配置 FMC 将审核日志发送到系统日志服务器

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 步骤1.启用到系统日志的审核日志
- 步骤2.配置系统日志信息

验证

故障排除

相关信息

简介

本文档介绍如何配置要发送到系统日志服务器的Secure Firewall Management Center Audit Logs。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科防火墙管理中心(FMC)的基本可用性
- 了解系统日志协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科防火墙管理中心虚拟v7.4.0
- 第三方系统日志服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

安全防火墙管理中心在只读审核日志中记录用户活动。从Firepower版本7.4.0开始，可以通过指定配置数据格式和主机，将配置更改作为审核日志数据的一部分流式传输到系统日志。通过将审核日志流式传输到外部服务器，可以节省管理中心上的空间，当您需要提供配置更改的审核跟踪时，此功能也非常有用。

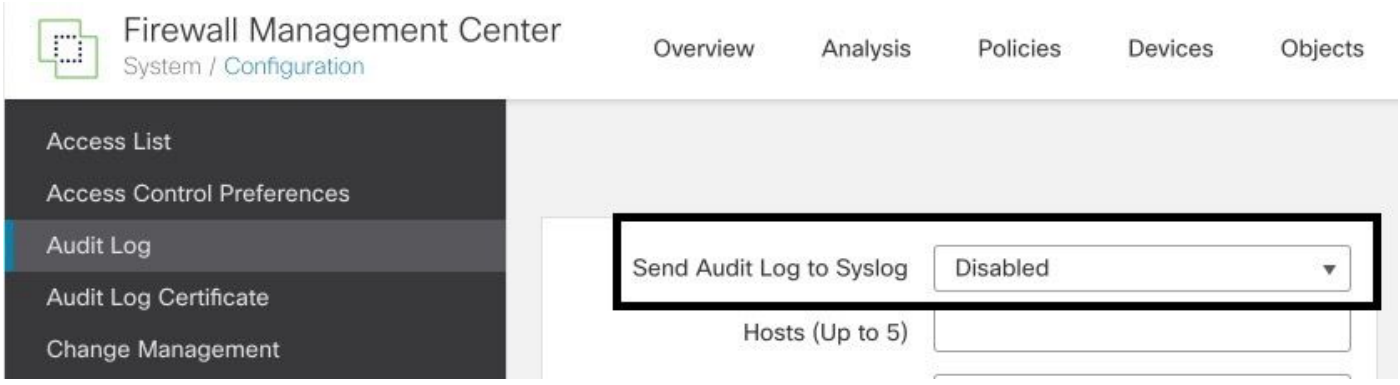
在高可用性情况下，只有主用管理中心将配置更改syslog发送到外部syslog服务器。日志文件在HA对之间同步，以便在故障切换或切换期间，新的活动管理中心将恢复发送更改日志。如果HA对以大脑分割模式工作，则该对中的两个管理中心都会将配置更改系统日志发送到外部服务器。

配置

步骤1.启用到系统日志的审核日志

要启用FMC将审核日志发送到系统日志服务器，请导航到System > Configuration > Audit Log > Send Audit Log to Syslog > Enabled。

