FireSIGHT 系统数据库访问指南

版本 5.4
9 25, 2015

Cisco Systems, Inc.
www.cisco.com
思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices。

目 录

简介

通过 FireSIGHT 系统® 数据库访问功能，您可以使用支持 JDBC SSL 连接的第三方客户端，在思科防御中心上查询入侵、发现、用户活动、关联、连接、漏洞和应用与 URL 统计数据库表。

您可以使用 Crystal Reports、Actuate BIRT 或 JasperSoft iReport 等行业标准报告工具来设计和提交查询。或者，您还可以配置自己的自定义应用，在程序控制下查询思科数据。例如，您可以创建 servlet 来定期报告入侵和发现事件数据或刷新警报控制面板。

请注意，您可以使用一个客户端连接多个防御中心但是必须逐个配置对每个防御中心的访问。

决定连接至哪一台设备或哪些设备时，请记住，在思科设备上查询数据库会减少可用的设备资源。您应根据贵组织的优先级，不时仔细设计并提交查询。

有关详细信息，请参阅以下各节：

- 版本 5.4 中数据库访问的重大更改，第 1-9 页
- 先决条件，第 1-12 页
- 我应该从哪里开始？，第 1-14 页

版本 5.4 中数据库访问的重大更改

如果您将 FireSIGHT 系统部署从 5.3.1 版本升级至 版本 5.4，请注意以下变更，其中某些变更可能要求您更新查询。

版本 5.4 已修改的字段

`fireamp_event` 和 `file_event` 中的 `file_name` 字段可以包含 UTF-8 字符。

版本 5.4 已修改的表

下表列出对 版本 5.4 中数据库访问表的更改。

表 1-1　　版本 5.4 中表的更改摘要

表	更改说明
application_host_map，第 6-4 页	已弃用的 application_tag_id 字段
connection_log，第 7-1 页	已添加以下字段： • access_control_policy_uuid • cert_valid_start_date • cert_valid_end_date • network_analysis_policy_name • network_analysis_policy_UUID • ssl_actual_action • ssl_cipher_suite • ssl_expected_action • ssl_flow_flags • ssl_flow_messages • ssl_flow_status • ssl_issuer_common_name • ssl_issuer_country • ssl_issuer_organization • ssl_issuer_organization_unit • ssl_policy_action • ssl_policy_name • ssl_policy_reason • ssl_rule_action • ssl_rule_name • ssl_serial_number • ssl_server_name • ssl_subject_common_name • ssl_subject_country • ssl_subject_organization • ssl_subject_organization_unit • ssl_url_category • ssl_version

表 1-1　　版本 5.4 中表的更改摘要（续）

表	更改说明
si_connection_log，第 7-13 页	已添加以下字段： • access_control_policy_uuid • cert_valid_start_date • cert_valid_end_date • network_analysis_policy_name • network_analysis_policy_UUID • ssl_actual_action • ssl_cipher_suite • ssl_expected_action • ssl_flow_flags • ssl_flow_messages • ssl_flow_status • ssl_issuer_common_name • ssl_issuer_country • ssl_issuer_organization • ssl_issuer_organization_unit • ssl_policy_action • ssl_policy_name • ssl_policy_reason • ssl_rule_action • ssl_rule_name • ssl_serial_number • ssl_server_name • ssl_subject_common_name • ssl_subject_country • ssl_subject_organization • ssl_subject_organization_unit • ssl_url_category • ssl_version
file_event，第 10-1 页	已添加以下字段： • cert_valid_start_date • cert_valid_end_date • ssl_issuer_common_name • ssl_issuer_country • ssl_issuer_organization • ssl_issuer_organization_unit • ssl_serial_number • ssl_subject_common_name • ssl_subject_country • ssl_subject_organization • ssl_subject_organization_unit

表 1-1　　版本 5.4 中表的更改摘要（续）

表	更改说明
fireamp_event，第 3-2 页	已添加以下字段： • cert_valid_start_date • cert_valid_end_date • ssl_issuer_common_name • ssl_issuer_country • ssl_issuer_organization • ssl_issuer_organization_unit • ssl_serial_number • ssl_subject_common_name • ssl_subject_country • ssl_subject_organization • ssl_subject_organization_unit
intrusion_event，第 4-1 页	已添加以下字段： • access_control_policy_UUID • network_analysis_policy_name • network_analysis_policy_UUID

先决条件

您必须满足以下各节列出的先决条件，然后才能使用数据库访问功能：

- 许可，第 1-12 页
- FireSIGHT 系统功能和术语，第 1-12 页
- 通信端口，第 1-13 页
- 客户端系统，第 1-13 页
- 查询应用，第 1-13 页
- 数据库查询，第 1-13 页

许可

安装任意思科许可证之后，就可以查询外部数据库。但是，某些表是与许可的功能关联的。只有在安装了相应思科许可证并且已将部署配置为生成数据的情况下，这些表才会填充数据。如果您查询这些表，但并未安装关联的思科许可证，就检索不到结果。有关许可的详细信息，请参阅《*FireSIGHT 系统用户指南*》中的“了解许可”。

FireSIGHT 系统功能和术语

要了解此指南中的信息，您应熟悉 FireSIGHT 系统的功能和术语以及其组件的功能。您应熟悉这些组件生成的不同类型的事件数据。请注意，您可以经常从《*FireSIGHT 系统用户指南*》获取不熟悉的或产品特定的术语的定义。此用户指南还包含关于本指南中记录的字段中的数据的其他信息。

通信端口

FireSIGHT 系统要求使用具体端口在设备间进行内外部通信，以及在网络部署内启用特定功能。

您在防御中心上启用数据库访问之后，系统会使用端口 1500 和 2000 进行连接，在客户端和设备之间传输 JDBC 流量。

客户端系统

在需要用来连接至思科数据库的计算机上，必须安装 Java 软件，其又称作 Java 运行时环境 (JRE) 或 Java 虚拟机 (JVM)。您可从 `http://java.com/` 下载最新版本的 Java。

您必须从防御中心下载并解压缩一个包含 JDBC 驱动程序文件的软件包，您将会需要使用此驱动程序文件来连接数据库。该软件包还包含用于安装与防御中心进行加密通信所需的 SSL 证书的可执行文件以及适用于这些实用程序的其他源文件。

您还应了解如何在计算机上更改适用的系统设置，例如环境变量等。

查询应用

要查询思科数据库，您可以使用市售的报告工具，例如 Actuate BIRT、JasperSoft iReport 或 Crystal Reports，或支持 JDBC SSL 连接的任何其他应用（包括自定义应用）。本指南提供连接数据库所需的信息，包括 JDBC URL、驱动程序 JAR 文件、驱动程序类等。但是，您应参考报告工具文档，了解有关如何配置 JDBC SSL 连接的详细说明。

思科还提供一个名为 RunQuery 的示例命令行 Java 应用，您可以使用此应用来测试数据库连接，查看架构以及手动执行基本即席查询。RunQuery 源代码也是在自定义 Java 应用中设置数据库连接的一个参考。RunQuery 源代码包含在您从防御中心下载的 ZIP 软件包中。

RunQuery 只是一个示例客户端，**不是**功能齐全的报告工具。思科**强烈**建议您不要将其用作查询数据库的主要方法。有关使用 RunQuery 的信息，请参阅 ZIP 软件包中包含的 README 文件。

请注意，数据库访问功能仅使用以下 JDBC 功能：

- 数据库元数据，包含架构、版本和支持的功能等信息
- SQL 查询执行

数据库访问不使用任何其他 JDBC 功能，包括存储的程序、事务、批命令、多个结果集或插入/更新/删除功能。

数据库查询

要查询数据库，您应了解如何在单个表上和多个表上使用联合条件构建和执行 `SELECT` 语句。

为了协助您，本指南包含有关所支持的 MySQL 查询语法、思科数据库架构、允许的联合和其他重要的与查询相关的要求和限制的信息。

我应该从哪里开始？

在您满足先决条件，第 1-12 页中说明的先决条件之后，可以开始将您的客户端系统配置为连接至防御中心。

设置数据库访问权限，第 2-1 页解释如何将设备配置为允许访问，如何将客户端系统配置为连接至设备，以及如何将报告应用配置为连接至设备。它还包含一些基本的查询说明和有关所支持的 MySQL 语法的信息。

本指南其余部分包含数据库和示例查询的架构与联合信息，并且划分为以下各章：

- 方案：系统级表，第 3-1 页包含审核日志和运行状况事件等系统级表的架构和联合信息。
- 方案：入侵表，第 4-1 页包含关于与入侵相关的表的架构和联合信息。
- 方案：统计跟踪表，第 5-1 页包含关于应用、URL 和用户统计表的架构和联合信息。
- 方案：发现事件和网络映射表，第 6-1 页包含关于含有发现事件和网络映射信息的表的架构和联合信息，即有关网络资产的信息。
- 方案：连接日志表，第 7-1 页包含关于含有连接事件和连接摘要事件信息的表的架构和联合信息。
- 方案：用户活动表，第 8-1 页包含关于含有用户发现与身份数据的表的架构和联合信息。
- 方案：关联表，第 9-1 页包含关于与关联相关的表的架构和联合信息，包括白名单事件和违规与补救状态数据。
- 方案：文件事件表，第 10-1 页包含关于含有文件事件的表的架构和联合信息。

设置数据库访问权限

要获得对数据库的只读访问权限，必须首先将设备配置为允许访问。然后，您必须从想要访问的设备下载 JDBC 驱动程序并接受 SSL 证书，以便将客户端系统配置为可连接此设备。最后，您必须配置报告应用，使其连接此设备。

注 在设置数据库访问权限之前，您应确保达到先决条件，第 1-12 页中描述的先决条件。

有关详细信息，请参阅以下各节：

决定要访问哪台设备

您可以使用一个客户端连接多台设备，但是必须逐个将每台设备配置为允许访问。

要决定连接哪一台或哪些设备，请记住，设备上的可用数据取决于已安装的许可证以及 FireSIGHT 系统的配置。

以下内容概括说明了查询可能不返回结果的某些具体原因：

- 查询过于具体。例如，您可能需要调整查询的时间范围或 IP 地址范围。
- 根据导致生成事件的网络流量，事件的各个字段不一定都已填充。例如，并非所有连接事件都包含负载信息。
- 设备没有适当的许可证。例如，除非已安装适当的功能许可证，否则网络发现和用户身份相关事件不会记录到数据库中。

- 您尚未将 FireSIGHT 系统配置为记录所查询的事件类型。例如：
  - 记录入侵事件、发现相关事件和运行状况事件要求您应用相应策略。
  - 网络发现事件和主机输入事件的记录可在系统策略中进行配置。请注意，默认情况下，这些事件的记录处于启用状态。
  - 记录用户身份数据需要您配置网络发现。
  - 为入侵事件传输数据包数据需要您在向防御中心添加受管设备时启用该选项。
  - 生成和记录关联事件、合规性白名单事件和补救状态事件需要您向活动的关联策略添加规则或响应。
  - 要记录连接事件，您必须在访问控制规则中启用连接记录，并将其作为访问控制策略中的默认操作。受管设备未接收导致生成事件的网络流量。
  - 在所查询的设备上的系统策略中，数据库限制设置为零。
  - 受管设备未接收导致生成事件的网络流量。

有关如何生成和记录事件的详细信息，请参阅《*FireSIGHT 系统用户指南*》。

创建数据库用户帐户

License: 任意

要配置对 FireSIGHT 系统数据库的访问权限，必须首先创建一个用户帐户并为其分配外部数据库用户权限。您可以通过为此帐户分配一个包含外部数据库用户权限的思科预定义用户角色或贵组织创建的包含外部数据库用户权限的自定义用户角色，来授予此权限。有关创建用户帐户和查看特定用户角色的权限的信息，请参阅《*FireSIGHT 系统用户指南*》。

提示 默认情况下，已分配预定义管理员角色的用户具有外部数据库用户权限。

在本地创建并进行身份验证的外部数据库用户可以在防御中心 Web 界面上更改密码。有关更改密码的信息，请参阅《*FireSIGHT 系统用户指南*》。下表描述可供本地创建的用户管理密码和帐户访问的某些选项。

表 2-1　　用户帐户密码选项

选项	说明
Use External Authentication Method	如果您希望此用户的凭证从外部进行身份验证，请选择此选项。 **注**　如果为用户选择此选项，并且外部身份验证服务器不可用，则该用户可以登录到 Web 界面中，但无法访问任何功能。
Maximum Number of Failed Logins	此项需输入不含空格的整数，用于确定在锁定帐户之前，允许用户连续出现登录尝试失败的最大次数。默认设置为五次尝试；使用 0 可允许无限次的登录失败。
Minimum Password Length	输入不含空格的整数，用于确定用户密码的最小所需长度（以字符数为单位）。默认设置为 8。值为 0 指示无需最小长度。
Days Until Password Expiration	输入用户密码到期之前经过的天数。默认设置为 0，指示密码永不过期。

表 2-1　　用户帐户密码选项（续）

选项	说明
Days Before Expiration Warning	输入在用户密码实际到期之前警告用户必须更改其密码的警告天数。默认设置为 0 天。 ⚠ **注意**　警告天数必须**小于**密码到期之前的天数。
Force Password Reset on Login	选择此选项以强制用户在其首次登录时更改其密码。
Check Password Strength	选择此选项以要求设置强密码。强密码必须为至少八个大小写混合的字母数字字符，并且必须包含至少一个数字字符和一个特殊字符。它不能是字典中出现的单词或包含连续的重复字符。
Exempt from Browser Session Timeout	如果不希望用户的登录会话由于不活动而终止，请选择此选项。具有管理员角色的用户无法获得豁免。

请注意，您可以从外部创建和验证外部数据库用户，在这种情况下，设备从外部存储库检索用户凭证，例如 LDAP 目录服务器或 RADIUS 身份验证服务器。您在外部服务器上管理这些用户的密码设置。有关外部身份验证的详细信息，请参阅《*FireSIGHT 系统用户指南*》。

在防御中心上启用数据库访问权限

License: 任意

在创建外部数据库用户后，必须将防御中心配置为允许访问设备上的数据库，还必须在设备上配置数据库访问列表并添加要查询此外部数据库的所有主机 IP 地址。

要启用数据库访问权限，请执行以下操作：

Access: 管理员

步骤 1　在防御中心上，选择 **System > Local > Configuration**。

步骤 2　点击 **Database**。

系统会显示 Database Settings 菜单。

步骤 3　选择 **Allow External Database Access** 复选框。

系统会显示 **Access List** 字段。

步骤 4　根据第三方应用要求，在 **Server Hostname** 字段中键入防御中心的完全限定域名 (FQDN) 或 IPv4 地址。因为您无法使用 IPv6 地址安装证书，所以无法使用 IPv6 地址。

如果键入 FQDN，必须确保客户端能够解析防御中心的 FQDN。如果键入 IP 地址，必须确保客户端能够连接至使用该 IP 地址的防御中心。

步骤 5　要为一个或多个 IP 地址添加数据库访问权限，请点击 **Add Hosts**。

此时，**Access List** 字段中将会显示 **IP Address** 字段。

步骤 6　在 **IP Address** 字段中，可根据要添加的 IP 地址从以下选项中进行选择：

- 确切的 IPv4 地址（例如 `192.168.1.101`）
- 确切的 IPv6 地址（例如 `2001:DB8::4`）

- 使用 CIDR 表示法的 IP 地址范围（例如 `192.168.1.1/24`）
- 有关在 FireSIGHT 系统中使用 CIDR 的信息，请参阅《*FireSIGHT 系统用户指南*》中的“IP 地址规则”
- `any`，指定任意 IP 地址

步骤 7　点击 **Add**。

IP 地址将添加到数据库访问列表中。

步骤 8　或者，要删除数据库访问列表中的条目，请点击删除图标 ( )。

步骤 9　点击 **Save**。

这样即会保存数据库访问权限设置。

步骤 10　继续执行下一节下载 JDBC 驱动程序中的操作步骤。

下载 JDBC 驱动程序

License: 任意

在创建外部数据库用户并将防御中心配置为允许数据库访问之后，请将 JDBC 驱动程序下载至客户端系统中。您必须使用此 JDBC 驱动程序连接数据库。

要下载 JDBC 驱动程序，请执行以下操作：

Access: 管理员

步骤 1　在防御中心上，选择 **System > Local > Configuration**。

步骤 2　点击 **Database**。

系统会显示 Database Settings 菜单。

步骤 3　点击 **Client JDBC Driver** 旁边的 **Download** 并按照浏览器提示下载 `client.zip` 软件包。

步骤 4　解压缩 ZIP 软件包。请注意位置。
确保保留该软件包的文件结构。
此驱动程序以及其他文件打包于一个 ZIP 文件 (`client.zip`) 内。此软件包包含以下目录：

- `bin`，包含一个称为 RunQuery 的示例客户端以及用于为客户端与防御中心之间的加密通信安装证书的可执行文件
- `lib`，包含 JDBC 驱动程序 JAR 文件
- `src`，包含 `bin` 目录中可执行文件的源代码

步骤 5　继续执行下一节安装客户端 SSL 证书中的操作步骤。

安装客户端 SSL 证书

下载 JDBC 驱动程序之后，请使用以思科提供的程序命名的 InstallCert 接受和安装防御中心提供的 SSL 证书。客户端系统和防御中心即会利用 SSL 证书身份验证安全地通信。当您接受证书时，计算机会将其添加到当前运行的 JRE 的 **security** 目录中的密钥库 (**jssecacerts**)：

```
$JAVA_HOME/jre[version]/lib/security
```

以下分别是运行 Microsoft Windows 和 UNIX 的计算机的密钥库常见位置：

- `C:\Program Files\Java\jre[version]\lib\security\jssecacerts`
- `/var/jre[version]/lib/security/jssecacerts`

注　如果您计划用于访问数据库访问功能的 Java 查询应用使用的是不同的 JRE，则必须将此密钥库复制到另一 JRE 的 `security` 目录中。

要使用 InstallCert 安装 SSL 证书，请执行以下操作：

步骤 1　在计算机上，打开命令行界面。

步骤 2　在命令提示符下，转到您解压缩 ZIP 软件包时创建的 `bin` 目录。

步骤 3　要安装防御中心的 SSL 证书，请键入以下内容并按 Enter 键：

```
java InstallCert defense_center
```

其中 *defense_center* 是防御中心的 FQDN 或 IP 地址。InstallCert 不支持 IPv6 地址。如果您在 IPv6 网络上，则必须使用一个可解析的主机名。

从运行 Microsoft Windows 的计算机中，系统会输出类似如下内容：

```
Loading KeyStore C:\Program Files\Java\jre6\lib\security...
Opening connection to defensecenter.example.com:2000...
Starting SSL handshake...
Subject GENERATION=server, T=vjdbc, O="思科, Inc.",
...
...
```

系统将会提示您查看证书。

步骤 4　您可以选择查看证书。

系统将会提示您接受证书。

步骤 5　接受证书。

系统即会接受此证书，并输入类似如下内容（在运行 Microsoft Windows 的计算机中）：

```
Added certificate to keystore 'C:\Program Files\Java\jre6\lib\security\jssecacerts'
using alias 'defensecenter.example.com-1'
```

如果您计划使用 Crystal Reports，请记录密钥库的位置 (`jssecacerts`)。您稍候会需要使用此信息。

步骤 6　您有以下选择：

- 如果有第三方应用，请继续执行下一节使用第三方应用连接数据库，第 2-6 页中的操作步骤。
- 如果有自定义应用，请继续执行使用自定义程序连接数据库，第 2-7 页中的操作步骤。

使用第三方应用连接数据库

安装证书后，您可以使用支持 JDBC SSL 连接的任何第三台方客户端在防御中心上查询数据库。下表列出了配置客户端和防御中心之间的连接时可能需要的信息。

表 2-2　数据库访问客户端的连接信息

信息	说明
JDBC URL	以下 JDBC URL 标识思科数据库，这样客户端上的 JDBC 驱动程序就可以与其建立连接： `jdbc:vjdbc:rmi://defense_center:2000/VJdbc,eqe` 其中 *defense_center* 是防御中心的 FQDN 或 IP 地址。
JDBC 驱动程序 JAR 文件	当配置与思科数据库的连接时，必须使用以下 JAR 文件： • `vjdbc.jar` • `commons-logging-1.1.jar` 这些文件位于解压缩已下载的 `client.zip` 文件后生成的 `lib` 子目录中，如下载 JDBC 驱动程序，第 2-4 页所述。
JDBC 驱动程序类	当配置与思科数据库的连接时，必须使用以下驱动程序类： `com.sourcefire.vjdbc.VirtualDriver`
用户名和密码	要连接设备上的数据库，请使用具有外部数据库用户权限的用户帐户。有关详细信息，请参阅创建数据库用户帐户，第 2-2 页。

以下各节包含有关使用三种常见行业标准报告工具连接思科数据库的提示。无论是使用何处的任何工具，还是使用其他基于 Java 的应用，都应参考适用于报告工具的文档，查阅关于如何创建 JDBC SSL 连接的详细说明。

Crystal Reports

以下说明适用于在 32 位 Windows 环境中安装 Crystal Reports 2011。如果您运行的是 64 位 Windows 环境，文件路径可能会不同。

要允许 Crystal Reports 2011 连接思科数据库，则必须执行以下操作：

- 将您从防御中心下载的 JDBC 驱动程序 JAR 文件添加至 Crystal Reports 类路径。采用 Crystal Reports 默认安装时，您可以在以下文件中编辑类路径部分：
  `C:\Program Files\SAP BusinessObjects\SAP Business Objects Enterprise XI 4.0\Java\CRConfig.xml`
- 将您安装客户端 SSL 证书时创建的密钥库复制到相应的 Crystal Reports 安全目录中。采用 Crystal Reports 默认安装时，该目录为：
  `C:\Program Files\SAP BusinessObjects\SAP Business Objects Enterprise XI 4.0\win32_x86\jdk\jre\lib\security`
- 创建与 Database Expert 的新 JDBC (JNDI) 连接，将思科作为数据库名称。

JasperSoft iReport

要允许 iReport 连接思科数据库，必须执行以下操作：

- 将您从防御中心下载的 JDBC 驱动程序 JAR 文件添加至 iReport 类路径。
- 使用从防御中心下载的 JDBC 驱动程序 JAR 文件添加新的 JDBC 驱动程序。添加驱动程序文件后，iReport 应该会找到正确的驱动程序类。
- 使用您刚刚创建的驱动程序，创建新的数据库连接。

Actuate BIRT

要允许 BIRT 连接思科数据库，则必须执行以下操作：

- 使用 **Generic JDBC Driver** 模板添加驱动程序定义。
- 使用 **Generic JDBC** 配置文件类型创建新数据库连接。
- 使用 **JDBC Data Source** 数据源类型为报告创建数据源。

提示 如果创建新 JDBC 数据源配置文件时无法选择思科驱动程序类，则使用您从防御中心下载的 JDBC 驱动程序 JAR 文件添加驱动程序。

使用自定义程序连接数据库

安装证书之后，您可以启用自定义 Java 报告工具来查询思科数据库。思科提供一个叫做 RunQuery 的示例 Java 命令行，其使用防御中心随附的 JDBC 驱动程序建立必需的 SSL 连接。RunQuery 可检索表记录和表元数据。源代码包含在您从防御中心下载的 ZIP 软件包的 `src` 目录中。请参阅下载 JDBC 驱动程序，第 2-4 页。

注 RunQuery 只是一个示例客户端，**不是**功能齐全的报告工具。思科**强烈**建议您不要将其用作查询数据库的主要方法。有关使用 RunQuery 的信息，请参阅 ZIP 软件包中包含的 README 文件。

有关使用自定义程序连接数据库的详细信息，请参阅以下节：

- 自定义 Java 程序的示例代码，第 2-7 页介绍 RunQuery 应用用于设置数据库连接和提交查询的 Java 类和方法。
- 运行应用，第 2-9 页讨论执行 Java 应用所需满足的环境要求。

自定义 Java 程序的示例代码

RunQuery 源代码使用下述功能。这些代码示例说明几个可能的实施方法之一。

动态设置 SSL 提供程序连接

在客户端上安装 SSL 安全证书之后（请参阅安装客户端 SSL 证书，第 2-5 页），您可以在程序中使用以下命令行动态注册 JSSE 提供程序：

```
Security.addProvider(new com.sun.net.ssl.internal.ssl.
Provider());
```

为程序初始化 JDBC 驱动程序

您可以使用 `Class.forName()` 方法，在 Java 应用中加载 JDBC 驱动程序类，如下所示：

```
Class.forName("com.sourcefire.vjdbc.VirtualDriver").newInstance();
```

如果程序是从命令行启动，则用户要提供如下所示 JDBC 类：

```
java -Djdbc.drivers="com.sourcefire.vjdbc.VirtualDriver" program_name ...
```

其中 *program_name* 是程序的名称。

将程序连接至数据库

程序必须获得 JDBC 连接对象，才能提交查询。使用如下所示 DriverManager.getConnection 方法，建立连接并获取连接对象：

```
Connection conn = DriverManager.getConnection("jdbc:vjdbc:rmi://my_dc:2000/VJdbc,eqe",
"user", "password");
```

其中 *my_dc* 为防御中心的 FQDN 或 IP 地址，user 为数据库访问用户帐户名称，*password* 为此帐户密码。

在思科表中查询数据

创建一个 SQL 查询对象，提交查询并将检索的记录分配给结果集，如下所示：

```
Statement stmt = conn.createStatement();
ResultSet rs = stmt.executeQuery("sql");
```

其中 *sql* 是 SQL 查询。有关支持的 SQL 功能，请参阅查询数据库，第 2-9 页。

生成表查询的结果

利用上述查询生成的结果集 (rs)，您可以输出以下字段：

```
while(rs.next())
{
    for(int i=1; i<= md.getColumnCount(); i++)
    {
        System.out.print(rs.getString(i) + " ");
    }
    System.out.print("\n");
}
```

获取方案信息

程序可以列出数据库中的表，如下所示：

```
DatabaseMetaData metaData = conn.getMetaData();
      ResultSet tables = meta.getTables(null, null, null, null);
      while (tables.next())
      {
System.out.println(tables.getString("TABLE_NAME"));
      }
```

程序可以列出表的列，如下所示：

```
ResultSet columns = metaData.getColumns(null, null, "table_name", null);
```

其中 *table_name* 是数据库表的名称。

运行应用

在运行应用之前，必须在客户端计算机上设置 CLASSPATH，以包含应用 JAR 文件的当前目录和位置。

如果您按照下载 JDBC 驱动程序，第 2-4 页中所述下载并解压缩 ZIP 软件包，请更新 CLASSPATH，如下所示：

要在 UNIX 环境中运行应用，请执行以下操作：

步骤 1　使用以下命令：

```
export CLASSPATH=$CLASSPATH:.:path/lib/vjdbc.jar:path/lib/commons-logging-1.1.jar
```

其中 *path* 是您解压缩您从防御中心下载的 ZIP 软件包的目录路径。

要在 Windows 7 环境中运行应用，请执行以下操作：

步骤 1　右键点击计算机图标并选择 **Properties**。

系统将会显示 **System** 窗口。

步骤 2　点击 **Advanced System Settings**。

系统将会显示 **System Properties** 窗口。

步骤 3　选择 **Advanced** 选项卡。

步骤 4　点击 **Environment Variables...**。

系统将会显示 **Environment Variables** 窗口。

步骤 5　选择 **CLASSPATH** 系统变量并点击 **Edit...**。

系统将会显示 **Edit System Variable** 窗口。

步骤 6　将以下内容添加至 **Variable value:** 字段：

```
.;path\bin;.;path\lib\vjdbc.jar;.;path\lib\commons-logging-1.1.jar;.;path\lib
```

其中 *path* 是您解压缩您从防御中心下载的 ZIP 软件包的目录路径。

步骤 7　点击 **OK**，保存该值。

系统将会显示 Environment Variables 窗口。

步骤 8　点击 **OK**，保存该值。您现在即可运行此应用。

查询数据库

以下各节包含有关支持的查询语法的信息以及其他重要的查询相关要求和限制：

- 支持的 SHOW 语句语法，第 2-10 页介绍用于查询思科数据库的支持的 MySQL **SHOW** 语句语法。
- 支持的 DESCRIBE 或 DESC 语句语法，第 2-10 页介绍用于查询思科数据库的支持的 MySQL **DESCRIBE** 语句语法。
- 支持的 SELECT 语句语法，第 2-11 页介绍用于查询思科数据库的支持的 MySQL **SELECT** 语句语法。

- 联合限制，第 2-12 页介绍用于查询思科数据库的支持的联合并解释如何获取有关任意表的具体允许联合的信息。
- 查询以不熟悉的格式存储的数据，第 2-12 页描述如何对以可能不熟悉的格式存储的数据执行查询（包含 UNIX 时间戳和 IP 地址），从而使您查询执行成功并且出现您所预期的结果。
- 由于性能原因限制查询，第 2-14 页包含有关限制查询从而不降低 FireSIGHT 系统的性能的建议。
- 查询提示，第 2-14 页包含查询若干设备上入侵事件的提示。

有关方案信息和允许的联合，请参阅以下章节：

- 方案：系统级表，第 3-1 页
- 方案：入侵表，第 4-1 页
- 方案：统计跟踪表，第 5-1 页
- 方案：发现事件和网络映射表，第 6-1 页
- 方案：连接日志表，第 7-1 页
- 方案：用户活动表，第 8-1 页
- 方案：关联表，第 9-1 页

支持的 SHOW 语句语法

SHOW 语句列出思科数据库中的所有表。以下是您在查询思科数据库时可以使用的受支持的 MySQL **SHOW** 语句语法：

```
SHOW TABLES;
```

上面未列出的任何 **SHOW** 语句语法均不受支持。

支持的 DESCRIBE 或 DESC 语句语法

思科数据库提供对 **DESCRIBE** 语句的有限使用。在思科数据库中，**DESCRIBE** 语句的输出仅列出列名以及各列中数据的类型。以下是您在查询思科数据库时可以使用的受支持的 MySQL **DESCRIBE** 语句语法：

```
DESCRIBE table_name;
```

