



# CHAPTER 6

## Schema: Discovery Event and Network Map Tables

This chapter contains information on the schema and supported joins for tables related to discovery events and the Cisco network map.

Your Firepower System generates discovery events continuously as it monitors the traffic produced by your hosts and network devices.

The network map is a repository of information about the network assets reported in discovery events. For each detected host and network device, the network map contains information such as operating system, servers, client applications, host attributes, vulnerabilities, and so on.

Vulnerabilities are descriptions of specific compromises or exploits to which hosts may be susceptible. Cisco maintains its own vulnerability database (VDB), which cross-references the Bugtraq database and MITRE's CVE database. You can also import third-party vulnerability data using the host input feature.

Note that the information about a given host in the network map can vary according to the type of host and the information available in the monitored traffic.

For more information, see the sections listed in the following table. The Version column indicates the Firepower System versions that support each table. While support for deprecated tables continues in the current product release, Cisco **strongly** recommends avoiding the use of deprecated tables and fields, to ensure continued support in the future.

**Table 6-1** Schema for Discovery Event and Network Map Tables

See...	For the table that stores information on...	Version
<a href="#">application_host_map, page 6-5</a>	Applications detected on the hosts in your monitored network.	5.0+
<a href="#">application_ip_map, page A-1</a>	The category, tags, productivity, and risk associated with an application detected in your monitored network.	5.2+
<a href="#">application_ip_map, page A-1</a>	The category, tags, productivity, and risk associated with an application detected in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">application_ip_map, page A-1</a> .	5.0-5.1.x
<a href="#">application_tag_map, page 6-9</a>	The tags associated with an application detected in your monitored network.	5.0+
<a href="#">domain_control_information, page 6-11</a>	Domain hierarchy information	6.0+
<a href="#">network_discovery_event, page 6-12</a>	Discovery and host input events.	5.0+

Table 6-1 Schema for Discovery Event and Network Map Tables (continued)

See...	For the table that stores information on...	Version
<a href="#">rna_host</a> , page 6-13	Basic information on the hosts in your monitored network.	5.2+
<a href="#">rna_host_attribute</a> , page 6-15	The host attributes associated with each host in your monitored network.	5.2+
<a href="#">rna_host_client_app</a> , page 6-17	The client applications detected on the hosts in your monitored network.	5.2+
<a href="#">rna_host_client_app</a> , page 6-17	The payloads associated with HTTP (web browser) client applications detected on the hosts in your monitored network.	5.2+
<a href="#">rna_host_ioc_state</a> , page 6-22	Stores compromise state for hosts.	5.3+
<a href="#">rna_host_ip_map</a> , page 6-26	Correlates host IDs to MAC addresses for hosts in your monitored network.	5.2+
<a href="#">rna_host_os</a> , page 6-29	The operating systems detected on the hosts in your monitored network.	5.2+
<a href="#">rna_host_os_vulns</a> , page 6-30	The vulnerabilities associated with the hosts in your monitored network.	5.2+
<a href="#">rna_host_protocol</a> , page 6-32	The protocols detected on the hosts in your monitored network.	4.10.x+
<a href="#">rna_host_protocol</a> , page 6-32	The hosts in your monitored network with regard to the managed device that detected them.	5.2+
<a href="#">rna_host_service</a> , page 6-35	The services detected on the hosts in your monitored network.	5.2+
<a href="#">rna_host_service_banner</a> , page 6-37	Headers from network traffic that advertise service vendors and versions (“banners”) for the services detected on hosts in your monitored network.	5.2+
<a href="#">rna_host_service_info</a> , page 6-38	Details of the services detected on the hosts in your monitored network.	5.2+
<a href="#">rna_host_service_payload</a> , page 6-43	The payloads associated with services detected on the hosts in your monitored network.	5.2+
<a href="#">rna_host_service_subtype</a> , page 6-46	The sub-services for the services detected on the hosts in your monitored network.	5.2+
<a href="#">rna_host_service_vulns</a> , page 6-47	The vulnerabilities associated with the services detected on the hosts in your monitored network.	5.2+
<a href="#">rna_host_third_party_vuln</a> , page 6-48	The third-party vulnerabilities associated with the hosts in your monitored network.	5.2+
<a href="#">rna_host_third_party_vuln_bugtraq_id</a> , page 6-50	The third-party vulnerabilities associated with the hosts in your monitored network that are also associated with a vulnerability in the Bugtraq database ( <a href="http://www.securityfocus.com/bid/">http://www.securityfocus.com/bid/</a> ).	5.2+
<a href="#">rna_host_third_party_vuln_cve_id</a> , page 6-51	The third-party vulnerabilities associated with the hosts in your monitored network that are also associated with a vulnerability in MITRE’s CVE database. ( <a href="http://www.cve.mitre.org/">http://www.cve.mitre.org/</a> ).	5.2+

**Table 6-1** Schema for Discovery Event and Network Map Tables (continued)

See...	For the table that stores information on...	Version
<a href="#">rna_host_third_party_vuln_rna_id</a> , page 6-53	The third-party vulnerabilities associated with the hosts in your monitored network that are also associated with a vulnerability in the VDB.	5.2+
<a href="#">rna_ip_host</a> , page A-1	Basic information on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host</a> , page 6-13.	4.10.x-5.1.x
<a href="#">rna_ip_host_client_app</a> , page A-1	The client applications detected on the hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host_client_app</a> , page 6-17.	4.10.x-5.1.x
<a href="#">rna_ip_host_client_app_payload</a> , page A-1	The payloads associated with HTTP (web browser) client applications detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host_client_app</a> , page 6-17.	4.10.x-5.1.x
<a href="#">rna_ip_host_os</a> , page A-1	The operating systems detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host_os</a> , page 6-29.	4.10.x-5.1.x
<a href="#">rna_ip_host_os_vulns</a> , page A-1	The vulnerabilities associated with the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host_os_vulns</a> , page 6-30.	4.10.x--5.1.x
<a href="#">rna_ip_host_sensor</a> , page A-1	The IP hosts in your monitored network with regard to the managed device that detected them. deprecated in Version 5.2. Superseded by <a href="#">rna_host_protocol</a> , page 6-32.	5.0-5.1.x
<a href="#">rna_ip_host_service</a> , page A-1	The services detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host_service</a> , page 6-35.	4.10.x-5.1.x
<a href="#">rna_ip_host_service_banner</a> , page A-1	Headers from network traffic that advertise service vendors and versions (“banners”) for the services detected on hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host_service_banner</a> , page 6-37.	4.10.x-5.1.x
<a href="#">rna_ip_host_service_info</a> , page A-1	Details of the services detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host_service_info</a> , page 6-38.	4.10.x-5.1.x

Table 6-1 Schema for Discovery Event and Network Map Tables (continued)

See...	For the table that stores information on...	Version
<a href="#">rna_ip_host_service_payload</a> , page A-1	The payloads associated with services detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host_service_payload</a> , page 6-43.	4.10.x-5.1.x
<a href="#">rna_ip_host_service_subtype</a> , page A-1	The sub-services for the services detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host_service_subtype</a> , page 6-46.	4.10.x-5.1.x
<a href="#">rna_ip_host_service_vulns</a> , page A-1	The vulnerabilities associated with the services detected on the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host_service_vulns</a> , page 6-47.	4.10.x-5.1.x
<a href="#">rna_ip_host_third_party_vuln</a> , page A-1	The third-party vulnerabilities associated with the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host_third_party_vuln</a> , page 6-48.	4.10.x-5.1.x
<a href="#">rna_ip_host_third_party_vuln_bugtraq_id</a> , page A-1	The third-party vulnerabilities associated with the IP hosts in your monitored network that are also associated with a vulnerability in the Bugtraq database ( <a href="http://www.securityfocus.com/bid/">http://www.securityfocus.com/bid/</a> ). deprecated in Version 5.2. Superseded by <a href="#">rna_host_third_party_vuln_bugtraq_id</a> , page 6-50.	4.10.x-5.1.x
<a href="#">rna_ip_host_third_party_vuln_cve_id</a> , page A-1	The third-party vulnerabilities associated with the IP hosts in your monitored network that are also associated with a vulnerability in MITRE's CVE database. ( <a href="http://www.cve.mitre.org/">http://www.cve.mitre.org/</a> ). deprecated in Version 5.2. Superseded by <a href="#">rna_host_third_party_vuln_cve_id</a> , page 6-51.	4.10.x-5.1.x
<a href="#">rna_ip_host_third_party_vuln_rna_id</a> , page A-1	The third-party vulnerabilities associated with the IP hosts in your monitored network that are also associated with a vulnerability in the VDB. deprecated in Version 5.2. Superseded by <a href="#">rna_host_third_party_vuln_rna_id</a> , page 6-53.	4.10.x-5.1.x
<a href="#">rna_ip_host_user_history</a> , page A-1	User activity for a particular IP host in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">user_ipaddr_history</a> , page 6-60.	4.10.x-5.1.x
<a href="#">rna_mac_host</a> , page A-1	The MAC hosts (hosts without an IP address) in your monitored network.	4.10.x-5.1.x
<a href="#">rna_mac_host_sensor</a> , page A-1	The IP hosts in your monitored network with regard to the managed devices that detected them.	5.0-5.1.x

**Table 6-1** Schema for Discovery Event and Network Map Tables (continued)

See...	For the table that stores information on...	Version
<a href="#">rna_mac_ip_map</a> , page A-2	The MAC addresses of the IP hosts in your monitored network. deprecated in Version 5.2. Superseded by <a href="#">rna_host_ip_map</a> , page 6-26 and <a href="#">rna_host_mac_map</a> , page 6-28.	4.10.x-5.1.x
<a href="#">rna_vuln</a> , page 6-55	The vulnerabilities in the Cisco VDB.	4.10.x+
<a href="#">tag_info</a> , page 6-58	The tags that characterize detected applications.	5.0+
<a href="#">url_categories</a> , page 6-59	The categories that characterize URLs accessed from hosts in your monitored network.	5.0+
<a href="#">url_reputations</a> , page 6-59	The reputations that characterize URLs accessed from hosts in your monitored network.	5.0+
<a href="#">user_ipaddr_history</a> , page 6-60	User activity for a particular host in your monitored network.	5.2+

## application\_host\_map

The `application_host_map` table contains information on the categories and tags associated with each application detected on your network.