此图显示如何启用将审核日志发送到系统日志功能：



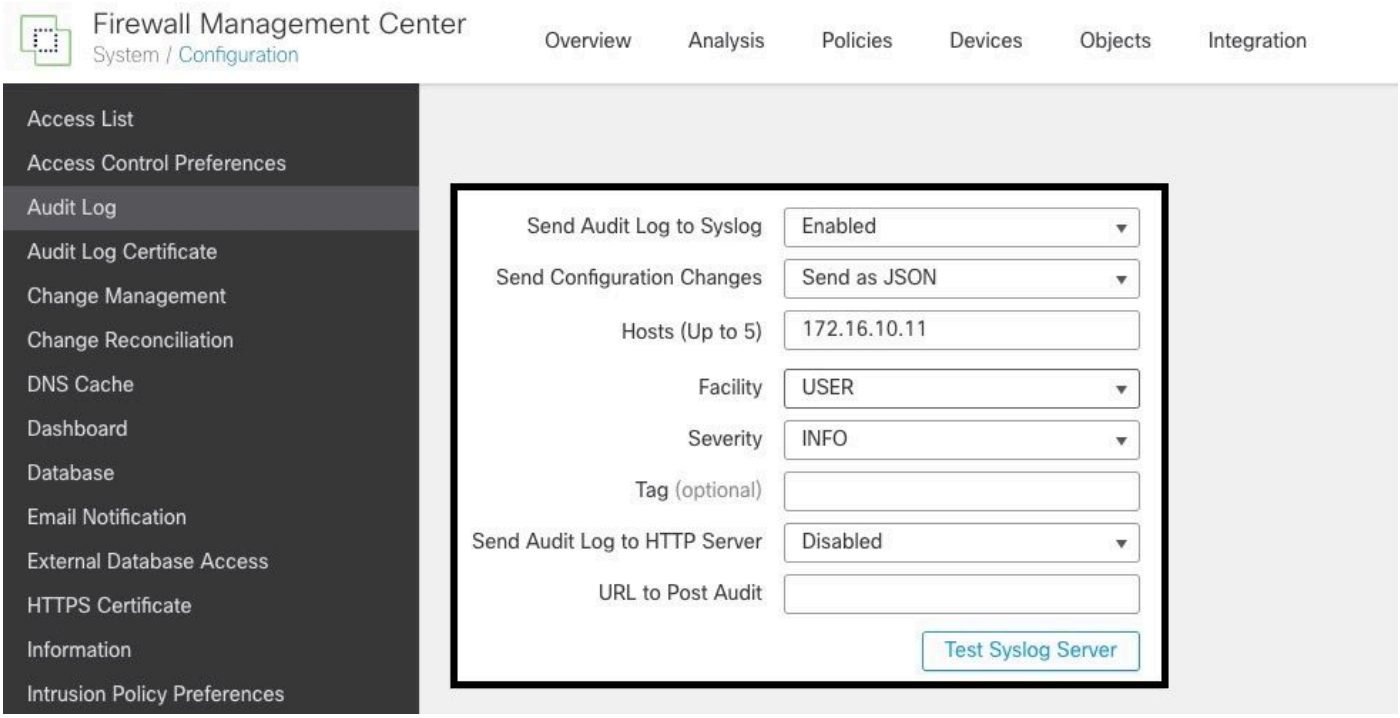
FMC最多可以将审核日志数据流式传输到五台系统日志服务器。

步骤2.配置系统日志信息

启用服务后，您可以配置系统日志信息。要配置系统日志信息，请导航到System > Configuration > Audit Log。

根据您的要求，选择Send Configuration Changes， Hosts， Facility， Severity。

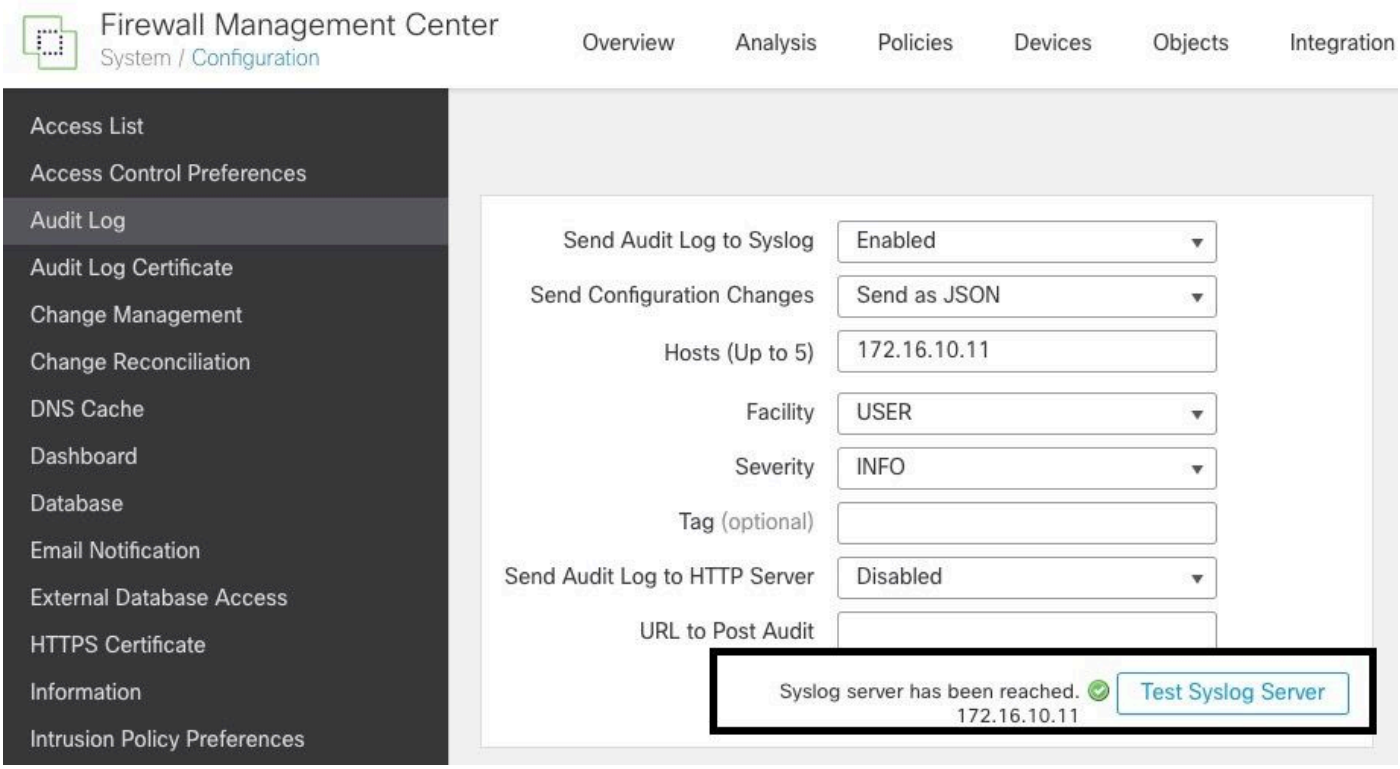
此图显示用于配置审核日志的系统日志服务器的参数：



验证

要验证参数是否配置正确，请选择System > Configuration > Audit Log > Test Syslog Server。

此图显示成功的Syslog服务器测试：



另一种验证系统日志是否工作的方法，检查系统日志接口以确认是否收到审核日志。

下图显示了Syslog服务器接收的审计日志的一些示例：



以下是一些可在系统日志服务器中接收的配置更改示例：

```
2023-09-29 16:12:18 localhost 172.16.10.2 Sep 29 16:12:23 firepower: [FMC-AUDIT] mojo_server.pl: admin@
2023-09-29 16:12:20 localhost 172.16.10.2 Sep 29 16:12:25 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1.
2023-09-29 16:12:23 localhost 172.16.10.2 Sep 29 16:12:28 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1.
2023-09-29 16:13:39 localhost 172.16.10.2 Sep 29 16:13:44 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1.
2023-09-29 16:14:32 localhost 172.16.10.2 Sep 29 16:14:37 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1.
2023-09-29 16:14:32 localhost 172.16.10.2 Sep 29 16:14:37 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1.
