



FireSIGHT System 데이터베이스 액세스 설명서

버전 5.4
1 26, 2016

이 설명서의 제품 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항은 정확한 것으로 간주되지만 이에 대해 명시적이든 묵시적이든 어떠한 보증도 없이 제공됩니다. 모든 제품의 애플리케이션 사용에 대한 책임은 전적으로 사용자에게 있습니다.

Cisco Systems, Inc.

www.cisco.com

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다.

주소, 전화 번호 및 팩스 번호는

Cisco 웹사이트

www.cisco.com/go/offices.

동봉된 제품의 소프트웨어 라이선스 및 제한 보증은 제품과 함께 제공되는 정보 패키지에 설명되어 있으며 본 참조 문서에 통합되어 있습니다. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2014년 Cisco Systems, Inc. All rights reserved.



목 차

1장

도입 1-9

버전 5.4의 데이터베이스 액세스와 관련된 주요 변경 사항	1-9
버전 5.4의 수정된 필드	1-9
버전 5.4의 수정된 테이블	1-9
사전 요구 사항	1-13
라이센싱	1-13
FireSIGHT System 기능 및 용어	1-13
통신 포트	1-13
클라이언트 시스템	1-13
쿼리 애플리케이션	1-14
데이터베이스 쿼리	1-14
시작해야 하는 위치	1-14

2장

데이터베이스 액세스 설정 2-1

액세스할 어플라이언스 결정	2-1
데이터베이스 사용자 어카운트 생성	2-2
방어 센터에 대한 데이터베이스 액세스 활성화	2-3
JDBC 드라이버 다운로드	2-4
클라이언트 SSL 인증서 설치	2-5
서드파티 애플리케이션을 사용하여 데이터베이스에 연결	2-6
맞춤형 프로그램을 사용하여 데이터베이스에 연결	2-8
맞춤형 Java 프로그램의 소스 코드	2-8
애플리케이션 실행	2-9
데이터베이스 쿼리	2-10
지원되는 SHOW 명령 구문	2-11
지원되는 DESCRIBE 또는 DESC 명령 구문	2-11
지원되는 SELECT 명령 구문	2-12
조인 제한	2-13
생소한 형식으로 저장된 데이터 쿼리	2-13
성능상의 이유로 쿼리 제한	2-15
쿼리 팁	2-16
샘플 쿼리	2-16

3장

스키마: 시스템 레벨 테이블 3-1

- audit_log 3-1
 - audit_log 필드 3-1
 - audit_log 조인 3-2
 - audit_log 샘플 쿼리 3-2
- fireamp_event 3-2
 - fireamp_event 필드 3-2
 - fireamp_event 조인 3-8
 - fireamp_event 샘플 쿼리 3-8
- health_event 3-8
 - health_event 필드 3-9
 - health_event 조인 3-9
 - health_event 샘플 쿼리 3-9
- sru_import_log 3-10
 - sru_import_log 필드 3-10
 - sru_import_log 조인 3-11
 - sru_import_log 샘플 쿼리 3-11

4장

스키마: 침입 테이블 4-1

- intrusion_event 4-1
 - intrusion_event 필드 4-2
 - intrusion_event 조인 4-6
 - intrusion_event 샘플 쿼리 4-7
- intrusion_event_packet 4-7
 - intrusion_event_packet 필드 4-7
 - intrusion_event_packet 조인 4-8
 - intrusion_event_packet 샘플 쿼리 4-8
- rule_message 4-8
 - rule_message 필드 4-8
 - rule_message 조인 4-8
 - rule_message 샘플 쿼리 4-9
- rule_documentation 4-9
 - rule_documentation 필드 4-9
 - rule_documentation 조인 4-10
 - rule_documentation 샘플 쿼리 4-10

5장

스키마: 통계 추적 테이블 5-1

- 통계 추적 테이블 이해 5-2
 - 통계 추적 테이블의 저장 특성 5-2
 - 통계 테이블 쿼리 시 시간 간격 지정 5-3
- app_ids_stats_current_timeframe 5-4
 - app_ids_stats_current_timeframe 필드 5-4
 - app_ids_stats_current_timeframe 조인 5-5
 - app_ids_stats_current_timeframe 샘플 쿼리 5-5
- app_stats_current_timeframe 5-6
 - app_stats_current_timeframe 필드 5-6
 - app_stats_current_timeframe 조인 5-7
 - app_stats_current_timeframe 샘플 쿼리 5-7
- geolocation_stats_current_timeframe 5-7
 - geolocation_stats_current_timeframe 필드 5-8
 - geolocation_stats_current_timeframe 조인 5-9
 - geolocation_stats_current_timeframe 샘플 쿼리 5-9
- ids_impact_stats_current_timeframe 5-9
 - ids_impact_stats_current_timeframe 필드 5-10
 - ids_impact_stats_current_timeframe 조인 5-10
 - ids_impact_stats_current_timeframe 샘플 쿼리 5-10
- session_stats_current_timeframe 5-11
 - session_stats_current_timeframe 필드 5-11
 - session_stats_current_timeframe 조인 5-11
 - session_stats_current_timeframe 샘플 쿼리 5-12
- ssl_stats_current_timeframe 5-12
 - ssl_stats_current_timeframe 필드 5-12
 - ssl_stats_current_timeframe 조인 5-14
 - ssl_stats_current_timeframe 샘플 쿼리 5-14
- storage_stats_by_disposition_current_timeframe 5-14
 - storage_stats_by_disposition_current_timeframe 필드 5-15
 - storage_stats_by_disposition_current_timeframe 조인 5-15
 - storage_stats_by_disposition_current_timeframe 샘플 쿼리 5-15
- storage_stats_by_file_type_current_timeframe 5-16
 - storage_stats_by_file_type_current_timeframe 필드 5-16
 - storage_stats_by_file_type_current_timeframe 조인 5-16
 - storage_stats_by_file_type_current_timeframe 샘플 쿼리 5-17
- transmission_stats_by_file_type_current_timeframe 5-17
 - transmission_stats_by_file_type_current_timeframe 필드 5-17

- transmission_stats_by_file_type_current_timeframe [조인](#) 5-18
- transmission_stats_by_file_type_current_timeframe [샘플 쿼리](#) 5-18
- url_category_stats_current_timeframe 5-18
 - url_category_stats_current_timeframe [필드](#) 5-18
 - url_category_stats_current_timeframe [조인](#) 5-19
 - url_category_stats_current_timeframe [샘플 쿼리](#) 5-19
- url_reputation_stats_current_timeframe 5-19
 - url_reputation_stats_current_timeframe [필드](#) 5-20
 - url_reputation_stats_current_timeframe [조인](#) 5-20
 - url_reputation_stats_current_timeframe [샘플 쿼리](#) 5-20
- user_ids_stats_current_timeframe 5-21
 - user_ids_stats_current_timeframe [필드](#) 5-21
 - user_ids_stats_current_timeframe [조인](#) 5-22
 - user_ids_stats_current_timeframe [샘플 쿼리](#) 5-22
- user_stats_current_timeframe 5-22
 - user_stats_current_timeframe [필드](#) 5-22
 - user_stats_current_timeframe [조인](#) 5-23
 - user_stats_current_timeframe [샘플 쿼리](#) 5-23

6장

스키마: 검색 이벤트 및 네트워크 맵 테이블 6-1

- application_host_map 6-5
 - application_host_map [필드](#) 6-5
 - application_host_map [조인](#) 6-6
 - application_host_map [샘플 쿼리](#) 6-7
- application_info 6-7
 - application_info [필드](#) 6-7
 - application_info [조인](#) 6-8
 - application_info [샘플 쿼리](#) 6-8
- application_tag_map 6-8
 - application_tag_map [필드](#) 6-9
 - application_tag_map [조인](#) 6-9
 - application_tag_map [샘플 쿼리](#) 6-10
- network_discovery_event 6-10
 - network_discovery_event [필드](#) 6-10
 - network_discovery_event [조인](#) 6-11
 - network_discovery_event [샘플 쿼리](#) 6-11
- rna_host 6-12
 - rna_host [필드](#) 6-12
 - rna_host [조인](#) 6-13

rna_host 샘플 쿼리	6-13
rna_host_attribute	6-13
rna_host_attribute 필드	6-14
rna_host_attribute 조인	6-14
rna_host_attribute 샘플 쿼리	6-14
rna_host_client_app	6-15
rna_host_client_app 필드	6-15
rna_host_client_app 조인	6-16
rna_host_client_app 샘플 쿼리	6-17
rna_host_client_app_payload	6-17
rna_host_client_app_payload 필드	6-18
rna_host_client_app_payload 조인	6-19
rna_host_client_app_payload 샘플 쿼리	6-20
rna_host_ioc_state	6-20
rna_host_ioc_state 필드	6-21
rna_host_ioc_state 조인	6-23
rna_host_ioc_state 샘플 쿼리	6-23
rna_host_ip_map	6-24
rna_host_ip_map 필드	6-24
rna_host_ip_map 조인	6-24
rna_host_ip_map 샘플 쿼리	6-25
rna_host_mac_map	6-25
rna_host_mac_map 필드	6-25
rna_host_mac_map 조인	6-26
rna_host_mac_map 샘플 쿼리	6-26
rna_host_os	6-26
rna_host_os 필드	6-27
rna_host_os 조인	6-27
rna_host_os 샘플 쿼리	6-28
rna_host_os_vulns	6-28
rna_host_os_vulns 필드	6-29
rna_host_os_vulns 조인	6-29
rna_host_os_vulns 샘플 쿼리	6-30
rna_host_protocol	6-30
rna_host_protocol 필드	6-30
rna_host_protocol 조인	6-31
rna_host_protocol 샘플 쿼리	6-31
rna_host_sensor	6-31
rna_host_sensor 필드	6-32

rna_host_sensor	조인	6-32
rna_host_sensor	샘플 쿼리	6-32
rna_host_service	6-33	
rna_host_service	필드	6-33
rna_host_service	조인	6-33
rna_host_service	샘플 쿼리	6-34
rna_host_service_banner	6-35	
rna_ip_host_service_banner	필드	6-35
rna_host_service_banner	조인	6-35
rna_host_service_banner	샘플 쿼리	6-36
rna_host_service_info	6-36	
rna_host_service_info	필드	6-37
rna_host_service_info	조인	6-38
rna_host_service_info	샘플 쿼리	6-39
rna_host_service_payload	6-39	
rna_host_service_payload	필드	6-39
rna_host_service_payload	조인	6-40
rna_host_service_payload	샘플 쿼리	6-41
rna_host_service_subtype	6-42	
rna_host_service_subtype	필드	6-42
rna_host_service_subtype	조인	6-43
rna_host_service_subtype	샘플 쿼리	6-43
rna_host_service_vulns	6-43	
rna_host_service_vulns	필드	6-43
rna_host_service_vulns	조인	6-44
rna_host_service_vulns	샘플 쿼리	6-44
rna_host_third_party_vuln	6-45	
rna_host_third_party_vuln	필드	6-45
rna_host_third_party_vuln	조인	6-46
rna_host_third_party_vuln	샘플 쿼리	6-46
rna_host_third_party_vuln_bugtraq_id	6-46	
rna_host_third_party_vuln_bugtraq_id	필드	6-47
rna_host_third_party_vuln_bugtraq_id	조인	6-47
rna_host_third_party_vuln_bugtraq_id	샘플 쿼리	6-48
rna_host_third_party_vuln_cve_id	6-48	
rna_host_third_party_vuln_cve_id	필드	6-49
rna_host_third_party_vuln_cve_id	조인	6-49
rna_host_third_party_vuln_cve_id	샘플 쿼리	6-50
rna_host_third_party_vuln_rna_id	6-50	

- rna_host_third_party_vuln_rna_id 필드 6-51
 - rna_host_third_party_vuln_rna_id 조인 6-51
 - rna_host_third_party_vuln_rna_id 샘플 쿼리 6-52
- rna_vuln 6-52
 - rna_vuln 필드 6-53
 - rna_vuln 조인 6-54
 - rna_vuln 샘플 쿼리 6-55
- tag_info 6-55
 - tag_info 필드 6-55
 - tag_info 조인 6-55
 - tag_info 샘플 쿼리 6-56
- url_categories 6-56
 - url_categories 필드 6-56
 - url_categories 조인 6-56
 - url_categories 샘플 쿼리 6-56
- url_reputations 6-57
 - url_reputations 필드 6-57
 - url_reputations 조인 6-57
 - url_reputations 샘플 쿼리 6-57
- user_ipaddr_history 6-57
 - user_ipaddr_history 필드 6-58
 - user_ipaddr_history 조인 6-58
 - user_ipaddr_history 샘플 쿼리 6-59

7장

스키마: 연결 로그 테이블 7-1

- connection_log 7-1
 - connection_log 필드 7-2
 - connection_log 조인 7-11
 - connection_log 샘플 쿼리 7-11
- connection_summary 7-11
 - connection_summary 필드 7-12
 - connection_summary 조인 7-14
 - connection_summary 샘플 쿼리 7-14
- si_connection_log 7-15
 - si_connection_log 필드 7-15
 - si_connection_log 조인 7-24
 - si_connection_log 샘플 쿼리 7-24

8장	스키마: 사용자 작업 테이블	8-1
	discovered_users	8-1
	discovered_users 필드	8-1
	discovered_users 조인	8-2
	discovered_users 샘플 쿼리	8-2
	user_discovery_event	8-2
	user_discovery_event 필드	8-3
	user_discovery_event 조인	8-4
	user_discovery_event 샘플 쿼리	8-4

9장	스키마: 상관관계 테이블	9-1
	compliance_event	9-1
	compliance_event 필드	9-1
	compliance_event 조인	9-5
	compliance_event 샘플 쿼리	9-5
	remediation_status	9-6
	remediation_status 필드	9-6
	remediation_status 조인	9-6
	remediation_status 샘플 쿼리	9-6
	white_list_event	9-7
	white_list_event 필드	9-7
	white_list_event 조인	9-8
	white_list_event 샘플 쿼리	9-8
	white_list_violation	9-9
	white_list_violation 필드	9-9
	white_list_violation 조인	9-9
	white_list_violation 샘플 쿼리	9-10

10장	스키마: 파일 이벤트 테이블	10-1
	file_event	10-1
	file_event 필드	10-1
	file_event 조인	10-6
	file_event 샘플 쿼리	10-6

부록 A	사용 중단된 테이블	A-1
-------------	-------------------	------------



도입

FireSIGHT System® 데이터베이스 액세스 기능을 사용하면 JDBC SSL 연결을 지원하는 타사 클라이언트를 사용하여 Cisco 방화 센터의 침입, 검색, 사용자 활동, 상관관계, 연결, 취약성, 애플리케이션 및 URL 통계 데이터베이스 테이블을 쿼리할 수 있습니다.

Crystal Reports, Actuate BIRT 또는 JasperSoft iReport와 같은 업계 표준 보고 툴을 사용하여 쿼리를 설계 및 제출할 수 있습니다. 또는 맞춤형 애플리케이션을 구성하여 프로그램 제어에 따라 Cisco 데이터를 쿼리할 수 있습니다. 예를 들어, 서블릿을 구축하여 침입 및 검색 이벤트 데이터를 정기적으로 보고하거나 알림 대시보드를 새로 고칠 수 있습니다.

단일 클라이언트로도 여러 방화 센터에 연결할 수 있으나, 이에 대한 액세스를 각각 개별적으로 구성해야 합니다.

어떤 어플라이언스를 연결할지 결정할 경우, Cisco 어플라이언스의 데이터베이스를 쿼리하면 사용 가능한 어플라이언스 리소스가 줄어듭니다. 쿼리를 주의 깊게 설계하고 조직의 우선 순위와 일치하는 시기에 이를 제출해야 합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [버전 5.4의 데이터베이스 액세스와 관련된 주요 변경 사항, 페이지 1-9](#)
- [사전 요구 사항, 페이지 1-13](#)
- [시작해야 하는 위치, 페이지 1-14](#)

버전 5.4의 데이터베이스 액세스와 관련된 주요 변경 사항

버전 5.3.1에서 FireSIGHT System 구축을 버전 5.4로 업그레이드하는 경우, 다음 변경 사항에 유의해야 하며 이 중 일부는 쿼리를 업데이트해야 할 수 있습니다.

버전 5.4의 수정된 필드

`fireamp_event` 및 `file_event`의 `file_name` 필드에는 UTF-8 문자를 포함할 수 있습니다.

버전 5.4의 수정된 테이블

아래 표에는 버전 5.4의 데이터베이스 액세스 테이블의 변경 사항이 나열되어 있습니다.

표 1-1 버전 5.4의 테이블 변경 사항 요약

표	변경 사항 설명
application_host_map , 페이지 6-5	application_tag_id 필드가 사용 중단됨
connection_log , 페이지 7-1	다음 필드가 추가됨: <ul style="list-style-type: none"> • access_control_policy_uuid • cert_valid_start_date • cert_valid_end_date • network_analysis_policy_name • network_analysis_policy_UUID • ssl_actual_action • ssl_cipher_suite • ssl_expected_action • ssl_flow_flags • ssl_flow_messages • ssl_flow_status • ssl_issuer_common_name • ssl_issuer_country • ssl_issuer_organization • ssl_issuer_organization_unit • ssl_policy_action • ssl_policy_name • ssl_policy_reason • ssl_rule_action • ssl_rule_name • ssl_serial_number • ssl_server_name • ssl_subject_common_name • ssl_subject_country • ssl_subject_organization • ssl_subject_organization_unit • ssl_url_category • ssl_version

표 1-1 버전 5.4의 테이블 변경 사항 요약(계속)

표	변경 사항 설명
si_connection_log , 페이지 7-15	다음 필드가 추가됨: <ul style="list-style-type: none"> • access_control_policy_uuid • cert_valid_start_date • cert_valid_end_date • network_analysis_policy_name • network_analysis_policy_UUID • ssl_actual_action • ssl_cipher_suite • ssl_expected_action • ssl_flow_flags • ssl_flow_messages • ssl_flow_status • ssl_issuer_common_name • ssl_issuer_country • ssl_issuer_organization • ssl_issuer_organization_unit • ssl_policy_action • ssl_policy_name • ssl_policy_reason • ssl_rule_action • ssl_rule_name • ssl_serial_number • ssl_server_name • ssl_subject_common_name • ssl_subject_country • ssl_subject_organization • ssl_subject_organization_unit • ssl_url_category • ssl_version

표 1-1 버전 5.4의 테이블 변경 사항 요약(계속)

표	변경 사항 설명
file_event , 페이지 10-1	<p>다음 필드가 추가됨:</p> <ul style="list-style-type: none"> • cert_valid_start_date • cert_valid_end_date • ssl_issuer_common_name • ssl_issuer_country • ssl_issuer_organization • ssl_issuer_organization_unit • ssl_serial_number • ssl_subject_common_name • ssl_subject_country • ssl_subject_organization • ssl_subject_organization_unit
fireamp_event , 페이지 3-2	<p>다음 필드가 추가됨:</p> <ul style="list-style-type: none"> • cert_valid_start_date • cert_valid_end_date • ssl_issuer_common_name • ssl_issuer_country • ssl_issuer_organization • ssl_issuer_organization_unit • ssl_serial_number • ssl_subject_common_name • ssl_subject_country • ssl_subject_organization • ssl_subject_organization_unit
intrusion_event , 페이지 4-1	<p>다음 필드가 추가됨:</p> <ul style="list-style-type: none"> • access_control_policy_UUID • network_analysis_policy_name • network_analysis_policy_UUID

사전 요구 사항

데이터베이스 액세스 기능을 사용하려면 우선 다음 섹션에 나와 있는 사전 요구 사항을 충족해야 합니다.

- 라이선싱, 페이지 1-13
- FireSIGHT System 기능 및 용어, 페이지 1-13
- 통신 포트, 페이지 1-13
- 클라이언트 시스템, 페이지 1-13
- 쿼리 애플리케이션, 페이지 1-14
- 데이터베이스 쿼리, 페이지 1-14

라이선싱

설치된 모든 Cisco 라이선스로 외부 데이터베이스를 쿼리할 수 있습니다. 그러나 특정 테이블은 라이선스가 제공된 기능과 연결되어 있습니다. 이러한 테이블은 적합한 Cisco 라이선스가 설치되고 데이터를 생성할 수 있도록 구축이 올바르게 구성된 경우에만 데이터가 채워집니다. 이러한 테이블을 쿼리하였으나 연결된 Cisco 라이선스가 설치되지 않은 경우, 아무런 결과가 검색되지 않습니다. 라이선싱에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*의 라이선싱 이해를 참조하십시오.

FireSIGHT System 기능 및 용어

이 설명서에 있는 정보를 이해하려면 FireSIGHT System의 기능 및 명명법, 그리고 구성 요소의 기능을 숙지하고 있어야 합니다. 또한 이러한 구성 요소가 생성하는 이벤트 데이터의 여러 가지 유형에 대해서도 숙지해야 합니다. 잘 모르는 정의 내용이나 제품별 용어에 대한 정보는 *FireSIGHT System 사용 설명서*에서 자주 참조할 수 있습니다. 이 사용 설명서에는 이 설명서에 설명된 필드의 데이터에 대한 추가 정보도 포함되어 있습니다.

통신 포트

FireSIGHT System의 경우 어플라이언스 간에 내부적으로 그리고 외부적으로 통신을 수행할 때 특정 포트를 사용해야 하며, 네트워크 구축 내에서 특정 기능을 활성화해야 합니다.

방어 센터에서 데이터베이스 액세스를 활성화하게 되면 시스템에서는 클라이언트와 어플라이언스 간에 JDBC 트래픽을 전달하는 연결에 포트 1500 및 2000을 사용합니다.

클라이언트 시스템

Cisco 데이터베이스에 연결하기 위해 사용하려는 컴퓨터에서는 JRE(Java Runtime Environment) 또는 JVM(Java Virtual Machine)으로도 알려진 Java 소프트웨어를 설치해야 합니다.

<http://java.com/>에서 최신 버전의 Java를 다운로드할 수 있습니다.

데이터베이스에 연결하는 데 사용할 JDBC 드라이버 파일이 포함된 패키지를 방어 센터에서 다운로드하고 압축을 풀어야 합니다. 이 패키지에는 방어 센터와의 암호화된 통신을 지원하는 SSL 인증서를 설치하는 데 사용되는 실행 파일 및 이러한 유틸리티에 대한 기타 소스 파일도 포함되어 있습니다.

또한 컴퓨터에 해당되는 시스템 설정(예: 환경 변수)을 변경하는 방법도 숙지해야 합니다.

쿼리 애플리케이션

Cisco 데이터베이스를 쿼리하려는 경우 Actuate BIRT, JasperSoft iReport, Crystal Reports 또는 JDBC SSL 연결을 지원하는 모든 기타 애플리케이션(맞춤형 애플리케이션 포함) 같은 상용 보고 툴을 사용할 수 있습니다. 이 설명서에서는 JDBC URL, 드라이버 JAR 파일, 드라이버 클래스를 비롯하여 데이터베이스에 연결하는 데 필요한 정보를 제공합니다. 그러나 JDBC SSL 연결을 구성하는 방법에 관한 자세한 지침은 해당 보고 툴의 설명서를 참조해야 합니다.

Cisco에서는 데이터베이스 연결을 테스트하고, 스키마를 보고, 기본 애드 혹 쿼리를 수동으로 실행하는 데 사용할 수 있는 샘플 명령줄 Java 애플리케이션인 RunQuery도 제공합니다. RunQuery 소스 코드는 맞춤형 Java 애플리케이션의 데이터베이스 연결 설정을 위한 참조이기도 합니다. RunQuery 소스 코드는 방어 센터에서 다운로드하는 ZIP 패키지에 포함되어 있습니다.

RunQuery는 샘플 클라이언트 전용이며, 완전한 기능을 제공하는 보고 툴이 **아닙니다**. Cisco에서는 데이터베이스 쿼리 시 이를 기본 방법으로 사용하는 것을 **강력하게** 권장합니다. RunQuery 사용에 대한 정보를 보려면 ZIP 패키지에 포함된 README 파일을 참조하십시오.

데이터베이스 액세스 기능은 다음과 같은 JDBC 기능만 사용합니다.

- 스키마, 버전, 지원되는 기능 등의 정보를 포함하는 데이터베이스 메타데이터
- SQL 쿼리 실행

데이터베이스 액세스에서는 저장된 절차, 트랜잭션, 배치 명령, 여러 결과 집합 또는 삽입/업데이트/삭제 함수를 포함한 그 밖의 JDBC 기능은 사용하지 않습니다.

데이터베이스 쿼리

데이터베이스를 쿼리하려면 조인 조건을 사용하여 단일 테이블 및 여러 테이블에서 SELECT 문을 구성하고 실행하는 방법을 알아야 합니다.

이를 지원하기 위해 이 설명서에는 지원되는 MySQL 쿼리 구문, Cisco 데이터베이스 스키마, 허용되는 조인, 그리고 그 밖의 중요한 쿼리 관련 요건 및 제한 사항에 대한 정보가 포함되어 있습니다.

시작해야 하는 위치

사전 요구 사항, 페이지 1-13에 설명된 사전 요구 사항을 충족한 후에는 클라이언트 시스템을 방어 센터에 연결하는 구성을 시작할 수 있습니다.

데이터베이스 액세스 설정, 페이지 2-1에서는 액세스를 허용하도록 어플라이언스를 구성하는 방법, 클라이언트 시스템을 어플라이언스에 연결하도록 구성하는 방법, 보고 애플리케이션을 어플라이언스에 연결하도록 구성하는 방법을 설명합니다. 여기에는 기본적인 쿼리 지침 및 지원되는 MySQL 구문에 대한 정보도 포함되어 있습니다.

설명서의 나머지 부분에는 데이터베이스 및 샘플 쿼리에 대한 스키마 및 조인 정보가 포함되어 있으며, 이는 다음과 같은 장으로 나뉘어 있습니다.

- **스키마: 시스템 레벨 테이블, 페이지 3-1**에는 감사 로그 및 상태 이벤트 같은 시스템 레벨 테이블에 대한 스키마 및 조인 정보가 포함되어 있습니다.
- **스키마: 침입 테이블, 페이지 4-1**에는 침입 관련 테이블에 대한 스키마 및 조인 정보가 포함되어 있습니다.
- **스키마: 통계 추적 테이블, 페이지 5-1**에는 애플리케이션, URL, 사용자 통계 테이블에 대한 스키마 및 조인 정보가 포함되어 있습니다.

- **스키마: 검색 이벤트 및 네트워크 맵 테이블, 페이지 6-1**에는 검색 이벤트 및 네트워크 맵 정보 (즉, 네트워크 자산에 대한 정보)가 있는 테이블의 스키마 및 조인 정보가 포함되어 있습니다.
- **스키마: 연결 로그 테이블, 페이지 7-1**에는 연결 이벤트 및 연결 요약 이벤트 정보가 있는 테이블의 스키마 및 조인 정보가 포함되어 있습니다.
- **스키마: 사용자 작업 테이블, 페이지 8-1**에는 사용자 검색 및 ID 데이터가 있는 테이블의 스키마 및 조인 정보가 포함되어 있습니다.
- **스키마: 상관관계 테이블, 페이지 9-1**에는 화이트리스트 이벤트 및 위반, 그리고 교정 상태 데이터를 비롯한 상관관계 관련 테이블의 스키마 및 조인 정보가 포함되어 있습니다.
- **스키마: 파일 이벤트 테이블, 페이지 10-1**에는 파일 이벤트가 있는 테이블의 스키마 및 조인 정보가 포함되어 있습니다.

■ 시작해야 하는 위치



데이터베이스 액세스 설정

데이터베이스에 대한 읽기 전용 액세스 권한을 얻으려면, 우선 액세스를 허용하도록 어플라이언스를 구성해야 합니다. 그런 다음, JDBC 드라이버를 다운로드한 후 액세스하려는 어플라이언스에서 SSL 인증서를 승인하여 어플라이언스에 연결하도록 클라이언트 시스템을 구성해야 합니다. 마지막으로, 어플라이언스에 연결할 보고 애플리케이션을 구성해야 합니다.



참고

데이터베이스 액세스를 설정하기 전에, [사전 요구 사항](#), [페이지 1-13](#)에 설명된 사전 요구 사항을 충족하는지 확인해야 합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [액세스할 어플라이언스 결정](#), [페이지 2-1](#)
- [데이터베이스 사용자 어카운트 생성](#), [페이지 2-2](#)
- [방어 센터에 대한 데이터베이스 액세스 활성화](#), [페이지 2-3](#)
- [JDBC 드라이버 다운로드](#), [페이지 2-4](#)
- [클라이언트 SSL 인증서 설치](#), [페이지 2-5](#)
- [서드파티 애플리케이션을 사용하여 데이터베이스에 연결](#), [페이지 2-6](#)
- [맞춤형 프로그램을 사용하여 데이터베이스에 연결](#), [페이지 2-8](#)
- [데이터베이스 쿼리](#), [페이지 2-10](#)
- [샘플 쿼리](#), [페이지 2-16](#)

액세스할 어플라이언스 결정

단일 클라이언트로도 여러 어플라이언스에 연결할 수 있으나, 액세스를 허용하려면 각 어플라이언스를 개별적으로 구성해야 합니다.

어떤 어플라이언스를 연결할지 결정하려면, 어플라이언스에서 사용 가능한 데이터는 설치한 라이선스에 따라, 그리고 FireSIGHT System의 컨피그레이션에 따라 달라집니다.

아래 목록에는 쿼리에서 결과가 반환되지 않을 수 있는 특정한 사유 중 몇 가지가 설명되어 있습니다.

- 쿼리가 너무 구체적입니다. 이를테면 쿼리의 시간 범위 또는 IP 주소 범위를 조정해야 할 수 있습니다.
- 이벤트를 생성하게 되는 네트워크 트래픽에 따라, 이벤트의 일부 필드가 채워지지 않을 수 있습니다. 일부 연결 이벤트에 페이로드 정보가 포함되지 않은 경우를 예로 들 수 있습니다.

- 어플라이언스에 적합한 라이선스가 없습니다. 예를 들어, 적합한 기능 라이선스가 설치되지 않은 경우 네트워크 검색 및 사용자 ID 관련 이벤트가 데이터베이스에 로깅되지 않습니다.
- 쿼리하려는 이벤트 유형을 로깅하도록 FireSIGHT System을 구성하지 않았습니다. 예를 들면 다음과 같습니다.
 - 침입 이벤트, 검색 관련 이벤트, 상태 이벤트를 로깅하려면 해당 정책을 적용해야 합니다.
 - 네트워크 검색 이벤트 및 호스트 입력 이벤트의 로깅은 시스템 정책에서 구성할 수 있습니다. 로깅은 기본적으로 활성화되어 있습니다.
 - 사용자 ID 데이터를 로깅하려면 네트워크 검색을 구성해야 합니다.
 - 침입 이벤트에 대한 패킷 데이터를 전송하려면 관리되는 디바이스를 방어 센터에 추가할 때 해당 옵션을 활성화해야 합니다.
 - 상관관계 이벤트, 규정준수 화이트리스트 이벤트, 교정 상태 이벤트를 생성하고 로깅하려면 규칙 또는 응답을 활성 교정 정책에 추가해야 합니다.
 - 연결 이벤트를 로깅하려면 액세스 제어 규칙의 연결 및 액세스 제어 정책의 기본 작업에 대한 로깅을 활성화해야 합니다. 관리되는 디바이스는 이벤트 생성을 유발하는 네트워크 트래픽을 수신하지 않습니다.
 - 데이터베이스 제한은 쿼리하려는 어플라이언스의 시스템 정책에서 0으로 설정됩니다.
 - 관리되는 디바이스는 이벤트 생성을 유발하는 네트워크 트래픽을 수신하지 않습니다.

