Implementazione del miglioramento delle funzionalità SNMP dell'ASA

Sommario

Introduzione

Questo documento descrive le nuove funzionalità del protocollo SNMP (Simple Network Management Protocol) disponibili per i firewall Cisco Adaptive Security Appliance (ASA) serie 5500-X nel software versione 9.1.5 e 9.2.2(1) e successive.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, è stato usato un firewall Cisco ASA serie 5500-X con software Cisco ASA® versione 9.1.5 e 9.2.2(1) e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Nelle versioni ASA 9.1.5 e 9.2.1, sono stati introdotti i seguenti miglioramenti del protocollo SNMP:

- Èstato aggiunto il supporto per 128 host SNMP.
- Viene aggiunto il supporto per gli OID (Object Identifier) SNMP cpmCPUTotal5minRev.
- Èstato aggiunto il supporto per i messaggi SNMP da 1.472 byte.

Supporto per 128 host SNMP

Questa funzione consente all'ASA di supportare più host SNMP degli attuali 32.

Scopo

Al momento, l'ASA ha un limite non superabile di 32 host SNMP in totale. Ciò include gli host che possono essere configurati per i trap e il polling. Nelle sezioni seguenti vengono descritti gli effetti di questa funzione sulle modalità contesto singolo e contesto multiplo.

Modalità contesto singolo

- Consente di configurare un numero significativamente più elevato di voci (host totali), fino a 4.096. Tuttavia, solo 128 di queste voci possono essere utilizzate per le trap.
- Per la configurazione del polling, è possibile configurare fino a 4.096 host di polling e 128 host trap. Tuttavia, il numero effettivo di server che eseguono il polling del sistema deve essere limitato a meno di 128, in quanto l'impatto sulle prestazioni di un numero maggiore di host è sconosciuto e non supportato.

Modalità contesto multiplo

- Ai fini della configurazione, sono consentiti fino a 4.000 host per contesto e viene imposto un limite a livello di sistema di 64.000 host totali.
- Sul totale di host configurati, solo 128 (per contesto) possono essere utilizzati per le trap e il limite di sistema complessivo per le trap in modalità multi-contesto è 32.000.

- Sebbene sia possibile configurare fino a 4.000 host totali per contesto, il numero effettivo di server che eseguono il polling di un contesto deve essere limitato a 128.

Descrizione

Si potrebbe preferire monitorare i dispositivi di rete da un pool di host SNMP di grandi dimensioni. In teoria, è possibile specificare un intervallo IP e/o una subnet di indirizzi IP autorizzati a monitorare i dispositivi di rete. Al momento, l'ASA non offre questa flessibilità e limita a 32 gli host SNMP massimi.

Il supporto per questa funzione comporta due aspetti:

- Fornire all'ASA la capacità di gestire fino a 128 host SNMP.

- Fornire i comandi di configurazione richiesti in modo da poter configurare un numero di host significativamente superiore, come descritto nella sezione precedente, con un unico comando.

Il progetto corrente sull'appliance ASA è tale che i singoli host possono essere configurati tramite la CLI. Per questa funzione sono stati presi in considerazione i seguenti requisiti di progettazione aggiuntivi:

- L'introduzione del comando **snmp-server host-group** CLI con **snmp-server host** CLI command retention.

- La possibilità che le voci provengano sia dal **gruppo host-server snmp** che dai comandi CLI dell'**host-server snmp**.

- Per il protocollo SNMP versione 3, l'introduzione del comando **snmp-server userlist** CLI con il comando **snmp-server user** CLI.

- Deve essere supportata anche una sovrapposizione di configurazione. Ad esempio, i comandi **host-group** multipli possono essere forniti con gli host che si sovrappongono negli oggetti di rete. Analogamente, è possibile specificare un host con un indirizzo IP che si sovrapponga agli host correnti o al gruppo host. Questo fornisce un meccanismo che può essere usato per sovrascrivere i parametri per alcuni host in un gruppo, senza la necessità di riconfigurare l'intero gruppo.

