

إلى تاهي بنت لاسرال FireSIGHT ماظن نيوكت ي جراخ syslog م داخ

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[إرسال تنبيهات إقحام](#)

[إرسال تنبيهات الحماية](#)

[الجزء 1: إنشاء تنبيه syslog](#)

[الجزء 2: إنشاء تنبيهات المراقبة الصحية](#)

[إرسال علامة التأثير واكتشاف الأحداث وتنبيهات البرامج الضارة](#)

المقدمة

في حين يوفر نظام FireSIGHT طرق عرض مختلفة للأحداث داخل واجهة الويب الخاصة به، فقد تحتاج إلى تكوين إعلام خارجي بالأحداث لتسهيل المراقبة المستمرة للأنظمة الحساسة. يمكنك تكوين نظام FireSIGHT لإنشاء تنبيهات تقوم بإعلامك عبر البريد الإلكتروني أو ملاءمة SNMP أو syslog عند إنشاء أحد الأمور التالية. يوضح هذا المقال كيفية تكوين مركز إدارة FireSIGHT لإرسال تنبيهات على خادم syslog خارجي.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة على syslog و FireSIGHT إدارة مركز. أيضا، ال syslog ميناء (تقصير هو 514) ينبغي كنت سمحت في جدار الحماية ك.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 5.2 من البرنامج أو إصدار أحدث.

تحذير: يتم إنشاء المعلومات الواردة في هذا المستند من جهاز في بيئة معملية خاصة، ويبدأ بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

إرسال تنبيهات إقحام

1. سجل الدخول إلى واجهة مستخدم الويب الخاصة بمركز إدارة FireSIGHT لديك.

2. انتقل إلى السياسات < الاختراق < سياسة الاختراق.

3. انقر فوق تحرير بجوار النهج الذي تريد تطبيقه.

4. انقر على إعدادات متقدمة.

5. حدد موقع تنبيه Syslog في القائمة وتعيينه على ممكن.

The screenshot shows the 'Edit Policy' page for an 'Intrusion Policy'. The left sidebar contains a navigation menu with 'Advanced Settings' selected. The main content area is titled 'Advanced Settings' and is divided into two sections: 'Performance Settings' and 'External Responses'. The 'Performance Settings' section includes options for 'Event Queue Configuration', 'Latency-Based Packet Handling', 'Latency-Based Rule Handling', 'Performance Statistics Configuration', 'Regular Expression Limits', and 'Rule Processing Configuration'. The 'External Responses' section includes 'SNMP Alerting' and 'Syslog Alerting'. The 'Syslog Alerting' option is highlighted with a red box, and a red arrow points to it from the left sidebar.

6. انقر فوق تحرير الموجود بجانب تنبيه Syslog.

7. اكتب عنوان IP الخاص بخادم syslog على حقل مضيفي التسجيل.

8. اختر وحدة مناسبة ومستوى الخطورة من القائمة المنسدلة. ويمكن ترك هذه العناصر عند القيم الافتراضية ما لم يتم تكوين خادم syslog لقبول التنبيهات الخاصة بمرفق معين أو مستوى خطورة محدد.

The screenshot shows the 'Edit Policy' page for 'Syslog Alerting'. The left sidebar contains a navigation menu with 'Advanced Settings' expanded. The main content area shows the 'Settings' section with a 'Logging Hosts' input field, a 'Facility' dropdown menu set to 'AUTH', and a 'Priority' dropdown menu set to 'EMERG'. A 'Revert to Defaults' button is located below the dropdowns.

9. انقر فوق **معلومات النهج** بالقرب من الجزء العلوي الأيسر من هذه الشاشة.

10. انقر فوق الزر **تنفيذ التغييرات**.

11. أعد تطبيق سياسة التطفل.

ملاحظة: لإنشاء التنبيهات، أستخدم نهج التطفل هذا في قاعدة التحكم بالوصول. في حالة عدم تكوين قاعدة التحكم في الوصول، قم بتعيين سياسة التطفل هذه لاستخدامها كإجراء افتراضي لنهج التحكم في الوصول، ثم أعد تطبيق نهج التحكم في الوصول.

