استعلامات ESA و SMA و WSA باستخدام مثال تكوين أمر snmpwalk

المحتويات

المقدمة
المتطلبات الأساسية
التكوين
تكوين ESA
تكوين SMA
تكوين WSA
التحقق من الصحة
استكشاف الأخطاء وإصلاحها

المقدمة

يوضح هذا المستند كيفية إستخدام snmpwalk أمر للاستعلام أو الاستطلاع حول جهاز أمان البريد الإلكتروني من Cisco (ESA)) أو جهاز إدارة أمان المحتوى (SMA) من Cisco أو جهاز أمان الويب (WSA) من Cisco.

المتطلبات الأساسية

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

- ESA مع AsyncOS 5.x أو إصدار أحدث
- SMA مع AsyncOS 5.x أو إصدار أحدث
- WSA مع AsyncOS 5.x أو إصدار أحدث
- يلزم توفر جهاز مضيف منفصل يعمل بنظام التشغيل Linux أو Unix مع تثبيت حزمة شبكة SNMP للتوزيع

ملاحظة: يشير هذا المستند إلى البرامج التي لا يتم صيانتها أو دعمها بواسطة Cisco. يتم توفير المعلومات كنوع من المجاملة لراحتك. للحصول على مزيد من المساعدة، اتصل بمورد البرامج.

التكوين

يغطي هذا القسم تكوينات ESA و SMA و WSA.

تكوين ESA

1. أدخل snmpconfig أمر واجهة سطر الأوامر (CLI) لضمان تمكين بروتوكول إدارة الشبكة البسيط (SNMP).
2. قم بتنزيل جميع ملفات قاعدة معلومات الإدارة (MIB) الخاصة بنظام التشغيل AsyncOS من جهاز أمان البريد الإلكتروني من Cisco تحت الأدوات ذات الصلة:
   قاعدة معلومات الإدارة (MIB) ل txt) ESA) عبر نظام التشغيل AsyncOS SMIAsyncOS Mail MIB ل (ESA (txt
3. ضع هذه الملفات في دليل SNMP للجهاز المحلي، والذي غالبا ما يتشابه **/usr/net-snmp/share/mibs/.**

4. أستخدم مضيف SNMP لتشغيل snmpwalk :

```
snmpwalk -O a -v 2c -c ironport -M /usr/net-snmp/share/mibs/ -m "ALL" host.example.com
iso.3.6.1.2.1.1
```

في الأمر السابق، حدد:

- كل حقول المخرجات ذات '-O a'.
- إصدار بروتوكول SNMP 2c مع '-v 2c'.
- سلسلة مجتمع للقراءة فقط أو عامة (يجب أن تطابق سلسلة تطبيقك snmpconfig عملية إعداد) أو 'cisco' مع '-c cisco'.
- المسار أو الموقع المطلق الاختياري لملفات قاعدة معلومات الإدارة الخاصة بك مع '-M //the/path/to/snmp/mibs'.
- أي ملفات قاعدة معلومات الإدارة (MIB) لتحميلها (كل الأحمال كل شيء) باستخدام '-m "all"'.
- عنوان المضيف الهدف الموجود على الجهاز الخاص بك للاستطلاع باستخدام 'hostname' أو 'x.x.x.x'.
- نقطة البداية لشجرة معرف الكائن (OID) للجهاز لبدء السير باستخدام 'iso.3.6.1.2.1.1'.

يقوم الأمر العينة المسرود مسبقا بإرجاع قائمة بكافة المعلومات التشخيصية التي تم سحبها من الجهاز الخاص بك:

```
"snmpwalk -O a -v 2c -c ironport -M "/usr/net-snmp/share/mibs/" -m "ALL $~:
                                                host.example.com iso.3.6.1.2.1.1
,iso.3.6.1.2.1.1.1.0 = STRING: "IronPort Model C10, AsyncOS Version: 7.0.0-702
                                "#######-Build Date: 2009-11-10, Serial #: 00C09F3AED0E
                                    iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.15497.1.1
```

مثال SNMPv3

```
snmpwalk -v3 -l authPriv -u v3get -a SHA -A "cisco" -x AES -X "cisco" x.x.x.x iso.3.6.1.2.1.1
```

