Monitoraggio di Cisco ESA con SNMP

Introduzione

In questo documento viene descritto come monitorare Cisco Secure Email Gateway tramite SNMP, tra cui la struttura MIB, l'utilizzo di OID e query pratiche.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base del protocollo SNMP
- Accesso all'appliance Cisco ESA
- Familiarità con la riga di comando di Linux
- Cisco ESA con servizio SNMP abilitato
- Client SNMP installato (ad esempio, strumenti Net-SNMP)
- File MIB IronPort disponibili e caricati
- Stringa della community o credenziali SNMP v3

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Email Gateway (ESA)
- Client Linux con strumenti Net-SNMP
- File MIB: IRONPORT-SMI.txt, ASYNCOS-MAIL-MIB.txt

Configurazione di SNMP

La configurazione SNMP su ESA viene eseguita tramite CLI. Per abilitare il protocollo SNMP su Cisco ESA, accedere alla CLI ed eseguire snmpconfig.

L'impostazione predefinita prevede:

- Abilitazione del servizio SNMP
- Scelta dell'interfaccia e della porta di gestione (generalmente 161)
- Abilitazione di SNMPv3 (protezione predefinita: authPriv con SHA e AES)
- Impostazione delle passphrase di autenticazione e privacy
- Abilitazione di SNMPv1/v2c, specificando la stringa della community (ad esempio, ironport)
- Definizione delle reti IPv4 consentite per le richieste SNMP
- Configurazione della versione trap SNMP e dell'indirizzo IP della destinazione trap
- Impostazione del percorso di sistema e delle informazioni di contatto

Dopo aver abilitato il protocollo SNMP, è possibile visualizzare un riepilogo simile al seguente:

```
esa1.ironport.com> snmpconfig

Current SNMP settings:
Listening on interface "Management"



      port 161.
SNMP v3: Enabled. Security level: authPriv
Authentication Protocol: SHA
Encryption Protocol: AES
SNMP v1/v2: Enabled, accepting requests from subnet



      , .
SNMP v1/v2 Community String: ironport
Trap version: V3
Trap target:



Location: esxi data center
System Contact: ciscoros soc
```

Dopo aver abilitato e configurato il protocollo SNMP, l'accessorio è pronto ad accettare query SNMP da indirizzi IP di origine consentiti.

SNMP Client Setup and Querying su Linux

Per questo esempio è stato utilizzato un server Debian. Si noti che i passaggi di installazione possono variare a seconda del gestore dei pacchetti di distribuzione.

Installare gli strumenti SNMP

```
sudo apt-get install snmp snmp-mibs-downloader
```

Verificare che il file binario di snmpwalk sia installato.

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk --version
NET-SNMP version: 5.9
```

Carica file MIB

Posizionare i file MIB IronPort nella cartella /usr/share/snmp/mibs.

```
root@debian-server:/usr/share/snmp/mibs# pwd
/usr/share/snmp/mibs
root@debian-server:/usr/share/snmp/mibs# ls
ASYNCOS-MAIL-MIB.txt  IRONPORT-SMI.txt        NET-SNMP-EXAMPLES-MIB.txt  NET-SNMP-PASS-MIB.txt  UCD-DEMO-MIB.txt    UCD-IPFWACC-MIB.txt
iana                  LM-SENSORS-MIB.txt      NET-SNMP-EXTEND-MIB.txt    NET-SNMP-TC.txt        UCD-DISKIO-MIB.txt  UCD-SNMP-MIB.txt
ietf                  NET-SNMP-AGENT-MIB.txt  NET-SNMP-MIB.txt           NET-SNMP-VACM-MIB.txt  UCD-DLMOD-MIB.txt
```

oid debian-server

Nota: I file MIB sono contenuti nell'articolo del protocollo SNMP condiviso alla fine di questo documento.

Utilizzo di un OID per monitorare l'utilizzo della CPU

Questo comando esegue una query sull'ESA per verificare l'utilizzo corrente della CPU. L'OID punta direttamente alla metrica CPU definita nel MIB. Nell'output viene visualizzato un valore, ad esempio INTEGER: 37, che indica l'utilizzo della CPU del dispositivo al 37%. In questo modo gli amministratori possono monitorare le prestazioni dei dispositivi in tempo reale e intervenire se l'utilizzo supera i limiti accettabili.

```
snmpwalk -v2c -c ironport
```

```
.1.3.6.1.4.1.15497.1.1.1.2
```

L'utilizzo degli OID nei comandi SNMP consente di accedere direttamente a metriche specifiche per un monitoraggio e una risoluzione dei problemi efficaci.

Abilita nomi simbolici

```
export MIBS=ALL
```

L'impostazione di export MIBS=ALL consente agli strumenti SNMP di utilizzare i nomi leggibili definiti nei file MIB anziché gli OID numerici lunghi. Ciò semplifica la scrittura, la comprensione e la risoluzione dei problemi delle query, poiché è possibile fare riferimento agli oggetti con nomi significativi, ad esempio workQueueMessages, anziché con sequenze di numeri.

Esegui query SNMP

Utilizzare snmpwalk per eseguire query su ESA per le metriche chiave. Le query SNMP consentono di recuperare in tempo reale i dati relativi allo stato e alle prestazioni dall'ESA Cisco. Utilizzando nomi simbolici, è possibile monitorare facilmente oggetti specifici quali lo stato della coda, la scadenza della licenza e l'utilizzo dell'hardware senza dover fare riferimento a OID numerici complessi.

Messaggi coda di lavoro

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk -v2c -c ironport
```

```
      workQueueMessages
ASYNCOS-MAIL-MIB::workQueueMessages.0 = Gauge32: 0
```

Questo output mostra che attualmente non sono presenti messaggi nella coda di lavoro ESA. Il valore rappresenta il numero in tempo reale di messaggi di posta elettronica in attesa di elaborazione.

