Aplicação do aprimoramento de recursos ASA SNMP

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Apoio para anfitriões 128 SNMP
Propósito
Modo do Único-contexto
Modo do Multi-contexto
Descrição
Configurar
Comandos CLI
Exemplo de configuração
Apoio para o cpmCPUTotal5minRev SNMP OID
Propósito
Comandos CLI
OID novos
Troubleshooting
comandos show

Introdução

Este documento descreve as características novas do Simple Network Management Protocol (SNMP) que estão disponíveis para o Firewall adaptável do 5500-X Series da ferramenta de segurança de Cisco (ASA) no Software Release 9.1.5 e nas liberações 9.2.(1) e mais atrasadas.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no Firewall do 5500-X Series de Cisco ASA que executa o Software Release 9.1.5 e as liberações do ® de Cisco ASA 9.2.(1) e mais atrasado.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Nas versões ASA 9.1.5 e 9.2.1, estes realces SNMP são introduzidos:

- O apoio para anfitriões 128 SNMP é adicionado.
- O apoio para os identificadores de objeto do cpmCPUTotal5minRev SNMP (OID) é adicionado.
- O apoio para os mensagens snmp 1,472-byte é adicionado.

Apoio para anfitriões 128 SNMP

Esta característica permite que o ASA apoie mais do que a corrente 32 anfitriões SNMP.

Propósito

Atualmente, o ASA tem um limite duro de um total de 32 anfitriões SNMP. Isto inclui os anfitriões que podem ser configurados para armadilhas e votando. As próximas seções descrevem as influências que esta característica tem modos em únicos e do multi-contexto.

Modo do Único-contexto

- Permite que um número significativamente mais alto de entradas (anfitriões totais) seja configurado, para cima de 4,096. Contudo, fora destas entradas, somente o 128 pode ser usado para armadilhas.
- Para propósitos de configuração de vatação, a até são permitidos 4,096 anfitriões e host de armadilha 128 de vatação ser configurados. Contudo, o número real de server que votam o sistema devem ser restringidos a menos do que o 128, porque os impactos no desempenho de um número mais alto de anfitriões são desconhecidos e não apoiados.

Modo do Multi-contexto

- Para propósitos de configuração, até 4,000 anfitriões pelo contexto são permitidos e um limite sistema-largo de 64,000 anfitriões totais é imposto.

- Fora do total os anfitriões configurados, somente 128 (pelo contexto) podem ser usados para armadilhas, e o limite de sistema total para armadilhas no modo do multi-contexto são 32,000.

- Embora você possa configurar até 4,000 anfitriões totais pelo contexto, o número real de server que votam todo o contexto deve ser limitado ao 128.

Descrição

Você pôde preferir monitorar os dispositivos de rede de um grande pool de anfitriões SNMP. Idealmente, você quer a capacidade para especificar uma escala IP e/ou uma sub-rede dos endereços IP de Um ou Mais Servidores Cisco ICM NT que são permitidos monitorar os dispositivos de rede. O ASA atualmente não fornece essa flexibilidade e limita os anfitriões do máximo SNMP a 32.

O apoio para esta característica envolve dois aspectos:

- Forneça a capacidade para que o ASA segure até anfitriões 128 SNMP.

- Forneça os comandos required configuration de modo que você possa configurar um número significativamente mais alto de anfitriões, como detalhado na seção anterior através de um comando único.

O projeto atual no ASA é tal que os host individuais podem ser configurados através do CLI. Para esta característica, estes requisitos de projeto adicionais foram considerados:

- A introdução do comando CLI do host-**grupo do servidor snmp** com retenção do comando CLI do **host do servidor snmp**.

- A capacidade para que as entradas venham do host-**grupo do servidor snmp** e dos comandos CLI do **host do servidor snmp**.

- Para o SNMP Versão 3, a introdução do comando CLI do **userlist do servidor snmp** com retenção do comando CLI do **usuário do servidor snmp**.

