Implementação de aprimoramento de recursos do ASA SNMP

Contents

Introduction

Este documento descreve os novos recursos do Simple Network Management Protocol (SNMP) disponíveis para o Cisco Adaptive Security Appliance (ASA) 5500-X Series Firewall no software versão 9.1.5 e versões 9.2.1 e posteriores.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco ASA 5500-X Series Firewall que executa o Cisco ASA® Software Release 9.1.5 e Versões 9.2.1(1) e posteriores.

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.

Informações de Apoio

Nas versões 9.1.5 e 9.2.1 do ASA, esses aprimoramentos do SNMP são apresentados:

- Éadicionado suporte para 128 hosts SNMP.
- O suporte para cpmCPUTotal5minRev SNMP Object Identifiers (OIDs) é adicionado.
- O suporte para mensagens SNMP de 1.472 bytes é adicionado.

Suporte para 128 hosts SNMP

Esse recurso permite que o ASA suporte mais do que os 32 hosts SNMP atuais.

Propósito

Atualmente, o ASA tem um limite rígido de 32 hosts SNMP no total. Isso inclui hosts que podem ser configurados para interceptações e para sondagem. As próximas seções descrevem os efeitos que esse recurso tem em modos de contexto único e multicontexto.

Modo de contexto único

- Permite que um número significativamente maior de entradas (total de hosts) seja configurado, mais de 4.096. Entretanto, dessas entradas, apenas 128 podem ser usados para armadilhas.
- Para fins de configuração de polling, até 4.096 hosts de polling e 128 hosts de trap podem ser configurados. No entanto, o número real de servidores que pesquisam o sistema deve ser restrito a menos de 128, pois o desempenho impacta de um número maior de hosts são desconhecidos e não são suportados.

Modo multicontexto

- Para fins de configuração, até 4.000 hosts por contexto são permitidos e um limite para todo o sistema de 64.000 hosts é imposto.
- Do total de hosts configurados, somente 128 (por contexto) podem ser usados para interceptações e o limite geral do sistema para interceptações no modo multicontexto é

32.000.

- Embora você possa configurar até 4.000 hosts por contexto, o número real de servidores que pesquisam qualquer contexto deve ser limitado a 128.

Descrição

Você pode preferir monitorar os dispositivos de rede de um grande pool de hosts SNMP. Idealmente, você deseja a capacidade de especificar um intervalo IP e/ou uma sub-rede dos endereços IP que têm permissão para monitorar os dispositivos de rede. O ASA atualmente não oferece essa flexibilidade e limita o máximo de hosts SNMP a 32.

O suporte para este recurso envolve dois aspectos:

- Forneça a capacidade do ASA para lidar com até 128 hosts SNMP.

- Forneça os comandos de configuração necessários para que você possa configurar um número significativamente maior de hosts, conforme detalhado na seção anterior por meio de um único comando.

O projeto atual no ASA é tal que os hosts individuais podem ser configurados via CLI. Para esse recurso, esses requisitos de projeto adicionais foram considerados:

- A introdução do comando CLI **snmp-server host-group** com retenção de comandos CLI **snmp-server host**.

- A capacidade das entradas virem dos comandos CLI **snmp-server host-group** e **snmp-server host**.

- Para SNMP Versão 3, a introdução do comando CLI **snmp-server userlist** com retenção de comandos CLI **snmp-server user**.

- Uma sobreposição de configuração também deve ser suportada. Por exemplo, os vários comandos **host-group** podem ser fornecidos com hosts que se sobrepõem nos objetos de rede. Da mesma forma, você pode especificar um host com um endereço IP que se sobreponha aos hosts atuais ou ao grupo de hosts. Isso fornece um mecanismo que pode ser usado para substituir os parâmetros de alguns hosts em um grupo, sem a necessidade de reconfigurar o grupo completo.

Algumas restrições de software e advertências associadas a este recurso são:

- Como parte do comando **snmp-server host-group**, o padrão é **poll** se **[trap|poll]** não for especificado. Também é importante observar que, para esse comando, as interceptações e a sondagem não podem ser ativadas para o mesmo grupo de hosts. Se isso for necessário, a Cisco recomenda que você use o comando **snmp-server host** para os hosts relevantes.