For more information, see the following sections:

- [application\\_host\\_map Fields](#), page 6-5
- [application\\_host\\_map Joins](#), page 6-6
- [application\\_host\\_map Sample Query](#), page 6-7

## application\_host\_map Fields

The following table describes the fields you can access in the `application_host_map` table.

**Table 6-2** application\_host\_map Fields

Field	Description
application_id	The internal identification number for the application.
application_name	The application name that appears in the user interface.
application_tag_id	This field has been deprecated and will now return null.
business_relevance	The index (from 1 to 5) of the application's relevance to business productivity, where 1 is very low and 5 is very high.
business_relevance_description	The description of the business relevance (very low, low, medium, high, very high).
host_id	ID number of the host.
risk	An index (from 1 to 5) of the application's risk, where 1 is very low risk and 5 is critical risk.
risk_description	The description of the risk (very low, low, medium, high, critical).

## application\_host\_map Joins

The following table describes the joins you can perform on the `application_host_map` table.

**Table 6-3** application\_host\_map Joins

You can join this table on...	And...
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 Sample Query

The following query returns information about the applications detected on the host with a `host_id` of 8.

```
SELECT host_id, application_id, application_name, business_relevance, risk
FROM application_host_map
```

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

## application\_info

The `application_info` table contains information about the applications that can be detected on the hosts in your monitored network.

You can retrieve the list of tags associated with an application from the `application_tag_map` table by joining on `application_id`. Similarly, you can retrieve an application's list of associated categories from the `application_host_map` by joining on `application_id`.

For more information, see the following sections:

- [application\\_info Fields, page 6-8](#)
- [application\\_info Joins, page 6-9](#)
- [application\\_info Sample Query, page 6-9](#)

## application\_info Fields

The following table describes the fields you can access in the `application_info` table.

**Table 6-4** *application\_info Fields*

Field	Description
<code>application_description</code>	A description of the application.
<code>application_id</code>	The internal identification number for the application.
<code>application_name</code>	The application name that appears in the user interface.
<code>business_relevance</code>	An index (from 1 to 5) of the application's relevance to business productivity, where 1 is very low and 5 is very high.
<code>business_relevance_description</code>	A description of business relevance (very low, low, medium, high, very high).
<code>domain_name</code>	Name of the domain on which the application was detected.
<code>domain_uuid</code>	UUID of the domain on which the application was detected. This is presented in binary.
<code>is_client_application</code>	A true-false flag that indicates if the detected application is a client.
<code>is_server_application</code>	A true-false flag that indicates if the detected application is a server application.
<code>is_web_application</code>	A true-false flag that indicates if the detected application is a web application.
<code>risk</code>	An index (from 1 to 5) of the application's estimated risk where 1 is very low risk and 5 is critical risk.
<code>risk_description</code>	A description of the risk (very low, low, medium, high, and critical).



## application\_info Joins

The following table describes the joins you can perform on the `application_info` table.

**Table 6-5** *application\_info Joins*

You can join this table on...	And...
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 Sample Query

The following query returns the record for the application with a `host_id` of 8 found within the Global \ Company B \ Edge domain.

```
SELECT application_id, application_name, application_description, business_relevance,
risk
FROM application_info
WHERE application_id="8" AND domain_name= "Global \ Company B \ Edge";
```

## application\_tag\_map

The `application_tag_map` table contains information on the tags associated with each application detected on your network.

For more information, see the following sections:

- [application\\_tag\\_map Fields](#), page 6-10
- [application\\_tag\\_map Joins](#), page 6-10
- [application\\_tag\\_map Sample Query](#), page 6-11

## application\_tag\_map Fields

The following table describes the fields you can access in the `application_tag_map` table.

**Table 6-6** *application\_tag\_map Fields*

Field	Description
<code>application_id</code>	The internal identification number for the application.
<code>application_name</code>	The application that appears in the user interface.
<code>domain_name</code>	Name of the domain on which the application was detected.
<code>domain_uuid</code>	UUID of the domain on which the application was detected. This is presented in binary.
<code>tag_id</code>	The internal identification number for the tag.
<code>tag_name</code>	The text of the tag that appears in the user interface.
<code>tag_type</code>	One of the following: <code>category</code> or <code>type</code> .

## application\_tag\_map Joins

The following table describes the joins you can perform on the `application_tag_map` table.

**Table 6-7** *application\_tag\_map Joins*

You can join this table on...	And...
<code>application_id</code>	<code>app_ids_stats_current_timeframe.application_id</code> <code>application_info.application_id</code> <code>application_host_map.application_id</code> <code>app_stats_current_timeframe.application_id</code> <code>connection_log.application_protocol_id</code> <code>connection_log.client_application_id</code> <code>connection_log.web_application_id</code> <code>connection_summary.application_protocol_id</code> <code>file_event.application_id</code> <code>intrusion_event.application_protocol_id</code> <code>intrusion_event.client_application_id</code> <code>intrusion_event.web_application_id</code> <code>rna_host_service_info.application_protocol_id</code> <code>rna_host_client_app_payload.web_application_id</code> <code>rna_host_client_app_payload.client_application_id</code> <code>rna_host_client_app.client_application_id</code> <code>rna_host_client_app.application_protocol_id</code> <code>rna_host_service_payload.web_application_id</code> <code>si_connection_log.application_protocol_name</code> <code>si_connection_log.application_protocol_id</code> <code>si_connection_log.client_application_id</code> <code>si_connection_log.web_application_id</code>
<code>tag_id</code>	<code>tag_info.tag_id</code>

## application\_tag\_map Sample Query

The following query returns all tag records associated with the specified application.

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

## domain\_control\_information

The `domain_control_information` table maps domains to their UUIDs and provides the name and UUID of each domain's parent domain.

For more information, see the following sections:

- [domain\\_control\\_information Fields, page 6-11](#)
- [domain\\_control\\_information Joins, page 6-11](#)
- [domain\\_control\\_information Sample Query, page 6-11](#)

## domain\_control\_information Fields

The following table describes the fields you can access in the `domain_control_information` table.

**Table 6-8** *domain\_control\_information Fields*

Field	Description
domain_name	Name of the domain
domain_uuid	UUID of the domain. This is presented in binary.
parent_domain_name	Name of the parent domain, if applicable.
parent_domain_uuid	UUID of the parent domain, if applicable. This is presented in binary.

## domain\_control\_information Joins

You cannot perform joins on the `domain_control_information` table.

## domain\_control\_information Sample Query

The following query returns all domain names, domain UUIDs in ASCII format, and their parent domains.

```
SELECT domain_name, uuid_btoa(domain_uuid), parent_domain_name
FROM domain_control_information;
```

## network\_discovery\_event

The `network_discovery_event` table contains information on discovery and host input events. The Firepower System generates discovery events when it detects a change on your monitored network, whether by discovering new network features or by detecting changes in previously identified network assets. The Firepower System generates host input events when a user manually modifies the network map by adding, modifying, or deleting network assets.

The `network_discovery_event` table supersedes the deprecated `rna_event` table starting with Version 5.0 of the Firepower System.

For more information, see the following sections:

- [network\\_discovery\\_event Fields, page 6-12](#)
- [network\\_discovery\\_event Joins, page 6-13](#)
- [network\\_discovery\\_event Sample Query, page 6-13](#)

## network\_discovery\_event Fields

The following table describes the fields you can access in the `network_discovery_event` table.

**Table 6-9** *network\_discovery\_event Fields*

Field	Description
<code>confidence</code>	The Firepower System-assigned confidence rating (from 0 to 100) for the identification of the service.
<code>description</code>	The description of the event.
<code>domain_name</code>	Name of the domain on which the event was detected.
<code>domain_uuid</code>	UUID of the domain on which the event was detected. This is presented in binary.
<code>event_id</code>	The internal identification number for the event.
<code>event_time_sec</code>	The UNIX timestamp of the date and time the event was generated.
<code>event_time_usec</code>	The microsecond increment of the event timestamp.
<code>event_type</code>	The event type. For example, <code>New Host Or Identity Conflict</code> .
<code>ip_address</code>	This field has been deprecated and will now return <code>null</code> .
<code>ipaddr</code>	A binary representation of the IPv4 or IPv6 address for the host involved in the event.
<code>mac_address</code>	The MAC address of the host involved in the event.
<code>mac_vendor</code>	The NIC hardware vendor of the host involved in the event.
<code>port</code>	The port used by the network traffic that triggered the event.
<code>sensor_address</code>	The IP address of the managed device that generated the discovery event. Format is <code>ipv4_address</code> , <code>ipv6_address</code> .
<code>sensor_name</code>	The managed device that generated the discovery event.
<code>sensor_uuid</code>	A unique identifier for the managed device, or 0 if <code>sensor_name</code> is <code>null</code> .
<code>user_dept</code>	The department of the user who last logged into the host.
<code>user_email</code>	The email address of the user who last logged into the host.
<code>user_first_name</code>	The first name of the user who last logged into the host.

**Table 6-9** *network\_discovery\_event Fields (continued)*

Field	Description
user_id	The internal identification number for the user who last logged into the host.
user_last_name	The last name of the user who last logged into the host.
user_last_seen_sec	The UNIX timestamp of the date and time the Firepower System last detected user activity for the user who last logged into the host.
user_last_updated_sec	The UNIX timestamp of the date and time the Firepower System last updated the user record for the user who last logged into the host.
user_name	The user name of the user who last logged into the host.
user_phone	The phone number of the user who last logged into the host.