في الأمر السابق، حدد:

- الإصدار 3 من بروتوكول SNMP مع '-v 3'.
- ال -ل يقوم الخيار بتكوين ميزات المصادقة والتشفير المراد إستخدامها.
- يعمل الخيار -u على تعيين اسم مستخدم SNMP إلى النظام الفرعي لوحدة أمان المستخدم. هذه سلسلة يتراوح طولها من 1 إلى 32 ثمانية. يجب تكوينها بنفس الطريقة في كل من كيانات SNMP التي تحاول الاتصال.
- الخيار -a هو تعيين المصادقة.
- ال -A هو مفتاح التشفير السري.
- الخيار -x هو تعيين نوع التشفير.
- الغرض من -X هو تعيين عبارة مرور خصوصية SNMPv3.

- عنوان المضيف الهدف الموجود على الجهاز الخاص بك للاستطلاع باستخدام 'hostname' أو 'x.x.x.x'.

- نقطة البداية لشجرة معرف الكائن (OID) للجهاز لبدء السير باستخدام 'iso.3.6.1.2.1.1'.

ارجع أيضا إلى برامج Net-SNMP التعليمية أو الاستخدام **snmpwalk --help** لمزيد من التفاصيل حول snmpwalk الأوامر والأدوات المساعدة الأخرى المتعلقة ب SNMP.

تكوين SMA

1. أدخل snmpconfig أمر واجهة سطر الأوامر (CLI) لضمان تمكين بروتوكول SNMP.

2. قم بتنزيل جميع ملفات قاعدة معلومات الإدارة (MIB) الخاصة بنظام التشغيل AsyncOS من جهاز إدارة أمان المحتوى من Cisco أسفل الأدوات ذات الصلة:
قاعدة معلومات الإدارة (MIB) ل AsyncOS SMI ل AsyncOS Mail MIB(txt) SMA ل SMA (txt))
3. ضع هذه الملفات في دليل SNMP للجهاز المحلي، والذي غالبا ما يتشابه /usr/net-snmp/share/mibs/.

4. أستخدم مضيف SNMP لتشغيل snmpwalk :

```
snmpwalk -O a -v 2c -c ironport -M /usr/net-snmp/share/mibs/ -m "ALL" host.example.com
iso.3.6.1.2.1.1
```

في الأمر السابق، حدد:

- كل حقول المخرجات ذات '-O a'.

- إصدار بروتوكول SNMP 2c مع '-v 2c'.

- سلسلة مجتمع للقراءة فقط أو عامة (يجب أن تطابق سلسلة تطبيقك snmpconfig عملية إعداد) أو 'cisco' مع '-c cisco'.

- المسار أو الموقع المطلق الاختياري لملفات قاعدة معلومات الإدارة الخاصة بك مع '-M //the/path/to/snmp/mibs'.

- أي ملفات قاعدة معلومات الإدارة (MIB) لتحميلها (كل الأحمال كل شيء) باستخدام '-m "all"'.

- عنوان المضيف الهدف الموجود على الجهاز الخاص بك للاستطلاع باستخدام 'hostname' أو 'x.x.x.x'.

- نقطة البداية لشجرة معرف الكائن (OID) للجهاز لبدء السير باستخدام 'iso.3.6.1.2.1.1'.

يقوم الأمر العينة المسرود مسبقا بإرجاع قائمة بكافة المعلومات التشخيصية التي تم سحبها من الجهاز الخاص بك:

```
"snmpwalk -O a -v 2c -c ironport -M "/usr/net-snmp/share/mibs/" -m "ALL $~:
                                                host.example.com iso.3.6.1.2.1.1
,iso.3.6.1.2.1.1.1.0 = STRING: "IronPort Model C10, AsyncOS Version: 7.0.0-702
                                "#######-Build Date: 2009-11-10, Serial #: 00C09F3AED0E
                                    iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.15497.1.1
```

مثال SNMPv3

```
snmpwalk -v3 -l authPriv -u v3get -a SHA -A "cisco" -x AES -X "cisco" x.x.x.x iso.3.6.1.2.1.1
```

