Context Explorer

以下主题介绍如何在 Firepower 系统中使用情景管理器：

关于情景管理器

Firepower 系统情景管理器在情景中显示有关受监控网络状态的详细、交互图形信息，包括有关应用、应用统计、连接、地理位置、危害表现、入侵事件、主机、服务器、安全情报、用户、文件（包括恶意软件文件）和相关URL的数据。不同部分以生动的曲线图、条形图、饼状图和环状图方式显示这些数据，附有详细列表。第一部分是随着时间推移的流量和事件计数曲线图，提供网络活动的最新趋势一览图。

可轻松创建和应用自定义过滤器以微调分析；此外，点击图形区域或将光标悬停在图形区域，还可更详细地查看各数据部分。还可配置情景管理器的时间范围，以反映短至前一小时或长至上一年的时间段。只有具备管理员、安全分析师或安全分析师（只读）用户角色的用户才能访问情景管理器。

Firepower 系统控制面板可自定义、分区且可实时更新。相反，情景管理器需手动更新，以便为其数据提供更广泛的上下文，而且拥有单一且一致的布局，以供活跃用户浏览。

可根据自己的特定需求使用控制面板监控网络和设备上的实时活动。相反，可用情景管理器在特别详细和清晰的情景中调查一组预定义的最新数据：例如，如果注意到网络中只有 15% 的主机在使用 Linux，但却占据了几乎所有的 YouTube 流量，则可快速应用过滤器查看仅适合 Linux 主机的数据和/或 YouTube 关联的应用数据。与紧凑、狭小的控制面板构件不同，情景管理器部分旨在以对 Firepower 系统的专家和普通用户均有效的格式醒目再现的系统活动。

显示的数据取决于您如何许可和部署受管设备以及是否配置提供数据的功能等因素。也可以应用过滤器限制所有情景管理器部分中显示的数据。

在多域部署中，在祖先域中查看数据时，情景管理器会显示所有子域的汇聚数据。在枝叶域中，只能查看特定于该域的数据。

控制面板和情景管理器之间的区别

下表概述控制面板与情景管理器之间的一些主要区别。

表 *1:* 比较：控制面板与情景管理器

功能	控制面板	Context Explorer
可显示数据	Firepower 系统监控的任何内容	应用、应用统计、地理定位、主机危害表现、入侵事件、文件（包括恶意软件文件）、主机、安全情报事件、服务器、用户和 URL
可自定义性	• 控制面板构件的选择可自定义 • 可按不同程度自定义各个构件	• 不能改变基本布局 • 应用的过滤器显示在情景管理器 URL 中且可标上书签供以后使用
数据更新频率	自动（默认）；用户配置的频率	手动
数据过滤	可用于某些构件（必须编辑构件首选项）	可用于情景管理器的所有部分，可支持多个过滤器
图形上下文	某些构件（特别是“自定义分析”[Custom Analysis]）可以图形方式显示数据	所有数据的广泛图形上下文，包括特别详细的环状图
链接到相关 Web 界面页面	在某些构件中	在每个部分
已显示数据的时间范围	用户配置	用户配置

相关主题

关于控制面板

“流量和入侵事件计数时间”图形

情景管理器顶部有一个随时间推移的流量和入侵事件曲线图。X 轴标绘时间间隔（从五分钟到一个月不等，取决于选定的时窗）。Y 轴以千字节标绘流量（蓝线）和入侵事件计数（红线）。

请注意，最小的 X 轴间隔为五分钟。为满足此要求，系统将在选定的时间范围内将起点和终点四舍五入至最近的五分钟间隔。

在默认情况下，此部分显示选定时间范围内的所有网络流量和生成的所有入侵事件。如果应用过滤器，该图表会改为仅显示与过滤器中指定条件相关联的流量和入侵事件。例如，过滤 `Windows` 的**操作系统名称 (OS Name)** 导致时间图形仅显示与使用 Windows 操作系统的主机相关联的流量和事件。

如果过滤情景管理器上的入侵事件数据（例如**优先级 (Priority)** 为 `High`），蓝色流量曲线将隐藏，以便单独突出入侵事件。

将鼠标指针悬停在图形线条的任何点上方，即可查看有关流量和事件计数的确切信息。将鼠标指针悬停在其中一个彩色线条上方，也可将该线条拖至图形前沿，提供更清晰的上下文。

此部分主要从“入侵事件”和“连接事件”表提取数据。

危害表现部分

Context Explorer 的 Indications of Compromise（危害表现）部分包含两个交互部分，提供受监控网络上可能受损主机的全局视图：已触发最常用 IOC 类型的比例视图，以及按已触发指示数量显示的主机视图。

