a implantação de diversas estações de coleta UNIX ou NT em localizações

remotas para executar coleta e filtragem de mensagens. Os filtros podem especificar quais mensagens de syslog serão encaminhadas para o servidor principal Essentials. Um maior benefício de executar a coleção distribuída é a redução de mensagens encaminhada aos servidores de SYSLOG principais.

Falha na detecção e notificação

A finalidade do gerenciamento de falhas é detectar, isolar, notificar e corrigir defeitos identificados na rede. Os dispositivos de rede são capazes de alertar estações de gerenciamento quando uma falha ocorre nos sistemas. Um sistema de administração da falha eficaz consiste em diversos subsistemas. A detecção de defeito é realizada quando os dispositivos enviam mensagens de armadilha de SNMP, polling snmp, pontos iniciais do Remote Monitoring (RMON), e mensagens do syslog. Um sistema de administração alerta o utilizador final quando uma falha é relatada e as ações corretiva podem ser tomadas.

As armadilhas devem ser permitidas consistentemente em dispositivos de rede. As armadilhas adicionais são apoiadas com software release do Novo Cisco IOS para o Roteadores e o Switches. É importante verificar e atualizar o arquivo de configuração para assegurar a decodificação apropriada de armadilhas. Um exame periódico dos desvios configurados com a equipe da Cisco Assured Network Services (ANS) assegurará a detecção eficaz de falha na rede.

A tabela a seguir alista as armadilhas CISCO-STACK-MIB por que são apoiados, e pode ser usada para monitorar sobre condições de defeito, Switches de rede de área local (LAN) do Cisco catalyst.

Armadilha	**Descrição**
moduleUp	A entidade agente detectou que o **objeto de status de módulo n**este MIB tem o concluiu a transição **ok(2) ao** estado para um de seus módulos.
moduleDown	A entidade de agente detectou que o objeto moduleStatus nesse MIB fez a transição para fora do estado ok(2) para um de seus módulos.
chassisAlarmOn	A entidade do agente detectou que o objeto chassisTempAlarm, chassisMinorAlarm ou chassisMajorAlarm nesse MIB mudou para o estado ligado(2). *Um chassisMajorAlarm* indica que uma das seguintes circunstâncias existe: • Qualquer falha de tensão • Temperatura simultânea e falha no ventilador • Cem por cento de falha de fonte de alimentação (duas em duas ou uma em uma). • Falha da EEPROM (Memória programável de somente leitura apagável) • Falha de RAM não-volátil (NVRAM) • Falha de comunicação do MCP • Desconhecido do estado NMP

	Um chassisMinorAlarm indica que existe uma das seguintes condições: • Alarme de temperatura • Falha de ventilador • Falha parcial da fonte de alimentação (uma de duas) • Duas fontes de alimentação de tipo incompatível
chassisAlarmOff	A entidade agente detectou que o *chassisTempAlarm*, o *chassisMinorAlarm*, ou o *objeto chassismajoralarm n*este MIB têm o concluiu a transição **off(1) ao** estado.

As armadilhas de monitor ambiental (envmon) são definidas na armadilha CISCO-ENVMON-MIB. O desvio envmon envia notificações do monitor ambiental específicas do empreendimento quando um limiar ambiental for excedido. Quando envmon é usado, um tipo de armadilha ambiental específica pode ser habilitada ou todos os tipos de armadilha do sistema de monitoramento ambiental podem ser aceitos. Se não forem especificadas opções, todos os tipos de ambiente serão habilitados. Pode ser um ou mais dos valores a seguir:

- tensão — Uma ciscoEnvMonVoltageNotification é enviada se a tensão medida em um ponto de teste dado é fora do intervalo normal para o ponto de teste (como está o de advertência, crítico, ou no estágio de parada).
- parada programada — Um ciscoEnvMonShutdownNotification é enviado se o monitor ambiental detecta que um ponto de teste está alcançando um estado crítico e está a ponto de iniciar uma parada programada.
- fonte — Uma ciscoEnvMonRedundantSupplyNotification está enviada se a fonte de alimentação redundante (onde extant) falha.
- fã — Um ciscoEnvMonFanNotification está enviado se qualquer dos fãs na disposição do fã (onde extant) falha.
- temperatura — Um ciscoEnvMonTemperatureNotification é enviado se a temperatura medida em um ponto de teste dado é fora do intervalo normal para o ponto de teste (como está o de advertência, crítico, ou no estágio de parada).

Detecção e monitoramento de falha dos elementos de rede podem ser ampliados do nível do dispositivo aos níveis de protocolo e interface, Para um ambiente de rede, o monitoramento de falhas pode incluir VLAN (Virtual Local Area Network), modo de transferência assíncrona (ATM), indicações de falha em interfaces físicas, etc. A implementação do gerenciamento de falha de nível de protocolo está disponível ao se utilizar um sistema de gerenciamento de elemento, tal como o gerenciador de campus CiscoWorks2000. O aplicativo trafficdirector no Campus Manager centra-se sobre o gerenciamento de switch que utiliza o apoio do miniRMON em Catalyst Switches.

Com o crescente número de elementos de rede e a complexidade dos problemas de rede, um sistema para gerenciamento de eventos capaz de correlacionar diferentes eventos de rede (syslog, desvios, arquivos de registro) poderá ser considerado. Essa arquitetura por trás de um sistema de gerenciamento de eventos é comparável a um sistema MOM. Um sistema de gerenciamento de evento bem programado permite que os pessoais no Network Operations Center (NOC) sejam dinâmicos e eficazes em detectar e em diagnosticar questões de rede. A prioritização de evento e a supressão permitem que os pessoais de operação de rede centrem-se sobre eventos da rede crítica, investiguem-se diversos sistemas de gerenciamento de evento que

incluem o Cisco Info Center, e conduzam-se uma análise de viabilidade para explorar inteiramente as capacidades de tais sistemas. Para obter mais informação, vá ao Cisco Info Center.

Monitoração e notificação de falha proativa

Evento e alarme de RMON são dois grupos definidos na especificação de RMON. Em geral, uma estação de gerenciamento executa poll em dispositivos de rede para determinar o status ou o valor de certas variáveis. Por exemplo, uma estação de gerenciamento faz uma chamada seletiva de um roteador para saber a utilização da CPU e gerar um evento quando as ocorrências de valor atingem um limiar configurado. Este método desperdiça largura de banda de rede e pode também perder o limiar atual dependendo do intervalo de chamada seletiva.