이벤트 생성 및 로깅 방법에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

데이터베이스 사용자 어카운트 생성

라이선스: 모두

FireSIGHT System 데이터베이스에 대한 액세스를 구성하려면 우선 사용자 어카운트를 생성하고 이를 External Database User 권한에 할당해야 합니다. Cisco에서 사전 정의한 사용자 역할(External Database User 권한 포함) 또는 조직에서 생성한 맞춤형 사용자 역할(External Database User 권한 포함)을 어카운트에 할당하여 이 권한을 부여할 수 있습니다. 사용자 어카운트를 생성하고 지정된 사용자 역할에서 권한을 보는 방법에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.




정보

사전 정의된 Administrator 역할이 할당된 사용자는 기본적으로 External Database User 권한을 갖고 있습니다.

로컬로 생성 및 인증된 External Database 사용자는 방어 센터 웹 인터페이스에서 비밀번호를 변경할 수 있습니다. 비밀번호 변경에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오. 다음 표에는 로컬로 생성된 사용자가 비밀번호 및 어카운트 액세스를 제어하는 데 사용할 수 있는 몇 가지 옵션이 설명되어 있습니다.

표 2-1 사용자 어카운트 비밀번호 옵션

옵션	설명
Use External Authentication Method	이 사용자의 자격 증명을 외부에서 인증하게 하려면 이 옵션을 선택합니다. 참고 사용자에 대해 이 옵션을 선택했지만 외부 인증 서버를 사용할 수 없는 상태라면 해당 사용자는 웹 인터페이스에 로그인할 수 있거나 어떤 기능도 액세스하지 못합니다.
Maximum Number of Failed Logins	공백 없이 정수를 입력하여 각 사용자가 어카운트가 잠길 때까지 로그인 시도에 연속으로 실패할 수 있는 최대 횟수를 지정합니다. 기본 설정은 5회입니다. 0을 입력하면 로그인 실패 횟수의 제한이 사라집니다.
Minimum Password Length	공백 없이 정수를 입력하여 사용자 비밀번호의 최소 길이를 글자 수로 지정합니다. 기본 설정은 8입니다. 값이 0이면 최소 길이 제한이 없습니다.
Days Until Password Expiration	여기에 입력한 일수가 지나면 사용자의 비밀번호가 만료됩니다. 기본 설정은 0이며, 이렇게 하면 비밀번호가 만료되지 않습니다.
Days Before Expiration Warning	비밀번호가 만료되기 전에 사용자에게 비밀번호를 변경하게 하는 경고 일수를 입력합니다. 기본 설정은 0일입니다.  주의 경고 일수는 비밀번호 만료 시점까지 남은 일수보다 적어야 합니다.
Force Password Reset on Login	사용자가 처음 로그인할 때 반드시 비밀번호를 변경하게 하려면 이 옵션을 선택합니다.
Check Password Strength	강력한 비밀번호를 요구하려면 이 옵션을 선택합니다. 강력한 비밀번호는 대/소문자가 혼합된 8자 이상의 영숫자이고 숫자와 특수 문자를 각각 하나 이상 포함해야 합니다. 사전에 나와 있는 단어일 수 없으며, 연속적으로 반복되는 문자를 포함할 수 없습니다.
Exempt from Browser Session Timeout	사용자의 로그인 세션이 무활동으로 인해 종료되지 않게 하려면 이 옵션을 선택합니다. 관리자 역할의 사용자는 면제받을 수 없습니다.

External Database 사용자를 외부에서 생성하고 인증할 수 있으며, 이 경우 어플라이언스는 외부 저장소(예: LDAP 디렉토리 서버 또는 RADIUS 인증 서버)에서 사용자 자격 증명을 검색합니다. 이러한 사용자의 비밀번호 설정은 외부 서버에서 관리합니다. 외부 인증에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.


방어 센터에 대한 데이터베이스 액세스 활성화

라이센스: 모두

External Database 사용자를 생성한 후에는 방어 센터가 어플라이언스의 데이터베이스에 액세스를 허용하도록 구성해야 합니다. 또한 어플라이언스에서 데이터베이스 액세스 목록을 구성하고 외부 데이터베이스를 쿼리할 모든 호스트 IP 주소를 추가해야 합니다.

데이터베이스 액세스를 활성화하려면

액세스: Admin

-
- 단계 1** 방어 센터에서 **System > Local > Configuration**(시스템 > 로컬 > 컨피그레이션)을 선택합니다.
- 단계 2** **Database**(데이터베이스)를 클릭합니다.
Database Settings(데이터베이스 설정) 메뉴가 나타납니다.
- 단계 3** **Allow External Database Access**(외부 데이터베이스 액세스 허용) 확인란을 선택합니다.
Access List(액세스 목록) 필드가 나타납니다.
- 단계 4** 서드파티 애플리케이션 요건에 따라 방어 센터의 FQDN(정규화된 도메인 이름) 또는 IPv4 주소를 **Server Hostname**(서버 호스트 이름) 필드에 입력합니다. IPv6 주소를 사용하여 인증서를 설치하는 것이 불가하므로 IPv6 주소는 사용할 수 없습니다.
FQDN을 입력할 경우 클라이언트가 방어 센터의 FQDN을 확인할 수 있도록 해야 합니다. IP 주소를 입력하는 경우 클라이언트가 IP 주소를 사용하여 방어 센터에 연결할 수 있도록 해야 합니다.
- 단계 5** 하나 이상의 IP 주소에 대한 데이터베이스 액세스를 추가하려면 **Add Hosts**(호스트 추가)를 클릭합니다.
Access List(액세스 목록) 필드에 **IP Address**(IP 주소) 필드가 나타납니다.
- 단계 6** 추가할 IP 주소에 따라 **IP Address**(IP 주소) 필드에 다음을 입력할 수 있습니다.
- 정확한 IPv4 주소(예: 192.168.1.101)
 - 정확한 IPv6 주소(예: 2001:DB8::4)
 - CIDR 표기법을 사용한 IP 주소 범위(예: 192.168.1.1/24)
 - FireSIGHT System에서 CIDR 사용에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*의 IP 주소 명명법을 참조하십시오.
 - any - 임의의 IP 주소 지정
- 단계 7** **Add**(추가)를 클릭합니다.
IP 주소가 데이터베이스 액세스 목록에 추가됩니다.
- 단계 8** 선택적으로, 데이터베이스 액세스 목록에서 항목을 제거하려면 삭제 아이콘()을 클릭합니다.
- 단계 9** **Save**(저장)를 클릭합니다.
데이터베이스 액세스 설정이 저장됩니다.
- 단계 10** 다음 [JDBC 드라이버 다운로드](#) 섹션에서 절차를 계속 진행합니다.
-

JDBC 드라이버 다운로드

라이선스: 모두

External Database 사용자를 생성한 후에는 방어 센터가 데이터베이스 액세스를 허용하도록 구성하고, JDBC 드라이버를 클라이언트 시스템에 다운로드합니다. 이 JDBC 드라이버를 사용하여 데이터베이스에 연결해야 합니다.

JDBC 드라이버를 다운로드하려면

액세스: Admin

-
- 단계 1** 방어 센터에서 **System > Local > Configuration**(시스템 > 로컬 > 컨피그레이션)을 선택합니다.
- 단계 2** **Database**(데이터베이스)를 클릭합니다.
Database Settings(데이터베이스 설정) 메뉴가 나타납니다.
- 단계 3** **Client JDBC Driver**(클라이언트 JDBC 드라이버) 옆에 있는 **Download**(다운로드)를 클릭하고 브라우저의 지시에 따라 **client.zip** 패키지를 다운로드합니다.
- 단계 4** ZIP 패키지의 압축을 풉니다. 위치에 유의합니다.
패키지의 파일 구조를 유지해야 합니다.
드라이버는 다른 파일과 함께 ZIP 파일(**client.zip**)에 패키지화됩니다. 패키지에는 다음 디렉토리가 포함됩니다.
- **bin** - RunQuery라는 샘플 클라이언트는 물론, 클라이언트와 방어 센터 간의 암호화된 통신을 위해 인증서를 설치하는 데 사용하는 실행 파일이 포함됨
 - **lib** - JDBC 드라이버 JAR 파일이 포함됨
 - **src** - bin 디렉토리의 실행 파일에 대한 소스 코드가 포함됨
- 단계 5** 다음 **클라이언트 SSL 인증서 설치** 섹션에서 절차를 계속 진행합니다.
-

클라이언트 SSL 인증서 설치

JDBC 드라이버를 다운로드한 후에는 Cisco에서 제공한 InstallCert라는 프로그램을 사용하여 방어 센터에서 SSL 인증서를 승인하고 설치합니다. 클라이언트 시스템과 방어 센터는 SSL 인증서 인증을 통해 안전하게 통신을 수행합니다. 인증서를 승인하면 해당 인증서는 현재 JRE를 실행 중인 **security** 디렉토리의 키 저장소(**jssecacerts**)에 추가됩니다.

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

다음은 각각 Microsoft Windows 및 UNIX를 실행 중인 컴퓨터의 일반적인 키 저장소 위치를 나타냅니다.

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

**참고**

데이터베이스 액세스 함수에 액세스하려는 Java 쿼리 애플리케이션이 다른 JRE를 사용할 경우, 키 저장소를 다른 JRE의 **security** 디렉토리에 복사해야 합니다.

InstallCert를 사용하여 SSL 인증서를 설치하려면

-
- 단계 1** 컴퓨터에서 명령행 인터페이스를 엽니다.
- 단계 2** 명령 프롬프트에서 ZIP 패키지의 압축을 풀었을 때 생성된 **bin** 디렉토리로 변경합니다.
- 단계 3** 방어 센터의 SSL 인증서를 설치하려면 다음을 입력하고 Enter 키를 누릅니다.

```
java InstallCert defense_center
```

defense_center는 방어 센터의 FQDN 또는 IP 주소입니다. InstallCert는 IPv6 주소를 지원하지 않습니다. IPv6 네트워크에 있는 경우, 확인 가능한 호스트 이름을 사용해야 합니다.

Microsoft Windows를 실행 중인 컴퓨터의 출력은 아래 예와 유사합니다.

```

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

```

인증서를 확인하라는 메시지가 표시됩니다.

단계 4 선택에 따라 인증서를 봅니다.

인증서를 승인하라는 메시지가 표시됩니다.

단계 5 인증서를 승인합니다.

인증서가 승인되며, Microsoft Windows를 실행 중인 컴퓨터의 출력은 다음 예와 유사하게 표시됩니다.

```

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

```

Crystal Reports를 사용하려는 경우, 키 저장소(jssecacerts)의 위치에 유의하십시오. 나중에 이 정보가 필요합니다.

단계 6 다음과 같은 옵션이 있습니다.

- 서드파티 애플리케이션이 있는 경우, 다음 [서드파티 애플리케이션을 사용하여 데이터베이스에 연결, 페이지 2-6](#) 섹션에서 절차를 계속 진행합니다.
- 맞춤형 애플리케이션이 있는 경우, 맞춤형 프로그램을 사용하여 데이터베이스에 연결, [페이지 2-8](#)의 절차를 계속 진행합니다.

서드파티 애플리케이션을 사용하여 데이터베이스에 연결

인증서를 설치한 후에는 JDBC SSL 연결을 지원하는 모든 서드파티 클라이언트를 사용하여 방어 센터에서 데이터베이스를 쿼리할 수 있습니다. 다음 표에는 클라이언트와 방어 센터 간에 연결을 구성하는 데 필요할 수 있는 정보가 나열되어 있습니다.

표 2-2 데이터베이스 액세스 클라이언트에 대한 연결 정보

정보	설명
JDBC URL	<p>다음 JDBC URL은 Cisco 데이터베이스를 식별하여 클라이언트의 JDBC 드라이버가 이에 대한 연결을 설정할 수 있도록 합니다.</p> <pre> jdbc:vjdbc:rmi://defense_center:2000/VJdbc,eqe </pre> <p>defense_center는 방어 센터의 FQDN 또는 IP 주소입니다.</p>
JDBC 드라이버 JAR 파일	<p>Cisco 데이터베이스에 대한 연결을 구성할 경우 다음 JAR 파일을 사용해야 합니다.</p> <ul style="list-style-type: none"> • vjdbc.jar • commons-logging-1.1.jar <p>이러한 파일은 JDBC 드라이버 다운로드, 페이지 2-4에 설명된 대로, client.zip 파일의 압축을 푼 위치인 lib 하위 디렉토리에 있습니다.</p>

표 2-2 데이터베이스 액세스 클라이언트에 대한 연결 정보(계속)

정보	설명
JDBC 드라이버 클래스	Cisco 데이터베이스에 대한 연결을 구성할 경우 다음 드라이버 클래스를 사용해야 합니다. com.sourcefire.vjdbc.VirtualDriver
사용자 이름 및 비밀번호	어플라이언스의 데이터베이스에 연결하려면 External Database User 권한이 있는 사용자 어카운트를 사용합니다. 자세한 내용은 데이터베이스 사용자 어카운트 생성, 페이지 2-2 을(를) 참고하십시오.

다음 섹션에는 널리 알려진 3가지 업계 표준 보고 툴을 사용하여 Cisco 데이터베이스에 연결하는 방법에 대한 팁이 포함되어 있습니다. 이러한 툴 중 하나를 사용하거나 다른 Java 기반 애플리케이션을 사용하는 경우와 상관없이, JDBC SSL 연결을 생성하는 방법에 대한 자세한 지침을 보려면 해당 보고 툴의 설명서를 참조해야 합니다.

Crystal Reports

다음 내용은 32비트 Windows 환경에 Crystal Reports 2011을 설치하는 경우에 적용됩니다. 64비트 Windows 환경을 실행 중인 경우 파일 경로가 다를 수 있습니다.

Crystal Reports 2011을 사용하여 Cisco 데이터베이스에 연결하려면 다음 작업을 수행해야 합니다.

- 방어 센터에서 다운로드한 JDBC 드라이버 JAR 파일을 Crystal Reports 클래스 경로에 추가합니다. Crystal Reports를 기본 설치한다고 가정할 경우, 다음 파일에서 클래스 경로 섹션을 편집할 수 있습니다.

```
C:\Program Files\SAP BusinessObjects\SAP Business Objects
Enterprise XI 4.0\Java\CRConfig.xml
```

- 클라이언트 SSL 인증서를 설치했을 때 생성된 키 저장소를 해당하는 Crystal Reports 보안 디렉토리에 복사합니다. Crystal Reports를 기본 설치한다고 가정할 경우, 해당 디렉토리는 다음과 같습니다.

```
C:\Program Files\SAP BusinessObjects\SAP Business Objects
Enterprise XI 4.0\win32_x86\jdk\jre\lib\security
```

- Cisco를 데이터베이스 이름으로 사용하여 Database Expert에 새 JDBC(JNDI) 연결을 생성합니다.

JasperSoft iReport

iReport가 Cisco 데이터베이스에 연결하도록 허용하려면 다음 작업을 수행해야 합니다.

- 방어 센터에서 다운로드한 JDBC 드라이버 JAR 파일을 iReport 클래스 경로에 추가합니다.
- 방어 센터에서 다운로드한 JDBC 드라이버 JAR 파일을 사용하여 새 JDBC 드라이버를 추가합니다. 드라이버 파일을 추가하면 iReport는 올바른 드라이버 종류를 찾아야 합니다.
- 방금 생성한 드라이버를 사용하여 새 데이터베이스 연결을 생성합니다.

Actuate BIRT

BIRT가 Cisco 데이터베이스에 연결하도록 허용하려면 다음 작업을 수행해야 합니다.

- **Generic JDBC Driver** 템플릿을 사용하여 드라이버 정의를 추가합니다.
- **Generic JDBC** 프로필 유형을 사용하여 새 데이터베이스 연결을 생성합니다.
- **JDBC Data Source** 데이터 소스 유형을 사용하여 보고서에 대한 데이터 소스를 생성합니다.



정보

새 JDBC 데이터 소스 프로필을 생성할 때 Cisco 드라이버 클래스를 선택할 수 없는 경우, 방어 센터에서 다운로드한 JDBC 드라이버 JAR 파일을 사용하여 드라이버를 추가합니다.

맞춤형 프로그램을 사용하여 데이터베이스에 연결

인증서를 설치한 후에는 맞춤형 Java 보고 툴을 활성화하여 Cisco 데이터베이스를 쿼리할 수 있습니다. Cisco에서는 RunQuery라는 샘플 Java 명령행 애플리케이션을 제공하며 이는 방어 센터와 함께 제공된 JDBC 드라이버를 사용하여 필요한 SSL 연결을 설정합니다. RunQuery는 테이블 레코드 및 테이블 메타데이터 두 가지를 모두 검색합니다. 소스 코드는 방어 센터에서 다운로드한 ZIP 패키지의 src 디렉토리에 포함되어 있습니다. [JDBC 드라이버 다운로드, 페이지 2-4](#)을(를) 참조하십시오.



참고

RunQuery는 샘플 클라이언트 전용이며, 완전한 기능을 제공하는 보고 툴이 **아닙니다**. Cisco에서는 데이터베이스 쿼리 시 이를 기본 방법으로 사용하는 것을 **강력하게** 권장합니다. RunQuery 사용에 대한 정보를 보려면 ZIP 패키지에 포함된 README 파일을 참조하십시오.

맞춤형 프로그램을 사용하여 데이터베이스에 연결하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- [맞춤형 Java 프로그램의 소스 코드, 페이지 2-8](#)에서는 RunQuery 애플리케이션이 데이터베이스 연결을 설정하고 쿼리를 제출하는 데 사용하는 Java 클래스 및 메서드에 대해 설명합니다.
- [애플리케이션 실행, 페이지 2-9](#)에서는 Java 애플리케이션을 실행하는 데 필요한 환경 요건에 대해 설명합니다.

맞춤형 Java 프로그램의 소스 코드

RunQuery 소스 코드는 아래에 설명된 함수를 사용합니다. 이러한 코드 샘플은 몇 가지 가능한 구현 접근 방식 중 하나를 설명합니다.

SSL 공급자 연결을 동적으로 설정

SSL 보안 인증서를 클라이언트에 설치하면([클라이언트 SSL 인증서 설치, 페이지 2-5](#) 참조), 프로그램에서 아래 행을 사용하여 JSSE 공급자를 동적으로 등록할 수 있습니다.

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

프로그램의 JDBC 드라이버 초기화

다음과 같이 `Class.forName()` 메서드를 사용하여 Java 애플리케이션에서 JDBC 드라이버 클래스를 로드할 수 있습니다.

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

명령행에서 프로그램이 실행된 경우, 사용자는 다음과 같이 JDBC 클래스를 제공합니다.

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

`program_name`은 프로그램의 이름입니다.

데이터베이스에 프로그램 연결

프로그램이 쿼리를 제출하려면 우선 JDBC 연결 개체를 가져와야 합니다. 다음과 같이 `DriverManager.getConnection` 메서드를 사용하여 연결을 설정하고 연결 개체를 가져옵니다.

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

`my_dc`는 방어 센터의 FQDN 또는 IP 주소이고, `user`는 데이터베이스 액세스 사용자 어카운트 이름, `password`는 어카운트 비밀번호입니다.

Cisco 테이블의 데이터 쿼리

다음과 같이 SQL 쿼리 개체를 생성하여 쿼리를 제출하고 검색된 레코드를 결과 집합에 할당할 수 있습니다.

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

`sql`은 SQL 쿼리입니다. 지원되는 SQL 함수에 대한 내용은 [데이터베이스 쿼리, 페이지 2-10](#)을(를) 참조하십시오.

테이블 쿼리의 결과 생성

위 쿼리에서 생성된 결과 집합(`rs`)을 사용하여 다음과 같이 필드를 출력할 수 있습니다.

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

스키마 정보 가져오기

프로그램은 데이터베이스의 테이블을 다음과 같이 나열할 수 있습니다.

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

프로그램은 테이블의 열을 다음과 같이 나열할 수 있습니다.

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

`table_name`은 데이터베이스 테이블의 이름입니다.

애플리케이션 실행

애플리케이션을 실행하기 전에 클라이언트 컴퓨터의 `CLASSPATH`에 현재 디렉토리 및 애플리케이션의 JAR 파일 위치가 포함되도록 설정해야 합니다.

[JDBC 드라이버 다운로드, 페이지 2-4](#)에 설명된 대로 Database Access에 대한 ZIP 패키지를 다운로드하고 압축을 푼 경우, `CLASSPATH`를 다음과 같이 업데이트합니다.

Unix 환경에서 애플리케이션을 실행하려면

단계 1 다음 명령을 사용합니다.

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

*path*는 방어 센터에서 다운로드한 ZIP 패키지의 압축을 풀 디렉토리 경로입니다.

Windows 7 환경에서 애플리케이션을 실행하려면

단계 1 Computer(컴퓨터) 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **System(속성)**을 선택합니다.

System(시스템) 창이 나타납니다.

단계 2 **Advanced System Settings(고급 시스템 설정)**를 클릭합니다.

System Properties(시스템 속성) 창이 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

단계 4 **Environment Variables...(환경 변수...)**를 클릭합니다.

Environment Variables(환경 변수) 창이 나타납니다.

단계 5 **CLASSPATH** 시스템 변수를 선택하고 **Edit...(편집...)**를 클릭합니다.

Edit System Variable(시스템 변수 편집) 창이 나타납니다.

단계 6 **Variable value:(변수 값):** 필드에 다음을 추가합니다.

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

*path*는 방어 센터에서 다운로드한 ZIP 패키지의 압축을 풀 디렉토리 경로입니다.

단계 7 **OK(확인)**를 클릭하여 값을 저장합니다.

Environment Variables(환경 변수) 창이 나타납니다.

단계 8 **OK(확인)**를 클릭하여 값을 저장합니다. 이제 애플리케이션을 실행할 수 있습니다.

데이터베이스 쿼리

다음 섹션에는 지원되는 쿼리 구문 및 쿼리와 관련한 중요한 요건 및 제한에 대한 정보가 포함되어 있습니다.

- 지원되는 **SHOW 명령 구문**, 페이지 2-11에서는 Cisco 데이터베이스 쿼리에 지원되는 MySQL **SHOW** 명령 구문에 대해 설명합니다.
- 지원되는 **DESCRIBE 또는 DESC 명령 구문**, 페이지 2-11에서는 Cisco 데이터베이스 쿼리에 지원되는 MySQL **DESCRIBE** 명령 구문에 대해 설명합니다.
- 지원되는 **SELECT 명령 구문**, 페이지 2-12에서는 Cisco 데이터베이스 쿼리에 지원되는 MySQL **SELECT** 명령 구문에 대해 설명합니다.
- **조인 제한**, 페이지 2-13에서는 Cisco 데이터베이스 쿼리에 지원되는 조인에 대해 설명하고 테이블에 허용되는 특정 조인에 대한 정보를 얻을 수 있는 방법을 설명합니다.
- **생소한 형식으로 저장된 데이터 쿼리**, 페이지 2-13에서는 생소한(예: UNIX 타임스탬프 및 IP 주소) 형식으로 저장된 데이터에 쿼리를 수행하여 쿼리를 성공적으로 수행하고, 원하는 대로 결과를 표시하는 방법에 대해 설명합니다.

- 성능상의 이유로 쿼리 제한, 페이지 2-15에는 FireSIGHT System의 성능을 저하하지 않기 위한 쿼리의 권장 사항 및 제한이 포함되어 있습니다.
- 쿼리 팁, 페이지 2-16에는 여러 어플라이언스 간에 침입 이벤트를 쿼리하는 방법에 대한 팁이 포함되어 있습니다.

스키마 및 허용되는 조인에 대한 내용은 다음 장을 참조하십시오.

- 스키마: 시스템 레벨 테이블, 페이지 3-1
- 스키마: 침입 테이블, 페이지 4-1
- 스키마: 통계 추적 테이블, 페이지 5-1
- 스키마: 검색 이벤트 및 네트워크 맵 테이블, 페이지 6-1
- 스키마: 연결 로그 테이블, 페이지 7-1
- 스키마: 사용자 작업 테이블, 페이지 8-1
- 스키마: 상관관계 테이블, 페이지 9-1

지원되는 SHOW 명령 구문

SHOW 문은 Cisco 데이터베이스의 모든 테이블을 나열합니다. 다음은 Cisco 데이터베이스를 쿼리할 때 사용할 수 있는 지원되는 MySQL SHOW 명령 구문을 나타냅니다.

```
SHOW TABLES;
```

위에 나열되지 않은 SHOW 명령 구문은 지원되지 않습니다.

지원되는 DESCRIBE 또는 DESC 명령 구문

Cisco 데이터베이스에서는 DESCRIBE 문을 제한적으로 사용할 수 있도록 합니다. Cisco 데이터베이스에서 DESCRIBE 문의 출력에서는 열의 이름 및 각 열의 데이터 유형만 나열합니다. 다음은 Cisco 데이터베이스를 쿼리할 때 사용할 수 있는 지원되는 MySQL DESCRIBE 명령 구문을 나타냅니다.

```
DESCRIBE table_name;
```

Cisco 데이터베이스는 동일한 명령인 DESC도 지원합니다.

```
DESC table_name;
```

표 2-3 지원되는 DESCRIBE 명령 구문

항목	설명
table_name	쿼리하려는 테이블의 이름

위에 나열되지 않은 DESCRIBE 명령 구문은 지원되지 않습니다. 특히, FireSIGHT System 데이터베이스 액세스 기능은 지원되지 않습니다.

- INDEX FOR 절
- TABLE 절
- PROCEDURE 절

지원되는 SELECT 명령 구문

다음은 Cisco 데이터베이스를 쿼리할 때 사용할 수 있는 지원되는 MySQL SELECT 명령 구문을 나타냅니다.

```
SELECT
[ALL | DISTINCT]

select_expr [,select_expr ...]

FROM table_references

[WHERE where_condition]

[GROUP BY { column_name | position } [ ASC | DESC ], ...]

[HAVING where_condition]

[ORDER BY { column_name | position } [ ASC | DESC ], ...]

[LIMIT { [offset,] row_count | row_count OFFSET offset}]
```

다음 표에는 위에 언급한 SELECT 문의 절 및 인수에 대한 필수 구문이 자세히 설명되어 있습니다.

표 2-4 지원되는 SELECT 명령 구문

항목	설명
select_expr	{column_name [[AS] alias] function(...)[[AS] alias] aggregate_function(...)[[AS] alias]}
column_name	쿼리하려는 필드의 이름
function	{ABS CAST CEILING CHAR_LENGTH COALESCE CONV CHARACTER_LENGTH CONCAT CONVERT CURRENT_DATE CURRENT_TIME CURRENT_TIMESTAMP EXTRACT FLOOR HEX INET_ATON INET_NTOA INET6_ATON INET6_NTOA LEFT LOWER LPAD MID MOD NULLIF OCTET_LENGTH POSITION RIGHT ROUND SUBSTRING SYSDATE TIME TIMESTAMP TRIM UPPER}
aggregate_function	{AVG COUNT COUNT(DISTINCT) MAX MIN SUM}
table_references	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> table_reference INNER JOIN table_reference join_condition table_reference LEFT [OUTER] JOIN table_reference join_condition
table_reference	table_name [[AS] alias]
table_name	쿼리하려는 테이블의 이름
join_condition	ON conditional_expr
conditional_expr	조인이 호환 가능한 필드 간의 동등 비교입니다. 자세한 내용은 조인 제한, 페이지 2-13 을 참조하십시오.
where_condition	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> IS NULL or IS NOT NULL NOT, ! BETWEEN ... AND ... LIKE =, !=, <>, >, >=, <, <=

지원되는 MySQL 구문이 어떻게 표현되는지 잘 모르는 경우, 다음 표에서 팁을 참조하십시오.

표 2-5 MySQL 구문 형식

기호	모양	의미
대괄호	[]	선택적인 절 또는 인수
중괄호	{ }	필수 절 또는 인수
세로 막대		절 또는 인수 간의 선택 항목

위에 나열되지 않은 SELECT 명령 구문은 지원되지 않습니다. 특히, FireSIGHT System 데이터베이스 액세스 기능은 지원되지 않습니다.

- SELECT * - 명시적으로 지정해야 하는 필드
- union
- subquery
- GROUP BY 절에 대한 WITH ROLLUP 수정자
- INTO 절
- FOR UPDATE 절

조인 제한

성능 및 기타 실질적인 이유로 인해 Cisco 데이터베이스 테이블에서 수행할 수 있는 조인은 제한되어 있습니다. 결과가 이벤트 분석에 유용하지 않을 경우 Cisco에서는 조인을 수행할 수 있도록 허용하지 않습니다.

Inner 조인 및 Left(Outer) 조인만 수행할 수 있습니다. Nested 조인, Cross 조인, Natural 조인, Right(Outer) 조인, Full(Outer) 조인 및 USING 절이 포함된 조인은 지원되지 않습니다.

스키마 문서는 각 테이블에 지원되는 조인을 나타냅니다. 나열되지 않은 조인은 지원되지 않습니다. 예를 들어, IP 주소 필드의 `compliance_event` 및 `intrusion_event` 테이블 모두에 IP 주소 정보가 포함된 경우에도 해당 테이블은 조인할 수 없습니다. 또한 사용 중단된 테이블 및 사용 중단된 필드의 조인은 나열되지 않았습니다.

생소한 형식으로 저장된 데이터 쿼리

Cisco 데이터베이스는 쉽게 알아보기 힘든 형식으로 일부 데이터를 저장하는 경우가 있습니다. 다음 섹션은 다양한 필드에 쿼리를 수행하여 쿼리를 성공적으로 수행하고 원하는 대로 결과를 표시하는 방법을 자세히 설명합니다.

- IPv6 주소, 페이지 2-14
- IPv4 주소, 페이지 2-14
- MAC 주소, 페이지 2-14
- 패킷 데이터, 페이지 2-14
- UNIX 타임스탬프, 페이지 2-14


```
SELECT FROM_UNIXTIME(action_time_sec), user, message
FROM audit_log
LIMIT 0, 25;
```

데이터베이스의 모든 시간은 UTC로 제공됩니다. `CONVERT_TZ()` 함수를 사용할 수 있긴 하지만 결과는 UTC로만 제공됩니다.

일부 이벤트에는 이와 관련된 마이크로초 해상도가 포함됩니다. `CONCAT()` 및 `LPAD()` 함수를 사용하여 UNIX 타임스탬프와 마이크로초 증가를 연결합니다. 예를 들어, 다음 문은 `intrusion_event` 테이블을 쿼리합니다.

```
SELECT CONCAT(FROM_UNIXTIME(event_time_sec), '.', LPAD (event_time_usec, 6, '0')),
HEX(host_id),
rule_message
FROM intrusion_event
LIMIT 0, 25;
```

특정 UNIX 타임스탬프가 포함된 이벤트의 데이터베이스를 쿼리하려면 `UNIX_TIMESTAMP()` 함수를 사용합니다.

