Como detectar e limpar conexões TCP suspensas usando SNMP

Contents

Introduction

Este documento descreve como usar o Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) para detectar e limpar conexões TCP suspensas em um dispositivo Cisco IOS. O documento também explica os objetos SNMP que você usa para essa finalidade.

A seção intitulada Script PERL para detectar e limpar conexões TCP suspensas, fornece um link para um script PERL que implementa essas instruções.

Prerequisites

Requirements

Os leitores deste documento devem estar cientes destes tópicos:

- Entender como visualizar informações de conexão TCP em dispositivos Cisco
- Uso geral de **comandos** SNMP **walk**, **get**, **get-next** e **set**
- Compreenda como configurar o SNMP em um dispositivo Cisco

Componentes Utilizados

Este documento se aplica aos roteadores e switches Cisco que executam o software IOS que suportam os módulos TCP-MIB e CISCO-TCP-MIB.

Observação: o módulo CISCO-TCP-MIB não é carregado por padrão em NET-SNMP. Se o módulo MIB não estiver carregado em seu sistema, você deverá usar o OID para referenciar um objeto em vez de seu nome.

As informações neste documento são baseadas em todas as versões de software e hardware do IOS.

As informações são baseadas nesta versão do NET-SNMP:

- NET-SNMP version 5.1.2 available at http://www.net-snmp.org/

O script PERL foi testado com versões PERL:

- 5.005_03 no FreeBSD
- 5.8.0 no Solaris 5.8
- 5.005_02 — enviado como parte do CiscoWorks SNMS no Microsoft Windows 2000
- ativePerl 5.8.4 no Microsoft Windows 2000, disponível em http://www.activestate.com/Products/ActivePerl/.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Informações de Apoio

Detalhes dos objetos MIB — inclui identificadores de objeto (OIDs)

Estes são os objetos que você usa:

No módulo CISCO-TCP-MIB:

- ciscoTcpConnInBytes, OID .1.3.6.1.4.1.9.9.6.1.1.1O número de bytes de entrada nesta conexão.
- ciscoTcpConnInPkts, OID 1.3.6.1.4.1.9.9.6.1.1.2O número de pacotes inseridos nesta conexão.
- ciscoTcpConnOutBytes, OID .1.3.6.1.4.1.9.9.6.1.1.3O número de bytes de saída nesta conexão
- ciscoTcpConnOutPkts, OID .1.3.6.1.4.1.9.9.6.1.1.1.4O número de saída de pacotes nesta conexão.
- ciscoTcpConnRetransPkts, OID .1.3.6.1.4.1.9.9.6.1.1.7O número de pacotes retransmitidos nesta conexão.

- ciscoTcpConnRto, OID .1.3.6.1.4.1.9.9.6.1.1.1.9O valor de tempo limite de retransmissão para esta conexão.

Do módulo TCP-MIB:

- tcpConnState, OID .1.3.6.1.2.1.6.13.1.1O status desta conexão.

Há mais detalhes sobre esses objetos em Informações Detalhadas do Objeto MIB.

Usar SNMP para detectar se uma conexão TCP trava

Summary

Estas etapas ajudam a determinar se uma conexão TCP trava:

1. Para determinar se os objetos ciscoTcpConnRetransPkts e ciscoTcpConnRto são suportados no dispositivo, execute uma **operação** SNMP **get-next** no ciscoTcpConnRto e verifique se algum objeto é retornado.**Nota:** Você só precisa verificar um objeto porque o suporte para ambos foi adicionado ao mesmo tempo.**Observação:** nem todos os dispositivos da Cisco suportam os dois últimos objetos (ciscoTcpConnRetransPkts e ciscoTcpConnRto), mas seu uso pode aumentar a precisão da detecção.Se os objetos ciscoTcpConnRetransPkts e ciscoTcpConnRto **tiverem** suporte, vá para a Etapa 2.Se os objetos ciscoTcpConnRetransPkts e ciscoTcpConnRto **não** tiverem suporte, vá para a Etapa 3.
2. Todos os objetos são suportados. Para cada conexão TCP, verifique estes:ciscoTcpConnOutBytes é 0.ciscoTcpConnOutPkts é 0.ciscoTcpConnRetransPkts é maior que 0.ciscoTcpConnRto é maior que 20.000.**Observação:** os 20.000 podem ser reduzidos para acelerar a detecção. Leva mais ou menos um minuto para Rto alcançar 20.000 quando a conexão é interrompida. No entanto, valores menores podem reduzir a precisão do resultado.Se todas as conexões anteriores forem verdadeiras, essa conexão TCP será interrompida e poderá ser limpa. Continue a usar o SNMP para limpar uma conexão TCP que trava.
3. Apenas os quatro primeiros objetos são suportados. Para cada conexão TCP, verifique estes:ciscoTcpConnInBytes é maior que 0.ciscoTcpConnInPkts é 0.ciscoTcpConnOutBytes é 0.ciscoTcpConnOutPkts é 0.Aguarde alguns segundos e **obtenha** os objetos novamente para verificar se não era uma conexão TCP no processo de estabelecimento.**Observação:** as duas primeiras verificações (um número positivo de bytes de entrada mas nenhum pacote de entrada) podem parecer estranhas, mas foram verificadas em relação a vários dispositivos e versões do IOS.**Observação:** as versões do IOS que suportam todos os seis objetos podem não exibir esse comportamento e, portanto, o teste na Etapa 2 não inclui esses dois primeiros testes.Se todos os objetos atenderem aos testes ambas as vezes, essa conexão TCP é suspensa e pode ser limpa. Continue a usar o SNMP para limpar uma conexão TCP que trava.