Com os eventos e o alarme do RMON, um dispositivo de rede é configurado para monitorar a si mesmo em limiares de elevação e queda. Em um intervalo de tempo pré-definido, a vontade do dispositivo de rede toma uma amostra de uma variável e compara-a contra os pontos iniciais. Uma armadilha de SNMP pode ser enviada a uma estação de gerenciamento se o valor real excede ou cai abaixo dos limiares configurados. O alarme de RMON e os grupos de evento fornecem um método pró-ativo de controlar dispositivos críticos de rede.

O Cisco Systems recomenda executar o alarme de RMON e o evento em dispositivos críticos de rede. Variáveis monitoradas podem incluir utilização da CPU, falhas de buffer, desconexões de entrada/saída ou qualquer variável de tipos inteiros. Começando com Cisco IOS Software Release 11.1(1), todas as imagens do roteador apoiam o alarme de RMON e os grupos de evento.

Para obter informações detalhadas sobre a implementação de evento e alarme RMON, consulte a seção Implementação de evento e alarme RMON.

Impedimentos de memória rmon

O uso da memória RMON é constante em todas as plataformas de switching em relação a estatística, históricos, alarmes e eventos. O RMON usa-se o que é chamado uma *cubeta* para armazenar histórias e estatísticas no agente de RMON (que é o interruptor neste caso). O tamanho do bucket é definido na prova de RMON (dispositivo SwitchProbe) ou aplicativo de RMON (ferramenta TrafficDirector) e, em seguida, é enviado ao switch para ser configurado.

Aproximadamente 450 K do espaço de código são precisados de apoiar o miniRMON (por exemplo, quatro grupos RMON: estatísticas, história, alarmes, e eventos). O requisito de memória dinâmica para o RMON varia porque depende da configuração de tempo de corrida.

A tabela a seguir define as informações de utilização de memória RMON de tempo de execução para cada minigrupo de RMON.

Definição de grupo RMON	Espaço DRAM usado	Notas
Estatísticas	140 bytes pela porta de Ethernet/fasts Ethernet comutada	Por porta
Histórico	3.6 K para cubetas dos 50	Cada bucket

	pés *	adicional utiliza 56 bytes.
Alarme e Evento	2.6 K pelo alarme e suas entradas correspondentes do evento	Pelo alarme pela porta

O *RMON usa-se o que é chamado uma *cubeta* para armazenar histórias e estatísticas no agente de RMON (tal como um interruptor).

Implementação de evento e alarme de RMON

Com a incorporação do RMON como parte de uma solução de gerenciamento de falhas, um usuário pode monitorar a rede, de forma pró-ativa, antes que ocorra um problema em potencial. Por exemplo, se o número de pacotes de broadcast recebidos aumentar significativamente, isso pode causar um aumento na utilização do CPU. Através da implementação do alarme e evento RMON, um usuário pode configurar um limiar para monitorar o número de pacotes de difusão recebidos e alertar a plataforma SNMP por meio de um desvio SNMP se o limiar configurado for atingido. Os alarmes e eventos de RMON eliminam o poll em excesso normalmente executado pela plataforma SNMP para atingir o mesmo objetivo.

Dois métodos estão disponíveis de qual para configurar o alarme de RMON e o evento:

- Interface de linha de comando (CLI)
- SNMP SET

A seguinte mostra dos procedimentos da amostra como ajustar um ponto inicial para monitorar o número de pacotes de transmissão recebidos em uma relação. O mesmo contador é utilizado nesses procedimentos, como mostrado no exemplo do comando show interface no final desta seção.

Exemplo de interface de linha de comando

Para implementar o alarme de RMON e o evento usando a interface CLI, efetue os seguintes passos:

1. Encontre o deslocamento predeterminado da relação associado com o ethernet0 andando o ifTable MIB.
```
interfaces.ifTable.ifEntry.ifDescr.1 = "Ethernet0"
interfaces.ifTable.ifEntry.ifDescr.2 = "Ethernet1"
interfaces.ifTable.ifEntry.ifDescr.3 = "FastEthernet0"
interfaces.ifTable.ifEntry.ifDescr.4 = "Fddi0"
```
2. Obtenha o OID associado ao campo CLI a ser monitorado. Neste exemplo, o OID de 'difusão é 1.3.6.1.2.1.2.2.1.12. Os OIDs da Cisco para variáveis de MIB específicas estão disponíveis no site da web cisco.com.
3. Determine os seguintes parâmetros para estabelecer pontos iniciais e eventos.limiares de elevação e de quedatipo de amostragem (absoluta ou delta)intervalo de amostragemação a ser realizada quando o limiar é alcançadoCom a finalidade deste exemplo, um ponto inicial está estabelecendo-se para monitorar o número de pacotes de transmissão recebidos no ethernet0. Uma armadilha será gerada se o número de pacotes de transmissão recebidos é maior de 500 entre 60-segundas amostras. O limiar será reativado quando o número de difusões de entrada não aumentar entre amostras tiradas.**Nota:** Para obter detalhes sobre esses parâmetros de comando,verifique a documentação do Cisco Connection Online

(CCO) para o alarme de RMON e comandos de evento para a sua versão específica de IOS Cisco.

4. Especifique trap sent (evento RMON) quando o limiar for atingido usando os seguintes comandos de CLI (os comandos do Cisco IOS são exibidos em negrito):**rmon event 1 trap gateway description "High Broadcast on Ethernet 0" owner ciscormon event 2 log description "normal broadcast received on ethernet 0" owner cisco**
5. Especifique os limiares e parâmetros relevantes (alarme RMON) usando os seguintes comandos de CLI:**rmon alarm 1 ifEntry.12.1 60 delta rising-threshold 500 1falling-threshold 0 2 owner cisco**
6. Use o SNMP para votar estas tabelas para verificar que as entradas de eventtable estiveram feitas no dispositivo.`rmon.event.eventTable.eventEntry.eventIndex.1 = 1`

   ```
   rmon.event.eventTable.eventEntry.eventIndex.2 = 2

   rmon.event.eventTable.eventEntry.eventDescription.1 =
   "High Broadcast on Ethernet 0"

   rmon.event.eventTable.eventEntry.eventDescription.2 =
   "normal broadcast received on ethernet 0"

   rmon.event.eventTable.eventEntry.eventType.1 = snmp-trap(3)

   rmon.event.eventTable.eventEntry.eventType.2 = log(2)

   rmon.event.eventTable.eventEntry.eventCommunity.1 = "gateway"

   rmon.event.eventTable.eventEntry.eventCommunity.2 = ""

   rmon.event.eventTable.eventEntry.eventLastTimeSent.1 =
   Timeticks: (0) 0:00:00

   rmon.event.eventTable.eventEntry.eventLastTimeSent.2 =
   Timeticks: (0) 0:00:00

   rmon.event.eventTable.eventEntry.eventOwner.1 = "cisco"

   rmon.event.eventTable.eventEntry.eventOwner.2 = "cisco"

   rmon.event.eventTable.eventEntry.eventStatus.1 = valid(1)

   rmon.event.eventTable.eventEntry.eventStatus.2 = valid(1)
   ```
7. Use o SNMP para votar estas tabelas para verificar que as entradas de alarmtable estiveram ajustadas.`rmon.alarm.alarmTable.alarmEntry.alarmIndex.1 = 1`