성능상의 이유로 쿼리 제한

Cisco 데이터베이스 테이블에서 수행할 수 있는 조인은 제한되어 있으나, 부담이 큰 몇 가지 쿼리를 계속 사용할 수는 있습니다. 이러한 쿼리는 방어 센터의 성능을 저하시킬 수 있습니다.

따라서 대용량 테이블의 결과 집합을 제한해야 합니다. 이를 위한 전략은 다음과 같습니다.

- 특정 시간 범위에 대한 쿼리 제한
- IP 주소를 기준으로 쿼리 제한
- `LIMIT` 절 사용

구축 방식에 따라, 많은 테이블을 쿼리할 경우 제한된 결과 집합이 필요할 수 있습니다. 특히, 다음 테이블에는 DC3000에 대한 최대 1억 개의 이벤트를 포함할 수 있습니다.

- `fireamp_event`
- `intrusion_event`
- `intrusion_event_packet`
- `connection_log` (5.0 이전 버전 이름: `rna_flow`)
- `connection_summary` (5.0 이전 버전 이름: `rna_flow_summary`)

모니터링되는 네트워크에서 탐지된 호스트 수에 따라, 네트워크 맵 테이블의 쿼리는 부담이 클 수도 있습니다.

쿼리 팁

다음 섹션에서는 탐지 엔진 또는 침입 이벤트를 포함하는 쿼리를 구축할 경우 고유한 결과를 얻을 수 있는 방법에 대한 팁을 제공합니다.

디바이스 이름

여러 방어 센터에서는 디바이스 이름이 반드시 고유하지 않아도 됩니다. 고유함을 유지하려면 쿼리에 특정 디바이스 UUID를 포함합니다.

침입 이벤트

여러 개의 관리되는 디바이스 전체에서 침입 이벤트가 고유하게 일치하도록 하려면 `intrusion_event` 테이블의 쿼리에 다음 필드를 포함합니다.

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

샘플 쿼리

다음 섹션에는 데이터베이스 액세스 기능을 사용할 수 있는 방법을 나타내는 샘플 쿼리가 포함되어 있습니다.

- [사용자의 감사 레코드, 페이지 2-16](#)
- [우선순위 및 분류를 기준으로 한 침입 이벤트, 페이지 2-17](#)
- [침입 이벤트 및 관련 정책, 페이지 2-17](#)
- [탐지된 호스트 목록, 페이지 2-17](#)
- [탐지된 서버 목록, 페이지 2-17](#)
- [네트워크의 서버 취약성, 페이지 2-18](#)
- [운영 체제 요약, 페이지 2-18](#)
- [호스트의 운영 체제 취약성, 페이지 2-18](#)
- [호스트 위반 카운트, 페이지 2-19](#)



주의

구축 방식에 따라, 이러한 샘플 쿼리를 실행하는 작업은 부담이 클 수 있습니다. 자세한 내용은 [성능상의 이유로 쿼리 제한, 페이지 2-15](#)을(를) 참조하십시오.

사용자의 감사 레코드

다음 쿼리는 특정 사용자의 감사 로그에 있는 모든 레코드를 반환하며, 모든 타임스탬프는 UTC로 표시됩니다.

```
SELECT FROM_UNIXTIME(action_time_sec), user, message
FROM audit_log
WHERE user = 'eventanalyst';
```

우선순위 및 분류를 기준으로 한 침입 이벤트

다음 쿼리는 Events By Priority and Classification(우선순위 및 분류별 이벤트) 워크플로우의 Drilldown of Event, Priority, and Classification(이벤트, 우선순위, 분류 드릴다운) 보기를 복제합니다. 사용자 환경 설정에서 기본 Intrusion Events(침입 이벤트) 워크플로우를 변경하지 않은 경우, 이는 방어 센터 웹 인터페이스에서 **Analysis > Intrusion Events**(분석 > 침입 이벤트)를 선택했을 때 표시되는 첫 번째 페이지입니다.

```
SELECT rule_message, priority, rule_classification, count(*) as Count
FROM intrusion_event
WHERE reviewed="0" GROUP BY rule_message, priority, rule_classification
ORDER BY Count
DESCLIMIT 0, 25;
```

침입 이벤트 및 관련 정책

다음 쿼리는 지정된 주의 침입 이벤트를 나열합니다. 각 이벤트에 대해 관련 침입 정책 위반 및 규칙 분류가 표시됩니다.

```
SELECT FROM_UNIXTIME(event_time_sec) AS event_time, event_id AS intrusion_event,
intrusion_event_policy_name AS policy, rule_classification AS classification
FROM intrusion_event
WHERE event_time_sec BETWEEN UNIX_TIMESTAMP('2011-10-01 00:00:00') AND
UNIX_TIMESTAMP('2011-10-07 23:59:59')
ORDER BY policy ASC;
```

탐지된 호스트 목록

다음 쿼리는 네트워크에서 탐지된 모든 MAC 호스트(IP 주소가 없는 호스트)의 호스트 네트워크 맵에 있는 기본 정보를 반환하며, 각 NIC의 하드웨어 공급업체도 함께 포함됩니다.

```
SELECT HEX(mac_address), mac_vendor, host_type, FROM_UNIXTIME(last_seen_sec)
FROM rna_mac_host;
```

다음 쿼리는 IP 주소를 MAC 주소로 매핑합니다.

```
SELECT HEX(ipaddr), HEX(mac_address), HEX(host_id)
FROM rna_host_ip_map LEFT JOIN rna_host_mac_map on
rna_host_ip_map.host_id=rna_host_mac_map.host_id;
```

탐지된 서버 목록

다음 쿼리는 두 개의 관련 테이블을 조인하여 네트워크에서 탐지된 서버 목록과 함께 여러 해당 특성을 제공하며, 이는 방어 센터 웹 인터페이스의 서버 테이블 보기에 표시되는 항목과 유사합니다.

```
SELECT FROM_UNIXTIME(s.last_used_sec), HEX(s.host_id), s.port, s.protocol, s.hits,
i.service_name, i.vendor, i.version, i.source_type, s.confidence
FROM AS s
```

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

이 쿼리는 Database Access의 요구 사항에 따라 `host_id`, `port`, `protocol`에 대한 테이블을 대상으로 Left 조인을 수행합니다. 참조: [rna_host_service 조인, 페이지 6-33](#) 및 [rna_host_service_info 조인, 페이지 6-38](#)

네트워크의 서버 취약성

다음 쿼리는 두 개의 취약성 관련 테이블을 조인하여 특정 호스트에 대해 탐지된 유효한 서버 관련 취약성 목록을 제공하며, 네트워크 전반에서 각 취약성이 악용될 수 있는지 여부도 포함됩니다.

```
SELECT h.rna_vuln_id, v.title, v.remote
FROM rna_host_service_vulns AS h
LEFT JOIN rna_vuln AS v ON (h.rna_vuln_id = v.rna_vuln_id)
WHERE h.ip_address = INET_ATON('10.10.10.4')
AND h.invalid = 0;
```

이 쿼리는 [rna_host_service_vulns, 페이지 6-43](#) 및 [rna_vuln 조인, 페이지 6-54](#)의 요구 사항에 따라 `rna_vuln_id`에 대한 테이블을 대상으로 Left 조인을 수행합니다.

운영 체제 요약

다음 쿼리는 Operating System Summary(운영 체제 요약) 워크플로우의 Summary of OS Names(OS 이름 요약) 페이지를 복제합니다. 사용자 환경 설정에서 기본 워크플로우를 변경하지 않은 경우, 이는 방어 센터 웹 인터페이스에서 **Analysis > Hosts**(분석 > 호스트)를 선택한 다음 **Hosts**(호스트)를 선택했을 때 표시되는 첫 번째 페이지입니다.

```
SELECT vendor, product, count(*) AS total
FROM rna_host_os
GROUP BY vendor, product
ORDER BY total DESC;
```

호스트의 운영 체제 취약성

다음 쿼리는 두 개의 취약성 관련 테이블을 조인하여 특정 호스트에 대해 탐지된 유효한 운영 체제 관련 취약성 목록을 제공하며, 네트워크 전반에서 각 취약성이 악용될 수 있는지 여부도 포함됩니다.

```
SELECT h.rna_vuln_id, v.title, v.remote
FROM rna_host_os_vulns AS h
LEFT JOIN rna_vuln AS v ON (h.rna_vuln_id = v.rna_vuln_id)
WHERE h.host_id = UNHEX('9610B6E6F1784DA4B39BEA7A210AAD68')
AND h.invalid = 0;
```

이 쿼리는 Database Access의 요구 사항에 따라 `rna_vuln_id`에 대한 테이블을 대상으로 Left 조인을 수행합니다. 참조: [rna_host_os_vulns, 페이지 6-28](#) 및 [rna_vuln 조인, 페이지 6-54](#)

호스트 위반 카운트

다음 쿼리는 Host Violation Count(호스트 위반 카운트) 워크플로우의 Host Violation Count(호스트 위반 카운트) 페이지를 복제합니다. 사용자 환경 설정에서 기본 Compliance White List Violations(규정준수 화이트리스트 위반) 워크플로우를 변경하지 않은 경우, 이는 방어 센터 웹 인터페이스에서 **Analysis > Correlation > White List Violations**(분석 > 상관관계 > 화이트리스트 위반)를 선택했을 때 표시되는 첫 번째 페이지입니다.

```
SELECT host_id, HEX(host_id), white_list_name, count(*) AS total
FROM white_list_violation
GROUP BY host_id, white_list_name
ORDER BY total DESC;
```

■ 샘플 쿼리



스키마: 시스템 레벨 테이블

이 장에는 시스템 레벨 기능(감사, 어플라이언스 상태 모니터링, 악성코드 탐지, 보안 업데이트 로깅 등)의 스키마 및 지원되는 조인에 대한 정보가 포함되어 있습니다.

자세한 내용은 아래 표에 나열된 섹션을 참조하십시오.

표 3-1 시스템 레벨 테이블의 스키마

참조	다음에 대한 정보가 저장되는 테이블	버전
audit_log , 페이지 3-1	어플라이언스의 웹 인터페이스와의 사용자 상호 작용	4.10.x+
fireamp_event , 페이지 3-2	FireAMP 악성코드 탐지 및 격리 이벤트	5.1+
health_event , 페이지 3-8	모니터링되는 어플라이언스의 상태 이벤트	4.10.x+
sru_import_log , 페이지 3-10	어플라이언스로 가져온 규칙 업데이트	5.0+

audit_log

`audit_log` 테이블에는 웹 인터페이스와의 FireSIGHT System 사용자 상호 작용에 대한 정보가 포함됩니다. 감사 로그는 관리되는 어플라이언스가 아닌 로컬 어플라이언스에 대한 레코드만 저장합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [audit_log 필드](#), 페이지 3-1
- [audit_log 조인](#), 페이지 3-2
- [audit_log 샘플 쿼리](#), 페이지 3-2

audit_log 필드

다음 표에는 `audit_log` 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 3-2 `audit_log` 필드

필드	설명
<code>action_time_sec</code>	어플라이언스가 감사 레코드를 생성한 날짜 및 시간의 UNIX 타임스탬프입니다.
<code>message</code>	사용자가 수행한 작업입니다.
<code>source</code>	웹 인터페이스 사용자의 호스트 IP 주소이며, 점으로 구분된 십진수 명명법으로 표기합니다.

표 3-2 audit_log 필드(계속)

필드	설명
subsystem	감사 레코드를 생성하기 위해 사용자가 따른 메뉴 경로입니다.
user	감사 이벤트를 트리거한 사용자의 사용자 이름입니다.

audit_log 조인

audit_log 테이블에서는 조인을 수행할 수 없습니다.

audit_log 샘플 쿼리

다음 쿼리는 가장 최근의 로그 항목을 최대 25개까지 반환하며, 이는 시간을 기준으로 정렬됩니다.

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

fireamp_event

fireamp_event 테이블에는 악성코드 이벤트에 대한 정보가 포함됩니다. 이러한 이벤트에는 클라우드 내에서 탐지 또는 격리된 악성코드, 탐지 방법, 악성코드의 영향을 받은 호스트 및 사용자에 대한 정보가 포함됩니다. 새로운 필드는 이벤트를 트리거한 애플리케이션을 식별하고, 이벤트를 처리한 방법을 확인하고, 이벤트를 연결, 침입, 파일 이벤트와 상호 연결하기 위해 추가되었습니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [fireamp_event 필드, 페이지 3-2](#)
- [fireamp_event 조인, 페이지 3-8](#)
- [fireamp_event 샘플 쿼리, 페이지 3-8](#)

fireamp_event 필드

다음 표에는 fireamp_event 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 3-3 fireamp_event 필드

필드	설명
application_id	파일 전송을 수행하는 애플리케이션에 매핑되는 ID 번호입니다.
application_name	전송을 수행하는 애플리케이션의 이름입니다.

표 3-3 fireamp_event 필드(계속)

필드	설명
cert_valid_end_date	연결에 사용된 SSL 인증서의 유효 기간이 만료되는 날짜에 대한 Unix 타임스탬프입니다.
cert_valid_start_date	연결에 사용된 SSL 인증서가 발행된 날짜에 대한 Unix 타임스탬프입니다.
client_application_id	해당하는 경우, 클라이언트 애플리케이션의 내부 ID 번호입니다.
client_application_name	해당하는 경우, 클라이언트 애플리케이션의 이름입니다.
cloud_name	FireAMP 이벤트가 시작된 클라우드 서비스의 이름입니다. 각 cloud_name 값에는 관련 cloud_uuid 값이 포함됩니다.
cloud_uuid	FireAMP 이벤트가 시작된 클라우드 서비스의 고유한 내부 ID입니다. 각 cloud_uuid 값에는 관련 cloud_name 값이 포함됩니다.
connection_sec	악성코드 이벤트와 관련된 연결 이벤트의 UNIX 타임스탬프(00:00:00 01/01/1970 이후의 초)입니다.
counter	동일한 초에 발생한 여러 개의 이벤트를 구분하기 위해 사용되는 특정 이벤트 카운터입니다.
detection_name	탐지 또는 격리된 악성코드의 이름입니다.
detector_type	악성코드를 탐지한 탐지기입니다. 각 detector_type 값에는 관련 detector_type_id가 포함됩니다. 가능한 표시 값 및 관련 ID는 다음과 같습니다. <ul style="list-style-type: none"> • ClamAV — 128 • ETHOS — 8 • SPERO — 32 • SHA — 4 • Tetra — 64
detector_type_id	악성코드를 탐지한 탐지 기술의 내부 ID입니다. 각 detector_type_id 값에는 관련 detector_type 값이 포함됩니다. 가능한 표시 값 및 관련 유형은 다음과 같습니다. <ul style="list-style-type: none"> • 4 — SHA • 8 — ETHOS • 32 — SPERO • 64 — Tetra • 128 — ClamAV
direction	파일이 업로드되거나 다운로드되었는지 나타내는 값입니다. 다음과 같은 값을 사용할 수 있습니다. <ul style="list-style-type: none"> • Download • Upload 현재 이 값은 프로토콜에 따라 좌우됩니다(예: 연결이 HTTP인 경우 다운로드임).

표 3-3 fireamp_event 필드(계속)

필드	설명
disposition	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. <ul style="list-style-type: none"> CLEAN — 파일이 깨끗하고 악성코드가 포함되어 있지 않습니다. UNKNOWN — 파일에 악성코드가 포함되어 있는지 알 수 없습니다. MALWARE — 파일에 악성코드가 포함되어 있습니다. UNAVAILABLE — 소프트웨어가 처리를 위한 요청을 Cisco 클라우드에 전송하지 못했거나, Cisco 클라우드 서비스가 요청에 응답하지 않았습니다. CUSTOM SIGNATURE — 파일이 사용자가 정의한 해시와 일치하며, 사용자가 지정한 방식으로 처리됩니다.
dst_continent_name	목적지 호스트의 대륙 이름입니다. <ul style="list-style-type: none"> ** — 알 수 없음 na — 북미 as — 아시아 af — 아프리카 eu — 유럽 sa — 남미 au — 호주 an — 남극 대륙
dst_country_id	목적지 호스트의 국가 코드입니다.
dst_country_name	목적지 호스트의 국가 이름입니다.
dst_ip_address_v6	이 필드는 사용이 중단되었으며 이제부터는 null을 반환합니다.
dst_ipaddr	연결의 목적지에 대한 IPv4 또는 IPv6 주소를 이진수로 나타낸 값입니다.
dst_port	연결 목적지에 대한 포트 번호입니다.
endpoint_user	Cisco 클라우드에서 이벤트를 탐지한 경우, Cisco FireAMP 에이전트에서 사용자를 확인합니다. 이 사용자는 LDAP와 관련이 없으며 discovered_users 테이블에 표시되지 않습니다.
event_description	이벤트 유형과 관련된 추가 이벤트 정보입니다.
event_id	FireAMP 이벤트의 고유한 내부 ID입니다.
event_subtype	악성코드를 탐지하도록 유도한 작업입니다. 각 event_subtype 값에는 관련 event_subtype_id 값이 포함됩니다. 가능한 표시 값 및 관련 ID는 다음과 같습니다. <ul style="list-style-type: none"> Create — 1 Execute — 2 Move — 22 Scan — 4

표 3-3 fireamp_event 필드(계속)

필드	설명
event_subtype_id	<p>악성코드를 탐지하도록 유도한 작업의 내부 ID입니다. 각 event_subtype_id 값에는 관련 event_subtype 값이 포함됩니다. 가능한 표시 값 및 관련 하위 유형은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 1 — Create • 2 — Execute • 4 — Scan • 22 — Move
event_type	<p>FireAMP 이벤트의 유형입니다. 각 event_type 값에는 관련 event_type_id 값이 포함됩니다. 가능한 표시 값 및 관련 ID는 다음과 같습니다.</p> <ul style="list-style-type: none"> • Blocked Execution — 553648168 • Cloud Recall Quarantine — 553648155 • Cloud Recall Quarantine Attempt Failed — 2164260893 • Cloud Recall Quarantine Started — 553648147 • Cloud Recall Restore from Quarantine — 553648154 • Cloud Recall Restore from Quarantine Failed — 2164260892 • Cloud Recall Restore from Quarantine Started — 553648146 • FireAMP IOC — 1107296256 • Quarantine Failure — 2164260880 • Quarantined Item Restored — 553648149 • Quarantine Restore Failed — 2164260884 • Quarantine Restore Started — 553648150 • Scan Completed, No Detections — 554696715 • Scan Completed With Detections — 1091567628 • Scan Failed — 2165309453 • Scan Started — 554696714 • Threat Detected — 1090519054 • Threat Detected in Exclusion — 553648145 • Threat Detected in Network File Transfer — 1 • Threat Detected in Network File Transfer (Retrospective) — 2 • Threat Quarantined — 553648143

표 3-3 fireamp_event 필드(계속)

필드	설명
event_type_id	<p>FireAMP 이벤트 유형의 내부 ID입니다. 각 event_type_id 값에는 관련 event_type 값이 포함됩니다. 가능한 표시 값 및 관련 유형은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 553648143 — Threat Quarantined • 553648145 — Threat Detected in Exclusion • 553648146 — Cloud Recall Restore from Quarantine Started • 553648147 — Cloud Recall Quarantine Started • 553648149 — Quarantined Item Restored • 553648150 — Quarantine Restore Started • 553648154 — Cloud Recall Restore from Quarantine • 553648155 — Cloud Recall Quarantine • 553648168 — Blocked Execution • 554696714 — Scan Started • 554696715 — Scan Completed, No Detections • 1090519054 — Threat Detected • 1091567628 — Scan Completed With Detections • 1107296256 — FireAMP IOC • 2164260880 — Quarantine Failure • 2164260893 — Cloud Recall Quarantine Attempt Failed • 2164260884 — Quarantine Restore Failed • 2164260892 — Cloud Recall Restore from Quarantine Failed • 2165309453 — Scan Failed
file_name	탐지 또는 격리된 파일의 이름입니다. 이 이름에는 UTF-8 문자를 포함할 수 있습니다.
file_path	탐지 또는 격리된 파일의 파일 경로이며, 파일 이름은 포함되지 않습니다.
file_sha	탐지 또는 격리된 파일의 SHA-256 해시 값입니다.
file_size	탐지 또는 격리된 파일의 바이트 크기입니다.
file_timestamp	탐지 또는 격리된 파일의 생성 타임스탬프입니다.
file_type	탐지 또는 격리된 파일의 파일 유형입니다.
file_type_id	탐지 또는 격리된 파일의 파일 유형에 대한 내부 ID입니다.
instance_id	이벤트를 생성한 관리되는 디바이스의 Snort 인스턴스의 숫자 ID입니다.
ioc_count	이벤트에서 발견된 IoC(Indications of Compromise: 보안침해지표)의 개수입니다.
parent_file_name	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 파일의 이름입니다.
parent_file_sha	탐지가 발생했을 때 탐지 또는 격리된 파일에 액세스한 부모 파일의 SHA-256 해시 값입니다.
policy_uuid	이벤트를 트리거한 액세스 제어 정책의 고유한 식별자 역할을 하는 ID 번호입니다.

표 3-3 fireamp_event 필드(계속)

필드	설명
retroactive_disposition	처리가 업데이트된 경우 파일의 처리입니다. 처리가 업데이트되지 않은 경우, 이 필드에는 disposition 필드와 동일한 값이 포함됩니다. 가능한 값은 disposition 필드와 동일합니다.
score	동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 0부터 100까지 나타낸 숫자 값입니다.
security_context	트래픽이 통과한 보안 컨텍스트(가상 방화벽)에 대한 설명입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
sensor_address	이벤트를 생성한 디바이스의 IP 주소입니다.
sensor_id	이벤트를 생성한 디바이스의 ID입니다.
sensor_name	이벤트 레코드를 생성한 관리되는 디바이스의 텍스트 이름입니다. 이 필드는 이벤트가 참조하는 대상이 연결된 디바이스가 아닌 보고 디바이스 자체일 경우 null이 됩니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 fireamp_event.sensor_name이 null인 경우 0입니다.
src_continent_name	소스 호스트의 대륙 이름입니다. ** — 알 수 없음 na — 북미 as — 아시아 af — 아프리카 eu — 유럽 sa — 남미 au — 호주 an — 남극 대륙
src_country_id	소스 호스트의 국가 코드입니다.
src_country_name	소스 호스트의 국가 이름입니다.
src_ip_address_v6	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
src_ipaddr	연결의 소스에 대한 IPv4 또는 IPv6 주소를 이진수로 나타낸 값입니다.
src_port	연결 소스의 포트 번호입니다.
ssl_issuer_common_name	SSL 인증서의 발급자 일반 이름입니다. 이는 일반적으로 인증서 발급자의 호스트 및 도메인 이름이지만, 다른 정보가 포함될 수도 있습니다.
ssl_issuer_country	SSL 인증서 발급자의 국가입니다.
ssl_issuer_organization	SSL 인증서 발급자의 조직입니다.
ssl_issuer_organization_unit	SSL 인증서 발급자의 조직 부서입니다.
ssl_serial_number	발급 CA가 할당한 SSL 인증서의 일련 번호입니다.
ssl_subject_common_name	SSL 인증서의 주체 일반 이름입니다. 이는 일반적으로 인증서 주체의 호스트 및 도메인 이름이지만, 다른 정보가 포함될 수도 있습니다.
ssl_subject_country	SSL 인증서 주체의 국가입니다.
ssl_subject_organization	SSL 인증서 주체의 조직입니다.

표 3-3 fireamp_event 필드(계속)

필드	설명
ssl_subject_organization_unit	SSL 인증서 주체의 조직 부서입니다.
threat_name	위협의 이름입니다.
timestamp	FireAMP 이벤트 생성 타임스탬프입니다.
url	연결의 소스 URL입니다.
user_id	파일을 전송 또는 수신한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다. 이 사용자는 discovered_users 테이블에 있습니다.
username	파일을 전송 또는 수신한 호스트에 마지막으로 로그인한 사용자의 이름입니다.
web_application_id	해당하는 경우, 웹 애플리케이션의 내부 ID 번호입니다.
web_application_name	해당하는 경우, 웹 애플리케이션의 이름입니다.

fireamp_event 조인

다음 표에는 `fireamp_event` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 3-4 fireamp_event 조인

다음에 대해 이 테이블 조인 가능	추가
dst_ipaddr 또는 src_ipaddr	<code>rna_host_ip_map.ipaddr</code> <code>user_ipaddr_history.ipaddr</code>

fireamp_event 샘플 쿼리

다음 쿼리는 지정된 사용자와 관련된 악성코드 이벤트를 최대 25개까지 반환하며, 이는 `timestamp`를 기준으로 내림차순 정렬됩니다.

```
SELECT event_id, timestamp, src_ipaddr, dst_ipaddr, username, cloud_name, event_type,
event_subtype, event_description, detection_name, detector_type, file_name,
parent_file_name
FROM fireamp_event
WHERE username="username" ORDER BY timestamp ASC
LIMIT 25;
```

health_event

`health_event` 테이블에는 FireSIGHT System에서 생성한 상태 이벤트에 대한 정보가 포함됩니다. 자세한 내용은 다음 섹션을 참조하십시오.

- [health_event 필드, 페이지 3-9](#)
- [health_event 조인, 페이지 3-9](#)
- [health_event 샘플 쿼리, 페이지 3-9](#)

health_event 필드

다음 표에는 `health_event` 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 3-5 `health_event` 필드

필드	설명
<code>description</code>	관련 상태 모듈이 상태 이벤트를 생성하도록 유발한 조건에 대한 설명입니다. 예를 들어, 프로세스를 실행할 수 없을 때 생성되는 상태 이벤트에는 <code>Unable to Execute</code> 라는 레이블이 지정됩니다.
<code>event_time_sec</code>	방어 센터가 상태 이벤트를 생성한 날짜 및 시간의 UNIX 타임스탬프입니다.
<code>id</code>	이벤트의 내부 ID 번호입니다.
<code>module_name</code>	이벤트를 생성한 상태 모듈의 이름입니다.
<code>sensor_name</code>	이벤트 레코드를 생성한 관리되는 디바이스의 텍스트 이름입니다. 이 필드는 상태 이벤트가 참조하는 대상이 연결된 디바이스가 아닌 보고 디바이스 자체일 경우 <code>null</code> 이 됩니다.
<code>sensor_uuid</code>	관리되는 디바이스의 고유한 식별자입니다. 또는 <code>sensor_name</code> 이 <code>null</code> 인 경우 0입니다.
<code>status</code>	<code>sensor_uuid</code> 에서 식별된 어플라이언스에 대해 보고된 상태 모니터의 상태입니다. 값은 다음과 같습니다. <ul style="list-style-type: none"> <code>red</code> — Critical 상태. 어플라이언스에서 하나 이상의 상태 모듈에 대해 제한이 초과되었으며 문제가 해결되지 않았습니다. <code>yellow</code> — Warning 상태. 어플라이언스에서 하나 이상의 상태 모듈에 대해 제한이 초과되었으며 문제가 해결되지 않았습니다. <code>green</code> — Normal 상태. 어플라이언스의 모든 상태 모듈이 어플라이언스에 적용된 상태 정책에 구성된 제한 내에서 실행되고 있습니다. <code>recovered</code> — 어플라이언스의 모든 상태 모듈(Critical 또는 Warning 상태에 있던 모듈 포함)이 어플라이언스에 적용된 상태 정책에 구성된 제한 내에서 실행되고 있습니다. <code>disabled</code> — 어플라이언스가 비활성화되거나, 차단 목록에 올랐거나, 현재 연결할 수 없거나, 상태 정책이 적용되지 않았습니다. <code>error</code> — 어플라이언스에서 하나 이상의 상태 모니터링 모듈이 실패했으며, 실패 이후 성공적으로 다시 실행되지 않았습니다.
<code>units</code>	상태 테스트에서 얻은 결과의 측정 단위입니다. 그 예로, %(디스크 사용량)를 들 수 있습니다.
<code>value</code>	상태 테스트에서 얻은 결과의 단위 수입니다. 예를 들어, 80%의 <code>value</code> 는 80입니다.

health_event 조인

`health_event` 테이블에서는 조인을 수행할 수 없습니다.

health_event 샘플 쿼리

다음 쿼리는 정의된 기간 내에 로깅된 가장 최근의 상태 이벤트를 최대 25개까지 반환합니다.

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

```

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

```

sru_import_log

sru_import_log 테이블은 어플라이언스에서 실행된 규칙 업데이트 프로세스에 대한 정보가 포함됩니다. FireSIGHT System 버전 5.0부터 사용 중단된 **seu_import_log** 테이블은 **sru_import_log** 테이블로 대체됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [sru_import_log 필드, 페이지 3-10](#)
- [sru_import_log 조인, 페이지 3-11](#)
- [sru_import_log 샘플 쿼리, 페이지 3-11](#)

sru_import_log 필드

다음 표에는 **sru_import_log** 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 3-6 sru_import_log 필드

필드	설명
action	<p>가져온 규칙 업데이트 개체 유형에 대해 발생한 작업을 나타냅니다.</p> <ul style="list-style-type: none"> • apply — 가져오기에 대해 <code>Reapply intrusion policies after the Rule Update import completes</code> 옵션이 활성화됨 • changed — 규칙 업데이트 구성 요소 또는 규칙의 경우, 규칙 업데이트 구성 요소가 수정되었거나 규칙에 더 높은 개정 번호 및 동일한 GID와 SID가 있음 • collision — 규칙 업데이트 구성 요소 또는 규칙의 경우, 개정이 어플라이언스에 있는 기존 구성 요소나 규칙과 충돌하므로 가져오기를 건너뛰었음 • deleted — 규칙의 경우, 규칙 업데이트에서 규칙이 삭제됨 • disabled — 규칙의 경우, Cisco에서 제공하는 기본 정책에서 규칙이 비활성화됨 • drop — 규칙의 경우, Cisco에서 제공하는 기본 정책에서 규칙이 <code>Drop and Generate Events</code>로 설정됨 • enabled — 규칙 업데이트 수정의 경우, 프리프로세서, 규칙 또는 기타 기능이 Cisco에서 제공하는 기본 정책에서 활성화됨 • error — 규칙 업데이트 또는 로컬 규칙 파일의 경우 가져오기가 실패함 • new — 규칙의 경우, 이 어플라이언스에 규칙이 처음 저장된 것임
detail	<p>가져온 규칙 업데이트에 의해 구성 요소 또는 규칙에 적용된 변경 사항의 고유한 설명 문자열입니다. 또는 규칙이 변경되지 않은 경우에는 비어 있습니다.</p>
generator_id	<p>규칙의 Generator에 대한 GID입니다.</p>

표 3-6 sru_import_log 필드(계속)

필드	설명
import_time_sec	규칙 업데이트 가져오기가 로깅된 날짜 및 시간의 UNIX 타임스탬프입니다.
name	가져온 개체의 이름입니다. 규칙의 경우 규칙 메시지에 해당합니다. 규칙 업데이트 구성 요소의 경우, 이는 온라인 도움말 또는 Snort 같은 구성 요소 이름입니다.
policy	All - 규칙이 모든 기본 정책에 포함되어 있음을 나타냅니다.
revision	규칙의 개정 번호입니다.
signature_id	규칙, 디코더 또는 프리프로세서의 SID입니다.
sru_name	규칙 업데이트에 대해 설명하는 이름입니다.
sru_uuid	규칙 업데이트의 고유한 식별자입니다.
type	규칙 업데이트에서 가져온 개체의 유형(update, rule, variable 등)입니다.

sru_import_log 조인

sru_import_log 테이블에서는 조인을 수행할 수 없습니다.

sru_import_log 샘플 쿼리

다음 쿼리는 타임스탬프를 기준으로 최대 25개의 결과를 반환하며, 이는 내림차순 정렬됩니다.