Di seguito sono riportate alcune limitazioni e avvertenze relative al software:

- Come parte del comando **snmp-server host-group**, il valore predefinito è **poll** se non è specificato **[trap|poll]**. È inoltre importante notare che per questo comando non è possibile abilitare le trap e il polling per lo stesso gruppo host. Se necessario, Cisco consiglia di utilizzare il comando **snmp-server host** per gli host interessati.

- Èpossibile specificare oggetti di rete che si sovrappongono in diversi comandi **del gruppo host**. I valori specificati nell'ultimo gruppo host vengono applicati al set comune di host nei diversi oggetti di rete.

Di seguito è riportato un esempio:

```
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
```

Immettere il comando **show snmp-server host** per visualizzare le voci dell'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
```

Di seguito sono riportate alcune note importanti sull'utilizzo di questa funzione:

- Se si elimina un gruppo host o un host che si sovrappone ad altri gruppi host, gli host vengono impostati nuovamente con i valori utilizzati per i gruppi host configurati.
- I valori o i parametri associati agli host dipendono dall'ordine di esecuzione dei comandi.
- L'elenco utenti configurato non può essere eliminato se è utilizzato da un particolare gruppo host.
- Non è possibile eliminare l'utente SNMP se vi si fa riferimento in un particolare elenco di utenti.
- Non è possibile eliminare un oggetto di rete se viene utilizzato dal comando CLI **host-group**.

Configurazione

Per configurare l'ASA in modo che questa nuova funzionalità sia implementata, usare le informazioni descritte in questa sezione.

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Comandi CLI