   ```
   rmon.alarm.alarmTable.alarmEntry.alarmInterval.1 = 60

   rmon.alarm.alarmTable.alarmEntry.alarmVariable.1 = OID:
   interfaces.ifTable.ifEntry.ifInNUcastPkts.2

   rmon.alarm.alarmTable.alarmEntry.alarmSampleType.1 = absoluteValue(1)

   rmon.alarm.alarmTable.alarmEntry.alarmValue.1 = 170183

   rmon.alarm.alarmTable.alarmEntry.alarmStartupAlarm.1 =
   risingOrFallingAlarm(3)

   rmon.alarm.alarmTable.alarmEntry.alarmRisingThreshold.1 = 500

   rmon.alarm.alarmTable.alarmEntry.alarmFallingThreshold.1 = 0
   ```

```
rmon.alarm.alarmTable.alarmEntry.alarmRisingEventIndex.1 = 1

rmon.alarm.alarmTable.alarmEntry.alarmFallingEventIndex.1 = 2

rmon.alarm.alarmTable.alarmEntry.alarmOwner.1 = "cisco"

rmon.alarm.alarmTable.alarmEntry.alarmStatus.1 = valid(1)
```

Exemplo de SET de SNMP

A fim executar o alarme de RMON e o evento com a operação SNMP set, termine estas etapas:

1. Especifique a armadilha enviada (evento de RMON) quando o ponto inicial é alcançado usando as seguintes operações SNMP set:`# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.2.1 octetstring "High Broadcast on Ethernet 0"`
   ```
   eventDescription.1 : DISPLAY STRING- (ascii): High Broadcast on Ethernet 0

   # snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.3.1
     integer 3 eventType.1 : INTEGER: SNMP-trap

   # snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.4.1 octetstring "gateway"
     eventCommunity.1 : OCTET STRING- (ASCII): gateway

   # snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.6.1
     octetstring "cisco" eventOwner.1 : OCTET STRING- (ASCII): cisco

   # snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.7.1 integer 1
     eventStatus.1 : INTEGER: valid
   ```
2. Especifique os pontos iniciais e os parâmetros relevantes (alarme de RMON) que usam as seguintes operações SNMP set:`# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.2.2 octetstring "normal broadcast received on ethernet 0"`
   ```
   eventDescription.2 : DISPLAY STRING- (ASCII): normal broadcast
   received on ethernet 0

   # snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.3.2 integer 2
     eventType.2 : INTEGER: log

   # snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.6.2 octetstring "cisco"
     eventOwner.2 : OCTET STRING- (ASCII): cisco

   # snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.7.2 integer 1
     eventStatus.2 : INTEGER: valid
   ```
3. Vote estas tabelas para verificar que as entradas de eventtable estiveram feitas no dispositivo.`% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.9.1`
   ```
   # snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.2.1 integer 60
     alarmInterval.1 : INTEGER: 60

   # snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.3.1
    objectidentifier .1.3.6.1.2.1.2.2.1.12.2
     alarmVariable.1 : OBJECT IDENTIFIER:
   .iso.org.dod.internet.mgmt.mib2.interfaces.ifTable
     ifEntry.ifInNUcastPkts.2

   # snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.4.1 integer 2

   alarmSampleType.1 : INTEGER: deltaValue
   ```

```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.7.1 integer 500
  alarmRisingThreshold.1 : INTEGER: 500

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.8.1 integer 0
  alarmFallingThreshold.1 : INTEGER: 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.9.1 integer 1
  alarmRisingEventIndex.1 : INTEGER: 1

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.10.1 integer 2
  alarmFallingEventIndex.1 : INTEGER: 2

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.11.1 octetstring
"cisco"
  alarmOwner.1 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.12.1 integer 1
  alarmStatus.1 : INTEGER: valid
```

4. Vote estas tabelas para verificar que as entradas de alarmtable estiveram ajustadas.`%`
   `snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.3.1`

show interface

Este exemplo é um resultado do **comando show interface**.

