CSM 3.x - إضافة أجهزة إستشعار IDS والوحدات النمطية إلى المخزون

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
إضافة أجهزة إلى مخزون مدير الأمان
خطوات إضافة مستشعر الهواة والوحدات النمطية
توفير معلومات الجهاز—جهاز جديد
استكشاف الأخطاء وإصلاحها
أسئلة الخطأ الشائعة
معلومات ذات صلة

المقدمة

يقدم هذه المستند معلومات حول كيفية إضافة أجهزة إستشعار ووحدات نظام اكتشاف الاقتحام (IDS) (تتضمن IDSM على محولات Catalyst 6500 switches، NM-CIDS على الموجهات، و AIP-SSM على ASA) في مدير أمان Cisco (CSM).

ملاحظة: الدعم CSM 3.2 لبروتوكول IPS 6.2. وهي ميزة في CSM 3.3.

المتطلبات الأساسية

المتطلبات

يفترض هذه المستند أن أجهزة CSM و IDS مثبتة وتعمل بشكل صحيح.

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى CSM 3.0.1.

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات

المستندات.

إضافة أجهزة إلى مخزون مدير الأمان

عندما تقوم بإضافة جهاز إلى "إدارة الأمان"، فإنك تجلب نطاق من معلومات تعريف الجهاز، مثل اسم DNS وعنوان IP الخاص به. بعد إضافة الجهاز، يظهر في مخزون جهاز "إدارة الأمان". يمكنك إدارة جهاز في "إدارة الأمان" فقط بعد إضافته إلى المخزون.

يمكنك إضافة أجهزة إلى مخزون "إدارة الأمان" باستخدام الأساليب التالية:

- إضافة جهاز من الشبكة.
- إضافة جهاز جديد غير موجود على الشبكة بعد
- قم بإضافة جهاز واحد أو أكثر من مستودع الأجهزة وبيانات الاعتماد (DCR).
- قم بإضافة جهاز واحد أو أكثر من ملف تكوين.

ملاحظة: يركز هذا المستند على الطريقة: إضافة جهاز جديد غير موجود على الشبكة بعد.

خطوات إضافة مستشعر الهوايات والوحدات النمطية

أستخدم الخيار إضافة جهاز جديد لإضافة جهاز واحد إلى مخزون مدير الأمان. يمكنك استخدام هذا الخيار للتوفير المسبق. يمكنك إنشاء الجهاز في النظام، وتعيين السياسات للجهاز، وإنشاء ملفات التكوين قبل استلام أجهزة الجهاز.

عند استلام أجهزة الجهاز، يجب تحضير الأجهزة لكي تتم إدارتها بواسطة إدارة الأمان. ارجع إلى إعداد الأجهزة لإدارة الأمان للحصول على مزيد من المعلومات.

يوضح هذا الإجراء كيفية إضافة مستشعر IDS جديد والوحدات النمطية:

1. انقر فوق زر عرض الجهاز في شريط الأدوات.

   تظهر صفحة الأجهزة.

2. انقر فوق الزر إضافة في محدد الجهاز.

   تظهر صفحة الجهاز الجديد - إختيار الأسلوب مع أربعة خيارات.

3. أختر إضافة جهاز جديد، ثم انقر فوق التالي.

   سوف تظهر صفحة معلومات الجهاز الجديد.

4. أدخل معلومات الجهاز في الحقول المناسبة.

   ارجع قسم توفير معلومات الجهاز الجديد للحصول على مزيد من المعلومات.

5. انقر فوق إنهاء.

   يقوم النظام بتنفيذ مهام التحقق من صحة الجهاز:

- إذا كانت البيانات غير صحيحة، يقوم النظام بإنشاء رسائل خطأ ويعرض الصفحة التي تحدث فيها الخطأ مع رمز خطأ أحمر يتوافق معه.
- إذا كانت البيانات صحيحة، تتم إضافة الجهاز إلى المخزون وتظهر في محدد الجهاز.