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




스키마: 침입 테이블

이 장에는 침입 이벤트, 이벤트를 트리거한 패킷, 관련 규칙 메시지의 스키마 및 지원되는 조인에 대한 정보가 포함되어 있습니다.

자세한 내용은 아래 표에 나열된 섹션을 참조하십시오.

표 4-1 침입 테이블의 스키마

참조	다음에 대한 정보가 저장되는 테이블	버전
intrusion_event , 페이지 4-1	침입 이벤트 - 날짜, 시간, 공격용 악성코드 유형, 공격의 출처 및 대상에 대한 컨텍스트 정보가 포함됨	4.10.x+
intrusion_event_packet , 페이지 4-7	침입 이벤트를 트리거한 패킷의 내용	4.10.x+
rule_message , 페이지 4-8	침입 이벤트에 대한 규칙 메시지 - 관련 GID(Generator ID), 서명 ID(SID), 버전 데이터가 포함됨	4.10.x+
rule_documentation , 페이지 4-9	규칙에 대한 정보 - 공격 시나리오, 영향을 받은 시스템, 규칙이 생성된 시기 및 생성자에 대한 정보가 포함됨	5.2+

intrusion_event

`intrusion_event` 테이블에는 FireSIGHT System에 의해 식별된 가능한 침입에 대한 정보가 포함됩니다. 각 가능한 침입에 대해 시스템에서는 데이터베이스에 이벤트 및 관련 레코드를 생성하며 여기에는 날짜, 시간, 공격용 악성코드 유형, 액세스 제어 정책 및 규칙, 침입 정책 및 규칙, 공격의 출처 및 대상에 대한 기타 컨텍스트 정보가 포함됩니다.



정보

패킷 기반 이벤트의 경우 이벤트를 트리거한 패킷의 사본도 제공될 수 있습니다. [intrusion_event_packet](#) 샘플 쿼리, [페이지 4-8](#)을(를) 참조하십시오.

자세한 내용은 다음 섹션을 참조하십시오.

- [intrusion_event](#) 필드, [페이지 4-2](#)
- [intrusion_event](#) 조인, [페이지 4-6](#)
- [intrusion_event](#) 샘플 쿼리, [페이지 4-7](#)

intrusion_event 필드

다음 표에는 `intrusion_event` 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 4-2 `intrusion_event` 필드

필드	설명
<code>access_control_policy_name</code>	침입 이벤트를 생성한 침입 정책과 관련된 액세스 제어 정책입니다. 액세스 제어 정책 이름과 액세스 제어 규칙 이름의 조합은 방화 센터에서 고유해야 합니다.
<code>access_control_policy_UUID</code>	침입 이벤트를 생성한 침입 정책과 관련된 액세스 제어 정책의 UUID입니다.
<code>access_control_rule_id</code>	침입 이벤트를 생성한 침입 정책과 관련된 액세스 제어 규칙의 내부 ID 번호입니다.
<code>access_control_rule_name</code>	침입 이벤트를 생성한 침입 정책과 관련된 액세스 제어 규칙의 이름입니다. 액세스 제어 규칙 이름은 정책 내에서 고유해야 하지만 다른 정책 간에는 그렇지 않아도 됩니다.
<code>application_protocol_id</code>	애플리케이션 프로토콜의 내부 ID 번호입니다.
<code>application_protocol_name</code>	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • <code>pending</code> - 시스템에 추가 데이터가 필요한 경우 • 연결에 애플리케이션 정보가 없는 경우 비어 있음
<code>blocked</code>	침입 이벤트를 트리거한 패킷에 무슨 상황이 발생했는지 나타내는 값입니다. <ul style="list-style-type: none"> • 0 - 패킷이 삭제되지 않음 • 1 - 패킷이 삭제됨(인라인, 스위치드 또는 라우티드 구축) • 2 - 이벤트를 트리거한 패킷이 삭제되었을 수 있음(침입 정책이 인라인, 스위치드 또는 라우티드 구축에 컴프레이션된 디바이스에 적용된 경우)
<code>client_application_id</code>	침입 이벤트에 사용된 클라이언트 애플리케이션의 내부 ID 번호입니다.
<code>client_application_name</code>	침입 이벤트에 사용된 클라이언트 애플리케이션(사용 가능한 경우)입니다. 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • 일반 클라이언트 이름 - 시스템에서 클라이언트 애플리케이션을 탐지했으나 특정한 애플리케이션을 식별하지는 못한 경우 • <code>null</code> - 연결에 애플리케이션 정보가 없는 경우 비어 있음
<code>connection_sec</code>	침입 이벤트와 관련된 연결 이벤트의 UNIX 타임스탬프(00:00:00 01/01/1970 이후의 초)입니다.
<code>counter</code>	지정된 초의 각 연결 이벤트 시 늘어나는 숫자이며, 이는 동일한 초에 발생하는 여러 개의 이벤트를 구분하기 위해 사용됩니다.
<code>detection_engine_name</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>detection_engine_uuid</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.

표 4-2 intrusion_event 필드(계속)

필드	설명
dst_continent_name	목적지 호스트의 대륙 이름입니다. ** — 알 수 없음 na — 북미 as — 아시아 af — 아프리카 eu — 유럽 sa — 남미 au — 호주 an — 남극 대륙
dst_country_id	목적지 호스트의 국가 코드입니다.
dst_country_name	목적지 호스트의 국가 이름입니다.
dst_ip_address	버전 5.2에서 사용 중단된 필드입니다. 이전 버전과의 호환성 때문에 이 필드의 값은 null로 설정되지 않으나, 신뢰할 수 없습니다.
dst_ip_address_v6	버전 5.2에서 사용 중단된 필드입니다. 이전 버전과의 호환성 때문에 이 필드의 값은 null로 설정되지 않으나, 신뢰할 수 없습니다.
dst_ipaddr	이벤트 트리거와 관련된 목적지 호스트의 IPv4 또는 IPv6 주소를 이진수로 나타낸 값입니다.
dst_port	다음 중 하나에 해당합니다. • 목적지 포트 번호 - 이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 • ICMP 코드 - 이벤트 프로토콜 유형이 ICMP인 경우
dst_user_dept	목적지 사용자의 부서입니다.
dst_user_email	목적지 사용자의 이메일 주소입니다.
dst_user_first_name	목적지 사용자의 이름입니다.
dst_user_id	목적지 사용자, 즉, 침입 이벤트가 발생하기 전에 목적지 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
dst_user_last_name	목적지 사용자의 성입니다.
dst_user_last_seen_sec	목적지 사용자의 마지막 로그인이 보고된 날짜 및 시간의 UNIX 타임스탬프입니다.
dst_user_last_updated_sec	목적지 사용자의 레코드가 마지막으로 업데이트된 날짜 및 시간의 UNIX 타임스탬프입니다.
dst_user_name	목적지 사용자의 사용자 이름입니다.
dst_user_phone	목적지 사용자의 전화 번호입니다.
event_id	이벤트의 내부 ID 번호입니다. 방어 센터에서 이벤트를 고유하게 식별합니다.
event_time_sec	이벤트 패킷이 캡처된 날짜 및 시간의 UNIX 타임스탬프입니다.
event_time_usec	이벤트 타임스탬프가 마이크로초 단위로 증가한 값입니다. 마이크로초 해상도를 사용할 수 없는 경우 이 값은 0입니다.

표 4-2 intrusion_event 필드(계속)

필드	설명
icmp_code	ICMP 코드 - 이벤트가 ICMP 트래픽인 경우 또는 null - 이벤트가 ICMP 트래픽에서 생성되지 않은 경우
icmp_type	ICMP 유형 - 이벤트가 ICMP 트래픽인 경우 또는 null - 이벤트가 ICMP 트래픽에서 생성되지 않은 경우
impact	이벤트의 영향 플래그 값입니다. 정수 값은 다음과 같습니다. <ul style="list-style-type: none"> • 1 - 빨간색(vulnerable) • 2 - 주황색(potentially vulnerable) • 3 - 노란색(currently not vulnerable) • 4 - 파란색(unknown target) • 5 - 회색(unknown impact)
instance_id	이벤트를 생성한 관리되는 디바이스의 Snort 인스턴스의 숫자 ID입니다.
interface_egress_name	아웃바운드 트래픽의 인터페이스의 이름입니다.
interface_ingress_name	인바운드 트래픽의 인터페이스의 이름입니다.
intrusion_event_policy_uuid	침입 이벤트를 트리거한 침입 정책의 고유한 식별자입니다.
intrusion_event_policy_name	침입 이벤트를 생성한 침입 정책입니다.
ioc_count	이벤트에서 발견된 IoC(Indications of Compromise: 보안침해지표)의 개수입니다.
network_analysis_policy_name	침입 이벤트를 생성한 침입 정책과 관련된 네트워크 분석 정책입니다.
network_analysis_policy_UUID	침입 이벤트를 생성한 침입 정책과 관련된 네트워크 분석 정책의 UUID입니다.
priority	이벤트와 관련된 규칙 분류의 우선순위입니다. 규칙 우선순위는 사용자 인터페이스에서 설정됩니다.
protocol_name	침입 이벤트와 관련된 트래픽 프로토콜의 텍스트 이름입니다.
protocol_num	프로토콜의 IANA 번호는 다음 사이트에 나와 있습니다. http://www.iana.org/assignments/protocol-numbers .
reviewed	침입 이벤트가 검토됨으로 표시되었는지 나타냅니다. <ul style="list-style-type: none"> • 1 - 검토됨 • 0 - 검토되지 않음
rule_classification	침입 이벤트와 관련된 규칙 분류에 대한 설명이며, 일반적으로 여기에는 이벤트를 트리거한 규칙에 의해 탐지된 공격이 설명되어 있습니다. 예: A Network Trojan was Detected.
rule_classification_id	침입 이벤트와 관련된 규칙 분류의 ID 번호입니다.
rule_generator	침입 이벤트를 생성한 구성 요소입니다. Generator는 규칙 엔진, 디코더 또는 프리프로세서일 수 있습니다.
rule_generator_id	침입 이벤트를 생성한 rule_generator에서 명명된 구성 요소의 GID(Generator ID)입니다.
rule_message	이벤트에 대한 설명 텍스트입니다. 규칙 기반 침입 이벤트의 경우 규칙에서 메시지가 생성됩니다. 디코더 및 프리프로세서 기반 이벤트의 경우 이벤트 메시지가 하드 코딩됩니다.

표 4-2 intrusion_event 필드(계속)

필드	설명
rule_revision	침입 이벤트와 관련된 규칙의 개정 번호입니다.
rule_signature_id	침입 이벤트의 서명 ID(SID)입니다. 이벤트를 생성하도록 유발한 특정 규칙, 디코더 메시지 또는 프리프로세서 메시지를 식별합니다.
security_context	트래픽이 통과한 보안 컨텍스트(가상 방화벽)에 대한 설명입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
security_zone_egress_name	정책 위반을 트리거한 침입 이벤트의 이그레스 보안 영역입니다.
security_zone_ingress_name	정책 위반을 트리거한 침입 이벤트의 인그레스 보안 영역입니다.
sensor_address	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 <i>ipv4_address</i> , <i>ipv6_address</i> 입니다.
sensor_name	침입 이벤트를 생성한 관리되는 디바이스의 이름입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 <i>sensor_name</i> 이 null인 경우 0입니다.
src_continent_name	목적지 호스트의 대륙 이름입니다. ** — 알 수 없음 na — 북미 as — 아시아 af — 아프리카 eu — 유럽 sa — 남미 au — 호주 an — 남극 대륙
src_country_id	목적지 호스트의 국가 코드입니다.
src_country_name	목적지 호스트의 국가 이름입니다.
src_ip_address	버전 5.2에서 사용 중단된 필드입니다. 이전 버전과의 호환성 때문에 이 필드의 값은 null로 설정되지 않으나, 신뢰할 수 없습니다.
src_ip_address_v6	버전 5.2에서 사용 중단된 필드입니다. 이전 버전과의 호환성 때문에 이 필드의 값은 null로 설정되지 않으나, 신뢰할 수 없습니다.
src_ipaddr	이벤트 트리거와 관련된 소스 호스트의 IPv4 또는 IPv6 주소를 이진수로 나타낸 값입니다.
src_port	다음 중 하나에 해당합니다. • 소스 포트 번호 - 이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 • ICMP 유형 - 이벤트 프로토콜 유형이 ICMP인 경우
src_user_dept	소스 사용자의 부서입니다.
src_user_email	소스 사용자의 이메일 주소입니다.
src_user_first_name	소스 사용자의 이름입니다.
src_user_id	소스 사용자, 즉, 침입 이벤트가 발생하기 전에 소스 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
src_user_last_name	소스 사용자의 성입니다.

표 4-2 intrusion_event 필드(계속)

필드	설명
src_user_last_seen_sec	소스 사용자의 로그인이 마지막으로 보고된 날짜 및 시간의 UNIX 타임스탬프입니다.
src_user_last_updated_sec	소스 사용자의 레코드가 마지막으로 업데이트된 날짜 및 시간의 UNIX 타임스탬프입니다.
src_user_name	소스 사용자의 사용자 이름입니다.
src_user_phone	소스 사용자의 전화 번호입니다.
vlan_id	침입 이벤트를 트리거한 패킷과 관련된 가장 안쪽 VLAN의 ID 번호입니다.
web_application_id	해당하는 경우, 침입 이벤트에 사용된 웹 애플리케이션의 내부 ID 번호입니다.
web_application_name	해당하는 경우, 침입 이벤트에 사용된 웹 애플리케이션입니다. 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • web browsing - HTTP의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 식별하지 못하는 경우 • 연결에 HTTP 트래픽이 없는 경우 비어 있음

intrusion_event 조인

다음 표에는 intrusion_event 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 4-3 intrusion_event 조인

다음에 대해 이 테이블 조인 가능	추가
application_protocol_id 또는 client_application_id 또는 web_application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id
dst_ipaddr 또는 src_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

intrusion_event 샘플 쿼리

다음 쿼리는 가장 일반적인 검토되지 않은 침입 이벤트 결과를 최대 25개까지 반환하며, Count를 기준으로 내림차순으로 정렬됩니다.

```
SELECT rule_message, priority, rule_classification, count(*) as Count
FROM intrusion_event
WHERE reviewed="0"
GROUP BY rule_message, priority, rule_classification
ORDER BY Count DESC LIMIT 0, 25;
```

intrusion_event_packet

`intrusion_event_packet` 테이블에는 침입 이벤트를 트리거한 패킷의 내용에 대한 정보가 포함됩니다. 관리되는 디바이스에서 방화 센터로 패킷 전송을 금지했거나, `intrusion_event_packet` 테이블에 데이터가 포함되지 않습니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [intrusion_event_packet 필드, 페이지 4-7](#)
- [intrusion_event_packet 조인, 페이지 4-8](#)
- [intrusion_event_packet 샘플 쿼리, 페이지 4-8](#)

intrusion_event_packet 필드

다음 표에는 `intrusion_event_packet` 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 4-4 `intrusion_event_packet` 필드

필드	설명
<code>detection_engine_name</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>detection_engine_uuid</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>event_id</code>	이벤트의 ID 번호입니다. ID는 특정한 관리되는 디바이스마다 고유합니다.
<code>linktype</code>	패킷의 외부 레이어의 형식을 나타내는 내부 키이며, 관리되는 디바이스가 패킷을 올바르게 디코딩하는 데 사용됩니다. 링크 유형 1만 지원됩니다.
<code>packet_data</code>	이벤트를 트리거한 패킷의 내용입니다.
<code>packet_time_sec</code>	이벤트 패킷이 캡처된 날짜 및 시간의 UNIX 타임스탬프입니다.
<code>packet_time_usec</code>	이벤트 타임스탬프가 마이크로초 단위로 증가한 값입니다. 마이크로초 해상도를 사용할 수 없는 경우 이 값은 0입니다.
<code>sensor_address</code>	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
<code>sensor_name</code>	침입 이벤트를 생성한 관리되는 디바이스의 이름입니다.
<code>sensor_uuid</code>	관리되는 디바이스의 고유한 식별자입니다. 또는 <code>sensor_name</code> 이 <code>null</code> 인 경우 0입니다.

intrusion_event_packet 조인

intrusion_event_packet 테이블에서는 조인을 수행할 수 없습니다.

intrusion_event_packet 샘플 쿼리

다음 쿼리는 선택한 이벤트 ID와 일치하는 모든 패킷에 대한 패킷 정보를 반환합니다.

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

rule_message

rule_message 테이블은 침입 규칙에 대한 모든 메시지의 마스터 목록입니다. 각 규칙 메시지는 해당 식별 정보와 함께 제공됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- rule_message 필드, 페이지 4-8
- rule_message 조인, 페이지 4-8
- rule_message 샘플 쿼리, 페이지 4-9

rule_message 필드

다음 표에는 rule_message 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 4-5 rule_message 필드

필드	설명
generator_id	규칙을 트리거하는 구성 요소의 GID입니다.
message	트리거된 규칙과 관련된 메시지입니다.
rev_uuid	규칙 개정의 고유한 식별자입니다.
revision	규칙의 개정 번호입니다.
signature_id	어플라이언스 사용자 인터페이스에서 렌더링된 규칙 ID 번호입니다.
uuid	규칙의 고유한 식별자입니다.

rule_message 조인

rule_message 테이블에서는 조인을 수행할 수 없습니다.

rule_message 샘플 쿼리

다음 쿼리는 GID가 1이고 SID가 1200인 침입 규칙의 침입 규칙 메시지를 반환합니다.

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

rule_documentation

`rule_documentation` 테이블에는 알림을 생성하는 데 사용되는 규칙에 대한 정보가 포함됩니다. 자세한 내용은 다음 섹션을 참조하십시오.

- [rule_documentation 필드, 페이지 4-9](#)
- [rule_documentation 조인, 페이지 4-10](#)
- [rule_documentation 샘플 쿼리, 페이지 4-10](#)

rule_documentation 필드

다음 표에는 `rule_documentation` 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 4-6 `rule_documentation` 필드

필드	설명
<code>additional_references</code>	추가 정보 및 참조입니다.
<code>affected_systems</code>	취약성에 의해 영향을 받은 시스템입니다.
<code>attack_scenarios</code>	가능한 공격의 예시입니다.
<code>contributors</code>	규칙 및 기타 관련 문서 작성자의 연락처 정보입니다.
<code>corrective_action</code>	패치, 업데이트 또는 취약성을 제거하거나 완화하기 위한 기타 수단에 관한 정보입니다.
<code>detailed_information</code>	근본적인 취약성, 규칙에서 실제로 찾는 항목, 영향을 받는 시스템에 관한 정보입니다.
<code>ease_of_attack</code>	공격의 난이도가 간단함, 중간, 강력함, 어려움 중 어느 정도인지 나타내고, 스크립트를 사용하여 수행할 수 있는 공격인지 나타냅니다.
<code>false_negatives</code>	미탐지가 발생할 수 있는 예시입니다. 기본값은 None Known입니다.
<code>false_positives</code>	미탐지가 발생할 수 있는 예시입니다. 기본값은 None Known입니다.
<code>impact</code>	보안 침해가 이러한 취약성을 이용하여 여러 시스템에 어떤 영향을 미칠 수 있는지 나타냅니다.
<code>rule_revision</code>	규칙 개정 번호입니다.
<code>rule_signature_id</code>	이벤트와 일치하는 규칙 ID 번호입니다.

표 4-6 rule_documentation 필드(계속)

필드	설명
summary	위협 또는 취약성에 대한 설명입니다.
updated	규칙이 마지막으로 업데이트된 날짜 및 시간의 UNIX 타임스탬프입니다.

rule_documentation 조인

rule_documentation 테이블에서는 조인을 수행할 수 없습니다.

rule_documentation 샘플 쿼리

다음 쿼리는 ID가 1인 침입 규칙에 대한 공격 시나리오, 수정 조치, 영향, 요약을 반환합니다.

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



스키마: 통계 추적 테이블

이 장에는 애플리케이션 및 URL 통계 추적 테이블의 스키마 및 지원되는 조인에 대한 정보가 포함되어 있습니다. 이러한 테이블에서는 다음에 대한 통계 정보를 수집합니다.

- 애플리케이션과 사용자를 기준으로 한 액세스 제어 및 침입 이벤트
 - 애플리케이션과 사용자를 기준으로 한 대역폭 사용량 및 연결 결정
 - URL 평판(위험)과 URL 비즈니스 연관성을 기준으로 한 대역폭 사용량 및 연결 결정
- 각 테이블에 대한 상세 정보가 포함된 링크를 보려면 아래 표를 참조하십시오.

표 5-1 애플리케이션 및 URL 통계 테이블

참조	다음에 대한 통계가 저장되는 테이블	버전
app_ids_stats_current_timeframe , 페이지 5-4	애플리케이션과 애플리케이션 특성의 범위를 기준으로 한 액세스 제어 및 침입 방지 활동	5.0+
app_stats_current_timeframe , 페이지 5-6	애플리케이션과 애플리케이션 특성의 범위를 기준으로 한 트래픽 볼륨 및 시스템 액세스 제어 활동(연결 허용 또는 거부)	5.0+
geolocation_stats_current_timeframe , 페이지 5-7	위치를 기준으로 한 액세스 제어 활동	5.2+
ids_impact_stats_current_timeframe , 페이지 5-9	영향력 레벨을 기준으로 한 침입 이벤트의 통계(연결이 차단되거나 삭제될 수 있음)	5.1.1+
session_stats_current_timeframe , 페이지 5-11	모든 연결에 대한 통계가 포함됨. 통계는 바이트, 연결, 센서, 시간을 기준으로 추출할 수 있음	5.2+
ssl_stats_current_timeframe , 페이지 5-12	SSL 연결에 대한 통계가 포함됨. 통계는 바이트, 연결, 센서, 시간을 기준으로 추출할 수 있음	5.4+
storage_stats_by_disposition_current_timeframe , 페이지 5-14	처리를 기준으로 파일에 대한 통계가 포함됨. 통계는 바이트, 처리, 센서, 시간을 기준으로 추출할 수 있음	5.3+
storage_stats_by_file_type_current_timeframe , 페이지 5-16	파일 유형을 기준으로 파일에 대한 통계가 포함됨. 통계는 바이트, 파일 유형, 센서, 시간을 기준으로 추출할 수 있음	5.3+
transmission_stats_by_file_type_current_timeframe , 페이지 5-17	파일 유형을 기준으로 연결에 대한 통계가 포함됨. 통계는 바이트, 연결, 파일 유형, 센서, 시간을 기준으로 추출할 수 있음	5.3+
url_category_stats_current_timeframe , 페이지 5-18	요청한 웹 사이트의 카테고리를 기준으로 한 트래픽 볼륨 및 시스템 액세스 제어 활동(연결 허용 또는 거부)	5.0+

표 5-1 애플리케이션 및 URL 통계 테이블(계속)

참조	다음에 대한 통계가 저장되는 테이블	버전
url_reputation_stats_current_timeframe , 페이지 5-19	요청한 웹 사이트의 평판을 기준으로 한 트래픽 볼륨 및 시스템 액세스 제어 활동(연결 허용 또는 거부)	5.0+
user_ids_stats_current_timeframe , 페이지 5-21	사용자를 기준으로 한 액세스 제어 및 침입 방지 활동	5.0+
user_stats_current_timeframe , 페이지 5-22	사용자를 기준으로 한 트래픽 볼륨 및 액세스 제어 활동(연결 허용 또는 거부)	5.0+

통계 추적 테이블 이해

테이블의 이름은 데이터의 기간을 나타내기 위해 `current_day`, `current_month` 또는 `current_year`로 끝납니다. 예를 들어, `app_ids_stats_current_timeframe`은 `app_stats_current_day`, `app_stats_current_month`, `app_stats_current_year`를 의미합니다. `app_stats_current_year` 테이블에는 360일간의 통계가 저장되며, `current_month` 테이블에는 30일간의 통계가 저장됩니다.

방어 센터는 네트워크의 관리되는 디바이스에서 원시 카운트를 수신할 때마다 3가지 테이블 유형을 모두 업데이트하지만, 이 작업을 수행할 경우 해상도가 연속적으로 저해됩니다. `current_day` 테이블에는 가장 정밀한 해상도(15초 또는 5분, 특정 테이블에 따라 다름)가 포함되고, `current_year` 테이블에는 가장 낮은 해상도(24시간)가 포함됩니다. 구체적인 내용은 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

통계 추적 테이블의 저장 특성

다음 표에서 중요한 상세 정보를 참조하십시오.

표 5-2 통계 테이블의 저장 특성

테이블 유형	간격(해상도)	저장 수명
<code>current_day</code>	15초 <code>app_ids_stats_current_timeframe</code> 및 <code>user_ids_stats_current_timeframe</code>	현재 간격 + 이전 24시간의 모든 간격
	5분 <code>app_stats_current_timeframe</code> , <code>user_stats_current_timeframe</code> , <code>url_category_stats_current_timeframe</code> , <code>url_reputation_stats_current_timeframe</code>	현재 간격 + 이전 24시간의 모든 간격
<code>current_month</code>	1시간	현재 시간 + 30일 이전의 시간
<code>current_year</code>	24시간	현재 일 + 이전 360일

저장 간격은 시작 시간에 의해 정의됩니다. 예를 들어, `current_month` 테이블에는 10:00:00에서 10:59:59까지의 시간에 대한 카운트가 하나의 레코드로 포함되며 타임스탬프는 10:00:00입니다. 일일은 00:00:00에 시작하고 23:59:59에 끝납니다. 간격 시작 시간은 UNIX 타임스탬프(GMT)로 저장됩니다.

통계 테이블 쿼리 시 시간 간격 지정

쿼리에 대한 유효 시간 간격은 쿼리의 테이블 및 `time_start_sec` 필드 두 가지 모두에 의해 정의됩니다.

예를 들어, SQL 문이 `time_start_sec = 6:00:00`을 지정할 경우 간격은 각 테이블 유형에 따라 달라집니다.

- `current_day` 테이블: 6:00:00에서 6:00:14까지(15초 테이블의 경우) 또는 6:00:00에서 6:04:59까지(5분 테이블의 경우)
- `current_month` 테이블: 6:00:00에서 6:59:59까지
- `current_year` 테이블: 0:00:00에서 다음날 23:59:59까지

데이터를 검색하는 가장 간단한 방법은 간격 시작 시간을 명시하는 것입니다. 예를 들어, `app_ids_stats_current_day` 테이블에서 검색하려면 다음 중 하나를 지정합니다.

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

쿼리에 간격 시작 시간이 아닌 타임스탬프가 포함된 경우, 요청이 다음과 같이 수정됩니다.

- 간격 시간과 가장 근사치가 되도록 시작 시간 올림
- 간격 시간과 가장 근사치가 되도록 끝 시간 버림

예를 들어, 다음 쿼리는 시작 시간으로 올림됩니다.

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec = UNIX_TIMESTAMP("2011-12-01 오후 0:30:00");
```

그리고 다음과 같습니다.

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec = UNIX_TIMESTAMP("2011-12-01 오전 1:00:00");
```

간격의 범위를 쿼리할 경우, 시작 시간 간격이 올림 되고 끝 시간 간격은 버림됩니다. 예를 들면 다음과 같습니다.

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

다음으로 변경합니다.

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec BETWEEN UNIX_TIMESTAMP("2011-12-10 오후 1:00:00") and
UNIX_TIMESTAMP("2011-12-12 오후 4:00:00");
```

쿼리 간격이 테이블의 기간보다 늘어날 경우, 일반적으로 다른 테이블에서 추가 데이터를 가져올 수 있습니다. 단, 다른 테이블의 데이터는 해상도가 저하됩니다. 예를 들어, 지난 2일간에 대역폭 사용량을 검색하려는 경우 어제에 대한 결과는 `current_day` 테이블(5분 해상도)에서 가져올 수 있으나, 이전 일에 대한 통계는 `current_month`(시간 체크 단위) 또는 `current_year`(일 체크 단위)에서 얻을 수 있습니다.

app_ids_stats_current_timeframe

`app_ids_stats_current_timeframe` 테이블에는 모니터링되는 네트워크상의 애플리케이션 활동 및 침입 이벤트에 대한 통계가 포함됩니다. 통계는 탐지된 애플리케이션, 애플리케이션 유형(애플리케이션 프로토콜, 클라이언트 애플리케이션 또는 웹 애플리케이션), 애플리케이션의 위험 및 비즈니스 연관성에 따라 추출할 수 있습니다. 이 테이블은 침입 정책 위반으로 인해 차단된 연결 및 침입 시 예상되는 잠재적인 영향도 추적합니다.

`current_day`, `current_month`, `current_year` 통계 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

`app_ids_stats_current_timeframe` 테이블에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- [app_ids_stats_current_timeframe 필드, 페이지 5-4](#)
- [app_ids_stats_current_timeframe 조인, 페이지 5-5](#)
- [app_ids_stats_current_timeframe 샘플 쿼리, 페이지 5-5](#)

app_ids_stats_current_timeframe 필드

다음 표에는 `app_ids_stats_current_timeframe` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다. 이러한 유형의 모든 테이블에는 동일한 필드가 포함됩니다.

표 5-3 `app_ids_stats_current_timeframe` 필드

필드	설명
<code>application_id</code>	애플리케이션의 내부 ID 번호입니다.
<code>application_name</code>	사용자 인터페이스에 표시되는 애플리케이션 이름입니다.
<code>blocked</code>	침입 정책 위반으로 인해 차단된 연결 수입니다.
<code>business_relevance</code>	애플리케이션의 비즈니스 생산성에 대한 연관성을 1에서 5까지 나타내는 지수이며 1은 매우 낮음, 5는 매우 높음을 의미합니다.
<code>business_relevance_description</code>	비즈니스 연관성(<code>very low</code> , <code>low</code> , <code>medium</code> , <code>high</code> , <code>very high</code>)에 대한 설명입니다.
<code>impact_level_1</code>	애플리케이션에 대해 기록된 영향 레벨 1(<code>vulnerable</code>) 침입 이벤트의 수입니다.
<code>impact_level_2</code>	영향 레벨 2(<code>potentially vulnerable</code>) 침입 이벤트의 수입니다.
<code>impact_level_3</code>	영향 레벨 3(<code>host currently not vulnerable</code>) 침입 이벤트의 수입니다.
<code>impact_level_4</code>	영향 레벨 4(<code>unknown target</code>) 침입 이벤트의 수입니다.
<code>impact_level_5</code>	영향 레벨 5(<code>unknown vulnerability</code>) 침입 이벤트의 수입니다.
<code>is_client_application</code>	탐지된 애플리케이션이 클라이언트 애플리케이션인지 나타내는 <code>true-false</code> 플래그입니다.
<code>is_server_application</code>	탐지된 애플리케이션이 애플리케이션 프로토콜인지 나타내는 <code>true-false</code> 플래그입니다.
<code>is_web_application</code>	탐지된 애플리케이션이 웹 애플리케이션인지 나타내는 <code>true-false</code> 플래그입니다.
<code>risk</code>	애플리케이션의 예상 위험도를 1에서 5까지 나타내는 지수이며 1은 매우 낮은 위험, 5는 심각한 위험을 의미합니다.

표 5-3 app_ids_stats_current_timeframe 필드(계속)

필드	설명
risk_description	예상 위험(very low, low, medium, high, critical)에 대한 설명입니다.
sensor_address	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 ipv4_address, ipv6_address입니다.
sensor_id	이벤트를 제공한 디바이스의 ID입니다.
sensor_name	침입 이벤트를 생성한 관리되는 디바이스의 이름입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 sensor_name이 null인 경우 0입니다.
start_time_sec	측정 간격이 시작된 날짜 및 시간의 UNIX 타임스탬프입니다. 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3을 참조하십시오.
would_have_dropped	인라인 구축에서 패킷을 삭제하도록 침입 정책을 구성한 경우 삭제되었을 가능성이 있는 패킷의 수입니다.

app_ids_stats_current_timeframe 조인

다음 표에는 app_ids_stats_current_timeframe 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 5-4 app_ids_stats_current_timeframe 조인

다음에 대해 이 테이블 조인 가능	추가
application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id

app_ids_stats_current_timeframe 샘플 쿼리

다음 쿼리는 app_ids_stats_current_month 테이블에서 애플리케이션 레코드를 최대 25개까지 반환합니다. 각 레코드에는 시간 간격 동안 애플리케이션의 차단된 연결 및 침입 이벤트 수가 포함됩니다.