有关 IOC 的详细信息，请参阅危害表现数据。

“按表现划分的主机”图形

“按表现划分的主机”图形以环状图形式显示受监控网络中主机触发的危害表现 (IOC) 的比例视图。内环按 IOC 类别划分的（例如，`CnC Connected` 或 `Malware Detected`），同时，外环进一步按特定事件类型划分数据（例如，`Impact 2 Intrusion Event - attempted-admin` 或 `Threat Detected in File Transfer`）。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“主机”(Hosts) 和“主机危害表现”(Host Indications of Compromise) 表中提取数据。

“按主机划分的表现”图形

“按主机划分的指示”图形以条形图形式显示受监控网络中 15 个 IOC 最活跃的主机触发的独特危害表现 (IOC) 的计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“主机”(Hosts) 和“主机危害表现”(Host Indications of Compromise) 表中提取数据。

网络信息部分

情景管理器的“网络信息”(Network Information) 部分包含六个交互图形，这六个交互图显示受监控网络中连接流量的全局视图：源、目标、用户、与流量关联的安全区域、网络主机使用的操作系统故障细分，以及 Firepower 系统对网络流量执行的访问控制措施的比例视图。

“操作系统”图形

“操作系统”图形以环状图形式显示在受监控网络中主机上检测到的操作系统的比例再现。内环按操作系统名称划分（例如，`Windows` 或 `Linux`），而外环按特定操作系统版本进一步划分该数据（例如，`Windows Server 2008` 或 `Linux 11.x`）。一些密切相关的操作系统（例如，Windows 2000、Windows XP 和 Windows Server 2003）组合在一起。非常罕见或无法识别的操作系统在**其他 (Other)** 下分组。

请注意，无论日期和时间限制如何，此图形均反映所有可用数据。如果更改情景管理器的时间范围，图形不变。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“主机”表提取数据。

“按源 IP 划分的流量”图形

“按源 IP 划分的流量”图形以条形图形式显示受监控网络中前 15 个最活跃源 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个源 IP 地址，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

注释 如果过滤入侵事件信息，“按源 IP 划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

“按源用户划分的流量”图形

“按源用户划分的流量”图形以条形图形式显示受监控网络中前 15 个最活跃源用户的网络流量（千字节每秒）和独特连接的计数。对于列出的每个源 IP 地址，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

注释 如果过滤入侵事件信息，“按源用户划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。它显示授权的用户数据。

“按访问控制操作划分的连接”图形

“按访问控制操作划分的连接”图形以饼图形式显示 Firepower 系统部署已对受监控流量采取的访问控制操作（例如阻止 [Block] 或允许 [Allow]）的比例视图。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

注释 如果过滤入侵事件信息，“按源用户划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

“按目标 IP 划分的流量”图形

“按目标 IP 划分的流量”图形以条形图形式显示受监控网络中前 15 个最活跃目标 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个目标 IP 地址，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

注释 如果过滤入侵事件信息，“按目标 IP 划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

“按入口/出口安全区域划分的流量”图形

“按入口/出口安全区域划分的流量”图形以条形图形式显示受监控网络上配置的每个安全区域的传入或传出网络流量（千字节每秒）和独特连接的计数。您可配置此图形，根据自己的需求显示入口（默认）或出口安全区域的信息。

对于列出的每个安全区域，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图形中的任何部分，即可过滤或向下展开该信息

提示 要限制此图形，使其仅按出口安全区域显示流量，将鼠标指针悬停在图形上方，然后在显示的切换按钮上点击**出口 (Egress)**。点击**入口 (Ingress)** 返回默认视图。请注意，离开情景管理器也会使此图形返回默认“入口”(Ingress) 视图。

注释 如果过滤入侵事件信息，“按入口/出口安全区域划分的流量”图形将隐藏。

此图形主要从“连接事件”表提取数据。

应用信息部分

情景管理器的“应用信息”(Application Information) 部分包含三个交互图形和一个表格式列表，它们显示受监控网络中应用活动的全局视图：流量、入侵事件以及与应用相关联且进一步按分配给每个应用的预估风险或业务关联性排列的主机。“应用详细信息”(Application Details) 列表列出了每个应用及其风险、业务关联性、类别和主机计数的交互列表。

对于此部分的所有“应用”实例，“应用信息”(Application Information) 图形集默认对应用协议（例如 DNS 或 SSH）进行具体检查。您还可配置“应用信息”(Application Information) 部分，具体检查客户端应用（例如 PuTTY 或 Firefox）或 Web 应用（例如 Facebook 或 Pandora）。

关注应用信息部分

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析** > **情景管理器**。

步骤 2 将鼠标指针悬停在 **Application Protocol Information** 部分的上方。

注释 如果之前在同一个情景管理器会话中更改了此设置，该部分标题可能改为显示**客户端应用信息 (Client Application Information)** 或 **Web 应用信息 (Web Application Information)**。