Per il protocollo SNMP versione 3, l'amministratore può associare vari utenti a un gruppo specifico di host. Ad esempio, se l'amministratore desidera che un gruppo di utenti abbia la possibilità di accedere all'ASA da un gruppo di host. Questo comando CLI è usato per configurare un elenco di utenti per più utenti:

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

Per associare l'elenco degli utenti a un gruppo host, immettere questo comando nella CLI:

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

Con questo unico comando, è possibile specificare un oggetto di rete per indicare gli host multipli da aggiungere. Con l'oggetto di rete è possibile specificare una subnet mask o l'intervallo di indirizzi IP da aggiungere, utilizzando un unico comando. Tutti gli indirizzi IP elencati come parte dell'oggetto di rete vengono aggiunti come voci host SNMP. Analogamente, per ciascuno degli utenti specificati nell'elenco degli utenti, è presente una voce host SNMP separata.

Questi comandi vengono utilizzati per consentire agli amministratori di cancellare e visualizzare le nuove opzioni di configurazione per i server SNMP:

- deselezionare configure snmp-server user-list
- clear configure snmp-server host-group
- show running-config snmp-server elenco-utenti
- show running-config snmp-server gruppo-host

Esempio di configurazione

Completare questi passaggi per utilizzare le nuove opzioni del gruppo SNMP e creare un gruppo host server SNMP per il polling della versione 2c:

1. Creare un oggetto di rete:

   ```
   asa(config)# object network network1
   asa(config-network-object)# range 64.103.236.40 64.103.236.50
   ```
2. Definire il gruppo host SNMP:

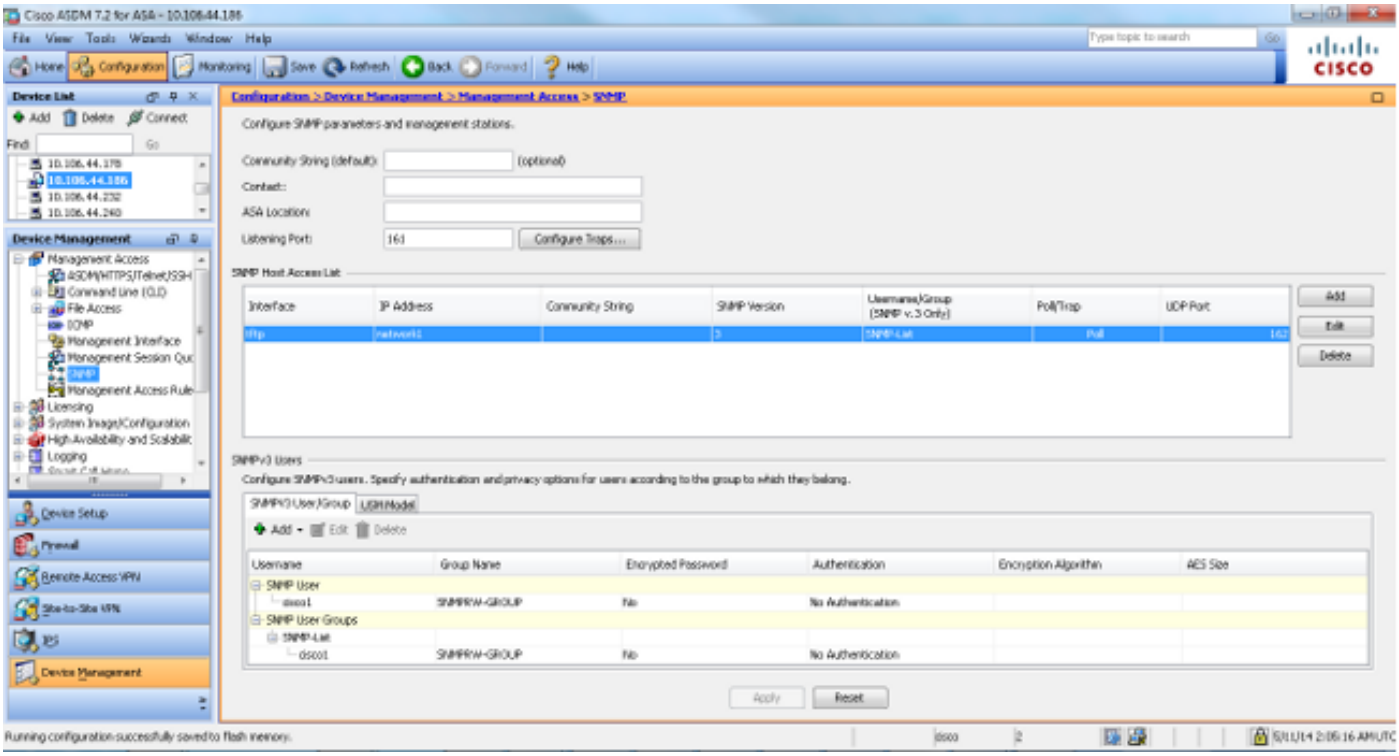
   ```
   asa(config)#snmp-server host-group inside network1 poll community ***** version 2c
   ```
3. Definire il gruppo SNMP versione 3:

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

4. Collegare i gruppi agli utenti:

```
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
```

L'immagine mostra le modifiche apportate in Cisco Adaptive Security Device Manager (ASDM):



Supporto per OID SNMP cpmCPUTotal5minRev

Questa funzione consente all'ASA di supportare gli OID SNMP **cpmCPUTotal5minRev**.

Scopo

Questa funzione aggiunge il supporto per gli OID **cpmCPUTotal5minRev** e **cpmCPUTotal1minRev** sull'appliance ASA e depreca gli OID attualmente supportati **cpmCPUTotal5min** e **cpmCPUTotal1min**. Lo scopo di questi OID è monitorare l'utilizzo della CPU. Gli OID attualmente supportati vanno da 1 a 100, mentre quelli appena supportati vanno da 0 a 100. Pertanto, è stato aggiunto il supporto per gli OID più recenti, poiché coprono un intervallo più ampio.

Èimportante notare che, poiché gli OID deprecati (**cpmCPUTotal5min** e **cpmCPUTotal1min**) non sono più supportati sull'appliance ASA, se questa viene aggiornata e viene eseguito il polling degli OID deprecati, l'appliance ASA non restituisce alcuna informazione per tali OID. Dopo un aggiornamento dell'ASA, è necessario monitorare **cpmCPUTotal5minRev** e **cpmCPUTotal1minRev** per l'utilizzo della CPU.

Comandi CLI

Non sono state introdotte modifiche CLI con questa nuova funzionalità.

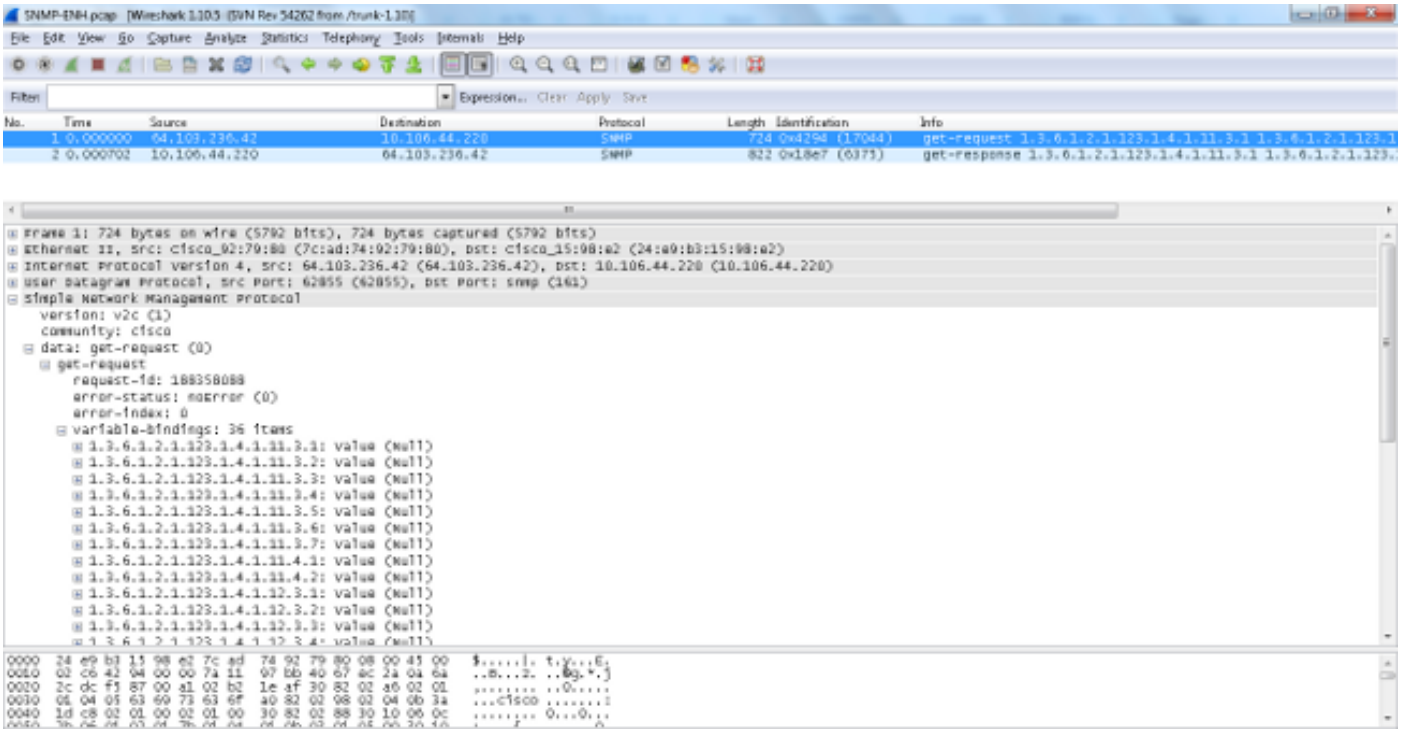
Nuovi OID

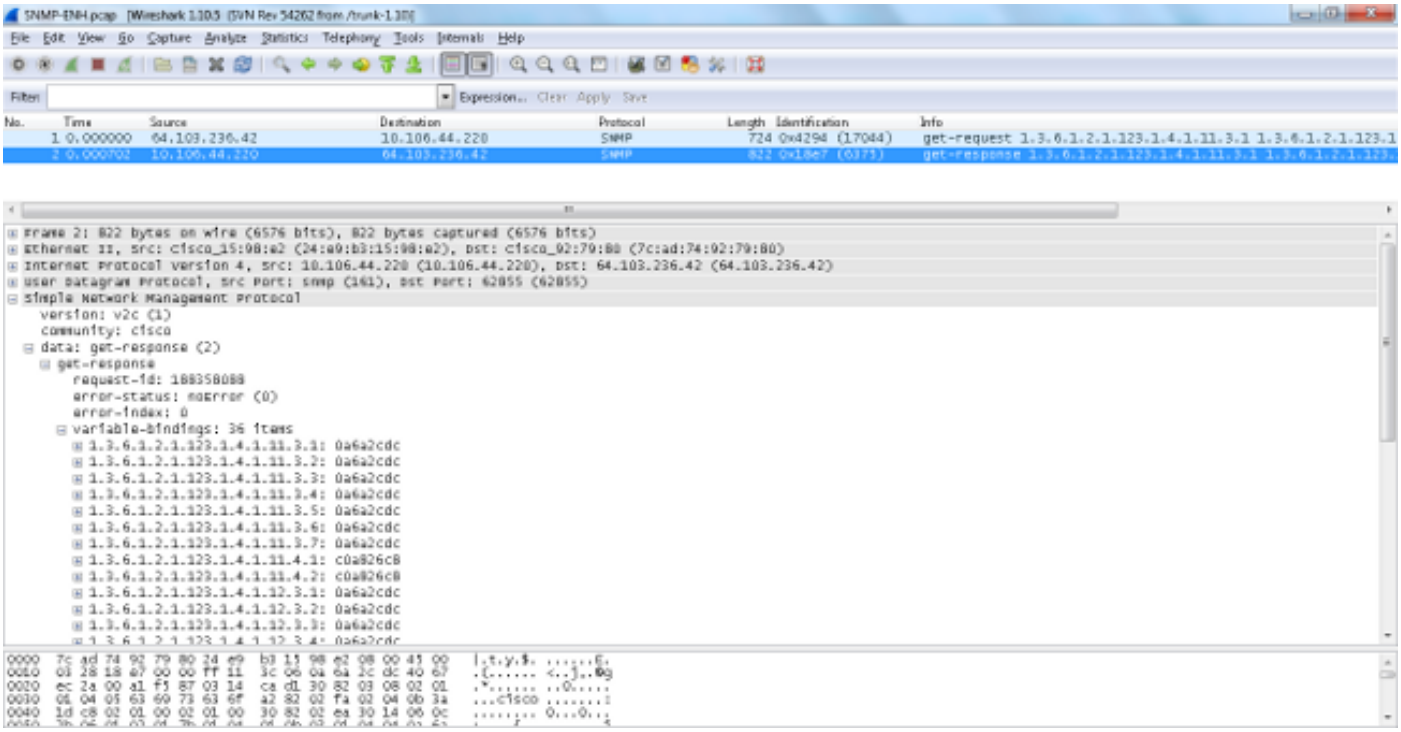
Questi sono i nuovi OID aggiunti con questa funzione:

- **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**

Supporto per messaggi SNMP da 1.472 byte