## network\_discovery\_event Joins

The following table describes the joins you can perform using the `network_discovery_event` table.

**Table 6-10** *network\_discovery\_event Joins*

You can join this table on...	And...
ipaddr	<code>rna_host_ip_map.ipaddr</code> <code>user_ipaddr_history.ipaddr</code>

## network\_discovery\_event Sample Query

The following query returns discovery event records that include the user, detecting device name, timestamp, host IP address, and so on within the specified times.

```
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

The `rna_host` table contains basic information on the hosts in your monitored network.

This table supersedes `rna_ip_host` as of Version 5.2.

For more information, see the following sections:

- [rna\\_host Fields, page 6-14](#)
- [rna\\_host Joins, page 6-14](#)
- [rna\\_host Sample Query, page 6-15](#)

## rna\_host Fields

The following table describes the fields you can access in the `rna_host` table.

**Table 6-11** `rna_host` Fields

Field	Description
<code>criticality</code>	The host criticality level: None, Low, Medium, Or High.
<code>domain_name</code>	Name of the domain on which the host was detected.
<code>domain_uuid</code>	UUID of the domain on which the host was detected. This is presented in binary.
<code>hops</code>	The number of network hops from the host to the managed device that detected the host.
<code>host_id</code>	ID number of the host.
<code>host_name</code>	Name of the host.
<code>host_type</code>	The host type: Host, Router, Bridge, NAT Device, Or Load Balancer.
<code>jailbroken</code>	A true-false flag indicating whether a mobile device operating system is jailbroken.
<code>last_seen_sec</code>	The UNIX timestamp of the date and time the system last detected host activity.
<code>mobile</code>	A true-false flag indicating whether the detected host is a mobile device.
<code>netbios_name</code>	The host NetBIOS name string.
<code>notes</code>	The contents of the Notes host attribute for the host.
<code>vlan_id</code>	The VLAN identification number, if applicable.
<code>vlan_priority</code>	The priority value included in the VLAN tag.
<code>vlan_type</code>	The type of encapsulated packet that contains the VLAN tag: <ul style="list-style-type: none"> <li>• 0 — Ethernet</li> <li>• 1 — Token Ring</li> </ul>

## rna\_host Joins

The following table describes the joins you can perform on the `rna_host` table.

Table 6-12 *rna\_host Joins*

You can join this table on...	And...
host_id	<a href="#">application_host_map.host_id</a> <a href="#">rna_host_attribute.host_id</a> <a href="#">rna_host_protocol.host_id</a> <a href="#">rna_host_os_vulns.host_id</a> <a href="#">rna_host_client_app.host_id</a> <a href="#">rna_host_client_app_payload.host_id</a> <a href="#">rna_host_ip_map.host_id</a> <a href="#">rna_host_ioc_state.host_id</a> <a href="#">rna_host_mac_map.host_id</a> <a href="#">rna_host_os.host_id</a> <a href="#">rna_host_sensor.host_id</a> <a href="#">rna_host_service.host_id</a> <a href="#">rna_host_service_banner.host_id</a> <a href="#">rna_host_service_info.host_id</a> <a href="#">rna_host_service_payload.host_id</a> <a href="#">rna_host_service_vulns.host_id</a> <a href="#">rna_host_third_party_vuln_bugtraq_id.host_id</a> <a href="#">rna_host_third_party_vuln_cve_id.host_id</a> <a href="#">rna_host_third_party_vuln_rna_id.host_id</a> <a href="#">rna_host_third_party_vuln.host_id</a>

## rna\_host Sample Query

The following query returns 25 **rna\_host** records that include the host ID, VLAN ID, when the host was last seen, and the type of host, within the Global \ Company B \ Edge domain, ordered by the type of host.

```
SELECT host_id, vlan_id, last_seen_sec, host_type
FROM rna_host
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY host_type
LIMIT 0, 25;
```

## rna\_host\_attribute

The **rna\_host\_attribute** table contains information on the host attributes associated with each host in your monitored network. It supersedes the deprecated **rna\_ip\_host\_attribute** table.

For more information, see the following sections:

- [rna\\_host\\_attribute Fields, page 6-16](#)
- [rna\\_host\\_attribute Joins, page 6-16](#)
- [rna\\_host\\_attribute Sample Query, page 6-16](#)

## rna\_host\_attribute Fields

The following table describes the fields you can access in the `rna_host_attribute` table.

**Table 6-13** *rna\_host\_attribute Fields*

Field	Description
<code>attribute_name</code>	The host attribute. For example, Host Criticality or Default Allow List.
<code>attribute_value</code>	The value of the host attribute.
<code>host_id</code>	ID number of the host.

## rna\_host\_attribute Joins

The following table describes the joins you can perform on the `rna_host_attribute` table.

**Table 6-14** *rna\_host\_attribute Joins*

You can join this table on...	And...
<code>host_id</code>	<code>application_host_map.host_id</code> <code>rna_host.host_id</code> <code>rna_host_protocol.host_id</code> <code>rna_host_os_vulns.host_id</code> <code>rna_host_client_app.host_id</code> <code>rna_host_client_app_payload.host_id</code> <code>rna_host_ioc_state.host_id</code> <code>rna_host_ip_map.host_id</code> <code>rna_host_mac_map.host_id</code> <code>rna_host_os.host_id</code> <code>rna_host_sensor.host_id</code> <code>rna_host_service.host_id</code> <code>rna_host_service_banner.host_id</code> <code>rna_host_service_info.host_id</code> <code>rna_host_service_payload.host_id</code> <code>rna_host_service_vulns.host_id</code> <code>rna_host_third_party_vuln_bugtraq_id.host_id</code> <code>rna_host_third_party_vuln_cve_id.host_id</code> <code>rna_host_third_party_vuln_rna_id.host_id</code> <code>rna_host_third_party_vuln.host_id</code>

## rna\_host\_attribute Sample Query

The following query returns all host attributes and values associated with the selected host ID.

```
SELECT attribute_name, attribute_value
FROM rna_host_attribute
WHERE HEX(host_id) = "00000000000000000000000000000008";
```



## rna\_host\_client\_app

The `rna_host_client_app` table contains information on the client applications detected on the hosts in your monitored network. It supersedes the deprecated `rna_ip_host_client_app` table.

For more information, see the following sections:

- [rna\\_host\\_client\\_app Fields, page 6-17](#)
- [rna\\_host\\_client\\_app Joins, page 6-17](#)
- [rna\\_host\\_client\\_app Sample Query, page 6-19](#)

## rna\_host\_client\_app Fields

The following table describes the fields you can access in the `rna_host_client_app` table.

**Table 6-15** *rna\_host\_client\_app Fields*

Field	Description
<code>application</code>	Field deprecated in Version 5.0. Returns <code>null</code> for all queries.
<code>application_protocol_id</code>	An internal identifier for the detected application protocol.
<code>application_protocol_name</code>	One of: <ul style="list-style-type: none"> <li>• the name of the application, if a positive identification can be made</li> <li>• <code>pending</code> if the system requires more data</li> <li>• blank if there is no application information in the connection</li> </ul>
<code>application_type</code>	Field deprecated in Version 5.0. Returns <code>null</code> for all queries.
<code>client_application_id</code>	The internal identification number for the application, if the application is identifiable.
<code>client_application_name</code>	One of: <ul style="list-style-type: none"> <li>• the name of the application, if a positive identification can be made.</li> <li>• a generic client name if the system detects a client application but cannot identify a specific one.</li> <li>• blank if there is no client application information in the connection.</li> </ul>
<code>hits</code>	The number of times the client application was detected.
<code>host_id</code>	ID number of the host.
<code>last_used_sec</code>	The UNIX timestamp of the date and time the system last detected application activity.
<code>version</code>	The version of the application detected on the host.

## rna\_host\_client\_app Joins

The following table describes the joins you can perform on the `rna_host_client_app` table.

**Table 6-16** *rna\_host\_client\_app Joins*

You can join this table on...	And...
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

Table 6-16 rna\_host\_client\_app Joins (continued)

You can join this table on...	And...
host_id and application_protocol_id and client_application_id and version	the set of: 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
application_protocol_id or 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 Sample Query

The following query returns information about the client applications detected on the host with `host_id` of 8.

```
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

The `rna_host_client_app_payload` table contains information on the payloads in HTTP traffic associated with web applications on hosts detected in your monitored network.

For more information, see the following sections:

- [rna\\_host\\_client\\_app\\_payload Fields, page 6-20](#)
- [rna\\_host\\_client\\_app\\_payload Joins, page 6-21](#)
- [rna\\_host\\_client\\_app\\_payload Sample Query, page 6-22](#)

## rna\_host\_client\_app\_payload Fields

The following table describes the fields you can access in the `rna_host_client_app_payload` table.

**Table 6-17** *rna\_host\_client\_app\_payload Fields*

Field	Description
<code>application</code>	Field deprecated in Version 5.0. Returns <code>null</code> for all queries.
<code>application_protocol_id</code>	An internal identifier for the detected application protocol, if available. For traffic that has characteristics of both client applications and web applications, the <code>client_application_id</code> and <code>web_application_id</code> fields have the same value.
<code>application_protocol_name</code>	One of: <ul style="list-style-type: none"> <li>• the name of the application, if a positive identification can be made</li> <li>• <code>pending</code> if the system requires more data</li> <li>• blank if there is no application information in the connection</li> </ul>
<code>application_type</code>	Field deprecated in Version 5.0. Returns <code>null</code> for all queries.
<code>client_application_id</code>	The internal identification number for the client application.
<code>client_application_name</code>	One of: <ul style="list-style-type: none"> <li>• the name of the application, if a positive identification can be made.</li> <li>• a generic client name if the system detects a client application but cannot identify a specific one.</li> <li>• blank if there is no client application information in the connection.</li> </ul>
<code>host_id</code>	ID number of the host.
<code>payload_name</code>	Field deprecated in Version 5.0. Returns <code>null</code> for all queries.
<code>payload_type</code>	Field deprecated in Version 5.0. Returns <code>null</code> for all queries.
<code>version</code>	The version of the web application detected on the host.
<code>web_application_id</code>	The internal identification number for the web application, if available. For traffic that has characteristics of both client applications and web applications, the <code>client_application_id</code> and <code>web_application_id</code> fields have the same value.
<code>web_application_name</code>	One of: <ul style="list-style-type: none"> <li>• the name of the application, if a positive identification can be made.</li> <li>• <code>web browsing</code> if the system detects an application protocol of HTTP but cannot identify a specific web application.</li> <li>• blank if the connection has no HTTP traffic.</li> </ul>

## rna\_host\_client\_app\_payload Joins

The following table describes the joins you can perform on the `rna_host_client_app_payload` table.