```
SELECT from_unixtime(start_time_sec), sum(blocked)
FROM app_ids_stats_current_day
WHERE start_time_sec = unix_timestamp("2013-12-15");
```

app_stats_current_timeframe

`app_stats_current_timeframe` 테이블에는 트래픽을 모니터링한 애플리케이션 및 디바이스를 기준으로 한 대역폭 사용량 및 액세스 제어 활동(연결 허용 또는 거부)에 대한 통계가 포함됩니다. 이러한 통계는 비즈니스 연관성, 예상 위험, 애플리케이션 유형을 기준으로 필터링할 수 있습니다.

`current_day`, `current_month`, `current_year` 통계 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

`app_stats_current_timeframe` 테이블에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- [app_stats_current_timeframe 필드, 페이지 5-6](#)
- [app_stats_current_timeframe 조인, 페이지 5-7](#)
- [app_stats_current_timeframe 샘플 쿼리, 페이지 5-7](#)

app_stats_current_timeframe 필드

다음 표에는 `app_stats_current_timeframe` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 5-5 `app_stats_current_timeframe` 필드

필드	설명
<code>application_id</code>	애플리케이션의 내부 ID 번호입니다.
<code>application_name</code>	사용자 인터페이스에 표시되는 애플리케이션 이름입니다.
<code>business_relevance</code>	애플리케이션의 비즈니스 생산성에 대한 연관성을 1에서 5까지 나타내는 지수이며 1은 매우 낮음, 5는 매우 높음을 의미합니다.
<code>business_relevance_description</code>	비즈니스 연관성(<code>very low</code> , <code>low</code> , <code>medium</code> , <code>high</code> , <code>very high</code>)에 대한 설명입니다.
<code>bytes_in</code>	지정된 간격 동안 애플리케이션에 대한 인바운드 트래픽의 바이트 수입니다.
<code>bytes_out</code>	지정된 간격 동안 애플리케이션에 대한 아웃바운드 트래픽의 바이트 수입니다.
<code>connections_allowed</code>	허용된 연결의 수입니다.
<code>connections_denied</code>	액세스 제어 정책 위반으로 인해 거부된 연결의 수입니다.
<code>is_client_application</code>	탐지된 애플리케이션이 클라이언트 애플리케이션인지 나타내는 <code>true-false</code> 플래그입니다.
<code>is_server_application</code>	탐지된 애플리케이션이 애플리케이션 프로토콜인지 나타내는 <code>true-false</code> 플래그입니다.
<code>is_web_application</code>	탐지된 애플리케이션이 웹 애플리케이션인지 나타내는 <code>true-false</code> 플래그입니다.
<code>risk</code>	애플리케이션의 예상 위험도를 1에서 5까지 나타내는 지수이며 1은 매우 낮은 위험, 5는 심각한 위험을 의미합니다.
<code>risk_description</code>	예상 위험(<code>very low</code> , <code>low</code> , <code>medium</code> , <code>high</code> , <code>critical</code>)에 대한 설명입니다.
<code>sensor_address</code>	트래픽을 모니터링한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.

표 5-5 app_stats_current_timeframe 필드(계속)

필드	설명
sensor_id	트래픽을 탐지한 관리되는 디바이스의 내부 ID 번호입니다.
sensor_name	트래픽을 탐지한 관리되는 디바이스의 이름입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 sensor_name이 null인 경우 0입니다.
start_time_sec	측정 간격의 시작에 대한 UNIX 타임스탬프입니다. 시작 시간 지정에 대한 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3 을(를) 참조하십시오.

app_stats_current_timeframe 조인

다음 표에는 `app_stats_current_timeframe` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 5-6 app_stats_current_timeframe 조인

다음에 대해 이 테이블 조인 가능	추가
application_id	<pre> application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id </pre>

app_stats_current_timeframe 샘플 쿼리

다음 쿼리는 방어 센터에 연결된 모든 관리되는 디바이스와 관련하여, 하루 동안 비즈니스 연관성이 낮고 위험도가 높은 애플리케이션과 관련된 인바운드 및 아웃바운드 트래픽을 반환합니다.

```

SELECT start_time_sec, sum(bytes_in), sum(bytes_out)

FROM app_stats_current_day

WHERE business_relevance <= 2

AND risk >= 4 AND start_time_sec = unix_timestamp("2013-12-15");

```

geolocation_stats_current_timeframe

`geolocation_stats_timeframe` 테이블에는 위치 레벨에 기반한 침입 이벤트와 관련된 통계가 포함됩니다. 통계는 영향 레벨, 디바이스, 패킷 처리 방법을 기준으로 추출할 수 있습니다.

`current_day`, `current_month`, `current_year` 통계 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

geolocation_stats_current_timeframe 테이블에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- geolocation_stats_current_timeframe 필드, 페이지 5-8
- geolocation_stats_current_timeframe 조인, 페이지 5-9
- geolocation_stats_current_timeframe 샘플 쿼리, 페이지 5-9

geolocation_stats_current_timeframe 필드

다음 표에는 geolocation_stats_current_timeframe 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다. 이러한 유형의 모든 테이블에는 동일한 필드가 포함됩니다.

표 5-7 geolocation_stats_current_timeframe 필드

필드	설명
bytes_from	세션 응답자가 전송한 총 바이트 수입니다.
bytes_to	세션 개시자가 전송한 총 바이트 수입니다.
destination_continent	목적지 호스트의 대륙 이름입니다. ** — 알 수 없음 na — 북미 as — 아시아 af — 아프리카 eu — 유럽 sa — 남미 au — 호주 an — 남극 대륙
destination_country	목적지 호스트의 국가 코드입니다.
flows_allowed	허용된 플로우의 수입니다.
flows_denied	액세스 제어 정책 위반으로 인해 거부된 플로우의 수입니다.
sensor_address	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 ipv4_address, ipv6_address입니다.
sensor_id	이벤트를 제공한 디바이스의 ID입니다.
sensor_name	침입 이벤트를 생성한 관리되는 디바이스의 이름입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 sensor_name이 null인 경우 0입니다.

표 5-7 geolocation_stats_current_timeframe 필드(계속)

필드	설명
source_continent	소스 호스트의 대륙 이름입니다. ** — 알 수 없음 na — 북미 as — 아시아 af — 아프리카 eu — 유럽 sa — 남미 au — 호주 an — 남극 대륙
source_country	소스 호스트의 국가 코드입니다.
start_time_sec	측정 간격이 시작된 날짜 및 시간의 UNIX 타임스탬프입니다. 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3 을(를) 참조하십시오.

geolocation_stats_current_timeframe 조인

geolocation_stats_current_timeframe 테이블에서는 조인을 수행할 수 없습니다.

geolocation_stats_current_timeframe 샘플 쿼리

다음 쿼리는 현재까지의 날짜 동안 아시아에서 가져온 연결 이벤트 중 처음 25개의 소스 국가 및 센서 이름을 반환합니다.

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

ids_impact_stats_current_timeframe

ids_impact_stats_timeframe 테이블에는 영향 레벨에 기반한 침입 이벤트와 관련된 통계가 포함됩니다. 통계는 영향 레벨, 디바이스, 패킷 처리 방법을 기준으로 추출할 수 있습니다.

current_day, current_month, current_year 통계 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

ids_impact_stats_current_timeframe 테이블에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- [ids_impact_stats_current_timeframe 필드, 페이지 5-10](#)
- [ids_impact_stats_current_timeframe 조인, 페이지 5-10](#)
- [ids_impact_stats_current_timeframe 샘플 쿼리, 페이지 5-10](#)

ids_impact_stats_current_timeframe 필드

다음 표에는 `ids_impact_stats_current_timeframe` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다. 이러한 유형의 모든 테이블에는 동일한 필드가 포함됩니다.

표 5-8 `ids_impact_stats_current_timeframe` 필드

필드	설명
<code>blocked</code>	침입 정책 위반으로 인해 차단된 연결 수입입니다.
<code>impact_level_1</code>	애플리케이션에 대해 기록된 영향 레벨 1(vulnerable) 침입 이벤트의 수입입니다.
<code>impact_level_2</code>	영향 레벨 2(potentially vulnerable) 침입 이벤트의 수입입니다.
<code>impact_level_3</code>	영향 레벨 3(host currently not vulnerable) 침입 이벤트의 수입입니다.
<code>impact_level_4</code>	영향 레벨 4(unknown target) 침입 이벤트의 수입입니다.
<code>impact_level_5</code>	영향 레벨 5(unknown vulnerability) 침입 이벤트의 수입입니다.
<code>sensor_address</code>	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
<code>sensor_id</code>	이벤트를 제공한 디바이스의 ID입니다.
<code>sensor_name</code>	침입 이벤트를 생성한 관리되는 디바이스의 이름입니다.
<code>sensor_uuid</code>	관리되는 디바이스의 고유한 식별자입니다. 또는 <code>sensor_name</code> 이 null인 경우 0입니다.
<code>start_time_sec</code>	측정 간격이 시작된 날짜 및 시간의 UNIX 타임스탬프입니다. 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3을(를) 참조하십시오.
<code>would_have_dropped</code>	인라인 구축에서 패킷을 삭제하도록 침입 정책을 설정한 경우 삭제되었을 가능성이 있는 패킷의 수입입니다.

ids_impact_stats_current_timeframe 조인

`ids_impact_stats_current_timeframe` 테이블에서는 조인을 수행할 수 없습니다.

ids_impact_stats_current_timeframe 샘플 쿼리

다음 쿼리는 현재까지의 날짜 동안 `blocked` 및 `would_have_dropped` 이벤트 중 처음 25개를 반환합니다.

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

session_stats_current_timeframe

`session_stats_timeframe` 테이블에는 모든 연결에 대한 통계가 포함됩니다. 통계는 바이트, 연결, 센서, 시간을 기준으로 추출할 수 있습니다.

`current_day`, `current_month`, `current_year` 통계 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

`session_stats_current_timeframe` 테이블에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- [session_stats_current_timeframe 필드, 페이지 5-11](#)
- [session_stats_current_timeframe 조인, 페이지 5-11](#)
- [session_stats_current_timeframe 샘플 쿼리, 페이지 5-12](#)

session_stats_current_timeframe 필드

다음 표에는 `session_stats_current_timeframe` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다. 이러한 유형의 모든 테이블에는 동일한 필드가 포함됩니다.

표 5-9 `session_stats_current_timeframe` 필드

필드	설명
<code>bytes_in</code>	지정된 간격 동안 인바운드 트래픽의 바이트 수입니다.
<code>bytes_out</code>	지정된 간격 동안 아웃바운드 트래픽의 바이트 수입니다.
<code>connections_allowed</code>	지정된 URL 카테고리에 허용된 연결의 수입니다.
<code>connections_denied</code>	액세스 제어 정책 위반으로 인해 지정된 URL 카테고리에 거부된 연결의 수입니다.
<code>id</code>	이 필드는 사용되지 않으며 항상 0을 반환합니다.
<code>sensor_address</code>	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
<code>sensor_id</code>	이벤트를 제공한 디바이스의 ID입니다.
<code>sensor_name</code>	침입 이벤트를 생성한 관리되는 디바이스의 이름입니다.
<code>sensor_uuid</code>	관리되는 디바이스의 고유한 식별자입니다. 또는 <code>sensor_name</code> 이 null인 경우 0입니다.
<code>start_time_sec</code>	측정 간격이 시작된 날짜 및 시간의 UNIX 타임스탬프입니다. 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3 을(를) 참조하십시오.

session_stats_current_timeframe 조인

`session_stats_current_timeframe` 테이블에서는 조인을 수행할 수 없습니다.

session_stats_current_timeframe 샘플 쿼리

다음 쿼리는 현재까지의 날짜 동안 각 센서에 거부 및 허용된 연결의 수를 반환하며, 이는 `sensor_name`을 기준으로 내림차순 정렬됩니다.

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

ssl_stats_current_timeframe

`ssl_stats_current_timeframe` 테이블에는 SSL 연결에 대한 통계가 포함됩니다. 통계는 바이트, 연결, 센서, 시간을 기준으로 추출할 수 있습니다.

`current_day`, `current_month`, `current_year` 통계 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

`ssl_stats_current_timeframe` 테이블에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- [ssl_stats_current_timeframe 필드, 페이지 5-12](#)
- [ssl_stats_current_timeframe 조인, 페이지 5-14](#)
- [ssl_stats_current_timeframe 샘플 쿼리, 페이지 5-14](#)

ssl_stats_current_timeframe 필드

다음 표에는 `ssl_stats_current_timeframe` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다. 이러한 유형의 모든 테이블에는 동일한 필드가 포함됩니다.

표 5-10 `ssl_stats_current_timeframe` 필드

필드	설명
<code>block</code>	재설정 없이 삭제되는 SSL 세션의 수입입니다.
<code>block_with_reset</code>	재설정과 함께 삭제되는 SSL 세션의 수입입니다.
<code>cached_session</code>	세션 캐시에서 발견된 SSL 세션의 수입입니다.
<code>cannot_determine_verdict</code>	SSL 규칙을 평가하는 도중 발생한 핸드셰이크 오류의 수입입니다.
<code>cert_expired</code>	인증서가 만료된 SSL 세션의 수입입니다.
<code>cert_invalid_issuer</code>	인증서 발급자가 유효하지 않거나 Trusted CA 목록에 없는 SSL 세션의 수입입니다.
<code>cert_invalid_signature</code>	인증서의 서명이 유효하지 않은 SSL 세션의 수입입니다.
<code>cert_not_checked</code>	인증서가 확인되지 않은 SSL 세션의 수입입니다.
<code>cert_not_yet_valid</code>	인증서가 아직 유효하지 않은 SSL 세션의 수입입니다.
<code>cert_revoked</code>	인증서가 폐기된 SSL 세션의 수입입니다.
<code>cert_self_signed</code>	인증서가 자체 서명된 SSL 세션의 수입입니다.
<code>cert_unknown</code>	인증서 상태를 알 수 없는 SSL 세션의 수입입니다.
<code>cert_valid</code>	인증서가 유효한 SSL 세션의 수입입니다.

표 5-10 ssl_stats_current_timeframe 필드(계속)

필드	설명
cert_validation_cache_hit	유효성 검사 캐시에서 인증서가 발견된 횟수입니다.
cert_validation_cache_miss	유효성 검사 캐시에서 인증서가 발견되지 않은 횟수입니다.
decrypt_resign_self_signed	자체 서명된 인증서를 사용하는 SSL 세션이 decrypt-resign 메서드를 사용하여 해독된 횟수입니다.
decrypt_resign_self_signed_replace_key_only	자체 서명된 인증서를 사용하는 SSL 세션이 decrypt-resign과 함께 replace key only 메서드를 사용하여 해독된 횟수입니다.
decrypt_resign_signed_cert	서명된 인증서를 사용하는 SSL 세션이 decrypt-resign 메서드를 사용하여 해독된 횟수입니다.
decrypt_with_known_key	known-key 메서드를 사용하여 SSL 세션이 해독된 횟수입니다.
decryption_error	해독 도중 오류가 발생한 SSL 세션의 수입니다.
do_not_decrypt	SSL 세션이 발견되었으나 해독되지 않은 횟수입니다.
handshake_error	SSL 규칙을 평가하기 전에 발생한 핸드셰이크 오류의 수입니다.
orig_cert_cache_hit	캐시에서 원본 인증서가 발견된 횟수입니다.
orig_cert_cache_miss	캐시에서 원본 인증서가 발견되지 않은 횟수입니다.
resigned_cert_cache_hit	캐시에서 재서명된 인증서가 발견된 횟수입니다.
resigned_cert_cache_miss	캐시에서 재서명된 인증서가 발견되지 않은 횟수입니다.
sensor_address	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 <i>ipv4_address</i> , <i>ipv6_address</i> 입니다.
sensor_id	이벤트를 제공한 디바이스의 ID입니다.
sensor_name	이벤트를 생성한 관리되는 디바이스의 이름입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 <i>sensor_name</i> 이 null인 경우 0입니다.
session_cache_hit	캐시에서 SSL 세션 ID 또는 티켓이 발견된 횟수입니다.
session_cache_miss	캐시에서 SSL 세션 ID 또는 티켓이 발견되지 않은 횟수입니다.
session_incorrectly_identified_as_ssl	SSL을 사용하여 잘못 식별된 세션의 수입니다.
ssl_compression	SSL 압축을 사용한 세션의 수입니다.
ssl_sessions_decrypted	성공적으로 해독된 SSL 세션의 수입니다.
ssl_sessions_not_decrypted	성공적으로 해독되지 않은 SSL 세션의 수입니다.
ssl_sessions_reused_by_id	SSL 세션이 ID를 재사용한 횟수입니다.
ssl_sessions_reused_by_ticket	SSL 세션이 티켓을 재사용한 횟수입니다.
ssl_sessions_with_errors	오류가 있는 SSL 세션의 수입니다.
ssl_v20	SSL 버전 2.0을 사용하는 SSL 세션의 수입니다.
ssl_v30	SSL 버전 3.0을 사용하는 SSL 세션의 수입니다.
ssl_version_unknown	알 수 없는 SSL 버전을 사용하는 SSL 세션의 수입니다.
start_time_sec	측정 간격이 시작된 날짜 및 시간의 UNIX 타임스탬프입니다. 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3(를) 참조하십시오.
tls_v10	TLS 버전 1.0을 사용하는 SSL 세션의 수입니다.

표 5-10 ssl_stats_current_timeframe 필드(계속)

필드	설명
tls_v11	TLS 버전 1.1을 사용하는 SSL 세션의 수입니다.
tls_v12	TLS 버전 1.2를 사용하는 SSL 세션의 수입니다.
total_ssl_sessions	탐지된 총 SSL 세션 수입니다.
uncached_session	ID 또는 티켓의 캐시 누락이 해독을 차단한 횟수입니다.
undecryptable_in_passive_mode	디바이스가 패시브 모드에 있어 해독하지 못한 SSL 세션의 수입니다.
unknown_cipher_suite	알 수 없는 암호를 사용하는 SSL 세션의 수입니다.
unsupported_cipher_suite	알려져 있지만 지원되지 않는 암호를 사용하는 SSL 세션의 수입니다.

ssl_stats_current_timeframe 조인

`ssl_stats_current_timeframe` 테이블에서는 조인을 수행할 수 없습니다.

ssl_stats_current_timeframe 샘플 쿼리

다음 쿼리는 현재까지의 날짜 동안 SSL 세션의 수, 해독된 세션, 해독되지 않은 세션, 각 센서의 패시브 모드에서 해독하지 못한 세션을 반환하며 이는 `sensor_name`을 기준으로 내림차순 정렬됩니다.

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

storage_stats_by_disposition_current_timeframe

`storage_stats_by_disposition_timeframe` 테이블에는 저장 파일에 대한 통계가 포함됩니다. 통계는 바이트, 연결, 센서, 시간을 기준으로 추출할 수 있음

`current_day`, `current_month`, `current_year` 통계 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

`storage_stats_by_disposition_timeframe` 테이블에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- [storage_stats_by_disposition_current_timeframe 필드, 페이지 5-15](#)
- [storage_stats_by_disposition_current_timeframe 조인, 페이지 5-15](#)
- [storage_stats_by_disposition_current_timeframe 샘플 쿼리, 페이지 5-15](#)

storage_stats_by_disposition_current_timeframe 필드

다음 표에는 `storage_stats_by_disposition_current_timeframe` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다. 이러한 유형의 모든 테이블에는 동일한 필드가 포함됩니다.

표 5-11 storage_stats_by_disposition_current_timeframe 필드

필드	설명
bytes_written	바이트 단위의 파일 크기입니다.
disposition	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. <ul style="list-style-type: none"> CLEAN — 파일이 깨끗하고 악성코드가 포함되어 있지 않습니다. UNKNOWN — 파일에 악성코드가 포함되어 있는지 알 수 없습니다. MALWARE — 파일에 악성코드가 포함되어 있습니다. UNAVAILABLE — 소프트웨어가 처리를 위한 요청을 Cisco 클라우드에 전송하지 못했거나, Cisco 클라우드 서비스가 요청에 응답하지 않았습니다. CUSTOM SIGNATURE — 파일이 사용자가 정의한 해시와 일치하며, 사용자가 지정한 방식으로 처리됩니다.
number_dropped	이러한 처리 방식의 파일이 삭제된 수입니다.
number_stored	이러한 처리 방식의 파일이 저장된 수입니다.
sensor	파일을 탐지한 디바이스의 ID입니다.
sensor_address	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
sensor_name	침입 이벤트를 생성한 관리되는 디바이스의 이름입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 <code>sensor_name</code> 이 null인 경우 0입니다.
start_time_sec	측정 간격이 시작된 날짜 및 시간의 UNIX 타임스탬프입니다. 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3 (를) 참조하십시오.

storage_stats_by_disposition_current_timeframe 조인

`session_stats_current_timeframe` 테이블에서는 조인을 수행할 수 없습니다.

storage_stats_by_disposition_current_timeframe 샘플 쿼리

다음 쿼리는 현재까지의 날짜 동안 각 센서에 삭제 및 저장된 파일의 수를 반환하며, 이는 `sensor_name`을 기준으로 내림차순 정렬됩니다.

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

storage_stats_by_file_type_current_timeframe

`storage_stats_by_file_type_current_timeframe` 테이블에는 파일 유형별로 저장된 파일에 대한 통계가 포함됩니다. 통계는 바이트, 연결, 센서, 시간을 기준으로 추출할 수 있습니다.

`current_day`, `current_month`, `current_year` 통계 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

`storage_stats_by_file_type_current_timeframe` 테이블에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- [storage_stats_by_file_type_current_timeframe 필드, 페이지 5-16](#)
- [storage_stats_by_file_type_current_timeframe 조인, 페이지 5-16](#)
- [storage_stats_by_file_type_current_timeframe 샘플 쿼리, 페이지 5-17](#)

storage_stats_by_file_type_current_timeframe 필드

다음 표에는 `storage_stats_by_file_type_current_timeframe` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다. 이러한 유형의 모든 테이블에는 동일한 필드가 포함됩니다.

표 5-12 storage_stats_by_file_type_current_timeframe 필드

필드	설명
<code>bytes_written</code>	바이트 단위의 파일 크기입니다.
<code>file_type</code>	탐지 또는 격리된 파일의 파일 유형입니다.
<code>file_type_id</code>	파일 유형에 매핑되는 ID 번호입니다.
<code>number_dropped</code>	이러한 유형의 파일이 삭제된 수입니다.
<code>number_stored</code>	이러한 유형의 파일이 저장된 수입니다.
<code>sensor</code>	파일을 탐지한 디바이스의 ID입니다.
<code>sensor_address</code>	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
<code>sensor_name</code>	침입 이벤트를 생성한 관리되는 디바이스의 이름입니다.
<code>sensor_uuid</code>	관리되는 디바이스의 고유한 식별자입니다. 또는 <code>sensor_name</code> 이 null인 경우 0입니다.
<code>start_time_sec</code>	측정 간격이 시작된 날짜 및 시간의 UNIX 타임스탬프입니다. 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3 을(를) 참조하십시오.

storage_stats_by_file_type_current_timeframe 조인

`session_stats_current_timeframe` 테이블에서는 조인을 수행할 수 없습니다.

storage_stats_by_file_type_current_timeframe 샘플 쿼리

다음 쿼리는 현재까지의 날짜 동안 각 센서에 삭제 및 저장된 파일의 수를 반환하며, 이는 file_type을 기준으로 내림차순 정렬됩니다.

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

transmission_stats_by_file_type_current_timeframe

transmission_stats_by_file_type_current_timeframe 테이블에는 파일 유형별로 저장된 파일에 대한 통계가 포함됩니다. 통계는 바이트, 연결, 센서, 시간을 기준으로 추출할 수 있음

current_day, current_month, current_year 통계 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

transmission_stats_by_file_type_current_timeframe 테이블에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- [transmission_stats_by_file_type_current_timeframe 필드, 페이지 5-17](#)
- [transmission_stats_by_file_type_current_timeframe 조인, 페이지 5-18](#)
- [transmission_stats_by_file_type_current_timeframe 샘플 쿼리, 페이지 5-18](#)

transmission_stats_by_file_type_current_timeframe 필드

다음 표에는 storage_stats_by_file_type_current_timeframe 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다. 이러한 유형의 모든 테이블에는 동일한 필드가 포함됩니다.

표 5-13 transmission_stats_by_file_type_current_timeframe 필드

필드	설명
bytes_sent	전송된 바이트의 수입입니다.
file_type	탐지 또는 격리된 파일의 파일 유형입니다.
file_type_id	파일 유형에 매핑되는 ID 번호입니다.
number_dropped	이러한 유형의 파일이 삭제된 수입입니다.
number_sent	이러한 유형의 파일이 전송된 수입입니다.
sensor	파일을 탐지한 디바이스의 ID입니다.
sensor_address	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 ipv4_address, ipv6_address입니다.
sensor_name	침입 이벤트를 생성한 관리되는 디바이스의 이름입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 sensor_name이 null인 경우 0입니다.
start_time_sec	측정 간격이 시작된 날짜 및 시간의 UNIX 타임스탬프입니다. 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3 을(를) 참조하십시오.

transmission_stats_by_file_type_current_timeframe 조인

`transmission_stats_current_timeframe` 테이블에서는 조인을 수행할 수 없습니다.

transmission_stats_by_file_type_current_timeframe 샘플 쿼리

다음 쿼리는 현재까지의 날짜 동안 각 센서에 삭제 및 전송된 연결의 수를 반환하며, 이는 `file_type`을 기준으로 내림차순 정렬됩니다.

```
SELECT sensor_name, number_dropped, number_sent, file_type
FROM transmission_stats_by_file_type_current_day
ORDER BY file_type DESC;
```

url_category_stats_current_timeframe

`url_category_stats_current_timeframe` 테이블에는 지정된 URL 카테고리의 URL에 대한 요청과 관련된 대역폭 사용량 및 연결에 대한 통계가 포함됩니다. 트래픽을 모니터링한 관리되는 디바이스에 대한 쿼리도 제한할 수 있습니다.

`current_day`, `current_month`, `current_year` 통계 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

`url_category_stats_current_timeframe` 테이블에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- [url_category_stats_current_timeframe 필드, 페이지 5-18](#)
- [url_category_stats_current_timeframe 조인, 페이지 5-19](#)
- [url_category_stats_current_timeframe 샘플 쿼리, 페이지 5-19](#)

url_category_stats_current_timeframe 필드

다음 표에는 `url_category_stats_current_timeframe` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 5-14 `url_category_stats_current_timeframe` 필드

필드	설명
<code>bytes_in</code>	지정된 간격 동안 인바운드 트래픽의 바이트 수입니다.
<code>bytes_out</code>	지정된 간격 동안 아웃바운드 트래픽의 바이트 수입니다.
<code>category</code>	URL의 카테고리입니다.
<code>connections_allowed</code>	지정된 URL 카테고리에 허용된 연결의 수입니다.
<code>connections_denied</code>	액세스 제어 정책 위반으로 인해 지정된 URL 카테고리에 거부된 연결의 수입니다.
<code>sensor_address</code>	트래픽을 모니터링한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
<code>sensor_id</code>	트래픽을 탐지한 관리되는 디바이스의 내부 ID 번호입니다.
<code>sensor_name</code>	트래픽을 모니터링한 관리되는 디바이스입니다.

표 5-14 url_category_stats_current_timeframe 필드(계속)

필드	설명
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 sensor_name이 null인 경우 0입니다.
start_time_sec	측정 간격의 시작에 대한 UNIX 타임스탬프입니다. 시작 시간 지정에 대한 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3 을(를) 참조하십시오.

url_category_stats_current_timeframe 조인

url_category_stats_current_timeframe 테이블에서는 조인을 수행할 수 없습니다.

url_category_stats_current_timeframe 샘플 쿼리

다음 쿼리는 URL 카테고리 레코드를 최대 25개까지 반환합니다. 각 레코드에는 인바운드 및 아웃바운드 트래픽과 관련된 바이트 수는 물론, 지정된 시간 간격 동안 허용 및 차단된 연결이 포함됩니다.

```
SELECT category, sensor_name, sensor_address, start_time_sec, bytes_in, bytes_out,
connections_allowed, connections_denied
FROM url_category_stats_current_year
WHERE category="Games"
LIMIT 0, 25;
```

url_reputation_stats_current_timeframe

url_reputation_stats_current_timeframe 테이블에는 지정된 평판이 포함된 URL에 대한 요청과 관련된 대역폭 사용량 및 연결에 대한 통계가 포함됩니다. 또한 쿼리 결과는 트래픽을 모니터링한 관리되는 디바이스에서 제한될 수 있습니다.

current_day, current_month, current_year 통계 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

url_reputation_stats_current_timeframe 테이블에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- url_reputation_stats_current_timeframe 필드, [페이지 5-20](#)
- url_reputation_stats_current_timeframe 조인, [페이지 5-20](#)
- url_reputation_stats_current_timeframe 샘플 쿼리, [페이지 5-20](#)

url_reputation_stats_current_timeframe 필드

다음 표에는 `url_category_stats_current_timeframe` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 5-15 url_reputation_stats_current_timeframe 필드

필드	설명
bytes_in	지정된 간격 동안 인바운드 트래픽의 바이트 수입니다.
bytes_out	지정된 간격 동안 아웃바운드 트래픽의 바이트 수입니다.
connections_allowed	허용된 연결의 수입니다.
connections_denied	액세스 제어 정책 위반으로 인해 거부된 연결의 수입니다.
reputation	요청한 URL과 관련된 위험입니다. 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> High risk Suspicious site Benign site with security risks Benign site Well known Risk unknown
sensor_address	트래픽을 모니터링한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
sensor_id	트래픽을 모니터링한 관리되는 디바이스의 내부 ID 번호입니다.
sensor_name	트래픽을 모니터링한 관리되는 디바이스의 이름입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 <code>sensor_name</code> 이 null인 경우 0입니다.
start_time_sec	측정 간격의 시작에 대한 UNIX 타임스탬프입니다. 시작 시간 지정에 대한 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3 을(를) 참조하십시오.

url_reputation_stats_current_timeframe 조인

`url_reputation_stats_current_timeframe` 테이블에서 조인을 수행할 수 있습니다.

url_reputation_stats_current_timeframe 샘플 쿼리

다음 쿼리는 `url_reputation_stats_current_month` 테이블에서 평판 레코드를 최대 25개까지 반환합니다. 각 레코드에는 인바운드 및 아웃바운드 트래픽의 바이트 수는 물론, 측정 기간 간격 동안 허용 및 차단된 연결이 포함됩니다.

