

事件搜索

以下主题介绍如何在工作流程中搜索事件：

- 事件搜索，第 1 页
- 通过外壳查询覆盖，第 9 页
- 搜索事件的历史记录，第 10 页

事件搜索

Firepower 系统生成的信息作为事件存储在数据库表中。事件包含多个字段，描述导致设备生成事件的活动。您可以创建并保存面向您的环境为任何不同事件类型自定义的搜索，并将其保存以供今后重复使用。

保存搜索时，请为其命名，并指定此搜索仅供您自己使用还是供设备的所有用户使用。如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。如果先前保存了一个搜索，则可加载该搜索，做出任何必要更改，然后开始搜索。自定义分析控制面板构件、报告模板和自定义角色也可以使用保存的搜索。如有已保存的搜索，可从 Search 页面删除这些搜索。

对于某些事件类型，Firepower 系统会提供预定义搜索，既可将其用作示例，又可借助其快速访问有关网络的重要信息。可针对网络环境修改预定义搜索中的字段，然后保存搜索，以供日后重复使用。

可使用的搜索条件取决于搜索类型，但搜索技巧相同。搜索仅返回与所有字段的指定搜索条件匹配的记录。

注释 搜索自定义表所需的程序略有不同。

相关主题

搜索自定义表

搜索限制

每个数据库表都有自己的搜索页面，您可以在此页面中输入搜索限制值以应用于为该表定义的字段。根据字段的类型，可使用专用语法来指定条件，例如通配符或数值范围。

搜索结果显示在工作流程页面，以柱状布局显示每个表字段。某些数据库表还可使用未在工作流程页面显示为列的字段进行搜索。查看工作流程页面中的结果时，要确定此类限制是否适用于搜索结果，请点击 **展开箭头** （ ） 以查看活动的搜索限制。

通用搜索限制

搜索事件时，请遵循以下通用准则：

- 许多字段需要通配符才能进行部分匹配搜索。所有字段都接受这些搜索的通配符。

  请参阅搜索中的通配符和符号 ， 第 2 页。

- 所有字段接受协商 (!)。
- 所有字段都接受逗号分隔的搜索值列表。包含指定字段中列出的任何值的记录与该搜索条件匹配。
- 所有字段都接受将用引号引起来的逗号分隔列表作为搜索值。
  - 对于只能包含一个值的字段，将包含指定精确字符串的指定字段放在引号内的记录与搜索条件匹配。例如，搜索 `A、B、"C、D、E" (A, B, "C, D, E")` 时，匹配记录为包含 `"A"` 或 `"B"` 或 `"C、D、E" ("C, D, E")` 的指定字段。这允许与可能的值中包含逗号的字段匹配。
  - 对于可能同时包含多个值的字段，指定字段包含所有引号引号引起来的逗号分隔列表中所有值的记录与该搜索条件匹配。
  - 对于可能同时包含多个值的字段，搜索条件可以包含单个值以及引号引起来的逗号分隔列表。例如，在某字段上搜索 `A, B, "C, D, E"` 时，如果该字段可能包含这其中一个或多个字母，则匹配的记录指定字段将包含 `A` 或 `B`或同时包含 `C`、`D`和 `E`。
- 在任何字段中指定 `n/a` 表示无字段相关信息的事件；使用 `!n/a` 表示该字段已填充的事件。
- 您可以在众多数字字段前面加上大于 (>)、大于或等于 (>=)、小于 (<)、小于或等于 (<=) 、等于 (=) 或不等于 (<>) 运算符。

提示 当搜索具有较长复杂值的字段（例如 SHA-256 散列值）时，可以从原材料复制搜索条件值，并将其粘贴到搜索页面上的合适字段中。

搜索中的通配符和符号

在连接和安全情报事件的所有文本字段以及其他事件类型的大多数文本字段中搜索时，搜索文本字段中的部分匹配项需要使用星号 (*) 来表示字符串中的未指定字符。不带星号的搜索是这些字段中的完全匹配搜索。即使在不需要通配符的字段中，我们也建议始终使用通配符进行部分匹配搜索。