思科 数据库还支持相同的命令 DESC：

```
DESC table_name;
```

表 2-3　　支持的 DESCRIBE 语句语法

关键字	含义
table_name	所查询的表的名称

上面未列出的任何 **DESCRIBE** 语句语法均不受支持。特别是，FireSIGHT 系统数据库访问功能不支持以下语句语法：

- INDEX FOR 子句
- TABLE 子句
- PROCEDURE 子句

支持的 SELECT 语句语法

以下是您在查询思科数据库时可以使用的受支持的 MySQL SELECT 语句语法：

```
SELECT
[ALL | DISTINCT]
select_expr [, select_expr ...]
FROM table_references
[WHERE where_condition]
[GROUP BY { column_name | position } [ ASC | DESC ], …]
[HAVING where_condition]
[ORDER BY { column_name | position } [ ASC | DESC ], …]
[LIMIT { [offset,] row_count | row_count OFFSET offset}]
```

下表详细说明上述 SELECT 语句中子句和参数的必需语法。

表 2-4　　支持的 SELECT 语句语法

关键字	含义
select_expr	{*column_name* [[AS] *alias*] | *function*(...) [[AS] *alias*] | *aggregate_function*(...) [[AS] *alias*]}
column_name	所查询的字段的名称
function	{ABS | CAST | CEILING | CHAR_LENGTH | COALESCE | CONV | CHARACTER_LENGTH | CONCAT | CONVERT | CURRENT_DATE | CURRENT_TIME | CURRENT_TIMESTAMP | EXTRACT | FLOOR | HEX | INET_ATON | INET_NTOA | INET6_ATON | INET6_NTOA | LEFT | LOWER | LPAD | MID | MOD | NULLIF | OCTET_LENGTH | POSITION | RIGHT | ROUND | SUBSTRING | SYSDATE | TIME | TIMESTAMP | TRIM | UPPER}
aggregate_function	{AVG | COUNT | COUNT(DISTINCT) | MAX | MIN | SUM}
table_references	以下任一项： • *table_reference* INNER JOIN *table_reference join_condition* • *table_reference* LEFT [OUTER] JOIN *table_reference join_condition*
table_reference	*table_name* [[AS] alias]
table_name	所查询的表的名称
join_condition	ON *conditional_expr*
conditional_expr	兼容联合的字段之间的等式比较；有关详细信息，请参阅联合限制，第 2-12 页
where_condition	以下任一项： • IS NULL 或 IS NOT NULL • NOT, ! • BETWEEN ... AND ... • LIKE • =, !=, <>, >, >=, <, <=

如果您不熟悉如何表示支持的 MySQL 语法，请参阅下表，获取提示。

表 2-5　MySQL 语法格式

符号名称	符号形式	含义
方括号	[]	可选子句或参数
花括号	{}	必需子句或参数
竖线	|	子句或参数之间的选择

上面未列出的任何 SELECT 语句语法均不受支持。特别是，FireSIGHT 系统数据库访问功能不支持以下语句语法：

- SELECT * 即您必须明确指定字段
- 并集
- 子查询
- GROUP BY 子句的 WITH ROLLUP 修饰符
- INTO 子句
- FOR UPDATE 子句

联合限制

由于性能和其他实际原因，可在思科数据库表上执行的联合有限。在结果不太可能用于事件分析的情况下，思科不允许执行联合。

您仅可执行内部联合和左（外部）联合。不支持嵌套联合、交叉联合、自然联合、左侧（外部）联合、完整（外部）联合和使用 USING 子句的联合。

方案文档指出了每个表支持的联合。不支持未列出的联合。例如，您无法联合 IP 地址字段上的 **compliance_event** 和 **intrusion_event** 表，即使这两个表都包含 IP 地址信息。此外，已废弃的表和已废弃的字段上的联合也未列出。

查询以不熟悉的格式存储的数据

思科数据库会以不易于查看的格式存储某些数据。以下各节详细介绍如何在各个字段上执行查询，从而使您的查询成功执行，并且显示您所预期的结果：

- IPv6 地址，第 2-13 页
- IPv4 地址，第 2-13 页
- MAC 地址，第 2-13 页
- 数据包数据，第 2-13 页
- UNIX 时间戳，第 2-13 页

IPv6 地址

思科数据库以二进制格式存储 IPv6 地址。要以十六进制显示结果，请使用 **HEX()** 函数。要查询特定 IPv6 地址上的数据库，请使用 **UNHEX()** 函数。

例如，以下语句查询的是 **connection_log** 表，此表包含有关受监视会话的信息，其通过特定 IPv6 地址限制查询：

```
SELECT HEX(initiator_ip), HEX(responder_ip), packets_sent, bytes_sent

FROM connection_log

WHERE initiator_ip = UNHEX('20010db8000000000000000000004321');
```

IPv4 地址

思科数据库以二进制格式将 IPv4 地址存储在和 IPv6 地址相同的字段内。对于 IPv6 地址，请使用 HEX() 函数获取十六进制表示。此数据库遵循 RFC，用 1 填充位 80-95，生成无效的 IPv6 地址。例如 IPv4 地址 10.5.15.1 会存储为 00000000000000000000FFFF0A050F01。

MAC 地址

思科数据库以二进制格式存储 MAC 地址。要以十六进制显示结果，请使用 HEX() 函数。

例如，以下语句查询的是 **rna_host_mac_map** 表，此表包含关于不使用 IP 地址进行标识，而是使用 MAC 地址的主机的信息，查询结果限制为前五个主机：

```
SELECT HEX(host_id), HEX(mac_address)

FROM rna_host_mac_map

LIMIT 5;
```

数据包数据

思科数据库以二进制格式存储入侵事件的数据包数据。要以十六进制显示结果，请使用 HEX() 函数。

例如，以下语句查询的是 **intrusion_event_packet** 表，以获取用于特定事件的数据包数据：

```
SELECT HEX(packet_data)

FROM intrusion_event_packet

WHERE event_id = 1234;
```

UNIX 时间戳

思科数据库将大多数时间戳存储为 UNIX 时间戳，其表示自 1970 年 1 月 1 日 00:00:00 (UTC) 起经过的秒数。要以当地时间显示结果，请使用 **FROM_UNIXTIME()** 函数。

例如，以下语句查询的是 **audit_log** 表，此表记录设备 Web 界面上的所有用户操作，并返回最多 25 条结果。

```
SELECT FROM_UNIXTIME(action_time_sec), user, message

FROM audit_log

LIMIT 0, 25;
```

请记住，数据库中的所有时间均为 UTC 时间。虽然允许使用 **CONVERT_TZ()** 函数，但是它只提供 UTC 格式的结果。

请注意，某些事件可能会有与之关联的微秒值。您可以使用 **CONCAT()** 和 **LPAD()** 函数来结合 UNIX 时间戳和微秒增量。例如，以下语句查询的是 **intrusion_event** 表：

```
SELECT CONCAT(FROM_UNIXTIME(event_time_sec)), '.', LPAD (event_time_usec, 6, '0')),
HEX(host_id),

rule_message

FROM intrusion_event

LIMIT 0, 25;
```

要就具有特定 UNIX 时间戳的事件查询数据库，请使用 **UNIX_TIMESTAMP()** 函数。

由于性能原因限制查询

虽然系统限制您可在思科数据库表上执行的联合，但是它仍然允许执行某些代价较高的查询，即可能对防御中心的性能产生负面影响的查询。

因此，您应尝试限制大表的结果集。其策略包括：

- 将查询限制于特定时间范围
- 按照 IP 地址限制查询
- 使用 **LIMIT** 子句

根据部署，查询很多表可能需要有限的结果集。特别是，以下表可能包含 DC3000 上的 1 亿个事件：

- fireamp_event
- intrusion_event
- intrusion_event_packet
- **connection_log** （5.0 版本之前名为：**rna_flow**）
- **connection_summary**（5.0 版本之前名为：**rna_flow_summary**）

根据系统在受监视网络上检测的主机的数量，网络映射表上的查询代价可能也很高。

查询提示

以下各节提供有关确保构建包含检测引擎或入侵事件的查询时结果唯一的提示。

设备名称

在多个防御中心上，设备名称不一定唯一。为了确保唯一性，请在查询中包含一个具体的设备 UUID。

入侵事件

为了与多个受管设备上的某个入侵事件唯一匹配，请在您对 **intrusion_event** 表的查询中包含以下字段：

- intrusion_event.event_id
- intrusion_event.event_time_sec
- intrusion_event.sensor_uuid

示例查询

以下各节包含一些示例查询，用以向您说明可以如何使用数据库访问功能：

注意　根据部署，执行其中某些示例查询可能代价很高。有关详细信息，请参阅由于性能原因限制查询，第 2-14 页。

用户的审核记录

以下查询返回审核记录中特定用户的所有记录，以 UTC 显示所有时间戳：

```
SELECT FROM_UNIXTIME(action_time_sec), user, message

FROM audit_log

WHERE user = 'eventanalyst';
```

按照优先级和分类显示入侵事件

以下查询复制 Events By Priority and Classification 工作流程中的 Drilldown of Event、Priority 和 Classification 视图。如果未在用户首选项中更改默认 Intrusion Events 工作流程，这就是在防御中心 Web 界面上选择 **Analysis > Intrusion Events** 时看到的第一个页面：

```
SELECT rule_message, priority, rule_classification, count(*) as Count

FROM intrusion_event

WHERE reviewed="0" GROUP BY rule_message, priority, rule_classification

ORDER BY Count

DESCLIMIT 0, 25;
```

入侵事件及其关联策略

以下查询列出从指定星期开始的入侵事件。对于每个事件，其显示关联入侵策略违规和规则分类。

```
SELECT FROM_UNIXTIME(event_time_sec) AS event_time, event_id AS intrusion_event,
intrusion_event_policy_name AS policy, rule_classification AS classification

FROM intrusion_event

WHERE event_time_sec BETWEEN UNIX_TIMESTAMP('2011-10-01 00:00:00') AND
```

```
UNIX_TIMESTAMP('2011-10-07 23:59:59')

ORDER BY policy ASC;
```

检测到的主机的列表

以下查询返回在网络上检测到的所有 MAC 主机（无 IP 地址的主机）的主机网络映射中的基本信息，以及每个 NIC 的硬件供应商：

```
SELECT HEX(mac_address), mac_vendor, host_type, FROM_UNIXTIME(last_seen_sec)

FROM rna_mac_host;
```

以下查询将 IP 地址映射至 MAC 地址：

```
SELECT HEX(ipaddr), HEX(mac_address), HEX(host_id)

FROM rna_host_ip_map LEFT JOIN rna_host_mac_map on

rna_host_ip_map.host_id=rna_host_mac_map.host_id;
```

检测到的服务器的列表

以下查询将两个相关表联合，向您提供在网络上检测到的服务器的列表及其很多属性，类似于可以在防御中心 Web 界面上看到的内容：

```
SELECT FROM_UNIXTIME(s.last_used_sec), HEX(s.host_id), s.port, s.protocol, s.hits,

i.service_name, i.vendor, i.version, i.source_type, s.confidence

FROM AS s

LEFT JOIN rna_ip_host_service_info AS i ON (s.host_id = i.host_id AND s.port = i.port AND
s.protocol =

i.protocol);
```

请注意，此查询按照数据库访问要求，向左联合 `host_id`、`port` 和 `protocol` 集合上的表。请参阅 rna_host_service 联合，第 6-33 页和 rna_host_service_info 联合，第 6-37 页。

网络上的服务器漏洞

以下查询联合两个与漏洞相关的表，向您提供面向特定主机所检测到的有效服务器相关漏洞的列表，以及每个漏洞在网络上是否会被利用：

```
SELECT h.rna_vuln_id, v.title, v.remote

FROM rna_host_service_vulns AS h

LEFT JOIN rna_vuln AS v ON (h.rna_vuln_id = v.rna_vuln_id)

WHERE h.ip_address = INET_ATON('10.10.10.4')

AND h.invalid = 0;
```

请注意，此查询按照 rna_host_service_vulns，第 6-42 页和 rna_vuln 联合，第 6-52 页的要求向左联合 `rna_vuln_id` 上的表。

操作系统摘要

以下查询复制 Operating System Summary 工作流程中的 Summary of OS Names 页面。如果未在用户首选项中更改默认工作流程，这就是在防御中心 Web 界面上选择 **Analysis > Hosts**，然后选择 **Hosts** 时看到的第一个页面：

```
SELECT vendor, product, count(*) AS total

FROM rna_host_os

GROUP BY vendor, product

ORDER BY total DESC;
```

主机的操作系统漏洞

以下查询联合两个与漏洞相关的表，向您提供面向特定主机所检测到的有效操作系统相关漏洞的列表，以及每个漏洞在网络上是否会被利用：

```
SELECT h.rna_vuln_id, v.title, v.remote

FROM rna_host_os_vulns AS h

LEFT JOIN rna_vuln AS v ON (h.rna_vuln_id = v.rna_vuln_id)

WHERE h.host_id = UNHEX('9610B6E6F1784DA4B39BEA7A210AAD68')

AND h.invalid = 0;
```

请注意，此查询按照数据库访问的要求向左联合 `rna_vuln_id` 上的表。请参阅 rna_host_os_vulns，第 6-27 页和 rna_vuln 联合，第 6-52 页。

主机违规计数

以下查询复制 Host Violation Count 工作流程上的 Host Violation Count 页面。如果未在用户首选项中更改默认 Compliance White List Violations 工作流程，这就是在防御中心 Web 界面上选择 **Analysis > Correlation > White List Violations** 时看到的第一个页面：

```
SELECT host_id, HEX(host_id), white_list_name, count(*) AS total

FROM white_list_violation

GROUP BY host_id, white_list_name

ORDER BY total DESC;
```

方案：系统级表

本章包含有关适用于审核、设备运行状况监控、恶意软件检测和安全更新记录等系统级功能的方案与所支持的联合的信息。

有关详细信息，请参阅下表列出的各节。

表 3-1　　系统级表的方案

请参阅……	存储有关以下内容的信息的表...	版本
audit_log，第 3-1 页	与设备的 Web 界面的用户交互。	4.10.x+
fireamp_event，第 3-2 页	FireAMP 恶意软件检测和隔离事件。	5.1+
health_event，第 3-8 页	受监控设备的运行状况事件。	4.10.x+
sru_import_log，第 3-10 页	您的设备上已导入的规则更新。	5.0+

audit_log

audit_log 表包含有关 FireSIGHT 系统用户与 Web 界面进行交互的信息。请记住，审核日志仅存储本地设备的记录，不存储受管设备的记录。

有关详细信息，请参阅以下各节：

- audit_log 字段，第 3-1 页
- audit_log 联合，第 3-2 页
- audit_log 示例查询，第 3-2 页

audit_log 字段

下表描述您可在 **audit_log** 表中访问的数据库字段。

表 3-2　　audit_log 字段

字段	说明
action_time_sec	设备生成审核记录的日期和时间的 UNIX 时间戳。
message	用户执行的操作。
source	用点分十进制表示法表示的 Web 界面用户主机的 IP 地址。

表 3-2　audit_log 字段（续）

字段	说明
subsystem	用户生成审核记录所遵循的菜单路径。
user	触发审核事件的用户的用户名。

audit_log 联合

您无法在 **audit_log** 表上执行联合。

audit_log 示例查询

以下查询返回最多 25 个按照时间排序的最近审核日志条目。

```
SELECT from_unixtime(action_time_sec)
AS Time, user, subsystem, message, source, count(*)
AS Total
FROM audit_log
GROUP BY source, subsystem, user, message
ORDER BY source DESC;
```

fireamp_event

fireamp_event 表包含关于恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。已添加新字段，用于标识触发事件的应用、处理事件的方式，以及用于将事件与连接、入侵和文件事件关联。

有关详细信息，请参阅以下各节：

- fireamp_event 字段，第 3-2 页
- fireamp_event 联合，第 3-8 页
- fireamp_event 示例查询，第 3-8 页

fireamp_event 字段

下表描述您可在 **fireamp_event** 表中访问的数据库字段。

表 3-3　fireamp_event 字段

字段	说明
application_id	映射到执行文件传送的应用的 ID 编号。
application_name	执行传送的应用的名称。
cert_valid_end_date	连接中使用的 SSL 证书停止有效的 Unix 时间戳。
cert_valid_start_date	颁发连接中使用的 SSL 证书时的 Unix 时间戳。

表 3-3　fireamp_event 字段（续）

字段	说明
client_application_id	客户端应用（如适用）的内部标别号。
client_application_name	客户端应用（如适用）的名称。
cloud_name	触发 FireAMP 事件的云端服务的名称。每个 cloud_name 值都有一个相关的 cloud_uuid 值。
cloud_uuid	触发 FireAMP 事件的云端服务的内部唯一 ID。每个 cloud_uuid 值都有一个相关的 cloud_name 值。
connection_sec	与恶意软件事件相关的连接事件的 UNIX 时间戳（自 00:00:00 01/01/1970 起经过的秒数）。
counter	事件的特定计数器，用于区别在同一秒内发生的多个事件。
detection_name	检测到或被隔离的恶意软件的名称。
detector_type	检测到恶意软件的检测器。每个 detector_type 值都有一个相关的 detector_type_id。可能的显示值和相关 ID 如下： • ClamAV - 128 • ETHOS - 8 • SPERO - 32 • SHA - 4 • Tetra - 64
detector_type_id	检测到恶意软件的检测技术的内部 ID。每个 detector_type_id 值都有一个相关的 detector_type 值。可能的显示值和相关类型如下： • 4 - SHA • 8 - ETHOS • 32 - SPERO • 64 - Tetra • 128 - ClamAV
direction	指示是否已上传或下载此文件的值。可能会有以下值： • Download • Upload 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
disposition	文件的恶意软件状态。可能的值包括： • CLEAN - 文件是安全的，不包含恶意软件。 • UNKNOWN - 不确定文件是否包含恶意软件。 • MALWARE - 文件包含恶意软件。 • UNAVAILABLE - 软件无法向思科云发送请求以了解处置情况，或思科云服务未响应此请求。 • CUSTOM SIGNATURE - 文件与用户定义的哈希匹配，并且以用户指定的方式进行处理。

表 3-3　fireamp_event 字段（续）

字段	说明
dst_continent_name	目标主机的大陆名称。 ** - 未知 na - 北美洲 as - 亚洲 af - 非洲 eu - 欧洲 sa - 南美洲 au - 澳大利亚 an - 南极洲
dst_country_id	目标主机的国家/地区代码。
dst_country_name	目标主机的国家/地区名称。
dst_ip_address_v6	此字段已弃用，现在会返回 null。
dst_ipaddr	连接的目标的 IPv4 或 IPv6 地址的二进制表示法。
dst_port	连接的目标的端口号。
endpoint_user	思科云检测到事件时，思科 FireAMP 代理确定的用户。此用户与 LDAP 无关，不在 discovered_users 表上显示。
event_description	与事件类型相关的其他事件信息。
event_id	FireAMP 事件的内部唯一 ID。
event_subtype	导致恶意软件检测的操作。每个 event_subtype 值都有一个相关的 event_subtype_id 值。可能的显示值和相关 ID 如下： • Create - 1 • Execute - 2 • Move - 22 • Scan - 4
event_subtype_id	导致恶意软件检测的操作的内部 ID。每个 event_subtype_id 值都有一个相关的 event_subtype 值。可能的显示值和相关子类型如下： • 1 - 创建 • 2 - 执行 • 4 - 扫描 • 22 - 移动

表 3-3　fireamp_event 字段（续）

字段	说明
event_type	FireAMP 事件的类型。每个 event_type 值都有一个相关的 event_type_id 值。可能的显示值和相关 ID 如下： • Blocked Execution - 553648168 • Cloud Recall Quarantine - 553648155 • Cloud Recall Quarantine Attempt Failed - 2164260893 • Cloud Recall Quarantine Started - 553648147 • Cloud Recall Restore from Quarantine - 553648154 • Cloud Recall Restore from Quarantine Failed - 2164260892 • Cloud Recall Restore from Quarantine Started - 553648146 • FireAMP IOC - 1107296256 • Quarantine Failure - 2164260880 • Quarantined Item Restored - 553648149 • Quarantine Restore Failed - 2164260884 • Quarantine Restore Started - 553648150 • Scan Completed, No Detections - 554696715 • Scan Completed With Detections - 1091567628 • Scan Failed - 2165309453 • Scan Started - 554696714 • Threat Detected - 1090519054 • Threat Detected in Exclusion - 553648145 • Threat Detected in Network File Transfer - 1 • Threat Detected in Network File Transfer (Retrospective) - 2 • Threat Quarantined - 553648143

表 3-3　fireamp_event 字段（续）

字段	说明
event_type_id	FireAMP 事件类型的内部 ID。每个 event_type_id 值都有一个相关的 event_type 值。可能的显示值和相关类型如下： • 553648143 - 已隔离威胁 • 553648145 - 排除部分检出威胁 • 553648146 - 从隔离中恢复云召回已启动 • 553648147 - 云召回隔离已启动 • 553648149 - 已隔离项目已恢复 • 553648150 - 隔离恢复已启动 • 553648154 - 从隔离中恢复云召回 • 553648155 - 云召回隔离 • 553648168 - 已阻止执行 • 554696714 - 扫描已启动 • 554696715 - 扫描已完成，无检测 • 1090519054 - 检测到威胁 • 1091567628 - 扫描已完成，有检测 • 1107296256 - FireAMP IOC • 2164260880 - 隔离失败 • 2164260893 - 云召回隔离尝试失败 • 2164260884 - 隔离恢复失败 • 2164260892 - 从隔离恢复云召回失败 • 2165309453 - 扫描失败
file_name	被检测或隔离的文件的名称。该名称可包含 UTF-8 字符。
file_path	被检测或隔离的文件的文件路径，不包括文件名。
file_sha	被检测或隔离的文件 SHA-256 哈希值。
file_size	被检测或隔离的文件的大小（字节）。
file_timestamp	被检测或隔离的文件的创建时间戳。
file_type	被检测或隔离文件的文件类型。
file_type_id	被检测或隔离的文件的文件类型内部 ID。
instance_id	生成事件的受管设备上 Snort 实例的数字 ID。
ioc_count	在事件中发现的威胁的指示数量。
parent_file_name	检测期间访问被检测或隔离文件的文件的名称。
parent_file_sha	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
policy_uuid	作为触发事件的访问控制策略的唯一标识符的标别号。
retroactive_ disposition	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与 disposition 字段相同。可能的值与 disposition 字段相同。
score	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。

表 3-3　fireamp_event 字段（续）

字段	说明
security_context	对流量通过的安全情景（虚拟防火墙）的说明。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
sensor_address	生成事件的设备的 IP 地址。
sensor_id	生成事件的设备的 ID。
sensor_name	生成事件记录的受管设备的文本名称。当事件指报告设备本身，而不是所连接的设备时，则此字段为 null。
sensor_uuid	受管设备的唯一标识符，如果 fireamp_event.sensor_name 为 null，则此字段为 0。
src_continent_name	源主机的大陆名称。 ** - 未知 na - 北美洲 as - 亚洲 af - 非洲 eu - 欧洲 sa - 南美洲 au - 澳大利亚 an - 南极洲
src_country_id	源主机的国家/地区代码。
src_country_name	源主机的国家/地区名称。
src_ip_address_v6	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
src_ipaddr	连接源的 IPv4 或 IPv6 地址的二进制表示。
src_port	连接源的端口号。
ssl_issuer_common_name	SSL 证书的颁发者常用名。这通常是证书颁发者的主机和域名，但也可能包含其他信息。
ssl_issuer_country	SSL 证书颁发者的国家/地区。
ssl_issuer_organization	SSL 证书颁发者的组织。
ssl_issuer_organization_unit	SSL 证书颁发者的组织单位。
ssl_serial_number	SSL 证书的序列号，由发行 CA 分配。
ssl_subject_common_name	SSL 证书的持有者常用名。这通常是证书持有者的主机和域名，但也可能包含其他信息。
ssl_subject_country	SSL 证书持有者的国家/地区。
ssl_subject_organization	SSL 证书持有者的组织。
ssl_subject_organization_unit	SSL 证书持有者的组织单位。
threat_name	威胁的名称。
timestamp	FireAMP 事件生成时间戳。
url	连接源的 URL。
user_id	最后一次登录发送或接收文件的主机的用户内部标别号。此用户在 **discovered_users** 表中。

表 3-3　fireamp_event 字段（续）

字段	说明
username	最后一次登录发送或接收文件的主机的用户的名称。
web_application_id	Web 应用（如适用）的内部标别号。
web_application_name	Web 应用（如适用）的名称。

fireamp_event 联合

下表描述可以在 **fireamp_event** 表上执行的联合。

表 3-4　fireamp_event 联合

您可以联合此表……	与……
dst_ipaddr 或 src_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

fireamp_event 示例查询

以下查询返回与指定用户相关的 25 个恶意软件事件，按照 timestamp 升序排列。

```
SELECT event_id, timestamp, src_ipaddr, dst_ipaddr, username, cloud_name, event_type,
event_subtype, event_description, detection_name, detector_type, file_name,
parent_file_name

FROM fireamp_event

WHERE username="username" ORDER BY timestamp ASC

LIMIT 25;
```

health_event

health_event 表包含关于 FireSIGHT 系统生成的运行状况事件的信息。

有关详细信息，请参阅以下各节：

- health_event 字段，第 3-9 页
- health_event 联合，第 3-9 页
- health_event 示例查询，第 3-9 页

health_event 字段

下表说明您可在 **health_event** 表中访问的数据库字段。

表 3-5　health_event 字段

字段	说明
说明	对导致相关运行状况模块生成运行状况事件的情况的描述。例如，当无法执行进程时生成的运行状况事件被标记为 Unable to Execute。
event_time_sec	防御中心生成运行状况事件的日期和时间的 UNIX 时间戳。
ID	事件的内部标别号。
module_name	生成事件的运行状况模块的名称。
sensor_name	生成事件记录的受管设备的文本名称。当运行状况事件指报告设备本身，而不是所连接的设备时，此字段为 null。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此字段为零。
status	为 sensor_uuid 中识别的设备报告的运行状况监控器状态。其值如下： • red - 严重状态。表示对于设备中的至少一个运行状况模块而言，已超过限值，并且该问题尚未解决。 • yellow - 警告状态。表示对于设备中的至少一个运行状况模块而言，已超过限值，并且该问题尚未解决。 • green - 正常状态。表示设备中的所有运行状况模块都在应用于该设备的运行状况策略中配置的限值内运行。 • recovered - 表示设备中的所有运行状况模块（包括处于“严重”或“警告”状态的模块）都在应用于该设备的运行状况策略中配置的限值内运行。 • disabled - 表示设备被禁用或列入黑名单，或当前无法连接，或没有应用运行状况策略。 • error - 表示设备中的至少一个运行状况监控模块出现故障，并且自故障发生后未能成功重新运行。
units	运行状况测试获得的结果的度量单位。例如，%（磁盘使用率）。
value	运行状况测试获得的结果的单位数。例如，80% 的 value 为 80。

health_event 联合

您无法在 **health_event** 表上执行联合。

health_event 示例查询

以下查询返回在定义的时间段内记录的最多 25 个最近运行状况事件。

```
SELECT module_name, FROM_UNIXTIME(event_time_sec)
AS event_time, description, value, units, status, sensor_name
FROM health_event
WHERE event_time_sec
```

```
BETWEEN UNIX_TIMESTAMP("2011-10-01 00:00:00")
AND UNIX_TIMESTAMP("2011-10-07 23:59:59")
ORDER BY event_time DESC
LIMIT 0, 25;
```

sru_import_log

sru_import_log 表包含有关已在设备上运行的规则更新过程的信息。从 FireSIGHT 系统 5.0 版本开始，**sru_import_log** 表代替已弃用的 **seu_import_log** 表。

有关详细信息，请参阅以下各节：

- sru_import_log 字段，第 3-10 页
- sru_import_log 联合，第 3-11 页
- sru_import_log 示例查询，第 3-11 页

sru_import_log 字段

下表描述您可在 **sru_import_log** 表中访问的数据库字段。

表 3-6　sru_import_log 字段

字段	说明
action	表示已对导入的规则更新对象类型执行的操作： • apply - 已为导入启用 Reapply intrusion policies after the Rule Update import completes 选项。 • changed - 对于规则更新组件或规则而言，规则更新组件已被修改，或者规则的版本号更高且 GID 和 SID 相同。 • collision - 对于规则更新组件或规则而言，由于版本与设备上的现有组件或规则冲突，因此跳过导入。 • deleted - 对于规则而言，已从规则更新删除规则。 • disabled - 对于规则而言，已在思科提供的默认策略中禁用规则。 • drop - 对于规则而言，已在思科提供的默认策略中将规则设置为 Drop and Generate Events。 • enabled - 对于规则更新而言，已在思科提供的默认策略中启用编辑、预处理器、规则或规格更新提供的其他功能。 • error - 对于规则更新或本地规则文件而言，导入失败。 • new - 对于规则而言，是指第一次把对象存储在此设备上。
detail	导入的规则更新应用于组件或规则的更改的唯一注释字符串，对于未更改的规则，此字段为空。
generator_id	规则生成器的 GID。
import_time_sec	记录规则更新导入的日期和时间的 UNIX 时间戳。

表 3-6　sru_import_log 字段（续）

字段	说明
name	导入的对象的名称。对于规则，这对应于规则消息。对于规则更新组件而言，这是组件名，例如在线帮助或 Snort。
policy	All，表示所有默认策略中均包含某条规则。
revision	规则的版本号。
signature_id	规则或规则集、解码器或预处理器的 SID。
sru_name	规则更新的描述性名称。
sru_uuid	规则更新的唯一标识符。
type	规则更新中导入的对象的类型：update、rule、variable 等。

sru_import_log 联合

您无法在 **sru_import_log** 表上执行联合。

sru_import_log 示例查询

以下查询返回最多 25 个结果，按时间戳降序排列。

```
SELECT FROM_UNIXTIME(import_time_sec)
AS time, name, type, action, generator_id, signature_id, revision, policy
FROM sru_import_log
ORDER BY time DESC
LIMIT 0, 25;
```

