Monitore o Cisco ESA com SNMP

Introdução

Este documento descreve como monitorar o Cisco Secure Email Gateway usando SNMP, incluindo estrutura MIB, uso de OID e consultas práticas.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do protocolo SNMP
- Acesso ao dispositivo Cisco ESA
- Familiaridade com a linha de comando do Linux
- Cisco ESA com serviço SNMP ativado
- Cliente SNMP instalado (como ferramentas Net-SNMP)
- Arquivos MIB IronPort disponíveis e carregados
- Cadeia de caracteres da comunidade ou credenciais SNMP v3

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Email Gateway (ESA)
- Cliente Linux com ferramentas Net-SNMP
- Arquivos MIB: IRONPORT-SMI.txt, ASYNCOS-MAIL-MIB.txt

Configurar SNMP

A configuração SNMP no ESA é feita via CLI. Para habilitar o SNMP no Cisco ESA, acesse a CLI e execute snmpconfig.

A configuração padrão envolve:

- Ativando o serviço SNMP
- Escolhendo a interface e a porta de gerenciamento (geralmente 161)
- Ativando o SNMPv3 (segurança padrão: authPriv com SHA e AES)
- Definindo senhas de autenticação e privacidade
- Ativação de SNMPv1/v2c, especificando a string de comunidade (por exemplo, ironport)
- Definição de redes IPv4 permitidas para solicitações SNMP
- Configuração da versão de interceptação SNMP e do endereço IP de destino da interceptação
- Definindo a localização do sistema e as informações de contato

Após habilitar o SNMP, você pode ver um resumo semelhante a este:

```
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
```

Depois que o SNMP for habilitado e configurado, o dispositivo estará pronto para aceitar consultas SNMP de IPs de origem permitidos.

Configuração e consulta de cliente SNMP no Linux

Para este exemplo, um servidor Debian foi usado. Observe que as etapas de instalação podem variar dependendo do gerenciador do encapsulamento de distribuição.

Instalar ferramentas SNMP

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

Verifique se o binário snmpwalk está instalado.

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

Carregar arquivos MIB

Coloque os arquivos MIB do IronPort na pasta /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 oids

Note: Os arquivos MIB podem ser encontrados no artigo SNMP compartilhado no final deste documento.

Usando um OID para Monitorar a Utilização da CPU

Esse comando consulta o ESA quanto à utilização atual da CPU. O OID aponta diretamente para a métrica da CPU definida na MIB. A saída exibe um valor, como INTEIRO: 37, indicando o uso da CPU do dispositivo em 37%. Isso permite que os administradores monitorem o desempenho do dispositivo em tempo real e interfiram se a utilização exceder os limites aceitáveis.

```
snmpwalk -v2c -c ironport

      .1.3.6.1.4.1.15497.1.1.1.2
```

O uso de OIDs em comandos SNMP fornece acesso direto a métricas específicas para monitoramento e solução de problemas eficazes.

Habilitar Nomes Simbólicos

```
export MIBS=ALL
```

A definição export MIBS=ALL permite que as ferramentas SNMP usem nomes legíveis por humanos definidos nos arquivos MIB em vez de OIDs numéricos longos. Isso torna as consultas mais fáceis de gravar, entender e solucionar problemas, já que você pode se referir a objetos por nomes significativos, como workQueueMessages, em vez de sequências de números.

Executar consultas SNMP

Use snmpwalk para consultar o ESA para métricas-chave. As consultas SNMP permitem recuperar dados de status e desempenho em tempo real do Cisco ESA. Usando nomes simbólicos, você pode monitorar facilmente objetos específicos, como status da fila, expiração de licença e utilização de hardware, sem precisar fazer referência a OIDs numéricos complexos.

Mensagens da fila de trabalho

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

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

Esta saída mostra que atualmente não há mensagens na fila de trabalho do ESA. O valor representa o número em tempo real de emails aguardando para serem processados.

Utilização da CPU

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

Isso indica que a utilização da CPU do ESA está atualmente em 37%. O valor fornece informações sobre a carga de processamento do equipamento no momento em que a consulta foi executada.

Tabela de Expiração da Chave de Licença

```
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: Cada índice representa uma chave de recurso exclusiva instalada no

Cisco ESA.

- keyDescription.X: Fornece o nome ou a descrição de cada chave de recurso, como 'Verificação de Devolução', 'Prevenção de Perda de Dados', 'Antisspam IronPort' e 'Antivírus Sophos'.
- keyIsPerpetual.X: Indica se a licença para cada recurso é vitalícia. O valor true (1) significa que a licença não expira.
- keySecondsUntilExpire.X: Mostra quantos segundos restam até que a licença expire. O valor 0 confirma que a licença é vitalícia ou já expirou.

```
[]> 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
```

exemplo de licença

Esta saída confirma as chaves de recurso atuais do equipamento, suas descrições e o status da licença. Todas as licenças listadas são perpétuas, conforme indicado por keyIsPerpetual e keySecondsUntilExpire. Essas informações ajudam a garantir que os recursos de segurança essenciais permaneçam ativos e válidos no Cisco ESA.

Diferença entre OIDs Numéricos e Nomes Simbólicos

OIDs Numéricos:

- Eles são universais e sempre funcionam, mesmo que os arquivos MIB não estejam carregados no sistema.
- Exemplo: 1.1.3.6.1.4.1.15497.1.1.1.2
- Eles são menos legíveis e podem ser difíceis de lembrar.

Nomes simbólicos:

- Esses são nomes amigáveis definidos nos arquivos MIB, como perCentCPUUtilization.
- Eles tornam os comandos mais fáceis de escrever e entender.
- Exigem que os arquivos MIB sejam carregados corretamente e que a variável de ambiente MIBS seja configurada.
- Exemplo: snmpwalk -v2c -c ironport 10.31.124.165 porCentCPUUtilização.

É o mesmo?

Ambos os métodos consultam a mesma métrica e produzem resultados idênticos, mas nomes simbólicos são mais práticos e legíveis por humanos, enquanto OIDs numéricos são mais confiáveis em ambientes onde arquivos MIB não podem estar presentes ou carregados.

Informações Relacionadas

- Monitorando a integridade e o status do sistema usando SNMP
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.