show interface ethernet0 do gateway**>**

```
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0000.0c38.1669 (bia 0000.0c38.1669)
Description: NMS workstation LAN
Internet address is 172.16.97.132/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 27 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 1 packets/sec
21337627 packets input, 3263376846 bytes, 0 no buffer

Received 7731303 broadcasts , 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
17328035 packets output, 2824522759 bytes, 0 underruns
174 output errors, 44368 collisions, 4 interface resets
0 babbles, 0 late collision, 104772 deferred
174 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Gerenciamento de configuração

O objetivo do gerenciamento de configuração é monitorar as informações de rede e de configuração do sistema, de modo que os efeitos da operação de rede de várias versões de elementos de hardware e software possam ser rastreados e gerenciados.

Padrões de configuração

Com um número de aumento de dispositivos de rede distribuídos, é crítico poder identificar exatamente o lugar de um dispositivo de rede. Essas informações de localização devem fornecer uma descrição detalhada significativa àqueles que estiverem encarregados das tarefas de envio de recursos, quando ocorrer um problema de rede. Para acelerar uma resolução se ocorrer um problema de rede, verifique se as informações de contato da pessoa ou do departamento responsável pelos dispositivos estão disponíveis. As informações de contato devem incluir número de telefone e nome da pessoa ou do departamento.

As convenções de nomenclatura de rede, iniciando no nome de dispositivo de cada interface, deve ser planejada e implementada como parte do padrão de configuração. Uma convenção de nomeação bem definida fornece pessoais a capacidade para fornecer a informação precisa ao pesquisar defeitos problemas de rede. A convenção de nomeação para dispositivos pode usar a localização geográfica, nome de construção, assoalho, e assim por diante. Para a convenção de nomenclatura da interface, é possível incluir o segmento ao qual uma porta está conectada, o nome do hub de conexão e assim por diante. Em interfaces seriais, ela deve incluir a largura de banda real, o número do Identificador da conexão do enlace de dados (DLCI) local (se Frame Relay), o destino e o ID do circuito ou informações fornecidas pela portadora.

Gerenciamento de arquivos de configuração

Quando você adiciona comandos configuration novos em necessidades dos dispositivos da rede existente, você deve verificar os comandos para a integridade antes que a implementação real ocorra. Um dispositivo de rede configurado incorretamente pode ter um efeito desastroso na conectividade e no desempenho da rede. Os parâmetros do comando de configuração devem ser verificados para evitar problemas de falta de correspondência ou incompatibilidade. É aconselhável agendar regularmente uma revisão completa das configurações com os engenheiros Cisco.

A inteiramente - os fundamentos funcionais do CiscoWorks2000 permitem arquivos de configuração de suportação no Roteadores e no Switches do Cisco catalyst automaticamente. O recurso de segurança do Essentials pode ser utilizado para executar a autenticação em alterações de configuração. Um registro de exame de alterações está disponível para rastrear alterações e o nome de usuário das pessoas que fazem as alterações. Para alterações de configuração em dispositivos múltiplos, duas opções estão disponíveis: o netconfig baseado na Web na versão atual de fundamentos do CiscoWorks2000 ou do script do **cwconfig**. Você pode fazer o download e o upload dos arquivos de configuração no CiscoWorks2000 Essentials, utilizando os moldes predefinidos ou definidos pelo usuário.

Estas funções podem ser realizadas com as ferramentas de gerenciamento de configuração em fundamentos do CiscoWorks2000:

- Retire os arquivos de configuração do arquivo de configuração Essentials (Fundamentos) para um dispositivo ou dispositivos múltiplos
- Extraia a configuração do dispositivo para o arquivo do Essentials
- Extraia a configuração a mais atrasada do arquivo e escreva-à um arquivo
- Importar a configuração de um arquivo e enviá-la aos dispositivos
- Compare as duas últimas configurações no arquivo Essentials
- Suprima das configurações mais velhas do que uma data especificada ou uma versão do arquivo
- Copiar a configuração de inicialização para a configuração de execução

Gerenciamento de inventário

A função de descoberta da maioria das plataformas de gerenciamento é planejada para fornecer uma listagem dinâmica de dispositivos encontrados na rede. Deve-se utilizar mecanismos de descoberta como os implementados nas plataformas de gerenciamento de rede.

Um base de dados do inventário fornece a informação de configuração detalhada em dispositivos de rede. As informações comuns incluem modelos de hardware, módulos instalados, imagens de software, níveis de microcódigo etc. Todas estas partes de informação são cruciais em terminar tarefas tais como a manutenção de software e hardware. A listagem atualizada de dispositivos de rede coletadas pelo processo de descoberta pode ser usada como lista principal para coletar informações de estoque usando SNMP ou scripts. Uma lista de dispositivos pode ser importada do Campus Manager do CiscoWorks2000 no base de dados do inventário de fundamentos do CiscoWorks2000 para obter um inventário atualizado do Switches do Cisco catalyst.

Gerenciamento do software

Uma atualização bem-sucedida de imagens do Cisco IOS em dispositivos de rede exige uma análise detalhada dos requisitos como memória, ROM de inicialização, nível de microcódigo e outros. As exigências estão documentadas normalmente e disponíveis no site de Cisco sob a forma dos Release Note e dos Guias de Instalação. O processo de atualização de um dispositivo de rede que esteja executando o Cisco IOS inclui fazer o download de uma imagem correta do CCO, fazer o backup da imagem atual, verificar se todos os requisitos de hardware foram atendidos e carregar a nova imagem no dispositivo.

O indicador da elevação para terminar a manutenção do dispositivo é razoavelmente limitado para algumas organizações. Em um ambiente de rede com recursos limitados, pode ser necessário programar e automatizar as atualizações de software para fora do horário comercial. O procedimento pode ser concluído com o uso da linguagem de scripts, como Expect, ou de um aplicativo gravado especificamente para realizar essa tarefa.

As mudanças ao software nos dispositivos de rede tais como imagens IOS Cisco e versões do microcódigo devem ser seguidas para ajudar na fase de análise em que uma outra manutenção de software é exigida. Com um relatório de histórico de modificação prontamente disponível, o responsável executando a atualização pode minimizar o risco de carregar imagens incompatíveis ou microcódigo nos dispositivos de rede.

Gerenciamento de desempenho

Contrato de nível de serviço