方案：入侵表

本章包含有关适用于入侵事件、触发事件的数据包和关联规则消息的方案和所支持的联合的信息。有关详细信息，请参阅下表列出的各节。

表 4-1　　入侵表的方案

请参阅……	存储有关以下内容的信息的表...	版本
intrusion_event，第 4-1 页	入侵事件，包括攻击的日期、时间、漏洞攻击类型和有关攻击的源和目标的情景信息。	4.10.x+
intrusion_event_packet，第 4-6 页	触发入侵事件的数据包的内容。	4.10.x+
rule_message，第 4-7 页	入侵事件的规则消息，包括关联的生成器 ID (GID)、签名 ID (SID) 和版本数据。	4.10.x+
rule_documentation，第 4-8 页	有关规则的信息，包括攻击场景、受影响的系统以及关于规则创建时间和创建者的信息。	5.2+

intrusion_event

`intrusion_event` 表包含关于 FireSIGHT 系统识别的可能的入侵的信息。对于每个可能的入侵，系统会在数据库中生成一个事件和关联记录，包含攻击的日期、时间与漏洞攻击类型、访问控制策略与规则、入侵策略与规则，以及关于攻击的源和目标的其他情景信息。

提示 对于基于数据包的事件；还可能提供触发事件的数据包的副本；请参阅 intrusion_event_packet 示例查询，第 4-7 页。

有关详细信息，请参阅以下各节：

- `intrusion_event` 字段，第 4-2 页
- `intrusion_event` 联合，第 4-6 页
- `intrusion_event` 示例查询，第 4-6 页

intrusion_event 字段

下表列出可在 **intrusion_event** 表中访问的数据库字段。

表 4-2　　intrusion_event 字段

字段	说明
access_control_policy_name	与生成入侵事件的入侵策略关联的访问控制策略。请注意，对于防御中心访问控制策略名称和访问控制规则名称组合是唯一的。
access_control_policy_UUID	与生成入侵事件的入侵策略关联的访问控制策略 UUID。
access_control_rule_id	与生成入侵事件的入侵策略关联的访问控制规则的内部标识号。
access_control_rule_name	与生成入侵事件的入侵策略关联的访问控制策略名称。请注意，访问控制规则名称在某个策略内是唯一的，但是在不同策略之间则不是唯一的。
application_protocol_id	应用协议的内部标识号。
application_protocol_name	以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果系统要求提供更多数据，则显示 pending • 如果连接中没有应用信息，则为空值
blocked	表示触发入侵事件的数据包发生何种情况的值： • 0 - 数据包未被丢弃 • 1 - 数据包已被丢弃（内联、交换或路由式部署） • 2 - 如果已向在内联、交换或路由式部署中配置的设备应用入侵策略，则触发事件的数据包应该已丢弃
client_application_id	入侵事件中使用的客户端应用的内部标识号。
client_application_name	入侵事件中使用的客户端应用（如有）。以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果系统检测到客户端应用，但无法识别具体应用，则显示通用客户端名称 • 如果连接中没有应用信息，则为 null
connection_sec	与入侵事件关联的连接事件的 UNIX 时间戳（自 00:00:00 01/01/1970 起经过的秒数）。
counter	在某一秒内每生成一个连接事件所增加的数值，用于区别在同一秒内发生的多个连接事件。
detection_engine_name	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
detection_engine_uuid	在 5.0 版本中已弃用此字段。对所有查询都返回 null。

表 4-2　intrusion_event 字段（续）

字段	说明
dst_continent_name	目标主机的大陆名称。 ** - 未知 na - 北美洲 as - 亚洲 af - 非洲 eu - 欧洲 sa - 南美洲 au - 澳大利亚 an - 南极洲
dst_country_id	目标主机的国家/地区代码。
dst_country_name	目标主机的国家/地区名称。
dst_ip_address	在 5.2 版本中已弃用此字段。由于向后兼容性，此字段中的值未设置为 null，但这并不可靠。
dst_ip_address_v6	在 5.2 版本中已弃用此字段。由于向后兼容性，此字段中的值未设置为 null，但这并不可靠。
dst_ipaddr	触发事件所涉及的目标主机的 IPv4 或 IPv6 地址的二进制表示。
dst_port	可以为以下任意一项： • 如果事件协议类型是 TCP 或 UDP，则为目标端口号 • 如果事件协议类型是 ICMP，则为 ICMP 代码
dst_user_dept	目标用户所在部门。
dst_user_email	目标用户的邮件地址。
dst_user_first_name	目标用户的名字。
dst_user_id	目标用户（即发生入侵事件之前最后登录目标主机的用户）的内部标识号。
dst_user_last_name	目标用户的姓氏。
dst_user_last_seen_sec	系统最后一次报告目标用户登录时的日期和时间的 UNIX 时间戳。
dst_user_last_updated_sec	系统最后一次更新目标用户记录时的日期和时间的 UNIX 时间戳。
dst_user_name	目标用户的用户名。
dst_user_phone	目标用户的电话号码。
event_id	事件的内部标别号。唯一标识防御中心上的事件。
event_time_sec	事件数据包被捕获时的日期和时间的 UNIX 时间戳。
event_time_usec	事件时间戳的微秒增量。如果微秒分辨率不可用，则此值为 0。
icmp_code	如果事件为 ICMP 流量，则此字段为 ICMP 代码；如果事件不是从 ICMP 流量生成的，则此字段为 null。
icmp_type	如果事件为 ICMP 流量，则此字段为 ICMP 类型；如果事件不是从 ICMP 流量生成的，则此字段为 null。

表 4-2　intrusion_event 字段（续）

字段	说明
impact	事件的影响标志值。整数值如下： • 1 - 红色（易受攻击） • 2 - 橙色（可能易受攻击） • 3 - 黄色（目前不易受攻击） • 4 - 蓝色（未知目标） • 5 - 灰色（未知影响）
instance_id	生成事件的受管设备上 Snort 实例的数字 ID。
interface_egress_name	出站流量的接口名称。
interface_ingress_name	入站流量的接口名称。
intrusion_event_policy_uuid	触发入侵事件的入侵策略的唯一标识符。
intrusion_event_policy_name	生成入侵事件的入侵策略。
ioc_count	在事件中发现的威胁的指示数量。
network_analysis_policy_name	与生成入侵事件的入侵策略关联的网络分析策略。
network_analysis_policy_UUID	与生成入侵事件的入侵策略关联的网络分析策略的 UUID。
priority	与事件关联的规则分类优先级。规则优先级在用户界面上进行设置。
protocol_name	与入侵事件关联的流量协议的文本名称。
protocol_num	协议的 IANA 编号，如以下网址所示： http://www.iana.org/assignments/protocol-numbers。
reviewed	入侵事件是否已标记为已审核： • 1 - 已审核 • 0 - 未审核
rule_classification	与入侵事件关联的规则分类的说明，通常说明的是触发事件的规则检测到的攻击。例如：A Network Trojan was Detected。
rule_classification_id	与入侵事件关联的规则分类标识号。
rule_generator	生成入侵事件的组件。生成器可以是规则引擎、解码器或预处理器。
rule_generator_id	生成入侵事件的 rule_generator 中命名的组件的生成器 ID (GID)。
rule_message	事件的说明文本。对于基于规则的入侵事件，自规则生成事件消息。对于基于解码器和预处理器的事件，事件消息是硬编码的。
rule_revision	与入侵事件关联的规则版本号。
rule_signature_id	入侵事件的签名 ID (SID)。确定导致生成事件的具体规则、解码器消息或预处理器消息。
security_context	对流量通过的安全情景（虚拟防火墙）的说明。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
security_zone_egress_name	触发策略违规的入侵事件的出口安全区域。
security_zone_ingress_name	触发策略违规的入侵事件的入口安全区域。
sensor_address	生成事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_name	生成入侵事件的受管设备的名称。

表 4-2　　intrusion_event 字段（续）

字段	说明
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
src_continent_name	目标主机的大陆名称。 ** - 未知 na - 北美洲 as - 亚洲 af - 非洲 eu - 欧洲 sa - 南美洲 au - 澳大利亚 an - 南极洲
src_country_id	目标主机的国家/地区代码。
src_country_name	目标主机的国家/地区名称。
src_ip_address	在 5.2 版本中已弃用此字段。由于向后兼容性，此字段中的值未设置为 null，但这并不可靠。
src_ip_address_v6	在 5.2 版本中已弃用此字段。由于向后兼容性，此字段中的值未设置为 null，但这并不可靠。
src_ipaddr	触发事件所涉及的源主机的 IPv4 或 IPv6 地址的二进制表示。
src_port	可以为以下任意一项： • 如果事件协议类型是 TCP 或 UDP，则为源端口号 • 如果事件协议类型是 ICMP，则为 ICMP 类型
src_user_dept	源用户所在部门。
src_user_email	源用户的邮件地址。
src_user_first_name	源用户的名字。
src_user_id	源用户（即发生入侵事件之前最后登录源主机的用户）的内部标识号。
src_user_last_name	源用户的姓氏。
src_user_last_seen_sec	系统最后一次报告源用户登录的日期和时间的 UNIX 时间戳。
src_user_last_updated_sec	最后一次更新源用户记录的日期和时间的 UNIX 时间戳。
src_user_name	源用户的用户名。
src_user_phone	源用户的电话号码。
vlan_id	与触发入侵事件的数据包关联的最内部 VLAN 的标识号。
web_application_id	入侵事件中使用的 Web 应用的内部标识号（如适用）。
web_application_name	入侵事件中使用的 Web 应用（如适用）。以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果系统检测到 HTTP 应用协议，但无法识别具体 Web 应用，则显示 web browsing • 如果连接没有 HTTP 流量，则为空值

intrusion_event 联合

下表列出可在 **intrusion_event** 表上执行的联合。

表 4-3　　intrusion_event 联合

您可以联合此表……	与……
application_protocol_id 或 client_application_id 或 web_application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id
dst_ipaddr 或 src_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

intrusion_event 示例查询

以下查询返回最多 25 个最常见的未审核入侵事件结果，按照 Count 降序排列。

```
SELECT rule_message, priority, rule_classification, count(*) as Count

FROM intrusion_event

WHERE reviewed="0"

GROUP BY rule_message, priority, rule_classification

ORDER BY Count DESCLIMIT 0, 25;
```

intrusion_event_packet

intrusion_event_packet 表包含关于触发入侵事件的数据包的内容的信息。请记住，如果禁止从受管设备向防御中心传送数据包，**intrusion_event_packet** 表不包含任何数据。

有关详细信息，请参阅以下各节：

- intrusion_event_packet 字段，第 4-7 页
- intrusion_event_packet 联合，第 4-7 页
- intrusion_event_packet 示例查询，第 4-7 页

intrusion_event_packet 字段

下表列出可在 **intrusion_event_packet** 表中访问的数据库字段。

表 4-4　　intrusion_event_packet 字段

字段	说明
detection_engine_name	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
detection_engine_uuid	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
event_id	事件的标识号。此 ID 在特定受管设备上是唯一的。
linktype	指示数据包外层格式的内部键；供受管设备用于正确解码数据包。仅支持链接类型 1。
packet_data	触发事件的数据包的内容。
packet_time_sec	事件数据包被捕获时的日期和时间 UNIX 时间戳。
packet_time_usec	事件时间戳的微秒增量。如果微秒分辨率不可用，则此值为 0。
sensor_address	生成事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_name	生成入侵事件的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。

intrusion_event_packet 联合

您无法在 **intrusion_event_packet** 表上执行联合。

intrusion_event_packet 示例查询

以下查询返回与所选事件 ID 匹配的所有数据包的数据包信息。

```
SELECT event_id, packet_time_sec, sensor_address, packet_data
FROM intrusion_event_packet
WHERE event_id="1";
```

rule_message

rule_message 表是针对入侵规则的规则消息主列表。每条规则消息都随带识别信息。

有关详细信息，请参阅以下各节：

- rule_message 字段，第 4-8 页
- rule_message 联合，第 4-8 页
- rule_message 示例查询，第 4-8 页

rule_message 字段

下表列出可在 **rule_message** 表中访问的数据库字段。

表 4-5　rule_message 字段

字段	说明
generator_id	触发规则的组件的 GID。
message	与被触发的规则关联的消息。
rev_uuid	规则版本的唯一标识符。
revision	规则的版本号。
signature_id	在设备用户界面上显示的规则识别号。
uuid	规则的唯一标识符。

rule_message 联合

您无法在 **rule_message** 表上执行联合。

rule_message 示例查询

以下查询返回 GID 为 1 且 SID 为 1200 的入侵规则的入侵规则消息。

```
SELECT generator_id, signature_id, revision, message
FROM rule_message
WHERE generator_id="1"
AND signature_id="1200";
```

rule_documentation

rule_documentation 表包含关于生成风险通告所用的规则的信息。

有关详细信息，请参阅以下各节：

- rule_documentation 字段，第 4-9 页
- rule_documentation 联合，第 4-9 页
- rule_documentation 示例查询，第 4-9 页

rule_documentation 字段

下表列出可在 **rule_documentation** 表中访问的数据库字段。

表 4-6　　rule_documentation 字段

字段	说明
additional_references	更多信息和参考。
affected_systems	受漏洞影响的系统。
attack_scenarios	可能的攻击的示例。
contributors	规则和其他相关文档的作者的联系信息。
corrective_action	有关补丁、升级，或其他消除或缓解漏洞的信息。
detailed_information	有关潜在漏洞、规则实际针对的对象、受影响的系统的信息。
ease_of_attack	攻击是被视为简单、中等、困难还是艰难，以及是否可以使用脚本执行此攻击。
false_negatives	可能导致漏报的示例。默认值为 None Known。
false_positives	可能导致误报的示例。默认值为 None Known。
impact	使用此漏洞的威胁可能影响各种系统的程度。
rule_revision	规则版本号。
rule_signature_id	与事件对应的规则标识号。
summary	威胁或漏洞的说明。
updated	最后一次更新规则的日期和时间 UNIX 时间戳。

rule_documentation 联合

您无法在 **rule_documentation** 表上执行联合。

rule_documentation 示例查询

以下查询返回 ID 为 1 的入侵规则的攻击场景、纠正措施、影响和摘要。

```
SELECT attack_scenarios, corrective_action, impact, summary
FROM rule_documentation
WHERE rule_signature_id="1";
```

方案：统计跟踪表

本章包含有关适用于应用和 URL 统计跟踪表的方案与所支持的联合的信息。这些表收集有关以下内容的统计信息：

- 按应用和按用户划分的访问控制和入侵事件
- 按应用和按用户划分的带宽使用量和连接决策
- 按 URL 信誉（风险）和按 URL 业务相关性划分的带宽使用量和连接决策

有关每个表的详细信息的链接，请参阅下表。

表 5-1　　应用和 URL 统计表

请参阅	存储有关以下内容的统计数据的表...	版本
app_ids_stats_current_timeframe，第 5-4 页	按应用和一系列应用属性划分的访问控制和入侵防御活动。	5.0+
app_stats_current_timeframe，第 5-5 页	按应用和一系列应用属性划分的流量和系统访问控制活动（允许或拒绝的连接）。	5.0+
geolocation_stats_current_timeframe，第 5-7 页	按位置划分的访问控制活动。	5.2+
ids_impact_stats_current_timeframe，第 5-8 页	按影响级别划分的入侵事件的统计数据（阻止和丢弃的连接）。	5.1.1+
session_stats_current_timeframe，第 5-10 页	包含所有连接的统计数据。可以根据字节、连接、传感器和时间提取统计数据。	5.2+
ssl_stats_current_timeframe，第 5-11 页	包含 SSL 连接的统计数据。可以根据字节、连接、传感器和时间提取统计数据。	5.4+
storage_stats_by_disposition_current_timeframe，第 5-13 页	包含基于处置情况的文件统计数据。可以根据字节、处置情况、传感器和时间提取统计数据。	5.3+
storage_stats_by_file_type_current_timeframe，第 5-14 页	包含基于文件类型的文件统计数据。可以根据字节、文件类型、传感器和时间提取统计数据。	5.3+
transmission_stats_by_file_type_current_timeframe，第 5-15 页	包含基于文件类型的连接统计数据。可以根据字节、连接、文件类型、传感器和时间提取统计数据。	5.3+
url_category_stats_current_timeframe，第 5-16 页	按所请求网站的类别划分的流量和系统访问控制活动（允许或拒绝的连接）。	5.0+
url_reputation_stats_current_timeframe，第 5-17 页	按所请求网站的信誉划分的流量和系统访问控制活动（允许或拒绝的连接）。	5.0+

表 5-1　应用和 URL 统计表（续）

请参阅	存储有关以下内容的统计数据的表...	版本
user_ids_stats_current_timeframe，第 5-19 页	按用户划分的访问控制和入侵防御活动。	5.0+
user_stats_current_timeframe，第 5-20 页	按用户划分的流量和系统访问控制活动（允许或拒绝的连接）。	5.0+

了解统计跟踪表

表的名称以 **current_day**、**current_month** 或 **current_year** 结尾，表示其数据的时间范围。例如，**app_ids_stats_current_***timeframe* 描述的是 **app_stats_current_day**、**app_stats_current_month** 和 **app_stats_current_year**。**app_stats_current_year** 表存储 360 天的统计数据；**current_month** 表存储 30 天的统计数据。

每次防御中心从网络中的受管设备接收原始计数时，它会更新全部三个表类型，但是分辨率会依次降低。**current_day** 表的时间分辨率最高（15 秒或 5 分钟，取决于特定的表）；**current_year** 表的时间分辨率最低（24 小时）。有关具体信息，请参阅统计跟踪表的存储特性，第 5-2 页。

统计跟踪表的存储特性

有关重要的详细信息，请参阅下表。

表 5-2　统计表的存储特性

表类型	间隔（分辨率）	存储寿命
current_day	15 秒： **app_ids_stats_current_***timeframe* 和 **user_ids_stats_current_***timeframe*	当前间隔加前 24 小时的所有间隔
	5 分钟： **app_stats_current_***timeframe*、 **user_stats_current_***timeframe*、 **url_category_stats_current_***timeframe* 和 **url_reputation_stats_current_***timeframe*	当前间隔加前 24 小时的所有间隔
current_month	1 小时	当前小时加前 30 天的小时数
current_year	24 小时	当日加前 360 天

存储间隔由其开始时间定义。例如，**current_month** 表包含 `10:00:00 - 10:59:59` 这一个小时的计数，作为一条以 `10:00:00` 为时间戳的记录。请注意，一天开始于 `00:00:00`，结束于 `23:59:59`。间隔开始时间存储为 UNIX 时间戳 (GMT)。

指定查询统计表时的时间间隔

查询的有效时间间隔由表和查询中的 time_start_sec 字段定义。

例如，如果您的 SQL 语句指定 time_start_sec = 6:00:00，则各个表类型的间隔会有所差异：

- 对于 **current_day** 表：6:00:00 至 6:00:14（对于 15 秒的表）或 6:00:00 至 6:04:59（对于 5 分钟的表）。
- 对于 **current_month** 表：6:00:00 至 6:59:59。
- 对于 **current_year** 表：次日 0:00:00 至 23:59:59。

检索数据最简单的方式是规定间隔开始时间。例如，要从 **app_ids_stats_current_day** 表进行检索，可指定以下其中一个时间：

```
00:00:00
00:00:15
00:00:30
23:59:45
```

如果您的查询包含间隔开始时间之外的时间戳，则系统会对请求进行如下修改：

- 将开始时间向上舍入为最近的间隔时间
- 将结束时间向下舍入为最近的间隔时间

例如，以下查询向上舍入开始时间：

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec = UNIX_TIMESTAMP("2011-12-01 12:30:00");
```

并且等同于：

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec = UNIX_TIMESTAMP("2011-12-01 01:00:00");
```

查询一系列间隔时，开始时间间隔向上舍入，结束时间间隔向下舍入。例如：

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec BETWEEN UNIX_TIMESTAMP("2011-12-10 12:59:00") and
UNIX_TIMESTAMP("2011-12-10 16:28:00");
```

被改为：

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec BETWEEN UNIX_TIMESTAMP("2011-12-10 13:00:00") and
UNIX_TIMESTAMP("2011-12-12 16:00:00");
```

如果查询间隔超出表的时间范围，尽管其他表中数据的时间分辨率会更低，您通常仍可从其他表获得额外数据。例如，要检索最近两天的带宽使用量，您可从 **current_day** 表获得昨天的结果（5 分钟分辨率），但您仅可从 **current_month**（以小时为单位）或 **current_year**（以天为单位）获得前一天的统计数据。

app_ids_stats_current_timeframe

app_ids_stats_current_*timeframe* 表包含有关您监控的网络中应用活动和入侵事件的统计数据。可以按照所检测的应用、应用类型（应用协议、客户端应用或 Web 应用）以及应用的风险和业务相关性来提取统计数据。这些表还会跟踪由于违反入侵策略而被阻止的连接以及入侵的预计潜在影响。

要了解 **current_day**、**current_month** 和 **current_year** 统计表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关 **app_ids_stats_current_***timeframe* 表的详细信息，请参阅以下各节：

- app_ids_stats_current_timeframe 字段，第 5-4 页
- app_ids_stats_current_timeframe 联合，第 5-5 页
- app_ids_stats_current_timeframe 示例查询，第 5-5 页

app_ids_stats_current_timeframe 字段

下表说明您可以在 **app_ids_stats_current_***timeframe* 表中访问的字段。此类型的所有表都包含相同的字段。

表 5-3　　app_ids_stats_current_timeframe 字段

字段	说明
application_id	应用的内部标别号。
application_name	在用户界面上显示的应用名称。
blocked	由于违反入侵策略而被阻止的连接数量。
business_relevance	应用与企业工作效率的相关性指数（1 至 5），其中 1 表示极低，5 表示极高。
business_relevance_description	对业务相关性的说明（very low、low、medium、high、very high）。
impact_level_1	针对应用记录的影响级别为 1（易受攻击）的入侵事件数量。
impact_level_2	影响级别为 2（可能易受攻击）的入侵事件数量。
impact_level_3	影响级别为 3（主机目前不易受攻击）的入侵事件数量。
impact_level_4	影响级别为 4（未知目标）的入侵事件数量。
impact_level_5	影响级别为 5（未知漏洞）的入侵事件数量。
is_client_application	指示所检测的应用是否为客户端应用的一个真假标志。
is_server_application	指示所检测的应用是否为应用协议的一个真假标志。
is_web_application	指示所检测的应用是否为 Web 应用的一个真假标志。
risk	应用的预估风险指数（1 至 5），其中 1 表示风险极低，5 表示严重风险。
risk_description	对预估风险的描述（very low、low、medium、high、critical）。
sensor_address	生成事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_id	提供事件的设备的 ID。
sensor_name	生成入侵事件的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。

表 5-3　app_ids_stats_current_timeframe 字段（续）

字段	说明
start_time_sec	测量间隔开始日期和时间的 UNIX 时间戳。有关详细信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。
would_have_dropped	如果在内嵌式部署中已将入侵策略配置为丢弃数据包，则表示已丢弃的数据包的数量。

app_ids_stats_current_timeframe 联合

下表说明您可以在 **app_ids_stats_current_*timeframe*** 表上执行的联合。

表 5-4　app_ids_stats_current_timeframe 联合

您可以联合此表……	与……
application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id

app_ids_stats_current_timeframe 示例查询

以下查询返回最多 25 条来自 **app_ids_stats_current_month** 表的应用记录。每条记录都包含在此时间间隔内应用的受阻止连接和入侵事件的数量。

```
SELECT from_unixtime(start_time_sec), sum(blocked)

FROM app_ids_stats_current_day

WHERE start_time_sec = unix_timestamp("2013-12-15");
```

app_stats_current_timeframe

app_stats_current_*timeframe* 表包含按照应用和监控流量的设备划分的有关带宽使用量和访问控制操作的统计数据。您可以按照应用的业务相关性、预估风险和类型过滤这些统计数据。

要了解 **current_day**、**current_month** 和 **current_year** 统计表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关 **app_stats_current_*timeframe*** 表的详细信息，请参阅以下各节：

app_stats_current_timeframe 字段

下表说明您可以在 **app_stats_current_*timeframe*** 表中访问的字段。

表 5-5　app_stats_current_timeframe 字段

字段	说明
application_id	应用的内部标别号。
application_name	在用户界面上显示的应用名称。
business_relevance	应用与企业工作效率的相关性指数（1 至 5），其中 1 表示极低，5 表示极高。
business_relevance_description	对业务相关性的说明（very low、low、medium、high、very high）。
bytes_in	在指定的间隔内应用的入站流量字节数。
bytes_out	在指定的间隔内应用的出站流量字节数。
connections_allowed	允许的连接数量。
connections_denied	由于违反访问控制策略而被拒绝的连接数量。
is_client_application	指示所检测的应用是否为客户端应用的一个真假标志。
is_server_application	指示所检测的应用是否为应用协议的一个真假标志。
is_web_application	指示所检测的应用是否为 Web 应用的一个真假标志。
risk	应用的预估风险指数（1 至 5），其中 1 表示风险极低，5 表示严重风险。
risk_description	对预估风险的描述（very low、low、medium、high、critical）。
sensor_address	监控流量的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_id	检测流量的受管设备的内部标识号。
sensor_name	检测流量的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
start_time_sec	测量间隔开始的 UNIX 时间戳。有关指定开始时间的信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。

app_stats_current_timeframe 联合

下表说明您可以在 **app_stats_current_*timeframe*** 表上执行的联合。

表 5-6　app_stats_current_timeframe 联合

您可以联合此表……	与……
application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id

app_stats_current_timeframe 示例查询

对于与防御中心连接的所有受管设备，以下查询返回一天内与业务相关性低且风险高的应用关联的入站和出站流量负载。

```
SELECT start_time_sec, sum(bytes_in), sum(bytes_out)
FROM app_stats_current_day
WHERE business_relevance <= 2
AND risk >= 4 AND start_time_sec = unix_timestamp("2013-12-15");
```

geolocation_stats_current_timeframe

geolocation_stats_*timeframe* 表包含有关基于位置级别的入侵事件的统计数据。可以根据影响级别、设备和处理数据包的方式提取统计数据。

要了解 **current_day**、**current_month** 和 **current_year** 统计表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关 **geolocation_stats_current_***timeframe* 表的详细信息，请参阅以下各节：

geolocation_stats_current_timeframe 字段

下表说明您可以在 **geolocation_stats_current_***timeframe* 表中访问的字段。此类型的所有表都包含相同的字段。

表 5-7　　geolocation_stats_current_timeframe 字段

字段	说明
bytes_from	会话响应方传输的总字节数。
bytes_to	会话发起方发送的总字节数。
destination_continent	目标主机的大陆名称。 ** - 未知 na - 北美洲 as - 亚洲 af - 非洲 eu - 欧洲 sa - 南美洲 au - 澳大利亚 an - 南极洲
destination_country	目标主机的国家/地区代码。
flows_allowed	允许的流数量。

表 5-7　geolocation_stats_current_timeframe 字段（续）

字段	说明
flows_denied	由于违反访问控制策略而被拒绝的流数量。
sensor_address	生成事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_id	提供事件的设备的 ID。
sensor_name	生成入侵事件的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
source_continent	源主机的大陆名称。 ** - 未知 na - 北美洲 as - 亚洲 af - 非洲 eu - 欧洲 sa - 南美洲 au - 澳大利亚 an - 南极洲
source_country	源主机的国家/地区代码。
start_time_sec	测量间隔开始日期和时间的 UNIX 时间戳。有关详细信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。

geolocation_stats_current_timeframe 联合

您无法在 **geolocation_stats_current_***timeframe* 表上执行联合。

geolocation_stats_current_timeframe 示例查询

以下查询返回当日来自亚洲的前 25 个连接事件的源国家/地区和传感器名称。

```
SELECT sensor_name, source_continent
FROM geolocation_stats_current_year
WHERE destination_continent='as'
LIMIT 20;
```

ids_impact_stats_current_timeframe

ids_impact_stats_*timeframe* 表包含有关基于影响级别的入侵事件的统计数据。可以根据影响级别、设备和处理数据包的方式提取统计数据。

要了解 **current_day**、**current_month** 和 **current_year** 统计表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关 **ids_impact_stats_current_***timeframe* 表的详细信息，请参阅以下各节：

ids_impact_stats_current_timeframe 字段

下表说明您可以在 **ids_impact_stats_current_***timeframe* 表中访问的字段。此类型的所有表都包含相同的字段。

表 5-8　　ids_impact_stats_current_timeframe 字段

字段	说明
blocked	由于违反入侵策略而被阻止的连接数量。
impact_level_1	针对应用记录的影响级别为 1（易受攻击）的入侵事件数量。
impact_level_2	影响级别为 2（可能易受攻击）的入侵事件数量。
impact_level_3	影响级别为 3（主机目前不易受攻击）的入侵事件数量。
impact_level_4	影响级别为 4（未知目标）的入侵事件数量。
impact_level_5	影响级别为 5（未知漏洞）的入侵事件数量。
sensor_address	生成事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_id	提供事件的设备的 ID。
sensor_name	生成入侵事件的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
start_time_sec	测量间隔开始日期和时间的 UNIX 时间戳。有关详细信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。
would_have_dropped	如果在内嵌式部署中已将入侵策略设置为丢弃数据包，则表示已丢弃的数据包的数量。

ids_impact_stats_current_timeframe 联合

您无法在 **ids_impact_stats_current_***timeframe* 表上执行联合。

ids_impact_stats_current_timeframe 示例查询

以下查询返回当日前 25 个 blocked 和 would_have_dropped 事件。

```
SELECT blocked, would_have_dropped
FROM ids_impact_stats_current_year
LIMIT 25;
```

session_stats_current_timeframe

session_stats_*timeframe* 表包含所有连接的统计数据。可以根据字节、连接、传感器和时间提取统计数据。

要了解 **current_day**、**current_month** 和 **current_year** 统计表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关 **session_stats_current_***timeframe* 表的详细信息，请参阅以下各节：