例如，要查找 `example.com`、`www.example.com` 或 `Department.example.com`，请搜索 `*.example.com`。在大多数情况下，搜索 `example.com` 只会返回 `example.com`。

如果想要搜索非字母数字字符（包括星号字符），请用引号将搜索字符串引起来。例如，要搜索字符串：

```
Find an asterisk (*)
```

输入：

```
"Find an asterisk (*)"
```

搜索中的对象和应用过滤器

Firepower 系统可用于创建可用作网络配置一部分的已命名对象、对象组和应用过滤器。执行或保存搜索时，可使用这些对象、组和过滤器作为搜索条件。

执行搜索时，对象、对象组和应用过滤器以 `${object_name}` 格式显示。例如，对象名称为 `ten_ten_network` 的网络对象在搜索中显示为 `${ten_ten_network}`。

在可使用对象作为搜索条件的搜索字段旁边，可点击 **对象** （ ） 。

相关主题

对象管理器

搜索中的时间限制

下表显示了采用时间值的搜索条件字段接受的格式。

表 *1:* 搜索字段中的时间规范

时间格式	示例
`today [at HH:MMam|pm]`	`today` `today at 12:45pm`
*YYYY-DD*MM- *HH:MM:SS*	2006-03-22 14:22:59

可在时间值前输入下列运算符之一。

表 *2:* 时间规范运算符

运算符	示例	说明
<	< 2006-03-22 14:22:59	返回时间戳早于 2006 年 3 月 22 日下午 2:23 的事件。
>	> today at 2:45pm	返回时间戳晚于今天下午 2:45 的事件。

搜索中的 IP 地址

在搜索中指定 IP 地址时，可输入单个 IP 地址、用逗号隔开的地址列表、地址块或者一系列用连字符 (-) 隔开的 IP 地址。也可使用求反。

对于支持 IPv6 的搜索（例如，入侵事件、连接数据和关联事件搜索），可输入 IPv4 和 IPv6 地址与 CIDR/前缀长度地址块的任意组合。按 IP 地址搜索主机时，结果包括至少有一个 IP 地址与搜索条件匹配的所有主机，即搜索 IPv6 地址可能会返回原地址是 IPv4 的主机。

使用 CIDR 或前缀长度表示法指定 IP 地址块时，Firepower 系统**只**使用掩码或前缀长度指定的那部分网络 IP 地址。例如，如果键入 `10.1.2.3/8`，则 Firepower 系统使用 `10.0.0.0/8`。

因为 IP 地址可以用网络对象表示，所以，也可点击 IP 地址搜索字段旁边的添加网络 **对象** （ ）使用网络对象作为 IP 地址搜索条件。

表 *3:* 可接受的 *IP* 地址语法

要指定的内容...	键入的内容...	示例
单个 IP 地址	IP 地址。	`192.168.1.1` `2001:db8::abcd`
多个 IP 地址，使用列表	用逗号隔开的 IP 地址列表。请**不要**在逗号前后添加空格。	`192.168.1.1,192.168.1.2` `2001:db8::b3ff,2001:db8::0202`
可以使用 CIDR 块或前缀长度指定的一系列 IP 地址	采用 IPv4 CIDR 或 IPv6 前缀长度表示法的 IP 地址块。	`192.168.1.0/24` 这可在子网掩码为 255.255.255.0 的 192.168.1.0 网络中指定任意 IP，即 192.168.1.0 至 192.168.1.255。
不可使用 CIDR 块或前缀长度指定的一系列 IP 地址	使用连字符的 IP 地址范围。请**勿**在连字符前后添加空格。	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

用于指定 IP 地址或 IP 地址范围的任何其他方法的求反	在 IP 地址、块或范围前面输入感叹号。	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

被阻止或受监控（但本应被阻止）的主机 请参阅主机配置文件图标。	在连接和安全情报事件中，在“发起方 IP”和“响应方 IP”字段中： • • block • 监控	--