Um Contrato de Nível de Serviço (SLA) é um contrato por escrito entre um fornecedor de serviço e seus clientes sobre o nível de desempenho esperado dos serviços de rede. O SLA consiste no medidor concordado entre o fornecedor e seus clientes. Os valores definidos para as métricas dever ser realistas, significativos e mensuráveis para ambas as partes.

As várias estatísticas da relação podem ser recolhidas dos dispositivos de rede para medir o nível de desempenho. Essas estatísticas podem ser incluídas como métricas no SLA. As estatísticas tais como quedas de fila de entrada, quedas da fila de saída, e pacotes ignorados são úteis para diagnosticar problemas relacionados com desempenho.

No nível de dispositivo, a métrica de desempenho pode incluir utilização de CPU, alocação de buffer (grande, médio, perdas, taxa de acerto) e alocação de memória. O desempenho de certos protocolos de rede está diretamente relacionado à disponibilidade de buffer nos dispositivos de rede. Medir as estatísticas de desempenho de nível do dispositivo é decisivo na otimização do desempenho de protocolos de um nível mais alto.

Os dispositivos de rede tais como o Roteadores apoiam vários protocolos de camada mais elevada tais como o Data Link Switching Workgroup (DLSW), Remote Source-Route Bridging (RSRB), APPLETALK, e assim por diante. Estatísticas de desempenho de tecnologias de WAN (rede de área ampla), incluindo Frame Relay, ATM, ISDN (Rede Digital de Serviços Integrados) e outros, podem ser monitoradas e coletadas.

Monitoramento, medição e relatório de desempenho

Diferentes métricas de desempenho em níveis de interface, dispositivo e protocolo devem ser coletadas regularmente com o uso do SNMP. O mecanismo de apuração em um sistema de gerenciamento de rede pode ser usado para propósitos de coleta de dados. A maioria dos sistemas de gerenciamento de rede é capaz de coletar, armazenar e apresentar dados em poll.

As várias soluções estão disponíveis no mercado para endereçar as necessidades de Gerenciamento de desempenho para ambientes de empreendimento. Esses sistemas são capazes de coletar, armazenar e apresentar dados a partir de dispositivos e servidores de rede. A interface baseada NA Web na maioria de Produtos faz os dados de desempenho acessíveis em qualquer lugar dentro da empresa. Algumas das soluções de gerenciamento de desempenho implantadas normalmente incluem:

- InfoVista VistaView
- Visão do serviço SAS a TI
- Trinagy trend

Uma avaliação dos produtos acima determinará se eles satisfazem às exigências dos diferentes usuários. Alguma integração de suporte de fornecedores com Plataformas do Gerenciamento de redes e do gerenciamento de sistema. Por exemplo, o InfoVista oferece suporte ao BMC Patrol Agent para fornecer estatísticas importantes de desempenho pelos servidores de aplicativos. Cada produto tem um modelo de preço diferente e recursos diferentes com a oferta base. O suporte para recursos de gerenciamento de desempenho para dispositivos da Cisco, como NetFlow, RMON e Agente de garantia de serviço Cisco IOS/Relator de tempo de resposta (RTR/SAA CSAA/RTR), está disponível em algumas soluções. A concórdia tem adicionado recentemente o apoio para os switch WAN de Cisco que podem ser usados para recolher e ver dados de desempenho.

O recurso CSAA/RTR Service Assurance Agent (SAA)/Response Time Reporter (RTR)(Agente de Garantia de Serviço (SAA)/Reporter de Tempo de Resposta (RTR)) do Cisco IOS pode ser utilizado para medir o tempo de resposta entre dispositivos IP. Um roteador de origem com CSAA configurado é capaz de medir o tempo de resposta para um dispositivo IP de destino, que pode ser um roteador ou um dispositivo IP. O tempo de resposta pode ser medido entre a origem e o destino ou para cada salto ao longo do caminho. Os desvios SNMP podem ser configurados para alertar consoles de gerenciamento de alertas quando o tempo de resposta excede aos limiares predefinidos.

As recentes melhorias no Cisco IOS ampliam os recursos do CSAA para medir o seguinte:

- Desempenho do serviço HTTP (HyperText Transfer Protocol)Consulta de DNS (sistema de

nome de domínio)Conexão de protocolo de controle de transmissão (TCP)Tempo de transação HTTP
- Variação (jitter) de retardo entre pacotes de tráfego de VoIP (Voz sobre IP)
- Tempo de resposta entre pontos finais para um Qualidade de Serviço (QoS) específicoBit do tipo do IP de serviço (ToS)
- Perda de pacotes usando pacotes gerados por CSAA

Configurar a característica CSAA no Roteadores pode ser realizado usando o aplicativo Cisco internetwork performance monitor (IPM). O CSSA/RTR está incluído em vários, mas não em todos os conjuntos de recursos do software Cisco IOS. Uma liberação do Cisco IOS Software Release que apoia o CSAA/RTR deve ser instalada no dispositivo que o IPM se usa para recolher estatísticas de desempenho. Para obter um resumo das versões do Cisco IOS que oferecem suporte a CSAA/RTR/IPM, consulte o site na Web Perguntas mais freqüentes sobre IPM.

A informação adicional em relação ao IPM inclui:

- Visão geral do IPM
- Agente de garantia de serviço

Análise e ajuste de desempenho

O tráfego de usuário aumentou significativamente e colocou uma procura mais alta em recursos de rede. As gerentes de rede têm tipicamente uma vista limitada nos tipos de tráfego que são executado na rede. A caracterização de perfil de tráfego de aplicativo e usuário fornece uma visão detalhada do tráfego na rede. Duas Tecnologias, as pontas de prova RMON e o Netflow, fornecem a capacidade para recolher perfis de tráfego.

RMON

Os padrões rmon são projetados ser distribuídos em uma arquitetura distribuída onde os agentes (ou encaixado ou nas sondas isoladas) se comuniquem com uma estação central (o console de gerenciamento) através do SNMP. O padrão RFC 1757 RMON organiza as funções de monitoração em nove grupos para oferecer suporte às topologias de Ethernet e adicione um décimo grupo na RFC 1513 para parâmetros exclusivos de Token Ring. A monitoração do enlace rápido de Ethernet é fornecida no âmbito do padrão do RFC 1757, e a monitoração do anél de interface de dados distribuídos em fibra ótica (FDDI) é fornecida no âmbito do RFC 1757 e do RFC 1513.

A especificação RFC 2021 RMON emergente leva os padrões de monitoramento remoto além da camada MAC (Media Access Control) para as camadas da rede e de aplicativos. Essa configuração permite que administradores analisem e solucionem problemas de aplicações em rede, como tráfego da Web, NetWare, Notes, e-mail, acesso a banco de dados, NFS e outros. Alarmes, estatísticas, histórico e host/grupos de conversação RMON podem ser usados para monitorar proativamente e manter a disponibilidade da rede com base no tráfego de camada do aplicativo, o tráfego mais crítico na rede. O RMON2 permite administradores de rede de continuar seu desenvolvimento de soluções com base em padrões da monitoração a apoiar a missão crítica, aplicativos baseados em servidor.

As tabelas a seguir alistam as funções dos grupos RMON.

Grupo	Função

RMON (RFC 1757)	
Estatísticas	Contadores para pacotes, octetos, transmissões, erros, e ofertas no segmento ou na porta.
Histórico	Faz amostragens e salva os contadores de grupo de estatística para a recuperação posterior periodicamente.