步骤 3 点击 **Application Protocol**、**Client Application** 或 **Web Application**。

“按风险/业务关联性和应用划分的流量”图形

“按风险/业务关联性和应用划分的流量”图形以环状图形式显示在受监控网络上检测到的应用流量的比例再现，这些受监控网络按应用的预估风险（默认值）或预估业务关联性进行排列。内环按预估的风险/业务关联性水平（例如，`Medium`或`High`）划分，而外环按特定应用对数据进行进一步的划分（例如，`SSH` 或 `NetBIOS`）。很少检测到的应用在**其他 (Other)** 下分组。

请注意，无论日期和时间限制如何，此图形均反映所有可用数据。如果更改情景管理器的时间范围，图形不变。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其按业务相关性和应用显示流量，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**业务相关性 (Business Relevance)**。点击**风险 (Risk)** 返回默认视图。请注意，离开情景管理器也会使此图形返回默认“风险”(Risk) 视图。

注释 如果过滤入侵事件信息，“按风险/业务和应用划分的流量”图形将隐藏。

此图形主要从“连接事件”和“应用统计信息”表提取数据。

“按风险/业务关联性和应用划分的入侵事件”图形

“按风险/业务关联性和应用划分的入侵事件”图形以环状图形式显示受监控网络上检测到的入侵事件以及与这些入侵事件相关联的应用的比例再现，这些事件按应用的预估风险（默认值）或预估业务关联性进行排列。内环按预估的风险/业务关联性水平（例如，`Medium`或`High`）划分，而外环按特定应用对数据进行进一步的划分（例如，`SSH` 或 `NetBIOS`）。很少检测到的应用在**其他 (Other)** 下分组。

将鼠标指针悬停在环状图形任何部分的上方，即可查看更详细的信息。点击图形中的任何部分，可过滤或向下展开该信息或（如适用）查看应用信息。

提示 要限制此图形，使其按业务相关性和应用显示入侵事件，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**业务相关性 (Business Relevance)**。点击**风险 (Risk)** 返回默认视图。请注意，离开情景管理器也会使此图形返回默认“风险”(Risk) 视图。

此图形主要从“入侵事件”和“应用统计数据”表提取数据。

“按风险/业务关联性和应用划分的主机”图形

“按风险/业务关联性和应用划分的主机”图形以环状图形式显示受监控网络上检测到的主机以及与这些主机相关联的应用的比例化再现，这些主机按应用的预估风险（默认值）或预估业务关联性进行排列。内环按预估的风险/业务关联性水平（例如，`Medium` 或 `High`）划分，而外环按特定应用对数据进行进一步的划分（例如，`SSH` 或 `NetBIOS`）。非常罕见的应用在**其他 (Other)** 下分组。

将鼠标指针悬停在环状图形任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其按业务相关性和应用显示主机，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**业务相关性 (Business Relevance)**。点击**风险 (Risk)** 返回默认视图。请注意，离开情景管理器也会使此图形返回默认“风险”(Risk) 视图。

此图形主要从“应用”表提取数据。

应用详细信息列表

“应用信息”(Application Information) 部分底端为“应用详细信息列表”(Application Details List)，该表格提供受监控网络上检测到的每个应用的预估风险、预估业务关联性、类别和主机计数信息。应用按关联主机计数的降序列出。

“应用详细信息列表”(Application Details List) 不能排序，但是，可以点击任何表条目过滤或向下展开该信息或（如适用）查看应用信息。此表主要从“应用”(Applications) 表提取数据。

请注意，无论日期和时间限制如何，此列表均反映所有可用数据。如果更改资源管理器的时间范围，列表不变。

安全情报部分

Context Explorer 的“安全情报”部分包含三个交互条形图，这些图显示被安全情报阻止或监控的受监控网络上流量的全局视图。这些图分别按类别、源 IP 地址和目标 IP 地址对相关流量排序；显示流量（每秒千字节数）和适用连接数。

“按类别划分的安全情报流量”图形

“按类别划分的安全情报流量”图形以条形图形式显示受监控网络上的网络流量（千字节每秒）和顶级安全情报类别流量的独特连接的计数。对于列出的每个类别，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按类别划分的安全情报流量”图形将隐藏。

此图形主要从“安全情报事件”表提取数据。

“按源 IP 划分的安全情报流量”图形

“按源 IP 划分的安全情报流量”视图以条形图形式显示受监控网络中安全情报监控流量的顶级源 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个类别，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按源 IP 划分的安全情报流量”图形将隐藏。

此图形主要从“安全情报事件”表提取数据。

“按目标 IP 划分的安全情报流量”图形

“按目标 IP 划分的安全情报流量”图形以条形图形式显示受监控网络中安全情报监控流量的顶级源 IP 地址的网络流量（千字节每秒）和独特连接的计数。对于列出的每个类别，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按目标 IP 划分的安全情报流量”图形将隐藏。

此图形主要从“安全情报事件”表提取数据。

入侵信息部分

Context Explorer 的 Intrusion Information 部分包含六个交互图形和一个表格式列表，它们显示受监控网络中入侵事件的全局视图：影响级别、攻击源、目标、用户、优先级、与入侵事件关联的安全区域，以及入侵事件分类、优先级和计数的详细列表。

