与搜索日志的REGEX的ESA、SMA和WSA Grep

目录

[简介](#)
[先决条件](#)
[与REGEX的Grep](#)
[情形 1：查找访问日志的一个特定的网站](#)
[方案 2：尝试查找一个特定的文件扩展或顶级域](#)
[情形 3：尝试查找网站的一特定的块](#)
[场景 4：](#) [查找在访问日志的一个机器名字](#)
[场景 5：](#) [查找在访问日志的一个特定的时间](#)
[场景 6：](#) [关键或警告消息的搜索](#)

简介

本文描述如何以**grep命令**为了搜索日志使用常规表达(REGEX)。

先决条件

本文档中的信息基于以下软件和硬件版本：

- 思科Web安全工具(WSA)
- 思科电子邮件安全工具(ESA)
- 安全性管理设备(SMA)

与REGEX的Grep

REGEX可以是一个强大的工具，当使用以**grep命令**通过日志搜索可用在设备，例如访问日志，代理日志和其他。您能搜索根据网站的日志，或者URL和用户名的任何部分与CLI命令的**grep**。

这是一些常见情况您能以**grep命令**为了协助使用REGEX故障排除的地方。

情形 1：查找访问日志的一个特定的网站

多数常见情况是，当您尝试查找被做到WSA的访问日志的一个网站的请求时。

示例如下：

对设备的连接通过安全壳SSH。一旦有提示符，请输入**grep命令**为了列出可用的日志。

```
CLI> grep
```
输入您希望对**grep**日志的编号。

```
[]> 1 (Choose the # for access logs here)
```
输入常规表示对**grep**。

```
[]> website\.com
```

方案 2：尝试查找一个特定的文件扩展或顶级域

您能使用**grep命令**为了查找特定的文件扩展(.doc， .pptx)在URL或顶级域(.com， .org)。

示例如下：

为了查找以.crl结束的所有URL，请使用此REGEX ：

```
[]> website\.com
```
为了查找包含文件扩展.pptx的所有URL，请使用此REGEX ：

```
[]> website\.com
```

情形 3：尝试查找网站的一特定的块

当您搜索一个特定的网站时，您也许也搜索一特定的HTTP响应。

示例如下：

如果要搜索domain.com的所有TCP_DENIED/403消息，请使用此REGEX ：

```
[]> website\.com
```

场景 4：查找在访问日志的一个机器名字

当您使用NTLMSSP认证机制时，您也许遇到用户代理的实例(Microsoft NCSI最普通)不正确地发送计算机凭证而不是用户凭证，当验证时。为了搜寻导致此问题的URL/User代理程序，请以**grep**使用REGEX为了隔离被做的请求，当验证出现。

如果没有使用的机器名字，请使用**grep**并且查找使用作为用户名的所有机器名字，当验证与此REGEX时：

```
[]> website\.com
```
一旦有这发生的线路，使用与此REGEX的特定机器名字的grep ：

```
[]> website\.com
```

出现的首先进入应该是被做，当用户验证与机器名字而不是用户名的请求。

场景 5：查找在访问日志的一个特定的时间

默认情况下，访问日志订阅不包括显示人类易读的日期/时间的字段。如果要检查访问日志一个特定的时间，请完成这些步骤：

1. 查寻从一个站点的UNIX时间戳例如联机转换。
2. 一旦有时间戳，一度在访问日志内的特定时间请搜索。

示例如下：

Unix时间戳1325419200相当于01/01/2012 12:00:00。

您能使用此REGEX条目为了搜索访问日志近12:00在一月1， 2012 ：

13254192

场景 6：关键或警告消息的搜索

您能搜索在所有可用的日志的关键或警告消息，例如代理日志或系统日志，与常规表达。

示例如下：

为了搜索在代理日志的警告消息，请输入此REGEX ：

```
CLI> grep
```

输入您希望对grep日志的编号。

```
[]> 17 (Choose the # for proxy logs here)
```

输入常规表示对grep。

```
[]> warning
```