- Uma sobreposição da configuração deve igualmente ser apoiada. Por exemplo, os comandos múltiplos do host-**grupo** podem ser dados com anfitriões que sobrepõem nos objetos de rede. Similarmente, você pode especificar um host com um endereço IP de Um ou Mais Servidores Cisco ICM NT que sobreponha com os anfitriões atuais ou o grupo do host. Isto fornece um mecanismo que possa ser usado a fim overwrite os parâmetros para alguns anfitriões em um grupo, sem a necessidade de reconfigurar o grupo completo.

Algumas restrições de software e advertências que são associadas com esta característica são:

- Como parte do comando do host-**grupo do servidor snmp**, o padrão é **votação** se **[armadilha|a votação]** não é especificada. É igualmente importante notar que para este comando, as armadilhas e a votação não podem ser permitidas para o mesmo grupo do host. Se isto é exigido, Cisco recomenda que você usa o **comando snmp-server host** para os anfitriões relevantes.

- Você pode especificar os objetos de rede que sobrepõem em comandos diferentes do host-**grupo**. Os valores que são especificados no último grupo do host tomam o efeito para o grupo comum de anfitriões nos objetos de rede diferentes.

Aqui está um exemplo:

```
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55

snmp-server host-group inside network1 poll version 3 user-list SNMP-List
snmp-server host-group inside network2 poll version 3 user-list SNMP-List
```

Inscreva o **comando snmp-server host da mostra** a fim ver entradas de host:

```
asa(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
host ip = 64.103.236.43, interface = inside  poll version 3 cisco1
host ip = 64.103.236.44, interface = inside  poll version 3 cisco1
host ip = 64.103.236.45, interface = inside  poll version 3 cisco1
host ip = 64.103.236.46, interface = inside  poll version 3 cisco1
host ip = 64.103.236.47, interface = inside  poll version 3 cisco1
host ip = 64.103.236.48, interface = inside  poll version 3 cisco1
host ip = 64.103.236.49, interface = inside  poll version 3 cisco1
host ip = 64.103.236.50, interface = inside  poll version 3 cisco1
host ip = 64.103.236.51, interface = inside  poll version 3 cisco1
host ip = 64.103.236.52, interface = inside  poll version 3 cisco1
host ip = 64.103.236.53, interface = inside  poll version 3 cisco1
host ip = 64.103.236.54, interface = inside  poll version 3 cisco1
host ip = 64.103.236.55, interface = inside  poll version 3 cisco1
```

Estão aqui algumas observações importantes sobre o uso desta característica:

- Se um grupo do host ou um host que sobreponham com outros grupos do host são suprimidos, os anfitriões estabelecem-se outra vez com os valores que são usados para os grupos configurados do host.
- Os valores ou os parâmetros que são associados com os anfitriões são dependentes da ordem que os comandos estão executados.
- A lista de usuários que é configurada não pode ser suprimida se a lista é usada por um grupo do host particular.
- O usuário SNMP não pode ser suprimido se o usuário é referido dentro uma lista de usuário particular.
- Um objeto de rede não pode ser suprimido se é usado pelo comando CLI do host-**grupo**.

Configurar

Use a informação que é descrita nesta seção a fim configurar o ASA de modo que estes novos recursos sejam executados.

> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Comandos CLI

Para o SNMP Versão 3, o administrador pode associar vários usuários com um grupo especificado de anfitriões. Isto é útil se o administrador quer um grupo de usuários ter a capacidade para alcançar o ASA de um grupo de anfitriões. Este comando CLI é usado a fim configurar uma lista de usuários para usuários múltiplos:

```
ASA(config)# [no] snmp-server user-list <list_name> username <user_name>
```

A fim associar a lista de usuários com um grupo do host, incorpore este comando no CLI:

```
[no] snmp-server host-group <interface> <network-object> [trap|poll]
[community [enc_type] <text>] [version {1 | 2c | 3 [user name | user-list
<list-name>]}] [udp-port <port_number>]
```

Com este comando único, você pode especificar um objeto de rede a fim indicar os host múltiplos que devem ser adicionados. Com o objeto de rede, você pode especificar uma máscara de sub-rede ou a escala dos endereços IP de Um ou Mais Servidores Cisco ICM NT que devem ser adicionados, com o uso de um comando único. Todos os endereços IP de Um ou Mais Servidores Cisco ICM NT que são alistados como parte do objeto de rede são adicionados como entradas de host SNMP. Similarmente, para cada um dos usuários que são especificados na lista de usuários, há uma entrada de host separada SNMP.