**Table 6-18** *rna\_host\_client\_app\_payload Joins*

You can join this table on...	And...
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

**Table 6-18** *rna\_host\_client\_app\_payload Joins (continued)*

You can join this table on...	And...
the set of: host_id, application_protocol_id, client_application_id, version	the set of: 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
client_application_id or 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 Sample Query

The following query returns information about the web applications detected on the host with `host_id` of 8.

```
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

The `rna_host_ioc_state` table stores the IOC state for hosts in your monitored network.

For more information, see the following sections:

- [rna\\_host\\_ioc\\_state Fields, page 6-23](#)
- [rna\\_host\\_ioc\\_state Joins, page 6-25](#)
- [rna\\_host\\_ioc\\_state Sample Query, page 6-25](#)

## rna\_host\_ioc\_state Fields

The following table describes the fields you can access in the `rna_host_ioc_state` table.

**Table 6-19** *rna\_host\_ioc\_state Fields*

Field	Description
<code>first_seen</code>	Unix timestamp when the compromise was first detected.
<code>first_seen_sensor_address</code>	The IP address of the managed device that first detected the compromise. Format is <i>ipv4_address, ipv6_address</i> .
<code>first_seen_sensor_name</code>	The managed device that first detected the compromise.
<code>host_id</code>	ID number of the host.
<code>ioc_category</code>	The category for the compromise. Possible values include: <ul style="list-style-type: none"> <li>• CnC Connected</li> <li>• Exploit Kit</li> <li>• High Impact Attack</li> <li>• Low Impact Attack</li> <li>• Malware Detected</li> <li>• Malware Executed</li> <li>• Dropper Infection</li> <li>• Java Compromise</li> <li>• Word Compromise</li> <li>• Adobe Reader Compromise</li> <li>• Excel Compromise</li> <li>• PowerPoint Compromise</li> <li>• QuickTime Compromise</li> </ul>
<code>ioc_description</code>	Description of the compromise.

Table 6-19 rna\_host\_ioc\_state Fields (continued)

Field	Description
ioc_event_type	<p>The event type for the compromise. Possible values include:</p> <ul style="list-style-type: none"> <li>• Adobe Reader launched shell</li> <li>• Dropper Infection Detected by AMP for Endpoints</li> <li>• Excel Compromise Detected by AMP for Endpoints</li> <li>• Excel launched shell</li> <li>• Impact 1 Intrusion Event – attempted-admin</li> <li>• Impact 1 Intrusion Event – attempted-user</li> <li>• Impact 1 Intrusion Event – successful-admin</li> <li>• Impact 1 Intrusion Event – successful-user</li> <li>• Impact 1 Intrusion Event – web-application-attack</li> <li>• Impact 2 Intrusion Event – attempted-admin</li> <li>• Impact 2 Intrusion Event – attempted-user</li> <li>• Impact 2 Intrusion Event – successful-admin</li> <li>• Impact 2 Intrusion Event – successful-user</li> <li>• Impact 2 Intrusion Event – web-application-attack</li> <li>• Intrusion Event – exploit-kit</li> <li>• Intrusion Event – malware-backdoor</li> <li>• Intrusion Event – malware-CnC</li> <li>• Java Compromise Detected by AMP for Endpoints</li> <li>• Java launched shell</li> <li>• PDF Compromise Detected by AMP for Endpoints</li> <li>• PowerPoint Compromise Detected by AMP for Endpoints</li> <li>• PowerPoint launched shell</li> <li>• QuickTime Compromise Detected by AMP for Endpoints</li> <li>• QuickTime launched shell</li> <li>• Security Intelligence Event – CnC</li> <li>• Suspected Botnet Detected by AMP for Endpoints</li> <li>• Threat Detected by AMP for Endpoints – Subtype is 'executed'</li> <li>• Threat Detected by AMP for Endpoints – Subtype is not 'executed'</li> <li>• Threat Detected in File Transfer – Action is not 'block'</li> <li>• Word Compromise Detected by AMP for Endpoints</li> <li>• Word launched shell</li> </ul>
ioc_id	Unique ID number for the compromise.
is_disabled	Whether this compromise has been disabled.
last_seen	Unix timestamp when this compromise was last detected.



**Table 6-19** *rna\_host\_ioc\_state Fields (continued)*

Field	Description
last_seen_sensor_address	The IP address of the managed device that last detected the compromise. Format is <i>ipv4_address, ipv6_address</i> .
last_seen_sensor_name	The managed device that last detected the compromise.

## rna\_host\_ioc\_state Joins

The following table describes the joins you can perform on the `rna_host_ioc_state` table.

**Table 6-20** *rna\_host\_ioc\_state Joins*

You can join this table on...	And...
host_id	<code>rna_host.host_id</code> <code>rna_host_attribute.host_id</code> <code>rna_host_protocol.host_id</code> <code>rna_host_os_vulns.host_id</code> <code>application_host_map.host_id</code> <code>rna_host_client_app.host_id</code> <code>rna_host_client_app_payload.host_id</code> <code>rna_host_ip_map.host_id</code> <code>rna_host_mac_map.host_id</code> <code>rna_host_os.host_id</code> <code>rna_host_sensor.host_id</code> <code>rna_host_service.host_id</code> <code>rna_host_service_banner.host_id</code> <code>rna_host_service_info.host_id</code> <code>rna_host_service_payload.host_id</code> <code>rna_host_service_vulns.host_id</code> <code>rna_host_third_party_vuln_bugtraq_id.host_id</code> <code>rna_host_third_party_vuln_cve_id.host_id</code> <code>rna_host_third_party_vuln_rna_id.host_id</code> <code>rna_host_third_party_vuln.host_id</code>

## rna\_host\_ioc\_state Sample Query

The following query returns up to 25 hosts with their ioc within a specified timespan.

```

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

The `rna_host_ip_map` table correlates host IDs to IP addresses for hosts in your monitored network.

For more information, see the following sections:

- [rna\\_host\\_ip\\_map Fields, page 6-26](#)
- [rna\\_host\\_ip\\_map Joins, page 6-26](#)
- [rna\\_host\\_ip\\_map Sample Query, page 6-27](#)

## rna\_host\_ip\_map Fields

The following table describes the fields you can access in the `rna_host_ip_map` table.

**Table 6-21** *rna\_host\_ip\_map Fields*

Field	Description
host_id	ID number of the host.
ipaddr	A binary representation of the IP address of the host.

## rna\_host\_ip\_map Joins

The following table describes the joins you can perform on the `rna_host_ip_map` table.

**Table 6-22** *rna\_host\_ip\_map Joins*

You can join this table on...	And...
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
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 Sample Query

The following query returns MAC information for the selected host.

```
SELECT host_id
FROM rna_host_ip_map
WHERE HEX(ipaddr) = "000000000000000000000000FFFF0A0A0A04";
```

## rna\_host\_mac\_map

The `rna_host_mac_map` table correlates host IDs to MAC addresses for hosts in your monitored network.

For more information, see the following sections:

- [rna\\_host\\_mac\\_map Fields](#), page 6-28
- [rna\\_host\\_mac\\_map Joins](#), page 6-28
- [rna\\_host\\_mac\\_map Sample Query](#), page 6-29

## rna\_host\_mac\_map Fields

The following table describes the fields you can access in the `rna_host_mac_map` table.

**Table 6-23** *rna\_host\_mac\_map Fields*

Field	Description
host_id	ID number of the host.
mac_address	The host's MAC address.
mac_vendor	Vendor of the network interface of the detected host.

## rna\_host\_mac\_map Joins

The following table describes the joins you can perform on the `rna_host_mac_map` table.

**Table 6-24** *rna\_host\_mac\_map Joins*

You can join this table on...	And...
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 Sample Query