Step-by-Step Instructions

Os valores neste exemplo são:

- Nome do host do dispositivo a = nms-7206a (suporta todos os objetos)

- Nome de host do dispositivo b = nms-1605 (suporta apenas os primeiros quatro objetos)
- Comunidade de leitura = público
- Comunidade de gravação = privado

Substitua as strings de comunidade e o nome do host nestes comandos:

1. Determine se este dispositivo suporta os objetos ciscoTcpConnRetransPkts e ciscoTcpConnRto:Execute uma operação **get-next** de **SNMP** em ciscoTcpConnRto:
   ```
   snmpgetnext -c public nms-7206a ciscoTcpConnRto
   ```

   Se os objetos **forem** suportados, você verá uma resposta como esta:
   ```
   CISCO-TCP-MIB::ciscoTcpConnRto.14.32.100.75.2065.172.18.86.111.23092 =
        INTEGER: 303 milliseconds
   ```

   Observação: o índice usado para esses objetos, neste caso `14.32.100.75.2065.172.18.86.111.23092`, é uma concatenação do endereço IP local—14.32.100,75, o número da porta TCP local—2065, o endereço IP remoto—172.18.86.111 e o número da porta TCP remota—23092.O retorno é para ciscoTcpConnRto. Vá para o Passo 2.Se os objetos **não** tiverem suporte, você verá uma resposta como esta:
   ```
   snmpgetnext -c public nms-1605 ciscoTcpConnRto
   CISCO-FLASH-MIB::ciscoFlashDevicesSupported.0 = INTEGER: 1
   ```

   O retorno **não** é para o objeto ciscoTcpConnRto. O objeto exato retornado não é importante. Vá para o Passo 3.
2. **Obtenha** informações sobre cada conexão TCP para dispositivos que suportam todos os seis objetos na tabela de conexão TCP da Cisco.Execute uma próxima operação get-next de SNMP em ciscoTcpConnOutBytes, ciscoTcpConnOutPkts, ciscoTcpConnRetransPkts e ciscoTcpConnRto:
   ```
   snmpgetnext -c public nms-7206a ciscoTcpConnOutBytes
                         ciscoTcpConnOutPkts
                         ciscoTcpConnRetransPkts
                         ciscoTcpConnRto
   ```

   Você vê uma resposta como esta:
   ```
   CISCO-TCP-MIB::ciscoTcpConnOutBytes.14.32.100.75.2065.172.18.86.111.23092 = Counter32:
   383556
   CISCO-TCP-MIB::ciscoTcpConnOutPkts.14.32.100.75.2065.172.18.86.111.23092 = Counter32: 8061
   CISCO-TCP-MIB::ciscoTcpConnRetransPkts.14.32.100.75.2065.172.18.86.111.23092 = Counter32: 2
   CISCO-TCP-MIB::ciscoTcpConnRto.14.32.100.75.2065.172.18.86.111.23092 = INTEGER: 303
   milliseconds
   ```