- session_stats_current_timeframe 字段，第 5-10 页
- session_stats_current_timeframe 联合，第 5-10 页
- session_stats_current_timeframe 示例查询，第 5-10 页

session_stats_current_timeframe 字段

下表说明您可以在 **session_stats_current_***timeframe* 表中访问的字段。此类型的所有表都包含相同的字段。

表 5-9　session_stats_current_timeframe 字段

字段	说明
bytes_in	在指定的间隔内的入站流量字节数。
bytes_out	在指定的间隔内的出站流量字节数。
connections_allowed	对于指定的 URL 类别所允许的连接数量。
connections_denied	对于指定的 URL 类别，由于违反访问控制策略而被拒绝的连接数量。
id	此字段未使用而且会始终返回 0。
sensor_address	生成事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_id	提供事件的设备的 ID。
sensor_name	生成入侵事件的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
start_time_sec	测量间隔开始日期和时间的 UNIX 时间戳。有关详细信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。

session_stats_current_timeframe 联合

您无法在 **session_stats_current_***timeframe* 表上执行联合。

session_stats_current_timeframe 示例查询

以下查询对每个传感器返回当日被拒绝和允许的连接的数量，按照 sensor_name 降序排列。

```
SELECT sensor_name, connections_denied, connections_allowed
FROM session_stats_current_day
ORDER BY sensor_id DESC;
```

ssl_stats_current_timeframe

ssl_stats_current_*timeframe* 表包含 SSL 连接的统计数据。可以根据字节、连接、传感器和时间提取统计数据。

要了解 **current_day**、**current_month** 和 **current_year** 统计表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关 **ssl_stats_current_***timeframe* 表的详细信息，请参阅以下各节：

- ssl_stats_current_timeframe 字段，第 5-11 页
- ssl_stats_current_timeframe 联合，第 5-13 页
- ssl_stats_current_timeframe 示例查询，第 5-13 页

ssl_stats_current_timeframe 字段

下表说明您可以在 **ssl_stats_current_***timeframe* 表中访问的字段。此类型的所有表都包含相同的字段。

表 5-10　ssl_stats_current_timeframe 字段

字段	说明
block	在未重置的情况下丢弃的 SSL 会话数量。
block_with_reset	在重置的情况下丢弃的 SSL 会话数量。
cached_session	在会话缓存中找到的 SSL 会话数量。
cannot_determine_verdict	评估 SSL 规则期间发生的握手错误数量。
cert_expired	证书已过期的 SSL 会话数量。
cert_invalid_issuer	证书颁发者无效或在可信 CA 列表内找不到的 SSL 会话的数量。
cert_invalid_signature	证书签名无效的 SSL 会话数量。
cert_not_checked	证书未检查的 SSL 会话数量。
cert_not_yet_valid	证书尚无效的 SSL 会话数量。
cert_revoked	证书被撤销的 SSL 会话数量。
cert_self_signed	证书为自签的 SSL 会话数量。
cert_unknown	证书状态未知的 SSL 会话数量。
cert_valid	证书有效的 SSL 会话数量。
cert_validation_cache_hit	在验证缓存中找到证书的次数。
cert_validation_cache_miss	在验证缓存中未找到证书的次数。
decrypt_resign_self_signed	使用自签证书的 SSL 会话借助解密重签方法被解密的次数。
decrypt_resign_self_signed_replace_key_only	使用自签证书的 SSL 会话借助仅含替换密钥的解密重签方法被解密的次数。
decrypt_resign_signed_cert	使用签名证书的 SSL 会话借助解密重签方法被解密的次数。
decrypt_with_known_key	SSL 会话借助已知密钥方法被解密的次数。
decryption_error	在解密期间出现错误的 SSL 会话数量。
do_not_decrypt	SSL 会话被发现但未被解密的次数。

表 5-10　ssl_stats_current_timeframe 字段（续）

字段	说明
handshake_error	评估 SSL 规则之前发生的握手错误数量。
orig_cert_cache_hit	在缓存中找到原始证书的次数。
orig_cert_cache_miss	在缓存中未找到原始证书的次数。
resigned_cert_cache_hit	在缓存中找到重签证书的次数。
resigned_cert_cache_miss	在缓存中未找到重签证书的次数。
sensor_address	生成事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_id	提供事件的设备的 ID。
sensor_name	生成事件的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
session_cache_hit	在缓存中找到 SSL 会话 ID 或通知单的次数。
session_cache_miss	在缓存中未找到 SSL 会话 ID 或通知单的次数。
session_incorrectly_identified_as_ssl	被错误地识别为 SSL 的会话数量。
ssl_compression	使用 SSL 压缩的会话数量。
ssl_sessions_decrypted	被成功解密的 SSL 会话数量。
ssl_sessions_not_decrypted	未被成功解密的 SSL 会话数量。
ssl_sessions_reused_by_id	SSL 会话重新使用 ID 的次数。
ssl_sessions_reused_by_ticket	SSL 会话重新使用通知单的次数。
ssl_sessions_with_errors	存在错误的 SSL 会话数量。
ssl_v20	使用 SSL 2.0 版本 的 SSL 会话数量。
ssl_v30	使用 SSL 3.0 版本 的 SSL 会话数量。
ssl_version_unknown	使用未知 SSL 版本的 SSL 会话数量。
start_time_sec	测量间隔开始日期和时间的 UNIX 时间戳。有关详细信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。
tls_v10	使用 TLS 1.0 版本的 SSL 会话数量。
tls_v11	使用 TLS 1.1 版本的 SSL 会话数量。
tls_v12	使用 TLS 1.2 版本的 SSL 会话数量。
total_ssl_sessions	检测到的 SSL 会话的总数。
uncached_session	ID 或通知单上的缓存缺失阻止解密的次数。
undecryptable_in_passive_mode	由于设备处于被动模式而无法解密的 SSL 会话数量。
unknown_cipher_suite	使用未知加密套件的 SSL 会话数量。
unsupported_cipher_suite	使用已知但却不受支持的加密套件的 SSL 会话数量。

ssl_stats_current_timeframe 联合

您无法在 **ssl_stats_current_***timeframe* 表上执行联合。

ssl_stats_current_timeframe 示例查询

以下查询对每个传感器返回当日的 SSL 会话数量、已解密的会话、未解密的会话以及在被动模式下无法解密的会话，按照 sensor_name 降序排列。

```
SELECT sensor_name, total_ssl_sessions, ssl_sessions_decrypted,
ssl_sessions_not_decrypted, undecryptable_in_passive_mode
FROM ssl_stats_current_day
ORDER BY sensor_id DESC;
```

storage_stats_by_disposition_current_timeframe

storage_stats_by_disposition_*timeframe* 表包含存储文件的统计数据。可以根据字节、连接、传感器和时间提取统计数据。

要了解 **current_day**、**current_month** 和 **current_year** 统计表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关 **storage_stats_by_disposition_***timeframe* 表的详细信息，请参阅以下个节：

- storage_stats_by_disposition_current_timeframe 字段，第 5-13 页
- storage_stats_by_disposition_current_timeframe 联合，第 5-14 页
- storage_stats_by_disposition_current_timeframe 示例查询，第 5-14 页

storage_stats_by_disposition_current_timeframe 字段

下表说明您可以在 **storage_stats_by_disposition_current_***timeframe* 表中访问的字段。此类型的所有表都包含相同的字段。

表 5-11　storage_stats_by_disposition_current_timeframe 字段

字段	说明
bytes_written	文件大小（字节）。
disposition	文件的恶意软件状态。可能的值包括： • CLEAN - 文件是安全的，不包含恶意软件。 • UNKNOWN - 不确定文件是否包含恶意软件。 • MALWARE - 文件包含恶意软件。 • UNAVAILABLE - 软件无法向思科云发送请求以了解处置情况，或思科云服务未响应此请求。 • CUSTOM SIGNATURE - 文件与用户定义的哈希匹配，并且以用户指定的方式进行处理。
number_dropped	此性质的文件被丢弃的数量。

表 5-11　storage_stats_by_disposition_current_timeframe 字段（续）

字段	说明
number_stored	此性质的文件被存储的数量。
sensor	检测到文件的设备的 ID。
sensor_address	生成事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_name	生成入侵事件的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
start_time_sec	测量间隔开始日期和时间的 UNIX 时间戳。有关详细信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。

storage_stats_by_disposition_current_timeframe 联合

您无法在 **session_stats_current_***timeframe* 表上执行联合。

storage_stats_by_disposition_current_timeframe 示例查询

以下查询对每个传感器返回当日被丢弃和存储的文件数量，按照 sensor_name 降序排列。

```
SELECT sensor_name, number_dropped, number_stored
FROM storage_stats_by_disposition_current_day
ORDER BY sensor_name DESC;
```

storage_stats_by_file_type_current_timeframe

storage_stats_by_file_type_current_*timeframe* 表包含按照文件类型划分的已存储文件的统计数据。可以根据字节、连接、传感器和时间提取统计数据。

要了解 **current_day**、**current_month** 和 **current_year** 统计表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关 **storage_stats_by_file_type_current_*timeframe*** 表的详细信息，请参阅以下各节：

storage_stats_by_file_type_current_timeframe 字段

下表说明您可以在 **storage_stats_by_file_type_current_***timeframe* 表中访问的字段。此类型的所有表都包含相同的字段。

表 5-12　storage_stats_by_file_type_current_timeframe 字段

字段	说明
bytes_written	文件大小（字节）。
file_type	被检测或隔离文件的文件类型。
file_type_id	映射至文件类型的 ID 编号。
number_dropped	被丢弃的此类型文件的数量。
number_stored	存储的此类型文件的数量。
sensor	检测到文件的设备的 ID。
sensor_address	生成事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_name	生成入侵事件的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
start_time_sec	测量间隔开始日期和时间的 UNIX 时间戳。有关详细信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。

storage_stats_by_file_type_current_timeframe 联合

您无法在 **session_stats_current_***timeframe* 表上执行联合。

storage_stats_by_file_type_current_timeframe 示例查询

以下查询对每个传感器返回当日被丢弃和存储的文件数量，按照 file_type 降序排列。

```
SELECT sensor_name, number_dropped, number_stored, file_type
FROM storage_stats_by_file_type_current_day
ORDER BY file_type DESC;
```

transmission_stats_by_file_type_current_timeframe

transmission_stats_by_file_type_current_*timeframe* 表包含按照文件类型划分的已存储文件的统计数据。可以根据字节、连接、传感器和时间提取统计数据。

要了解 **current_day**、**current_month** 和 **current_year** 统计表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关 **transmission_stats_by_file_type_current_***timeframe* 表的详细信息，请参阅以下各节：

transmission_stats_by_file_type_current_timeframe 字段

下表说明您可以在 **storage_stats_by_file_type_current_***timeframe* 表中访问的字段。此类型的所有表都包含相同的字段。

表 5-13　transmission_stats_by_file_type_current_timeframe 字段

字段	说明
bytes_sent	传输的字节数。
file_type	被检测或隔离文件的文件类型。
file_type_id	映射至文件类型的 ID 编号。
number_dropped	被丢弃的此类型文件的数量。
number_sent	被发送的此类型文件的数量。
sensor	检测到文件的设备的 ID。
sensor_address	生成事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_name	生成入侵事件的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
start_time_sec	测量间隔开始日期和时间的 UNIX 时间戳。有关详细信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。

transmission_stats_by_file_type_current_timeframe 联合

您无法在 **transmission_stats_current_***timeframe* 表上执行联合。

transmission_stats_by_file_type_current_timeframe 示例查询

以下查询对每个传感器返回当日被丢弃和发送的连接数量，按照 file_type 降序排列。

```
SELECT sensor_name, number_dropped, number_sent, file_type

FROM transmission_stats_by_file_type_current_day

ORDER BY file_type DESC;
```

url_category_stats_current_timeframe

url_category_stats_current_*timeframe* 表包含指定 URL 类别中与 URL 请求关联的连接和带宽使用量的统计数据。您也可以限制对监控流量的受管设备的查询。

要了解 **current_day**、**current_month** 和 **current_year** 统计表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关 **url_category_stats_current_***timeframe* 表的详细信息，请参阅以下各节：

- url_category_stats_current_timeframe 字段，第 5-17 页
- url_category_stats_current_timeframe 联合，第 5-17 页
- url_category_stats_current_timeframe 示例查询，第 5-17 页

url_category_stats_current_timeframe 字段

下表说明您可以在 **url_category_stats_current_***timeframe* 表中访问的字段。

表 5-14　url_category_stats_current_timeframe 字段

字段	说明
bytes_in	在指定的间隔内的入站流量字节数。
bytes_out	在指定的间隔内的出站流量字节数。
category	URL 的类别。
connections_allowed	对于指定的 URL 类别所允许的连接数量。
connections_denied	对于指定的 URL 类别，由于违反访问控制策略而被拒绝的连接数量。
sensor_address	监控流量的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_id	检测流量的受管设备的内部标识号。
sensor_name	监控流量的受管设备。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
start_time_sec	测量间隔开始的 UNIX 时间戳。有关指定开始时间的信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。

url_category_stats_current_timeframe 联合

您无法在 **url_category_stats_current_***timeframe* 表上执行联合。

url_category_stats_current_timeframe 示例查询

以下查询返回最多 25 条 URL 类别记录。每条记录均包含在指定时间间隔内的关联入站和出站流量的字节数以及允许和拒绝的连接。

```
SELECT category, sensor_name, sensor_address, start_time_sec, bytes_in, bytes_out,
connections_allowed, connections_denied

FROM url_category_stats_current_year

WHERE category="Games"

LIMIT 0, 25;
```

url_reputation_stats_current_timeframe

url_reputation_stats_current_*timeframe* 表包含与指定信誉的 URL 请求关联的连接和带宽使用量的统计数据。也可以在监控流量的受管设备上限制查询结果。

要了解 **current_day**、**current_month** 和 **current_year** 统计表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关 **url_reputation_stats_current_***timeframe* 表的详细信息，请参阅以下各节：

- url_reputation_stats_current_timeframe 字段，第 5-18 页
- url_reputation_stats_current_timeframe 联合，第 5-18 页
- url_reputation_stats_current_timeframe 示例查询，第 5-18 页

url_reputation_stats_current_timeframe 字段

下表说明您可以在 **url_category_stats_current_*timeframe*** 表中访问的字段。

表 5-15　url_reputation_stats_current_timeframe 字段

字段	说明
bytes_in	在指定的间隔内的入站流量字节数。
bytes_out	在指定的间隔内的出站流量字节数。
connections_allowed	允许的连接数量。
connections_denied	由于违反访问控制策略而被拒绝的连接数量。
reputation	与所请求的 URL 关联的风险。以下项之一： • High risk • Suspicious site • Benign site with security risks • Benign site • Well known • Risk unknown
sensor_address	监控流量的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_id	监控流量的受管设备的内部标识号。
sensor_name	监控流量的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
start_time_sec	测量间隔开始的 UNIX 时间戳。有关指定开始时间的信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。

url_reputation_stats_current_timeframe 联合

您无法在 **url_reputation_stats_current_*timeframe*** 表上执行联合。

url_reputation_stats_current_timeframe 示例查询

以下查询返回最多 25 条来自 **url_reputation_stats_current_month** 表的信誉记录。每条记录均包含在测量时间间隔内入站和出站流量的字节数以及允许和拒绝的连接。

```
SELECT sensor_name, sensor_address, reputation, start_time_sec, bytes_in, bytes_out,
connections_allowed, connections_denied

FROM url_reputation_stats_current_year

WHERE reputation="High risk"

LIMIT 0, 25;
```

user_ids_stats_current_timeframe

user_ids_stats_current_*timeframe* 表为轮询表，包含访问过滤统计数据以及按用户划分的影响统计数据。

要了解这种类型的 **current_day**、**current_month** 和 **current_year** 表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关使用轮询统计表的一般信息，请参阅了解统计跟踪表，第 5-2 页。

有关 **user_ids_stats_current_***timeframe* 表的详细信息，请参阅以下各节：

user_ids_stats_current_timeframe 字段

下表说明您可以在 **user_ids_stats_current_***timeframe* 表中访问的字段。

表 5-16　user_ids_stats_current_timeframe 字段

字段	说明
blocked	由于违反入侵策略而被阻止的连接数量。
impact_level_1	为用户记录的影响级别为 1（易受攻击）的入侵事件数量。
impact_level_2	为用户记录的影响级别为 2（可能易受攻击）的入侵事件数量。
impact_level_3	为用户记录的影响级别为 3（主机目前不易受攻击）的入侵事件数量。
impact_level_4	为用户记录的影响级别为 4（未知目标）的入侵事件数量。
impact_level_5	为用户记录的影响级别为 5（未知漏洞）的入侵事件数量。
sensor_address	监控流量的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_id	检测流量的受管设备的内部标识号。
sensor_name	检测流量的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
start_time_sec	测量间隔开始的 UNIX 时间戳。有关指定开始时间的信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。
user_id	最后登录主机的用户的内部标识号。
username	最后登录主机的用户的用户名。
would_have_dropped	如果在内嵌式部署中已将入侵策略配置为丢弃数据包，则表示已丢弃的数据包的数量。

user_ids_stats_current_timeframe 联合

您无法在 **user_ids_stats_current_***timeframe* 表上执行联合。

user_ids_stats_current_timeframe 示例查询

以下查询返回最多 25 条来自 **user_ids_stats_current_month** 表的用户记录。每个记录都包含所选 username 的阻止连接和入侵事件的数量。

```
SELECT username, start_time_sec, blocked, impact_level_1, impact_level_2,
impact_level_3, impact_level_4, impact_level_5 FROM user_ids_stats_current_year
WHERE username="username"
LIMIT 0, 25;
```

user_stats_current_timeframe

user_stats_current_*timeframe* 表包含按用户划分的带宽使用量和访问控制操作（允许或拒绝的连接）的统计数据。您也可以限制对监控流量的受管设备的查询。

要了解 **current_day**、**current_month** 和 **current_year** 统计表，请参阅统计跟踪表的存储特性，第 5-2 页。

有关详细信息，请参阅以下各节：

user_stats_current_timeframe 字段

下表说明您可以在 **user_stats_current_***timeframe* 表中访问的字段。

表 5-17　user_stats_current_timeframe 字段

字段	说明
bytes_in	在测量间隔内对于此用户入站流量的字节数。
bytes_out	在测量间隔内对于此用户出站流量的字节数。
connections_allowed	在测量时间段内对于此用户所允许的连接数量。
connections_denied	对于此用户由于违反访问控制策略而被拒绝的连接数量。
sensor_address	监控流量的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_id	检测流量的受管设备的内部标识号。
sensor_name	检测流量的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
start_time_sec	测量间隔开始的 UNIX 时间戳。有关指定开始时间的信息，请参阅指定查询统计表时的时间间隔，第 5-3 页。
user_id	最后登录到生成流量的主机的用户的内部标识号。
username	最后登录到生成流量的主机的用户的用户名。

user_stats_current_timeframe 联合

您无法在 **user_stats_current_***timeframe* 表上执行联合。

user_stats_current_timeframe 示例查询

以下查询返回最多 25 条用户记录。每条记录均包含在测量时间间隔内入站和出站流量的字节数以及允许和拒绝的连接。

```
SELECT sensor_name, sensor_address, username, start_time_sec, bytes_in, bytes_out,
connections_allowed, connections_denied
FROM user_stats_current_year
WHERE username="username" LIMIT 0, 25;
```

第 6 章

方案：发现事件和网络映射表

本章包含有关适用于发现事件和思科网络映射相关的表的方案和所支持的联合信息。

FireSIGHT 系统在监控主机和网络设备所产生的流量时持续生成发现事件。

网络映射是关于发现事件中报告的网络资产的信息的存储库。对于每个检测到的主机和网络设备，网络映射都包含操作系统、服务器、客户端应用、主机属性、漏洞等信息。

漏洞是对主机可能容易遭受的具体威胁或漏洞攻击的说明。思科维护自己的漏洞数据库 (VDB)，此数据库交叉参考 Bugtraq 数据库和 MITRE 的 CVE 数据库。您还可以使用主机输入功能，导入第三方漏洞数据。

请注意，网络映射中关于特定主机的信息可能会根据主机的类型以及受监控流量中可用的信息而不同。

有关详细信息，请参阅下表列出的各节。Version 列指示支持各表的 FireSIGHT 系统版本。虽然当前产品版本中继续支持已弃用的表，但是思科**强烈**建议避免使用已弃用的表和字段，以确保将来继续获得支持。

表 6-1　　发现事件和网络映射表的方案

请参阅……	存储有关以下内容的信息的表…	版本
application_host_map，第 6-4 页	在监控网络中主机上检测到的应用。	5.0+
application_ip_map，第 A-1 页	与在监控网络中检测到的应用关联的类别、标记、工作效率和风险。	5.2+
application_ip_map，第 A-1 页	与在监控网络中检测到的应用关联的类别、标记、工作效率和风险。 在 5.2 版本中已弃用。由 application_ip_map，第 A-1 页替代。	5.0-5.1.x
application_tag_map，第 6-7 页	与在监控网络中检测到的应用关联的标记。	5.0+
network_discovery_event，第 6-9 页	发现和主机输入事件。	5.0+
rna_host，第 6-10 页	关于监控网络中主机的基本信息。	5.2+
rna_host_attribute，第 6-12 页	与监控网络中的每台主机关联的主机属性。	5.2+
rna_host_client_app，第 6-14 页	在监控网络中主机上检测到的客户端应用。	5.2+
rna_host_client_app，第 6-14 页	与在监控网络中主机上检测到的 HTTP（Web 浏览器）客户端应用关联的负载。	5.2+
rna_host_ioc_state，第 6-19 页	存储主机的威胁状态。	5.3+
rna_host_ip_map，第 6-23 页	针对监控网络中的主机将主机 ID 与 MAC 地址关联。	5.2+
rna_host_os，第 6-26 页	在监控网络中主机上检测到的操作系统。	5.2+

表 6-1　发现事件和网络映射表的方案（续）

请参阅……	存储有关以下内容的信息的表...	版本
rna_host_os_vulns，第 6-27 页	与监控网络中的主机关联的漏洞。	5.2+
rna_host_protocol，第 6-29 页	在监控网络中主机上检测到的协议。	4.10.x+
rna_host_protocol，第 6-29 页	监控网络中与检测到主机的受管设备相关的主机。	5.2+
rna_host_service，第 6-32 页	在监控网络中主机上检测到的服务。	5.2+
rna_host_service_banner，第 6-34 页	网络流量中作为在监控网络中主机上检测到的服务的服务供应商和版本（“横幅”）广告的标题。	5.2+
rna_host_service_info，第 6-35 页	在监控网络中主机上检测到的服务的详细信息。	5.2+
rna_host_service_payload，第 6-38 页	与在监控网络中主机上检测到的服务关联的负载。	5.2+
rna_host_service_subtype，第 6-41 页	在监控网络中主机上检测到的服务的子服务。	5.2+
rna_host_service_vulns，第 6-42 页	与在监控网络中主机上检测到的服务关联的漏洞。	5.2+
rna_host_third_party_vuln，第 6-43 页	与监控网络中的主机关联的第三方漏洞。	5.2+
rna_host_third_party_vuln_bugtraq_id，第 6-45 页	与监控网络中的主机关联而且还与 Bugtraq 数据库中的漏洞关联的第三方漏洞 (http://www.securityfocus.com/bid/)。	5.2+
rna_host_third_party_vuln_cve_id，第 6-46 页	与监控网络中的主机关联而且还与 MITRE 的 CVE 数据库中的漏洞关联的第三方漏洞。 (http://www.cve.mitre.org/)。	5.2+
rna_host_third_party_vuln_rna_id，第 6-48 页	与监控网络中的主机关联而且还与 VDB 中的漏洞关联的第三方漏洞。	5.2+
rna_ip_host，第 A-1 页	关于监控网络中 IP 主机的基本信息。 在 5.2 版本中已弃用。由 **rna_host，第 6-10 页**替代。	4.10.x-5.1.x
rna_ip_host_client_app，第 A-1 页	在监控网络中主机上检测到的客户端应用。 在 5.2 版本中已弃用。由 **rna_host_client_app，第 6-14 页**替代。	4.10.x-5.1.x
rna_ip_host_client_app_payload，第 A-1 页	与在监控网络中 IP 主机上检测到的 HTTP（Web 浏览器）客户端应用关联的负载。 在 5.2 版本中已弃用。由 **rna_host_client_app，第 6-14 页**替代。	4.10.x-5.1.x
rna_ip_host_os，第 A-1 页	在监控网络中 IP 主机上检测到的操作系统。 在 5.2 版本中已弃用。由 **rna_host_os，第 6-26 页**替代。	4.10.x-5.1.x
rna_ip_host_os_vulns，第 A-1 页	与监控网络中的 IP 主机关联的漏洞。 在 5.2 版本中已弃用。由 **rna_host_os_vulns，第 6-27 页**替代。	4.10.x--5.1.x
rna_ip_host_sensor，第 A-1 页	监控网络中与检测到 IP 主机的受管设备相关的 IP 主机。 在 5.2 版本中已弃用。由 **rna_host_protocol，第 6-29 页**替代。	5.0-5.1.x

表 6-1　发现事件和网络映射表的方案（续）

请参阅……	存储有关以下内容的信息的表…	版本
rna_ip_host_service，第 A-1 页	在监控网络中 IP 主机上检测到的服务。 在 5.2 版本中已弃用。由 **rna_host_service，第 6-32 页**替代。	4.10.x-5.1.x
rna_ip_host_service_banner，第 A-1 页	网络流量中作为在监控网络中主机上检测到的服务的服务供应商和版本（“横幅”）广告的标题。 在 5.2 版本中已弃用。由 **rna_host_service_banner，第 6-34 页**替代。	4.10.x-5.1.x
rna_ip_host_service_info，第 A-1 页	在监控网络中 IP 主机上检测到的服务的详细信息。 在 5.2 版本中已弃用。由 **rna_host_service_info，第 6-35 页**替代。	4.10.x-5.1.x
rna_ip_host_service_payload，第 A-1 页	与在监控网络中 IP 主机上检测到的服务关联的负载。 在 5.2 版本中已弃用。由 **rna_host_service_payload，第 6-38 页**替代。	4.10.x-5.1.x
rna_ip_host_service_subtype，第 A-1 页	在监控网络中 IP 主机上检测到的服务的子服务。 在 5.2 版本中已弃用。由 **rna_host_service_subtype，第 6-41 页**替代。	4.10.x-5.1.x
rna_ip_host_service_vulns，第 A-1 页	与在监控网络中 IP 主机上检测到的服务关联的漏洞。 在 5.2 版本中已弃用。由 **rna_host_service_vulns，第 6-42 页**替代。	4.10.x-5.1.x
rna_ip_host_third_party_vuln，第 A-1 页	与监控网络中的 IP 主机关联的第三方漏洞。 在 5.2 版本中已弃用。由 **rna_host_third_party_vuln，第 6-43 页**替代。	4.10.x-5.1.x
rna_ip_host_third_party_vuln_bugtraq_id，第 A-1 页	与监控网络中的 IP 主机关联而且还与 Bugtraq 数据库中的漏洞关联的第三方漏洞 (http://www.securityfocus.com/bid/)。 在 5.2 版本中已弃用。由 **rna_host_third_party_vuln_bugtraq_id，第 6-45 页**替代。	4.10.x-5.1.x
rna_ip_host_third_party_vuln_cve_id，第 A-1 页	与监控网络中的 IP 主机关联而且还与 MITRE 的 CVE 数据库中的漏洞关联的第三方漏洞。(http://www.cve.mitre.org/)。 在 5.2 版本中已弃用。由 **rna_host_third_party_vuln_cve_id，第 6-46 页**替代。	4.10.x-5.1.x
rna_ip_host_third_party_vuln_rna_id，第 A-1 页	与监控网络中的 IP 主机关联而且还与 VDB 中的漏洞关联的第三方漏洞。 在 5.2 版本中已弃用。由 **rna_host_third_party_vuln_rna_id，第 6-48 页**替代。	4.10.x-5.1.x
rna_ip_host_user_history，第 A-1 页	监控网络中特定 IP 主机的用户活动。 在 5.2 版本中已弃用。由 **user_ipaddr_history，第 6-55 页**替代。	4.10.x-5.1.x
rna_mac_host，第 A-1 页	监控网络中的 MAC 主机（无 IP 地址的主机）。	4.10.x-5.1.x

表 6-1　发现事件和网络映射表的方案（续）

请参阅……	存储有关以下内容的信息的表...	版本
rna_mac_host_sensor，第 A-1 页	监控网络中与检测到 IP 主机的受管设备相关的 IP 主机。	5.0-5.1.x
rna_mac_ip_map，第 A-1 页	在监控网络中 IP 主机的 MAC 地址。 在 5.2 版本中已弃用。由 rna_host_ip_map，第 6-23 页和 rna_host_mac_map，第 6-24 页替代。	4.10.x-5.1.x
rna_vuln，第 6-50 页	思科 VDB 中的漏洞。	4.10.x+
tag_info，第 6-53 页	展示检测到的应用的特征的标记。	5.0+
url_categories，第 6-54 页	展示从监控网络中主机上访问的 URL 特征的类别。	5.0+
url_reputations，第 6-55 页	展示从监控网络中主机上访问的 URL 特征的信誉。	5.0+
user_ipaddr_history，第 6-55 页	监控网络中特定主机的用户活动。	5.2+

application_host_map

application_host_map 表包含与在网络上检测到的每个应用关联的类别和标记的信息。

有关详细信息，请参阅以下各节：

- application_host_map 字段，第 6-4 页
- application_host_map 联合，第 6-5 页
- application_host_map 示例查询，第 6-6 页

application_host_map 字段

下表列出可在 application_host_map 表中访问的字段。

表 6-2　application_host_map 字段

字段	说明
application_id	应用的内部标别号。
application_name	在用户界面上显示的应用名称。
application_tag_id	此字段已弃用，现在会返回 null。
business_relevance	应用与企业工作效率的相关性指数（1 至 5），其中 1 表示极低，5 表示极高。
business_relevance_description	对业务相关性的说明（very low、low、medium、high、very high）。
host_id	主机的 ID 编号。
risk	应用的风险指数（1 至 5），其中 1 表示风险极低，5 表示严重风险。
risk_description	对风险的说明（very low、low、medium、high、critical）。

application_host_map 联合

下表列出可在 **application_host_map** 表上执行的联合。

表 6-3　application_host_map 联合

您可以联合此表……	与……
application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

application_host_map 示例查询

以下查询返回关于在 host_id 为 8 的主机上检测到的应用的信息。

```
SELECT host_id, application_id, application_name, business_relevance, risk
FROM application_host_map
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

application_info

application_info 表包含关于可在监控网络上检测到的应用的信息。

您可以通过联合 **application_id** 检索与来自 **application_tag_map** 表的应用关联的标记列表。同样，您可以通过联合 **application_id** 检索来自 **application_host_map** 的应用的关联类别列表。

有关详细信息，请参阅以下各节：

- application_info 字段，第 6-6 页
- application_info 联合，第 6-7 页
- application_info 示例查询，第 6-7 页

application_info 字段

下表列出可在 **application_info** 表中访问的字段。

表 6-4　application_info 字段

字段	说明
application_description	对应用的说明。
application_id	应用的内部标别号。
application_name	在用户界面上显示的应用名称。
business_relevance	应用与企业工作效率的相关性的指数（1 至 5），其中 1 表示极低，5 表示极高。
business_relevance_description	对业务相关性的说明（very low、low、medium、high、very high）。
is_client_application	指示所检测的应用是否为客户端的一个真假标志。
is_server_application	指示所检测的应用是否为服务器应用的一个真假标志。
is_web_application	指示所检测的应用是否为 Web 应用的一个真假标志。
risk	应用的预估风险指数（1 至 5），其中 1 表示风险极低，5 表示严重风险。
risk_description	对风险的说明（very low、low、medium、high 和 critical）。

application_info 联合

下表列出可在 **application_info** 表上执行的联合。

表 6-5　application_info 联合

您可以联合此表……	与……
application_id	application_host_map.application_id app_ids_stats_current_timeframe.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id si_connection_log.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id connection_summary.application_protocol_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id

application_info 示例查询

以下查询返回 host_id 为 8 的应用的记录。