الآن إذا تم تشغيل حدث إقحام على هذا النهج، سيتم أيضا إرسال تنبيه إلى خادم syslog الذي تم تكوينه على نهج التطفل.

إرسال تنبيهات الحماية

الجزء 1: إنشاء تنبيه syslog

1. سجل الدخول إلى واجهة مستخدم الويب الخاصة بمركز إدارة FireSIGHT لديك.

2. انتقل إلى السياسات < الإجراءات < التنبيهات.

The screenshot shows the 'Alerts' page in the FireAMP interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. The 'Alerts' page has a sub-navigation bar with 'Alerts', 'Impact Flag Alerts', 'Discovery Event Alerts', and 'Advanced Malware Protection Alerts'. A 'Create Alert' button with a green plus icon is highlighted with a red box. Below the button is a table with columns for 'Name', 'Type', 'In Use', and 'Enabled'.

3. حدد **إنشاء تنبيه**، الموجود على الجانب الأيمن من واجهة الويب.



4. انقر فوق إنشاء تنبيه syslog. تظهر نافذة منبثقة للتكوين.

5. قم بتوفير اسم للتنبيه.

6. املأ عنوان IP الخاص بخادم syslog في حقل المضيف.

7. قم بتغيير المنفذ إذا لزم الأمر بواسطة خادم syslog (المنفذ الافتراضي هو 514).

8. حدد منشئاً مناسباً ومستوى الخطورة.

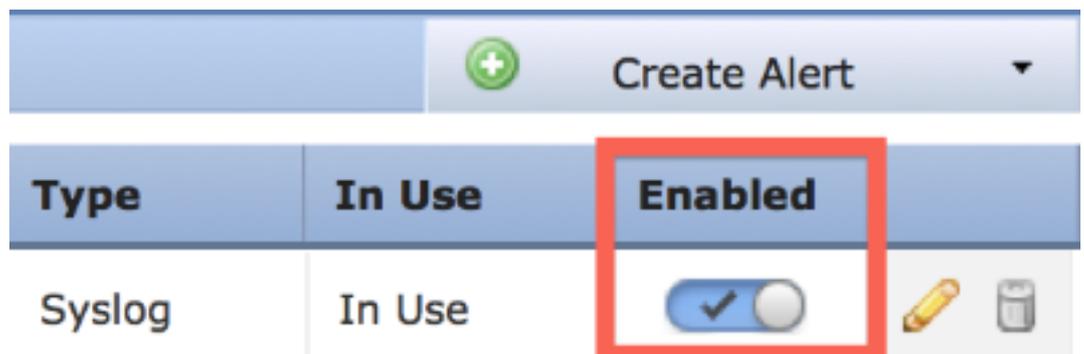
Create Syslog Alert Configuration ? x

| | |
|----------|----------------------|
| Name | <input type="text"/> |
| Host | <input type="text"/> |
| Port | 514 |
| Facility | ALERT |
| Severity | ALERT |
| Tag | <input type="text"/> |

Save Cancel

9. انقر فوق الزر حفظ. سوف تعود إلى صفحة السياسات < العمليات < التنبيهات.

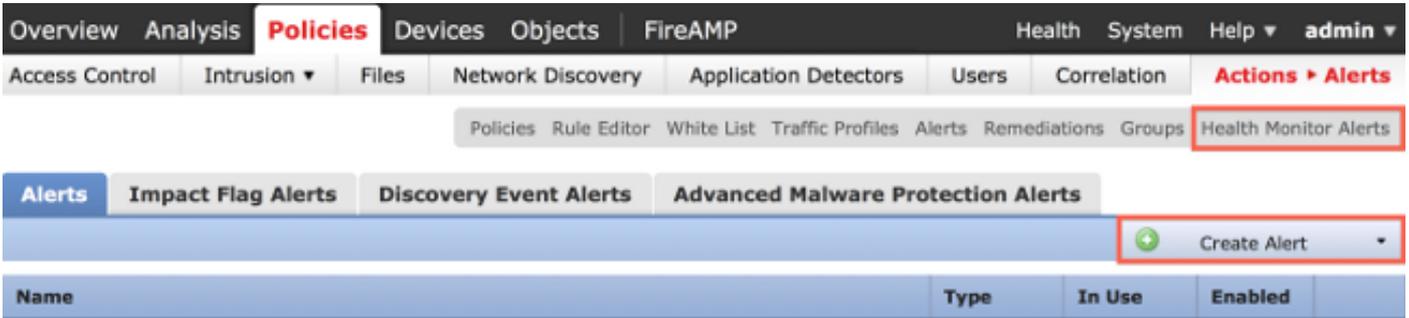
10. مكنت ال syslog تشكيل.