توفير معلومات الجهاز—جهاز جديد

أكمل الخطوات التالية:

1. حدد نوع الجهاز للجهاز الجديد:
   a. حدد مجلد نوع الجهاز من المستوى الأعلى لعرض عائلات الأجهزة المدعومة.
   b. حدد مجلد عائلة الجهاز لعرض أنواع الأجهزة المدعومة.
   a. حدد الواجهات والوحدات النمطية من Cisco > وحدات شبكة Cisco النمطية لإضافة الوحدة النمطية لشبكة موجه المرور Cisco IDS Access Router. وبالمثل، حدد الواجهات والوحدات النمطية من Cisco > وحدات Network Module. لإضافة وحدات AIP-SSM و IDSM النمطية الموضحة Cisco Services Modules.
   b. حدد الأمان والشبكة الخاصة الظاهرية (VPN) > أجهزة إستشعار Cisco IPS 4200 لإضافة مستشعر Cisco IDS 4210 إلى مخزون CSM. Series
   c. حدد نوع الجهاز.

   ملاحظة: بعد إضافة جهاز، لا يمكنك تغيير نوع الجهاز.

   يتم عرض معرفات كائن النظام الخاصة بنوع الجهاز هذا في حقل SysObjectId. يتم تحديد معرف كائن النظام الأول بشكل افتراضي. يمكنك تحديد آخر إذا لزم الأمر.
2. أدخل معلومات الأداة وهي معلومة، مثل الـ ip نوع (ساكن إستاتيكي أو حركي)، hostname، domain name، عنوان، وعرض إسم.
3. أدخل معلومات نظام تشغيل الجهاز، مثل نوع نظام التشغيل واسم الصورة وإصدار نظام التشغيل. حدد الهدف والسياقات ووضع التشغيل.
4. حدد نوع الجهاز الذي يظهر حقل التحديث التلقائي أو محرك التكوين CNS، والذي يعتمد على نوع التحديث التلقائي—معروض لجدار حماية PIX أو أجهزة ASA.
   - التحديث التلقائي—معروض لموجهات Cisco IOS®.
   - محرك تكوين CNS—معروض لـ FWSM و Catalyst 6500/7600.

   ملاحظة: هذا الحقل غير نشط لأجهزة الخدمات.
5. أكمل الخطوات التالية:
   - إذا لم يظهر الخادم في القائمة، أكمل الخطوات التالية: -انقر فوق السهم لعرض قائمة بالخوادم. حدد الخادم الذي يدير تحديث تلقائي للجهاز.
     a. انقر فوق السهم، ثم حدد + إضافة خادم... يظهر مربع الحوار خصائص الخادم.

b. أدخل المعلومات في الحقول المطلوبة.

c. وانقر فوق OK. تتم إضافة الخادم الجديد إلى قائمة الخوادم المتوفرة.

- CNS-Configuration Engine (محرك التكوين CNS)- يتم عرض معلومات مختلفة، والتي تعتمد على ما إذا كنت قد حددت نوع IP الثابت أو الديناميكي:

ساكن إستاتيكي—انقر على السهم لعرض قائمة بمحركات التكوين. حدد محرك التكوين الذي يدير الجهاز. إذا لم يظهر محرك التكوين في القائمة، أكمل الخطوات التالية:

a. انقر فوق السهم، ثم حدد + محرك إضافة تكوين... يظهر مربع الحوار خصائص محرك التكوين.

b. أدخل المعلومات في الحقول المطلوبة.

c. وانقر فوق OK. تتم إضافة محرك التكوين الجديد إلى قائمة محركات التكوين المتوفرة.

- Dynamic—انقر فوق السهم لعرض قائمة بالخوادم. حدد الخادم الذي يدير الجهاز. إذا لم يظهر الخادم في القائمة، أكمل الخطوات التالية:

a. انقر فوق السهم، ثم حدد + إضافة خادم... يظهر مربع الحوار خصائص الخادم.

b. أدخل المعلومات في الحقل المطلوب.

c. وانقر فوق OK. تتم إضافة الخادم الجديد إلى قائمة الخوادم المتوفرة.

6. أكمل الخطوات التالية:

- وهذا من Cisco. في مدير الأمان، حدد خانة الاختيار إدارة الجهاز في إدارة الأمان، لإدارة الإعداد الافتراضي.