“按影响划分的入侵事件”图形

“按影响划分的入侵事件”图形以饼状图形式显示受监控网络上入侵事件的比例视图，按预估的影响级别（从 0 - 4）分组。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵检测 (IDS 数据)”和“入侵事件”表提取数据。

“主要攻击者”图形

“主要攻击者”图形以条形图形式显示受监控网络中主要攻击性主机 IP 地址（导致这些事件的地址）的入侵事件的计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵事件”表提取数据。

“主要用户”图形

“主要用户”图形以条形图形式按事件计数显示与最高入侵事件计数关联的受监控网络上的用户。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵检测 (IDS) 用户数据”和“入侵事件”表提取数据。它显示授权的用户数据。

“按优先级划分的入侵事件”图形

“按优先级划分的入侵事件”图形以饼状图形式显示受监控网络中入侵事件的比例视图，按预估的优先级（例如，高 (High)、中 (Medium) 或低 (Low)）分组。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵事件”表提取数据。

“主要目标”图形

“主要目标”图形以条形图形式显示受监控网络中主要目标主机 IP 地址（导致这些事件的连接中的目标）的入侵事件计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

此图形主要从“入侵事件”表提取数据。

“主要入口/出口安全区域”图形

“主要入口/出口安全区域”图形以条形图形式显示与受监控网络上配置的每个安全区域（入口或出口，取决于图形设置）关联的入侵事件计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅按出口安全区域显示流量，将鼠标指针悬停在图形上方，然后在显示的切换按钮上点击**出口 (Egress)**。点击**入口 (Ingress)** 返回默认视图。请注意，离开情景管理器也会使此图形返回默认“入口”(Ingress) 视图。

此图形主要从“入侵事件”表提取数据。

您可配置此图形，根据自己的需求显示入口（默认）或出口安全区域的信息。

入侵事件详细信息列表

“入侵信息”(Intrusion Information) 部分的底端为“入侵事件详细信息”列表，该表格提供了受监控网络上检测到的每个入侵事件的分类、预估优先级和事件计数信息。这些事件按事件计数降序列出。

“入侵事件详细信息”列表不能排序，但是，可点击任何表条目过滤或向下展开该信息。此表主要从“入侵事件”表提取数据。

文件信息部分

Context Explorer 的 Files Information 部分包含六个交互图形，它们显示受监控网络上的文件和恶意事件的全局视图。

五个图形显示恶意软件防护（以前称为面向 Firepower 的 AMP）相关的数据：网络流量中检测到的文件的文件类型、文件名和恶意软件处置情况，以及发送（上传）和接收（下载）这些文件的主机。最终图形显示在您的组织中检测到的所有恶意软件威胁，无论是由恶意软件防护 还是面向终端的 AMP 检测到。

注释 如果过滤入侵信息，整个 Files Information 部分将隐藏。

“主要文件类型”图形

“主要文件类型”图形以饼状图形式显示网络流量中检测到的文件类型的比例视图（外环），按文件类别（内环）分组。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

请注意，您必须具有 恶意软件防御 许可证才能使此图形显示 恶意软件防护 数据。

此图形主要从“文件事件”表提取数据。

“主要文件名”图形

“主要文件名”图形以条形图形式显示网络流量中检测到的主要独特文件名的计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

请注意，您必须具有 恶意软件防御 许可证才能使此图形显示 恶意软件防护 数据。

此图形主要从“文件事件”表提取数据。

“按处置情况划分的文件”图形

“主要文件类型”图形以饼状图形式显示恶意软件防护 功能检测到的文件恶意软件处置情况的比例视图。请注意，只有 Cisco Secure Firewall Management Center对其执行恶意软件云查找的文件才具有处置情况。未触发云查找的文件性质为 `N/A`。`Unavailable` 性质表示Cisco Secure Firewall Management Center无法执行恶意软件云查找。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

请注意，您必须具有 恶意软件防御 许可证才能使此图形显示 恶意软件防护 数据。

此图形主要从“文件事件”表提取数据。

“发送文件的主要主机”图形

“发送文件的主要主机”图形以条形图形式显示网络流量中检测到的主要文件发送主机 IP 地址的文件数量计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示发送恶意软件的主机，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**恶意软件 (Malware)**。点击**文件 (Files)** 以返回默认文件视图。请注意，离开情景管理器也会使此图形返回默认文件视图。

请注意，您必须具有 恶意软件防御 许可证才能使此图形显示 恶意软件防护 数据。

此图形主要从“文件事件”表提取数据。

“接收文件的主要主机”图形

“接收文件的主要主机”图形以条形图形式显示网络流量中检测到的主要文件接收主机 IP 地址的文件数量计数。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示接收恶意软件的主机，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**恶意软件 (Malware)**。点击**文件 (Files)** 以返回默认文件视图。请注意，离开情景管理器也会使此图形返回默认文件视图。