   Verifique estes:ciscoTcpConnOutBytes é 0.ciscoTcpConnOutPkts é 0.ciscoTcpConnRetransPkts é maior que 0.ciscoTcpConnRto é maior que 20.000.**Observação:** os 20.000 podem ser reduzidos para acelerar a detecção. Leva mais ou menos um minuto para Rto alcançar 20.000 quando a conexão é interrompida. No entanto, valores menores podem reduzir a precisão do resultado.Se tudo isso for verdade, essa conexão TCP será interrompida e poderá ser limpa. Continue a usar o SNMP para limpar uma conexão TCP que trava.Continue **andando** pela tabela de conexão TCP. Para fazer isso, execute uma operação **get-next** do SNMP repetidamente enquanto você verifica conexões suspensas, usando os objetos retornados como estes:
   ```
   snmpgetnext -c public nms-7206a ciscoTcpConnOutBytes.14.32.100.75.2065.172.18.86.111.23092
                         ciscoTcpConnOutPkts.14.32.100.75.2065.172.18.86.111.23092
   ```

```
                    ciscoTcpConnRetransPkts.14.32.100.75.2065.172.18.86.111.23092
                    ciscoTcpConnRto.14.32.100.75.2065.172.18.86.111.23092
```

Verifique cada entrada usando o teste anterior até que a operação **get-next** retorne objetos desta maneira:

```
CISCO-TCP-MIB::ciscoTcpConnInPkts.14.32.100.75.2065.172.18.86.111.23092 = Counter32: 8097
CISCO-TCP-MIB::ciscoTcpConnElapsed.14.32.100.75.2065.172.18.86.111.23092 =
  Timeticks: (17296508) 2 days, 0:02:45.08
CISCO-TCP-MIB::ciscoTcpConnFastRetransPkts.14.32.100.75.2065.172.18.86.111.23092 =
Counter32: 0
CISCO-FLASH-MIB::ciscoFlashDevicesSupported.0 = INTEGER: 5
```

Você agora andou por todas as conexões TCP neste dispositivo e terminou.

3. **Obtenha** informações sobre cada conexão TCP para dispositivos que suportam somente os quatro primeiros objetos na tabela de conexão TCP da Cisco.Execute uma operação **get-next** de SNMP em ciscoTcpConnInBytes, ciscoTcpConnInPkts ciscoTcpConnOutBytes e ciscoTcpConnOutPkts:

```
snmpgetnext -c public nms-1605 ciscoTcpConnInBytes
                    ciscoTcpConnInPkts
                    ciscoTcpConnOutBytes
                    ciscoTcpConnOutPkts
```

Você vê uma resposta como esta:

```
CISCO-TCP-MIB::ciscoTcpConnInBytes.14.32.6.185.23.14.32.100.33.2249 = Counter32: 68
CISCO-TCP-MIB::ciscoTcpConnInPkts.14.32.6.185.23.14.32.100.33.2249 = Counter32: 12
CISCO-TCP-MIB::ciscoTcpConnOutBytes.14.32.6.185.23.14.32.100.33.2249 = Counter32: 170
CISCO-TCP-MIB::ciscoTcpConnOutPkts.14.32.6.185.23.14.32.100.33.2249 = Counter32: 17
```

Verifique se eles são verdadeiros:ciscoTcpConnInBytes é maior que 0.ciscoTcpConnInPkts é 0.ciscoTcpConnOutBytes é 0.ciscoTcpConnOutPkts é 0.Aguarde alguns segundos e **obtenha** os objetos novamente. Verifique se não era uma conexão TCP no processo de estabelecimento.Se todas as opções acima **forem** verdadeiras, essa conexão TCP será interrompida e poderá ser limpa. Continue a usar o SNMP para limpar uma conexão TCP que trava.Continue **andando** pela tabela de conexão TCP. Para fazer isso, execute uma operação **get-next** do SNMP repetidamente enquanto você verifica conexões suspensas, usando os objetos retornados como estes:

```
snmpgetnext -c public nms-1605 ciscoTcpConnInBytes.14.32.6.185.23.14.32.100.33.2249
                    ciscoTcpConnInPkts.14.32.6.185.23.14.32.100.33.2249
                    ciscoTcpConnOutBytes.14.32.6.185.23.14.32.100.33.2249
                    ciscoTcpConnOutPkts.14.32.6.185.23.14.32.100.33.2249
```

Verifique cada entrada usando o teste anterior até que a operação **get-next** retorne objetos desta maneira:

```
CISCO-TCP-MIB::ciscoTcpConnOutBytes.14.32.6.185.23.14.32.100.33.4184 = Counter32: 170
CISCO-TCP-MIB::ciscoTcpConnOutPkts.14.32.6.185.23.14.32.100.33.4184 = Counter32: 17
CISCO-TCP-MIB::ciscoTcpConnInPkts.14.32.6.185.23.14.32.100.33.4184 = Counter32: 12
CISCO-TCP-MIB::ciscoTcpConnElapsed.14.32.6.185.23.14.32.100.33.4184 = Timeticks: (4345)
0:00:43.45
```

Você agora andou por todas as conexões TCP neste dispositivo e terminou.