相关主题

Firepower 系统 IP 地址约定

搜索中的 URL

搜索 URL 时，请包含通配符。例如，使用 **`*example.com*`** 查找域的所有变体，例如 **`https://example.com`** 和 **`division.example.com`** 以及 **`example.com/division/`**。

搜索中的受管设备

如果您对设备进行分组（无论是仅在FMC上，还是作为实际的高可用性或可扩展性配置），则搜索组的名称会正确返回组中所有设备的结果。

如果系统找到组、则系统会用用于执行搜索的相应成员设备名称替换组名称。在设备字段保存使用了设备组 的搜索时，系统会保存设备字段中指定的名称，并且每次执行搜索时都会再次执行设备名称替换。

搜索中的端口

Firepower 系统接受搜索中端口号的特定语法。可输入：

- 单个端口号
- 用逗号隔开的端口号列表。
- 两个用连字号隔开的端口号，代表端口号范围
- 后接协议缩写、并用正斜杠隔开的端口号（仅限搜索入侵事件时）
- 一个端口号或端口号范围，前面带有感叹号，表示指定端口的求反



注释 指定端口号或范围时，请**不要**使用空格。

表 4: 端口语法示例

示例	说明
`21`	返回端口 21 上的所有事件，包括 TCP 和 UDP 事件。
`!23`	返回除端口 23 上的事件以外的所有事件。
`25/tcp`	返回端口 25 上的所有与 TCP 相关的入侵事件。
`21/tcp,25/tcp`	返回端口 21 和 25 上所有与 TCP 相关的入侵事件。
`21-25`	返回端口 21 到 25 上的所有事件。

搜索中的事件字段

当搜索事件时，可以使用以下字段作为搜索条件：

- 审核日志工作流程字段
- 应用数据字段
- 应用详细信息数据字段

- 捕获文件字段
- 允许 名单事件字段
- 连接和 安全情报 事件字段
- 关联事件字段
- 发现事件字段
- 运行状况事件表
- 主机属性数据字段
- 主机数据字段
- 文件和恶意软件事件字段
- 入侵事件字段
- 入侵规则更新日志中的字段
- 补救状态表字段
- 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 *Nmap* 扫描结果字段
- 服务器数据字段
- 第三方漏洞数据字段
- 用户相关字段
- 漏洞数据字段
- 允许 列表违规事件字段

执行搜索

您必须具有管理员或安全分析师权限才能执行搜索。

过程

步骤 1 选择 **分析** > **搜索**。

提示 也可以点击工作流程中任何页面上的**搜索 (Search)**。

步骤 2 从表下拉列表中，选择想搜索的事件或数据的类型。

步骤 3 在相应的字段中输入搜索条件。请参阅以下各节，了解有关可使用的搜索条件的详细信息：

- 搜索限制，第 1 页
- 审核日志工作流程字段

- 应用数据字段
- 应用详细信息数据字段
- 捕获文件字段
- 允许 名单事件字段
- 连接和 安全情报 事件字段
- 关联事件字段
- 发现事件字段
- 运行状况事件表
- 主机属性数据字段
- 主机数据字段
- 文件和恶意软件事件字段
- 入侵事件字段
- 入侵规则更新日志中的字段
- 补救状态表字段
- 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的 *Nmap* 扫描结果字段
- 服务器数据字段
- 第三方漏洞数据字段
- 用户数据字段
- 用户活动数据字段
- 漏洞数据字段
- 允许 列表违规事件字段

步骤 4 如果要在以后再次使用搜索，请保存搜索，如保存搜索 ， 第 8 页中所述。

步骤 5 点击**搜索 (Search)** 开始搜索。搜索结果出现在正在搜索的表的默认工作流程中，受时间约束（如适用）。

下一步做什么

- 要使用工作流程分析搜索结果，请参阅使用工作流程。

相关主题

配置事件视图设置

保存搜索

您必须具有管理员或安全分析师权限才能保存搜索。

在多域部署中，系统会显示在当前域中创建的已保存搜索，您可以对其进行编辑。系统还会显示在祖先域中创建的已保存搜索，您不可以对其进行编辑。要查看和编辑在较低域中创建的搜索，请切换至该域。