请注意，您必须具有 恶意软件防御 许可证才能使此图形显示 恶意软件防护 数据。

此图形主要从“文件事件”表提取数据。

“主要恶意软件检测”图形

“主要恶意软件检测”图形以条形图形式显示在您的组织中检测到的主要恶意软件威胁的计数，无论是由 恶意软件防护 还是由 Cisco Secure EndpointSecure Endpoint进行检测。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

请注意，您必须具有 恶意软件防御 许可证才能使此图形显示 恶意软件防护 数据。

此图形主要从“文件事件”和“恶意软件事件”表提取数据。

地理位置信息部分

Context Explorer 的 Geolocation Information 部分包含三个交互环状图形，它们显示与受监控网络上主机交换数据的国家/地区的全局视图：发起方或响应方国家/地区的独特连接、按源或目标国家/地区划分的入侵事件以及按发送或接收国家/地区划分的文件事件。

“按发起方/响应方国家/地区划分的连接”图形

甜甜圈形的“按发起方/响应方国家/地区划分的连接”图形显示了一幅作为发起方（默认值）或响应方参与您网络上的连接的国家/地区的比例视图。内环将这些国家/地区按大陆组合。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示作为连接响应方的国家/地区，将鼠标指针悬停在图形上方，然后在显示的切换按钮上，点击**响应方 (Responder)**。点击**发起方 (Initiator)** 返回默认视图。请注意，离开 Context Explorer 也会使此图形返回默认“发起方”(Initiator) 视图。

此图形主要从“连接摘要数据”表提取数据。

“按源/目标国家/地区划分的入侵事件”图形

“按源/目标国家/地区划分的入侵事件”图形以环状图形式显示作为事件（默认值）或目标来源的网络上入侵事件涉及的国家/地区的比例视图。内环将这些国家/地区按大陆组合。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示作为入侵事件目标的国家/地区，将鼠标指针悬停在图形上方，然后在显示的切换按钮上，点击**目标 (Destination)**。点击**源 (Source)** 以返回默认视图。请注意，离开情景管理器也会使此图形返回默认“源”(Source) 视图。

此图形主要从“入侵事件”表提取数据。

“按发送/接收国家/地区划分的文件事件”图形

“按发送/接收国家/地区划分的文件事件”图形以环状图形式显示网络上文件事件中检测到作为发送（默认值）或接收文件的国家/地区的比例视图。内环将这些国家/地区按大陆组合。

将鼠标指针悬停在图形中任何部分的上方，即可查看更详细的信息。点击图表中的任何部分，即可过滤或向下展开该信息。

提示 要限制此图形，使其仅显示接收文件的国家/地区，请将鼠标指针悬停在此图形上方，然后在所显示的切换按钮上，点击**接收方 (Receiver)**。点击**发送方 (Sender)** 返回默认视图。请注意，离开情景管理器也会使此图形返回默认“发送方”(Sender) 视图。

此图形主要从“文件事件”表提取数据。

URL 信息部分

Context Explorer 的“URL 信息”(URL Information) 部分包含三个交互条形图形，它们显示与受监控网络上主机交换数据的 URL 的全局视图：与 URL 相关联、按单个 URL、 URL 类别和 URL 声誉排序的流量和独特连接。不能过滤 URL 信息。

注释 如果过滤入侵事件信息，整个“URL 信息”(URL Information) 部分将隐藏。

请注意，您必须具有 URL 过滤 可证才能使此图形包含 URL 类别和信誉数据。

“按 URL 划分的流量”图形

“按 URL 划分的流量”图形以条形图形式显示受监控网络中请求最频繁的 15 个 URL 的网络流量（千字节每秒）和独特连接的计数。对于列出的每个 URL，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按 URL 划分的流量”图形将隐藏。

请注意，您必须具有 URL 过滤 可证才能使此图形包含 URL 类别和信誉数据。

此图形主要从“连接事件”表提取数据。

“按 URL 类别划分的流量”图形

“按 URL 类别划分的流量”图形以条形图形式显示受监控网络中请求最频繁的 URL 类别 （例如，搜索引擎 [Search Engines] 和流媒体 [Streaming Media]）的网络流量（千字节每秒）和独特连接的计数。对于列出的每个 URL 类别，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按 URL 类别划分的流量”图形将隐藏。

请注意，您必须具有 URL 过滤 可证才能使此图形包含 URL 类别和信誉数据。

此图形主要从“URL 统计数据”和“连接事件”表提取数据。

“按 URL 信誉划分的流量”图形

“按URL信誉划分的流量”图形以条形图形式显示受监控网络中请求最频繁的URL信誉组（例如，受信任的 或 中立）的网络流量（千字节每秒）和独特连接的计数。对于列出的每个 URL 声誉组，蓝条代表流量数据，红条代表连接数据。