Usar o SNMP para limpar uma conexão TCP que trava

Step-by-Step Instructions

Você pode usar o SNMP para limpar uma conexão TCP suspensa. O comando SNMP é equivalente ao comando clear tcp local <*local_ip*> <*local_port*> ***remote*** <*remote_ip*> <*remote_port*>. O objeto que você usa para limpar uma linha é **tcpConnState**.

Para limpar uma conexão TCP suspensa com SNMP, emita este comando:

```
snmpset -c private nms-7206a tcpConnState.14.32.100.75.2065.172.18.86.111.23092 integer
deleteTCB
TCP-MIB::tcpConnState.14.32.100.75.2065.172.18.86.111.23092 = INTEGER: deleteTCB(12)
```

Observação: o índice usado para esses objetos, neste caso `14.32.100.75.2065.172.18.86.111.23092`, é uma concatenação do endereço IP local—14.32.10 0,75, o número da porta TCP local—2065, o endereço IP remoto—172.18.86.111 e o número da porta TCP remota—23092.

Observação: você deve usar o índice exato que determinou que foi suspenso em Usar SNMP para detectar se uma conexão TCP trava. Lembre-se de que esse comando desconecta uma conexão TCP sem aviso prévio.

Informações detalhadas do objeto MIB

```
.1.3.6.1.4.1.9.9.6.1.1.1.1
ciscoTcpConnInBytes OBJECT-TYPE
        -- FROM CISCO-TCP-MIB
        SYNTAX          Counter
        MAX-ACCESS      read-only
        STATUS          Current
        DESCRIPTION     "Number of bytes that have been input on this TCP
                        connection."
::= { ciscoTcpConnEntry 1 }

.1.3.6.1.4.1.9.9.6.1.1.1.2
ciscoTcpConnOutBytes OBJECT-TYPE
        -- FROM CISCO-TCP-MIB
        SYNTAX          Counter
        MAX-ACCESS      read-only
        STATUS          Current
        DESCRIPTION     "Number of bytes that have been output on this TCP
                        connection."
::= { ciscoTcpConnEntry 2 }

.1.3.6.1.4.1.9.9.6.1.1.1.3
ciscoTcpConnInPkts OBJECT-TYPE
        -- FROM CISCO-TCP-MIB
        SYNTAX          Counter
        MAX-ACCESS      read-only
        STATUS          Current
        DESCRIPTION     "Number of packets that have been input on this TCP
                        connection."
::= { ciscoTcpConnEntry 3 }

.1.3.6.1.4.1.9.9.6.1.1.1.4
ciscoTcpConnOutPkts OBJECT-TYPE
        -- FROM CISCO-TCP-MIB
        SYNTAX          Counter
```

```
        MAX-ACCESS      read-only
        STATUS          Current
        DESCRIPTION     "Number of packets that have been output on this TCP
                        connection."
::= { ciscoTcpConnEntry 4 }

.1.3.6.1.4.1.9.9.6.1.1.1.7
ciscoTcpConnRetransPkts OBJECT-TYPE
        -- FROM CISCO-TCP-MIB
        SYNTAX          Counter
        MAX-ACCESS      read-only
        STATUS          Current
        DESCRIPTION     "The total number of packets retransmitted due to a timeout -
                        that is, the number of TCP segments transmitted containing
                        one or more previously transmitted octets."
::= { ciscoTcpConnEntry 7 }

.1.3.6.1.4.1.9.9.6.1.1.1.9
ciscoTcpConnRto OBJECT-TYPE
        -- FROM CISCO-TCP-MIB
        SYNTAX          Integer
        MAX-ACCESS      read-only
        STATUS          Current
        DESCRIPTION     "The current value used by a TCP implementation for the
                        retransmission timeout."
::= { ciscoTcpConnEntry 9 }

.1.3.6.1.2.1.6.13.1.1
tcpConnState OBJECT-TYPE
        -- FROM RFC1213-MIB
        SYNTAX          Integer { closed(1), listen(2), synSent(3), synReceived(4),
                        established(5), finWait1(6), finWait2(7), closeWait(8), lastAck(9),
                        closing(10), timeWait(11), deleteTCB(12) }
        MAX-ACCESS      read-write
        STATUS          Mandatory
        DESCRIPTION     "The state of this TCP connection.

                        The only value which may be set by a management
                        station is deleteTCB(12).  Accordingly, it is
                        appropriate for an agent to return a `badValue'
                        response if a management station attempts to set
                        this object to any other value.

                        If a management station sets this object to the
                        value deleteTCB(12), then this has the effect of
                        deleting the TCB (as defined in RFC 793) of the
                        corresponding connection on the managed node,
                        resulting in immediate termination of the
                        connection.

                        As an implementation-specific option, a RST

                        segment may be sent from the managed node to the
                        other TCP endpoint (note however that RST segments
                        are not sent reliably)."
::= { tcpConnEntry 1 }
```