2023-09-29 16:14:54 localhost 172.16.10.2 Sep 29 16:14:59 firepower: [FMC-AUDIT] ActionQueueScrape.pl:
2023-09-29 16:14:55 localhost 172.16.10.2 Sep 29 16:15:00 firepower: [FMC-AUDIT] ActionQueueScrape.pl:
```

故障排除

应用配置后，确保FMC可以与syslog服务器通信。

系统使用ICMP/ARP和TCP SYN数据包验证系统日志服务器是否可访问。然后，如果您保护信道，系统默认使用端口514/UDP传输审核日志，使用TCP端口1470。

要在FMC上配置数据包捕获，请应用以下命令：

- tcpdump。此命令可捕获网络上的流量。

```
> expert
admin@firepower:~$ sudo su
Password:

root@firepower:/Volume/home/admin# tcpdump -i eth0 host 172.16.10.11 and port 514
```

此外，要测试ICMP可达性，请应用以下命令：

- ping。此命令有助于确认设备是否可访问，并了解连接的延迟。

```
> expert
admin@firepower:~$ sudo su
Password:
root@firepower:/Volume/home/admin#ping 172.16.10.11
PING 172.16.10.11 (172.16.10.11) 56(84) bytes of data.
64 bytes from 172.16.10.11: icmp_seq=1 ttl=128 time=3.07 ms
64 bytes from 172.16.10.11: icmp_seq=2 ttl=128 time=2.06 ms
64 bytes from 172.16.10.11: icmp_seq=3 ttl=128 time=2.04 ms
64 bytes from 172.16.10.11: icmp_seq=4 ttl=128 time=0.632 ms
```

相关信息

- 技术支持和文档 - Cisco Systems
- 思科安全防火墙管理中心管理指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。