将鼠标指针悬停在图形中任何部分的上方，即可查看详细信息。点击图中的任何部分，即可向下展开该信息。

注释 如果过滤入侵事件信息，“按 URL 声誉划分的流量”图形将隐藏。

请注意，您必须具有 URL 过滤 可证才能使此图形包含 URL 类别和信誉数据。

此图形主要从“URL 统计数据”和“连接事件”表提取数据。

情景管理器的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 安全分析师

刷新情景管理器

情景管理器不会自动更新显示的信息。要更新数据，必须手动刷新情景管理器。

请注意，虽然重新加载情景管理器（通过刷新资源管理器程序或离开，然后返回情景管理器）可刷新所有显示的信息，但此操作不会保留对部分配置做出的任何更改（例如“入口/出口”图形和“应用信息”[Application Information] 部分）且可能导致加载延迟。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析** > **情景管理器**。

步骤 2 点击右上角的**重新加载 (Reload)**。

在刷新完成之前，**重新加载** 按钮呈灰色显示。

设置情景管理器时间范围

可配置情景管理器的时间范围，以反映短至前一小时或长至上一年的时间段。请注意，如果更改时间范围，情景管理器无法自动更新反映所做的更改。要应用新的时间范围，必须手动刷新情景管理器。

即使离开情景管理器或终止登录会话，对时间范围所做的更改也会持续。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析** > **情景管理器**。

步骤 2 从**显示最后时间 (Show the last)** 下拉列表，选择时间范围。

步骤 3 或者，要从新时间范围查看数据，请点击 **Reload**。

提示 点击 **Apply Filters** 也可应用任何时间范围更新。

最小化和最大化情景管理器部分

可最小化和隐藏情景管理器的一个或多个部分。如要仅重点关注某些部分，或如果想要更简单的视图，此操作很有用。不能最小化“流量和入侵事件计数时间”图形。

即使刷新页面或注销设备，情景管理器部分仍会保持处于配置的最小化或最大化状态。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析** > **情景管理器**。

步骤 2 要最小化某个部分，请点击部分的标题栏中的 **折叠箭头** （ ） 。

步骤 3 要最大化某个部分，请点击最小化部分的标题栏中的最大化 **展开箭头** （ ） 。

向下展开情景管理器数据

如果想要超出 Context Explorer 允许的范围，更详细地检查图形和列表数据，可向下展开相关数据的表视图。（请注意，不能向下展开“随时间推移的流量和入侵事件”[Traffic and Intrusion Events over Time] 图形。）例如，向下展开“按源 IP 划分的流量”(Traffic by Source IP) 图形中的 IP 地址可显示“连接事件”(Connection Events) 表的“具有应用详细信息的连接”(Connections with Application Details) 视图，仅包括与所选源 IP 地址关联的数据。

视乎要检查的数据类型，情景菜单中会显示其他选项。与特定 IP 地址相关联的数据点提供的选项可用于查看有关所选 IP 地址的主机或域名信息。与特定应用相关联的数据点提供的选项可用于查看有关所选应用的应用信息。与特定用户相关联的数据点提供的选项可用于查看该用户的用户配置文件页。与入侵事件消息相关联的数据点提供了查看与该事件相关联的入侵规则的规则文档的选项，与特定IP地址相关联的数据点提供了将该地址添加到阻止或不阻止列表的选项。有关这些列表的详细信息，请参阅 全局和域安全情报列表 。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析** > **情景管理器**。

步骤 2 在除 **随时间推移的流量和入侵事件**以外的任何部分中，点击要调查的数据点。

步骤 3 视乎所选数据点，系统提供多个选项：

- 要在表视图中查看此数据的更多详细信息，请选择**深入分析 (Drill into Analysis)**。
- 如果选择了与特定 IP 地址相关联的数据点并要查看有关关联主机的详细信息，请选择**查看主机信息 (View Host Information)**。
- 如果选择了具有特定 IP 地址的数据点并要对该地址执行 whois 搜索，请选择 **Whois**。
- 如果选择了与特定应用相关联的数据点并要查看有关该应用的详细信息，请选择**查看应用信息 (View Application Information)**。
- 如果选择了与特定用户相关联的数据点并要查看有关该用户的详细信息，请选择**查看用户信息 (View User Information)**。
- 如果选择了与特定入侵事件消息相关联的数据点并要查看有关关联入侵规则的详细信息，请选择**查看规则文档**；或者，然后点击**规则文档**，以查看更具体的规则详细信息
- 如果您选择了与特定IP地址关联的数据点，并希望将该IP地址添加到安全情报全局阻止或不阻止列表，请选择适当的选项。

情景管理器中的过滤器

除了 Context Explorer 初始显示的基本、广泛数据外，可选择为网络中活动的更精细的上下文照片过滤该数据。过滤器包含除 URL 信息外的所有类型 Firepower 系统数据，支持排除和纳入，点击情景管理器图形数据点即可快速应用，并影响整个管理器。可以一次应用最多 20 个过滤器。

