اليوم 41 - Syslog

مقدمة عن نظام تسجيل الأحداث المركزي

بروتوكول Syslog هو معيار عالمي لتسجيل الأحداث (Logging) من أجهزة الشبكة وإرسالها إلى خادم مركزي. في أي شبكة احترافية، تحتاج إلى تتبع ما يحدث على أجهزتك من تغييرات في التكوين، وأعطال في الواجهات، ومحاولات دخول فاشلة، وأحداث أمنية أخرى. بدلاً من تسجيل الدخول إلى كل جهاز على حدة لقراءة سجلاته، يقوم Syslog بإرسال جميع هذه السجلات إلى خادم مركزي واحد حيث يمكن閲覽ها وتحليلها والبحث فيها بسهولة. يعمل Syslog على المنفذ 514 باستخدام بروتوكول UDP، مما يعني أنه لا يضمن وصول الرسائل (Best Effort)، ولكن هذا مقبول لأن فقدان بعض الرسائل في حالات ازدحام الشبكة أفضل من إبطاء الشبكة بسبب إعادة إرسالها.

مستويات الخطورة في Syslog (Severity Levels)

يصنف Syslog الرسائل حسب مستوى خطورتها من 0 إلى 7. المستوى 0 هو Emergency ويعني أن النظام غير صالح للاستخدام (مثل فشل في وحدة التخزين). المستوى 1 هو Alert ويتطلب اتخاذ إجراء فوري. المستوى 2 هو Critical ويشير إلى حالة حرجة مثل عطل في إحدى الوظائف الأساسية. المستوى 3 هو Error ويشير إلى خطأ في إحدى الوظائف. المستوى 4 هو Warning ويحذر من احتمال حدوث مشكلة. المستوى 5 هو Notification ويعطي معلومات عن حدث طبيعي لكنه مهم. المستوى 6 هو Informational ويعطي معلومات عامة عن تشغيل النظام. المستوى 7 هو Debug ويستخدم لأغراض تصحيح الأخطاء ويولد كمية هائلة من الرسائل التي قد تؤثر على أداء الجهاز. في الشبكات الإنتاجية، نادراً ما يتم تسجيل المستوى 7 لأن كمية البيانات الناتجة عنه تكون هائلة.

```
المستويات من الأكثر خطورة إلى الأقل:
0  Emergency - النظام غير قابل للاستخدام
1  Alert - يجب اتخاذ إجراء فوري
2  Critical - حالة حرجة
3  Error - خطأ
4  Warning - تحذير
5  Notification - إشعار مهم
6  Informational - معلومات عامة
7  Debug - تصحيح أخطاء
```

تنسيق رسالة Syslog

تتبع رسائل Syslog على أجهزة سيسكو تنسيقاً موحداً يسهل قراءته وتحليله. التنسيق القياسي هو: timestamp %FACILITY-SEVERITY-MNEMONIC: description. على سبيل المثال: Mar 1 02:45:12.345: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up. هنا، timestamp

هو وقت حدوث الحدث، FACILITY هو مصدر الرسالة (مثل LINEPROTO أو SYS أو IF)، SEVERITY هو رقم مستوى الخطورة، MNEMONIC هو اختصار وصف الحدث، والوصف هو شرح تفصيلي باللغة الإنجليزية. فهم هذا التنسيق يساعد مهندسي الشبكات في تصفية السجلات والبحث عن أحداث معينة بسرعة.

تكوين Syslog على أجهزة سيسكو

لتكوين إرسال سجلات Syslog إلى خادم مركزي، نستخدم الأمر `logging host` متبوعاً بعنوان IP الخاص بخادم Syslog. بعد ذلك، نحدد مستوى الخطورة الذي نريد إرساله باستخدام الأمر `logging trap` متبوعاً برقم المستوى أو اسمه، حيث سيتم إرسال جميع الرسائل التي لها هذا المستوى أو أعلى خطورة (أي رقم أقل). على سبيل المثال، `logging trap 4` يعني إرسال جميع الرسائل من المستوى 0 إلى 4. لتخزين السجلات محلياً على الجهاز نفسه، نستخدم الأمر `logging buffered` متبوعاً بحجم الذاكرة المخصصة (بالبايت) ومستوى الخطورة. لعرض السجلات على شاشة وحدة التحكم (Console)، نستخدم الأمر `logging console` مع مستوى الخطورة المطلوب.

```
Router(config)# logging host 192.168.1.100
Router(config)# logging trap 4
Router(config)# logging buffered 8192
Router(config)# logging console 3
Router(config)# logging source-interface loopback 0
Router(config)# logging on
```