```
SELECT sensor_name, sensor_address, reputation, start_time_sec, bytes_in, bytes_out,
connections_allowed, connections_denied
FROM url_reputation_stats_current_year
WHERE reputation="High risk"
LIMIT 0, 25;
```


user_ids_stats_current_timeframe

`user_ids_stats_current_timeframe` 테이블은 액세스 필터링에 대한 통계 및 사용자에 의한 영향 통계가 포함된 Round Robin 테이블입니다.

이러한 유형의 `current_day`, `current_month`, `current_year` 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

Round Robin 통계 테이블 사용에 대한 일반적인 정보는 [통계 추적 테이블 이해, 페이지 5-2](#)을(를) 참조하십시오.

`user_ids_stats_current_timeframe` 테이블에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- [user_ids_stats_current_timeframe 필드, 페이지 5-21](#)
- [user_ids_stats_current_timeframe 조인, 페이지 5-22](#)
- [user_ids_stats_current_timeframe 샘플 쿼리, 페이지 5-22](#)

user_ids_stats_current_timeframe 필드

다음 표에는 `user_ids_stats_current_timeframe` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 5-16 `user_ids_stats_current_timeframe` 필드

필드	설명
<code>blocked</code>	침입 정책 위반으로 인해 차단된 연결 수입입니다.
<code>impact_level_1</code>	사용자에 대해 기록된 영향 레벨 1(vulnerable) 침입 이벤트의 수입입니다.
<code>impact_level_2</code>	사용자에 대해 기록된 영향 레벨 2(potentially vulnerable) 침입 이벤트의 수입입니다.
<code>impact_level_3</code>	사용자에 대해 기록된 영향 레벨 3(host currently not vulnerable) 침입 이벤트의 수입입니다.
<code>impact_level_4</code>	사용자에 대해 기록된 영향 레벨 4(unknown target) 침입 이벤트의 수입입니다.
<code>impact_level_5</code>	사용자에 대해 기록된 영향 레벨 5(unknown vulnerability) 침입 이벤트의 수입입니다.
<code>sensor_address</code>	트래픽을 모니터링한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
<code>sensor_id</code>	트래픽을 탐지한 관리되는 디바이스의 내부 ID 번호입니다.
<code>sensor_name</code>	트래픽을 탐지한 관리되는 디바이스의 이름입니다.
<code>sensor_uuid</code>	관리되는 디바이스의 고유한 식별자입니다. 또는 <code>sensor_name</code> 이 null인 경우 0입니다.
<code>start_time_sec</code>	측정 간격의 시작에 대한 UNIX 타임스탬프입니다. 시작 시간 지정에 대한 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3 을(를) 참조하십시오.
<code>user_id</code>	호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
<code>username</code>	호스트에 마지막으로 로그인한 사용자의 사용자 이름입니다.
<code>would_have_dropped</code>	인라인 구축에서 패킷을 삭제하도록 침입 정책을 구성한 경우 삭제되었을 가능성이 있는 패킷의 수입입니다.

user_ids_stats_current_timeframe 조인

`user_ids_stats_current_timeframe` 테이블에서는 조인을 수행할 수 없습니다.

user_ids_stats_current_timeframe 샘플 쿼리

다음 쿼리는 `user_ids_stats_current_month` 테이블에서 사용자 레코드를 최대 25개까지 반환합니다. 각 레코드에는 선택한 `username`의 차단된 연결 및 침입 이벤트 수가 포함됩니다.

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

LIMIT 0, 25;
```

user_stats_current_timeframe

`user_stats_current_timeframe` 테이블에는 사용자를 기준으로 한 대역폭 사용량 및 액세스 제어 활동(연결 허용 또는 거부)에 대한 통계가 포함됩니다. 트래픽을 모니터링한 관리되는 디바이스에 대한 쿼리도 제한할 수 있습니다.

`current_day`, `current_month`, `current_year` 통계 테이블에 대해 알아보려면 [통계 추적 테이블의 저장 특성, 페이지 5-2](#)을(를) 참조하십시오.

자세한 내용은 다음 섹션을 참조하십시오.

- [user_stats_current_timeframe 필드, 페이지 5-22](#)
- [user_stats_current_timeframe 조인, 페이지 5-23](#)
- [user_stats_current_timeframe 샘플 쿼리, 페이지 5-23](#)

user_stats_current_timeframe 필드

다음 표에는 `user_stats_current_timeframe` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 5-17 `user_stats_current_timeframe` 필드

필드	설명
<code>bytes_in</code>	측정된 간격 동안 사용자에 대한 인바운드 트래픽의 바이트 수입니다.
<code>bytes_out</code>	측정된 간격 동안 사용자에 대한 아웃바운드 트래픽의 바이트 수입니다.
<code>connections_allowed</code>	측정된 기간 동안 이 사용자에게 허용된 연결의 수입니다.
<code>connections_denied</code>	액세스 제어 정책 위반으로 인해 이 사용자에게 거부된 연결의 수입니다.
<code>sensor_address</code>	트래픽을 모니터링한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
<code>sensor_id</code>	트래픽을 탐지한 관리되는 디바이스의 내부 ID 번호입니다.
<code>sensor_name</code>	트래픽을 탐지한 관리되는 디바이스의 이름입니다.

표 5-17 user_stats_current_timeframe 필드(계속)

필드	설명
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 sensor_name이 null인 경우 0입니다.
start_time_sec	측정 간격의 시작에 대한 UNIX 타임스탬프입니다. 시작 시간 지정에 대한 자세한 내용은 통계 테이블 쿼리 시 시간 간격 지정, 페이지 5-3 을(를) 참조하십시오.
user_id	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
username	트래픽을 생성한 호스트에 마지막으로 로그인한 사용자의 사용자 이름입니다.

user_stats_current_timeframe 조인

user_stats_current_timeframe 테이블에서는 조인을 수행할 수 없습니다.

user_stats_current_timeframe 샘플 쿼리

다음 쿼리는 사용자 레코드를 최대 25개까지 반환합니다. 각 레코드에는 인바운드 및 아웃바운드 트래픽의 바이트 수는 물론, 측정 기간 간격 동안 허용 및 차단된 연결이 포함됩니다.

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

■ user_stats_current_timeframe



스키마: 검색 이벤트 및 네트워크 맵 테이블

이 장에는 검색 이벤트 및 Cisco 네트워크 맵과 관련된 테이블의 스키마 및 지원되는 조인에 대한 정보가 포함되어 있습니다.

FireSIGHT System은 호스트 및 네트워크 디바이스에서 생성된 트래픽을 모니터링하므로 검색 이벤트를 지속적으로 생성합니다.

네트워크 맵은 검색 이벤트에서 보고된 네트워크 자산에 대한 정보의 저장소입니다. 네트워크 맵에는 각 탐지된 호스트 및 네트워크 디바이스의 운영 체제, 서버, 클라이언트 애플리케이션, 호스트 속성, 취약성 등과 같은 정보가 포함됩니다.

취약성은 호스트가 영향을 받기 쉬운 특정 보안 침해 또는 공격용 악성코드에 대한 설명입니다. Cisco에서는 Bugtraq 데이터베이스 및 MITRE의 CVE 데이터베이스를 상호 참조하는 자체적인 취약성 데이터베이스(VDB)를 유지하고 있습니다. 또한 호스트 입력 기능을 사용하여 서드파티 취약성 데이터를 가져올 수도 있습니다.

네트워크 맵의 특정 호스트에 대한 정보는 호스트 유형 및 모니터링된 트래픽에서 제공되는 정보에 따라 달라질 수 있습니다.

자세한 내용은 아래 표에 나열된 섹션을 참조하십시오. 버전 열은 각 테이블을 지원하는 FireSIGHT System 버전을 나타냅니다. 현재 제품 릴리스에서도 사용 중단된 테이블을 계속 지원하고 있으나, 향후에도 지속적인 지원을 받으려면 사용 중단된 테이블 및 필드를 사용하지 않는 것이 좋습니다.

표 6-1 검색 이벤트 및 네트워크 맵 테이블의 스키마

참조	다음에 대한 정보가 저장되는 테이블	버전
application_host_map , 페이지 6-5	모니터링되는 네트워크에 있는 호스트에서 탐지된 애플리케이션	5.0+
application_ip_map , 페이지 A-1	모니터링되는 네트워크에서 탐지된 애플리케이션과 관련된 카테고리, 태그, 생산성, 위험	5.2+
application_ip_map , 페이지 A-1	모니터링되는 네트워크에서 탐지된 애플리케이션과 관련된 카테고리, 태그, 생산성, 위험 버전 5.2에서 사용 중단되었으며 application_ip_map , 페이지 A-1(으)로 대체됨	5.0-5.1.x
application_tag_map , 페이지 6-8	모니터링되는 네트워크에서 탐지된 애플리케이션과 관련된 태그	5.0+
network_discovery_event , 페이지 6-10	검색 및 호스트 입력 이벤트	5.0+
rna_host , 페이지 6-12	모니터링되는 네트워크에 있는 호스트에 대한 기본 정보	5.2+

표 6-1 검색 이벤트 및 네트워크 맵 테이블의 스키마(계속)

참조	다음에 대한 정보가 저장되는 테이블	버전
rna_host_attribute, 페이지 6-13	모니터링되는 네트워크에 있는 각 호스트와 관련된 호스트 속성	5.2+
rna_host_client_app, 페이지 6-15	모니터링되는 네트워크에 있는 호스트에서 탐지된 클라이언트 애플리케이션	5.2+
rna_host_client_app, 페이지 6-15	모니터링되는 네트워크에 있는 호스트에서 탐지된 HTTP(웹 브라우저) 웹클라이언트 애플리케이션과 관련된 페이로드	5.2+
rna_host_ioc_state, 페이지 6-20	호스트의 보안 침해 상태를 저장함	5.3+
rna_host_ip_map, 페이지 6-24	호스트 ID를 모니터링되는 네트워크에 있는 호스트의 MAC 주소와 상호 연결함	5.2+
rna_host_os, 페이지 6-26	모니터링되는 네트워크에 있는 호스트에서 탐지된 운영 체제	5.2+
rna_host_os_vulns, 페이지 6-28	모니터링되는 네트워크에 있는 호스트와 관련된 취약성	5.2+
rna_host_protocol, 페이지 6-30	모니터링되는 네트워크에 있는 호스트에서 탐지된 프로토콜	4.10.x+
rna_host_protocol, 페이지 6-30	호스트를 탐지한 관리되는 디바이스와 관련한 모니터링되는 네트워크에 있는 호스트	5.2+
rna_host_service, 페이지 6-33	모니터링되는 네트워크에 있는 호스트에서 탐지된 서비스	5.2+
rna_host_service_banner, 페이지 6-35	모니터링되는 네트워크에 있는 호스트에서 탐지된 서비스의 서비스 공급업체 및 버전("배너")을 광고하는 네트워크 트래픽의 헤더	5.2+
rna_host_service_info, 페이지 6-36	모니터링되는 네트워크에 있는 호스트에서 탐지된 서비스의 상세 정보	5.2+
rna_host_service_payload, 페이지 6-39	모니터링되는 네트워크에 있는 호스트에서 탐지된 서비스와 관련된 페이로드	5.2+
rna_host_service_subtype, 페이지 6-42	모니터링되는 네트워크에 있는 호스트에서 탐지된 서비스의 하위 서비스	5.2+
rna_host_service_vulns, 페이지 6-43	모니터링되는 네트워크에 있는 호스트에서 탐지된 서비스와 관련된 취약성	5.2+
rna_host_third_party_vuln, 페이지 6-45	모니터링되는 네트워크에 있는 호스트와 관련된 서드파티 취약성	5.2+
rna_host_third_party_vuln_bugtraq_id, 페이지 6-46	모니터링되는 네트워크에 있는 호스트와 관련되어 있고 Bugtraq 데이터베이스의 취약성과도 관련된 서드파티 취약성(http://www.securityfocus.com/bid/)	5.2+
rna_host_third_party_vuln_cve_id, 페이지 6-48	모니터링되는 네트워크에 있는 호스트와 관련되어 있고 MITRE CVE 데이터베이스의 취약성과도 관련된 서드파티 취약성 (http://www.cve.mitre.org/)	5.2+
rna_host_third_party_vuln_rna_id, 페이지 6-50	모니터링되는 네트워크에 있는 호스트와 관련되어 있고 VDB 내의 취약성과도 관련된 서드파티 취약성	5.2+

표 6-1 검색 이벤트 및 네트워크 맵 테이블의 스키마(계속)

참조	다음에 대한 정보가 저장되는 테이블	버전
rna_ip_host, 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트에 대한 기본 정보. 버전 5.2에서 사용 중단되었으며 rna_host, 페이지 6-12(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_client_app, 페이지 A-1	모니터링되는 네트워크에 있는 호스트에서 탐지된 클라이언트 애플리케이션 버전 5.2에서 사용 중단되었으며 rna_host_client_app, 페이지 6-15(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_client_app_payload, 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트에서 탐지된 HTTP(웹 브라우저) 웹클라이언트 애플리케이션과 관련된 페이로드. 버전 5.2에서 사용 중단되었으며 rna_host_client_app, 페이지 6-15(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_os, 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트에서 탐지된 운영 체제 버전 5.2에서 사용 중단되었으며 rna_host_os, 페이지 6-26(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_os_vulns, 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트와 관련된 취약성. 버전 5.2에서 사용 중단되었으며 rna_host_os_vulns, 페이지 6-28(으)로 대체됨	4.10.x--5.1.x
rna_ip_host_sensor, 페이지 A-1	IP 호스트를 탐지한 관리되는 디바이스와 관련한 모니터링되는 네트워크에 있는 IP 호스트. 버전 5.2에서 사용 중단되었으며 rna_host_protocol, 페이지 6-30(으)로 대체됨	5.0-5.1.x
rna_ip_host_service, 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트에서 탐지된 서비스. 버전 5.2에서 사용 중단되었으며 rna_host_service, 페이지 6-33(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_service_banner, 페이지 A-1	모니터링되는 네트워크에 있는 호스트에서 탐지된 서비스의 서비스 공급업체 및 버전("배너")을 광고하는 네트워크 트래픽의 헤더 버전 5.2에서 사용 중단되었으며 rna_host_service_banner, 페이지 6-35(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_service_info, 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트에서 탐지된 서비스의 상세 정보. 버전 5.2에서 사용 중단되었으며 rna_host_service_info, 페이지 6-36(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_service_payload, 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트에서 탐지된 서비스와 관련된 페이로드. 버전 5.2에서 사용 중단되었으며 rna_host_service_payload, 페이지 6-39(으)로 대체됨	4.10.x-5.1.x

표 6-1 검색 이벤트 및 네트워크 맵 테이블의 스키마(계속)

참조	다음에 대한 정보가 저장되는 테이블	버전
rna_ip_host_service_subtype , 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트에서 탐지된 서비스의 하위 서비스. 버전 5.2에서 사용 중단되었으며 rna_host_service_subtype , 페이지 6-42(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_service_vulns , 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트에서 탐지된 서비스와 관련된 취약성. 버전 5.2에서 사용 중단되었으며 rna_host_service_vulns , 페이지 6-43(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_third_party_vuln , 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트와 관련된 서드파티 취약성. 버전 5.2에서 사용 중단되었으며 rna_host_third_party_vuln , 페이지 6-45(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_third_party_vuln_bugtraq_id , 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트와 관련되어 있고 Bugtraq 데이터베이스의 취약성과도 관련된 서드파티 취약성(http://www.securityfocus.com/bid/). 버전 5.2에서 사용 중단되었으며 rna_host_third_party_vuln_bugtraq_id , 페이지 6-46(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_third_party_vuln_cve_id , 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트와 관련되어 있고 MITRE CVE 데이터베이스의 취약성과도 관련된 서드파티 취약성. (http://www.cve.mitre.org/) 버전 5.2에서 사용 중단되었으며 rna_host_third_party_vuln_cve_id , 페이지 6-48(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_third_party_vuln_rna_id , 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트와 관련되어 있고 VDB 내의 취약성과도 관련된 서드파티 취약성. 버전 5.2에서 사용 중단되었으며 rna_host_third_party_vuln_rna_id , 페이지 6-50(으)로 대체됨	4.10.x-5.1.x
rna_ip_host_user_history , 페이지 A-1	모니터링되는 네트워크에 있는 특정 IP 호스트에 대한 사용자 활동. 버전 5.2에서 사용 중단되었으며 user_ipaddr_history , 페이지 6-57(으)로 대체됨	4.10.x-5.1.x
rna_mac_host , 페이지 A-1	모니터링되는 네트워크에 있는 MAC 호스트(IP 주소가 없는 호스트)	4.10.x-5.1.x
rna_mac_host_sensor , 페이지 A-1	IP 호스트를 탐지한 관리되는 디바이스와 관련한 모니터링되는 네트워크에 있는 IP 호스트	5.0-5.1.x
rna_mac_ip_map , 페이지 A-1	모니터링되는 네트워크에 있는 IP 호스트의 MAC 주소. 버전 5.2에서 사용 중단되었으며 rna_host_ip_map , 페이지 6-24 및 rna_host_mac_map , 페이지 6-25(으)로 대체됨	4.10.x-5.1.x

표 6-1 검색 이벤트 및 네트워크 맵 테이블의 스키마(계속)

참조	다음에 대한 정보가 저장되는 테이블	버전
rna_vuln , 페이지 6-52	Cisco VDB 내의 취약성	4.10.x+
tag_info , 페이지 6-55	탐지된 애플리케이션을 구분하는 태그	5.0+
url_categories , 페이지 6-56	모니터링되는 네트워크에 있는 호스트에서 액세스한 URL을 구분하는 카테고리	5.0+
url_reputations , 페이지 6-57	모니터링되는 네트워크에 있는 호스트에서 액세스한 URL을 구분하는 평판	5.0+
user_ipaddr_history , 페이지 6-57	모니터링되는 네트워크에 있는 특정 호스트에 대한 사용자 활동	5.2+

application_host_map

`application_host_map` 테이블에는 네트워크에서 탐지된 각 애플리케이션과 관련된 카테고리 및 태그에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [application_host_map 필드](#), 페이지 6-5
- [application_host_map 조인](#), 페이지 6-6
- [application_host_map 샘플 쿼리](#), 페이지 6-7

application_host_map 필드

다음 표에는 `application_host_map` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-2 application_host_map 필드

필드	설명
<code>application_id</code>	애플리케이션의 내부 ID 번호입니다.
<code>application_name</code>	사용자 인터페이스에 표시되는 애플리케이션 이름입니다.
<code>application_tag_id</code>	이 필드는 사용이 중단되었으며 이제부터는 <code>null</code> 을 반환합니다.
<code>business_relevance</code>	애플리케이션의 비즈니스 생산성에 대한 연관성을 1에서 5까지 나타내는 지수이며 1은 매우 낮음, 5는 매우 높음을 의미합니다.
<code>business_relevance_description</code>	비즈니스 연관성(<code>very low, low, medium, high, very high</code>)에 대한 설명입니다.
<code>host_id</code>	호스트의 ID 번호입니다.
<code>risk</code>	애플리케이션의 위험도를 1에서 5까지 나타내는 지수이며 1은 매우 낮은 위험, 5는 심각한 위험을 의미합니다.
<code>risk_description</code>	위험(<code>very low, low, medium, high, critical</code>)에 대한 설명입니다.

application_host_map 조인

다음 표에는 `application_host_map` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-3 application_host_map 조인

다음에 대해 이 테이블 조인 가능	추가
application_id	<pre> 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 </pre>
host_id	<pre> 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 </pre>

application_host_map 샘플 쿼리

다음 쿼리는 host_id가 8인 호스트에서 탐지된 애플리케이션에 대한 정보를 반환합니다.

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

application_info

application_info 테이블에는 모니터링되는 네트워크에 있는 호스트에서 탐지될 수 있는 애플리케이션에 대한 정보가 포함됩니다.

application_id에서 조인을 수행하여 application_tag_map 테이블의 애플리케이션과 관련된 태그 목록을 검색할 수 있습니다. 이와 마찬가지로, application_id에서 조인을 수행하여 application_host_map의 카테고리화 관련된 애플리케이션을 검색할 수 있습니다.

자세한 내용은 다음 섹션을 참조하십시오.

- application_info 필드, 페이지 6-7
- application_info 조인, 페이지 6-8
- application_info 샘플 쿼리, 페이지 6-8

application_info 필드

다음 표에는 application_info 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-4 application_info 필드

필드	설명
application_description	애플리케이션에 대한 설명입니다.
application_id	애플리케이션의 내부 ID 번호입니다.
application_name	사용자 인터페이스에 표시되는 애플리케이션 이름입니다.
business_relevance	애플리케이션의 비즈니스 생산성에 대한 연관성을 1에서 5까지 나타내는 지수이며 1은 매우 낮음, 5는 매우 높음을 의미합니다.
business_relevance_description	비즈니스 연관성(very low, low, medium, high, very high)에 대한 설명입니다.
is_client_application	탐지된 애플리케이션이 클라이언트인지 나타내는 true-false 플래그입니다.
is_server_application	탐지된 애플리케이션이 서버 애플리케이션인지 나타내는 true-false 플래그입니다.
is_web_application	탐지된 애플리케이션이 웹 애플리케이션인지 나타내는 true-false 플래그입니다.
risk	애플리케이션의 예상 위험도를 1에서 5까지 나타내는 지수이며 1은 매우 낮은 위험, 5는 심각한 위험을 의미합니다.
risk_description	위험(very low, low, medium, high, critical)에 대한 설명입니다.

application_info 조인

다음 표에는 `application_info` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-5 application_info 조인

다음에 대해 이 테이블 조인 가능	추가
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 샘플 쿼리

다음 쿼리는 `host_id`가 8인 애플리케이션의 레코드를 반환합니다.

```
SELECT application_id, application_name, application_description, business_relevance,
risk
FROM application_info
WHERE application_id="8";
```

application_tag_map

`application_tag_map` 테이블에는 네트워크에 탐지된 각 애플리케이션과 관련된 태그에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- `application_tag_map` 필드, 페이지 6-9
- `application_tag_map` 조인, 페이지 6-9
- `application_tag_map` 샘플 쿼리, 페이지 6-10

application_tag_map 필드

다음 표에는 `application_tag_map` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-6 application_tag_map 필드

필드	설명
application_id	애플리케이션의 내부 ID 번호입니다.
application_name	사용자 인터페이스에 표시되는 애플리케이션입니다.
tag_id	태그의 내부 ID 번호입니다.
tag_name	사용자 인터페이스에 표시되는 태그의 텍스트입니다.
tag_type	다음 중 하나에 해당합니다. category 또는 type

application_tag_map 조인

다음 표에는 `application_tag_map` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-7 application_tag_map 조인

다음에 대해 이 테이블 조인 가능	추가
application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id si_connection_log.application_protocol_name si_connection_log.application_protocol_id si_connection_log.client_application_id si_connection_log.web_application_id
tag_id	tag_info.tag_id

application_tag_map 샘플 쿼리

다음 쿼리는 지정된 애플리케이션과 관련된 모든 태그 레코드를 반환합니다.

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

network_discovery_event

`network_discovery_event` 테이블에는 검색 및 호스트 입력 이벤트에 대한 정보가 포함됩니다. FireSIGHT System은 모니터링되는 네트워크에서 변경 사항이 탐지되면, 새 네트워크 기능을 검색하거나 이전에 식별된 네트워크 자산의 변경 사항을 탐지하여 검색 이벤트를 생성합니다. FireSIGHT System은 사용자가 네트워크 자산을 추가, 수정 또는 삭제하여 네트워크 맵을 수동으로 수정한 경우 호스트 입력 이벤트를 생성합니다.

FireSIGHT System 버전 5.0부터 사용 중단된 `rna_events` 테이블은 `network_discovery_event` 테이블로 대체됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [network_discovery_event 필드, 페이지 6-10](#)
- [network_discovery_event 조인, 페이지 6-11](#)
- [network_discovery_event 샘플 쿼리, 페이지 6-11](#)

network_discovery_event 필드

다음 표에는 `network_discovery_event` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-8 `network_discovery_event` 필드

필드	설명
<code>confidence</code>	서비스 확인을 위해 FireSIGHT System에서 할당한 신뢰도 등급(0~100)입니다.
<code>description</code>	이벤트에 대한 설명입니다.
<code>event_id</code>	이벤트의 내부 ID 번호입니다.
<code>event_time_sec</code>	이벤트가 생성된 날짜 및 시간의 UNIX 타임스탬프입니다.
<code>event_time_usec</code>	이벤트 타임스탬프가 마이크로초 단위로 증가한 값입니다.
<code>event_type</code>	이벤트 유형 예를 들어, <code>New Host</code> 또는 <code>Identity Conflict</code> 입니다.
<code>ip_address</code>	이 필드는 사용이 중단되었으며 이제부터는 <code>null</code> 을 반환합니다.
<code>ipaddr</code>	이벤트와 관련된 호스트의 IPv4 또는 IPv6 주소를 이진수로 나타낸 값입니다.
<code>mac_address</code>	이벤트와 관련된 호스트의 MAC 주소입니다.
<code>mac_vendor</code>	이벤트와 관련된 호스트의 NIC 하드웨어 공급업체입니다.
<code>port</code>	이벤트를 트리거한 네트워크 트래픽에서 사용하는 포트입니다.
<code>sensor_address</code>	검색 이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.

표 6-8 network_discovery_event 필드(계속)

필드	설명
sensor_name	검색 이벤트를 생성한 관리되는 디바이스입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 sensor_name이 null인 경우 0입니다.
user_dept	호스트에 마지막으로 로그인한 사용자의 부서입니다.
user_email	호스트에 마지막으로 로그인한 사용자의 이메일 주소입니다.
user_first_name	호스트에 마지막으로 로그인한 사용자의 이름입니다.
user_id	호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
user_last_name	호스트에 마지막으로 로그인한 사용자의 성입니다.
user_last_seen_sec	호스트에 마지막으로 로그인한 사용자의 사용자 활동을 FireSIGHT System에서 마지막으로 탐지한 날짜 및 시간의 UNIX 타임스탬프입니다.
user_last_updated_sec	호스트에 마지막으로 로그인한 사용자의 사용자 레코드를 FireSIGHT System에서 마지막으로 업데이트한 날짜 및 시간의 UNIX 타임스탬프입니다.
user_name	호스트에 마지막으로 로그인한 사용자의 사용자 이름입니다.
user_phone	호스트에 마지막으로 로그인한 사용자의 전화 번호입니다.

network_discovery_event 조인

다음 표에는 network_discovery_event 테이블을 사용하여 수행할 수 있는 조인이 설명되어 있습니다.

표 6-9 network_discovery_event 조인

다음에 대해 이 테이블 조인 가능	추가
ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

network_discovery_event 샘플 쿼리

다음 쿼리는 지정된 기간 내의 사용자, 탐지한 디바이스 이름, 타임스탬프, 호스트 IP 주소 등이 포함된 검색 이벤트 레코드를 반환합니다.

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

rna_host

rna_host 테이블에는 모니터링되는 네트워크에 있는 호스트에 대한 기본 정보가 포함됩니다.

