Cisco ESA monitoren met SNMP

Inleiding

In dit document wordt beschreven hoe u Cisco Secure Email Gateway kunt controleren met behulp van SNMP, inclusief MIB-structuur, OID-gebruik en praktische vragen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis SNMP-protocol
- Toegang tot Cisco ESA-apparaat
- Bekendheid met Linux-opdrachtregel
- Cisco ESA met SNMP-service ingeschakeld
- SNMP-client geïnstalleerd (zoals Net-SNMP-tools)
- IronPort MIB-bestanden beschikbaar en geladen
- Community-tekenreeks of SNMP v3-referenties

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Email Gateway (ESA)
- Linux-client met Net-SNMP-tools
- MIB-bestanden: IRONPORT-SMI.txt, ASYNCOS-MAIL-MIB.txt

SNMP configureren

De SNMP-configuratie op ESA gebeurt via CLI. Als u SNMP wilt inschakelen voor Cisco ESA, opent u de CLI en voert u snmpconfig uit.

De standaardinstelling omvat:

- SNMP-service inschakelen
- De beheerinterface en -poort kiezen (meestal 161)
- SNMPv3 inschakelen (standaardbeveiliging: authPriv met SHA en AES)
- Authenticatie- en privacywachtwoordgroepen instellen
- SNMPv1/v2c inschakelen, de communitystring opgeven (bijvoorbeeld ironport)
- Toegestane IPv4-netwerken definiëren voor SNMP-verzoeken
- SNMP-trapversie en doel-IP-adres overvullen configureren
- Systeemlocatie en contactgegevens instellen

Nadat u SNMP hebt ingeschakeld, ziet u een samenvatting die hierop lijkt:

```
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
```

Zodra SNMP is ingeschakeld en geconfigureerd, is het toestel klaar om SNMP-query's van toegestane bron-IP's te accepteren.

SNMP-clientconfiguratie en -query's op Linux

In dit voorbeeld is een Debian-server gebruikt. Houd er rekening mee dat de installatiestappen kunnen variëren, afhankelijk van uw distributiepakketbeheer.

SNMP-tools installeren

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

Controleer of de snmpwalk binary is geïnstalleerd.

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

MIB-bestanden laden

Plaats IronPort MIB-bestanden in de map /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
```

Debian-server-OID's

Opmerking: MIB-bestanden zijn te vinden in het SNMP-artikel dat aan het einde van dit document wordt gedeeld.

Een OID gebruiken om het CPU-gebruik te bewaken

Met deze opdracht wordt de ESA gevraagd naar het huidige CPU-gebruik. De OID verwijst rechtstreeks naar de CPU-metriek die is gedefinieerd in de MIB. De uitvoer geeft een waarde weer, zoals INTEGER: 37, wat aangeeft dat het CPU-gebruik van het apparaat 37% bedraagt. Hierdoor kunnen beheerders de prestaties van apparaten in realtime controleren en ingrijpen als het gebruik de aanvaardbare limieten overschrijdt.

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

```
.1.3.6.1.4.1.15497.1.1.1.2
```

Het gebruik van OID's in SNMP-opdrachten biedt directe toegang tot specifieke statistieken voor effectieve bewaking en probleemoplossing.

Symbolische namen inschakelen

```
export MIBS=ALL
```

Met het instellen van export MIBS=ALL kunnen SNMP-tools door mensen leesbare namen gebruiken die zijn gedefinieerd in de MIB-bestanden in plaats van lange numerieke OID's. Dit maakt query's gemakkelijker te schrijven, te begrijpen en problemen op te lossen, omdat u naar objecten kunt verwijzen met betekenisvolle namen zoals workQueueMessages in plaats van reeksen getallen.

SNMP-query's uitvoeren

Gebruik snmpwalk om ESA te bevragen voor belangrijke statistieken. Met SNMP-query's kunt u realtime status- en prestatiegegevens ophalen van uw Cisco ESA. Door symbolische namen te gebruiken, kunt u eenvoudig specifieke objecten zoals wachtrijstatus, licentievervaldatum en hardwaregebruik controleren zonder dat u complexe numerieke OID's hoeft te raadplegen.

Berichten in de werkvoorraad

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

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

Deze uitvoer laat zien dat er momenteel nul berichten in de ESA-werkvoorraad staan. De waarde vertegenwoordigt het real-time aantal e-mails dat wacht om te worden verwerkt.

CPU-gebruik

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

Dit geeft aan dat de CPU van ESA momenteel op 37% gebruik staat. De waarde geeft u inzicht in de verwerkingsbelasting van het toestel op het moment dat de query werd uitgevoerd.

Vervaltabel licentiesleutel

```
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: Elke index vertegenwoordigt een unieke functietoets die op de Cisco

ESA is geïnstalleerd.

- keyDescription.X: geeft de naam of beschrijving van elke functietoets, zoals 'Bounce Verification', 'Data Loss Prevention', 'IronPort Anti-Spam' en 'Sophos Anti-Virus'.
- keyIsPerpetual.X: Geeft aan of de licentie voor elke functie eeuwigdurend is. De waarde true (1) betekent dat de licentie niet verloopt.
- keySecondsUntilExpire.X: Geeft aan hoeveel seconden er nog over zijn totdat de licentie verloopt. Een waarde van 0 bevestigt dat de licentie eeuwigdurend is of al is verlopen.

```
[]> 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
```

licentievoorbeeld

Deze uitvoer bevestigt de huidige functietoetsen van het toestel, de beschrijvingen ervan en de licentiestatus. Alle vermelde licenties zijn eeuwigdurend, zoals aangegeven door keyIsPerpetual en keySecondsUntilExpire. Deze informatie helpt ervoor te zorgen dat essentiële beveiligingsfuncties actief en geldig blijven op uw Cisco ESA.

Verschil tussen numerieke OID's en symbolische namen

Numerieke OID's:

- Ze zijn universeel en werken altijd, zelfs als de MIB-bestanden niet op het systeem zijn geladen.
- Voorbeeld: .1.3.6.1.4.1.15497.1.1.1.2.
- Ze zijn minder leesbaar en kunnen moeilijk te onthouden zijn.

Symbolische namen:

- Dit zijn gebruiksvriendelijke namen die zijn gedefinieerd in de MIB-bestanden, zoals perCentCPUtilization.
- Ze maken opdrachten gemakkelijker te schrijven en te begrijpen.
- Ze vereisen dat de MIB-bestanden correct worden geladen en dat de MIBS-omgevingsvariabele wordt geconfigureerd.
- Voorbeeld: snmpwalk -v2c -c ironport 10.31.124.165 perCentCPUUtilization.

Is het hetzelfde?

Beide methoden vragen dezelfde metriek en leveren identieke resultaten op, maar symbolische namen zijn praktischer en leesbaarder voor de mens, terwijl numerieke OID's betrouwbaarder zijn in omgevingen waar MIB-bestanden niet aanwezig of geladen kunnen zijn.

Gerelateerde informatie

- De status en gezondheid van het systeem bewaken met SNMP
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.