- إذا كانت الوظيفة الوحيدة للجهاز الذي تضيفه هي أن تعمل كنقطة نهاية VPN، قم بإلغاء تحديد خانة الاختيار إدارة الأمان من Cisco.

لن يقوم مدير الأمان بإدارة التكوينات أو تحميل التكوينات على هذا الجهاز أو تنزيلها.

7. حدد خانة الاختيار سياق الأمان للجهاز غير المدار لإدارة سياق الأمان، والذي لا يقوم مدير الأمان بإدارة جهازه الأصلي (جدار حماية PIX أو ASA أو FWSM).

يمكنك تقسيم جدار حماية PIX أو ASA أو FWSM إلى جدران حماية أمان متعددة، تعرف أيضا بسياقات الأمان. وكل سياق هو نظام مستقل له تشكيله وسياساته الخاصة. يمكن إدارة هذه السياقات المستقلة في "إدارة الأمان"، حتى وإن لم تكن إدارة الأمان تدير الأصل (جدار حماية PIX أو ASA أو FWSM).

ملاحظة: يكون هذا الحقل نشطا فقط إذا كان الجهاز الذي حددته في أداة تحديد الجهاز جهاز جدار حماية، مثل جدار حماية PIX أو ASA أو FWSM، يدعم سياق الأمان.

8. حدد خانة الاختيار إدارة في IPS Manager لإدارة موجه Cisco IOS في مدير IPS.

يكون هذا الحقل نشطا فقط إذا قمت بتحديد موجه Cisco IOS من محدد الجهاز.

ملاحظة: يستطيع مدير IPS إدارة ميزات IPS فقط على موجه Cisco IOS الذي يحتوي على إمكانيات IPS. لمزيد من المعلومات، راجع وثائق IPS.

إذا قمت بتحديد خانة الاختيار إدارة في IPS، فيجب عليك تحديد خانة الاختيار إدارة في مدير الأمان من Cisco أيضا.

إذا كان الجهاز المحدد هو IDS، فإن هذا الحقل غير نشط. ومع ذلك، يتم التحقق من خانة الاختيار لأن إدارة IPS موقوف بإدارة أجهزة إستشعار IDS.

إذا كان الجهاز المحدد هو جدار حماية PIX أو ASA أو FWSM، فإن هذا الحقل غير نشط لأن مدير IPS لا يدير أنواع الأجهزة هذه.

9. انقر فوق إنهاء.

يقوم النظام بتنفيذ مهام التحقق من صحة الجهاز:

- إذا كانت البيانات التي أدخلتها غير صحيحة، يقوم النظام بإنشاء رسائل خطأ ويعرض الصفحة التي يحدث فيها الخطأ.
- إذا كانت البيانات التي أدخلتها صحيحة، تتم إضافة الجهاز إلى المخزون وتظهر في أداة تحديد الأجهزة.

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

رسائل الخطأ

عند إضافة IPS إلى CSM، `يظهر الجهاز غير الصحيح: تعذر على SysObjId` أخطأ الرسالة `نوع النظام الأساسي.`

الحل

أتمت هذا steps in order to حللت هذا أخطأ رسالة.

1. قم بإيقاف تشغيل خدمة CSM Daemon في Windows، ثم أختر ملفات البرامج > CiscoPX > MDC > Athena > config > Directory، حيث يمكنك العثور على `VMS-SysObjID.xml`.
2. في ايضارتفا دوجوملا يلصألا VMS-SysObjID.xml فلم لدبتسا ،CSM ماظن ىلع `C:\Program Files\CSCOpx\MDC\athena\config\directory` بأحدث ملف `VMS-SysObjID.xml`.
3. قم بإعادة تشغيل خدمة "إدارة برنامج تشغيل برنامج CSM" (CRMDmgtd)، وأعد محاولة إضافة الجهاز (الأجهزة) المتأثرة أو اكتشافها مرة أخرى.

معلومات ذات صلة

- [صفحة دعم مدير الأمان من Cisco]()

- صفحة دعم نظام اكتشاف الاقتحام من Cisco
- الدعم التقني والمستندات - Cisco Systems

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).