Script PERL para detectar e limpar conexões TCP suspensas

Esse link fornece um arquivo de arquivo com um script PERL e os módulos MIB necessários. Clique com o botão direito do mouse no link e salve o arquivo no sistema.

- fixTCPhang.tgz

Os arquivos no arquivo são:

- bin/fixTCPhang.pl
- mibs/CISCO-SMI.my
- mibs/CISCO-TCP-MIB.my

Para extrair o script e os módulos MIB, use um utilitário como gzip e tar em sistemas operacionais semelhantes a UNIX. Por exemplo, para extrair os arquivos para **/tmp** supondo que o arquivo morto seja colocado em **/tmp**:

```
cd /tmp; gzip -dc fixTCPhang.tgz | tar -xvf -
```

Observação: talvez seja necessário editar a primeira linha do script para especificar o local do PERL.

Use winzip ou outros utilitários em sistemas operacionais Microsoft Windows para extrair os arquivos. Se você extrair os arquivos para **c:\tmp**, então não precisará especificar a opção -m quando executar o script.

Chame os arquivos com este comando:

```
fixTCPhang.pl -c public -C private -f nms-7206a
```

Para cada conexão TCP suspensa encontrada, você vê uma linha como esta saída:

```
Found bad TCP connection: Local IP: 14.32.100.75 port 23 Remote IP: 172.18.100.33 port 47878:
CLEARED
```

Como a string de comunidade de leitura/gravação foi fornecida e a opção -f foi especificada, o script limpou a conexão. Observe a instrução `CLEARED` no final da saída.

O script suporta SNMP versões 1, 2c e 3. Se você especificar a versão 3 do SNMP, deverá especificar todas as informações de autenticação no argumento -v. Este é um exemplo de uso do SNMP v3:

```
fixTCPhang.pl -v "3 -a MD5 -u chelliot -A chelliot -l authNoPriv" -f nms-dmz-ap1200-b
```

Os comandos IOS para configurar SNMP v3 para o exemplo anterior são:

```
snmp-server group chelliot-group v3 auth write v1default
snmp-server user chelliot chelliot-group v3 auth md5 chelliot
```

Observação: parece haver um bug na versão Windows do NET-SNMP usado neste teste. O bug não permite que a autenticação SHA funcione corretamente.

Há várias outras opções que você pode usar com este script. Algumas das opções de script incluem onde encontrar os utilitários de linha de comando NET-SNMP e onde encontrar os módulos MIB se eles não estiverem em **/tmp/mibs**. Você também pode exibir este resumo dessas opções:

```
fixTCPhang.pl
fixTCPhang.pl [-dfhV -c <read_community> -C <write_community> -m <mib_directory>
               -p <command_path> -t <timeout> -v <snmp_version>] <device>
  Version 1.2
  Detect hung TCP connections on <device>, optionally clearing them.
  Options:  -c  Specify read community string. Defaults to public.
            -C  Specify the readwrite community string. No default.
                 Must be supplied for the script to clear hung connections.
            -d  Turn on debug mode.
            -f  Fix or clear any hung TCP connections found.
            -h  Print this message.
            -m  Specify the directory to find CISCO-SMI.my and CISCO-TCP-MIB.my.
                 Defaults to /tmp/mibs.
            -p  Where to find the net-snmp utilities.
                 Optional if the utilities are in the path.
            -t  SNMP Timeout value. Defaults to 5 sec.
            -v  Specify SNMP version to use: One of 1, 2c, or 3.
                 If 3 is specified then this option must include all of the
                 authentication information for SNMPv3. For example:
                 "3 -a MD5 -u chelliot -A chelliot -l authNoPriv"
                 Note: NET-SNMP seems to have a bug with SHA authentication on Windows.
                 See the NET-SNMP documentation for more information.
                 Defaults to SNMP version 1.
            -V  Print version number.
```

Informações Relacionadas

- Suporte Técnico - Cisco Systems