Estes comandos são usados a fim permitir que os administradores cancelem e ver as opções de configuração novas para os servidores SNMP:

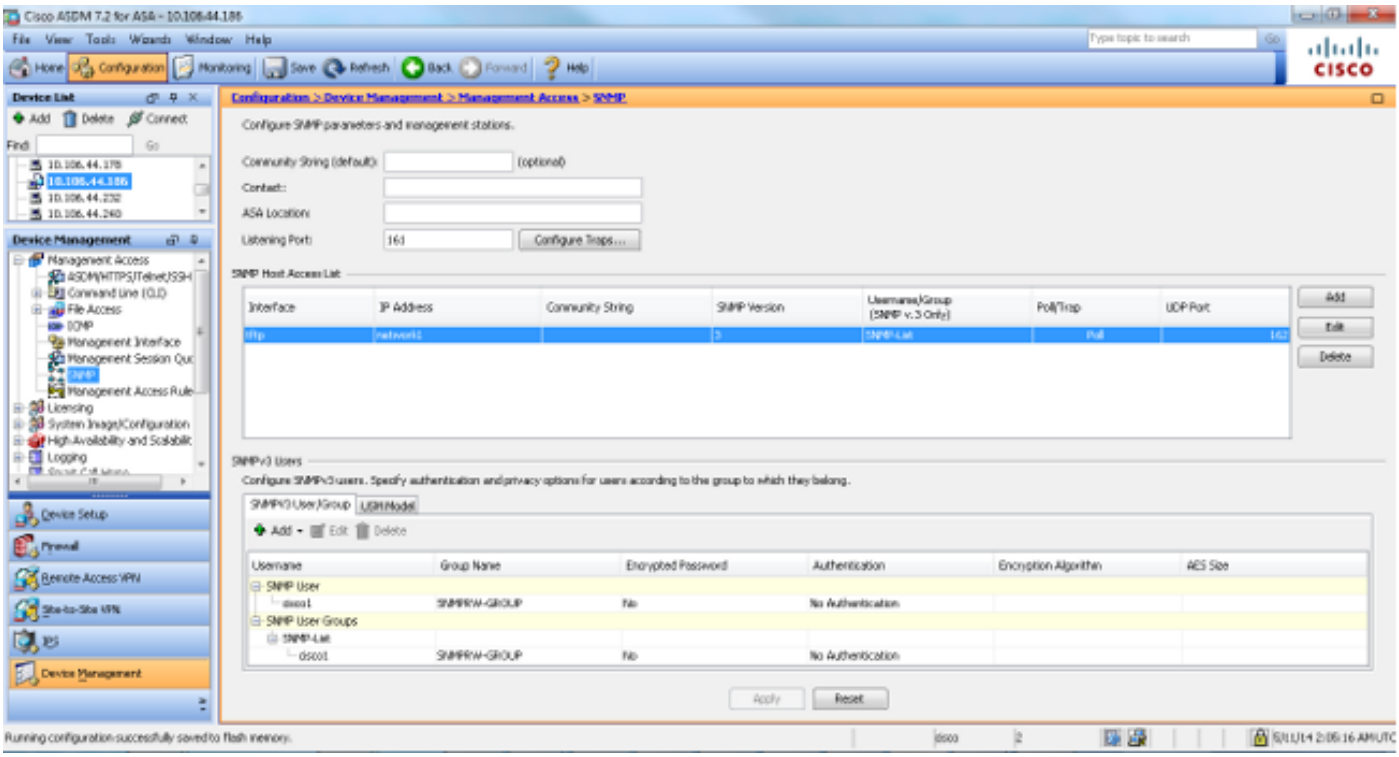
- o espaço livre configura a lista de usuários do servidor snmp
- o espaço livre configura o host-grupo do servidor snmp
- mostre a lista de usuários do servidor snmp da executar-configuração
- mostre o host-grupo do servidor snmp da executar-configuração