Utilizzo CPU

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk -v2c -c ironport
```

Ciò indica che la CPU dell'ESA è attualmente al 37% di utilizzo. Il valore consente di conoscere il carico di elaborazione dell'accessorio al momento dell'esecuzione della query.

Tabella Scadenza chiave di licenza

```
diegoher@debian-server:/usr/share/snmp/mibs$ snmpwalk -v2c -c ironport
```

```
       keyExpirationTable
ASYNCOS-MAIL-MIB::keyExpirationIndex.1 = INTEGER: 1
ASYNCOS-MAIL-MIB::keyExpirationIndex.2 = INTEGER: 2
ASYNCOS-MAIL-MIB::keyExpirationIndex.3 = INTEGER: 3
ASYNCOS-MAIL-MIB::keyExpirationIndex.4 = INTEGER: 4
ASYNCOS-MAIL-MIB::keyExpirationIndex.5 = INTEGER: 5
ASYNCOS-MAIL-MIB::keyExpirationIndex.6 = INTEGER: 6
ASYNCOS-MAIL-MIB::keyExpirationIndex.7 = INTEGER: 7
ASYNCOS-MAIL-MIB::keyExpirationIndex.8 = INTEGER: 8
ASYNCOS-MAIL-MIB::keyDescription.1 = STRING: Bounce Verification
ASYNCOS-MAIL-MIB::keyDescription.2 = STRING: Data Loss Prevention
ASYNCOS-MAIL-MIB::keyDescription.3 = STRING: External Threat Feeds
ASYNCOS-MAIL-MIB::keyDescription.4 = STRING: Incoming Mail Handling
ASYNCOS-MAIL-MIB::keyDescription.5 = STRING: IronPort Anti-Spam
ASYNCOS-MAIL-MIB::keyDescription.6 = STRING: IronPort Email Encryption
ASYNCOS-MAIL-MIB::keyDescription.7 = STRING: Outbreak Filters
ASYNCOS-MAIL-MIB::keyDescription.8 = STRING: Sophos Anti-Virus
ASYNCOS-MAIL-MIB::keyIsPerpetual.1 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.2 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.3 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.4 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.5 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.6 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.7 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keyIsPerpetual.8 = INTEGER: true(1)
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.1 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.2 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.3 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.4 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.5 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.6 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.7 = Gauge32: 0
ASYNCOS-MAIL-MIB::keySecondsUntilExpire.8 = Gauge32: 0
```

- keyExpirationIndex.X: Ogni indice rappresenta una chiave di funzionalità univoca

installata sull'ESA Cisco.

- keyDescription.X: Fornisce il nome o la descrizione di ciascuna chiave di funzionalità, ad esempio 'Verifica rimbalzo', 'Prevenzione della perdita di dati', 'IronPort Anti-Spam' e 'Sophos Anti-Virus'.
- keyIsPerpetual.X: Indica se la licenza per ciascuna funzionalità è perpetua. Il valore true (1) indica che la licenza non scade.
- KeySecondsUntilExpire.X: Mostra il numero di secondi rimanenti prima della scadenza della licenza. Il valore 0 conferma che la licenza è perpetua o è già scaduta.

```
[]> summary

Feature Name                                                    License Authorization Status
-------------------------------------------------------------------------------------------
Email Security Appliance Anti-Spam License                        In Compliance
Email Security Appliance Outbreak Filters                         In Compliance
Email Security Appliance Graymail Safe-unsubscribe                Not requested
Email Security Appliance External Threat Feeds                    In Compliance
Email Security Appliance Advanced Malware Protection Reputation   Not requested
Mail Handling                                                     In Compliance
Email Security Appliance Sophos Anti-Malware                      In Compliance
Email Security Appliance PXE Encryption                           In Compliance
Email Security Appliance Advanced Malware Protection              Not requested
Email Security Appliance McAfee Anti-Malware                      Not requested
Email Security Appliance Intelligent Multi-Scan                   Not requested
Email Security Appliance Image Analyzer                           Not requested
Email Security Appliance Bounce Verification                      In Compliance
Email Security Appliance Data Loss Prevention                     In Compliance
```

esempio licenza

In questo output vengono confermate le chiavi di funzionalità correnti dell'accessorio, le descrizioni e lo stato della licenza. Tutte le licenze elencate sono perpetue, come indicato da keyIsPerpetual e keySecondsUntilExpire. Queste informazioni garantiscono che le funzionalità di sicurezza essenziali rimangano attive e valide sull'ESA Cisco.

Differenza tra OID numerici e nomi simbolici

OID numerici:

- Sono universali e funzionano sempre, anche se i file MIB non sono caricati sul sistema.
- Esempio: 1.1.3.6.1.4.1.15497.1.1.1.2.
- Sono meno leggibili e possono essere difficili da ricordare.

Nomi simbolici:

- Si tratta di nomi descrittivi definiti nei file MIB, ad esempio perCentCPUUtilization.
- Rendono i comandi più facili da scrivere e comprendere.
- Richiedono il caricamento corretto dei file MIB e la configurazione della variabile di ambiente MIBS.
- Esempio: snmpwalk -v2c -c porta-ferro 10.31.124.165 perCentCPUUtilizzazione.

È lo stesso?

Entrambi i metodi eseguono query sulla stessa metrica e producono risultati identici, ma i nomi simbolici sono più pratici e leggibili, mentre gli OID numerici sono più affidabili negli ambienti in cui i file MIB non possono essere presenti o caricati.

Informazioni correlate

- Monitoraggio dello stato e del funzionamento del sistema tramite SNMP
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).