开始之前

- 建立搜索条件（如执行搜索，第 6 页中所述）或加载已保存的搜索（如加载已保存的搜索，第 8 页中所述）。

过程

步骤 1 从“搜索”(Search) 页面中，如果要将搜索另存为专用，以便只有您才能对搜索进行访问，请选中**专用 (Private)** 复选框。

提示 如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 2 此时您有两种选择：

- 如果要保存已加载搜索的新版本，请点击**另存为新项目 (Save As New)**。
- 如果要保存新搜索或使用同一名称覆盖自定义搜索，请点击**保存 (Save)**。如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

加载已保存的搜索

您必须具有管理员或安全分析师权限才能载入已保存的搜索。

在多域部署中，系统会显示在当前域中创建的已保存搜索，您可以对其进行编辑。系统还会显示在祖先域中创建的已保存搜索，您不可以对其进行编辑。要查看和编辑在较低域中创建的搜索，请切换至该域。

过程

步骤 1 选择**分析** > **搜索**。

提示 也可以点击工作流程中任何页面上的**搜索 (Search)**。

步骤 2 从表下拉列表中，选择要搜索的事件或数据的类型。

步骤 3 从**自定义搜索 (Custom Searches)** 列表或**预定义搜索 (Predefined Searches)** 列表中选择要加载的搜索。

步骤 4 如果要使用其他搜索条件，请更改搜索限制。

步骤 5 如果要在以后再次使用更改的搜索，请保存搜索，如保存搜索，第 8 页中所述。

步骤 6 单击**搜索 (Search)**。

通过外壳查询覆盖

系统管理员可以使用 Linux 基于外壳的查询管理工具找到和停止长期查询。

借助于查询管理工具，可找到并停止运行时间超过指定分钟数的查询。停止查询时，此工具会将事件记入审计日志和系统日志。

请注意， 管理员 内部用户可以访问 FMC CLI。如果使用授予 CLI 访问权限的外部身份验证对象，匹配外壳访问过滤器的用户也可以登录 CLI。

注释 退出 Web 界面的搜索页面不会停止查询。需要很长时间才返回结果的查询在运行时会影响总体系统性能。

基于外壳的查询管理语法

使用以下语法管理长期运行的查询：

```
query_manager [-v] [-l [minutes]] [-k query_id [...]] [--kill-all minutes]
```

表 5: `query_manager` 选项

选项	说明
`-h, --help`	打印简短的帮助消息。
`-l, --list [minutes]`	列出所有运行时间超过已用分钟数的查询。默认情况下，将显示所有运行时间超过 1 分钟的查询。
`-k, --kill query_id [...]`	通过传入 ID 终止查询。该选项可使用多个 ID。
`--kill-all minutes`	终止所有运行时间超过已用分钟数的查询。
`-v, --verbose`	包含完整 SQL 查询的详细输出。

注意 出于系统安全原因，思科强烈建议您不要在任何设备上建立其他 Linux 外壳用户。

停止长期查询

您必须是 **管理员** 用户或具有 CLI 访问权限的外部身份验证用户

过程

步骤 1 通过 `ssh` 连接至Cisco Secure Firewall Management Center。

步骤 2 发出命令 `专家` 以访问 Linux 外壳。

步骤 3 使用基于外壳的查询管理语法，第 9 页中所述的语法在 `sudo` 下运行 `query_manager`。

搜索事件的历史记录

特性	版本	详细信息
许多字段中的部分匹配搜索现在需要通配符	6.6	例如，搜索 URL 时，请使用 **`*example.com*`** 查找 **`example.com`** 的所有变量。 在搜索连接或安全情报事件时，此行为更改适用于 **分析 > 搜索** 页面上的搜索。也可以通过其他页面上的链接访问此搜索页面。 在不需要使用通配符进行部分匹配搜索的字段中，可以选择使用通配符。 受影响的平台：FMC

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。