Hosts	Mantém as estatísticas sobre cada dispositivo host no segmento ou na porta.
HostN superior	Um relatório de subconjunto definido pelo usuário do grupo Hosts, classificado por um contador estatístico. Ao retornar apenas os resultados, o tráfego de gerenciamento é minimizado.
Matriz de Tráfego	Mantém estatísticas de conversação entre anfitriões na rede.
Alarmes	Um ponto inicial que possa ser ajustado em variáveis de RMON crítica para o gerenciamento pró-ativo.
Eventos	Gera armadilhas de SNMP e entradas de registro quando é ultrapassado um limiar de grupo de alarmes.
Captura do pacote	Os Gerencia buffer de pacotes capturaram pelo grupo de filtros para transferir arquivos pela rede ao console de gerenciamento.
Token Ring	Estação de token ring — as estatísticas detalhadas no indivíduo postam a ordem da estação de token ring — uma lista de estação requisitada atualmente na configuração da estação de token ring do anel — configuração e inserção/remoção pelo roteamento de origem da estação — estatísticas no roteamento de origem, tal como contagens de saltos, e outro

RMON2	Função
Diretório do Protocolo	Protocolos para os quais o agente monitora e mantém estatísticas.
Distribuição de protocolo	Estatísticas para cada protocolo.
Host da camada	Estatísticas para cada endereço de camada de rede no segmento, anel ou porta.

da rede	
Matriz da camada da rede	As estatísticas de tráfego para pares de endereços de camada de rede.
Host de Camada de Aplicativos	Estatísticas por protocolo de camada de aplicação de cada endereço da rede.
Matriz da Camada de Aplicativo	Estatísticas de tráfego por protocolo da camada de aplicativos para os pares de endereços da camada de rede.
Histórico definível por usuário	Estatística da camada de link rmon1 do Estende histórico além para incluir algumas estatísticas RMON, RMON2, de MIB-I, ou MIB-II.
Mapeamento de endereços	Ligações de endereço de camada MAC a rede.
Grupo de configuração	Capacidades e configurações de agente.

Netflow

O recurso Cisco NetFlow permite que estatísticas detalhadas de fluxos de tráfego sejam coletadas para as funções de planejamento de capacidade, faturamento e Troubleshooting. O NetFlow pode ser configurado em interfaces individuais, fornecendo informações sobre o tráfego que passa por essas interfaces. Os seguintes tipos de informação são parte das estatísticas de tráfego detalhadas:

- Endereços IP de origem e de destino
- Número da interface de entrada e de saída
- Porta de origem TCP/UDP e portas de destino
- Número de bytes e pacotes no fluxo
- Números de sistemas autônomos de origem e de destino
- ToS (Tipo de serviço) de IP

Os dados do NetFlow coletados nos dispositivos de rede são exportados para uma máquina coletora. O coletor realiza funções como redução do volume de dados (filtragem e agregação), armazenamento de dados hierárquicos e gerenciamento do sistema de arquivos. Cisco fornece o coletor de Netflow e os aplicativos de analisador de Netflow para recolher e analisar dados do Roteadores e do Switches do Cisco catalyst. Existem também ferramentas shareware, como cflowd, que podem coletar os registros de UDP (protocolo de datagrama do usuário) Cisco NetFlow.

Os dados do NetFlow são transportados usando pacotes UDP em três formatos diferentes:

- Versão 1 — O formato original apoiado nas versões de Netflow inicial.

- Versão 5 — Um realce mais atrasado que adicionasse números de sequência da informação do sistema autônomo do protocolo de gateway de borda (BGP) e do fluxo.
- Versão 7 — Um realce ainda mais atrasado que adicionasse o apoio do Netflow Switching para Cisco Catalyst 5000 Series Switch equipou-se com um Netflow Feature Card (NFFC).

As versões de 2 a 4 e a versão 6 não foram lançadas ou não são suportadas pelo FlowCollector. Em todas as três versões, o datagrama consiste em um cabeçalho e um ou mais registros de fluxo.

Para mais informação, refira o White Paper do guia das soluções dos serviços de Netflow.

A tabela a seguir esboça versões do Cisco IOS apoiadas para recolher dados de Netflow do Roteadores e dos Catalyst Switches.

Versão do Cisco IOS Software	Plataformas de Hardware da Cisco Suportadas	Versões Exportadas de NetFlow Suportado
11.1 CA e 11.1 CC	Cisco 7200, 7500 e RSP7000	V1 e V5
11.2 e 11.2P	Cisco 7200, 7500 e RSP7000	V1
11.2P	Cisco Route Switch Module (RSM)	V1
11.3 e 11.3 T	Cisco 7200, 7500 e RSP7000	V1
12.0	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000 e RSM	V1 e V5
12.0T	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX 8800 RPM e BPX 8600	V1 e V5
12.0(3)T e posterior	Cisco 1600*, 1720, 2500**, 2600, 3600, 4500, 4700, AS5300*, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX8800 RPM e BPX 8650	V1, V5 e V8
12.0(6)S	Cisco 12000	V1, V5 e V8
	Cisco catalyst 5000 com Netflow Feature Card *** (NFFC)	V7

* O apoio para a exportação de Netflow V1, V5, e V8 no Cisco 1600 and 2500 platforms é visado para o Cisco IOS Software Release 12.0(T). O apoio do Netflow para estas Plataformas não está disponível na versão de linha principal do Cisco IOS 12.0.

** O apoio para o Netflow V1, V5, e V8 na plataforma AS5300 é visado para o Cisco IOS Software Release 12.06(T).

*** O MLS e a exportação de dados NetFlow são suportados no Catalyst 5000 Series Supervisor Engine Software Release 4.1(1) ou mais recente.

Gerenciamento de segurança

O objetivo do gerenciamento de segurança é controlar o acesso aos recursos de rede de acordo com diretrizes local de modo que a rede não possa ser sabotaged (intencionalmente ou involuntariamente). Um subsistema de gerenciamento da segurança, por exemplo, pode monitorar o registro de usuários em um recurso de rede, recusando acesso àqueles que inserirem códigos inadequados de acesso. O Gerenciamento de segurança é muito um assunto extenso; portanto, essa área do documento aborda somente a segurança relacionada ao SNMP e a segurança básica de acesso ao dispositivo.

A informação detalhada na segurança avançada inclui:

- Aumentando a segurança em redes IP
- OpenSystems

Começos bons de uma implementação de gerenciamento de segurança com políticas de segurança sonora e procedimentos no lugar. É importante criar uma configuração padrão mínima específica para plataforma para todo o Roteadores e Switches que seguem melhores prática da indústria para a Segurança e o desempenho.

Há uns vários métodos de controlar o acesso em roteadores Cisco e em Catalyst Switches. Alguns desses métodos incluem:

- Listas de controle de acesso (ACL)
- Usuário - ids e senhas localizam ao dispositivo
- Terminal Access Controller Access Control System (TACACS)

O TACACS é um protocolo de segurança padrão do Internet Engineering Task Force (RFC 1492) que seja executado entre dispositivos do cliente em uma rede e contra um servidor de TACACS. TACACS é um mecanismo de autenticação usado para autenticar a identidade de um dispositivo que busca acesso remoto a um banco de dados com privilégios. As variações do TACACS incluem o TACACS+, a arquitetura de AAA que separa funções do autenticação, autorização e relatório.