过滤器可以通过多种方式添加至 Context Explorer 数据：

- 从“添加过滤器”(Add Filter) 对话框添加
- 在管理器中选择一个数据点时，从情景菜单添加
- 从特定详细信息视图页面（“应用详细信息”[Application Detail]、“主机配置文件”[Host Profile]、“规则详细信息”[Rule Detail] 和“用户配置文件”[User Profile]）显示的文本链接添加。点击这些链接，根据详细信息视图页面的相关数据自动打开并过滤情景管理器。例如，点击一个用户详细信息页面上的情景管理器以便用户 `jenkins` 限制管理器仅显示与该用户相关的数据。

某些过滤器类型与其他类型不兼容：例如，与入侵事件相关的过滤器（例如，**设备 [Device]** 和**内联结果 [Inline Result]**）无法与连接事件相关的过滤器（例如，**访问控制操作 (Access Control Action)**）同时应用，因为系统无法按入侵事件数据对连接事件数据进行排序。系统将自动阻止同时应用不兼容过滤器；只要存在不兼容性，当一个过滤器类型最近被激活时，不兼容的过滤器会被隐藏。

当多个过滤器活跃时，同一种数据类型的值被视为 OR 搜索条件：将出现至少与其中一个值相匹配的所有数据。不同数据类型的值被视为 AND 搜索条件：显示至少与每种过滤数据类型相匹配的数

据。例如，为 Application: 2channel、Application: Reddit 和 User: edickinson 的过滤器集显示的数据必须与用户 edickinson **和** 应用2channel **或**应用 Reddit 相关联。

在多域部署中，当查看祖先域中的情景管理器时，可以通过多个后代域来过滤。在这种情况下，还添加 **IP 地址 (IP Address)** 过滤器时，要特别注意。系统会为每个枝叶域构建单独的网络映射。使用文字 IP 地址限制此配置可能会出现意外结果。

请注意，显示的数据取决于您如何许可和部署受管设备以及是否配置提供数据的功能等因素。

注释 过滤器用作一种简单、灵活的工具，可在任何指定时间获取准确的Firepower数据情景。过滤器不用作永久性配置设置，在离开 Context Explorer 或结束会话时会消失。要保留过滤器设置以备以后使用，请参阅保存过滤的情景管理器视图，第 21 页。

数据类型字段选项

下表列出可用作过滤器的数据类型，并带有每种类型的示例和简要定义。

表 *2:* 过滤器数据类型

类型	示例值	定义
访问控制操作 (Access Control Action)	Allow、Block	访问控制策略为允许或阻止流量而采取的操作。
应用类别 (Application Category)	web browser、email	应用的最基本功能的一般分类。
应用名称	Facebook、HTTP	应用的名称。
应用风险	Very High、Medium	应用的预计安全风险
应用标记 (Application Tag)	encrypts communications、sends mail	有关应用的其他信息；应用可以具有任意数量的标记，包括无任何标记。
应用类型	Client、Web Application	应用的类型：应用协议、客户端或 Web 应用。
业务相关性	Very Low、High	应用与业务活动的预计关联性（与娱乐相对）。
大陆 (Continent)	North America、Asia	与受监控网络上检测到的可路由IP地址相关联的大陆。
国家/地区	Canada、Japan	与受监控网络上检测到的可路由 IP 地址相关联的国家/地区。
设备	device1.example.com, 192.168.1.3	受监控网络上的设备的名称或 IP 地址。
域	Asia Division、Europe Division	要绘制网络活动图表的设备的域。此数据类型只存在于多域部署中。

类型	示例值	定义
事件分类 (Event Classification)	`Potential Corporate Policy Violation`、`Attempted Denial of Service`	入侵事件的概要说明，由触发该事件的规则、解码器或预处理器的分类确定。
事件消息 (Event Message)	`dns response`、`P2P`	事件生成的消息，由触发该事件的规则、解码器或预处理器确定。
文件性质 (File Disposition)	`Malware`、`Clean`	Cisco Secure Firewall Management Center对其执行了恶意软件云查找的文件的处置情况。
文件名	`Packages.bz2`	网络流量中检测到的文件的名称。
文件 SHA256	任何 32 位字符串	Cisco Secure Firewall Management Center对其执行了恶意软件云查找的文件的 SHA-256 散列值。
文件类型	`GZ`、`SWF`、`MOV`	网络流量中检测到的文件类型。
文件类型类别 (File Type Category)	`Archive`、`Multimedia`、`Executables`	网络流量中检测到的文件类型的一般类别。
IP 地址	`192.168.1.3`、`2001:0db8:85a3::0000/24`	IPv4 或 IPv6 地址、地址范围或地址块。 请注意，搜索 IP 地址时可返回事件，其中，该地址是事件的源或目标。
影响级别 (Impact Level)	`Impact Level 1`、`Impact Level 2`	受监控网络上的事件的预计影响。
内联结果	`dropped`、`would have dropped`	流量是已丢弃、应已丢弃还是未由系统处理
IOC 类别 (IOC Category)	`High Impact Attack`、`Malware Detected`	已触发的危害表现 (IOC) 事件的类别。
IOC 事件类型 (IOC Event Type)	`exploit-kit`, `malware-backdoor`	与特定危害表现 (IOC) 相关联的标识符，指代触发该标识符的事件。
恶意软件威胁名称 (Malware Threat Name)	`W32.Trojan.a6b1`	恶意软件威胁的名称。
OS 名称 (OS Name)	`Windows`、`Linux`	操作系统的名称。
OS 版本	`XP`, `2.6`	操作系统的特定版本。
优先级	`high`、`low`	事件的预计紧急程度。
安全情报类别 (Security Intelligence Category)	`Malware`、`Spam`	危险流量的类别，由安全情报确定。
安全区	`My Security Zone`、`Security Zone X`	接口集，流量通过其进行分析，并在内联部署中传递