이 테이블은 버전 5.2부터 rna_ip_host를 대체합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- rna_host 필드, 페이지 6-12
- rna_host 조인, 페이지 6-13
- rna_host 샘플 쿼리, 페이지 6-13

rna_host 필드

다음 표에는 rna_host 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-10 rna_host 필드

필드	설명
criticality	호스트 중요도(None, Low, Medium, High)입니다.
hops	호스트에서 호스트를 탐지한 관리되는 디바이스로의 네트워크 홉 수입니다.
host_id	호스트의 ID 번호입니다.
host_name	호스트의 이름입니다.
host_type	호스트 유형(Host, Router, Bridge, NAT Device, Load Balancer)입니다.
jailbroken	모바일 디바이스의 운영 체제가 탈옥되었는지 나타내는 true-false 플래그입니다.
last_seen_sec	호스트 작업이 마지막으로 탐지된 날짜 및 시간의 UNIX 타임스탬프입니다.
mobile	탐지된 호스트가 모바일 디바이스인지 나타내는 true-false 플래그입니다.
netbios_name	호스트 NetBIOS 이름 문자열입니다.
notes	호스트에 대한 Notes 호스트 특성의 내용입니다.
vlan_id	해당하는 경우, VLAN ID 번호입니다.
vlan_priority	VLAN 태그에 포함된 우선순위 값입니다.
vlan_type	VLAN 태그를 포함한 캡슐화된 패킷의 유형입니다. <ul style="list-style-type: none"> • 0 – 이더넷 • 1 – 토큰 링

rna_host 조인

다음 표에는 `rna_host` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-11 `rna_host` 조인

다음에 대해 이 테이블 조인 가능	추가
host_id	application_host_map.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ip_map.host_id rna_host_ioc_state.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host 샘플 쿼리

다음 쿼리는 호스트 ID, VLAN ID, 호스트가 마지막으로 표시된 시기, 호스트 유형, 호스트 유형을 기준으로 한 순서가 포함된 `rna_host` 레코드를 최대 25개까지 반환합니다.

```
SELECT host_id, vlan_id, last_seen_sec, host_type
FROM rna_host
ORDER BY host_type
LIMIT 0, 25;
```

rna_host_attribute

`rna_host_attribute` 테이블에는 모니터링되는 네트워크에 있는 각 호스트와 관련된 호스트 속성에 대한 정보가 포함됩니다. 이는 사용 중단된 `rna_ip_host_attribute` 테이블을 대체합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_attribute 필드, 페이지 6-14](#)
- [rna_host_attribute 조인, 페이지 6-14](#)
- [rna_host_attribute 샘플 쿼리, 페이지 6-14](#)

rna_host_attribute 필드

다음 표에는 rna_host_attribute 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-12 rna_host_attribute 필드

필드	설명
attribute_name	호스트 속성입니다. 예를 들어, Host Criticality 또는 Default White List입니다.
attribute_value	호스트 특성의 값입니다.
host_id	호스트의 ID 번호입니다.

rna_host_attribute 조인

다음 표에는 rna_host_attribute 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-13 rna_host_attribute 조인

다음에 대해 이 테이블 조인 가능	추가
host_id	<pre> application_host_map.host_id rna_host.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id </pre>

rna_host_attribute 샘플 쿼리

다음 쿼리는 선택한 호스트 ID와 관련된 모든 호스트 특성 및 값을 반환합니다.

```

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

```

rna_host_client_app

`rna_host_client_app` 테이블에는 모니터링되는 네트워크에 있는 호스트에서 탐지된 클라이언트 애플리케이션에 대한 정보가 포함됩니다. 이는 사용 중단된 `rna_ip_host_client_app` 테이블을 대체합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_client_app 필드, 페이지 6-15](#)
- [rna_host_client_app 조인, 페이지 6-16](#)
- [rna_host_client_app 샘플 쿼리, 페이지 6-17](#)

rna_host_client_app 필드

다음 표에는 `rna_host_client_app` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-14 `rna_host_client_app` 필드

필드	설명
<code>application</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>application_protocol_id</code>	탐지된 애플리케이션 프로토콜의 내부 식별자입니다.
<code>application_protocol_name</code>	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • <code>pending</code> - 시스템에 추가 데이터가 필요한 경우 • 연결에 애플리케이션 정보가 없는 경우 비어 있음
<code>application_type</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>client_application_id</code>	애플리케이션이 식별 가능한 경우, 애플리케이션의 내부 ID 번호입니다.
<code>client_application_name</code>	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • 일반 클라이언트 이름 - 시스템에서 클라이언트 애플리케이션을 탐지했으나 특정한 애플리케이션을 식별하지는 못한 경우 • 연결에 클라이언트 애플리케이션 정보가 없는 경우 비어 있음
<code>hits</code>	클라이언트 애플리케이션이 탐지된 횟수입니다.
<code>host_id</code>	호스트의 ID 번호입니다.
<code>last_used_sec</code>	애플리케이션이 마지막으로 탐지된 날짜 및 시간의 UNIX 타임스탬프입니다.
<code>version</code>	호스트에서 탐지된 애플리케이션의 버전입니다.

rna_host_client_app 조인

다음 표에는 `rna_host_client_app` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-15 `rna_host_client_app` 조인

다음에 대해 이 테이블 조인 가능	추가
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_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>
host_id 및 application_protocol_id 및 client_application_id 및 version	다음 집합: <code>rna_host_client_app_payload.host_id</code> <code>rna_host_client_app_payload.application_protocol_id</code> <code>rna_host_client_app_payload.client_application_id</code> <code>rna_host_client_app_payload.version</code>

표 6-15 rna_host_client_app 조인(계속)

다음에 대해 이 테이블 조인 가능	추가
application_protocol_id 또는 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 샘플 쿼리

다음 쿼리는 host_id가 8인 호스트에서 탐지된 클라이언트 애플리케이션에 대한 정보를 반환합니다.

```
SELECT host_id, client_application_id, client_application_name, version, hits,
application_protocol_id, application_protocol_name, last_used_sec
FROM rna_host_client_app
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_client_app_payload

rna_host_client_app_payload 테이블에는 모니터링되는 네트워크에서 탐지된 호스트의 웹 애플리케이션과 관련된 HTTP 트래픽의 페이로드에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_client_app_payload 필드, 페이지 6-18](#)
- [rna_host_client_app_payload 조인, 페이지 6-19](#)
- [rna_host_client_app_payload 샘플 쿼리, 페이지 6-20](#)

rna_host_client_app_payload 필드

다음 표에는 `rna_host_client_app_payload` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-16 `rna_host_client_app_payload` 필드

필드	설명
<code>application</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>application_protocol_id</code>	탐지된 애플리케이션 프로토콜의 내부 식별자입니다(제공되는 경우). 클라이언트 애플리케이션과 웹 애플리케이션의 두 가지 특성을 모두 갖고 있는 트래픽의 경우, <code>client_application_id</code> 및 <code>web_application_id</code> 필드의 값이 동일합니다.
<code>application_protocol_name</code>	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • <code>pending</code> - 시스템에 추가 데이터가 필요한 경우 • 연결에 애플리케이션 정보가 없는 경우 비어 있음
<code>application_type</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>client_application_id</code>	클라이언트 애플리케이션의 내부 ID 번호입니다.
<code>client_application_name</code>	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • 일반 클라이언트 이름 - 시스템에서 클라이언트 애플리케이션을 탐지했으나 특정한 애플리케이션을 식별하지는 못한 경우 • 연결에 클라이언트 애플리케이션 정보가 없는 경우 비어 있음
<code>host_id</code>	호스트의 ID 번호입니다.
<code>payload_name</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>payload_type</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>version</code>	호스트에서 탐지된 웹 애플리케이션의 버전입니다.
<code>web_application_id</code>	웹 애플리케이션의 내부 ID 번호입니다(제공되는 경우). 클라이언트 애플리케이션과 웹 애플리케이션의 두 가지 특성을 모두 갖고 있는 트래픽의 경우, <code>client_application_id</code> 및 <code>web_application_id</code> 필드의 값이 동일합니다.
<code>web_application_name</code>	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • <code>web browsing</code> - HTTP의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 식별하지 못하는 경우 • 연결에 HTTP 트래픽이 없는 경우 비어 있음

rna_host_client_app_payload 조인

다음 표에는 `rna_host_client_app_payload` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-17 *rna_host_client_app_payload* 조인

다음에 대해 이 테이블 조인 가능	추가
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_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>
다음 집합: <code>host_id</code> , <code>application_protocol_id</code> , <code>client_application_id</code> , <code>version</code>	다음 집합: <code>rna_host_client_app.host_id</code> <code>rna_host_client_app.application_protocol_id</code> <code>rna_host_client_app.client_application_id</code> <code>rna_host_client_app.version</code>

표 6-17 rna_host_client_app_payload 조인(계속)

다음에 대해 이 테이블 조인 가능	추가
client_application_id 또는 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 샘플 쿼리

다음 쿼리는 host_id가 8인 호스트에서 탐지된 웹 애플리케이션에 대한 정보를 반환합니다.

```
SELECT host_id, web_application_id, web_application_name, version,
client_application_id, client_application_name
FROM rna_host_client_app_payload
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_ioc_state

rna_host_ioc_state 테이블에는 모니터링되는 네트워크에 있는 호스트의 IOC 상태가 저장됩니다. 자세한 내용은 다음 섹션을 참조하십시오.

- rna_host_ioc_state 필드, 페이지 6-21
- rna_host_ioc_state 조인, 페이지 6-23
- rna_host_ioc_state 샘플 쿼리, 페이지 6-23

rna_host_ioc_state 필드

다음 표에는 `rna_host_ioc_state` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-18 `rna_host_ioc_state` 필드

필드	설명
<code>first_seen</code>	보안 침해가 처음으로 탐지되었을 때의 Unix 타임스탬프입니다.
<code>first_seen_sensor_address</code>	보안 침해를 처음으로 탐지한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
<code>first_seen_sensor_name</code>	보안 침해를 처음으로 탐지한 관리되는 디바이스입니다.
<code>host_id</code>	호스트의 ID 번호입니다.
<code>ioc_category</code>	보안 침해의 카테고리입니다. 가능한 값은 다음과 같습니다. <ul style="list-style-type: none"> • CnC Connected • Exploit Kit • High Impact Attack • Low Impact Attack • Malware Detected • Malware Executed • Dropper Infection • Java Compromise • Word Compromise • Adobe Reader Compromise • Excel Compromise • PowerPoint Compromise • QuickTime Compromise
<code>ioc_description</code>	보안 침해에 대한 설명입니다.

표 6-18 rma_host_ioc_state 필드(계속)

필드	설명
ioc_event_type	<p>보안 침해의 이벤트 유형입니다. 가능한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • Adobe Reader launched shell • Dropper Infection Detected by FireAMP • Excel Compromise Detected by FireAMP • Excel launched shell • Impact 1 Intrusion Event - attempted-admin • Impact 1 Intrusion Event - attempted-user • Impact 1 Intrusion Event - successful-admin • Impact 1 Intrusion Event - successful-user • Impact 1 Intrusion Event - web-application-attack • Impact 2 Intrusion Event - attempted-admin • Impact 2 Intrusion Event - attempted-user • Impact 2 Intrusion Event - successful-admin • Impact 2 Intrusion Event - successful-user • Impact 2 Intrusion Event - web-application-attack • Intrusion Event - exploit-kit • Intrusion Event - malware-backdoor • Intrusion Event - malware-CnC • Java Compromise Detected by FireAMP • Java launched shell • PDF Compromise Detected by FireAMP • PowerPoint Compromise Detected by FireAMP • PowerPoint launched shell • QuickTime Compromise Detected by FireAMP • QuickTime launched shell • Security Intelligence Event - CnC • Suspected Botnet Detected by FireAMP • Threat Detected by FireAMP - Subtype is 'executed' • Threat Detected by FireAMP - Subtype is not 'executed' • Threat Detected in File Transfer - Action is not 'block' • Word Compromise Detected by FireAMP • Word launched shell
ioc_id	보안 침해의 고유한 ID 번호입니다.
is_disabled	이 보안 침해가 비활성화되었는지 나타냅니다.
last_seen	이 보안 침해가 마지막으로 탐지되었을 때의 Unix 타임스탬프입니다.

표 6-18 rna_host_ioc_state 필드(계속)

필드	설명
last_seen_sensor_address	보안 침해를 마지막으로 탐지한 관리되는 디바이스의 IP 주소입니다. 형식은 <i>ipv4_address, ipv6_address</i> 입니다.
last_seen_sensor_name	보안 침해를 마지막으로 탐지한 관리되는 디바이스입니다.

rna_host_ioc_state 조인

다음 표에는 `rna_host_ioc_state` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-19 rna_host_ioc_state 조인

다음에 대해 이 테이블 조인 가능	추가
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_ioc_state 샘플 쿼리

다음 쿼리는 지정된 기간 내의 호스트를 해당 `ioc`와 함께 최대 25개까지 반환합니다.

```
SELECT host_id, ioc_id
FROM rna_host_ioc_state
WHERE first_seen
BETWEEN UNIX_TIMESTAMP("2011-10-01 00:00:00")
AND UNIX_TIMESTAMP("2011-10-07 23:59:59")
ORDER BY ioc_id DESC
LIMIT 0, 25;
```

rna_host_ip_map

`rna_host_ip_map` 테이블은 호스트 ID를 모니터링되는 네트워크에 있는 호스트의 IP 주소와 상호 연결합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_ip_map 필드, 페이지 6-24](#)
- [rna_host_ip_map 조인, 페이지 6-24](#)
- [rna_host_ip_map 샘플 쿼리, 페이지 6-25](#)

rna_host_ip_map 필드

다음 표에는 `rna_host_ip_map` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-20 `rna_host_ip_map` 필드

필드	설명
<code>host_id</code>	호스트의 ID 번호입니다.
<code>ipaddr</code>	호스트 IP 주소를 이진수로 나타낸 값입니다.

rna_host_ip_map 조인

다음 표에는 `rna_host_ip_map` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-21 `rna_host_ip_map` 조인

다음에 대해 이 테이블 조인 가능	추가
<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_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>

표 6-21 rna_host_ip_map 조인(계속)

다음에 대해 이 테이블 조인 가능	추가
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 샘플 쿼리

다음 쿼리는 선택한 호스트에 대한 MAC 정보를 반환합니다.

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

rna_host_mac_map

`rna_host_mac_map` 테이블은 호스트 ID를 모니터링되는 네트워크에 있는 호스트의 MAC 주소와 상호 연결합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_mac_map 필드, 페이지 6-25](#)
- [rna_host_mac_map 조인, 페이지 6-26](#)
- [rna_host_mac_map 샘플 쿼리, 페이지 6-26](#)

rna_host_mac_map 필드

다음 표에는 `rna_host_mac_map` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-22 rna_host_mac_map 필드

필드	설명
host_id	호스트의 ID 번호입니다.
mac_address	호스트의 MAC 주소입니다.
mac_vendor	탐지된 호스트의 네트워크 인터페이스 공급업체입니다.

rna_host_mac_map 조인

다음 표에는 `rna_host_mac_map` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-23 `rna_host_mac_map` 조인

다음에 대해 이 테이블 조인 가능	추가
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_ioc_state.host_id</code> <code>rna_host_ip_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_mac_map 샘플 쿼리

다음 쿼리는 `host_id`가 8인 호스트의 MAC 정보를 반환합니다.

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

rna_host_os

`rna_host_os` 테이블에는 모니터링되는 네트워크에 있는 호스트에서 탐지된 운영 체제에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- `rna_host_os` 필드, 페이지 6-27
- `rna_host_os` 조인, 페이지 6-27
- `rna_host_os` 샘플 쿼리, 페이지 6-28

rna_host_os 필드

다음 표에는 `rna_host_os` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-24 `rna_host_os` 필드

필드	설명
<code>confidence</code>	운영 체제 확인을 위해 FireSIGHT System에서 할당한 신뢰도 등급(0~100)입니다.
<code>created_sec</code>	호스트 작업이 처음으로 탐지된 날짜 및 시간의 UNIX 타임스탬프입니다.
<code>host_id</code>	호스트의 ID 번호입니다.
<code>last_seen_sec</code>	호스트 작업이 마지막으로 탐지된 날짜 및 시간의 UNIX 타임스탬프입니다.
<code>os_uuid</code>	호스트에서 탐지된 운영 체제의 고유한 식별자입니다. UUID는 Cisco 데이터베이스의 운영 체제 이름, 공급업체, 버전에 매핑됩니다.
<code>product</code>	호스트에서 탐지된 운영 체제입니다.
<code>source_type</code>	호스트 운영 체제 ID의 소스입니다. <ul style="list-style-type: none"> • <code>User</code> — 웹 사용자 인터페이스를 통해 데이터를 입력한 사용자의 이름 • <code>Application</code> — 호스트 입력 기능을 통해 다른 애플리케이션에서 가져온 애플리케이션 • <code>Scanner</code> — 시스템 정책을 통해 추가된 Nmap 또는 다른 스캐너 • <code>rna</code> — FireSIGHT System에 의해 탐지됨(검색 이벤트, 포트 일치 또는 패턴 일치를 기준으로 함) • <code>NetFlow</code> — NetFlow 지원 디바이스에서 내보낸 데이터
<code>vendor</code>	호스트에서 탐지된 운영 체제의 공급업체입니다.
<code>version</code>	호스트에서 탐지된 운영 체제의 버전입니다.

rna_host_os 조인

다음 표에는 `rna_host_os` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-25 rna_host_os 조인

다음에 대해 이 테이블 조인 가능	추가
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_os 샘플 쿼리

다음 쿼리는 host_id가 8인 호스트의 운영 체제 정보를 반환합니다.

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

rna_host_os_vulns

rna_host_os_vulns 테이블에는 모니터링되는 네트워크에 있는 호스트와 관련된 취약성에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_os_vulns 필드, 페이지 6-29](#)
- [rna_host_os_vulns 조인, 페이지 6-29](#)
- [rna_host_os_vulns 샘플 쿼리, 페이지 6-30](#)

rna_host_os_vulns 필드

다음 표에는 `rna_host_os_vulns` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-26 *rna_host_os_vulns* 필드

필드	설명
<code>host_id</code>	호스트의 ID 번호입니다.
<code>invalid</code>	취약성이 호스트에 유효한지 나타내는 값입니다. <ul style="list-style-type: none"> 0 – 취약성이 유효함 1 – 취약성이 유효하지 않음
<code>rna_vuln_id</code>	취약성의 내부 ID 번호입니다.

rna_host_os_vulns 조인

다음 표에는 `rna_host_os_vulns` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-27 *rna_host_os_vulns* 조인

다음에 대해 이 테이블 조인 가능	추가
<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 샘플 쿼리

다음 쿼리는 host_id가 8인 호스트의 운영 체제 취약성을 반환합니다.

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

rna_host_protocol

rna_host_protocol 테이블에는 모니터링되는 네트워크에 있는 호스트에서 탐지된 프로토콜에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- rna_host_protocol 필드, 페이지 6-30
- rna_host_protocol 조인, 페이지 6-31
- rna_host_protocol 샘플 쿼리, 페이지 6-31

rna_host_protocol 필드

다음 표에는 rna_host_protocol 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-28 rna_host_protocol 필드

필드	설명
host_id	호스트의 ID 번호입니다.
ip_address	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
layer	프로토콜이 실행되는 네트워크 레이어(Network 또는 Transport)입니다.
mac_address	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
mac_vendor	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
protocol_name	호스트에서 사용하는 트래픽 프로토콜입니다.
protocol_num	프로토콜의 IANA 지정 프로토콜 번호입니다.

rna_host_protocol 조인

다음 표에는 `rna_host_protocol` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-29 `rna_host_protocol` 조인

다음에 대해 이 테이블 조인 가능	추가
host_id	<code>rna_host.host_id</code> <code>rna_host_attribute.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> <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_protocol 샘플 쿼리

다음 쿼리는 `host_id`가 8인 호스트의 모든 프로토콜 레코드를 반환합니다.

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

rna_host_sensor

`rna_host_sensor` 테이블에는 모니터링되는 네트워크에 있는 호스트 IP 주소가 나열되며 각 호스트를 탐지한 관리되는 디바이스가 표시됩니다.

FireSIGHT System 버전 5.2부터 사용 중단된 `rna_ip_host_sensor` 테이블은 `rna_host_sensor` 테이블로 대체됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- `rna_host_sensor` 필드, 페이지 6-32
- `rna_host_sensor` 조인, 페이지 6-32
- `rna_host_sensor` 샘플 쿼리, 페이지 6-32

rna_host_sensor 필드

다음 표에는 `rna_host_sensor` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-30 rna_host_sensor 필드

필드	설명
host_id	호스트의 ID 번호입니다.
sensor_address	검색 이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
sensor_name	관리되는 디바이스의 이름입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 <code>sensor_name</code> 이 null인 경우 0입니다.

rna_host_sensor 조인

다음 표에는 `rna_host_sensor` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-31 rna_host_sensor 조인

다음에 대해 이 테이블 조인 가능	추가
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_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_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_sensor 샘플 쿼리

다음 쿼리는 `rna_host_sensor` 테이블에서 최대 25개의 호스트 및 해당 호스트를 탐지한 센서를 반환합니다.

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

rna_host_service

`rna_host_service` 테이블에는 네트워크 포트 및 트래픽 프로토콜 조합을 통해 관리되는 네트워크에 있는 호스트에서 탐지된 서버에 대한 일반적인 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_service 필드, 페이지 6-33](#)
- [rna_host_service 조인, 페이지 6-33](#)
- [rna_host_service 샘플 쿼리, 페이지 6-34](#)

rna_host_service 필드

다음 표에는 `rna_host_service` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-32 `rna_host_service` 필드

필드	설명
<code>confidence</code>	서버 확인을 위해 FireSIGHT System에서 할당한 신뢰도 등급(0~100)입니다.
<code>hits</code>	서버가 탐지된 횟수입니다.
<code>host_id</code>	호스트의 ID 번호입니다.
<code>last_used_sec</code>	서버가 마지막으로 탐지된 날짜 및 시간의 UNIX 타임스탬프입니다.
<code>port</code>	서버에서 사용하는 포트입니다.
<code>protocol</code>	트래픽 프로토콜(TCP 또는 UDP)입니다.

rna_host_service 조인

다음 표에는 `rna_host_service` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-33 rna_host_service 조인

다음에 대해 이 테이블 조인 가능	추가
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
다음 집합: host_id port protocol	다음 집합: rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol 다음 집합: rna_host_service_info.host_id rna_host_service_info.port rna_host_service_info.protocol 다음 집합: rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol

rna_host_service 샘플 쿼리

다음 쿼리는 host_id가 8인 호스트에 대해 탐지된 서버 레코드 중 처음 25개를 반환합니다.

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

rna_host_service_banner

`rna_ip_host_service_banner` 테이블에는 모니터링되는 네트워크에 있는 호스트의 서버에 대한 공급업체 및 버전("배너")을 광고하는 네트워크 트래픽의 헤더 정보가 포함됩니다. 네트워크 검색 정책에서 **Capture Banners**(배너 캡처) 옵션을 활성화하지 않는 한 FireSIGHT System에서는 서버 배너를 저장하지 않습니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_ip_host_service_banner 필드, 페이지 6-35](#)
- [rna_host_service_banner 조인, 페이지 6-35](#)
- [rna_host_service_banner 샘플 쿼리, 페이지 6-36](#)

rna_ip_host_service_banner 필드

다음 표에는 `rna_host_service_banner` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-34 `rna_host_service_banner` 필드

필드	설명
<code>banner</code>	서버 배너에는 서버에 대해 탐지된 첫 번째 패킷의 처음 256바이트가 표시됩니다.
<code>host_id</code>	호스트의 ID 번호입니다.
<code>port</code>	서버에서 사용하는 포트입니다.
<code>protocol</code>	트래픽 프로토콜(TCP 또는 UDP)입니다.

rna_host_service_banner 조인

다음 표에는 `rna_host_service_banner` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-35 `rna_host_service_banner` 조인

다음에 대해 이 테이블 조인 가능	추가
다음 집합: <code>host_id</code> <code>port</code> <code>protocol</code>	다음 집합: <code>rna_host_service.host_id</code> <code>rna_host_service.port</code> <code>rna_host_service.protocol</code> 다음 집합: <code>rna_host_service_info.host_id</code> <code>rna_host_service_info.port</code> <code>rna_host_service_info.protocol</code> 다음 집합: <code>rna_host_service_payload.host_id</code> <code>rna_host_service_payload.port</code> <code>rna_host_service_payload.protocol</code>

표 6-35 rna_host_service_banner 조인(계속)

다음에 대해 이 테이블 조인 가능	추가
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 샘플 쿼리

다음 쿼리는 host_id가 8인 호스트의 서버 배너를 반환합니다.

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

rna_host_service_info

rna_host_service_info 테이블에는 모니터링되는 네트워크에 있는 호스트에서 탐지된 서버에 대한 자세한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_service_info 필드, 페이지 6-37](#)
- [rna_host_service_info 조인, 페이지 6-38](#)
- [rna_host_service_info 샘플 쿼리, 페이지 6-39](#)

rna_host_service_info 필드

다음 표에는 rna_host_service_info 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-36 rna_host_service_info 필드

필드	설명
application_id	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 빈칸을 반환합니다.
application_protocol_id	탐지된 애플리케이션 프로토콜의 내부 식별자입니다(제공되는 경우).
application_protocol_name	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> 애플리케이션 프로토콜의 이름 - 올바른 식별이 이루어진 경우 pending - 시스템에 추가 데이터가 필요한 경우 연결에 애플리케이션 정보가 없는 경우 비어 있음
business_relevance	애플리케이션의 비즈니스 생산성에 대한 연관성을 1에서 5까지 나타내는 지수이며 1은 매우 낮음, 5는 매우 높음을 의미합니다.
business_relevance_description	비즈니스 연관성(very low, low, medium, high, very high)에 대한 설명입니다.
created_sec	애플리케이션 프로토콜이 처음으로 탐지된 날짜 및 시간의 UNIX 타임스탬프입니다.
host_id	호스트의 ID 번호입니다.
ip_address	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
last_used_sec	서버 작업이 마지막으로 탐지된 날짜 및 시간의 UNIX 타임스탬프입니다.
port	서버에서 사용하는 포트입니다.
protocol	트래픽 프로토콜(TCP 또는 UDP)입니다.
risk	애플리케이션의 위험도를 1에서 5까지 나타내는 지수이며 1은 매우 낮은 위험, 5는 매우 높은 위험을 의미합니다.
risk_description	위험(very low, low, medium, high, very high)에 대한 설명입니다.
service_info_id	서버의 내부 ID 번호입니다.
service_name	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
source_type	서버 ID의 소스입니다. <ul style="list-style-type: none"> User — 웹 사용자 인터페이스를 통해 데이터를 입력한 사용자의 이름 Application — 호스트 입력 기능을 통해 다른 애플리케이션에서 가져온 애플리케이션 Scanner — NMAP를 통해 추가되거나 소스 유형이 Scanner인 호스트 입력 기능을 통해 가져옴 rna — FireSIGHT System에 의해 탐지됨(검색 이벤트, 포트 일치 또는 패턴 일치를 기준으로 함) NetFlow — NetFlow 지원 디바이스에서 내보낸 데이터
vendor	호스트에 있는 서버의 공급업체입니다.
version	호스트에서 탐지된 서버의 버전입니다.

rna_host_service_info 조인

다음 표에는 rna_host_service_info 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-37 rna_host_service_info 조인

다음에 대해 이 테이블 조인 가능	추가
application_protocol_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_payload.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

표 6-37 rna_host_service_info 조인(계속)

다음에 대해 이 테이블 조인 가능	추가
다음 집합: host_id 및 port 및 protocol	다음 집합: rna_host_service.host_id rna_host_service.port rna_host_service.protocol 다음 집합: rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol 다음 집합: rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol

