مراقبة Cisco ESA باستخدام SNMP

المقدمة

يصف هذا المستند كيفية مراقبة عبارة البريد الإلكتروني الآمنة من Cisco باستخدام SNMP، بما في ذلك بنية MIB واستخدام OID والاستعلامات العملية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية ببروتوكول SNMP
- الوصول إلى جهاز Cisco ESA
- التشابه مع سطر أوامر Linux
- تمكين خدمة SNMP مع Cisco ESA
- عميل SNMP المثبت (مثل أدوات Net-SNMP)
- تتوفر ملفات قاعدة معلومات الإدارة (MIB) من IronPort ويتم تحميلها
- بيانات اعتماد سلسلة المجتمع أو SNMP v3

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- عبارة البريد الإلكتروني الآمنة (ESA) من Cisco
- عميل Linux مع أدوات Net-SNMP
- ملفات MIB: IronPort-SMI.txt و Asynco-Mail-MIB.txt

تكوين SNMP

يتم تكوين SNMP على ESA عبر CLI. لتمكين SNMP على Cisco ESA، يمكنك الوصول إلى واجهة سطر الأوامر (CLI) وتشغيل snmpconfig.

يتضمن الإعداد الافتراضي ما يلي:

- تمكين خدمة SNMP
- إختيار واجهة الإدارة والمنفذ (عادة 161)
- تمكين SNMPv3 (الأمان الافتراضي: المصادقة مع SHA و AES)
- تعيين عبارات مرور المصادقة والخصوصية
- تمكين SNMPv1/v2c، وتحديد سلسلة المجتمع (على سبيل المثال، ironPort)
- تحديد شبكات IPv4 المسموح بها لطلبات SNMP
- تكوين إصدار مالئمة SNMP وعنوان IP لهدف المالئمة
- إعداد موقع النظام ومعلومات االتصال

بعد تمكين بروتوكول SNMP، يمكنك رؤية ملخص مماثل لهذا:

```
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
```

بمجرد تمكين بروتوكول SNMP وتكوينه، يكون الجهاز مستعد لقبول استعالمات SNMP من عناوين IP المصدر المسموح بها.

إعداد عميل SNMP والاستعالم عنه على Linux

على سبيل المثال، تم إستخدام خادم Debian. لاحظ أن خطوات التثبيت يمكن أن تختلف بناء على مدير حزمة التوزيع.

تثبيت أدوات SNMP

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

تحقق من تثبيت ثنائي SnmpWalk.

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

تحميل ملفات MIB

وضع ملفات IronPort MIB في مجلد /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
```

ديبيان سيرفس

ملاحظة: يمكن العثور على ملفات قاعدة معلومات الإدارة في مقالة SNMP المشتركة في نهاية هذا المستند.

إستخدام OID لمراقبة إستخدام وحدة المعالجة المركزية (CPU)

يستعلم هذا الأمر ESA عن إستخدام وحدة المعالجة المركزية (CPU) الحالية لديه. يشير OID مباشرة إلى قياس وحدة المعالجة المركزية المحدد في قاعدة معلومات الإدارة (MIB). يعرض الإخراج قيمة، مثل عدد صحيح: 37، يشير إلى إستخدام وحدة المعالجة المركزية (CPU) الخاصة بالجهاز بنسبة 37٪. وهذا يمكن المسؤولين من مراقبة أداء الجهاز في الوقت الفعلي والتدخل إذا تجاوز الاستخدام الحدود المقبولة.

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

```
.1.3.6.1.4.1.15497.1.1.1.2
```

ةنيعم سيياقم ىلإ رشابملا لوصولا SNMP رماوأ يف (OIDs) ةزهجألا تافرعم مادختسإ رفوي
.اهحالصإو ءاطخألا فاشكتساو ةلاعفلا ةبقارملل

ةيزمرلا ءامسألا نيكمت