Exemplo de configuração

Termine estas etapas a fim usar as opções novas do grupo SNMP e criar um grupo do host do servidor SNMP para a votação da versão 2c:

1. Crie um objeto de rede:
   ```
   asa(config)# object network network1
   asa(config-network-object)# range 64.103.236.40 64.103.236.50
   ```
2. Defina o grupo do host SNMP:
   ```
   asa(config)#snmp-server host-group inside network1 poll community ***** version 2c
   ```
3. Defina o grupo do SNMP Versão 3:
   ```
   asa(config)#snmp-server group SNMPRW-GROUP v3 noauth
   ```
4. Amarre os grupos aos usuários:
   ```
   asa(config)#snmp-server user cisco1 SNMPRW-GROUP v3
   asa(config)#snmp-server user-list SNMP-List username cisco1
   asa(config)#snmp-server host-group inside network1 poll version 3 user-list SNMP-List
   ```

Esta imagem ilustra as mudanças que são feitas dentro do Cisco Adaptive Security Device Manager (ASDM):



Apoio para o cpmCPUTotal5minRev SNMP OID

Esta característica permite que o ASA apoie o **cpmCPUTotal5minRev** SNMP OID.

Propósito

Esta característica adiciona o apoio para o **cpmCPUTotal5minRev** e o **cpmCPUTotal1minRev** OID no ASA e suplica o **cpmCPUTotal5min** OID e o **cpmCPUTotal1min atual-**apoiados. A finalidade destes OID é monitorar o USO de CPU. Os OID atual-apoiados variam de 1 a 100, quando os OID novo-apoiados variarem de 0 a 100. Daqui, o apoio foi adicionado para uns OID mais novos, como cobrem uma escala mais larga.

Éimportante notar que desde que os OID suplicados (**cpmCPUTotal5min** e **cpmCPUTotal1min**) estão apoiados já não no ASA, se o ASA são promovidos e os OID suplicados estão votados, o ASA não retorna nenhuma informação para aqueles OID. Depois que uma elevação do ASA, você é exigida agora para monitorar o **cpmCPUTotal5minRev** e o **cpmCPUTotal1minRev** para o USO de CPU.

Comandos CLI

Não há nenhuma mudança CLI introduzida com estes novos recursos.