```
SELECT application_id, application_name, application_description, business_relevance,
risk

FROM application_info

WHERE application_id="8";
```

application_tag_map

application_tag_map 表包含与在网络上检测到的每个应用关联的标记的信息。

有关详细信息，请参阅以下各节：

- application_tag_map 字段，第 6-8 页
- application_tag_map 联合，第 6-8 页
- application_tag_map 示例查询，第 6-9 页

application_tag_map 字段

下表列出可在 **application_tag_map** 表中访问的字段。

表 6-6　application_tag_map 字段

字段	说明
application_id	应用的内部标别号。
application_name	在用户界面上显示的应用。
tag_id	标记的内部标别号。
tag_name	在用户界面上显示的标记的文本。
tag_type	以下项之一：category 或 type。

application_tag_map 联合

下表列出可在 **application_tag_map** 表上执行的联合。

表 6-7　application_tag_map 联合

您可以联合此表……	与……
application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id si_connection_log.application_protocol_name si_connection_log.application_protocol_id si_connection_log.client_application_id si_connection_log.web_application_id
tag_id	tag_info.tag_id

application_tag_map 示例查询

以下查询返回与指定应用关联的所有标记记录。

```
SELECT application_id, application_name, tag_id, tag_name
FROM application_tag_map
WHERE application_name="Active Directory";
```

network_discovery_event

network_discovery_event 表包含关于发现和主机输入事件的信息。FireSIGHT 系统在检测到监控网络上有变化时会生成发现事件，无论是发现新网络功能，还是检测到之前确定的网络资产中有变化。在用户通过添加、修改或删除网络资产手动修改网络映射时，FireSIGHT 系统生成主机输入事件。

从 FireSIGHT 系统 5.0 版本开始，**network_discovery_event** 表代替已弃用的 **rna_events** 表。

有关详细信息，请参阅以下各节：

- network_discovery_event 字段，第 6-9 页
- network_discovery_event 联合，第 6-10 页
- network_discovery_event 示例查询，第 6-10 页

network_discovery_event 字段

下表列出可在 **network_discovery_event** 表中访问的字段。

表 6-8　network_discovery_event 字段

字段	说明
confidence	FireSIGHT 系统为服务识别分配的置信度（分值从 0 至 100）。
description	对事件的说明。
event_id	事件的内部标别号。
event_time_sec	生成事件的日期和时间的 UNIX 时间戳。
event_time_usec	事件时间戳的微秒增量。
event_type	事件类型。例如，New Host 或 Identity Conflict。
ip_address	此字段已弃用，现在会返回 null。
ipaddr	事件所涉及的主机的 IPv4 或 IPv6 地址的二进制表示。
mac_address	事件所涉及主机的 MAC 地址。
mac_vendor	事件所涉及主机的 NIC 硬件供应商。
port	触发事件的网络流量所使用的端口。
sensor_address	生成发现事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_name	生成发现事件的受管设备。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
user_dept	最后登录主机的用户所在的部门。

表 6-8　network_discovery_event 字段（续）

字段	说明
user_email	最后登录主机的用户的邮件地址。
user_first_name	最后登录主机的用户的名字。
user_id	最后登录主机的用户的内部标别号。
user_last_name	最后登录主机的用户的姓氏。
user_last_seen_sec	对于最后登录主机的用户，FireSIGHT 系统最后检测到用户活动的日期和时间的 UNIX 时间戳。
user_last_updated_sec	对于最后登录主机的用户，FireSIGHT 系统最后更新用户记录的日期和时间的 UNIX 时间戳。
user_name	最后登录主机的用户的用户名。
user_phone	最后登录主机的用户的电话号码。

network_discovery_event 联合

下表列出可在 **anetwork_discovery_event** 表上执行的联合。

表 6-9　network_discovery_event 联合

您可以联合此表……	与……
ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

network_discovery_event 示例查询

以下查询返回指定时间内的发现事件记录，包括用户、检测设备名称、时间戳、主机 IP 地址等。

```
SELECT sensor_name, event_time_sec, event_time_usec, event_type, ipaddr, user_id,
hex(mac_address), mac_vendor, port, confidence FROM network_discovery_event
WHERE event_time_sec
BETWEEN UNIX_TIMESTAMP("2013-01-01 00:00:00") AND UNIX_TIMESTAMP("2013-01-01 23:59:59")
ORDER BY event_time_sec DESC, event_time_usec DESC;
```

rna_host

rna_host 表包含关于监控网络中的主机的基本信息。

从 5.2 版本开始，此表代替 **rna_ip_host**。

有关详细信息，请参阅以下各节：

- rna_host 字段，第 6-11 页
- rna_host 联合，第 6-12 页
- rna_host 示例查询，第 6-12 页

rna_host 字段

下表列出可在 **rna_host** 表中访问的字段。

表 6-10　rna_host 字段

字段	说明
criticality	主机重要性等级：None、Low、Medium 或 High。
hops	从主机到检测到主机的受管设备的网络跳数。
host_id	主机的 ID 编号。
host_name	主机的名称。
host_type	主机的类型：Host、Router、Bridge、NAT Device 或 Load Balancer。
jailbroken	指示移动设备操作系统是否被越狱的一个真假标志。
last_seen_sec	系统最后检测到主机活动的日期和时间的 UNIX 时间戳。
mobile	指示检测到的主机是否为移动设备的一个真假标志。
netbios_name	主机 NetBIOS 名称字符串。
notes	主机的 Notes 主机属性的内容。
vlan_id	VLAN 标别号（如果适用）。
vlan_priority	VLAN 标记内包含的优先级值。
vlan_type	包含 VLAN 标记的封装数据包的类型： • 0 - 以太网 • 1 - 令牌环

rna_host 联合

下表列出可在 **rna_host** 表上执行的联合。

表 6-11　　rna_host 联合

您可以联合此表……	与……
host_id	application_host_map.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ip_map.host_id rna_host_ioc_state.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host 示例查询

以下查询返回 25 条 **rna_host** 记录，包括主机 ID、VLAN ID、最后看到主机的时间和主机类型，按照主机类型排序。

```
SELECT host_id, vlan_id, last_seen_sec, host_type

FROM rna_host

ORDER BY host_type

LIMIT 0, 25;
```

rna_host_attribute

rna_host_attribute 表包含关于与监控网络中每台主机关联的主机属性的信息， 其代替已弃用的 **rna_ip_host_attribute** 表。

有关详细信息，请参阅以下各节：

- rna_host_attribute 字段，第 6-13 页
- rna_host_attribute 联合，第 6-13 页
- rna_host_attribute 示例查询，第 6-13 页

rna_host_attribute 字段

下表列出可在 **rna_host_attribute** 表中访问的字段。

表 6-12　rna_host_attribute 字段

字段	说明
attribute_name	主机属性。例如，Host Criticality 或 Default White List。
attribute_value	主机属性值。
host_id	主机的 ID 编号。

rna_host_attribute 联合

下表列出可在 **rna_host_attribute** 表上执行的联合。

表 6-13　rna_host_attribute 联合

您可以联合此表……	与……
host_id	application_host_map.host_id rna_host.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_attribute 示例查询

以下查询返回与所选主机 ID 关联的所有主机属性和值。

```
SELECT attribute_name, attribute_value

FROM rna_host_attribute

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_client_app

rna_host_client_app 表包含关于在监控网络中主机上检测到的客户端应用的信息， 其代替已弃用的 **rna_host_client_app** 表。

有关详细信息，请参阅以下各节：

- rna_host_client_app 字段，第 6-14 页
- rna_host_client_app 联合，第 6-15 页
- rna_host_client_app 示例查询，第 6-16 页

rna_host_client_app 字段

下表列出可在 **rna_host_client_app** 表中访问的字段。

表 6-14　rna_host_client_app 字段

字段	说明
application	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
application_protocol_id	检测到的应用协议的内部标识符。
application_protocol_name	以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果系统要求提供更多数据，则显示 pending • 如果连接中没有应用信息，则为空值
application_type	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
client_application_id	如果可以识别应用，则显示应用的内部标别号。
client_application_name	以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果系统检测到客户端应用，但无法识别具体应用，则显示通用客户端名称 • 如果连接中没有客户端应用信息，则为空值
hits	检测到客户端应用的次数。
host_id	主机的 ID 编号。
last_used_sec	系统最后检测到应用活动的日期和时间的 UNIX 时间戳。
version	在主机上检测的应用的版本。

rna_host_client_app 联合

下表列出可在 **rna_host_client_app** 表上执行的联合。

表 6-15　rna_host_client_app 联合

您可以联合此表……	与……
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id
host_id 和 application_protocol_id 和 client_application_id 和 version	以下项的集合： rna_host_client_app_payload.host_id rna_host_client_app_payload.application_protocol_id rna_host_client_app_payload.client_application_id rna_host_client_app_payload.version

表 6-15　rna_host_client_app 联合（续）

您可以联合此表……	与……
application_protocol_id 或 client_application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_service_info.application_protocol_id rna_host_service_payload.web_application_id

rna_host_client_app 示例查询

以下查询返回关于在 host_id 为 8 的主机上检测到的客户端应用的信息。

```
SELECT host_id, client_application_id, client_application_name, version, hits,
application_protocol_id, application_protocol_name, last_used_sec

FROM rna_host_client_app

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_client_app_payload

rna_host_client_app_payload 表包含与在监控网络中检测到的主机上的 Web 应用关联的 HTTP 流量中的负载信息。

有关详细信息，请参阅以下各节：

- rna_host_client_app_payload 字段，第 6-17 页
- rna_host_client_app_payload 联合，第 6-18 页
- rna_host_client_app_payload 示例查询，第 6-19 页

rna_host_client_app_payload 字段

下表列出可在 **rna_host_client_app_payload** 表中访问的字段。

表 6-16　rna_host_client_app_payload 字段

字段	说明
application	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
application_protocol_id	检测到的应用协议的内部标识符（如果有）。对于既具有客户端应用特性，又具有 Web 应用特性的流量，client_application_id 和 web_application_id 字段具有相同的值。
application_protocol_name	以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果系统要求提供更多数据，则显示 pending • 如果连接中没有应用信息，则为空值
application_type	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
client_application_id	客户端应用的内部标别号。
client_application_name	以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果系统检测到客户端应用，但无法识别具体应用，则显示通用客户端名称 • 如果连接中没有客户端应用信息，则为空值
host_id	主机的 ID 编号。
payload_name	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
payload_type	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
version	在主机上检测的 Web 应用的版本。
web_application_id	Web 应用的内部标别号（如果有）。对于既具有客户端应用特性，又具有 Web 应用特性的流量，client_application_id 和 web_application_id 字段具有相同的值。
web_application_name	以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果系统检测到 HTTP 应用协议，但无法识别具体 Web 应用，则显示 web browsing • 如果连接没有 HTTP 流量，则为空值

rna_host_client_app_payload 联合

下表列出可在 **rna_host_client_app_payload** 表上执行的联合。

表 6-17　rna_host_client_app_payload 联合

您可以联合此表……	与……
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id
以下项的集合： host_id, application_protocol_id, client_application_id, version	以下项的集合： rna_host_client_app.host_id rna_host_client_app.application_protocol_id rna_host_client_app.client_application_id rna_host_client_app.version

表 6-17　rna_host_client_app_payload 联合（续）

您可以联合此表……	与……
client_application_id 或 web_application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_id rna_host_service_info.application_protocol_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id

rna_host_client_app_payload 示例查询

以下查询返回关于在 host_id 为 8 的主机上检测到的 Web 应用的信息。

```
SELECT host_id, web_application_id, web_application_name, version,
client_application_id, client_application_name

FROM rna_host_client_app_payload

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_ioc_state

rna_host_ioc_state 表存储监控网络中主机的 IOC 状态。

有关详细信息，请参阅以下各节：

- rna_host_ioc_state 字段，第 6-20 页
- rna_host_ioc_state 联合，第 6-22 页
- rna_host_ioc_state 示例查询，第 6-22 页

rna_host_ioc_state 字段

下表列出可在 **rna_host_ioc_state** 表中访问的字段。

表 6-18　rna_host_ioc_state 字段

字段	说明
first_seen	首次检测到漏洞时的 Unix 时间戳。
first_seen_sensor_address	首先检测到威胁的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
first_seen_sensor_name	首先检测到威胁的受管设备。
host_id	主机的 ID 编号。
ioc_category	威胁的类别。可能的值包括： • CnC Connected • Exploit Kit • High Impact Attack • Low Impact Attack • Malware Detected • Malware Executed • Dropper Infection • Java Compromise • Word Compromise • Adobe Reader Compromise • Excel Compromise • PowerPoint Compromise • QuickTime Compromise
ioc_description	对威胁的说明。

表 6-18　rna_host_ioc_state 字段（续）

字段	说明
ioc_event_type	威胁的事件类型。可能的值包括： • Adobe Reader launched shell • Dropper Infection Detected by FireAMP • Excel Compromise Detected by FireAMP • Excel launched shell | • Impact 1 Intrusion Event — attempted-admin • Impact 1 Intrusion Event — attempted-user • Impact 1 Intrusion Event — successful-admin • Impact 1 Intrusion Event — successful-user • Impact 1 Intrusion Event — web-application-attack • Impact 2 Intrusion Event — attempted-admin • Impact 2 Intrusion Event — attempted-user • Impact 2 Intrusion Event — successful-admin • Impact 2 Intrusion Event — successful-user • Impact 2 Intrusion Event — web-application-attack • Intrusion Event — exploit-kit • Intrusion Event — malware-backdoor • Intrusion Event — malware-CnC • Java Compromise Detected by FireAMP • Java launched shell • PDF Compromise Detected by FireAMP • PowerPoint Compromise Detected by FireAMP • PowerPoint launched shell • QuickTime Compromise Detected by FireAMP • QuickTime launched shell • Security Intelligence Event — CnC • Suspected Botnet Detected by FireAMP • Threat Detected by FireAMP — Subtype is 'executed' • Threat Detected by FireAMP — Subtype is not 'executed' • Threat Detected in File Transfer — Action is not 'block' • Word Compromise Detected by FireAMP • Word launched shell
ioc_id	威胁的唯一 ID 编号。
is_disabled	此危害是否已禁用。
last_seen	最后检测到此威胁时的 Unix 时间戳。

表 6-18　rna_host_ioc_state 字段（续）

字段	说明
last_seen_sensor_address	最后检测到此威胁的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
last_seen_sensor_name	最后检测到此威胁的受管设备。

rna_host_ioc_state 联合

下表列出可在 **rna_host_ioc_state** 表上执行的联合。

表 6-19　rna_host_ioc_state 联合

您可以联合此表……	与……
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_ioc_state 示例查询

以下查询返回指定时间范围内的最多 25 个主机及其 ioc。

```
SELECT host_id, ioc_id

FROM rna_host_ioc_state

WHERE first_seen

BETWEEN UNIX_TIMESTAMP("2011-10-01 00:00:00")

AND UNIX_TIMESTAMP("2011-10-07 23:59:59")

ORDER BY ioc_id DESC

LIMIT 0, 25;
```

rna_host_ip_map

rna_host_ip_map 表将监控网络中的主机的主机 ID 与 IP 地址关联。

有关详细信息，请参阅以下各节：

rna_host_ip_map 字段

下表列出可在 rna_host_ip_map 表中访问的字段。

表 6-20　rna_host_ip_map 字段

字段	说明
host_id	主机的 ID 编号。
ipaddr	主机 IP 地址的二进制表示。

rna_host_ip_map 联合

下表列出可在 rna_host_ip_map 表上执行的联合。

表 6-21　rna_host_ip_map 联合

您可以联合此表……	与……
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

表 6-21　rna_host_ip_map 联合（续）

您可以联合此表……	与……
ipaddr	compliance_event.dst_ipaddr compliance_event.src_ipaddr connection_log.initiator_ipaddr connection_log.responder_ipaddr connection_summary.initiator_ipaddr connection_summary.responder_ipaddr fireamp_event.dst_ipaddr fireamp_event.src_ipaddr intrusion_event.dst_ipaddr intrusion_event.src_ipaddr network_discovery_event.ipaddr si_connection_log.initiator_ipaddr si_connection_log.responder_ipaddr user_discovery_event.ipaddr user_ipaddr_history.ipaddr white_list_event.ipaddr

rna_host_ip_map 示例查询

以下查询返回所选主机的 MAC 信息。

```
SELECT host_id
FROM rna_host_ip_map
WHERE HEX(ipaddr) = "00000000000000000000FFFF0A0A0A04";
```

rna_host_mac_map

rna_host_mac_map 表将监控网络中的主机的主机 ID 与 MAC 地址关联。

有关详细信息，请参阅以下各节：

- rna_host_mac_map 字段，第 6-25 页
- rna_host_mac_map 联合，第 6-25 页
- rna_host_mac_map 示例查询，第 6-25 页

rna_host_mac_map 字段

下表列出可在 **rna_host_mac_map** 表中访问的字段。

表 6-22　rna_host_mac_map 字段

字段	说明
host_id	主机的 ID 编号。
mac_address	主机的 MAC 地址。
mac_vendor	检测到的主机的网络接口供应商。

rna_host_mac_map 联合

下表列出可在 **rna_host_mac_map** 表上执行的联合。

表 6-23　rna_host_mac_map 联合

您可以联合此表……	与……
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_mac_map 示例查询

以下查询返回 host_id 为 8 的主机的 MAC 信息。

```
SELECT HEX(mac_address)

FROM rna_host_mac_map

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_os

rna_host_os 表包含关于在监控网络中主机上检测到的操作系统的信息。

有关详细信息，请参阅以下各节：

- rna_host_os 字段，第 6-26 页
- rna_host_os 联合，第 6-27 页
- rna_host_os 示例查询，第 6-27 页

rna_host_os 字段

下表列出可在 **rna_host_os** 表中访问的字段。

表 6-24　rna_host_os 字段

字段	说明
confidence	FireSIGHT 系统为识别操作系统而分配的置信度（分值从 0 至 100）。
created_sec	系统首次检测到主机活动的日期和时间的 UNIX 时间戳。
host_id	主机的 ID 编号。
last_seen_sec	系统最后检测到主机活动的日期和时间的 UNIX 时间戳。
os_uuid	在主机上检测到的操作系统的唯一标识符。在思科数据库中，UUID 向操作系统映射名称、供应商和版本。
product	在主机上检测到的操作系统。
source_type	主机的操作系统标识的来源： • User - 通过 Web 用户界面输入数据的用户的名称 • Application - 通过主机输入功能从另一应用导入 • Scanner - Nmap 或通过系统策略添加的另一个扫描仪 • rna - 通过发现事件、端口匹配或模式匹配由 FireSIGHT 系统检测 • NetFlow - 由支持 NetFlow 的设备导出数据
vendor	在主机上检测的操作系统的供应商。
version	在主机上检测到的操作系统的版本。

rna_host_os 联合

下表列出可在 **rna_host_os** 表上执行的联合。

表 6-25　rna_host_os 联合

您可以联合此表……	与……
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_os 示例查询

以下查询返回 host_id 为 8 的主机的操作系统信息。

```
SELECT vendor, product, version, source_type, confidence
FROM rna_host_os
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_os_vulns

rna_host_os_vulns 表包含关于与监控网络中主机关联的漏洞的信息。

有关详细信息，请参阅以下各节：

- rna_host_os_vulns 字段，第 6-28 页
- rna_host_os_vulns 联合，第 6-28 页
- rna_host_os_vulns 示例查询，第 6-29 页

rna_host_os_vulns 字段

下表列出可在 **rna_host_os_vulns** 表中访问的字段。

表 6-26　rna_host_os_vulns 字段

字段	说明
host_id	主机的 ID 编号。
invalid	指示漏洞对于主机是否有效的一个值： • 0 - 漏洞有效 • 1 - 漏洞无效
rna_vuln_id	漏洞的内部标别号。

rna_host_os_vulns 联合

下表列出可在 **rna_host_os_vulns** 表上执行的联合。

表 6-27　rna_host_os_vulns 联合

您可以联合此表……	与……
rna_vuln_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_third_party_vuln_rna_id.rna_vuln_id rna_host_third_party_vuln_cve_id.cve_id rna_host_third_party_vuln_bugtraq_id.bugtraq_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_os_vulns 示例查询

以下查询返回 host_id 为 8 的主机的操作系统漏洞。

```
SELECT rna_vuln_id, invalid
FROM rna_host_os_vulns
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_protocol

rna_host_protocol 表包含关于在监控网络中主机上检测到的协议的信息。

有关详细信息，请参阅以下各节：

- rna_host_protocol 字段，第 6-29 页
- rna_host_protocol 联合，第 6-30 页
- rna_host_protocol 示例查询，第 6-30 页

rna_host_protocol 字段

下表列出可在 **rna_host_protocol** 表中访问的字段。

表 6-28　rna_host_protocol 字段

字段	说明
host_id	主机的 ID 编号。
ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
layer	协议运行的网络层：Network 或 Transport。
mac_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
mac_vendor	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
protocol_name	主机使用的流量协议。
protocol_num	协议的 NANA 指定协议编号。

rna_host_protocol 联合

下表列出可在 **rna_host_protocol** 表上执行的联合。

表 6-29　　rna_host_protocol 联合

您可以联合此表……	与……
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_protocol 示例查询

以下查询返回 host_id 为 8 的主机的所有协议记录。

```
SELECT protocol_num, protocol_name

FROM rna_host_protocol

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_sensor

rna_host_sensor 表列出在监控网络中的主机 IP 地址并指出检测到每个主机 IP 地址的受管设备。从 FireSIGHT 系统 5.2 版本开始，**rna_host_sensor** 表代替已弃用的 **rna_ip_host_sensor** 表。有关详细信息，请参阅以下各节：

- rna_host_sensor 字段，第 6-31 页
- rna_host_sensor 联合，第 6-31 页
- rna_host_sensor 示例查询，第 6-31 页

rna_host_sensor 字段

下表列出可在 **rna_host_sensor** 表中访问的字段。

表 6-30　rna_host_sensor 字段

字段	说明
host_id	主机的 ID 编号。
sensor_address	生成发现事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_name	受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。

rna_host_sensor 联合

下表列出可在 **rna_host_sensor** 表上执行的联合。

表 6-31　rna_host_sensor 联合

您可以联合此表……	与……
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_sensor 示例查询

以下查询返回来自 **rna_host_sensor** 表的最多 25 个主机以及检测到这些主机的传感器。

```
SELECT host_id, sensor_address, sensor_name

FROM rna_host_sensor

LIMIT 0, 25;
```

rna_host_service

rna_host_service 表包含关于通过网络端口和流量协议的组合在受管网络中的主机上检测到的服务器的一般信息。

有关详细信息，请参阅以下各节：

- rna_host_service 字段，第 6-32 页
- rna_host_service 联合，第 6-33 页
- rna_host_service 示例查询，第 6-33 页

rna_host_service 字段

下表列出可在 **rna_host_service** 表中访问的字段。

表 6-32　rna_host_service 字段

字段	说明
confidence	FireSIGHT 系统为识别服务器而分配的置信度（分值从 0 至 100）。
hits	检测到服务器的次数。
host_id	主机的 ID 编号。
last_used_sec	系统最后检测到服务器活动的日期和时间的 UNIX 时间戳。
port	服务器使用的端口。
protocol	流量协议：TCP 或 UDP。

rna_host_service 联合

下表列出可在 **rna_host_service** 表上执行的联合。

表 6-33　rna_host_service 联合

您可以联合此表……	与……
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id
以下项的集合： host_id port protocol	以下项的集合： rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol 以下项的集合： rna_host_service_info.host_id rna_host_service_info.port rna_host_service_info.protocol 以下项的集合： rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol

rna_host_service 示例查询

以下查询返回 host_id 为 8 的主机的前 25 个检测到的服务器记录。

```
SELECT hits, protocol, port, confidence

FROM rna_host_service

WHERE HEX(host_id) = "00000000000000000000000000000008"

LIMIT 0, 25;
```

rna_host_service_banner

rna_ip_host_service_banner 表包含作为在监控网络中主机上服务器的供应商和版本（“横幅”）广告的网络流量的报头信息。请记住，FireSIGHT 系统不存储服务器横幅，除非您在网络发现策略中启用 **Capture Banners** 选项。

有关详细信息，请参阅以下各节：

- rna_ip_host_service_banner 字段，第 6-34 页
- rna_host_service_banner 联合，第 6-34 页
- rna_host_service_banner 示例查询，第 6-35 页

rna_ip_host_service_banner 字段

下表列出可在 **rna_host_service_banner** 表中访问的字段。

表 6-34　rna_host_service_banner 字段

字段	说明
banner	服务器横幅，即针对服务器检测到的第一个数据包中的前 256 个字节。
host_id	主机的 ID 编号。
port	服务器使用的端口。
protocol	流量协议：TCP 或 UDP。

rna_host_service_banner 联合

下表列出可在 **rna_host_service_banner** 表上执行的联合。

表 6-35　rna_host_service_banner 联合

您可以联合此表……	与……
以下项的集合： host_id port protocol	以下项的集合： rna_host_service.host_id rna_host_service.port rna_host_service.protocol 以下项的集合： rna_host_service_info.host_id rna_host_service_info.port rna_host_service_info.protocol 以下项的集合： rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol

表 6-35　rna_host_service_banner 联合（续）

您可以联合此表.....	与.....
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_service_banner 示例查询

以下查询返回 host_id 为 8 的主机的服务器横幅。

```
SELECT port, protocol, banner

FROM rna_host_service_banner

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_info

rna_host_protocol 表包含关于在监控网络中主机上检测到的服务器的详细信息。

有关详细信息，请参阅以下各节：

- rna_host_service_info 字段，第 6-36 页
- rna_host_service_info 联合，第 6-37 页
- rna_host_service_info 示例查询，第 6-38 页

rna_host_service_info 字段

下表列出可在 **rna_host_service_info** 表中访问的字段。

表 6-36　rna_host_service_info 字段

字段	说明
application_id	在 5.0 版本中已弃用此字段。对所有查询都返回空值。
application_protocol_id	检测到的应用协议的内部标识符（如果有）。
application_protocol_name	以下任一项： • 如果能够明确识别应用协议，则显示应用协议的名称 • 如果系统要求提供更多数据，则显示 pending • 如果连接中没有应用信息，则为空值
business_relevance	应用与企业工作效率的相关性指数（1 至 5），其中 1 表示极低，5 表示极高。
business_relevance_ description	对业务相关性的说明（very low、low、medium、high、very high）。
created_sec	系统首次检测到应用协议的日期和时间的 UNIX 时间戳。
host_id	主机的 ID 编号。
ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
last_used_sec	系统最后检测到服务器活动的日期和时间的 UNIX 时间戳。
port	服务器使用的端口。
protocol	流量协议：TCP 或 UDP。
risk	应用的风险指数（1 至 5），其中 1 表示风险极低，5 表示风险极高。
risk_description	对风险的说明（very low、low、medium、high、very high）。
service_info_id	服务器的内部标别号。
service_name	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
source_type	服务器的标识的来源： • User - 通过 Web 用户界面输入数据的用户的名称 • Application - 通过主机输入功能从另一应用导入 • Scanner - 通过 NMAP 添加或使用源类型扫描仪通过主机输入功能导入 • rna - 通过发现事件、端口匹配或模式匹配由 FireSIGHT 系统检测 • NetFlow - 由支持 NetFlow 的设备导出数据
vendor	主机上服务器的供应商。
version	在主机上检测到的服务器的版本。

rna_host_service_info 联合

下表列出可在 **rna_host_service_info** 表上执行的联合。

表 6-37　rna_host_service_info 联合

您可以联合此表……	与……
application_protocol_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_payload.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

表 6-37　rna_host_service_info 联合（续）

您可以联合此表……	与……
以下项的集合： host_id 和 port 和 protocol	以下项的集合： rna_host_service.host_id rna_host_service.port rna_host_service.protocol 以下项的集合： rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol 以下项的集合： rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol

rna_host_service_info 示例查询

以下查询返回关于在 host_id 为 8 的主机上检测到的应用协议的信息。

```
SELECT host_id, application_protocol_name, version, vendor, created_sec, last_used_sec,
business_relevance, risk