```
export MIBS=ALL
```

ةلباق ءامسأ مادختساب SNMP تاودأل لكلا=ةرادإلا تامولعم ةدعاق ريدصت دادعإ حمسي
.ةليوط OID ماقرأ نم الدب ةرادإلا تامولعم ةدعاق تافلم يف ةفرعم ناسنإلا لبق نم ةءارقلل
كنكمي ثيح ،اهحالصإو ءاطخألا فاشكتساو مهفلاو ةباتكلل لهسأ تامالعتسالا لعجي اذهو
نم الدب WorkQueueMessages لثم ىنعم تاذ ءامسأ مادختساب تانئاكلا ىلإ عوجرلا
.ماقرألا تالسلست

SNMP تامالعتسا ليغشت

SNMP تامالعتسا كل حيتت .حيتافملا سيياقم نع ESA مالعتسالا SnmpWalk مدختسأ
،ةيزمر ءامسأ مادختساب .كيدل Cisco ESA نم يلعفلا تقولا يف ءادألا ةلاح تانايب دادرتسإ
ةيحالص ءاهتنا ،راظتنالا ةمئاق ةلاح لثم ،ةلوهسب ةنيعم تانئاك ةبقارم كنكمي
.ةدقعم ةيمقر تافرعم مادختسإ ىلإ ةجاحلا نودب ةزهجألا مادختساو ،صيخرتلا

لمعلا راظتنا ةمئاق لئاسر

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

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

ددع ةميقلا لثمت .ESA لمع راظتنا ةمئاق يف لئاسر يأ ايلاح دجوت ال هنأ جارخإلا اذه حضوي
.اهتجلاعم رظتنت يتلا يلعفلا تقولا يف ينورتكلإلا ديربلا لئاسر

استخدام CPU

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

وهذا يشير إلى أن إستخدام وحدة المعالجة المركزية ل ESA حاليا يبلغ 37%. تمنحك القيمة رؤية حول حمل المعالجة الخاص بالجهاز في اللحظة التي تم فيها تنفيذ الاستعلام.

جدول انتهاء صلاحية مفتاح الترخيص

```
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: يمثل كل فهرس مفتاح ميزة فريد مثبت على Cisco ESA.

- keyDescription.X: يوفر اسم أو وصف كل مفتاح ميزة، مثل "التحقق من الارتداد" و"منع فقدان البيانات" و"مكافحة البريد العشوائي ل IronPort" و"Sophos Anti-Virus".
- keyIsدائم.X: الإشارة إلى ما إذا كان ترخيص كل ميزة دائما أم لا. القيمة true (1) تعني أن الترخيص لا تنتهي صلاحيته.
- keySecondsUntilExpire.X: عرض عدد الثواني المتبقية حتى انتهاء صلاحية الترخيص. تؤكد القيمة 0 أن الترخيص دائم أو انتهت صلاحيته بالفعل.

```
[]> 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
```

مثال على الترخيص

يؤكد هذا الإخراج مفاتيح الميزات الحالية للجهاز وأوصافها و الحالة الترخيص. تكون جميع التراخيص المدرجة دائمة، كما هو موضح بواسطة keyIsدائم و keySecondsUntilExpired. تساعد هذه المعلومات على ضمان بقاء ميزات الأمان الأساسية نشطة وسارية على Cisco ESA لديك.

الفرق بين أرقام OID الرقمية والأسماء الرمزية

OIDs الرقمية:

- إنها ملفات عامة وتعمل دائما، حتى إذا لم يتم تحميل ملفات قاعدة معلومات الإدارة على النظام.
- مثال: .1.3.6.1.4.1.15497.1.1.1.2.
- فهي أقل قراءة ويمكن أن يكون تذكرها صعبا.

أسماء رمزية:

- هذه أسماء سهلة الاستخدام معرفة في ملفات قاعدة معلومات الإدارة، مثل PerCentCPUUtile.
- إنهم يجعلون الأوامر أسهل للكتابة والفهم.
- إنها تتطلب تحميل ملفات قاعدة معلومات الإدارة بشكل صحيح وتكوين متغير بيئة قاعدة معلومات الإدارة (MIBS).
- مثال: snmpWalk -v2c -c-ironPort 10.31.124.165 في الماقة CPUUtile.

هل هو نفس الشيء؟

الكل الطريقتين يستطيعان نفس القياس ويحصلان على نتائج متماثلة، ولكن الأسماء الرمزية أكثر عملية وقابلة للقراءة من قبل الإنسان، بينما تكون معرفات الأرقام أكثر موثوقية في البيئات التي لا يمكن فيها وجود ملفات قاعدة معلومات الإدارة أو تحميلها.

ةلص تاذ تامولعم

- SNMP مادختساب هتاجلاو ماظنلا ةمالس ةبارم
- Cisco نم تالينزلتو ليفنلا معدلا

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).