

# 目录

[问题](#)

[环境](#)

[解决方案](#)

[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：搜索关键或警告消息](#)

## 问题

如何以grep使用常规表达(REGEX)搜索日志？

## 环境

思科Web安全工具  
思科电子邮件安全工具  
Cisco安全管理设备

## 解决方案

常规表达(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。当使用CLI命令“grep”时，我们能搜索根据网站的日志，或者URL或者用户名的任何部分，命名一些。

下面一些常见情况您能以与故障排除的地方grep协助使用REGEX。

### [情形 1：查找访问日志的一个特定的网站](#)

多数常见情况尝试查找做到思科Web安全工具(WSA)的访问日志的一个网站请求。

例如：

对设备的连接通过SSH。一旦有提示符，我们能键入“grep”命令列出可用的日志。

CLI> grep
输入您希望对“grep”日志的编号。
[]> 1 (请选择#访问日志的此处)
输入常规表示对“grep”。

## 方案 2 : 尝试查找一个特定的文件扩展或顶级域

我们能使用“grep”命令查找特定的文件扩展(.doc , .pptx)在URL或顶级域(.com , .org)。

例如 :

要查找以.crl结束我们的所有URL可能使用以下REGEX : \.crl\$

要查找包含文件扩展.pptx的所有URL , 我们可能使用以下REGEX : \.pptx

## 情形 3 : 尝试查找网站的一特定的块

当搜索一个特定的网站时 , 我们也许也搜索一特定的HTTP响应。

例如 :

如果我们要搜索domain.com的所有TCP\_DENIED/403消息 , 我们可能使用以下REGEX : tcp\_denied/403.\*domain\ .com

## 场景 4 : 查找在访问日志的一个机器名字

当曾经NTLMSSP认证机制时 , 我们可能遇到用户代理的实例(Microsoft NCSI最普通)将不正确地发送计算机凭证而不是用户凭证 , 当验证时。要搜寻导致此的URL/User代理程序 , 我们能以“grep”使用REGEX隔离被做的请求 , 当验证出现。

如果我们没有使用的机器名字 , 我们能使用“grep”和找到使用作为用户名的所有机器名字 , 当验证使用以下REGEX时 : \ \$@

一旦我们有这发生的线路 , 我们能“grep”通过使用以下REGEX , 使用的特定机器名字的 : machinename \ \$

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 , 访问日志订阅不会包括显示人类易读的日期/时间的字段。如果我们要检查访问日志一个特定的时间 , 我们能遵从下面步骤 :

查寻从一个站点的UNIX时间戳例如[http://www.onlineconversion.com/unix\\_time.htm](http://www.onlineconversion.com/unix_time.htm)。一旦有时间戳 , 您能一度在访问日志内的特定时间搜索。

例如 :

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

我们能使用以下REGEX条目在时期的12:00附近搜索访问日志在一月第1 , 2012 : 13254192

## [场景 6 : 搜索关键或警告消息](#)

使用常规表达，我们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。

例如：

要搜索在代理日志的警告消息，我们能输入以下REGEX：

1. CLI> grep
2. 输入您希望对“grep”日志的编号。  
[]> 17 (请选择#代理日志的此处)
3. 输入常规表示对“grep”。  
[]>警告

其他有用的链路：

[常规表达-用户指南](#)