O TACACS+ é usado pelo Cisco para permitir um controle maior sobre quem acessa o dispositivo Cisco no modo privilegiado e não-privilegiado. Os server múltiplos TACACS+ podem ser configurados para a tolerância de defeito. Com o TACACS+ permitido, o roteador e o interruptor alertam o usuário para um nome de usuário e uma senha. A autenticação pode ser configurada para controle de logon ou para autenticar comandos individuais.

Autenticação

A autenticação é o processo de identificação de usuários, incluindo o login e senha, desafio e resposta, e suporte para mensagens. A autenticação é a maneira que um usuário é identificado antes de ser permitida o acesso ao roteador ou ao interruptor. Existe uma relação fundamental entre autenticação e autorização. Quanto mais privilégios de autorização um usuário recebe, mais segura deverá ser a autenticação.

Autorização

A autorização fornece controle de acesso remoto, incluindo autorização de uma vez e autorização para cada serviço que for solicitado pelo usuário. Em um Cisco Router, o intervalo de nível de autorização para usuários é de 0 a 15 com 0 sendo o nível mais baixo e 15 o mais alto.

Relatório

A contabilidade permite a coleta e a emissão da informação de segurança usada para a fatura, o exame, e o relatório, tal como identidades do usuário, horários de início e de parada, e comandos executados. O relatório permite aos gerentes de rede rastrear os serviços que os usuários estão acessando, bem como a quantidade de recursos de rede que estão consumindo.

A tabela a seguir alista comandos do exemplo básico para usar o TACACS+, o autenticação, autorização e relatório em um roteador Cisco e um Catalyst Switch. Refira o documento dos comandos do autenticação, autorização e relatório para uns comandos mais detalhados.

Comando do Cisco IOS	**Propósito**
Router	
aaa new-model	Permita a autenticação, autorização, explicando (AAA) como o método principal o controle de acesso.
Contabilidade AAA {*sistema* | *rede* | *conexão* | *exec* | *nível de comando*} {*start-stop* | *espera-início* | *parada-somente*} {*tacacs+* | *raio*}	Habilite o relatório com os comandos de configuração global.
Login padrão tacacs+ da autenticação de AAA	Estabelecer o roteador de modo que as conexões a toda a linha terminal configurada com o login padrão sejam autenticadas com o TACACS+, e falhará se a autenticação falha por qualquer razão.
AAA authorization exec default tacacs+ none	Configure o roteador para verificar se o usuário tem permissão para executar um shell EXEC perguntando ao servidor TACACS+.

endereço IP de Um ou Mais Servidores Cisco ICM NT do server do **host** *tacacs+ do TACACS-* **server**	Especifique o servidor TACACS+ que será usado para autenticação com comandos de configuração global.
tacacs-server key shared-secret	Especifique o segredo compartilhado conhecido pelos servidores TACACS+ e o roteador Cisco com o comando de configuração global.
Catalyst Switch	
set authentication login tacacs enable [*tudo	console	http |* **[primary] do** *telnet*]	Permita a autenticação TACACS+ para o modo de login normal. Use as palavras-chave do console ou do telnet para permitir o TACACS+ somente para a porta de Console ou as tentativas de conexão telnet.
opção de recuo} **do {option} do set authorization exec enable** [*console	telnet	ambos*]	Habilite autorização para o modo de logon normal. Use o console ou palavras-chave de Telnet para habilitar a autorização somente para a porta de console ou as tentativas de conexão Telnet.
Ajuste o compartilhar-*segredo* **chave do TACACS-server**	Especifique o segredo compartilhado que é sabido pelos server e pelo interruptor TACACS+.
Set tacacs-server host tacacs+ server ip address	Especifique o servidor TACACS+ que será usado para autenticação com comandos de configuração global.
Set accounting commands enable {*configuração	tudo*} *tacacs do* **{stop-only} +**	Ative a contabilização dos comandos de configuração.

Para obter mais informações sobre de como configurar o AAA para monitorar e controlar o acesso à interface de linha de comando nos Catalyst Enterprise LAN switch, refira o acesso de controlo ao interruptor usando o documento de autenticação, autorização e contabilidade.

Segurança de SNMP

O protocolo de SNMP pode ser usado para fazer alterações de configuração no Roteadores e Catalyst Switches similares àqueles emitidos do CLI. Configure medidas de segurança apropriadas nos dispositivos de rede para impedir acesso não autorizado e alterações via SNMP. Os string de comunidade devem seguir as diretrizes de senha padrão para o comprimento, os caráteres, e a dificuldade da suposição. É importante alterar as strings de comunidade dos padrões público e privado.

Todos os hosts de gerenciamento de SNMP devem ter um endereço IP estático e receber explicitamente direitos de comunicação de SNMP com o dispositivo de rede por aquele endereço IP predefinido e Lista de Controle de Acesso (ACL). Os softwares Cisco IOS e Cisco Catalyst fornecem recursos de segurança que garantem que apenas as estações de gerenciamento autorizadas tenham permissão para fazer alterações em dispositivos de rede.

Recursos de segurança de roteador

Nível de privilégio SNMP

Esse recurso limita os tipos de operações que uma estação de gerenciamento pode ter em um roteador. Há dois tipos de nível de privilégio no Roteadores: Read-Only (RO) e leitura/gravação (RW). O nível de RO só permite que uma estação de gerenciamento consulte os dados do roteador. Ele não permite a execução de comandos de configuração, como a reinicialização de um roteador e o fechamento de interfaces. Apenas o nível de privilégio RW pode ser usado para realizar essas operações.

Lista ACL de SNMP

Épossível usar o recurso SNMP ACL com o recurso de privilégio SNMP para limitar as requisições de informações das estações de gerenciamento específico feitas aos roteadores.

Opinião SNMP

Esse recurso limita as informações específicas que as estações de gerenciamento podem recuperar dos roteadores. Pode ser utilizado com recursos de nível de privilégio de SNMP e de ACL para aplicar acesso restrito de dados por consoles de gerenciamento. Para exemplos de configuração da opinião SNMP, vá à opinião do servidor snmp.

SNMP Versão 3

O SNMP versão 3 (SNMPv3) fornece trocas seguras de dados de gerenciamento entre dispositivos de rede e estações de gerenciamento. Os recursos de criptografia e autenticação do SNMPv3 garantem elevado grau de segurança no transporte de pacotes para um console de gerenciamento. O SNMPv3 é apoiado no Cisco IOS Software Release 12.0(3)T e Mais Recente. Para uma visão geral técnica do SNMPv3, vá à documentação SNMPv3.

Lista de Controle de Acesso (ACL) em interfaces

O recurso de ACL fornece medidas de segurança que evitam ataques, como falsificação de IP. O ACL pode ser aplicado em interfaces de entrada ou de saída nos roteadores.

Recursos de segurança de Catalyst LAN Switch

Lista da licença IP

A característica da lista da licença IP restringe o telnet de entrada e o acesso SNMP ao interruptor dos endereços IP de Um ou Mais Servidores Cisco ICM NT do origem não autorizada. As mensagens do syslog e as armadilhas do SNMP são suportadas para notificar um sistema de gerenciamento quando ocorre uma violação ou acesso não autorizado.