- Você pode especificar objetos de rede que se sobrepõem em diferentes comandos **host-group**. Os valores especificados no último grupo de hosts entram em vigor para o conjunto comum de hosts nos diferentes objetos de rede.

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
```

Insira o comando **show snmp-server host** para exibir as entradas do 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
```

Aqui estão algumas notas importantes sobre o uso deste recurso:

- Se um grupo de hosts ou host que se sobrepõe a outros grupos de hosts for excluído, os hosts serão configurados novamente com os valores usados para os grupos de hosts configurados.
- Os valores ou parâmetros associados aos hosts dependem da ordem em que os comandos são executados.
- A lista de usuários configurada não pode ser excluída se a lista for usada por um grupo de hosts específico.
- O usuário SNMP não pode ser excluído se o usuário for mencionado em uma lista de usuários específica.
- Um objeto de rede não pode ser excluído se for usado pelo comando CLI **host-group**.

Configurar

Use as informações descritas nesta seção para configurar o ASA de modo que esse novo recurso seja implementado.

Note: 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 a um grupo especificado de hosts. Isso é útil se o administrador desejar que um conjunto de usuários tenha a capacidade de acessar o ASA de um grupo de hosts. Este comando CLI é usado para configurar uma lista de usuários para vários usuários:

```
ASA(config)# [no] snmp-server user-list
```

Para associar a lista de usuários a um grupo de hosts, insira este comando na CLI:

```
[no] snmp-server host-group
```

Com esse único comando, você pode especificar um objeto de rede para indicar os vários hosts que devem ser adicionados. Com o objeto de rede, você pode especificar uma máscara de sub-rede ou o intervalo de endereços IP que devem ser adicionados, com o uso de um único comando. Todos os endereços IP listados como parte do objeto de rede são adicionados como entradas de host SNMP. Da mesma forma, para cada um dos usuários especificados na lista de usuários, há uma entrada de host SNMP separada.

Esses comandos são usados para permitir que os administradores limpem e visualizem as novas opções de configuração para os servidores SNMP:

- clear configure snmp-server user-list
- clear configure snmp-server host-group
- show running-config snmp-server user-list
- show running-config snmp-server host-group

Exemplo de configuração

Conclua estes passos para usar as novas opções de grupo SNMP e criar um grupo de hosts de servidor SNMP para polling da Versão 2c:

1. Criar 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 de hosts SNMP:

```
asa(config)#snmp-server host-group inside network1 poll community ***** version 2c
```