الأمر show logging

الأمر `show logging` هو الأداة الرئيسية لعرض سجلات النظام على جهاز سيسكو. يعرض هذا الأمر جميع الرسائل المخزنة في الذاكرة المخصصة (Buffer) مرتبة حسب وقت حدوثها. كما يعرض معلومات عن تكوين Syslog نفسه مثل عنوان خادم Syslog المستهدف، ومستوى الخطورة المرسل، وحجم الذاكرة المستخدمة. يمكن استخدام هذه المعلومات للتأكد من أن نظام تسجيل الأحداث يعمل بشكل صحيح. من الممارسات الجيدة فحص السجلات بانتظام لاكتشاف أي أنماط غير طبيعية قد تشير إلى مشاكل أمنية أو تشغيلية في الشبكة.

```
Router> show logging
Router> show logging | include %LINEPROTO
Router> show logging | include ERROR
```

نصيحة مهمة: عند استخدام الأمر `logging console 7` لتصحيح الأخطاء، ستظهر كمية هائلة من الرسائل على شاشة وحدة التحكم وقد تجعل الجهاز بطيئاً في الاستجابة. تأكد من إعادة تعيين مستوى Console إلى مستوى أعلى (مثل 3) فور الانتهاء من التصحيح. تذكر أيضاً أن استخدام مستوى Debug يستهلك موارد المعالج بشكل كبير وقد يؤثر على أداء الجهاز.

أهمية Syslog في الشبكات

فوائد نظام Syslog تتجاوز مجرد تسجيل الأحداث. في التحقيقات الأمنية، تعتبر سجلات Syslog المصدر الأول للأدلة الرقمية (Digital Forensics) حيث تظهر محاولات الاختراق والتسلل. في تحليل أداء الشبكة، يمكن استخدام سجلات Syslog لتحديد أنماط الأعطال المتكررة واتخاذ إجراءات وقائية. في الامتثال للمعايير (Compliance)، مثل PCI-DSS أو HIPAA أو ISO 27001، يعتبر وجود نظام مركزي لتسجيل الأحداث وتخزينها شرطاً إلزامياً. أنظمة إدارة السجلات المركزية مثل Splunk و ELK Stack (Elasticsearch و Logstash و Kibana) و Graylog تستقبل رسائل Syslog وتوفر أدوات متقدمة للبحث وتحليل البيانات والتنبيه عند حدوث أحداث معينة.

تنسيق الطابع الزمني في Syslog

لضمان دقة السجلات، من المهم جداً أن تكون الساعة على أجهزة الشبكة متزامنة باستخدام NTP كما تعلمنا سابقاً. بدون مزامنة الوقت، ستحتوي سجلات Syslog على طوابع زمنية غير صحيحة، مما يجعل من المستحيل تتبع تسلسل الأحداث عبر أجهزة متعددة. يمكن تحسين دقة الطوابع الزمنية باستخدام الأمر `service timestamps log datetime msec` الذي يضيف الملي ثانية إلى الطابع الزمني، و `service timestamps debug datetime msec` لرسائل التصحيح.

```
Router(config)# service timestamps log datetime msec
Router(config)# service timestamps debug datetime msec
```

في الختام، Syslog هو عنصر أساسي في أي بنية تحتية شبكية حديثة. فهم مستويات الخطورة المختلفة وتنسيق الرسائل وكيفية تكوين إرسال السجلات إلى خادم مركزي سيساعدك في بناء نظام مراقبة فعال لشبكتك. تذكر أن السجلات لا تفيد إلا إذا تمت مراجعتها وتحليلها بانتظام، لذا احرص على تخصيص وقت لفحصها والبحث عن الأنماط غير الطبيعية.