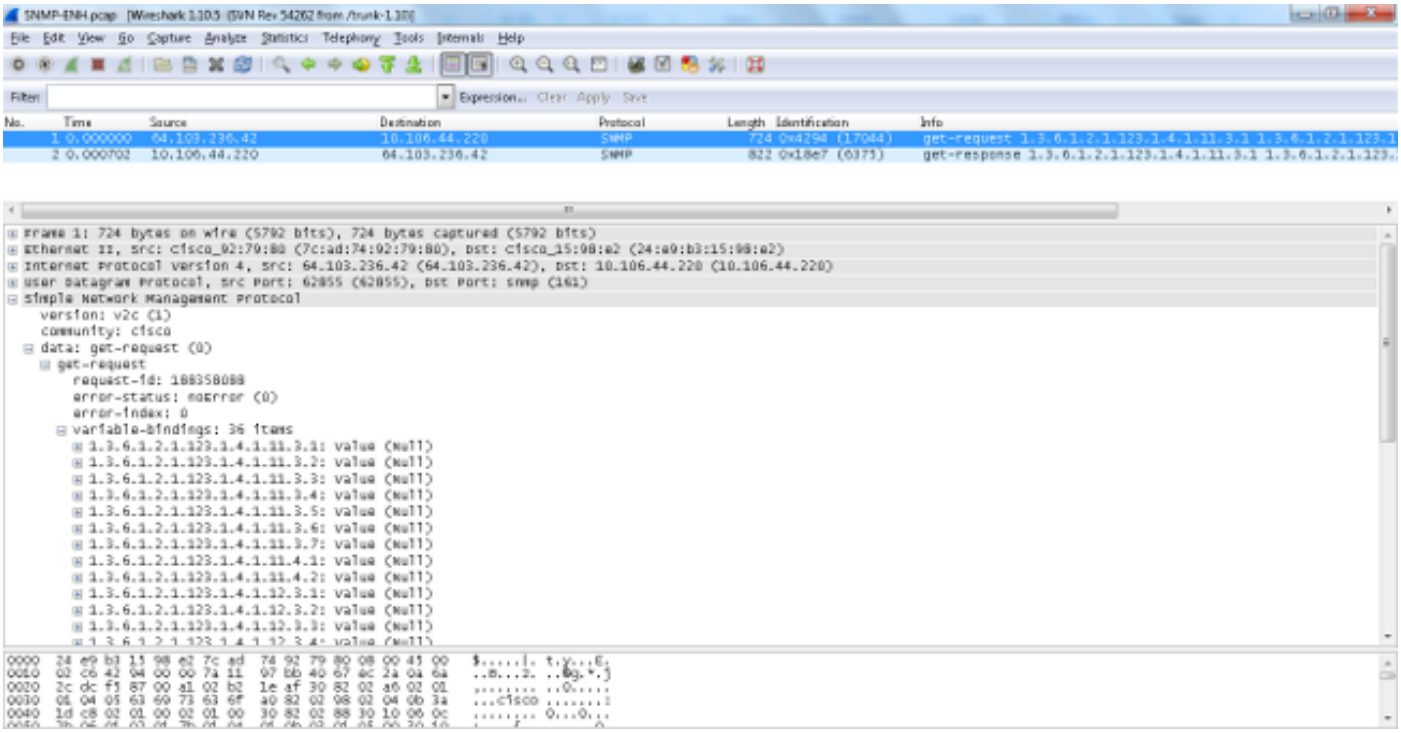
OID novos

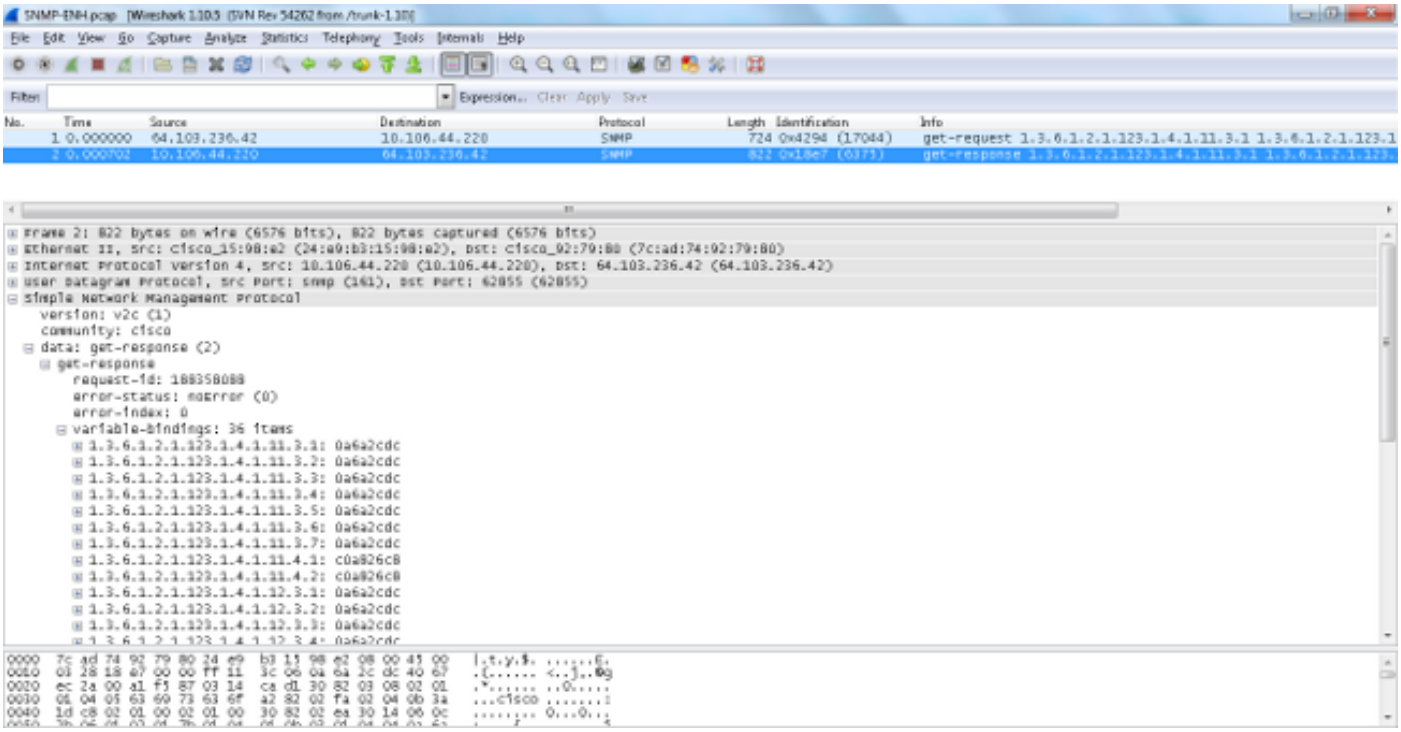
Estes são os OID novos que são adicionados com esta característica:

- 1.3.6.1.4.1.9.9.109.1.1.1.1.7. cpmCPUTotal1minRev
- 1.3.6.1.4.1.9.9.109.1.1.1.1.8. cpmCPUTotal5minRev

Apoio para os mensagens snmp 1,472-Byte

As Plataformas ASA limitam o tamanho máximo do pacote para pedidos SNMP a 512 bytes. Quando você executa uma pergunta maioria para um grande número MIB OID dentro de um único pedido SNMP, os intervalos de conexão SNMP e um Syslog do erro estão gerados no ASA. O RFC3417 sugere que o tamanho máximo do pacote para pedidos SNMP seja 1,472 bytes. Este é o tamanho do payload SNMP para o pacote. Adicionalmente, o cabeçalho de Ethernet e o tamanho do cabeçalho IP devem ser adicionados a fim computar o tamanho total do pacote.





Nota: O único-contexto e os modos de contexto múltiplo são apoiados com esta característica.

Troubleshooting

Esta seção fornece a informação que você pode usar a fim pesquisar defeitos edições do sistema no ASA.

Comandos show

Estes **comandos show** podem ser úteis quando as tentativas são feitas para pesquisar defeitos edições no ASA:

- **host-grupo do servidor snmp da corrida da mostra do** asa#
  host-grupo do servidor snmp dentro da SNMP-lista da lista de usuários da versão 3 da votação network1

- **lista de usuários do servidor snmp da corrida da mostra do** asa#
  username cisco1 da SNMP-lista da lista de usuários do servidor snmp

- **host do servidor snmp da mostra do** asa#

Este comando CLI indica as entradas que estam presente na tabela de endereço do servidor SNMP, que inclui o host e as configurações de grupo do host:

```
asa(config)#show run object network
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55
```

```
object network network3
range 64.103.236.60 64.103.236.70 ciscoasa/admin(config)# show run snmp-server
snmp-server group cisco-group v3 noauth
snmp-server user user1 cisco-group v3
snmp-server user user2 cisco-group v3
snmp-server user user3 cisco-group v3
snmp-server user-list cisco username user1
snmp-server user-list cisco username user2
snmp-server user-list cisco username user3
snmp-server host-group management0/0 net2 poll version 3 user-list cisco
no snmp-server locationno snmp-server contact ciscoasa/admin(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
```

Como mostrado, estes comandos show todos os anfitriões que são configurados através do comando do host-grupo. Você pode usar este comando a fim verificar se todas as entradas estão disponíveis e cruz-para verificar igualmente os grupos do host que sobrepõem.