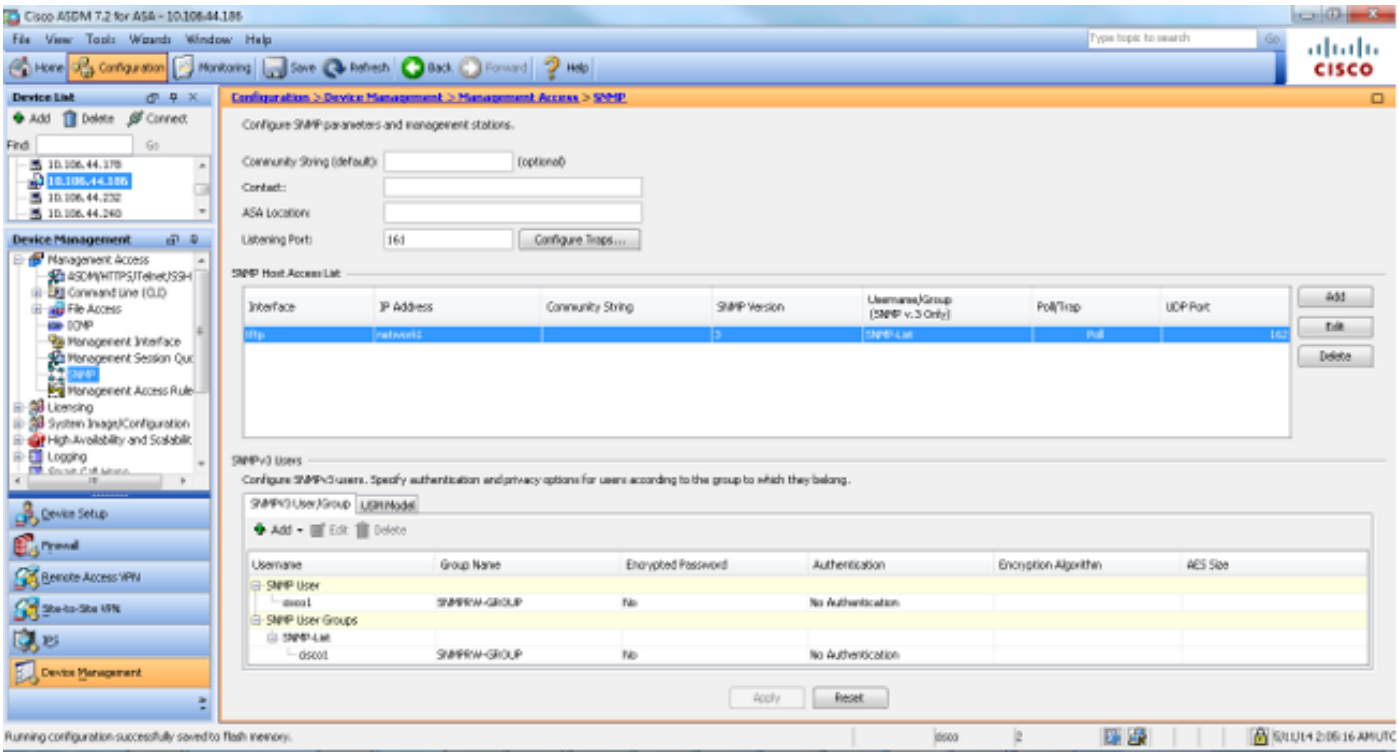
3. Defina o grupo SNMP Versão 3:

```
asa(config)#snmp-server group SNMPRW-GROUP v3 noauth
```

4. Vincule 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 alterações feitas no Cisco Adaptive Security Device Manager (ASDM):



Suporte para OIDs SNMP cpmCPUTotal5minRev

Este recurso permite que o ASA suporte **cpmCPUTotal5minRev** SNMP OIDs.

Propósito

Este recurso adiciona suporte para **cpmCPUTotal5minRev** e **cpmCPUTotal1minRev** OIDs no ASA e pretere os OIDs **cpmCPUTotal5min** e **cpmCPUTotal1min**. A finalidade desses OIDs é monitorar o uso da CPU. Os OIDs suportados no momento variam de 1 a 100, enquanto os OIDs suportados recentemente variam de 0 a 100. Assim, foi adicionado suporte para OIDs mais recentes, pois eles cobrem uma faixa maior.

Éimportante observar que como os OIDs preteridos (**cpmCPUTotal5min** e **cpmCPUTotal1min**) não são mais suportados no ASA, se o ASA for atualizado e os OIDs preteridos forem consultados, o ASA não retornará nenhuma informação para esses OIDs. Depois de uma atualização do ASA, você agora precisa monitorar o **cpmCPUTotal5minRev** e o **cpmCPUTotal1minRev** para o uso da CPU.

Comandos CLI

Não há alterações de CLI introduzidas com este novo recurso.