FROM rna_host_service_info

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_payload

rna_host_service_payload 表包含关于与监控网络中主机关联的 Web 应用的信息。

有关详细信息，请参阅以下各节：

- rna_host_service_payload 字段，第 6-38 页
- rna_host_service_payload 联合，第 6-39 页
- rna_host_service_payload 示例查询，第 6-40 页

rna_host_service_payload 字段

下表列出可在 **rna_host_service_payload** 表中访问的字段。

表 6-38　rna_host_service_payload 字段

字段	说明
application_id	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
application_name	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
host_id	主机的 ID 编号。
ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。

表 6-38　rna_host_service_payload 字段（续）

字段	说明
payload_name	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
payload_type	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
port	服务器使用的端口。
protocol	流量协议：TCP 或 UDP。
web_application_id	Web 应用的内部标别号。
web_application_name	以下任一项： • 如果能够明确识别 Web 应用，则显示此应用的名称 • 如果系统检测到 HTTP 应用协议，但无法识别具体 Web 应用，则显示 web browsing • 如果连接没有 HTTP 流量，则为空值

rna_host_service_payload 联合

下表列出可在 **rna_host_service_payload** 表上执行的联合。

表 6-39　rna_host_service_payload 联合

您可以联合此表……	与……
web_application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id

表 6-39　rna_host_service_payload 联合（续）

您可以联合此表……	与……
以下项的集合： host_id port protocol	以下项的集合： rna_host_service.host_id rna_host_service.port rna_host_service.protocol 以下项的集合： rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol 以下项的集合： rna_host_service_info.host_id rna_host_service_info.port rna_host_service_info.protocol
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_service_payload 示例查询

以下查询返回关于在 host_id 为 8 的主机上检测到的 Web 应用的信息。

```
SELECT host_id, web_application_id, web_application_name, port, protocol
FROM rna_host_service_payload
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_subtype

rna_host_service_subtype 表包含关于在监控网络中主机上检测到的服务器的子服务器信息。

有关详细信息，请参阅以下各节：

- rna_host_service_subtype 字段，第 6-41 页
- rna_host_service_subtype 联合，第 6-42 页
- rna_host_service_subtype 示例查询，第 6-42 页

rna_host_service_subtype 字段

下表列出可在 **rna_host_service_subtype** 表中访问的字段。

表 6-40　rna_host_service_subtype 字段

字段	说明
host_id	主机的 ID 编号。
port	服务器使用的端口。
protocol	流量协议：TCP 或 UDP。
service_name	以下任一项： • 与触发事件关联的主机上的服务器 • 如果无法提供用于识别的数据，则为 none 或空值 • 如果需要其他数据，则为 pending • 如果根据已知服务器指纹，系统无法识别服务器，则为 unknown
source_type	服务器的标识的来源： • User - 通过 Web 用户界面输入数据的用户的名称 • Application - 通过主机输入功能从另一应用导入 • Scanner - 通过 NMAP 添加或使用源类型扫描仪通过主机输入功能导入 • rna - 通过发现事件、端口匹配或模式匹配由 FireSIGHT 系统检测 • NetFlow - 由支持 NetFlow 的设备导出数据
sub_service_name	在主机上检测到的子服务器。
sub_service_vendor	在主机上检测到的子服务器的供应商。
sub_service_version	在主机上检测到的子服务器的版本。
vendor	在主机上检测到的服务器的供应商。
version	在主机上检测到的服务器的版本。

rna_host_service_subtype 联合

您无法在 **rna_host_service_subtype** 表上执行联合。

rna_host_service_subtype 示例查询

以下查询返回 host_id 为 8 的主机的所有检测到的子服务器记录。

```
SELECT host_id, service_name, version, sub_service_name, sub_service_version,
sub_service_vendor
FROM rna_host_service_subtype
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_vulns

rna_host_service_vulns 表包含关于映射至在监控网络中主机上检测到的服务器的漏洞的信息。

有关详细信息，请参阅以下各节：

- rna_host_service_vulns 字段，第 6-42 页
- rna_host_service_vulns 联合，第 6-43 页
- rna_host_service_vulns 示例查询，第 6-43 页

rna_host_service_vulns 字段

下表列出可在 **rna_host_service_vulns** 表中访问的字段。

表 6-41　rna_host_service_vulns 字段

字段	说明
application_id	在主机上运行的应用协议的内部标别号。
application_name	在用户界面上显示的应用协议名称。
host_id	主机的 ID 编号。
invalid	指示漏洞对于运行此应用协议的主机是否有效的值： • 0 - 漏洞有效 • 1 - 漏洞无效
ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
port	服务器使用的端口。
protocol	流量协议：TCP 或 UDP。
rna_vuln_id	漏洞的内部标别号。
service_name	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
vendor	在主机上检测到的服务器的供应商。
version	在主机上检测到的服务器的版本。

rna_host_service_vulns 联合

下表列出可在 **rna_host_service_vulns** 表上执行的联合。

表 6-42　rna_host_service_vulns 联合

您可以联合此表.....	与.....
rna_vuln_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_third_party_vuln_rna_id.rna_vuln_id rna_host_third_party_vuln_cve_id.cve_id rna_host_third_party_vuln_bugtraq_id.bugtraq_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_payload.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_service_vulns 示例查询

以下查询返回关于 host_id 为 8 的主机的所有服务器漏洞的信息。

```
SELECT host_id, rna_vuln_id, vendor, service_name, version, invalid FROM
rna_host_service_vulns
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_third_party_vuln

rna_host_third_party_vuln 表包含关于与监控网络中主机关联的第三方漏洞的信息。请注意，此表中的信息取决于通过主机输入功能导入的第三方漏洞数据。

有关详细信息，请参阅以下各节：

- rna_host_third_party_vuln 字段，第 6-44 页
- rna_host_third_party_vuln 联合，第 6-44 页
- rna_host_third_party_vuln 示例查询，第 6-45 页

rna_host_third_party_vuln 字段

下表列出可在 **rna_host_third_party_vuln** 表中访问的字段。

表 6-43　rna_host_third_party_vuln 字段

字段	说明
description	对漏洞的说明。
host_id	主机的 ID 编号。
invalid	指示漏洞对于主机是否有效的一个值： • 0 - 漏洞有效 • 1 - 漏洞无效
name	漏洞的标题。
port	如果漏洞与特定端口上检测到的服务器或相关应用关联，则显示端口号。
protocol	如果漏洞与使用该协议的应用关联，则显示流量协议（TCP 或 UDP）。
source	漏洞的来源。
third_party_vuln_id	与漏洞关联的标别号。

rna_host_third_party_vuln 联合

下表列出可在 **rna_host_third_party_vuln** 表上执行的联合。

表 6-44　rna_host_third_party_vuln 联合

您可以联合此表……	与……
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln 示例查询

以下查询返回关于 host_id 为 8 的主机的第三方漏洞信息。

```
SELECT host_id, third_party_vuln_id, name, description, source, invalid
FROM rna_host_third_party_vuln
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_third_party_vuln_bugtraq_id

rna_host_third_party_vuln_bugtraq_id 表包含映射至 Bugtraq 数据库中的漏洞而且与监控网络中的主机关联的第三方漏洞的信息。请注意，此表中的第三方漏洞数据通过主机输入功能导入。

有关详细信息，请参阅以下各节：

- rna_host_third_party_vuln_bugtraq_id 字段，第 6-45 页
- rna_host_third_party_vuln_bugtraq_id 联合，第 6-46 页
- rna_host_third_party_vuln_bugtraq_id 示例查询，第 6-46 页

rna_host_third_party_vuln_bugtraq_id 字段

下表列出可在 **rna_host_third_party_vuln_bugtraq_id** 表中访问的字段。

表 6-45　rna_host_third_party_vuln_bugtraq_id 字段

字段	说明
bugtraq_id	与漏洞关联的 Bugtraq 数据库标别号。
description	对漏洞的说明。
host_id	主机的 ID 编号。
invalid	指示漏洞对于主机是否有效的一个值： • 0 - 漏洞有效 • 1 - 漏洞无效
ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
name	漏洞的名称或标题。
port	如果漏洞与特定端口上检测到的服务器或相关应用关联，则显示端口号。
protocol	如果漏洞与使用该协议的应用关联，则显示流量协议（TCP 或 UDP）。
source	漏洞的来源。
third_party_vuln_id	与漏洞关联的第三方标别号。

rna_host_third_party_vuln_bugtraq_id 联合

下表列出可在 **rna_host_third_party_vuln_bugtraq_id** 表上执行的联合。

表 6-46　rna_host_third_party_vuln_bugtraq_id 联合

您可以联合此表……	与……
bugtraq_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_os_vulns.rna_vuln_id rna_host_service_vulns.rna_vuln_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln_bugtraq_id 示例查询

以下查询返回 host_id 为 8 的主机的 BugTraq 漏洞。

```
SELECT host_id, third_party_vuln_id, bugtraq_id, name, description, source, invalid

FROM rna_host_third_party_vuln_bugtraq_id

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_third_party_vuln_cve_id

rna_host_third_party_vuln_cve_id 表包含映射至 MITRE 的 CVE 数据库中的漏洞而且与监控网络中的主机关联的第三方漏洞的信息。请注意，此表包含通过主机输入功能导入的第三方漏洞数据。

有关详细信息，请参阅以下各节：

- rna_host_third_party_vuln_cve_id 字段，第 6-47 页
- rna_host_third_party_vuln_cve_id 联合，第 6-48 页
- rna_host_third_party_vuln_cve_id 示例查询，第 6-48 页

rna_host_third_party_vuln_cve_id 字段

下表列出可在 **rna_host_third_party_vuln_cve_id** 表中访问的字段。

表 6-47　rna_host_third_party_vuln_cve_id 字段

字段	说明
cve_id	与 MITRE 的 CVE 数据库中的漏洞关联的标别号。
description	对漏洞的说明。
host_id	主机的 ID 编号。
invalid	指示漏洞对于主机是否有效的一个值： • 0 - 漏洞有效 • 1 - 漏洞无效
ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
name	漏洞的名称或标题。
port	如果漏洞与特定端口上检测到的服务器或相关应用关联，则显示端口号。
protocol	如果漏洞与使用该协议的应用关联，则显示流量协议（TCP 或 UDP）。
source	漏洞的来源。
third_party_vuln_id	与漏洞关联的标别号。

rna_host_third_party_vuln_cve_id 联合

下表列出可在 **rna_host_third_party_vuln_cve_id** 表上执行的联合。

表 6-48　rna_host_third_party_vuln_cve_id 联合

您可以联合此表……	与……
cve_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_os_vulns.rna_vuln_id rna_host_service_vulns.rna_vuln_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln_cve_id 示例查询

以下查询返回 host_id 为 8 的主机的 CVE 漏洞。

```
SELECT host_id, third_party_vuln_id, cve_id, name, description, source, invalid
FROM rna_host_third_party_vuln_cve_id
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_third_party_vuln_rna_id

rna_host_third_party_vuln_rna_id 表包含映射至思科漏洞数据库 (VDB) 中的漏洞而且与监控网络中的主机关联的第三方漏洞的信息。请注意，此表中的第三方漏洞数据通过主机输入功能导入。

有关详细信息，请参阅以下各节：

- rna_host_third_party_vuln_rna_id 字段，第 6-49 页
- rna_host_third_party_vuln_rna_id 联合，第 6-50 页
- rna_host_third_party_vuln_rna_id 示例查询，第 6-50 页

rna_host_third_party_vuln_rna_id 字段

下表列出可在 **rna_host_third_party_vuln_rna_id** 表中访问的字段。

表 6-49　rna_host_third_party_vuln_rna_id 字段

字段	说明
description	对漏洞的说明。
host_id	主机的 ID 编号。
invalid	指示漏洞对于主机是否有效的一个值： • 0 - 漏洞有效 • 1 - 漏洞无效
ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
name	漏洞的名称或标题。
port	如果漏洞与特定端口上检测到的服务器或相关应用关联，则显示端口号。
protocol	如果漏洞与使用该协议的应用关联，则显示流量协议（TCP 或 UDP）。
rna_vuln_id	思科用于跟踪漏洞的漏洞标别号。
source	漏洞的来源。
third_party_vuln_id	与漏洞关联的标别号。

rna_host_third_party_vuln_rna_id 联合

下表列出可在 **rna_host_third_party_vuln_rna_id** 表上执行的联合。

表 6-50　rna_host_third_party_vuln_rna_id 联合

您可以联合此表……	与……
rna_vuln_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_os.rna_vuln_id rna_host_service_vulns.rna_vuln_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln_rna_id 示例查询

以下查询返回 host_id 为 8 的主机的具有 VDB ID 的所有第三方漏洞。

```
SELECT host_id, third_party_vuln_id, rna_vuln_id, name, description, source, invalid
FROM rna_host_third_party_vuln_rna_id
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_vuln

rna_vuln 表包含关于思科 VDB 中漏洞的信息。

有关详细信息，请参阅以下各节：

- rna_vuln 字段，第 6-51 页
- rna_vuln 联合，第 6-52 页
- rna_vuln 示例查询，第 6-53 页

rna_vuln 字段

下表列出可在 **rna_vuln** 表中访问的字段。

表 6-51　rna_vuln 字段

字段	说明
authentication	是否需要通过身份验证才能利用漏洞： • Required • Not Required • Unknown
availability	漏洞何时可被利用： • Always • User Initiated • Time Dependent • Unknown
available_exploits	是否有漏洞可以利用的漏洞攻击： • TRUE • FALSE
bugtraq_id	与 Bugtraq 数据库中漏洞关联的标别号。
class	漏洞的类： • Configuration Error • Boundary Condition Error • Design Error
credibility	漏洞的可信程度为： • Conflicting Reports • Conflicting Details • Single Source • Reliable Source • Multiple Sources • Vendor Confirmed
credit	被认为报告此漏洞的人员或组织。
ease	利用漏洞的难易程度： • No Exploit Required • Exploit Available • No Exploit Available
effect	关于漏洞被利用时可能发生的情况的详细信息。
entry_date	在数据库中输入漏洞时的日期。
exploit	关于在何处可以找到漏洞攻击的信息。

表 6-51　rna_vuln 字段（续）

字段	说明
impact	漏洞影响，与通过入侵数据、发现事件和漏洞评估的关联确定的影响级别对应。其值可能为 1 至 10，其中 10 表示其严重程度最高。漏洞的影响级别由 Bugtraq 条目编写者确定。
local	指示漏洞是否必须在本地被利用： • TRUE • FALSE
long_description	对漏洞的一般说明。
mitigation	对如何降低漏洞风险的说明。
modified_date	最近修改漏洞的日期（如果适用）。
publish_date	发布漏洞的日期。
remote	指示漏洞是否会通过网络被利用： • TRUE • FALSE
rna_vuln_id	系统用于跟踪漏洞的思科漏洞 ID 编号。
scenario	对攻击者利用漏洞的场景的说明。
short_description	对漏洞的概述。
snort_id	与 Snort ID (SID) 数据库中漏洞关联的标别号。也就是说，如果入侵规则能检测到利用特殊漏洞的网络流量，则此漏洞与入侵规则的 SID 关联。
solution	对漏洞的解决方案。
technical_description	对漏洞的技术说明。
title	漏洞的标题。

rna_vuln 联合

下表列出可在 **rna_vuln** 表上执行的联合。

表 6-52　rna_vuln 联合

您可以联合此表……	与……
rna_vuln_id 或 bugtraq_id	rna_host_os_vulns.rna_vuln_id rna_host_service_vulns.rna_vuln_id rna_host_third_party_vuln_rna_id.rna_vuln_id rna_host_third_party_vuln_cve_id.cve_id rna_host_third_party_vuln_bugtraq_id.bugtraq_id

rna_vuln 示例查询

以下查询返回关于最多 25 个漏洞的信息。这些记录按照生成事件最多的漏洞依次排序。

```
SELECT rna_vuln_id, bugtraq_id, snort_id, title, publish_date, impact, remote, exploit,
long_description, technical_description, solution, count(*) as count

FROM rna_vuln

GROUP BY rna_vuln_id

ORDER BY rna_vuln_id DESC LIMIT 0, 25;
```

tag_info

tag_info 表包含与在网络上检测到的应用关联的标记的信息。请注意，一个应用可能会有多个关联的标记。

有关详细信息，请参阅以下各节：

- tag_info 字段，第 6-53 页
- tag_info 联合，第 6-53 页
- tag_info 示例查询，第 6-54 页

tag_info 字段

下表列出可在 **tag_info** 表中访问的字段。

表 6-53　tag_info 字段

字段	说明
tag_description	标记说明。
tag_id	标记的内部标识符。
tag_name	在用户界面上显示的标记的文本。
tag_type	以下项之一： • category • tag

tag_info 联合

下表列出可在 **tag_info** 表上执行的联合。

表 6-54　tag_info 联合

您可以联合此表……	与……
tag_id	application_tag_map.tag_id

tag_info 示例查询

以下查询返回所选标记 ID 的应用标记记录。

```
SELECT tag_id, tag_name, tag_type, tag_description

FROM tag_info

WHERE tag_id="100";
```

url_categories

url_categories 表列出展示监控网络中主机所请求的 URL 特征的类别。

有关详细信息，请参阅以下各节：

- url_categories 字段，第 6-54 页
- url_categories 联合，第 6-54 页
- url_categories 示例查询，第 6-54 页

url_categories 字段

下表列出 **url_categories** 表中的字段。

表 6-55　　url_categories 字段

字段	说明
category_description	对 URL 类别的说明。
category_id	URL 类别的内部标别号。

url_categories 联合

您无法在 **url_categories** 表上执行联合。

url_categories 示例查询

以下查询返回选定类别 ID 的类别记录。

```
SELECT category_id, category_description

FROM url_categories

WHERE category_id="1";
```

url_reputations

url_reputations 表列出展示监控网络中主机所请求的 URL 特征的信誉。

有关详细信息，请参阅以下各节：

- url_reputations 字段，第 6-55 页
- url_reputations 联合，第 6-55 页
- url_reputations 示例查询，第 6-55 页

url_reputations 字段

下表列出 **url_reputations** 表中的字段。

表 6-56　　url_reputations 字段

字段	说明
reputation_description	对信誉的说明。
reputation_id	URL 信誉的内部标别号。

url_reputations 联合

您无法在 **url_reputations** 表上执行联合。

url_reputations 示例查询

以下查询返回某个信誉 ID 的 URL 信誉信息。

```
SELECT reputation_id, reputation_description
FROM url_reputations
WHERE reputation_id="1";
```

user_ipaddr_history

user_ipaddr_history 表包含关于监控网络中特定主机的用户活动信息。

有关详细信息，请参阅以下各节：

- user_ipaddr_history 字段，第 6-56 页
- user_ipaddr_history 联合，第 6-57 页
- user_ipaddr_history 示例查询，第 6-57 页

user_ipaddr_history 字段

下表列出可在 **user_ipaddr_history** 表中访问的字段。

表 6-57　user_ipaddr_history 字段

字段	说明
end_time_sec	FireSIGHT 系统检测到另一用户正在登录主机（标志着假设前一用户会话结束）时的日期和时间的 UNIX 时间戳。请注意，FireSIGHT 系统不检测注销。
ID	用户历史记录的内部标别号。
ipaddr	主机 IP 地址的二进制表示。
start_time_sec	FireSIGHT 系统检测到用户登录主机时的日期和时间的 UNIX 时间戳。
user_dept	用户所在部门。
user_email	用户的邮件地址。
user_first_name	用户的名字。
user_id	用户的内部标别号。
user_last_name	用户的姓氏。
user_last_seen_sec	FireSIGHT 系统最后检测到用户的用户活动的日期和时间的 UNIX 时间戳。
user_last_updated_sec	FireSIGHT 系统最后更新用户的用户记录的日期和时间 UNIX 时间戳。
user_name	用户的用户名。
user_phone	用户的电话号码。
user_rna_service	检测到用户时，正在使用的应用协议的名称（如果有）。

user_ipaddr_history 联合

下表列出可在 **user_ipaddr_history** 表上执行的联合。

表 6-58　user_ipaddr_history 联合

您可以联合此表……	与……
ipaddr	compliance_event.dst_ipaddr compliance_event.src_ipaddr connection_log.initiator_ipaddr connection_log.responder_ipaddr connection_summary.initiator_ipaddr connection_summary.responder_ipaddr fireamp_event.dst_ipaddr fireamp_event.src_ipaddr intrusion_event.dst_ipaddr intrusion_event.src_ipaddr network_discovery_event.ipaddr rna_host_ip_map.ipaddr si_connection_log.initiator_ipaddr si_connection_log.responder_ipaddr user_discovery_event.ipaddr white_list_event.ipaddr
user_id	discovered_users.user_id user_discovery_event.user_id

user_ipaddr_history 示例查询

以下查询返回自指定的开始时间戳之后选定 IP 地址的所有用户活动记录。

```
SELECT ipaddr, start_time_sec, end_time_sec, user_name, user_rna_service,
user_last_seen_sec, user_last_updated_sec

FROM user_ipaddr_history

WHERE HEX(ipaddr) = "00000000000000000000FFFF0A0A0A04" AND start_time_sec >=
UNIX_TIMESTAMP("2011-10-01 00:00:00");
```

user_ipaddr_history

方案：连接日志表

本章包含有关适用于连接数据的方案与所支持的联合的信息。

有关详细信息，请参阅下表列出的各节。“Version” 列指示列出的各表所支持的数据库访问版本。

表 7-1 连接日志表的方案

请参阅……	存储有关以下内容的信息的表...	版本
connection_log，第 7-1 页	各个连接。代替已废弃的表 `rna_flow`。	5.0+
connection_summary，第 7-10 页	连接日志摘要。代替已废弃的表 `rna_flow_summary`。	5.0+
si_connection_log，第 7-13 页	各个连接。用于安全智能。	5.3+

connection_log

`connection_log` 表包含有关连接事件的信息。当受监控主机和任意其他主机之间建立连接时，FireSIGHT 系统会生成连接事件；此事件包含关于受监控流量的详细信息。

从 5.0 版本的 FireSIGHT 系统开始，`connection_log` 表代替已废弃的 `rna_flow` 表。

有关详细信息，请参阅以下各节：

- connection_log 字段，第 7-1 页
- connection_log 联合，第 7-10 页
- connection_log 示例查询，第 7-10 页

connection_log 字段

下表列出您可在 `connection_log` 表中访问的数据库字段。

表 7-2 connection_log 字段

字段	说明
access_control_policy_name	包含记录连接的访问控制规则（或默认操作）的访问控制策略。
access_control_policy_UUID	包含记录连接的访问控制规则（或默认操作）的访问控制策略的 UUID。

表 7-2　connection_log 字段（续）

字段	说明
access_control_reason	访问控制规则记录连接的原因。以下项之一： • User Bypass • IP Block • IP Monitor • File Monitor • File Block • File Resume • Intrusion Block • 如果未记录连接，则为空白
access_control_rule_action	与访问控制规则关联的操作（或默认操作）：allow、block等。
access_control_rule_id	规则的内部标识号。
access_control_rule_name	记录连接的访问控制规则（或默认操作）。
application_protocol_id	应用协议的内部标识号。
application_protocol_name	以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果根据已知服务器指纹，系统无法识别服务器，则为 unknown • 如果系统要求提供更多数据，则显示 pending • 如果连接中没有应用信息，则为空值
bytes_recv	会话响应方传输的总字节数。
bytes_sent	会话发起方发送的总字节数。
cert_valid_end_date	连接中使用的 SSL 证书停止有效的 Unix 时间戳。
cert_valid_start_date	颁发连接中使用的 SSL 证书时的 Unix 时间戳。
client_application_id	入侵事件中使用的客户端应用的内部标识号。
client_application_name	入侵事件中使用的客户端应用（如有）。以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果系统检测到客户端应用，但无法识别具体应用，则显示通用客户端名称 • 如果连接中没有客户端应用信息，则为空值
client_application_version	客户端应用的版本。
connection_type	连接信息的检测源。可以为以下任意一项： • 如果是思科设备检测的，则为 rna • 如果由支持 NetFlow 的设备导出，则为 netflow
counter	与连接事件关联的入侵事件计数器。
file_count	Snort 在会话中识别的文件数。对于会话中识别的每个文件都会生成一条记录。
first_packet_sec	检测到会话的第一个数据包时的日期和时间 UNIX 时间戳。

表 7-2　connection_log 字段（续）

字段	说明
flow_id	连接的内部标识号。
icmp_code	如果事件为 ICMP 流量，则此字段为 ICMP 代码；如果事件不是从 ICMP 流量生成的，则此字段为 null。
icmp_type	如果事件为 ICMP 流量，则此字段为 ICMP 类型；如果事件不是从 ICMP 流量生成的，则此字段为 null。
initiator_continent_name	发起会话的主机的大陆名称： ** - 未知 na - 北美洲 as - 亚洲 af - 非洲 eu - 欧洲 sa - 南美洲 au - 澳大利亚 an - 南极洲
initiator_country_id	发起会话的主机的国家/地区代码。
initiator_country_name	发起会话的主机的国家/地区名称。
initiator_ip	在 5.2 版本中已弃用此字段。由于向后兼容性，此字段中的值未设置为 null，但这并不可靠。
initiator_ip_address	在 5.0 版本中已弃用此字段。对所有查询都会返回 null。
initiator_ipaddr	发起会话的主机的 IP 地址二进制表示。
initiator_ipv4	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
initiator_port	会话发起者使用的端口。
initiator_user_dept	最后登录发起者主机的用户所在的部门。
initiator_user_email	最后登录发起者主机的用户的邮件地址。
initiator_user_first_name	最后登录发起者主机的用户的名字。
initiator_user_id	最后登录发起者主机的用户的内部识别号。
initiator_user_last_name	最后登录发起者主机的用户的姓氏。
initiator_user_last_seen_sec	对于最后登录发起者主机的用户，FireSIGHT 系统最后一次检测到用户活动的日期和时间的 UNIX 时间戳。
initiator_user_last_updated_sec	对于最后登录发起者主机的用户，FireSIGHT 系统最后一次更新用户记录的日期和时间的 UNIX 时间戳。
initiator_user_name	最后登录发起者主机的用户的用户名。
initiator_user_phone	最后登录发起者主机的用户的电话号码。
instance_id	生成事件的受管设备上 Snort 实例的数字 ID。
interface_egress_name	与连接相关的入口接口。
interface_ingress_name	与连接相关的出口接口。
ioc_count	在连接中找到的威胁指示数量。

表 7-2　connection_log 字段（续）

字段	说明
ips_event_count	达到入侵事件阈值之前连接中生成的入侵事件的数量。
last_packet_sec	检测到会话的最后一个数据包时的日期和时间 UNIX 时间戳。
monitor_rule_id_1	与连接关联的第一个监控器规则的 ID。此 ID 与 monitor_rule_name_1 中存储的名称关联。
monitor_rule_id_2	与连接关联的第二个监控器规则的 ID。此 ID 与 monitor_rule_name_2 中存储的名称关联。
monitor_rule_id_3	与连接关联的第三个监控器规则的 ID。此 ID 与 monitor_rule_name_3 中存储的名称关联。
monitor_rule_id_4	与连接关联的第四个监控器规则的 ID。此 ID 与 monitor_rule_name_4 中存储的名称关联。
monitor_rule_id_5	与连接关联的第五个监控器规则的 ID。此 ID 与 monitor_rule_name_5 中存储的名称关联。
monitor_rule_id_6	与连接关联的第六个监控器规则的 ID。此 ID 与 monitor_rule_name_6 中存储的名称关联。
monitor_rule_id_7	与连接关联的第七个监控器规则的 ID。此 ID 与 monitor_rule_name_7 中存储的名称关联。
monitor_rule_id_8	与连接关联的第八个监控器规则的 ID。此 ID 与 monitor_rule_name_8 中存储的名称关联。
monitor_rule_name_1	与连接关联的第一个监控器规则的名称。此名称与 monitor_rule_id_1 中存储的 ID 关联。
monitor_rule_name_2	与连接关联的第二个监控器规则的名称。此名称与 monitor_rule_id_2 中存储的 ID 关联。
monitor_rule_name_3	与连接关联的第三个监控器规则的名称。此名称与 monitor_rule_id_3 中存储的 ID 关联。
monitor_rule_name_4	与连接关联的第四个监控器规则的名称。此名称与 monitor_rule_id_4 中存储的 ID 关联。
monitor_rule_name_5	与连接关联的第五个监控器规则的名称。此名称与 monitor_rule_id_5 中存储的 ID 关联。
monitor_rule_name_6	与连接关联的第六个监控器规则的名称。此名称与 monitor_rule_id_6 中存储的 ID 关联。
monitor_rule_name_7	与连接关联的第七个监控器规则的名称。此名称与 monitor_rule_id_7 中存储的 ID 关联。
monitor_rule_name_8	与连接关联的第八个监控器规则的名称。此名称与 monitor_rule_id_8 中存储的 ID 关联。
netbios_domain	连接中使用的 NetBIOS 域。
netflow_dst_as	作为源或对等体的目标 Netflow 自主系统的编号。
netflow_dst_mask	Netflow 目标地址前缀掩码。
netflow_dst_tos	数据包从目标流向源时 IP 报头的服务类型。
netflow_snmp_in	从源流向目标的数据包所采用的接口的 ID。
netflow_snmp_out	从目标流向源的数据包所采用的接口的 ID。

表 7-2　connection_log 字段（续）

字段	说明
netflow_src_as	作为源或对等体的源 Netflow 自主系统的编号。
netflow_src_mask	Netflow 源地址前缀掩码。
netflow_src_tos	数据包从源流向目标时 IP 报头的服务类型。
network_analysis_policy_name	与生成入侵事件的入侵策略关联的网络分析策略。
network_analysis_policy_UUID	与生成入侵事件的入侵策略关联的网络分析策略的 UUID。
packets_recv	发起会话的主机接收的数据包的总数。
packets_sent	发起会话的主机传输的数据包的总数。
protocol_name	连接中使用的协议的名称。
protocol_num	协议的 IANA 编号，如以下网址所示： http://www.iana.org/assignments/protocol-numbers。
responder_continent_name	响应会话发起者的主机的大陆名称： ** - 未知 na - 北美洲 as - 亚洲 af - 非洲 eu - 欧洲 sa - 南美洲 au - 澳大利亚 an - 南极洲
responder_country_id	响应会话发起者的主机的国家/地区代码。
responder_country_name	响应会话发起者的主机的国家/地区名称。
responder_ip	在 5.2 版本中已弃用此字段。由于向后兼容性，此字段中的值未设置为 null，但这并不可靠。
responder_ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
responder_ipaddr	响应会话发起者的主机的 IPv4 或 IPv6 地址的二进制表示。
responder_ipv4	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
responder_port	会话响应者使用的端口。
responder_user_dept	最后一次登录响应会话发起者的主机的用户所在的部门。
responder_user_email	最后一次登录响应会话发起者的主机的用户的邮件地址。
responder_user_first_name	最后一次登录响应会话发起者的主机的用户的名字。
responder_user_id	最后一次登录响应会话发起者的主机的用户的用户内部标识号。
responder_user_last_name	最后一次登录响应会话发起者的主机的用户的姓氏。
responder_user_last_seen_sec	对于最后一次登录响应会话发起者的主机的用户，FireSIGHT 系统最后一次检测到用户活动的日期和时间的 UNIX 时间戳。
responder_user_last_updated_sec	对于最后一次登录响应会话发起者的主机的用户，FireSIGHT 系统最后一次更新用户记录的日期和时间的 UNIX 时间戳。
responder_user_name	最后一次登录响应会话发起者的主机的用户的用户名。

表 7-2　connection_log 字段（续）

字段	说明
responder_user_phone	最后一次登录响应会话发起者的主机的用户的电话号码。
security_context	对流量通过的安全情景（虚拟防火墙）的说明。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
security_intelligence_category	与连接关联的安全智能类别。
security_intelligence_ip	与连接关联的安全智能监控的 IP 地址是源 IP (src) 还是目标 IP (dst)。
security_zone_egress_name	连接事件中的出口安全区。
security_zone_ingress_name	连接事件中的入口安全区。
sensor_address	生成事件的受管设备的 IP 地址。格式为 ipv4 address,ipv6 address。
sensor_name	监控会话的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
source_device	在 5.0 版本中已弃用此字段。对所有查询都会返回 null。
src_device_ip	在 5.2 版本中已弃用此字段。由于向后兼容性，此字段中的值未设置为 null，但这并不可靠。
src_device_ipaddr	可以为以下任意一项： • 导出连接数据的支持 NetFlow 的设备的 IP 地址二进制表示。 • 对于思科受管设备检测到的连接，此字段为 0。
src_device_ipv4	• 在 5.2 版本中已弃用此字段。对所有查询都返回 null。
ssl_actual_action	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括： • Unknown • Do Not Decrypt • Block • Block With Reset • Decrypt (Known Key) • Decrypt (Replace Key) • Decrypt (Resign)
ssl_cipher_suite	SSL 连接使用的加密套件。该值存储为 十进制格式。请参阅 www.iana.org/assignments/tls-parameters/tls-parameters。 对于此值指定的加密套件，此字段为 xhtml。

表 7-2　connection_log 字段（续）

字段	说明
ssl_expected_action	根据 SSL 规则应该对连接执行的操作。可能的值包括： • *Unknown* • *Do Not Decrypt* • *Block* • *Block With Reset* • *Decrypt (Known Key)* • *Decrypt (Replace Key)* • *Decrypt (Resign)*
ssl_flow_flags	加密连接的调试级别标志。可能的值包括： • 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 • 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 • 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
ssl_flow_messages	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246 。 • 0x00000001 - NSE_MT__HELLO_REQUEST • 0x00000002 - NSE_MT__CLIENT_ALERT • 0x00000004 - NSE_MT__SERVER_ALERT • 0x00000008 - NSE_MT__CLIENT_HELLO • 0x00000010 - NSE_MT__SERVER_HELLO • 0x00000020 - NSE_MT__SERVER_CERTIFICATE • 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 - NSE_MT__CERTIFICATE_REQUEST • 0x00000100 - NSE_MT__SERVER_HELLO_DONE • 0x00000200 - NSE_MT__CLIENT_CERTIFICATE • 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 - NSE_MT__CERTIFICATE_VERIFY • 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 - NSE_MT__CLIENT_FINISHED • 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 - NSE_MT__SERVER_FINISHED • 0x00010000 - NSE_MT__NEW_SESSION_TICKET • 0x00020000 - NSE_MT__HANDSHAKE_OTHER • 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER

表 7-2　connection_log 字段（续）

字段	说明
ssl_flow_status	SSL 流量的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括： • "Unknown" • "No Match" • "Success" • "Uncached Session" • "Unknown Cipher Suite" • "Unsupported Cipher Suite" • "Unsupported SSL Version" • "SSL Compression Used" • "Session Undecryptable in Passive Mode" • "Handshake Error" • "Decryption Error" • "Pending Server Name Category Lookup" • "Pending Common Name Category Lookup" • "Internal Error" • "Network Parameters Unavailable" • "Invalid Server Certificate Handle" • "Server Certificate Fingerprint Unavailable" • "Cannot Cache Subject DN" • "Cannot Cache Issuer DN" • "Unknown SSL Version" • "External Certificate List Unavailable" • "External Certificate Fingerprint Unavailable" • "Internal Certificate List Invalid" • "Internal Certificate List Unavailable" • "Internal Certificate Unavailable" • "Internal Certificate Fingerprint Unavailable" • "Server Certificate Validation Unavailable" • "Server Certificate Validation Failure" • "Invalid Action"
ssl_issuer_common_name	SSL 证书的颁发者常用名。这通常是证书颁发者的主机和域名，但也可能包含其他信息。
ssl_issuer_country	SSL 证书颁发者的国家/地区。
ssl_issuer_organization	SSL 证书颁发者的组织。
ssl_issuer_organization_unit	SSL 证书颁发者的组织单位。

表 7-2　connection_log 字段（续）

字段	说明
ssl_policy_action	为策略配置的无规则匹配情况下的默认操作。
ssl_policy_name	处理连接的 SSL 策略的 ID 编号。
ssl_policy_reason	SSL 策略记录 SSL 会话的原因。
ssl_rule_action	针对 SSL 规则在用户界面中选择的操作（allow、block 等）。
ssl_rule_name	处理连接的 SSL 规则或默认操作的 ID 编号。
ssl_serial_number	SSL 证书的序列号，由发行 CA 分配。
ssl_server_name	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。
ssl_subject_common_name	SSL 证书的持有者常用名。这通常是证书持有者的主机和域名，但也可能包含其他信息。
ssl_subject_country	SSL 证书持有者的国家/地区。
ssl_subject_organization	SSL 证书持有者的组织。
ssl_subject_organization_unit	SSL 证书持有者的组织单位。
ssl_url_category	根据服务器名称和证书常用名识别的流量类别。
ssl_version	用来加密连接的 SSL 或 TLS 协议版本。
tcp_flags	在会话中检测到的 TCP 标志。
url	在会话期间受监控主机所请求的 URL（如果可用）。
url_category	受监控主机所请求的 URL 的类别。
url_reputation	受监控主机所请求的 URL 的信誉。以下项之一： • 1 - 高风险 • 2 - 可疑站点 • 3 - 存在安全风险的良性站点 • 4 - 良性站点 • 5 - 已知
web_application_id	Web 应用的内部标识号。
web_application_name	以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果系统检测到 HTTP 应用协议，但无法识别具体 Web 应用，则显示 web browsing • 如果连接没有 HTTP 流量，则为空值

connection_log 联合

下表列出您可使用 **connection_log** 表执行的联合。

表 7-3　connection_log 联合

您可以联合此表……	与……
application_protocol_id 或 client_application_id 或 web_application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id
initiator_ipaddr 或 responder_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

connection_log 示例查询

以下查询返回来自 **connection_log** 表的最多 25 条连接事件记录，这些记录按照数据包时间戳降序排列。