الجزء 2: إنشاء تنبيهات المراقبة الصحية

يصف الأمر التالي الخطوات لتكوين تنبيهات Health Monitor التي تستخدم تنبيه syslog الذي قمت بإنشائه للتو (في القسم السابق):

1. انتقل إلى السياسات < الإجراءات > التنبيهات، واختر تنبيهات Health Monitor، والتي تقع بالقرب من أعلى الصفحة.



2. قم بتسمية التنبيه الصحي.

3. اختر خطورة (مع الاستمرار في الضغط على مفتاح CTRL أثناء إمكانية استخدام النقر لتحديد أكثر من نوع خطورة واحد).

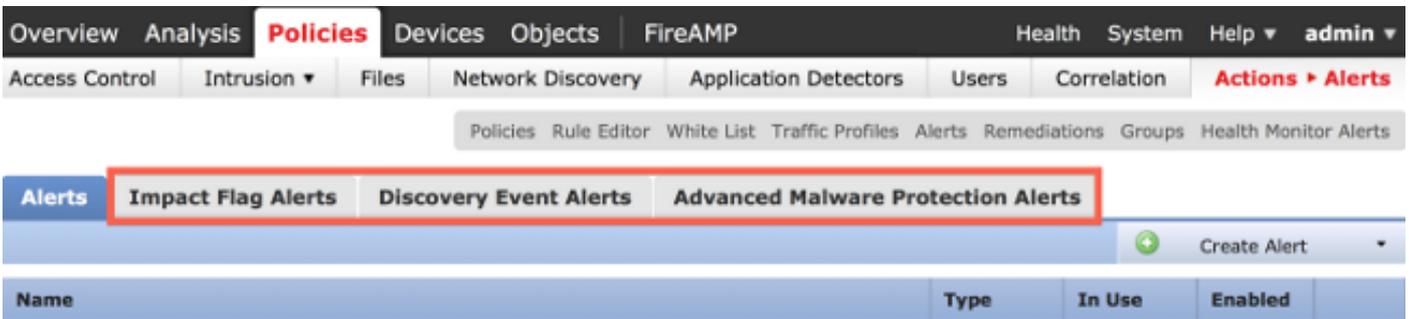
4. من الوحدة النمطية اختر وحدات الحماية التي ترغب في إرسال تنبيهات لها إلى خادم syslog (على سبيل المثال، استخدام القرص).

5. حدد تنبيه syslog الذي تم إنشاؤه مسبقاً من عمود التنبيهات.

6. انقر فوق الزر حفظ.

إرسال علامة التأثير واكتشاف الأحداث وتنبيهات البرامج الضارة

كما يمكنك تكوين مركز إدارة FireSIGHT لإرسال تنبيهات syslog للأحداث باستخدام علامة تأثير محددة ونوع محدد من أحداث الاكتشاف وأحداث البرامج الضارة. in order to تمت هذا، أنت يضطر أن [جزء 1: خلقت syslog تنبيه](#) وبعد ذلك شكلت النوع الحدث أن أنت تريد أن يرسل إلى ك syslog نادل. يمكنك القيام بذلك عن طريق الانتقال إلى صفحة السياسات < العمليات > التنبيهات، ثم تحديد صفحة لنوع التنبيه المرغوب.



ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةفارتحال ةمچرتل عم لاعلاء و
ىل إأمءءاد ءوچرلاب ةصوء و تامچرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إلال دن تسمل