The following query returns MAC information for the host with `host_id` of 8.

```
SELECT HEX(mac_address)
FROM rna_host_mac_map
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

## rna\_host\_os

The `rna_host_os` table contains information on the operating systems detected on the hosts in your monitored network.

For more information, see the following sections:

- [rna\\_host\\_os Fields, page 6-29](#)
- [rna\\_host\\_os Joins, page 6-30](#)
- [rna\\_host\\_os Sample Query, page 6-30](#)

## rna\_host\_os Fields

The following table describes the fields you can access in the `rna_host_os` table.

**Table 6-25** *rna\_host\_os Fields*

Field	Description
<code>confidence</code>	The Firepower System-assigned confidence rating (from 0 to 100) for the identification of the operating system.
<code>created_sec</code>	The UNIX timestamp of the date and time the system first detected host activity.
<code>host_id</code>	ID number of the host.
<code>last_seen_sec</code>	The UNIX timestamp of the date and time the system last detected host activity.
<code>os_uuid</code>	A unique identifier for the operating system detected on the host. The UUID maps to the operating system name, vendor, and version in the Firepower System database.
<code>product</code>	The operating system detected on the host.
<code>source_type</code>	The source of the host's operating system identity: <ul style="list-style-type: none"> <li>• <code>User</code> — Name of the user who entered the data via the web user interface</li> <li>• <code>Application</code> — Imported from another application via the host input feature</li> <li>• <code>Scanner</code> — Either Nmap or another scanner added through system policy</li> <li>• <code>rna</code> — Detected by the Firepower System, either by a discovery event, port match, or pattern match</li> <li>• <code>NetFlow</code> — The data was exported by a NetFlow-enabled device</li> </ul>
<code>vendor</code>	The vendor of the operating system detected on the host.
<code>version</code>	The version of the operating system detected on the host.

## rna\_host\_os Joins

The following table describes the joins you can perform on the `rna_host_os` table.

**Table 6-26** *rna\_host\_os Joins*

You can join this table on...	And...
host_id	<a href="#">rna_host.host_id</a> <a href="#">rna_host_attribute.host_id</a> <a href="#">rna_host_protocol.host_id</a> <a href="#">application_host_map.host_id</a> <a href="#">rna_host_client_app.host_id</a> <a href="#">rna_host_client_app_payload.host_id</a> <a href="#">rna_host_ioc_state.host_id</a> <a href="#">rna_host_ip_map.host_id</a> <a href="#">rna_host_mac_map.host_id</a> <a href="#">rna_host_sensor.host_id</a> <a href="#">rna_host_service.host_id</a> <a href="#">rna_host_service_banner.host_id</a> <a href="#">rna_host_service_info.host_id</a> <a href="#">rna_host_service_payload.host_id</a> <a href="#">rna_host_service_vulns.host_id</a> <a href="#">rna_host_third_party_vuln_bugtraq_id.host_id</a> <a href="#">rna_host_third_party_vuln_cve_id.host_id</a> <a href="#">rna_host_third_party_vuln_rna_id.host_id</a> <a href="#">rna_host_third_party_vuln.host_id</a>

## rna\_host\_os Sample Query

The following query returns operating system information for the host with `host_id` of 8.

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

## rna\_host\_os\_vulns

The `rna_host_os_vulns` table contains information on the vulnerabilities associated with the hosts in your monitored network.

For more information, see the following sections:

- [rna\\_host\\_os\\_vulns Fields](#), page 6-31
- [rna\\_host\\_os\\_vulns Joins](#), page 6-31
- [rna\\_host\\_os\\_vulns Sample Query](#), page 6-31

## rna\_host\_os\_vulns Fields

The following table describes the fields you can access in the `rna_host_os_vulns` table.

**Table 6-27** *rna\_host\_os\_vulns Fields*

Field	Description
<code>host_id</code>	ID number of the host.
<code>invalid</code>	A value indicating whether the vulnerability is valid for the host: <ul style="list-style-type: none"> <li>• 0 — Vulnerability is valid</li> <li>• 1 — Vulnerability is invalid</li> </ul>
<code>rna_vuln_id</code>	An internal identification number for the vulnerability.

## rna\_host\_os\_vulns Joins

The following table describes the joins you can perform on the `rna_host_os_vulns` table.

**Table 6-28** *rna\_host\_os\_vulns Joins*

You can join this table on...	And...
<code>rna_vuln_id</code>	<code>rna_vuln.bugtraq_id</code> <code>rna_vuln.rna_vuln_id</code> <code>rna_host_third_party_vuln_rna_id.rna_vuln_id</code> <code>rna_host_third_party_vuln_cve_id.cve_id</code> <code>rna_host_third_party_vuln_bugtraq_id.bugtraq_id</code>
<code>host_id</code>	<code>rna_host.host_id</code> <code>rna_host_attribute.host_id</code> <code>rna_host_protocol.host_id</code> <code>application_host_map.host_id</code> <code>rna_host_client_app.host_id</code> <code>rna_host_client_app_payload.host_id</code> <code>rna_host_ioc_state.host_id</code> <code>rna_host_ip_map.host_id</code> <code>rna_host_mac_map.host_id</code> <code>rna_host_sensor.host_id</code> <code>rna_host_service.host_id</code> <code>rna_host_service_banner.host_id</code> <code>rna_host_service_info.host_id</code> <code>rna_host_service_payload.host_id</code> <code>rna_host_third_party_vuln_bugtraq_id.host_id</code> <code>rna_host_third_party_vuln_cve_id.host_id</code> <code>rna_host_third_party_vuln_rna_id.host_id</code> <code>rna_host_third_party_vuln.host_id</code>

## rna\_host\_os\_vulns Sample Query

The following query returns the operating system vulnerabilities for the host with `host_id` of 8.

```

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

```

## rna\_host\_protocol

The `rna_host_protocol` table contains information on the protocols detected on the hosts in your monitored network.

For more information, see the following sections:

- [rna\\_host\\_protocol Fields, page 6-32](#)
- [rna\\_host\\_protocol Joins, page 6-32](#)
- [rna\\_host\\_protocol Sample Query, page 6-33](#)

## rna\_host\_protocol Fields

The following table describes the fields you can access in the `rna_host_protocol` table.

**Table 6-29** *rna\_host\_protocol Fields*

Field	Description
host_id	ID number of the host.
ip_address	Field deprecated in Version 5.2. Returns null for all queries.
layer	The network layer where the protocol is running: Network or Transport.
mac_address	Field deprecated in Version 5.2. Returns null for all queries.
mac_vendor	Field deprecated in Version 5.2. Returns null for all queries.
protocol_name	The traffic protocol used by the host.
protocol_num	The IANA-specified protocol number for the protocol.

## rna\_host\_protocol Joins

The following table describes the joins you can perform on the `rna_host_protocol` table.



Table 6-30 *rna\_host\_protocol Joins*

You can join this table on...	And...
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 Sample Query

The following query returns all protocol records for the host with `host_id` of 8.

```
SELECT protocol_num, protocol_name
FROM rna_host_protocol
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

## rna\_host\_sensor

The `rna_host_sensor` table lists the host IP addresses in your monitored network and indicates the managed device that detected each one.

The `rna_host_sensor` table supersedes the deprecated `rna_ip_host_sensor` table starting with Version 5.2 of the Firepower System.

For more information, see the following sections:

- [rna\\_host\\_sensor Fields, page 6-33](#)
- [rna\\_host\\_sensor Joins, page 6-34](#)
- [rna\\_host\\_sensor Sample Query, page 6-34](#)

## rna\_host\_sensor Fields

The following table describes the fields you can access in the `rna_host_sensor` table.

**Table 6-31** *rna\_host\_sensor Fields*

Field	Description
host_id	ID number of the host.
sensor_address	The IP address of the managed device that generated the discovery event. Format is <i>ipv4_address, ipv6_address</i> .
sensor_name	The name of the managed device.
sensor_uuid	A unique identifier for the managed device, or 0 if <i>sensor_name</i> is null.

## rna\_host\_sensor Joins

The following table describes the joins you can perform on the **rna\_host\_sensor** table.

**Table 6-32** *rna\_host\_sensor Joins*

You can join this table on...	And...
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 Sample Query

The following query returns up to 25 hosts, and the sensor that detected them, from the **rna\_host\_sensor** table.

```
SELECT host_id, sensor_address, sensor_name
FROM rna_host_sensor
LIMIT 0, 25;
```

## rna\_host\_service

The `rna_host_service` table contains general information about the servers detected on the hosts in your managed network through network port and traffic protocol combinations.

For more information, see the following sections:

- [rna\\_host\\_service Fields, page 6-35](#)
- [rna\\_host\\_service Joins, page 6-35](#)
- [rna\\_host\\_service Sample Query, page 6-36](#)

## rna\_host\_service Fields

The following table describes the fields you can access in the `rna_host_service` table.

**Table 6-33** *rna\_host\_service Fields*

Field	Description
<code>confidence</code>	The Firepower System-assigned confidence rating (from 0 to 100) for the identification of the server.
<code>hits</code>	The number of times the server was detected.
<code>host_id</code>	ID number of the host.
<code>last_used_sec</code>	UNIX timestamp of the date and time the system last detected server activity.
<code>port</code>	The port used by the server.
<code>protocol</code>	The traffic protocol: TCP or UDP.

## rna\_host\_service Joins

The following table describes the joins you can perform on the `rna_host_service` table.

**Table 6-34** rna\_host\_service Joins

You can join this table on...	And...
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
The set of: host_id port protocol	The set of: rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol  The set of: rna_host_service_info.host_id rna_host_service_info.port rna_host_service_info.protocol  The set of: rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol

## rna\_host\_service Sample Query

The following query returns the first 25 detected server records for the host with host\_id of 8:

```
SELECT hits, protocol, port, confidence
FROM rna_host_service
WHERE HEX(host_id) = "00000000000000000000000000000008"
LIMIT 0, 25;
```

## rna\_host\_service\_banner

The `rna_ip_host_service_banner` table contains header information from network traffic that advertises vendors and versions (“banners”) for the servers on hosts in your monitored network. Keep in mind that the Firepower System does not store server banners unless you enable the **Capture Banners** option in the your network discovery policy.

For more information, see the following sections:

- [rna\\_host\\_service\\_banner Fields, page 6-37](#)
- [rna\\_host\\_service\\_banner Joins, page 6-37](#)
- [rna\\_host\\_service\\_banner Sample Query, page 6-38](#)

## rna\_host\_service\_banner Fields

The following table describes the fields you can access in the `rna_host_service_banner` table.

**Table 6-35** *rna\_host\_service\_banner Fields*

Field	Description
banner	The server banner, that is, the first 256 bytes of the first packet detected for the server.
host_id	ID number of the host.
port	The port used by the server.
protocol	The traffic protocol: TCP or UDP.

## rna\_host\_service\_banner Joins

The following table describes the joins you can perform on the `rna_host_service_banner` table.