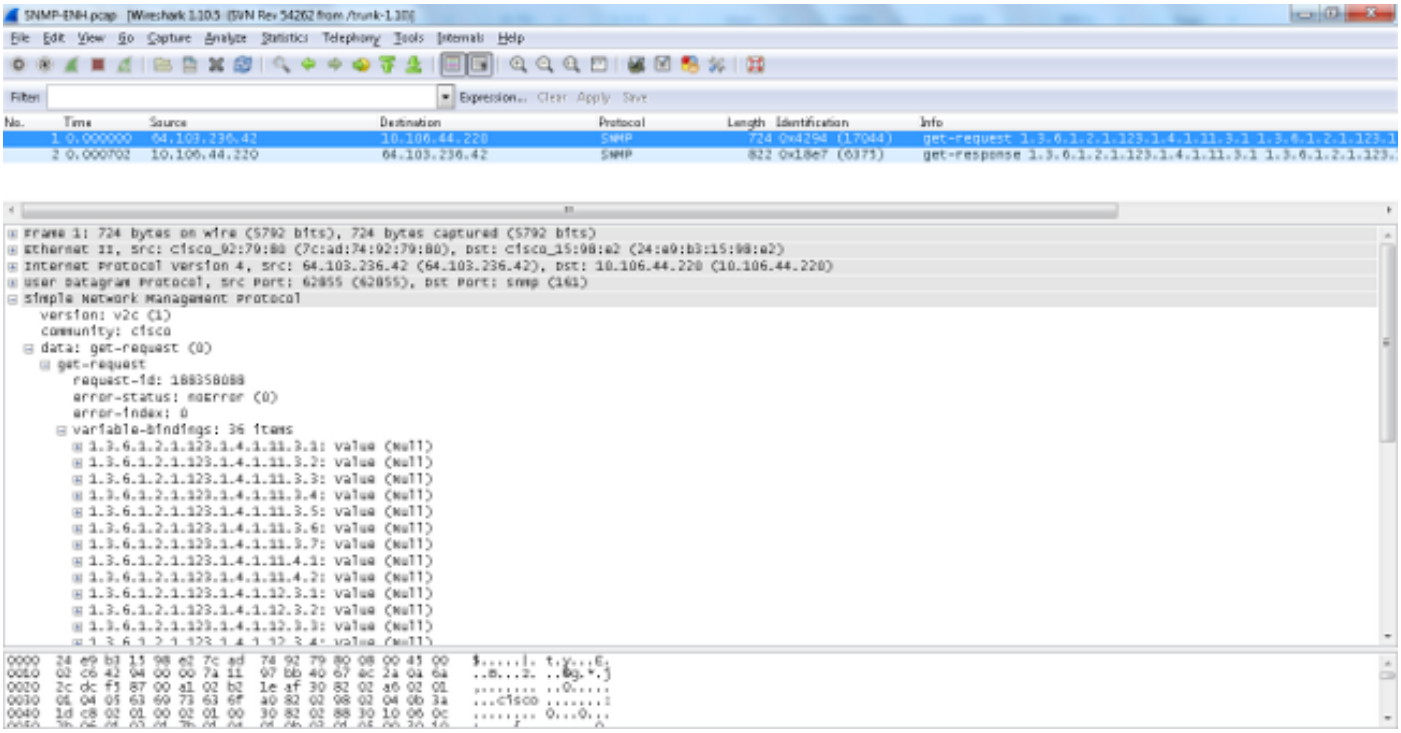
Novos OIDs

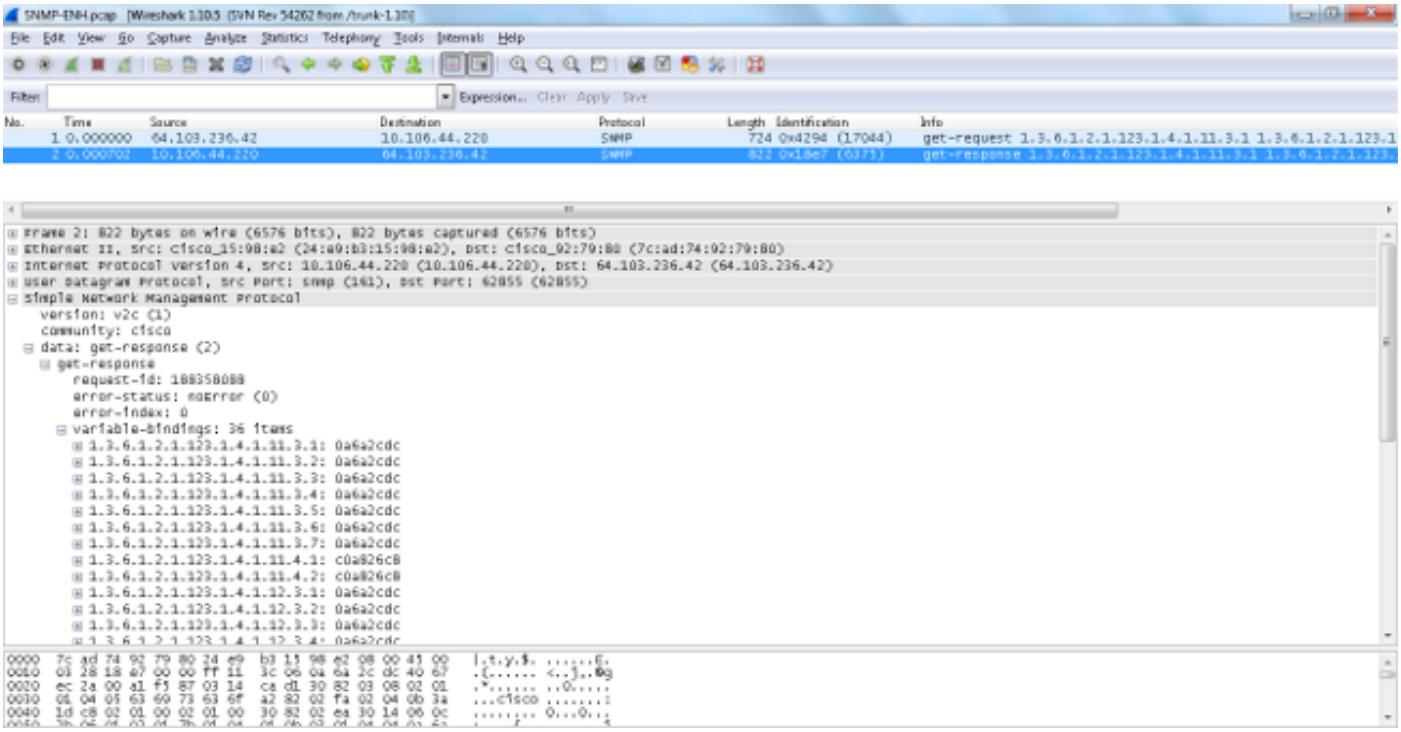
Estes são os novos OIDs adicionados com este recurso:

- 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

Suporte para mensagens SNMP de 1.472 bytes

As plataformas ASA limitam o tamanho máximo de pacote para solicitações SNMP a 512 bytes. Quando você executa uma consulta em massa para um grande número de OIDs MIB em uma única solicitação SNMP, o tempo limite da conexão SNMP e um syslog de erro são gerados no ASA. O RFC3417 sugere que o tamanho máximo do pacote para solicitações SNMP deve ser de 1.472 bytes. Esse é o tamanho do payload SNMP para o pacote. Além disso, o cabeçalho Ethernet e o tamanho do cabeçalho IP devem ser adicionados para calcular o tamanho total do pacote.





Note: Os modos de contexto único e de contexto múltiplo são suportados com este recurso.

Troubleshoot

Esta seção fornece informações que você pode usar para solucionar problemas do sistema no ASA.

comandos show

Esses comandos **show** podem ser úteis quando são feitas tentativas para solucionar problemas no ASA:

- asa# **show run snmp-server host-group**
  snmp-server host-group inside network1 poll versão 3 user-list SNMP-List

- asa# **show run snmp-server user-list**
  snmp-server user-list SNMP-List username cisco1

- asa# **show snmp-server host**

Este comando CLI exibe as entradas presentes na tabela de endereços do servidor SNMP, que inclui as configurações do host e do grupo de hosts:

```
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, esses comandos mostram todos os hosts configurados por meio do comando **host-group**. Você pode usar esse comando para verificar se todas as entradas estão disponíveis e também verificar os grupos de hosts que se sobrepõem.