类型	示例值	定义
SSL	yes、no	SSL 或 TLS 加密流量。
用户	wsmith、mtwain	登录到受监控网络上的主机的用户的身份。

从“添加过滤器”(Add Filter) 窗口新建过滤器

使用此程序，通过“添加过滤器”(Add Filter) 窗口从头开始创建过滤器。（也可以使用情景菜单创建快速过滤器。）

点击情景管理器左上方的 **过滤器** 下的 **加号**（+） 即可访问的“添加过滤器”窗口，该窗口仅包含两个字段：

- **数据类型 (Data Type)** 下拉列表包含许多可用于限制情景管理器的不同类型的 Firepower 系统数据。选择一个数据类型后，在**过滤器 (Filter)** 字段为该类型输入一个特定的值（例如，为类型**大洲 [Continent]** 输入一个值亚洲 [Asia]）。为了便于操作，“过滤器”(Filter) 字段将所选数据类型提供多个灰显示例值。（在该字段中输入数据时，这些示例值将被擦除。）
- 在**过滤器 (Filter)** 字段中，可以输入特殊搜索参数，例如，* 和 !，本质上与事件搜索中一致。可以通过为过滤器参数加上 ! 符号作为前缀来创建排斥过滤器。

注释 添加的过滤器不会自动应用；必须点击**应用过滤器 (Apply Filters)** 才能查看情景管理器中的过滤内容。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析** > **情景管理器**。

步骤 2 在左上角的 **过滤器** 下，点击 **加号**（+）。

步骤 3 从**数据类型 (Data Type)** 下拉列表中，选择要过滤的数据类型。

步骤 4 在**过滤器 (Filter)** 字段中，输入要过滤的数据类型值。

步骤 5 点击 **OK**。

步骤 6 或者，请重复以上步骤添加更多的过滤器，直至添加完所需的过滤器集。

步骤 7 点击 **Apply Filters**。

相关主题

数据类型字段选项，第 18 页
搜索限制

从情景菜单创建快速过滤器

浏览情景管理器图形和列表数据时，可点击数据点，然后使用上下文菜单根据该数据快速创建一个过滤器（包容性或排除性）。如用上下文菜单过滤“应用”、“用户”或“入侵事件消息”数据类型的信息，或任何单个主机，则过滤器构件包括一个构件信息，该图标链接至该数据类型（例如应用数据的“应用详细信息”）的相关详细信息页面。请注意，不能过滤 URL 数据。

上下文菜单还可用于更详细地调查特定图形或列表数据。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析** > **情景管理器**。

步骤 2 在资源管理器的任何部分（“随时间推移的流量和入侵事件”部分或包含URL数据的部分除外），点击要过滤的数据点。

步骤 3 此时您有两种选择：

- 要为该数据添加一个过滤器，请点击**添加过滤器 (Add Filter)**。
- 要为该数据添加一个排除过滤器，请点击**添加排除过滤器 (Add Exclude Filter)**。应用后，该过滤器显示与排除值**不**关联的所有数据。排除过滤器的过滤器值之前显示一个感叹号 (!)。

保存过滤的情景管理器视图

要在离开情景管理器或结束会话后在情景管理器中保留过滤设置，请使用所应用的首选过滤器创建情景管理器的浏览器书签。由于已应用的过滤器已纳入Context Explorer页面URL，加载该页面的书签也会加载相应的过滤器。

过程

使用所应用的首选过滤器创建情景管理器的浏览器书签。

查看过滤器数据

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析** > **情景管理器**。

步骤 2 在任何符合条件的过滤器构件上，点击 **信息** 。

删除过滤器

过程

步骤 1 选择**分析** > **情景管理器**。

步骤 2 在左上方的 **过滤器** 下，单独点击 **关闭**（×） 以删除过滤器构件。

提示 如果要一次性删除所有过滤器，可点击 **清除**按钮。

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。