**Table 6-36** *rna\_host\_service\_banner Joins*

You can join this table on...	And...
The set of: host_id port protocol	The set of: rna_host_service.host_id rna_host_service.port rna_host_service.protocol  The set of: rna_host_service_info.host_id rna_host_service_info.port rna_host_service_info.protocol  The set of: rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.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_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 Sample Query

The following query returns the server banner for the host with `host_id` of 8.

```
SELECT port, protocol, banner
FROM rna_host_service_banner
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

## rna\_host\_service\_info

The `rna_host_service_info` table contains detailed information about the servers detected on the hosts in your monitored network.

For more information, see the following sections:

- [rna\\_host\\_service\\_info Fields, page 6-39](#)
- [rna\\_host\\_service\\_info Joins, page 6-40](#)
- [rna\\_host\\_service\\_info Sample Query, page 6-42](#)

## rna\_host\_service\_info Fields

The following table describes the fields you can access in the `rna_host_service_info` table.

**Table 6-37** *rna\_host\_service\_info Fields*

Field	Description
<code>application_id</code>	Field deprecated in Version 5.0. Returns blank for all queries.
<code>application_protocol_id</code>	An internal identifier for the detected application protocol, if available.
<code>application_protocol_name</code>	One of: <ul style="list-style-type: none"> <li>• the name of the application protocol, if a positive identification can be made</li> <li>• pending if the system requires more data</li> <li>• blank if there is no application information in the connection</li> </ul>
<code>business_relevance</code>	An index (from 1 to 5) of the application's relevance to business productivity where 1 is very low and 5 is very high.
<code>business_relevance_description</code>	A description of business relevance (very low, low, medium, high, very high).
<code>created_sec</code>	The UNIX timestamp of the date and time the system first detected the application protocol.
<code>host_id</code>	ID number of the host.
<code>ip_address</code>	Field deprecated in Version 5.2. Returns null for all queries.
<code>last_used_sec</code>	The UNIX timestamp of the date and time the system last detected server activity.
<code>port</code>	The port used by the server.
<code>protocol</code>	The traffic protocol: TCP or UDP.
<code>risk</code>	An index (from 1 to 5) of the application's risk where 1 is very low risk and 5 is very high risk.
<code>risk_description</code>	A description of the risk (very low, low, medium, high, very high).
<code>service_info_id</code>	An internal identification number for the server.
<code>service_name</code>	Field deprecated in Version 5.0. Returns null for all queries.

**Table 6-37** *rna\_host\_service\_info Fields (continued)*

Field	Description
source_type	<p>The source of the identity of the server:</p> <ul style="list-style-type: none"> <li>• <code>User</code> — Name of the user who entered the data via the web user interface</li> <li>• <code>Application</code> — Imported from another application via the host input feature</li> <li>• <code>Scanner</code> — Added through NMAP or imported via the host input feature with a source type of Scanner</li> <li>• <code>rna</code> — Detected by the Firepower System, either by a discovery event, port match, or pattern match</li> <li>• <code>NetFlow</code> — The data was exported by a NetFlow-enabled device</li> </ul>
vendor	The vendor of the server on the host.
version	The version of the server detected on the host.

## rna\_host\_service\_info Joins

The following table describes the joins you can perform on the `rna_host_service_info` table.



**Table 6-38** *rna\_host\_service\_info Joins*

You can join this table on...	And...
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

**Table 6-38** rna\_host\_service\_info Joins (continued)

You can join this table on...	And...
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
The set of: host_id and port and protocol	The set of: rna_host_service.host_id rna_host_service.port rna_host_service.protocol  The set of: rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol  The set of: rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol

## rna\_host\_service\_info Sample Query

The following query returns information about the application protocols detected on the host with host\_id of 8.

```
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

The `rna_host_service_payload` table contains information on the web applications associated by the hosts in your monitored network.

For more information, see the following sections:

- [rna\\_host\\_service\\_payload Fields, page 6-43](#)
- [rna\\_host\\_service\\_payload Joins, page 6-43](#)
- [rna\\_host\\_service\\_payload Sample Query, page 6-45](#)

## rna\_host\_service\_payload Fields

The following table describes the fields you can access in the `rna_host_service_payload` table.

**Table 6-39** *rna\_host\_service\_payload Fields*

Field	Description
<code>application_id</code>	Field deprecated in Version 5.0. Returns null for all queries.
<code>application_name</code>	Field deprecated in Version 5.0. Returns null for all queries.
<code>host_id</code>	ID number of the host.
<code>ip_address</code>	Field deprecated in Version 5.2. Returns null for all queries.
<code>payload_name</code>	Field deprecated in Version 5.0. Returns null for all queries.
<code>payload_type</code>	Field deprecated in Version 5.0. Returns null for all queries.
<code>port</code>	The port used by the server.
<code>protocol</code>	The traffic protocol: TCP or UDP.
<code>web_application_id</code>	The internal identification number for the web application.
<code>web_application_name</code>	One of: <ul style="list-style-type: none"> <li>• the name of the web application, if a positive identification can be made</li> <li>• <code>web browsing</code> if the system detects an application protocol of HTTP but cannot identify a specific web application</li> <li>• blank if the connection has no HTTP traffic</li> </ul>

## rna\_host\_service\_payload Joins

The following table describes the joins you can perform on the `rna_host_service_payload` table.

**Table 6-40** *rna\_host\_service\_payload Joins*

You can join this table on...	And...
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

Table 6-40 rna\_host\_service\_payload Joins (continued)

You can join this table on...	And...
The set of: host_id port protocol	The set of: rna_host_service.host_id rna_host_service.port rna_host_service.protocol  The set of: rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol  The set of: 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 Sample Query

The following query returns information about the web applications detected on the host with `host_id` of 8.

```
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

The `rna_host_service_subtype` table contains information on the sub-servers for a server detected on the hosts in your monitored network.

For more information, see the following sections:

- [rna\\_host\\_service\\_subtype Fields, page 6-46](#)
- [rna\\_host\\_service\\_subtype Joins, page 6-46](#)
- [rna\\_host\\_service\\_subtype Sample Query, page 6-47](#)

## rna\_host\_service\_subtype Fields

The following table describes the fields you can access in the `rna_host_service_subtype` table.

**Table 6-41** *rna\_host\_service\_subtype Fields*

Field	Description
host_id	ID number of the host.
port	The port used by the server.
protocol	The traffic protocol: TCP or UDP.
service_name	One of: <ul style="list-style-type: none"> <li>• the server on the host that is associated with the triggering event</li> <li>• none or blank if data for an identification is unavailable</li> <li>• pending if additional data is required</li> <li>• unknown if the system cannot identify the server based on known server fingerprints</li> </ul>
source_type	The source of the identity of the server: <ul style="list-style-type: none"> <li>• User - name of the user who entered the data via the web user interface</li> <li>• Application - imported from another application via the host input feature</li> <li>• Scanner - added through NMAP or imported via the host input feature with a source type of Scanner</li> <li>• rna - detected by the Firepower System, either by a discovery event, port match, or pattern match</li> <li>• NetFlow - the data was exported by a NetFlow-enabled device</li> </ul>
sub_service_name	The sub-server detected on the host.
sub_service_vendor	The vendor of the sub-server detected on the host.
sub_service_version	The version of the sub-server detected on the host.
vendor	The vendor of the server detected on the host.
version	The version of the server detected on the host.

## rna\_host\_service\_subtype Joins

You cannot perform joins on the `rna_host_service_subtype` table.

## rna\_host\_service\_subtype Sample Query

The following query returns all detected sub-server records for the host with `host_id` of 8.

```
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

The `rna_host_service_vulns` table contains information on the vulnerabilities mapped to the servers detected on the hosts in your monitored network.

For more information, see the following sections:

- [rna\\_host\\_service\\_vulns Fields, page 6-47](#)
- [rna\\_host\\_service\\_vulns Joins, page 6-48](#)
- [rna\\_host\\_service\\_vulns Sample Query, page 6-48](#)

## rna\_host\_service\_vulns Fields

The following table describes the fields you can access in the `rna_host_service_vulns` table.

**Table 6-42** *rna\_host\_service\_vulns Fields*

Field	Description
<code>application_id</code>	An internal identification number for the application protocol running on the host.
<code>application_name</code>	The application protocol name that appears in the user interface.
<code>host_id</code>	ID number of the host.
<code>invalid</code>	A value indicating whether the vulnerability is valid for the host running the application protocol: <ul style="list-style-type: none"> <li>• 0 — Vulnerability is valid</li> <li>• 1 — Vulnerability is invalid</li> </ul>
<code>ip_address</code>	Field deprecated in Version 5.2. Returns <code>null</code> for all queries.
<code>port</code>	The port used by the server.
<code>protocol</code>	The traffic protocol: TCP or UDP.
<code>rna_vuln_id</code>	An internal identification number for the vulnerability.
<code>service_name</code>	Field deprecated in Version 5.0. Returns <code>null</code> for all queries.
<code>vendor</code>	The vendor of the server detected on the host.
<code>version</code>	The version of the server detected on the host.

## rna\_host\_service\_vulns Joins

The following table describes the joins you can perform on the `rna_host_service_vulns` table.