```
SELECT first_packet_sec, last_packet_sec, initiator_ipaddr, responder_ipaddr,
security_zone_ingress_name, security_zone_egress_name, initiator_port, protocol_name,
responder_port, application_protocol_id, client_application_id, web_application_id, url,
url_category, url_reputation

FROM connection_log

WHERE first_packet_sec <= UNIX_TIMESTAMP("2011-10-01 00:00:00" ) ORDER BY
first_packet_sec

DESC, last_packet_sec DESC LIMIT 0, 25;
```

connection_summary

connection_summary 表包含有关连接摘要或汇总连接的信息。FireSIGHT 系统汇总五分钟间隔内的连接。连接必须满足以下条件才能汇总到连接摘要：

- 具有相同的源和目标 IP 地址
- 使用相同的协议
- 使用相同的应用
- 由相同的受管设备检测（对于由受管设备使用FireSIGHT检测到的会话），或由支持 NetFlow 的设备导出并由相同的受管设备处理

连接摘要中的汇总数据包含发起者与响应者主机发送的数据包和字节的总数以及摘要中的连接数量。

从 5.0 版本的 FireSIGHT 系统开始，**connection_summary** 表代替已废弃的 **rna_flow_summary** 表。有关详细信息，请参阅以下各节：

- connection_summary 字段，第 7-11 页
- connection_summary 联合，第 7-13 页
- connection_summary 示例查询，第 7-13 页

connection_summary 字段

下表列出您可在 **connection_summary** 表中访问的数据库字段。

表 7-4　connection_summary 字段

字段	说明
application_protocol_id	应用协议的内部标识号。
application_protocol_name	以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果根据已知服务器指纹，系统无法识别服务器，则为 unknown • 如果系统要求提供更多数据，则显示 pending • 如果连接中没有应用信息，则为空值
bytes_recv	会话响应方传输的总字节数。
bytes_sent	会话发起方传输的总字节数。
connection_type	连接信息的检测源。可以为以下任意一项： • 如果是思科设备检测的，则为 rna • 如果由支持 NetFlow 的设备导出，则为 netflow
flow_type	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
id	连接摘要的内部标识号。
initiator_ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
initiator_ipaddr	发起会话的主机的 IP 地址二进制表示。
initiator_user_dept	最后登录发起者主机的用户所在的部门。
initiator_user_email	最后登录发起者主机的用户的邮件地址。
initiator_user_first_name	最后登录发起者主机的用户的名字。
initiator_user_id	最后登录发起者主机的用户的内部识别号。
initiator_user_last_name	最后登录发起者主机的用户的姓氏。
initiator_user_last_seen_sec	对于最后登录发起者主机的用户，FireSIGHT 系统最后一次检测到用户活动的日期和时间的 UNIX 时间戳。
initiator_user_last_updated_sec	对于最后登录发起者主机的用户，FireSIGHT 系统最后一次更新用户记录的日期和时间的 UNIX 时间戳。
initiator_user_name	最后登录发起者主机的用户的用户名。
initiator_user_phone	最后登录发起者主机的用户的电话号码。
interface_egress_name	与连接相关的入口接口。

表 7-4　connection_summary 字段（续）

字段	说明
interface_ingress_name	与连接相关的出口接口。
num_connections	摘要中的连接数量。对于长期运行的连接，即跨越多个连接摘要间隔的连接，只有第一个连接摘要间隔可递增。
packets_recv	会话响应方发送的数据包总数。
packets_sent	会话发起方发送的数据包总数。
protocol_name	汇总会话中使用的协议的名称。
protocol_num	协议的 IANA 编号，如以下网址所示： http://www.iana.org/assignments/protocol-numbers。
responder_ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
responder_ipaddr	响应汇总会话发起者的主机的 IP 地址二进制表示。
responder_port	汇总会话中响应者使用的端口。
responder_user_dept	最后一次登录响应汇总会话发起者的主机的用户所在的部门。
responder_user_email	最后一次登录响应汇总会话发起者的主机的用户的邮件地址。
responder_user_first_name	最后一次登录响应汇总会话发起者的主机的用户的名字。
responder_user_id	最后一次登录响应汇总会话发起者的主机的用户的内部标识号。
responder_user_last_name	最后一次登录响应汇总会话发起者的主机的用户的姓氏。
responder_user_last_seen_sec	对于最后一次登录响应汇总会话发起者的主机的用户，FireSIGHT 系统最后一次检测到用户活动的日期和时间的 UNIX 时间戳。
responder_user_last_updated_sec	对于最后一次登录响应会话发起者的主机的用户，FireSIGHT 系统最后一次更新用户记录的日期和时间的 UNIX 时间戳。
responder_user_name	最后一次登录响应汇总会话发起者的主机的用户的用户名。
responder_user_phone	最后一次登录响应汇总会话发起者的主机的用户的电话号码。
security_zone_egress_name	连接事件中的出口安全区。
security_zone_ingress_name	连接事件中的入口安全区。
sensor_address	生成事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_name	监控汇总会话的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
source_device	源设备的标识，可能是以下任一项： • 导出连接数据的支持 NetFlow 的设备的 IP 地址 • FireSIGHT （如果连接是被思科受管设备检测到的）
start_time_sec	摘要中用于汇总会话的五分钟时间间隔开始时的日期和时间 UNIX 时间戳。

connection_summary 联合

下表列出您可使用 **connection_summary** 表执行的联合。

表 7-5　connection_summary 联合

您可以联合此表……	与……
application_protocol_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id
initiator_ipaddr 或 responder_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

connection_summary 示例查询

以下查询返回所选设备检测到的最多五个连接事件摘要记录。

```
SELECT initiator_ipaddr, responder_ipaddr, protocol_name, application_protocol_id,
source_device, sensor_name, sensor_address, packets_recv, packets_sent, bytes_recv,
bytes_sent, connection_type, num_connections

FROM connection_summary

WHERE sensor_name='linden' limit 5;
```

si_connection_log

si_connection_log 表包含有关安全智能事件的信息。连接被列入黑名单或受安全智能监控时，FireSIGHT 系统会生成安全智能事件；此事件包含关于受监控流量的详细信息。

有关详细信息，请参阅以下各节：

- si_connection_log 字段，第 7-14 页
- si_connection_log 联合，第 7-22 页
- si_connection_log 示例查询，第 7-22 页

si_connection_log 字段

下表列出您可在 **si_connection_log** 表中访问的数据库字段。

表 7-6　　si_connection_log 字段

字段	说明
access_control_policy_name	包含记录连接的访问控制规则（或默认操作）的访问控制策略。
access_control_policy_UUID	包含记录连接的访问控制规则（或默认操作）的访问控制策略的 UUID。
access_control_reason	访问控制规则记录连接的原因。以下项之一： • User Bypass • IP Block • IP Monitor • File Monitor • File Block • File Resume • Intrusion Block • 如果未记录连接，则为空白
access_control_rule_action	与访问控制规则关联的操作（或默认操作）：allow、block等。
access_control_rule_id	规则的内部标识号。
access_control_rule_name	记录连接的访问控制规则（或默认操作）。
application_protocol_id	应用协议的内部标识号。
application_protocol_name	以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果根据已知服务器指纹，系统无法识别服务器，则为 unknown • 如果系统要求提供更多数据，则显示 pending • 如果连接中没有应用信息，则为空值
bytes_recv	会话响应方传输的总字节数。
bytes_sent	会话发起方发送的总字节数。
cert_valid_end_date	连接中使用的 SSL 证书停止有效的 Unix 时间戳。
cert_valid_start_date	颁发连接中使用的 SSL 证书时的 Unix 时间戳。
client_application_id	入侵事件中使用的客户端应用的内部标识号。
client_application_name	入侵事件中使用的客户端应用（如有）。以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果系统检测到客户端应用，但无法识别具体应用，则显示通用客户端名称 • 如果连接中没有客户端应用信息，则为空白
client_application_version	客户端应用的版本。

表 7-6　si_connection_log 字段（续）

字段	说明
connection_type	连接信息的检测源。可以为以下任意一项： • 如果是思科设备检测的，则为 rna • 如果由支持 NetFlow 的设备导出，则为 netflow
counter	与连接事件关联的入侵事件计数器。
file_count	Snort 在会话中识别的文件数。对于会话中识别的每个文件都会生成一条记录。
first_packet_sec	检测到会话的第一个数据包时的日期和时间 UNIX 时间戳。
icmp_code	如果事件为 ICMP 流量，则此字段为 ICMP 代码；如果事件不是从 ICMP 流量生成的，则此字段为 null。
icmp_type	如果事件为 ICMP 流量，则此字段为 ICMP 类型；如果事件不是从 ICMP 流量生成的，则此字段为 null。
initiator_continent_name	发起会话的主机的大陆名称。 ** - 未知 na - 北美洲 as - 亚洲 af - 非洲 eu - 欧洲 sa - 南美洲 au - 澳大利亚 an - 南极洲
initiator_country_id	发起会话的主机的国家/地区代码。
initiator_country_name	发起会话的主机的国家/地区名称。
initiator_ipaddr	发起会话的主机的 IP 地址二进制表示。
initiator_port	会话发起者使用的端口。
initiator_user_dept	最后登录发起者主机的用户所在的部门。
initiator_user_email	最后登录发起者主机的用户的邮件地址。
initiator_user_first_name	最后登录发起者主机的用户的名字。
initiator_user_id	最后登录发起者主机的用户的内部识别号。
initiator_user_last_name	最后登录发起者主机的用户的姓氏。
initiator_user_last_seen_sec	对于最后登录发起者主机的用户，FireSIGHT 系统最后一次检测到用户活动的日期和时间的 UNIX 时间戳。
initiator_user_last_updated_sec	对于最后登录发起者主机的用户，FireSIGHT 系统最后一次更新用户记录的日期和时间的 UNIX 时间戳。
initiator_user_name	最后登录发起者主机的用户的用户名。
initiator_user_phone	最后登录发起者主机的用户的电话号码。
instance_id	生成事件的受管设备上 Snort 实例的数字 ID。
interface_egress_name	与连接相关的入口接口。

表 7-6　si_connection_log 字段（续）

字段	说明
interface_ingress_name	与连接相关的出口接口。
ioc_count	在连接中找到的威胁指示数量。
ips_event_count	达到入侵事件阈值之前连接中生成的入侵事件的数量。
last_packet_sec	检测到会话的最后一个数据包时的日期和时间 UNIX 时间戳。
monitor_rule_id_1	与连接关联的第一个监控器规则的 ID。此 ID 与 monitor_rule_name_1 中存储的名称关联。
monitor_rule_id_2	与连接关联的第二个监控器规则的 ID。此 ID 与 monitor_rule_name_2 中存储的名称关联。
monitor_rule_id_3	与连接关联的第三个监控器规则的 ID。此 ID 与 monitor_rule_name_3 中存储的名称关联。
monitor_rule_id_4	与连接关联的第四个监控器规则的 ID。此 ID 与 monitor_rule_name_4 中存储的名称关联。
monitor_rule_id_5	与连接关联的第五个监控器规则的 ID。此 ID 与 monitor_rule_name_5 中存储的名称关联。
monitor_rule_id_6	与连接关联的第六个监控器规则的 ID。此 ID 与 monitor_rule_name_6 中存储的名称关联。
monitor_rule_id_7	与连接关联的第七个监控器规则的 ID。此 ID 与 monitor_rule_name_7 中存储的名称关联。
monitor_rule_id_8	与连接关联的第八个监控器规则的 ID。此 ID 与 monitor_rule_name_8 中存储的名称关联。
monitor_rule_name_1	与连接关联的第一个监控器规则的名称。此名称与 monitor_rule_id_1 中存储的 ID 关联。
monitor_rule_name_2	与连接关联的第二个监控器规则的名称。此名称与 monitor_rule_id_2 中存储的 ID 关联。
monitor_rule_name_3	与连接关联的第三个监控器规则的名称。此名称与 monitor_rule_id_3 中存储的 ID 关联。
monitor_rule_name_4	与连接关联的第四个监控器规则的名称。此名称与 monitor_rule_id_4 中存储的 ID 关联。
monitor_rule_name_5	与连接关联的第五个监控器规则的名称。此名称与 monitor_rule_id_5 中存储的 ID 关联。
monitor_rule_name_6	与连接关联的第六个监控器规则的名称。此名称与 monitor_rule_id_6 中存储的 ID 关联。
monitor_rule_name_7	与连接关联的第七个监控器规则的名称。此名称与 monitor_rule_id_7 中存储的 ID 关联。
monitor_rule_name_8	与连接关联的第八个监控器规则的名称。此名称与 monitor_rule_id_8 中存储的 ID 关联。
netbios_domain	连接中使用的 NetBIOS 域。
netflow_dst_as	作为源或对等体的目标 Netflow 自主系统的编号。
netflow_dst_mask	Netflow 目标地址前缀掩码。
netflow_dst_tos	数据包从目标流向源时 IP 报头的服务类型。

表 7-6　　si_connection_log 字段（续）

字段	说明
netflow_snmp_in	从源流向目标的数据包所采用的接口的 ID。
netflow_snmp_out	从目标流向源的数据包所采用的接口的 ID。
netflow_src_as	作为源或对等体的源 Netflow 自主系统的编号。
netflow_src_mask	Netflow 源地址前缀掩码。
netflow_src_tos	数据包从源流向目标时 IP 报头的服务类型。
network_analysis_policy_name	与生成入侵事件的入侵策略关联的网络分析策略。
network_analysis_policy_UUID	与生成入侵事件的入侵策略关联的网络分析策略的 UUID。
packets_recv	发起会话的主机接收的数据包的总数。
packets_sent	发起会话的主机传输的数据包的总数。
protocol_name	连接中使用的协议的名称。
protocol_num	协议的 IANA 编号，如以下网址所示： http://www.iana.org/assignments/protocol-numbers。
responder_continent_name	响应会话发起者的主机的大陆名称。 ** - 未知 na - 北美洲 as - 亚洲 af - 非洲 eu - 欧洲 sa - 南美洲 au - 澳大利亚 an - 南极洲
responder_country_id	响应会话发起者的主机的国家/地区代码。
responder_country_name	响应会话发起者的主机的国家/地区名称。
responder_ipaddr	响应会话发起者的主机的 IPv4 或 IPv6 地址的二进制表示。
responder_port	会话响应者使用的端口。
responder_user_dept	最后一次登录响应会话发起者的主机的用户所在的部门。
responder_user_email	最后一次登录响应会话发起者的主机的用户的邮件地址。
responder_user_first_name	最后一次登录响应会话发起者的主机的用户的名字。
responder_user_id	最后一次登录响应会话发起者的主机的用户的用户内部标识号。
responder_user_last_name	最后一次登录响应会话发起者的主机的用户的姓氏。
responder_user_last_seen_sec	对于最后一次登录响应会话发起者的主机的用户，FireSIGHT 系统最后一次检测到用户活动的日期和时间的 UNIX 时间戳。
responder_user_last_updated_sec	对于最后一次登录响应会话发起者的主机的用户，FireSIGHT 系统最后一次更新用户记录的日期和时间的 UNIX 时间戳。
responder_user_name	最后一次登录响应会话发起者的主机的用户的用户名。
responder_user_phone	最后一次登录响应会话发起者的主机的用户的电话号码。

表 7-6　si_connection_log 字段（续）

字段	说明
security_context	对流量通过的安全情景（虚拟防火墙）的说明。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
security_intelligence_category	与连接关联的安全智能类别。
security_intelligence_ip	与连接关联的安全智能监控的 IP 地址是源 IP (src) 还是目标 IP (dst)。
security_zone_egress_name	连接事件中的出口安全区。
security_zone_ingress_name	连接事件中的入口安全区。
sensor_address	生成事件的受管设备的 IP 地址。格式为 ipv4 address,ipv6 address。
sensor_name	监控会话的受管设备的名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
src_device_ipaddr	可以为以下任意一项： • 导出连接数据的支持 NetFlow 的设备的 IP 地址二进制表示 • 对于思科受管设备检测到的连接，此字段为 0
ssl_actual_action	根据 SSL 规则对连接执行的操作。 由于规则中指定的操作可能无法执行， 此操作可能与预期操作不同。可能的值包括： • "Unknown" • "Do Not Decrypt" • "Block" • "Block With Reset" • "Decrypt (Known Key)" • "Decrypt (Replace Key)" • "Decrypt (Resign)"
ssl_cipher_suite	SSL 连接使用的加密套件。该值存储为 十进制格式。请参阅 www.iana.org/assignments/tls-parameters/tls-parameters。 对于此值指定的加密套件，此字段为 xhtml。
ssl_expected_action	根据 SSL 规则 应该对连接执行的操作。可能的值包括： • "Unknown" • "Do Not Decrypt" • "Block" • "Block With Reset" • "Decrypt (Known Key)" • "Decrypt (Replace Key)" • "Decrypt (Resign)"

表 7-6　si_connection_log 字段（续）

字段	说明
ssl_flow_flags	加密连接的调试级别标志。可能的 值包括： • 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 • 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 • 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
ssl_flow_messages	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246 。 • 0x00000001 - NSE_MT__HELLO_REQUEST • 0x00000002 - NSE_MT__CLIENT_ALERT • 0x00000004 - NSE_MT__SERVER_ALERT • 0x00000008 - NSE_MT__CLIENT_HELLO • 0x00000010 - NSE_MT__SERVER_HELLO • 0x00000020 - NSE_MT__SERVER_CERTIFICATE • 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 - NSE_MT__CERTIFICATE_REQUEST • 0x00000100 - NSE_MT__SERVER_HELLO_DONE • 0x00000200 - NSE_MT__CLIENT_CERTIFICATE • 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 - NSE_MT__CERTIFICATE_VERIFY • 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 - NSE_MT__CLIENT_FINISHED • 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 - NSE_MT__SERVER_FINISHED • 0x00010000 - NSE_MT__NEW_SESSION_TICKET • 0x00020000 - NSE_MT__HANDSHAKE_OTHER • 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER

表 7-6　si_connection_log 字段（续）

字段	说明
ssl_flow_status	SSL 流量的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括： • "Unknown" • "No Match" • "Success" • "Uncached Session" • "Unknown Cipher Suite" • "Unsupported Cipher Suite" • "Unsupported SSL Version" • "SSL Compression Used" • "Session Undecryptable in Passive Mode" • "Handshake Error" • "Decryption Error" • "Pending Server Name Category Lookup" • "Pending Common Name Category Lookup" • "Internal Error" • "Network Parameters Unavailable" • "Invalid Server Certificate Handle" • "Server Certificate Fingerprint Unavailable" • "Cannot Cache Subject DN" • "Cannot Cache Issuer DN" • "Unknown SSL Version" • "External Certificate List Unavailable" • "External Certificate Fingerprint Unavailable" • "Internal Certificate List Invalid" • "Internal Certificate List Unavailable" • "Internal Certificate Unavailable" • "Internal Certificate Fingerprint Unavailable" • "Server Certificate Validation Unavailable" • "Server Certificate Validation Failure" • "Invalid Action"
ssl_issuer_common_name	SSL 证书的颁发者常用名。这通常是证书颁发者的主机和域名，但也可能包含其他信息。
ssl_issuer_country	SSL 证书颁发者的国家/地区。
ssl_issuer_organization	SSL 证书颁发者的组织。
ssl_issuer_organization_unit	SSL 证书颁发者的组织单位。

表 7-6　si_connection_log 字段（续）

字段	说明
ssl_policy_action	为策略配置的无规则匹配情况下的默认操作。
ssl_policy_name	处理连接的 SSL 策略的 ID 编号。
ssl_policy_reason	SSL 策略记录 SSL 会话的原因。
ssl_rule_action	针对 SSL 规则在用户界面中选择的操作（allow、block 等）。
ssl_rule_name	处理连接的 SSL 规则或默认操作的 ID 编号。
ssl_serial_number	SSL 证书的序列号，由发行 CA 分配。
ssl_server_name	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。
ssl_subject_common_name	SSL 证书的持有者常用名。这通常是证书持有者的主机和域名，但也可能包含其他信息。
ssl_subject_country	SSL 证书持有者的国家/地区。
ssl_subject_organization	SSL 证书持有者的组织。
ssl_subject_organization_unit	SSL 证书持有者的组织单位。
ssl_url_category	根据服务器名称和证书常用名识别的流量类别。
ssl_version	用来加密连接的 SSL 或 TLS 协议版本。
tcp_flags	在会话中检测到的 TCP 标志。
url	在会话期间受监控主机所请求的 URL（如果可用）。
url_category	受监控主机所请求的 URL 的类别。
url_reputation	受监控主机所请求的 URL 的信誉。以下项之一： • 1 - 高风险 • 2 - 可疑站点 • 3 - 存在安全风险的良性站点 • 4 - 良性站点 • 5 - 已知
web_application_id	Web 应用的内部标识号。
web_application_name	以下任一项： • 如果能够明确识别应用，则显示应用的名称 • 如果系统检测到 HTTP 应用协议，但无法识别具体 Web 应用，则显示 web browsing • 如果连接没有 HTTP 流量，则为空值

si_connection_log 联合

下表列出您可使用 **si_connection_log** 表执行的联合。

表 7-7　si_connection_log 联合

您可以联合此表……	与……
application_protocol_name 或 application_id 或 client_application_id 或 web_application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id
initiator_ipaddr 或 responder_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

si_connection_log 示例查询

以下查询返回来自 **si_connection_log** 表的最多 25 条连接事件记录，这些记录按照数据包时间戳降序排列。

```
SELECT first_packet_sec, last_packet_sec, initiator_ipaddr, responder_ipaddr,
security_zone_ingress_name, security_zone_egress_name, initiator_port, protocol_name,
responder_port, application_protocol_id, client_application_id, web_application_id, url,
url_category, url_reputation

FROM si_connection_log

WHERE first_packet_sec <= UNIX_TIMESTAMP("2011-10-01 00:00:00") ORDER BY
first_packet_sec