Uma combinação dos recursos de segurança do Cisco IOS pode ser usada para controlar o

Roteadores e os Catalyst Switches. Uma política de segurança precisa de ser estabelecida que limite o número de estações de gerenciamento capazes de alcançar o Switches e o Roteadores.

Para obter mais informações sobre de como aumentar a Segurança em redes IP, vá à segurança crescente em redes IP.

Gerenciamento de relatórios

Gerenciamento de contabilidade é o processo utilizado para medir os parâmetros de utilização da rede, de modo que cada usuário ou grupos de usuários na rede possam ser adequadamente regulados para finalidades contábeis ou de cobrança retroativa. Similar ao gerenciamento de desempenho, o primeiro passo em direção a um gerenciamento correto de relatório é medir a utilização de todos os recursos de rede importantes. A utilização do recurso de rede pode ser medida, utilizando os recursos Cisco NetFlow e Cisco IP Accounting. Uma análise dos dados coletados por esses métodos fornece uma percepção nos padrões atuais de utilização.

Uma contabilidade e sistema de faturamento uso-baseada é uma parte essencial de todo o contrato de nível de serviço (SLA). Fornece uma maneira prática de definir obrigações em um SAL e as conseqüências para comportamentos que não estejam de acordo com os termos do SLA.

Os dados podem ser recolhidos através das pontas de prova ou do cisco netflow. Cisco fornece o coletor de Netflow e os aplicativos de analisador de Netflow para recolher e analisar dados do Roteadores e dos Catalyst Switches. Aplicativos shareware, como cflowd, também são usados para a coleta de dados do NetFlow. Uma medição contínua do uso dos recursos pode conceder informações de faturamento, bem como as avaliações de informações contínuas consideráveis e recursos ideais. Algumas soluções de gerenciamento de relatório implantadas normalmente incluem:

- Evident Software

Estratégia de ativação de NetFlow e de coleta de dados

NetFlow (fluxo de rede) é uma tecnologia de medida lateral de entrada que permite a captura dos dados necessários para o planejamento de rede, monitoramento e aplicativos de relatório. O NetFlow deve ser distribuído em interfaces de roteador de ponta/agregação para provedores de serviço ou interfaces de roteador de acesso de WAN para clientes de empreendimento.

A Cisco Systems recomenda uma distribuição de NetFlow cuidadosamente planejada com os serviços NetFlow ativados nesses roteadores estrategicamente localizados. O NetFlow pode ser implementado incrementalmente (interface por interface) e estrategicamente (em roteadores selecionados meticulosamente), ao invés de ser implementado em cada roteador da rede. Os Ciscos personnel trabalharão com clientes para determinar em que Roteadores e Netflow chaves das relações da chave deve ser ativado com base nos padrões de fluxo de tráfego, na topologia de rede, e na arquitetura do cliente.

As principais considerações de distribuição incluem:

- Os serviços de NetFlow devem ser utilizados como medidores de margem e ferramenta de aceleração de desempenho da lista de acesso e não devem ser ativados em roteadores hot core/backbone ou roteadores que estejam sendo executados em taxas de utilização de CPU

muito altas.
- Compreendendo os requisitos de levantamento de dados direcionados ao aplicativo. Aplicativos de contabilidade só podem requerer informações de fluxo do roteador de origem e terminação, enquanto aplicativos de monitoramento podem requerer uma visão mais abrangente de ponta-a-ponta (com muitos dados).
- Compreenda o impacto da topologia de rede e da política de roteamento na estratégia de coleção do fluxo. Por exemplo, evite coletar fluxos duplicados ao ativar o NetFlow em roteadores de agregação-chave em que o tráfego se origina ou termina, e não em roteadores de backbone ou intermediários, o que forneceria visões duplicadas das informações do mesmo fluxo.
- Os provedores de serviços no negócio de *portador de trânsito* (tráfego levando nem que origina nem que termina em sua rede) podem utilizar dados de exportação de Netflow para o uso de tráfego de trânsito de recurso de rede de medição para finalidades de contabilidade e faturamento.

Configurar a contabilidade IP

O suporte de relatório de IP Cisco fornece funções básicas de relatório de IP. Ao habilitar a contabilização de IP, os usuários podem visualizar o número de bytes e pacotes comutados pelo Cisco IOS Software com IP Addresses de base de origem e de destino. Apenas o tráfego IP de trânsito é medido e apelas em base de saída. O tráfego gerado pelo software ou terminando no software não foi incluído nas estatísticas de contabilidade. Para manter relatórios precisos total, o software mantém dois bases de dados de contabilidade: um banco de dados ativo e um de ponto de controle.

O suporte de contabilidade IP da Cisco também fornece informações que identificam o tráfego IP com falha nas listas de acesso IP. Identificar a fonte de endereço IP que viola as listas de acesso de IP, sinaliza as possíveis tentativas de romper a segurança. Os dados igualmente indicam que as configurações da lista de acesso IP devem ser verificadas. Para tornar esse recurso disponível para os usuários, habilite a contabilidade IP de violações da lista de acesso, usando o comando ip accounting access-violations. Os usuários podem então indicar o número de byte e pacote de um origem única que tente à ruptura de segurança contra a lista de acessos para o par de destino de origem. Como padrão, o relatório de IP exibe o número de pacotes que passaram por listas de acesso e foram roteados.

Para permitir a contabilidade IP, use um dos comandos seguintes para cada relação no modo de configuração da interface:

Comando	Propósito
ip accounting	Permita a contabilidade básica IP.
ip accounting access violations	Habilite a contabilidade IP com a capacidade de identificar tráfego IP que falhe nas listas de acessos IP.

Para configurar outras funções de relatório de IP, use um ou mais dos seguintes comandos no modo de configuração global:

Comando	Propósito

ip accounting-threshold threshold	Ajuste os números máximos de entrada de relatórios a ser criados.
ip accounting-list ip-address wildcard	Filtre informações de contabilização para hosts.
ip accounting-transits count	Controle o número de registros de transmissão que serão armazenados no banco de dados de contabilidade de IP.

Informações Relacionadas

- Guia de configuração de fundamentos da configuração
- Soluções de gerenciamento de empresa Cisco, volume mim pela impressão Cisco, ISBN 1587050064
- Suporte Técnico e Documentação - Cisco Systems

Era este documento útil? Sim nenhum

Obrigado para seu feedback.

Abra um caso de suporte (exige um contrato de serviço Cisco.)

Cisco relacionado apoia discussões da comunidade

Cisco apoia a comunidade é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira convenções dos dicas técnicas da Cisco para obter informações sobre das convenções usadas neste documento.

Atualizado em: julho 11, 2007
ID do Documento: 15114