**Table 6-43** *rna\_host\_service\_vulns Joins*

You can join this table on...	And...
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 Sample Query

The following query returns information about all server vulnerabilities for the host with `host_id` of 8.

```
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

The `rna_host_third_party_vuln` table contains information on the third-party vulnerabilities associated with the hosts in your monitored network. Note that the information in this table is determined by the third-party vulnerability data imported via the host input feature.

For more information, see the following sections:

- [rna\\_host\\_third\\_party\\_vuln Fields, page 6-49](#)
- [rna\\_host\\_third\\_party\\_vuln Joins, page 6-49](#)



- [rna\\_host\\_third\\_party\\_vuln Sample Query, page 6-50](#)

## rna\_host\_third\_party\_vuln Fields

The following table describes the fields you can access in the `rna_host_third_party_vuln` table.

**Table 6-44** *rna\_host\_third\_party\_vuln Fields*

Field	Description
<code>description</code>	A description of the vulnerability.
<code>host_id</code>	ID number of the host.
<code>invalid</code>	A value indicating whether the vulnerability is valid for the host: <ul style="list-style-type: none"> <li>• 0 — Vulnerability is valid</li> <li>• 1 — Vulnerability is invalid</li> </ul>
<code>name</code>	The title of the vulnerability.
<code>port</code>	A port number, if the vulnerability is associated with a server or related application detected on a specific port.
<code>protocol</code>	The traffic protocol (TCP or UDP), if the vulnerability is associated with an application using that protocol.
<code>source</code>	The source of the vulnerability.
<code>third_party_vuln_id</code>	An identification number associated with the vulnerability.

## rna\_host\_third\_party\_vuln Joins

The following table describes the joins you can perform on the `rna_host_third_party_vuln` table.

**Table 6-45** *rna\_host\_third\_party\_vuln Joins*

You can join this table on...	And...
<code>host_id</code>	<code>rna_host.host_id</code> <code>rna_host_attribute.host_id</code> <code>rna_host_protocol.host_id</code> <code>rna_host_os_vulns.host_id</code> <code>application_host_map.host_id</code> <code>rna_host_client_app.host_id</code> <code>rna_host_client_app_payload.host_id</code> <code>rna_host_ioc_state.host_id</code> <code>rna_host_ip_map.host_id</code> <code>rna_host_mac_map.host_id</code> <code>rna_host_os.host_id</code> <code>rna_host_sensor.host_id</code> <code>rna_host_service.host_id</code> <code>rna_host_service_banner.host_id</code> <code>rna_host_service_info.host_id</code> <code>rna_host_service_payload.host_id</code> <code>rna_host_service_vulns.host_id</code>

## rna\_host\_third\_party\_vuln Sample Query

The following query returns information about the third party vulnerabilities for host with `host_id` of 8.

```
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

The `rna_host_third_party_vuln_bugtraq_id` table contains information on the third-party vulnerabilities that are mapped to vulnerabilities in the Bugtraq database and also associated with hosts in your monitored network. Note that the third-party vulnerability data in this table is imported via the host input feature.

For more information, see the following sections:

- [rna\\_host\\_third\\_party\\_vuln\\_bugtraq\\_id Fields, page 6-50](#)
- [rna\\_host\\_third\\_party\\_vuln\\_bugtraq\\_id Joins, page 6-51](#)
- [rna\\_host\\_third\\_party\\_vuln\\_bugtraq\\_id Sample Query, page 6-51](#)

## rna\_host\_third\_party\_vuln\_bugtraq\_id Fields

The following table describes the fields you can access in the `rna_host_third_party_vuln_bugtraq_id` table.

**Table 6-46** *rna\_host\_third\_party\_vuln\_bugtraq\_id Fields*

Field	Description
<code>bugtraq_id</code>	The Bugtraq database identification number associated with the vulnerability.
<code>description</code>	A description of the vulnerability.
<code>host_id</code>	ID number of the host.
<code>invalid</code>	A value indicating whether the vulnerability is valid for the host: <ul style="list-style-type: none"> <li>• 0 — Vulnerability is valid</li> <li>• 1 — Vulnerability is invalid</li> </ul>
<code>ip_address</code>	Field deprecated in Version 5.2. Returns <code>null</code> for all queries.
<code>name</code>	The name, or title, of the vulnerability.
<code>port</code>	A port number, if the vulnerability is associated with a server or related application detected on a specific port.
<code>protocol</code>	The traffic protocol (TCP or UDP), if the vulnerability is associated with an application using that protocol.
<code>source</code>	The source of the vulnerability.
<code>third_party_vuln_id</code>	The third-party identification number associated with the vulnerability.

## rna\_host\_third\_party\_vuln\_bugtraq\_id Joins

The following table describes the joins you can perform on the `rna_host_third_party_vuln_bugtraq_id` table.

**Table 6-47** *rna\_host\_third\_party\_vuln\_bugtraq\_id Joins*

You can join this table on...	And...
bugtraq_id	<a href="#">rna_vuln.bugtraq_id</a> <a href="#">rna_vuln.rna_vuln_id</a> <a href="#">rna_host_os_vulns.rna_vuln_id</a> <a href="#">rna_host_service_vulns.rna_vuln_id</a>
host_id	<a href="#">rna_host.host_id</a> <a href="#">rna_host_attribute.host_id</a> <a href="#">rna_host_protocol.host_id</a> <a href="#">rna_host_os_vulns.host_id</a> <a href="#">application_host_map.host_id</a> <a href="#">rna_host_client_app.host_id</a> <a href="#">rna_host_client_app_payload.host_id</a> <a href="#">rna_host_ioc_state.host_id</a> <a href="#">rna_host_ip_map.host_id</a> <a href="#">rna_host_mac_map.host_id</a> <a href="#">rna_host_os.host_id</a> <a href="#">rna_host_sensor.host_id</a> <a href="#">rna_host_service.host_id</a> <a href="#">rna_host_service_banner.host_id</a> <a href="#">rna_host_service_info.host_id</a> <a href="#">rna_host_service_payload.host_id</a> <a href="#">rna_host_service_vulns.host_id</a>

## rna\_host\_third\_party\_vuln\_bugtraq\_id Sample Query

The following query returns the BugTraq vulnerabilities for the host with `host_id` of 8.

```
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

The `rna_host_third_party_vuln_cve_id` table contains information on the third-party vulnerabilities that are mapped to vulnerabilities in MITRE's CVE database and also associated with the hosts in your monitored network. Note that this table contains third-party vulnerability data imported via the host input feature.

For more information, see the following sections:

- [rna\\_host\\_third\\_party\\_vuln\\_cve\\_id Fields, page 6-52](#)
- [rna\\_host\\_third\\_party\\_vuln\\_cve\\_id Joins, page 6-52](#)

- [rna\\_host\\_third\\_party\\_vuln\\_cve\\_id Sample Query, page 6-53](#)

## rna\_host\_third\_party\_vuln\_cve\_id Fields

The following table describes the fields you can access in the `rna_host_third_party_vuln_cve_id` table.

**Table 6-48** *rna\_host\_third\_party\_vuln\_cve\_id Fields*

Field	Description
<code>cve_id</code>	The identification number associated with the vulnerability in MITRE's CVE database.
<code>description</code>	A description of the vulnerability.
<code>host_id</code>	ID number of the host.
<code>invalid</code>	A value indicating whether the vulnerability is valid for the host: <ul style="list-style-type: none"> <li>• 0 — Vulnerability is valid</li> <li>• 1 — Vulnerability is invalid</li> </ul>
<code>ip_address</code>	Field deprecated in Version 5.2. Returns <code>null</code> for all queries.
<code>name</code>	The name, or title, of the vulnerability.
<code>port</code>	A port number, if the vulnerability is associated with a server or related application detected on a specific port.
<code>protocol</code>	The traffic protocol (TCP or UDP), if the vulnerability is associated with an application using that protocol.
<code>source</code>	The source of the vulnerability.
<code>third_party_vuln_id</code>	The identification number associated with the vulnerability.

## rna\_host\_third\_party\_vuln\_cve\_id Joins

The following table describes the joins you can perform on the `rna_host_third_party_vuln_cve_id` table.

**Table 6-49** *rna\_host\_third\_party\_vuln\_cve\_id Joins*

You can join this table on...	And...
cve_id	<a href="#">rna_vuln.bugtraq_id</a> <a href="#">rna_vuln.rna_vuln_id</a> <a href="#">rna_host_os_vulns.rna_vuln_id</a> <a href="#">rna_host_service_vulns.rna_vuln_id</a>
host_id	<a href="#">rna_host.host_id</a> <a href="#">rna_host_attribute.host_id</a> <a href="#">rna_host_protocol.host_id</a> <a href="#">rna_host_os_vulns.host_id</a> <a href="#">application_host_map.host_id</a> <a href="#">rna_host_client_app.host_id</a> <a href="#">rna_host_client_app_payload.host_id</a> <a href="#">rna_host_ioc_state.host_id</a> <a href="#">rna_host_ip_map.host_id</a> <a href="#">rna_host_mac_map.host_id</a> <a href="#">rna_host_os.host_id</a> <a href="#">rna_host_sensor.host_id</a> <a href="#">rna_host_service.host_id</a> <a href="#">rna_host_service_banner.host_id</a> <a href="#">rna_host_service_info.host_id</a> <a href="#">rna_host_service_payload.host_id</a> <a href="#">rna_host_service_vulns.host_id</a>

## rna\_host\_third\_party\_vuln\_cve\_id Sample Query

The following query returns the CVE vulnerabilities for the host with `host_id` of 8.

```
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

The `rna_host_third_party_vuln_rna_id` table contains information on third-party vulnerabilities that are mapped to vulnerabilities in the Firepower System vulnerability database (VDB) and also associated with hosts in your monitored network. Note that the third-party vulnerability data in this table is imported via the host input feature.

For more information, see the following sections:

- [rna\\_host\\_third\\_party\\_vuln\\_rna\\_id Fields, page 6-54](#)
- [rna\\_host\\_third\\_party\\_vuln\\_rna\\_id Joins, page 6-54](#)
- [rna\\_host\\_third\\_party\\_vuln\\_rna\\_id Sample Query, page 6-55](#)

## rna\_host\_third\_party\_vuln\_rna\_id Fields

The following table describes the fields you can access in the `rna_host_third_party_vuln_rna_id` table.

**Table 6-50** *rna\_host\_third\_party\_vuln\_rna\_id Fields*

Field	Description
<code>description</code>	A description of the vulnerability.
<code>host_id</code>	ID number of the host.
<code>invalid</code>	A value indicating whether the vulnerability is valid for the host: <ul style="list-style-type: none"> <li>0 — Vulnerability is valid</li> <li>1 — Vulnerability is invalid</li> </ul>
<code>ip_address</code>	Field deprecated in Version 5.2. Returns <code>null</code> for all queries.
<code>name</code>	The name, or title, of the vulnerability.
<code>port</code>	A port number, if the vulnerability is associated with a server or related application detected on a specific port.
<code>protocol</code>	The traffic protocol (TCP or UDP), if the vulnerability is associated with an application using that protocol.
<code>rna_vuln_id</code>	The vulnerability identification number that Cisco uses to track the vulnerability.
<code>source</code>	The source of the vulnerability.
<code>third_party_vuln_id</code>	The identification number associated with the vulnerability.