DESC, last_packet_sec DESC LIMIT 0, 25;
```

方案：用户活动表

本章包含有关适用于用户活动和身份事件的方案与所支持的联合的信息。FireSIGHT 系统可以通过跟踪各种类型的用户登录（包括 LDAP、POP3、IMAP、SMTP、AIM 和 SIP）检测网络上的用户活动。

有关详细信息，请参阅下表列出的各节。

表 8-1　用户身份表的方案

请参阅……	存储有关以下内容的信息的表...	版本
discovered_users，第 8-1 页	有关系统检测到的用户的信息。	5.0+
user_discovery_event，第 8-2 页	用户发现事件，传达关于网络上用户活动的详细信息。	5.0+

discovered_users

discovered_users 表包含有关系统检测到的每位用户的详细信息。

从 FireSIGHT 系统 5.0 版本开始，**discovered_users** 表代替已废弃的 **rua_users** 表。

有关详细信息，请参阅以下各节：

- discovered_users 字段，第 8-1 页
- discovered_users 联合，第 8-2 页
- discovered_users 示例查询，第 8-2 页

discovered_users 字段

下表列出可在 **discovered_users** 表中访问的字段。

表 8-2　discovered_users 字段

字段	说明
dept	用户所在部门。
email	用户的邮件地址。
first_name	用户的名字。
ip_address	此字段已废弃，对所有查询都会返回 null。

表 8-2　discovered_users 字段（续）

字段	说明
ipaddr	检测到用户登录的主机上 IPv4 或 IPv6 地址的二进制表示。
last_name	用户的姓氏。
last_seen_sec	系统最后一次报告用户登录的日期和时间的 UNIX 时间戳。
last_updated_sec	最后一次更新用户信息的日期和时间的 UNIX 时间戳。
name	用户的姓名。
phone	用户的电话号码。
rna_service	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
user_id	最后登录主机的用户的内部标识号。

discovered_users 联合

下表列出可在 **rua_user** 表上执行的联合。

表 8-3　discovered_users 联合

您可以在此字段联合……	和具有以下联合类型的其他表……
user_id	user_discovery_event.user_id user_ipaddr_history.user_id

discovered_users 示例查询

以下查询返回自从指定日期和时间以来生成的最多 25 条已发现的用户记录。

```
SELECT user_id, ip_address, email, name, last_seen_sec, last_updated_sec
FROM discovered_users
WHERE last_seen_sec >= UNIX_TIMESTAMP("2011-10-01 00:00:00")
LIMIT 0, 25;
```

user_discovery_event

user_discovery_event 表包含每个用户发现事件的记录。

请注意，从 5.0 版本开始，FireSIGHT 系统会记录受管设备级别的用户活动检测，而不再由检测引擎检测。此表中的 detection_engine_name 和 detection_engine_uuid 字段已分别由 sensor_name 和 sensor_uuid 字段代替。这些字段的查询将返回关于生成用户发现事件的受管设备的信息。

有关详细信息，请参阅以下各节：

- user_discovery_event 字段，第 8-3 页
- user_discovery_event 联合，第 8-4 页
- user_discovery_event 示例查询，第 8-4 页

user_discovery_event 字段

下表列出可在 **user_discovery_event** 表中访问的字段。

表 8-4　　user_discovery_event 字段

字段	说明
application_protocol_id	检测到的应用协议的内部标识符。
application_protocol_name	以下任一项： • 连接中所用应用的名称：LDAP、POP3 等 • 如果系统由于多种原因中的一个原因无法识别应用，则会显示为 pending • 如果连接中没有应用信息，则为空值
description	发现事件类型为 Delete User Identity 或 User Identity Dropped 时，显示用户名否则为空值。
event_id	发现事件的内部标识号。
event_time_sec	发现事件的日期和时间的 UNIX 时间戳。
event_type	发现事件的类型。例如，New User Identity 或 User Login。
ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
ipaddr	检测到用户活动的主机上 IP 地址的二进制表示。
reported_by	报告用户登录的 Active Directory 服务器的 IPv4 地址、IPv6 地址或 NetBIOS
sensor_address	检测到用户发现事件的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_name	检测到用户发现事件的受管设备的文本名称。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
user_dept	最后登录主机的用户所在的部门。
user_email	最后登录主机的用户的邮件地址。
user_first_name	用户的名字。
user_id	最后登录主机的用户的内部标识号。
user_last_name	用户的姓氏。
user_last_seen_sec	系统最后一次报告用户登录的日期和时间的 UNIX 时间戳。
user_last_updated_sec	最后一次更新用户信息的日期和时间的 UNIX 时间戳。
user_name	最后登录主机的用户的用户名。
user_phone	最后登录主机的用户的电话号码。

user_discovery_event 联合

下表列出可在 **user_discovery_event** 表上执行的联合。

表 8-5　　user_discovery_event 联合

您可以联合此表……	与……
ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr
user_id	discovered_users.user_id user_ipaddr_history.user_id

user_discovery_event 示例查询

以下查询返回自从特定日期和时间之后选定受管设备生成的最多 25 条用户事件记录。

```
SELECT event_time_sec, ipaddr, sensor_name, event_type, user_name, user_last_seen_sec,
user_last_updated_sec

FROM user_discovery_event

WHERE sensor_name = sensor_name

AND user_last_seen_sec >= UNIX_TIMESTAMP("2011-10-01 00:00:00") ORDER BY event_type ASC

LIMIT 0, 25;
```

方案：关联表

本章包含有关适用于与关联相关的事件的方案与所支持的联合的信息，包括补救状态和白名单事件。有关详细信息，请参阅下表列出的各节。

表 9-1　　关联表方案

请参阅……	存储有关以下内容的信息的表...	版本
compliance_event，第 9-1 页	当活跃关联策略内的关联规则触发时生成的关联事件。	4.10.x+
remediation_status，第 9-5 页	当活跃关联策略触发补救作为响应时生成的补救状态事件。	4.10.x+
white_list_event，第 9-6 页	当系统检测到主机违反活动白名单合规策略中的白名单时生成的白名单事件。	4.10.x+
white_list_violation，第 9-8 页	白名单违规信息，其跟踪您的网络上主机违反活动合规性策略中的合规白名单的方式。	4.10.x+

compliance_event

compliance_event 表包含关于您的防御中心生成的关联事件的信息。

有关详细信息，请参阅以下各节：

- compliance_event 字段，第 9-1 页
- compliance_event 联合，第 9-5 页
- compliance_event 示例查询，第 9-5 页

compliance_event 字段

请记住，此表中很多字段都可能是空的，具体取决于是什么类型的事件触发了关联规则。例如，如果防御中心由于系统检测到在具体端口上运行的具体应用协议或 Web 应用而生成关联事件，则此关联事件不包含与入侵相关的信息。根据您的 FireSIGHT 系统配置，此表中的字段也可能是空的。例如，如果您没有 Control 许可证，则关联事件就不包含用户身份信息。

请注意，从 5.0 版本开始，FireSIGHT 系统会记录受管设备级别的网络和用户活动检测，而不由检测引擎检测。在 **compliance_event** 中，detection_engine_name 和 detection_engine_uuid 字段现在仅返回空白，并且联合这两个字段的查询也返回零记录。有关事件检测位置的信息，您必须查询 sensor_uuid 字段，而不是查询 detection_engine_uuid 字段。

下表列出您可在 **compliance_event** 表中访问的字段。

表 9-2　compliance_event 字段

字段	说明
blocked	表示触发入侵事件的数据包发生了什么情况的值： • 0 - 数据包未被丢弃 • 1 - 数据包已被丢弃（内嵌式、交换或路由式部署） • 2 - 如果已向在内嵌式、交换或路由式部署中配置的设备应用入侵策略，则触发事件的数据包本应已丢弃
description	关于关联事件及其触发方式的信息。
detection_engine_name	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
detection_engine_uuid	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
dst_host_criticality	涉及关联事件的目标主机的用户分配的主机重要性：None、Low、Medium 或 High。
dst_host_type	目标主机类型：Host、Router、Bridge、NAT Device 或 Load Balancer。
dst_ip_address	在 5.2 版本中已弃用此字段。由于向后兼容性，此字段中的值未设置为 null，但这并不可靠。
dst_ip_address_v6	在 5.2 版本中已弃用此字段。由于向后兼容性，此字段中的值未设置为 null，但这并不可靠。
dst_ipaddr	触发事件所涉及的目标主机的 IPv4 或 IPv6 地址的二进制表示。
dst_os_product	目标主机上的操作系统名称。
dst_os_vendor	目标主机上的操作系统供应商。
dst_os_version	目标主机上的操作系统版本号。
dst_port	如果事件协议类型是 TCP 或 UDP，则为接收流量的主机的端口号。如果协议类型是 ICMP，则为 ICMP 代码。
dst_rna_service	如果可以识别，则为与触发事件关联的源主机上的应用协议。如果无法识别，则为以下任一项： • none 或空白 - 无应用协议流量 • unknown - 如果根据已知服务器指纹，无法识别服务器 • pending - 系统要求更多信息
dst_user_dept	目标用户所在部门。
dst_user_email	目标用户的邮件地址。
dst_user_first_name	目标用户的名字。
dst_user_id	目标用户（即发生事件之前最后登录目标主机的用户）的内部标识号。
dst_user_last_name	目标用户的姓氏。
dst_user_last_seen_sec	系统最后一次报告目标用户登录的日期和时间的 UNIX 时间戳。
dst_user_last_updated_sec	最后一次更新目标用户信息的日期和时间的 UNIX 时间戳。
dst_user_name	目标用户的用户名。
dst_user_phone	目标用户的电话号码。
dst_vlan_id	目标主机的 VLAN 标识号（如果适用）。

表 9-2　compliance_event 字段（续）

字段	说明
event_id	设备生成的触发入侵事件的标识号。
event_time_sec	触发事件的日期和时间的 UNIX 时间戳。
event_time_usec	触发事件时间戳的微秒增量。
event_type	触发关联规则或导致防御中心生成关联事件的基本事件类型。其值如下： • ids，针对入侵事件触发器 • rna，针对发现事件、主机输入事件、连接事件或流量配置文件更改触发器 • rua，针对用户发现事件触发器 • whitelist，针对合规白名单违规触发器
host_event_type	事件类型，例如，New Host 或 Identity Conflict。
id	关联事件的内部标识号。
impact	事件的影响标志值。其值如下： • 1 - 红色（易受攻击） • 2 - 橙色（可能易受攻击） • 3 - 黄色（目前不易受攻击） • 4 - 蓝色（未知目标） • 5 - 灰色（未知影响） 仅在入侵事件触发关联规则时设置。
interface_egress_name	与连接相关的入口接口。
interface_ingress_name	与连接相关的出口接口。
policy_name	所违反的关联策略。
policy_rule_name	触发策略违规的关联规则。
policy_rule_uuid	关联规则的唯一标识符。
policy_time_sec	生成关联事件的日期和时间的 UNIX 时间戳。
policy_uuid	关联策略的唯一标识符。
priority	关联事件的优先级，在用户界面上设置。事件优先级根据触发的规则或违反的关联策略的优先级确定。
protocol_name	与事件关联的协议（如果可用）。
protocol_num	NANA 指定的协议编号（如果可用）。
rna_event_type	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
rua_event_type	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
rule_generator_id	生成触发入侵事件的组件的生成器 ID 编号 (GID)。
rule_message	关于触发关联规则的入侵事件的说明文本。对于基于规则的事件，此消息生成自规则。对于基于解码器和预处理器的事件，事件消息是硬编码的。
rule_signature_id	事件的签名 ID (SID)。确定导致生成触发入侵事件的具体规则、解码器消息或预处理器消息。
security_zone_egress_name	关联事件中的出口安全区。

表 9-2　compliance_event 字段（续）

字段	说明
security_zone_ingress_name	关联事件中的入口安全区。
sensor_address	生成触发合规性事件的基本事件的受管设备 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_name	生成触发合规性事件的基本事件的受管设备。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
src_host_criticality	涉及合规性事件的源主机的用户分配的主机重要性：None、Low、Medium 或 High。
src_host_type	源主机类型：Host、Router、Bridge、NAT Device 或 Load Balancer。
src_ip_address	在 5.2 版本中已弃用此字段。由于向后兼容性，此字段中的值未设置为 null，但这并不可靠。
src_ip_address_v6	在 5.2 版本中已弃用此字段。由于向后兼容性，此字段中的值未设置为 null，但这并不可靠。
src_ipaddr	触发事件所涉及的源主机的 IPv4 或 IPv6 地址的二进制表示。
src_os_product	源主机上的操作系统名称。
src_os_vendor	源主机上的操作系统供应商。
src_os_version	源主机上的操作系统版本号。
src_port	源主机上的端口号。对于 ICMP 流量，显示的是 ICMP 类型。
src_rna_service	如果可以识别，则为与触发事件关联的源主机上的应用协议。如果无法识别，则为以下任一项： • none 或空白 - 无应用协议流量 • unknown - 根据已知服务器指纹，无法识别服务器和应用协议 • pending - 系统要求更多信息
src_user_dept	源用户所在部门。
src_user_email	源用户的邮件地址。
src_user_first_name	源用户的名字。
src_user_id	源用户，即发生事件之前最后登录源主机的用户，的内部标识号。
src_user_last_name	源用户的姓氏。
src_user_last_seen_sec	系统最后一次报告源用户登录的日期和时间的 UNIX 时间戳。
src_user_last_updated_sec	最后一次更新源用户信息的日期和时间的 UNIX 时间戳。
src_user_name	源用户的登录用户名。
src_user_phone	源用户的电话号码。
src_vlan_id	源主机的 VLAN 标识号（如果适用）。
user_event_type	触发用户事件的类型，例如，New User Identity 或 User Login。

compliance_event 联合

下表列出您可在 **compliance_event** 表上执行的联合。

表 9-3　compliance_event 联合

您可以联合此表……	与……
dst_ipaddr 或 src_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

compliance_event 示例查询

以下查询返回一周内的最多 25 条关联事件记录，其中的事件信息包括事件时间、源和目标 IP 地址、源和目标端口、策略信息等。

```
SELECT event_id, policy_time_sec, impact, blocked, src_ipaddr, dst_ipaddr, src_port,
dst_port, description, policy_name, policy_rule_name, priority, src_host_criticality,
dst_host_criticality, security_zone_egress_name, security_zone_ingress_name,
sensor_name, interface_egress_name, interface_ingress_name

FROM compliance_event WHERE event_type!="whitelist"

AND policy_time_sec

BETWEEN UNIX_TIMESTAMP("2011-10-01 00:00:00")

AND UNIX_TIMESTAMP("2011-10-07 23:59:59")

ORDER BY policy_time_sec

DESC LIMIT 0, 25;
```

remediation_status

remediation_status 表包含关于补救事件的信息，其中当防御中心发起补救以响应关联策略违规时生成这些补救事件。

有关详细信息，请参阅以下各节：

- remediation_status 字段，第 9-6 页
- remediation_status 联合，第 9-6 页
- remediation_status 示例查询，第 9-6 页

remediation_status 字段

下表列出您可在 **remediation_status** 表中访问的数据库字段。

表 9-4　remediation_status 字段

字段	说明
id	已被违反并触发补救的策略的标识号。
policy_name	已被违反并触发补救的关联策略。
policy_rule_name	触发补救的具体关联规则。
policy_rule_uuid	关联规则的唯一标识符。
policy_time_sec	生成触发补救的关联事件的日期和时间 UNIX 时间戳。
policy_uuid	触发关联事件的关联策略的唯一标识符。
remediation_name	已发起的补救。
remediation_time_sec	防御中心发起补救的日期和时间的 UNIX 时间戳。
status_text	描述在发起补救后所发生情况的消息，例如 “successful completion of remediation”。

remediation_status 联合

您无法在 **remediation_status** 表上执行联合。

remediation_status 示例查询

以下查询返回特定日期之前生成的最多 25 条记录。这些记录包括补救状态信息，例如补救时间戳、状态消息等。

```
SELECT policy_time_sec, remediation_time_sec, remediation_name, policy_name,
policy_rule_name, status_text

FROM remediation_status WHERE remediation_time_sec <= UNIX_TIMESTAMP("2011-10-01
00:00:00")

ORDER BY policy_time_sec

DESC LIMIT 0, 25;
```

white_list_event

white_list_event 表包含当系统检测到主机违反活动白名单合规策略中的白名单时生成的白名单事件。

请注意，从 5.0 版本开始，FireSIGHT 系统会记录受管设备级别的网络和用户活动的检测，而不再由检测引擎检测。在**white_list_event**中，detection_engine_name 和 detection_engine_uuid 字段现在仅返回 null，并且联合这两个字段的查询也返回零记录。查询 sensor_uuid 字段，而不是 detection_engine_uuid 字段，可提供同等信息。

有关详细信息，请参阅以下各节：

white_list_event 字段

下表列出您可在 **white_list_event** 表中访问的数据库字段。

表 9-5　　white_list_event 字段

字段	说明
description	说明白名单是如何被违反的。
detection_engine_name	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
detection_engine_uuid	在 5.0 版本中已弃用此字段。对所有查询都返回 null。
host_criticality	用户向不符合白名单规定的主机所分配的主机重要性：None、Low、Medium 或 High。
host_type	主机的类型：Host、Router、Bridge、NAT Device 或 Load Balancer。
id	白名单事件的内部标识符。
ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
ip_address_v6	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
ipaddr	不合规主机 IP 地址的二进制表示。
os_product	操作系统的产品名称。
os_vendor	操作系统的供应商。
os_version	操作系统的版本号。
policy_name	所违反的合规性策略，包括白名单。
policy_time_sec	生成事件的日期和时间的 UNIX 时间戳。
policy_uuid	包含白名单事件的合规性策略的唯一标识符。
port	与触发服务白名单违规（由于不合规服务造成的违规）的事件关联的端口（如有）。对于其他类型的白名单违规事件，该字段为空白。
priority	白名单事件的优先级，在用户界面上设置。
protocol_name	与事件关联的协议（如果可用）。
protocol_num	NANA 指定的协议编号（如果可用）。
rna_service	触发白名单违规的服务（如果可用）。
sensor_address	检测到流量的受管设备的 IP 地址。格式为 *ipv4_address,ipv6_address*。
sensor_name	生成白名单事件的设备。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
user_dept	用户所在部门。
user_email	用户的邮件地址。
user_first_name	用户的名字。

表 9-5　white_list_event 字段（续）

字段	说明
user_id	发生事件之前最后登录主机的用户的内部标识号。
user_last_name	用户的姓氏。
user_last_seen_sec	系统最后一次报告用户登录的日期和时间的 UNIX 时间戳。
user_last_updated_sec	最后一次更新用户信息的日期和时间的 UNIX 时间戳。
user_name	用户的登录用户名。
user_phone	用户的电话号码。
vlan_id	VLAN 标别号（如果适用）。
white_list_name	所违反的白名单。
white_list_uuid	白名单的唯一标识符。

white_list_event 联合

下表列出您可在 **white_list_event** 表上执行的联合。

表 9-6　white_list_event 联合

您可以联合此表……	与……
ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

white_list_event 示例查询

以下查询返回指定日期之前生成的最多 25 条记录。这些记录包括白名单事件信息，例如合规性策略名称、触发事件的时间戳、白名单名称等。

```
SELECT policy_name, policy_time_sec, ipaddr, user_name, port, description,
white_list_name, priority, host_criticality, sensor_name

FROM white_list_event WHERE policy_time_sec <= UNIX_TIMESTAMP("2011-10-01 00:00:00")

ORDER BY policy_time_sec DESC LIMIT 0, 25;
```

white_list_violation

white_list_violation 表跟踪合规性白名单违规，其跟踪您网络上的主机违反活动合规性策略中的合规白名单的方式。

有关详细信息，请参阅以下各节：

- white_list_violation 字段，第 9-9 页
- white_list_violation 联合，第 9-9 页
- white_list_violation 示例查询，第 9-9 页

white_list_violation 字段

下表列出您可在 **white_list_violation** 表中访问的数据库字段。

表 9-7　　white_list_violation 字段

字段	说明
host_id	违反白名单的主机的 ID 编号。
info	与该白名单违规事件相关的任何可用的供应商、产品或版本信息。 对于违反白名单的协议，此字段还指出违规是由网络协议还是传输协议造成的。
ip_address	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
port	与触发服务白名单违规（由于不合规服务造成的违规）的事件关联的端口（如有）。对于其他类型的白名单违规事件，该字段为空白。
protocol_name	与事件关联的协议。
type	白名单违规的类型，指示违规是否是由于下列内容不合规而导致的： • 操作系统 (os) • 服务 (service) • 客户端应用 (client app) • 协议 (protocol)
violation_time_sec	违规被记录的日期和时间的 UNIX 时间戳。
white_list_name	所违反的白名单。
white_list_uuid	白名单的唯一标识符。

white_list_violation 联合

您无法在 **white_list_violation** 表上执行联合。

white_list_violation 示例查询

以下查询返回最多 25 条记录，包含白名单违规信息，例如违反白名单的主机 IP 地址、被违反的白名单名称和违规计数。

```
SELECT host_id, white_list_name, count(*)

FROM white_list_violation

GROUP BY white_list_name, host_id

ORDER BY white_list_name

DESC LIMIT 0, 25;
```

white_list_violation

方案：文件事件表

本章包含有关文件事件的方案和支持联合的信息。有关详细信息，请参阅下表列出的章节。

表 10-1　　文件事件表的方案

请参阅……	存储有关以下内容的信息的表...	版本
file_event，第 10-1 页	当监控网络中检测到文件传送时生成的文件事件。	5.1.1+

虽然以下表可用，但是思科目前还不支持在这些表上进行查找：

- file_categories
- file_rules
- file_types
- file_type_rule_map
- file_type_category_map

file_event

file_event 表包含关于防御中心生成的文件事件的信息。每次在监控网络上检测到文件传送时都会生成一个新的文件事件。

有关详细信息，请参阅以下各节：

- file_event 字段，第 10-2 页
- file_event 联合，第 10-6 页
- file_event 示例查询，第 10-6 页

file_event 字段

file_event 表包含通过监控网络检测到的文件的相关信息。每个文件事件都可与一个连接事件关联。系统会记录文件和文件传送的详细信息，包括文件的名称、大小、源、目标和方向，文件的 SHA256 哈希、检测到文件的设备，以及文件是否被视为恶意软件。

表 10-2　file_event 字段

字段	说明
action	根据文件类型对文件执行的操作。可能会有以下值： • 1 - 检测 • 2 - 阻止 • 3 - 恶意软件云查找 • 4 - 恶意软件阻止 • 5 - 恶意软件白名单 • 6 - 云查找超时
application_id	通过文件传送映射至应用的 ID 编号。
application_name	以下任一项： • 连接中使用的应用的名称 • 如果系统无法识别此应用，则会显示为 pending 或 unknown • 如果连接中没有应用信息，则为空值
archived	指示文件是否已存档。
cert_valid_end_date	连接中使用的 SSL 证书停止有效的 Unix 时间戳。
cert_valid_start_date	颁发连接中使用的 SSL 证书时的 Unix 时间戳。
client_application_id	客户端应用（如适用）的内部标别号。
client_application_name	客户端应用（如适用）的名称。
connection_sec	与文件事件关联的连接事件的 UNIX 时间戳（自 00:00:00 01/01/1970 起经过的秒数）。
counter	事件的特定计数器，用于区别在同一秒内发生的多个事件。
direction	文件是否已上传或下载。目前该值完全取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
disposition	文件的恶意软件状态。可能的值包括： • CLEAN - 文件是安全的，不包含恶意软件 • UNKNOWN - 不确定文件是否包含恶意软件 • MALWARE - 文件包含恶意软件 • UNAVAILABLE - 软件无法向思科云发送请求以了解处置情况，或思科云服务未响应此请求 • CUSTOM SIGNATURE - 文件与用户定义的哈希匹配，并且以用户指定的方式进行处理

表 10-2　file_event 字段（续）

字段	说明
dst_continent_name	目标主机的大陆名称。 ** - 未知 na - 北美洲 as - 亚洲 af - 非洲 eu - 欧洲 sa - 南美洲 au - 澳大利亚 an - 南极洲
dst_country_id	目标主机的国家/地区代码。
dst_country_name	目标主机的国家/地区名称。
dst_ip_address_v6	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
dst_ipaddr	触发事件所涉及的目标主机的 IP 地址的二进制表示。
dst_port	连接的目标的端口号。
event_description	与事件类型相关的其他事件信息。
event_id	事件标识号。
file_name	检测到的文件的名称。该名称可包含 UTF-8 字符。
file_sha	文件的 SHA256 哈希。
file_size	检测到的文件的大小（字节数）。
file_type	被检测或隔离文件的文件类型。
file_type_category	文件类别的说明。
file_type_category_id	文件类别的数字标识符。
file_type_id	映射至文件类型的 ID 编号。
instance_id	生成事件的受管设备上 Snort 实例的数字 ID。
policy_uuid	作为触发事件的访问控制策略的唯一标识符的标别号。

表 10-2　file_event 字段（续）

字段	说明
sandboxed	是否已发送该文件进行动态分析。可能的值如下： • Sent for Analysis • Failed to Send • File Size is Too Small • File Size is Too Large • Sent for Analysis • Analysis Complete • Failure (Network Issue) • Failure (Rate Limit) • Failure (File Too Large) • Failure (File Read Error) • Failure (Internal Library Error) • File Not Sent, Disposition Unavailable • Failure (Cannot Run File) • Failure (Analysis Timeout) • File Not Supported
score	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
security_context	对流量通过的安全情景（虚拟防火墙）的说明。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
sensor_address	提供事件的设备的 IP 地址二进制表示。
sensor_id	提供事件的设备的 ID。
sensor_name	生成事件记录的受管设备的文本名称。当事件指报告设备本身，而不是所连接的设备时，则此字段为 null。
sensor_uuid	受管设备的唯一标识符，如果 sensor_name 为 null，则此标识符为 0。
signature_processed	指示文件签名是否已进行处理。
src_continent_name	源主机的大陆名称。 ** - 未知 na - 北美洲 as - 亚洲 af - 非洲 eu - 欧洲 sa - 南美洲 au - 澳大利亚 an - 南极洲
src_country_id	源主机的国家/地区代码。
src_country_name	源主机的国家/地区名称。

表 10-2　file_event 字段（续）

字段	说明
src_ip_address_v6	在 5.2 版本中已弃用此字段。对所有查询都返回 null。
src_ipaddr	触发事件所涉及的源主机的 IPv4 或 IPv6 地址的二进制表示。
src_port	连接源的端口号。
ssl_issuer_common_name	SSL 证书的颁发者常用名。这通常是证书颁发者的主机和域名，但也可能包含其他信息。
ssl_issuer_country	SSL 证书颁发者的国家/地区。
ssl_issuer_organization	SSL 证书颁发者的组织。
ssl_issuer_organization_unit	SSL 证书颁发者的组织单位。
ssl_serial_number	SSL 证书的序列号，由发行 CA 分配。
ssl_subject_common_name	SSL 证书的持有者常用名。这通常是证书持有者的主机和域名，但也可能包含其他信息。
ssl_subject_country	SSL 证书持有者的国家/地区。
ssl_subject_organization	SSL 证书持有者的组织。
ssl_subject_organization_unit	SSL 证书持有者的组织单位。
storage	文件的存储状态。可能的值如下： • File Stored • Unable to Store File • File Size is Too Large • File Size is Too Small • Unable to Store File • File Not Stored, Disposition Unavailable
threat_name	威胁的名称。
timestamp	已传输的文件内容足以识别文件类型时的 UNIX 时间戳。
url	文件源的 URL。
user_id	目标用户（即发生事件之前最后登录目标主机的用户）的内部标识号。
username	与 user_id 关联的名称。
web_application_id	Web 应用（如适用）的内部标别号。
web_application_name	Web 应用（如适用）的名称。

file_event 联合

下表列出可在 **file_event** 表上执行的联合。

表 10-3　file_event 联合

您可以联合此表……	与……
application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id

file_event 示例查询

以下查询返回文件性质不是 CLEAN 的情况下的最多 10 个文件事件，包含应用名称、连接信息和文件名。

```
SELECT file_event.application_name, file_event.connection_sec, file_event.counter,
file_event.file_name

FROM file_event

WHERE file_event.disposition != 'CLEAN' limit 10;
```

弃用的表

本附录包含有关之前版本中曾使用但现在已弃用的表的信息。虽然您仍然可以查询这些表，但是其字段内的值可能不正确，而且在大多数情况下为 null。不支持在这些表上执行联合。

表 A-1　　弃用的表

表	替换成	最后使用的版本
application_ip_map	application_host_map，第 6-4 页	5.1.1
rna_ip_host	rna_host，第 6-10 页	5.1.1
rna_ip_host_attribute	rna_host_attribute，第 6-12 页	5.1.1
rna_ip_host_client_app	rna_host_client_app，第 6-14 页	5.1.1
rna_ip_host_client_app_payload	rna_host_client_app_payload，第 6-16 页	5.1.1
rna_ip_host_os	rna_host_os，第 6-26 页	5.1.1
rna_ip_host_os_vulns	rna_host_os_vulns，第 6-27 页	5.1.1
rna_ip_host_sensor	rna_host_sensor，第 6-30 页	5.1.1
rna_ip_host_service	rna_host_service，第 6-32 页	5.1.1
rna_ip_host_service_banner	rna_host_service_banner，第 6-34 页	5.1.1
rna_ip_host_service_info	rna_host_service_info，第 6-35 页	5.1.1
rna_ip_host_service_payload	rna_host_service_payload，第 6-38 页	5.1.1
rna_ip_host_service_subtype	rna_host_service_subtype，第 6-41 页	5.1.1
rna_ip_host_service_vulns	rna_host_service_vulns，第 6-42 页	5.1.1
rna_ip_host_third_party_vuln	rna_host_third_party_vuln，第 6-43 页	5.1.1
rna_ip_host_third_party_vuln_bugtraq_id	rna_host_third_party_vuln_bugtraq_id，第 6-45 页	5.1.1
rna_ip_host_third_party_vuln_cve_id	rna_host_third_party_vuln_cve_id，第 6-46 页	5.1.1
rna_ip_host_third_party_vuln_rna_id	rna_host_third_party_vuln_rna_id，第 6-48 页	5.1.1
rna_ip_host_user_history	user_ipaddr_history，第 6-55 页	5.1.1
rna_mac_host	rna_host_mac_map，第 6-24 页	5.1.1
rna_mac_host_sensor	rna_host_mac_map，第 6-24 页	5.1.1
rna_mac_ip_map	rna_host_ip_map，第 6-23 页 rna_host_mac_map，第 6-24 页	5.1.1

索 引

英文

D

M

S

Y