Le piattaforme ASA limitano a 512 byte le dimensioni massime del pacchetto per le richieste SNMP. Quando si esegue una query in blocco per un numero elevato di OID MIB in una singola richiesta SNMP, il timeout della connessione SNMP e il syslog di errore vengono generati sull'appliance ASA. La RFC 3417 suggerisce che le dimensioni massime del pacchetto per le richieste SNMP debbano essere di 1.472 byte. Queste sono le dimensioni del payload SNMP del pacchetto. Inoltre, è necessario aggiungere l'intestazione Ethernet e le dimensioni dell'intestazione IP per calcolare le dimensioni totali del pacchetto.





Nota: Questa funzionalità supporta sia la modalità a contesto singolo che la modalità a contesto multiplo.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi al sistema sull'appliance ASA.

Comandi show

I seguenti comandi **show** possono essere utili quando si cerca di risolvere problemi sull'appliance ASA:

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

- asa# **show run snmp-server user-list**
  snmp-server elenco utenti SNMP-List nome utente cisco1

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

Questo comando CLI visualizza le voci presenti nella tabella degli indirizzi del server SNMP, che include sia la configurazione dell'host che quella del gruppo 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
```

Come mostrato, questi comandi mostrano tutti gli host configurati tramite il comando **host-group**. È possibile utilizzare questo comando per verificare se tutte le voci sono disponibili e per eseguire la verifica incrociata dei gruppi host che si sovrappongono.