## rna\_host\_third\_party\_vuln\_rna\_id Joins

The following table describes the joins you can perform on the `rna_host_third_party_vuln_rna_id` table.

**Table 6-51** *rna\_host\_third\_party\_vuln\_rna\_id Joins*

You can join this table on...	And...
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 Sample Query

The following query returns all third party vulnerabilities with VDB IDs for the host with `host_id` of 8.

```
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

The `rna_vuln` table contains information on the vulnerabilities in the Cisco VDB.

For more information, see the following sections:

- [rna\\_vuln Fields](#), page 6-55
- [rna\\_vuln Joins](#), page 6-57
- [rna\\_vuln Sample Query](#), page 6-57

## rna\_vuln Fields

The following table describes the fields you can access in the `rna_vuln` table.

Table 6-52 rna\_vuln Fields

Field	Description
authentication	Whether authentication is required to exploit the vulnerability: <ul style="list-style-type: none"> <li>• Required</li> <li>• Not Required</li> <li>• Unknown</li> </ul>
availability	When the vulnerability can be exploited: <ul style="list-style-type: none"> <li>• Always</li> <li>• User Initiated</li> <li>• Time Dependent</li> <li>• Unknown</li> </ul>
available_exploits	Whether there are available exploits for the vulnerability: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>
bugtraq_id	The identification number associated with the vulnerability in the Bugtraq database.
class	The class of vulnerability: <ul style="list-style-type: none"> <li>• Configuration Error</li> <li>• Boundary Condition Error</li> <li>• Design Error</li> </ul>
credibility	How credible the vulnerability is: <ul style="list-style-type: none"> <li>• Conflicting Reports</li> <li>• Conflicting Details</li> <li>• Single Source</li> <li>• Reliable Source</li> <li>• Multiple Sources</li> <li>• Vendor Confirmed</li> </ul>
credit	The person or organization credited with reporting the vulnerability.
ease	The ease of exploiting the vulnerability: <ul style="list-style-type: none"> <li>• No Exploit Required</li> <li>• Exploit Available</li> <li>• No Exploit Available</li> </ul>
effect	Details on what could happen when the vulnerability is exploited.
entry_date	The date the vulnerability was entered in the database.
exploit	Information on where you can find exploits for the vulnerability.
impact	The vulnerability impact, corresponding to the impact level determined through correlation of intrusion data, discovery events, and vulnerability assessments. The value can be from 1 to 10, with 10 being the most severe. The impact value of a vulnerability is determined by the writer of the Bugtraq entry.



**Table 6-52** *rna\_vuln Fields (continued)*

Field	Description
local	Indicates whether the vulnerability must be exploited locally: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>
long_description	A general description of the vulnerability.
mitigation	A description of how you can mitigate the vulnerability.
modified_date	The date of the most recent modification to the vulnerability, if applicable.
publish_date	The date the vulnerability was published.
remote	Indicates whether the vulnerability can be exploited across a network: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>
rna_vuln_id	The Cisco vulnerability ID number that the system uses to track vulnerabilities.
scenario	A description of a scenario where an attacker is exploiting the vulnerability.
short_description	A summary description of the vulnerability.
snort_id	The identification number associated with the vulnerability in the Snort ID (SID) database. That is, if an intrusion rule can detect network traffic that exploits a particular vulnerability, that vulnerability is associated with the intrusion rule's SID.
solution	The solution to the vulnerability.
technical_description	The technical description of the vulnerability.
title	The title of the vulnerability.

## rna\_vuln Joins

The following table describes the joins you can perform on the `rna_vuln` table.

**Table 6-53** *rna\_vuln Joins*

You can join this table on...	And...
rna_vuln_id	<code>rna_host_os_vulns.rna_vuln_id</code>
or	<code>rna_host_service_vulns.rna_vuln_id</code>
bugtraq_id	<code>rna_host_third_party_vuln_rna_id.rna_vuln_id</code>
	<code>rna_host_third_party_vuln_cve_id.cve_id</code>
	<code>rna_host_third_party_vuln_bugtraq_id.bugtraq_id</code>

## rna\_vuln Sample Query

The following query returns information about up to 25 vulnerabilities. The records are sorted in order of most events generated based on the vulnerability.

```
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

The **tag\_info** table contains information on the tags that are associated with the applications detected on your network. Note that an application can have multiple associated tags.

For more information, see the following sections:

- [tag\\_info Fields, page 6-58](#)
- [tag\\_info Joins, page 6-58](#)
- [tag\\_info Sample Query, page 6-58](#)

## tag\_info Fields

The following table describes the fields you can access in the **tag\_info** table.

**Table 6-54** tag\_info Fields

Field	Description
domain_name	Name of the domain on which the application was detected.
domain_uuid	UUID of the domain on which the application was detected. This is presented in binary.
tag_description	Tag description.
tag_id	Internal identifier for the tag.
tag_name	Text of the tag that appears in the user interface.
tag_type	One of the following: <ul style="list-style-type: none"> <li>• category</li> <li>• tag</li> </ul>

## tag\_info Joins

The following table describes the joins you can perform on the **tag\_info** table.

**Table 6-55** tag\_info Joins

You can join this table on...	And...
tag_id	<code>application_tag_map.tag_id</code>

## tag\_info Sample Query

The following query returns the application tag record for a selected tag ID within the Global \ Company B \ Edge domain.

```
SELECT tag_id, tag_name, tag_type, tag_description
```

```
FROM tag_info
WHERE tag_id="100" AND domain_name= "Global \ Company B \ Edge";
```

## url\_categories

The **url\_categories** table lists the categories that characterize URLs requested by hosts in your monitored network.

For more information, see the following sections:

- [url\\_categories Fields, page 6-59](#)
- [url\\_categories Joins, page 6-59](#)
- [url\\_categories Sample Query, page 6-59](#)

## url\_categories Fields

The following table describes the fields in the **url\_categories** table.

**Table 6-56** *url\_categories Fields*

Field	Description
category_description	The description of the URL category.
category_id	The internal identification number of the URL category.

## url\_categories Joins

You cannot perform joins on the **url\_categories** table.

## url\_categories Sample Query

The following query returns a category record for the selected category ID.

```
SELECT category_id, category_description
FROM url_categories
WHERE category_id="1";
```

## url\_reputations

The **url\_reputations** table lists the reputations that characterize URLs requested by hosts in your monitored request.

For more information, see the following sections:

- [url\\_reputations Fields, page 6-60](#)
- [url\\_reputations Joins, page 6-60](#)

- [url\\_reputations Sample Query, page 6-60](#)

## url\_reputations Fields

The following table describes the fields in the `url_reputations` table.

**Table 6-57** *url\_reputations Fields*

Field	Description
<code>reputation_description</code>	The description of the reputation.
<code>reputation_id</code>	An internal identification number for the URL reputation.

## url\_reputations Joins

You cannot perform joins on the `url_reputations` table.

## url\_reputations Sample Query

The following query returns URL reputation information for a reputation ID.

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

## user\_ipaddr\_history

The `user_ipaddr_history` table contains information on user activity for a particular host in your monitored network.

For more information, see the following sections:

- [user\\_ipaddr\\_history Fields, page 6-60](#)
- [user\\_ipaddr\\_history Joins, page 6-61](#)
- [user\\_ipaddr\\_history Sample Query, page 6-62](#)

## user\_ipaddr\_history Fields

The following table describes the fields you can access in the `user_ipaddr_history` table.

**Table 6-58** *user\_ipaddr\_history* Fields

Field	Description
authentication_type	Type of authentication used by the user. Values may be: <ul style="list-style-type: none"> <li>• 0 - no authorization required</li> <li>• 1 - passive authentication, AD agent, or ISE session</li> <li>• 2 - captive portal successful authentication</li> <li>• 3 - captive portal guest authentication</li> <li>• 4 - captive portal failed authentication</li> </ul>
domain_name	Name of the domain on which the user was detected.
domain_uuid	UUID of the domain on which the user was detected. This is presented in binary.
endpoint_profile	Name of the type of device used by the connection endpoint.
end_time_sec	The UNIX timestamp of the date and time the Firepower System detected a different user logging into the host, marking the assumed end of the previous user's session. Note that the Firepower System does not detect logoffs.
id	An internal identification number for the user history record.
ipaddr	A binary representation of the IP address of the host.
location_ip	IP address of the interface communicating with ISE. Can be IPv4 or IPv6.
start_time_sec	The UNIX timestamp of the date and time the Firepower System detected the user logging into host.
security_group	ID number of the network traffic group.
user_dept	The department of the user.
user_email	The email address of the user.
user_first_name	The first name of the user.
user_id	An internal identification number for the user.
user_last_name	The last name of the user.
user_last_seen_sec	The UNIX timestamp of the date and time the Firepower System last detected user activity for the user.
user_last_updated_sec	The UNIX timestamp of the date and time the Firepower System last updated the user record for the user.
user_name	The user name of the user.
user_phone	The phone number of the user.
user_rna_service	Name of the application protocol being used when the user was detected, if available.

## user\_ipaddr\_history Joins

The following table describes the joins you can perform on the `user_ipaddr_history` table.

Table 6-59 user\_ipaddr\_history Joins

You can join this table on...	And...
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 rna_host_ioc_state.host_id

## user\_ipaddr\_history Sample Query

The following query returns all user activity records for the selected IP address after the specified start timestamp.

```

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) = "00000000000000000000000000000000FFFF0A0A0A04" AND start_time_sec >=
UNIX_TIMESTAMP("2011-10-01 00:00:00");

```