في الأمر السابق، حدد:

- الإصدار 3 من بروتوكول SNMP مع '-v 3'.
- يقوم الخيار بتكوين ميزات المصادقة والتشفير المراد إستخدامها.
- يعمل الخيار -u على تعيين اسم مستخدم SNMP إلى النظام الفرعي لوحدة أمان المستخدم. هذه سلسلة يتراوح طولها من 1 إلى 32 ثمانية. يجب تكوينها بنفس الطريقة في كل من كيانات SNMP التي تحاول الاتصال.
- الخيار -a هو تعيين المصادقة.
- ال -A هو مفتاح التشفير السري.
- الخيار -x هو تعيين نوع التشفير.
- الغرض من -X هو تعيين عبارة مرور خصوصية SNMPv3.
- عنوان المضيف الهدف الموجود على الجهاز الخاص بك للاستطلاع باستخدام 'hostname' أو 'x.x.x.x'.
- نقطة البداية لشجرة معرف الكائن (OID) للجهاز لبدء السير باستخدام 'iso.3.6.1.2.1.1'.

ارجع أيضا إلى برامج Net-SNMP التعليمية أو الاستخدام **snmpwalk --help** لمزيد من التفاصيل حول snmpwalk الأوامر والأدوات المساعدة الأخرى المتعلقة ب SNMP.

تكوين WSA

1. أدخل snmpconfig أمر واجهة سطر الأوامر (CLI) لضمان تمكين بروتوكول SNMP.
2. قم بتنزيل جميع ملفات قاعدة معلومات الإدارة (MIB) المتعلقة ب AsyncOS من جهاز أمان الويب من Cisco تحت الأدوات ذات الصلة:
   قاعدة معلومات الإدارة (MIB) ل AsyncOS SMI ل WSA (txt)AsyncOS Mail MIB ل WSA ((txt)AsyncOS Web MIB (txt
3. ضع هذه الملفات في دليل SNMP للجهاز المحلي، والذي غالبا ما يتشابه **/usr/net-snmp/share/mibs/**.
4. أستخدم مضيف SNMP لتشغيل snmpwalk :

```
snmpwalk -O a -v 2c -c ironport -M /usr/net-snmp/share/mibs/ -m "ALL" host.example.com
iso.3.6.1.2.1.1
```

في الأمر السابق، حدد:

- كل حقول المخرجات ذات '-O a'.
- إصدار بروتوكول SNMP 2c مع '-v 2c'.
- سلسلة مجتمع للقراءة فقط أو عامة (يجب أن تطابق سلسلة تطبيقك snmpconfig عملية إعداد) أو 'cisco' مع '-c cisco'.
- المسار أو الموقع المطلق الاختياري لملفات قاعدة معلومات الإدارة الخاصة بك مع '-M //the/path/to/snmp/mibs'.
- أي ملفات قاعدة معلومات الإدارة (MIB) لتحميلها (كل الأحمال كل شيء) باستخدام '-m "all"'.

- عنوان المضيف الهدف الموجود على الجهاز الخاص بك للاستطلاع باستخدام 'hostname' أو 'x.x.x.x'.

- نقطة البداية لشجرة معرف الكائن (OID) للجهاز لبدء السير باستخدام 'iso.3.6.1.2.1.1'.

يقوم الأمر العينة المسرود مسبقا بإرجاع قائمة بكافة المعلومات التشخيصية التي تم سحبها من الجهاز الخاص بك:

```
"snmpwalk -O a -v 2c -c ironport -M "/usr/net-snmp/share/mibs/" -m "ALL $~:
                                                host.example.com iso.3.6.1.2.1.1
,iso.3.6.1.2.1.1.1.0 = STRING: "IronPort Model C10, AsyncOS Version: 7.0.0-702
                                "#######-Build Date: 2009-11-10, Serial #: 00C09F3AED0E
                                    iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.15497.1.1
```

ارجع أيضا إلى برامج Net-SNMP التعليمية أو الاستخدام **snmpwalk --help** لمزيد من التفاصيل حول snmpwalk الأوامر والأدوات المساعدة الأخرى المتعلقة ب SNMP.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

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).