rna_host_service_info 샘플 쿼리

다음 쿼리는 host_id가 8인 호스트에서 탐지된 애플리케이션 프로토콜에 대한 정보를 반환합니다.

```
SELECT host_id, application_protocol_name, version, vendor, created_sec, last_used_sec,
business_relevance, risk
FROM rna_host_service_info
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_payload

rna_host_service_payload 테이블에는 모니터링되는 네트워크에 있는 호스트에 의해 연관된 웹 애플리케이션에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_service_payload 필드, 페이지 6-39](#)
- [rna_host_service_payload 조인, 페이지 6-40](#)
- [rna_host_service_payload 샘플 쿼리, 페이지 6-41](#)

rna_host_service_payload 필드

다음 표에는 rna_host_service_payload 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-38 rna_host_service_payload 필드

필드	설명
application_id	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
application_name	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
host_id	호스트의 ID 번호입니다.

rna_host_service_payload

표 6-38 rna_host_service_payload 필드(계속)

필드	설명
ip_address	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
payload_name	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
payload_type	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
port	서버에서 사용하는 포트입니다.
protocol	트래픽 프로토콜(TCP 또는 UDP)입니다.
web_application_id	웹 애플리케이션의 내부 ID 번호입니다.
web_application_name	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> 웹 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 web browsing - HTTP의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 식별하지 못하는 경우 연결에 HTTP 트래픽이 없는 경우 비어 있음

rna_host_service_payload 조인

다음 표에는 rna_host_service_payload 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-39 rna_host_service_payload 조인

다음에 대해 이 테이블 조인 가능	추가
web_application_id	<pre> 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 </pre>

표 6-39 rna_host_service_payload 조인(계속)

다음에 대해 이 테이블 조인 가능	추가
다음 집합: host_id port protocol	다음 집합: rna_host_service.host_id rna_host_service.port rna_host_service.protocol 다음 집합: rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol 다음 집합: 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 샘플 쿼리

다음 쿼리는 host_id가 8인 호스트에서 탐지된 웹 애플리케이션에 대한 정보를 반환합니다.

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

rna_host_service_subtype

`rna_host_service_subtype` 테이블에는 모니터링되는 네트워크에 있는 호스트에서 탐지된 서버의 하위 서버에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_service_subtype 필드, 페이지 6-42](#)
- [rna_host_service_subtype 조인, 페이지 6-43](#)
- [rna_host_service_subtype 샘플 쿼리, 페이지 6-43](#)

rna_host_service_subtype 필드

다음 표에는 `rna_host_service_subtype` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-40 `rna_host_service_subtype` 필드

필드	설명
<code>host_id</code>	호스트의 ID 번호입니다.
<code>port</code>	서버에서 사용하는 포트입니다.
<code>protocol</code>	트래픽 프로토콜(TCP 또는 UDP)입니다.
<code>service_name</code>	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 이벤트 트리거와 관련된 호스트에 있는 서버입니다. • <code>none</code> 또는 빈칸 - 데이터 식별이 불가능한 경우 • <code>pending</code> - 추가 데이터가 필요한 경우 • <code>unknown</code> - 알려진 서버 지문을 기반으로 서버를 식별할 수 없는 경우
<code>source_type</code>	서버 ID의 소스입니다. <ul style="list-style-type: none"> • <code>User</code> - 웹 사용자 인터페이스를 통해 데이터를 입력한 사용자의 이름 • <code>Application</code> - 호스트 입력 기능을 통해 다른 애플리케이션에서 가져온 애플리케이션 • <code>Scanner</code> - NMAP를 통해 추가되거나 소스 유형이 <code>Scanner</code>인 호스트 입력 기능을 통해 가져옴 • <code>rna</code> - FireSIGHT System에 의해 탐지됨(검색 이벤트, 포트 일치 또는 패턴 일치를 기준으로 함) • <code>NetFlow</code> - NetFlow 지원 디바이스에서 내보낸 데이터
<code>sub_service_name</code>	호스트에서 탐지된 하위 서버입니다.
<code>sub_service_vendor</code>	호스트에서 탐지된 하위 서버의 공급업체입니다.
<code>sub_service_version</code>	호스트에서 탐지된 하위 서버의 버전입니다.
<code>vendor</code>	호스트에서 탐지된 서버의 공급업체입니다.
<code>version</code>	호스트에서 탐지된 서버의 버전입니다.

rna_host_service_subtype 조인

`rna_host_service_subtype` 테이블에서는 조인을 수행할 수 없습니다.

rna_host_service_subtype 샘플 쿼리

다음 쿼리는 `host_id`가 8인 호스트에 대해 탐지된 모든 하위 서버 레코드를 반환합니다.

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

rna_host_service_vulns

`rna_host_service_vulns` 테이블에는 모니터링되는 네트워크에 있는 호스트에서 탐지된 서버에 매핑된 취약성에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_service_vulns 필드, 페이지 6-43](#)
- [rna_host_service_vulns 조인, 페이지 6-44](#)
- [rna_host_service_vulns 샘플 쿼리, 페이지 6-44](#)

rna_host_service_vulns 필드

다음 표에는 `rna_host_service_vulns` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-41 `rna_host_service_vulns` 필드

필드	설명
<code>application_id</code>	호스트에서 실행되는 애플리케이션 프로토콜의 내부 ID 번호입니다.
<code>application_name</code>	사용자 인터페이스에 표시되는 애플리케이션 프로토콜 이름입니다.
<code>host_id</code>	호스트의 ID 번호입니다.
<code>invalid</code>	애플리케이션 프로토콜을 실행하는 호스트에 취약성이 유효한지 나타내는 값입니다. <ul style="list-style-type: none"> • 0 — 취약성이 유효함 • 1 — 취약성이 유효하지 않음
<code>ip_address</code>	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>port</code>	서버에서 사용하는 포트입니다.
<code>protocol</code>	트래픽 프로토콜(TCP 또는 UDP)입니다.
<code>rna_vuln_id</code>	취약성의 내부 ID 번호입니다.
<code>service_name</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.

표 6-41 rna_host_service_vulns 필드(계속)

필드	설명
vendor	호스트에서 탐지된 서버의 공급업체입니다.
version	호스트에서 탐지된 서버의 버전입니다.

rna_host_service_vulns 조인

다음 표에는 rna_host_service_vulns 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-42 rna_host_service_vulns 조인

다음에 대해 이 테이블 조인 가능	추가
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 샘플 쿼리

다음 쿼리는 host_id가 8인 호스트의 모든 서버 취약성에 대한 정보를 반환합니다.

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


rna_host_third_party_vuln

`rna_host_third_party_vuln` 테이블에는 모니터링되는 네트워크에 있는 호스트와 관련된 서드파티 취약성에 대한 정보가 포함됩니다. 이 테이블의 정보는 호스트 입력 기능을 통해 가져온 서드파티 취약성 데이터에 의해 결정됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_third_party_vuln 필드, 페이지 6-45](#)
- [rna_host_third_party_vuln 조인, 페이지 6-46](#)
- [rna_host_third_party_vuln 샘플 쿼리, 페이지 6-46](#)

rna_host_third_party_vuln 필드

다음 표에는 `rna_host_third_party_vuln` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-43 `rna_host_third_party_vuln` 필드

필드	설명
<code>description</code>	취약성에 대한 설명입니다.
<code>host_id</code>	호스트의 ID 번호입니다.
<code>invalid</code>	취약성이 호스트에 유효한지 나타내는 값입니다. <ul style="list-style-type: none"> • 0 — 취약성이 유효함 • 1 — 취약성이 유효하지 않음
<code>name</code>	취약성의 제목입니다.
<code>port</code>	포트 번호 - 취약성이 지정된 포트에서 실행 중인 서버와 연결된 경우
<code>protocol</code>	트래픽 프로토콜(TCP 또는 UDP) - 취약성이 해당 프로토콜을 사용하는 애플리케이션과 관련된 경우
<code>source</code>	취약성의 소스입니다.
<code>third_party_vuln_id</code>	취약성과 관련된 ID 번호입니다.

rna_host_third_party_vuln 조인

다음 표에는 `rna_host_third_party_vuln` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-44 `rna_host_third_party_vuln` 조인

다음에 대해 이 테이블 조인 가능	추가
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 샘플 쿼리

다음 쿼리는 `host_id`가 8인 호스트의 서드파티 취약성에 대한 정보를 반환합니다.

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

rna_host_third_party_vuln_bugtraq_id

`rna_host_third_party_vuln_bugtraq_id` 테이블에는 Bugtraq 데이터베이스의 취약성에 매핑되고, 모니터링되는 네트워크에 있는 호스트와도 연관된 서드파티 취약성에 대한 정보가 포함됩니다. 이 테이블의 서드파티 취약성 데이터는 호스트 입력 기능에서 가져옵니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_third_party_vuln_bugtraq_id 필드, 페이지 6-47](#)
- [rna_host_third_party_vuln_bugtraq_id 조인, 페이지 6-47](#)
- [rna_host_third_party_vuln_bugtraq_id 샘플 쿼리, 페이지 6-48](#)

rna_host_third_party_vuln_bugtraq_id 필드

다음 표에는 rna_host_third_party_vuln_bugtraq_id 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-45 rna_host_third_party_vuln_bugtraq_id 필드

필드	설명
bugtraq_id	취약성과 관련된 Bugtraq 데이터베이스 ID 번호입니다.
description	취약성에 대한 설명입니다.
host_id	호스트의 ID 번호입니다.
invalid	취약성이 호스트에 유효한지 나타내는 값입니다. <ul style="list-style-type: none"> • 0 — 취약성이 유효함 • 1 — 취약성이 유효하지 않음
ip_address	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
name	취약성의 이름 또는 제목입니다.
port	포트 번호 - 취약성이 지정된 포트에서 실행 중인 서버와 연결된 경우
protocol	트래픽 프로토콜(TCP 또는 UDP) - 취약성이 해당 프로토콜을 사용하는 애플리케이션과 관련된 경우
source	취약성의 소스입니다.
third_party_vuln_id	취약성과 관련된 서드파티 ID 번호입니다.

rna_host_third_party_vuln_bugtraq_id 조인

다음 표에는 rna_host_third_party_vuln_bugtraq_id 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-46 rna_host_third_party_vuln_bugtraq_id 조인

다음에 대해 이 테이블 조인 가능	추가
bugtraq_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_os_vulns.rna_vuln_id rna_host_service_vulns.rna_vuln_id

표 6-46 rna_host_third_party_vuln_bugtraq_id 조인(계속)

다음에 대해 이 테이블 조인 가능	추가
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln_bugtraq_id 샘플 쿼리

다음 쿼리는 host_id가 8인 호스트의 BugTraq 취약성을 반환합니다.

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

rna_host_third_party_vuln_cve_id

rna_host_third_party_vuln_cve_id 테이블에는 MITRE CVE 데이터베이스의 취약성에 매핑되고, 모니터링되는 네트워크에 있는 호스트와도 연관된 서드파티 취약성에 대한 정보가 포함됩니다. 이 테이블에는 호스트 입력 기능을 통해 가져온 서드파티 취약성 데이터가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- rna_host_third_party_vuln_cve_id 필드, 페이지 6-49
- rna_host_third_party_vuln_cve_id 조인, 페이지 6-49
- rna_host_third_party_vuln_cve_id 샘플 쿼리, 페이지 6-50

rna_host_third_party_vuln_cve_id 필드

다음 표에는 `rna_host_third_party_vuln_cve_id` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-47 `rna_host_third_party_vuln_cve_id` 필드

필드	설명
<code>cve_id</code>	MITRE CVE 데이터베이스의 취약성과 관련된 ID 번호입니다.
<code>description</code>	취약성에 대한 설명입니다.
<code>host_id</code>	호스트의 ID 번호입니다.
<code>invalid</code>	취약성이 호스트에 유효한지 나타내는 값입니다. <ul style="list-style-type: none"> 0 — 취약성이 유효함 1 — 취약성이 유효하지 않음
<code>ip_address</code>	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>name</code>	취약성의 이름 또는 제목입니다.
<code>port</code>	포트 번호 - 취약성이 지정된 포트에서 실행 중인 서버와 연결된 경우
<code>protocol</code>	트래픽 프로토콜(TCP 또는 UDP) - 취약성이 해당 프로토콜을 사용하는 애플리케이션과 관련된 경우
<code>source</code>	취약성의 소스입니다.
<code>third_party_vuln_id</code>	취약성과 관련된 ID 번호입니다.

rna_host_third_party_vuln_cve_id 조인

다음 표에는 `rna_host_third_party_vuln_cve_id` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-48 `rna_host_third_party_vuln_cve_id` 조인

다음에 대해 이 테이블 조인 가능	추가
<code>cve_id</code>	<code>rna_vuln.bugtraq_id</code> <code>rna_vuln.rna_vuln_id</code> <code>rna_host_os_vulns.rna_vuln_id</code> <code>rna_host_service_vulns.rna_vuln_id</code>

표 6-48 rna_host_third_party_vuln_cve_id 조인(계속)

다음에 대해 이 테이블 조인 가능	추가
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln_cve_id 샘플 쿼리

다음 쿼리는 host_id가 8인 CVE 취약성을 반환합니다.

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

rna_host_third_party_vuln_rna_id

rna_host_third_party_vuln_rna_id 테이블에는 Cisco 취약성 데이터(VDB) 내의 취약성에 매핑되고, 모니터링되는 호스트와도 연관된 서드파티 취약성에 대한 정보가 포함됩니다. 이 테이블의 서드파티 취약성 데이터는 호스트 입력 기능에서 가져옵니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [rna_host_third_party_vuln_rna_id 필드, 페이지 6-51](#)
- [rna_host_third_party_vuln_rna_id 조인, 페이지 6-51](#)
- [rna_host_third_party_vuln_rna_id 샘플 쿼리, 페이지 6-52](#)

rna_host_third_party_vuln_rna_id 필드

다음 표에는 `rna_host_third_party_vuln_rna_id` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-49 `rna_host_third_party_vuln_rna_id` 필드

필드	설명
<code>description</code>	취약성에 대한 설명입니다.
<code>host_id</code>	호스트의 ID 번호입니다.
<code>invalid</code>	취약성이 호스트에 유효한지 나타내는 값입니다. <ul style="list-style-type: none"> 0 - 취약성이 유효함 1 - 취약성이 유효하지 않음
<code>ip_address</code>	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>name</code>	취약성의 이름 또는 제목입니다.
<code>port</code>	포트 번호 - 취약성이 지정된 포트에서 실행 중인 서버와 연결된 경우
<code>protocol</code>	트래픽 프로토콜(TCP 또는 UDP) - 취약성이 해당 프로토콜을 사용하는 애플리케이션과 관련된 경우
<code>rna_vuln_id</code>	Cisco에서 취약성을 추적하는 데 사용하는 취약성 ID 번호입니다.
<code>source</code>	취약성의 소스입니다.
<code>third_party_vuln_id</code>	취약성과 관련된 ID 번호입니다.

rna_host_third_party_vuln_rna_id 조인

다음 표에는 `rna_host_third_party_vuln_rna_id` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-50 `rna_host_third_party_vuln_rna_id` 조인

다음에 대해 이 테이블 조인 가능	추가
<code>rna_vuln_id</code>	<code>rna_vuln.bugtraq_id</code> <code>rna_vuln.rna_vuln_id</code> <code>rna_host_os.rna_vuln_id</code> <code>rna_host_service_vulns.rna_vuln_id</code>

표 6-50 rna_host_third_party_vuln_rna_id 조인(계속)

다음에 대해 이 테이블 조인 가능	추가
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 샘플 쿼리

다음 쿼리는 host_id가 8인 호스트의 모든 서드파티 취약성과 함께 VDB ID를 반환합니다.

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

rna_vuln

rna_vuln 테이블에는 Cisco VDB 내의 취약성에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- rna_vuln 필드, 페이지 6-53
- rna_vuln 조인, 페이지 6-54
- rna_vuln 샘플 쿼리, 페이지 6-55

rna_vuln 필드

다음 표에는 `rna_vuln` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-51 `rna_vuln` 필드

필드	설명
<code>authentication</code>	인증 시 취약성을 악용할 필요가 있는지 나타냅니다. <ul style="list-style-type: none"> • Required • Not Required • Unknown
<code>availability</code>	취약성을 악용할 수 있는 경우를 나타냅니다. <ul style="list-style-type: none"> • Always • User Initiated • Time Dependent • Unknown
<code>available_exploits</code>	취약성에 대한 알려진 공격용 악성코드가 있는지 나타냅니다. <ul style="list-style-type: none"> • TRUE • FALSE
<code>bugtraq_id</code>	Bugtraq 데이터베이스의 취약성과 관련된 ID 번호입니다.
<code>class</code>	취약성의 클래스를 나타냅니다. <ul style="list-style-type: none"> • Configuration Error • Boundary Condition Error • Design Error
<code>credibility</code>	취약성의 신뢰도를 나타냅니다. <ul style="list-style-type: none"> • Conflicting Reports • Conflicting Details • Single Source • Reliable Source • Multiple Sources • Vendor Confirmed
<code>credit</code>	취약성 보고를 수행한 신뢰할 수 있는 사람 또는 조직입니다.
<code>ease</code>	취약성을 악용하기 쉬운 정도를 나타냅니다. <ul style="list-style-type: none"> • No Exploit Required • Exploit Available • No Exploit Available
<code>effect</code>	취약성이 악용되었을 때 발생할 수 있는 상황에 대한 상세 정보입니다.
<code>entry_date</code>	데이터베이스에 취약성이 입력된 날짜입니다.
<code>exploit</code>	취약성에 대한 공격용 악성코드를 찾을 수 있는 위치에 대한 정보입니다.

표 6-51 rna_vuln 필드(계속)

필드	설명
impact	침입 데이터, 검색 이벤트, 취약성 평가의 상관관계를 통해 결정되는 영향력 수준에 따라 나타낸 취약성이 미치는 영향입니다. 이 값은 1에서 10까지이며 10은 가장 심각한 경우를 의미합니다. 취약성의 영향력 값은 Bugtraq 항목의 작성자에 의해 결정됩니다.
local	취약성을 로컬로 악용해야 하는지 나타냅니다. <ul style="list-style-type: none"> • TRUE • FALSE
long_description	취약성에 대한 일반적인 설명입니다.
mitigation	취약성을 완화할 수 있는 방법에 대한 설명입니다.
modified_date	해당하는 경우, 취약성을 가장 최근에 수정한 날짜입니다.
publish_date	취약성이 게시된 날짜입니다.
remote	취약성을 네트워크를 통해 악용할 수 있는지 나타냅니다. <ul style="list-style-type: none"> • TRUE • FALSE
rna_vuln_id	시스템에서 취약성 추적에 사용하는 Cisco 취약성 ID 번호입니다.
scenario	공격자가 취약성을 악용하는 상황에 대한 설명입니다.
short_description	취약성에 대한 요약 설명입니다.
snort_id	SID(Snort ID) 데이터베이스의 취약성과 관련된 ID 번호입니다. 즉, 침입 규칙이 특정 취약성을 악용하는 네트워크 트래픽을 탐지할 수 있으면 해당 취약성은 침입 규칙의 SID와 연결됩니다.
solution	취약성에 대한 솔루션입니다.
technical_description	취약성에 대한 기술적 설명입니다.
title	취약성의 제목입니다.

rna_vuln 조인

다음 표에는 rna_vuln 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-52 rna_vuln 조인

다음에 대해 이 테이블 조인 가능	추가
rna_vuln_id	<code>rna_host_os_vulns.rna_vuln_id</code>
또는	<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 샘플 쿼리

다음 쿼리는 취약성에 대한 정보를 최대 25개까지 반환합니다. 이러한 레코드는 취약성을 기준으로 생성된 최근의 이벤트 순서대로 정렬됩니다.

```
SELECT rna_vuln_id, bugtraq_id, snort_id, title, publish_date, impact, remote, exploit,
long_description, technical_description, solution, count(*) as count
FROM rna_vuln
GROUP BY rna_vuln_id
ORDER BY rna_vuln_id DESC LIMIT 0, 25;
```

tag_info

`tag_info` 테이블에는 네트워크에서 탐지된 애플리케이션과 관련된 태그에 대한 정보가 포함됩니다. 애플리케이션에는 여러 개의 관련 태그가 포함될 수 있습니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [tag_info 필드, 페이지 6-55](#)
- [tag_info 조인, 페이지 6-55](#)
- [tag_info 샘플 쿼리, 페이지 6-56](#)

tag_info 필드

다음 표에는 `tag_info` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-53 tag_info 필드

필드	설명
tag_description	태그 설명입니다.
tag_id	태그의 내부 식별자입니다.
tag_name	사용자 인터페이스에 표시되는 태그의 텍스트입니다.
tag_type	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • category • tag

tag_info 조인

다음 표에는 `tag_info` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-54 tag_info 조인

다음에 대해 이 테이블 조인 가능	추가
tag_id	application_tag_map.tag_id

tag_info 샘플 쿼리

다음 쿼리는 선택한 태그 ID에 대한 애플리케이션 태그 레코드를 반환합니다.

```
SELECT tag_id, tag_name, tag_type, tag_description
FROM tag_info
WHERE tag_id="100";
```

url_categories

`url_categories` 테이블에는 모니터링되는 네트워크에 있는 호스트에서 요청한 URL을 구분하는 카테고리가 나열됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [url_categories 필드, 페이지 6-56](#)
- [url_categories 조인, 페이지 6-56](#)
- [url_categories 샘플 쿼리, 페이지 6-56](#)

url_categories 필드

다음 표에는 `url_categories` 테이블에 있는 필드가 설명되어 있습니다.

표 6-55 url_categories 필드

필드	설명
category_description	URL 카테고리에 대한 설명입니다.
category_id	URL 카테고리의 내부 ID 번호입니다.

url_categories 조인

`url_categories` 테이블에서는 조인을 수행할 수 없습니다.

url_categories 샘플 쿼리

다음 쿼리는 선택한 카테고리 ID에 대한 카테고리 레코드를 반환합니다.

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

url_reputations

`url_reputations` 테이블에는 모니터링되는 요청의 호스트에서 요청한 URL을 구분하는 평판이 나열됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [url_reputations 필드, 페이지 6-57](#)
- [url_reputations 조인, 페이지 6-57](#)
- [url_reputations 샘플 쿼리, 페이지 6-57](#)

url_reputations 필드

다음 표에는 `url_reputations` 테이블에 있는 필드가 설명되어 있습니다.

표 6-56 `url_reputations` 필드

필드	설명
<code>reputation_description</code>	평판에 대한 설명입니다.
<code>reputation_id</code>	URL 평판의 내부 ID 번호입니다.

url_reputations 조인

`url_reputations` 테이블에서는 조인을 수행할 수 없습니다.

url_reputations 샘플 쿼리

다음 쿼리는 평판 ID에 대한 URL 평판 정보를 반환합니다.

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

user_ipaddr_history

`user_ipaddr_history` 테이블에는 모니터링되는 네트워크에 있는 특정 호스트의 사용자 활동에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [user_ipaddr_history 필드, 페이지 6-58](#)
- [user_ipaddr_history 조인, 페이지 6-58](#)
- [user_ipaddr_history 샘플 쿼리, 페이지 6-59](#)

user_ipaddr_history 필드

다음 표에는 user_ipaddr_history 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 6-57 user_ipaddr_history 필드

필드	설명
end_time_sec	호스트에 로그인한 다른 사용자를 FireSIGHT System이 탐지한 날짜 및 시간의 UNIX 타임스탬프이며, 이전 사용자 세션의 마지막을 추정하여 표시합니다. FireSIGHT System은 로그오프를 탐지하지 않습니다.
id	사용자 기록 레코드의 내부 ID 번호입니다.
ipaddr	호스트 IP 주소를 이진수로 나타낸 값입니다.
start_time_sec	호스트에 로그인한 사용자를 FireSIGHT System이 탐지한 날짜 및 시간의 UNIX 타임스탬프입니다.
user_dept	사용자의 부서입니다.
user_email	사용자의 이메일 주소입니다.
user_first_name	사용자의 이름입니다.
user_id	사용자의 내부 ID 번호입니다.
user_last_name	사용자의 성입니다.
user_last_seen_sec	FireSIGHT System이 사용자의 사용자 활동을 마지막으로 탐지한 날짜 및 시간의 UNIX 타임스탬프입니다.
user_last_updated_sec	FireSIGHT System이 사용자의 사용자 레코드를 마지막으로 업데이트한 날짜 및 시간의 UNIX 타임스탬프입니다.
user_name	사용자의 사용자 이름입니다.
user_phone	사용자의 전화 번호입니다.
user_rna_service	사용자가 탐지되었을 때 사용된 애플리케이션 프로토콜의 이름입니다(제공되는 경우).

user_ipaddr_history 조인

다음 표에는 user_ipaddr_history 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 6-58 user_ipaddr_history 조인

다음에 대해 이 테이블 조인 가능	추가
ipaddr	compliance_event.dst_ipaddr compliance_event.src_ipaddr connection_log.initiator_ipaddr connection_log.responder_ipaddr connection_summary.initiator_ipaddr connection_summary.responder_ipaddr fireamp_event.dst_ipaddr fireamp_event.src_ipaddr intrusion_event.dst_ipaddr intrusion_event.src_ipaddr network_discovery_event.ipaddr rna_host_ip_map.ipaddr si_connection_log.initiator_ipaddr si_connection_log.responder_ipaddr user_discovery_event.ipaddr white_list_event.ipaddr
user_id	discovered_users.user_id user_discovery_event.user_id

user_ipaddr_history 샘플 쿼리

다음 쿼리는 지정된 시작 타임스탬프 후에 선택한 IP 주소의 모든 사용자 활동 레코드를 반환합니다.

```

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) = "000000000000000000000000FFFF0A0A0A04" AND start_time_sec >=
UNIX_TIMESTAMP("2011-10-01 00:00:00");

```




스키마: 연결 로그 테이블

이 장에는 연결 데이터의 스키마 및 지원되는 조인에 대한 정보가 포함되어 있습니다.

자세한 내용은 아래 표에 나열된 섹션을 참조하십시오. 버전 열은 각 나열된 테이블에서 지원하는 데이터베이스 액세스 버전을 나타냅니다.

표 7-1 *연결 로그 테이블의 스키마*

참조	다음에 대한 정보가 저장되는 테이블	버전
connection_log , 페이지 7-1	개별 연결. 사용 중단된 <code>rna_flow</code> 테이블을 대체함	5.0+
connection_summary , 페이지 7-11	연결 로그 요약. 사용 중단된 <code>rna_flow_summary</code> 테이블을 대체함	5.0+
si_connection_log , 페이지 7-15	개별 연결. 보안 인텔리전스에 사용됨	5.3+

connection_log

`connection_log` 테이블에는 연결 이벤트에 대한 정보가 포함됩니다. FireSIGHT System에서는 모니터링되는 호스트와 다른 호스트 간에 연결이 설정될 경우 연결을 생성합니다. 해당 이벤트에는 모니터링된 트래픽에 대한 자세한 정보가 포함됩니다.

FireSIGHT System 버전 5.0부터 사용 중단된 `rna_flow` 테이블은 `connection_log` 테이블로 대체됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [connection_log](#) 필드, [페이지 7-2](#)
- [connection_log](#) 조인, [페이지 7-11](#)
- [connection_log](#) 샘플 쿼리, [페이지 7-11](#)

connection_log 필드

다음 표에는 connection_log 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 7-2 connection_log 필드

필드	설명
access_control_policy_name	연결을 로깅하는 액세스 제어 규칙(또는 기본 작업)이 포함된 액세스 제어 정책입니다.
access_control_policy_UUID	연결을 로깅하는 액세스 제어 규칙(또는 기본 작업)이 포함된 액세스 제어 정책의 UUID입니다.
access_control_reason	<p>액세스 제어 규칙이 연결을 로깅한 이유입니다. 다음 중 하나에 해당합니다.</p> <ul style="list-style-type: none"> • User Bypass • IP Block • IP Monitor • File Monitor • File Block • File Resume • Intrusion Block • 연결을 로깅하지 않은 경우 비어 있음
access_control_rule_action	액세스 제어 규칙(또는 기본 작업)인 allow, block 등과 관련된 작업
access_control_rule_id	규칙의 내부 ID 번호입니다.
access_control_rule_name	연결을 로깅한 액세스 제어 규칙(또는 기본 작업)입니다.
application_protocol_id	애플리케이션 프로토콜의 내부 ID 번호입니다.
application_protocol_name	<p>다음 중 하나에 해당합니다.</p> <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • unknown - 알려진 서버 지문을 기반으로 서버를 식별할 수 없는 경우 • pending - 시스템에 추가 데이터가 필요한 경우 • 연결에 애플리케이션 정보가 없는 경우 비어 있음
bytes_recv	세션 응답자가 전송한 총 바이트 수입니다.
bytes_sent	세션 개시자가 전송한 총 바이트 수입니다.
cert_valid_end_date	연결에 사용된 SSL 인증서의 유효 기간이 만료되는 날짜에 대한 Unix 타임스탬프입니다.
cert_valid_start_date	연결에 사용된 SSL 인증서가 발행된 날짜에 대한 Unix 타임스탬프입니다.
client_application_id	침입 이벤트에 사용된 클라이언트 애플리케이션의 내부 ID 번호입니다.

표 7-2 connection_log 필드(계속)

필드	설명
client_application_name	침입 이벤트에 사용된 클라이언트 애플리케이션(사용 가능한 경우)입니다. 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • 일반 클라이언트 이름 - 시스템에서 클라이언트 애플리케이션을 탐지했으나 특정한 애플리케이션을 식별하지는 못한 경우 • 연결에 클라이언트 애플리케이션 정보가 없는 경우 비어 있음
client_application_version	클라이언트 애플리케이션의 버전입니다.
connection_type	연결 정보의 탐지 소스입니다. 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • rna - Cisco 디바이스에서 탐지된 경우 • netflow - NetFlow 지원 디바이스에서 내보낸 경우
counter	연결 이벤트와 관련된 침입 이벤트의 카운터입니다.
file_count	한 세션에서 Snort에 의해 식별된 파일의 수입니다. 세션에서 식별된 각 파일당 레코드가 생성됩니다.
first_packet_sec	세션의 첫 번째 패킷이 표시된 날짜 및 시간의 UNIX 타임스탬프입니다.
flow_id	연결의 내부 ID 번호입니다.
icmp_code	ICMP 코드 - 이벤트가 ICMP 트래픽인 경우 또는 null - 이벤트가 ICMP 트래픽에서 생성되지 않은 경우
icmp_type	ICMP 유형 - 이벤트가 ICMP 트래픽인 경우 또는 null - 이벤트가 ICMP 트래픽에서 생성되지 않은 경우
initiator_continent_name	세션을 개시한 호스트의 대륙 이름입니다. <ul style="list-style-type: none"> ** - 알 수 없음 na - 북미 as - 아시아 af - 아프리카 eu - 유럽 sa - 남미 au - 호주 an - 남극 대륙
initiator_country_id	세션을 개시한 호스트의 국가 코드입니다.
initiator_country_name	세션을 개시한 호스트의 국가 이름입니다.
initiator_ip	버전 5.2에서 사용 중단된 필드입니다. 이전 버전과의 호환성 때문에 이 필드의 값은 null로 설정되지 않으나, 신뢰할 수 없습니다.
initiator_ip_address	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
initiator_ipaddr	세션을 개시한 호스트의 IP 주소를 이진수로 나타낸 값입니다.
initiator_ipv4	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
initiator_port	세션 개시자가 사용한 포트입니다.
initiator_user_dept	개시자 호스트에 마지막으로 로그인한 사용자의 부서입니다.

표 7-2 connection_log 필드(계속)

필드	설명
initiator_user_email	개시자 호스트에 마지막으로 로그인한 사용자의 이메일 주소입니다.
initiator_user_first_name	개시자 호스트에 마지막으로 로그인한 사용자의 이름입니다.
initiator_user_id	개시자 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
initiator_user_last_name	개시자 호스트에 마지막으로 로그인한 사용자의 성입니다.
initiator_user_last_seen_sec	개시자 호스트에 마지막으로 로그인한 사용자의 사용자 활동을 FireSIGHT System에서 마지막으로 탐지한 날짜 및 시간의 UNIX 타임스탬프입니다.
initiator_user_last_updated_sec	개시자 호스트에 마지막으로 로그인한 사용자의 사용자 레코드를 FireSIGHT System에서 마지막으로 업데이트한 날짜 및 시간의 UNIX 타임스탬프입니다.
initiator_user_name	개시자 호스트에 마지막으로 로그인한 사용자 이름입니다.
initiator_user_phone	개시자 호스트에 마지막으로 로그인한 사용자의 전화 번호입니다.
instance_id	이벤트를 생성한 관리되는 디바이스의 Snort 인스턴스의 숫자 ID입니다.
interface_egress_name	연결과 관련된 이그레스 인터페이스.
interface_ingress_name	연결과 관련된 이그레스 인터페이스.
ioc_count	연결에서 발견된 IoC(Indications of Compromise: 보안침해지표)의 개수입니다.
ips_event_count	침입 이벤트 임계값 이전에 연결에서 생성된 침입 이벤트의 개수입니다.
last_packet_sec	세션의 마지막 패킷이 표시된 날짜 및 시간의 UNIX 타임스탬프입니다.
monitor_rule_id_1	연결과 관련된 첫 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_1에 저장된 이름과 연결됩니다.
monitor_rule_id_2	연결과 관련된 두 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_2에 저장된 이름과 연결됩니다.
monitor_rule_id_3	연결과 관련된 세 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_3에 저장된 이름과 연결됩니다.
monitor_rule_id_4	연결과 관련된 네 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_4에 저장된 이름과 연결됩니다.
monitor_rule_id_5	연결과 관련된 다섯 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_5에 저장된 이름과 연결됩니다.
monitor_rule_id_6	연결과 관련된 여섯 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_6에 저장된 이름과 연결됩니다.
monitor_rule_id_7	연결과 관련된 일곱 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_7에 저장된 이름과 연결됩니다.
monitor_rule_id_8	연결과 관련된 여덟 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_8에 저장된 이름과 연결됩니다.
monitor_rule_name_1	연결과 관련된 첫 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_1에 저장된 이름과 연결됩니다.
monitor_rule_name_2	연결과 관련된 두 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_2에 저장된 ID와 연결됩니다.

표 7-2 connection_log 필드(계속)

필드	설명
monitor_rule_name_3	연결과 관련된 세 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_3에 저장된 ID와 연결됩니다.
monitor_rule_name_4	연결과 관련된 네 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_4에 저장된 ID와 연결됩니다.
monitor_rule_name_5	연결과 관련된 다섯 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_5에 저장된 ID와 연결됩니다.
monitor_rule_name_6	연결과 관련된 여섯 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_6에 저장된 ID와 연결됩니다.
monitor_rule_name_7	연결과 관련된 일곱 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_7에 저장된 ID와 연결됩니다.
monitor_rule_name_8	연결과 관련된 여덟 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_8에 저장된 ID와 연결됩니다.
netbios_domain	연결에 사용된 NetBIOS 도메인입니다.
netflow_dst_as	목적지(원본 또는 피어)의 Netflow 자동 시스템 수입입니다.
netflow_dst_mask	NetFlow 목적지 주소 접두사 마스크입니다.
netflow_dst_tos	패킷이 목적지에서 소스로 전달될 경우 IP 헤더의 서비스 유형입니다.
netflow_snmp_in	소스에서 목적지로 전달되는 패킷에서 사용된 인터페이스의 ID입니다.
netflow_snmp_out	목적지에서 소스로 전달되는 패킷에서 사용된 인터페이스의 ID입니다.
netflow_src_as	소스(원본 또는 피어)의 Netflow 자동 시스템 수입입니다.
netflow_src_mask	NetFlow 소스 주소 접두사 마스크입니다.
netflow_src_tos	패킷이 소스에서 목적지로 전달될 경우 IP 헤더의 서비스 유형입니다.
network_analysis_policy_name	침입 이벤트를 생성한 침입 정책과 관련된 네트워크 분석 정책입니다.
network_analysis_policy_UUID	침입 이벤트를 생성한 침입 정책과 관련된 네트워크 분석 정책의 UUID입니다.
packets_recv	세션을 개시한 호스트에서 수신한 총 패킷 수입입니다.
packets_sent	세션을 개시한 호스트에서 전송한 총 패킷 수입입니다.
protocol_name	연결에 사용된 프로토콜의 이름입니다.
protocol_num	프로토콜의 IANA 번호는 다음 사이트에 나와 있습니다. http://www.iana.org/assignments/protocol-numbers .
responder_continent_name	세션 개시자에게 응답한 호스트의 대륙 이름입니다. ** — 알 수 없음 na — 북미 as — 아시아 af — 아프리카 eu — 유럽 sa — 남미 au — 호주 an — 남극 대륙

표 7-2 connection_log 필드(계속)

필드	설명
responder_country_id	세션 개시자에게 응답한 호스트의 국가 코드입니다.
responder_country_name	세션 개시자에게 응답한 호스트의 국가 이름입니다.
responder_ip	버전 5.2에서 사용 중단된 필드입니다. 이전 버전과의 호환성 때문에 이 필드의 값은 null로 설정되지 않으나, 신뢰할 수 없습니다.
responder_ip_address	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
responder_ipaddr	세션 개시자에게 응답한 호스트의 IPv4 또는 IPv6 주소를 이진수로 나타낸 값입니다.
responder_ipv4	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
responder_port	세션 응답자가 사용한 포트입니다.
responder_user_dept	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 부서입니다.
responder_user_email	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 이메일 주소입니다.
responder_user_first_name	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 이름입니다.
responder_user_id	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
responder_user_last_name	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 성입니다.
responder_user_last_seen_sec	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 사용자 활동을 FireSIGHT System에서 마지막으로 탐지한 날짜 및 시간의 UNIX 타임스탬프입니다.
responder_user_last_updated_sec	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 사용자 활동을 에서 마지막으로 업데이트한 날짜 및 시간의 UNIX 타임스탬프입니다.
responder_user_name	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 사용자 이름입니다.
responder_user_phone	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 전화번호입니다.
security_context	트래픽이 통과한 보안 컨텍스트(가상 방화벽)에 대한 설명입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
security_intelligence_category	연결과 관련된 보안 인텔리전스 카테고리입니다.
security_intelligence_ip	연결과 관련된 보안 인텔리전스 모니터링 IP 주소가 소스 IP(src)인지 또는 목적지 IP(dst)인지 나타냅니다.
security_zone_egress_name	연결 이벤트의 이그레스 보안 영역입니다.
security_zone_ingress_name	연결 이벤트의 인그레스 보안 영역입니다.
sensor_address	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 ipv4 address, ipv6 address입니다.
sensor_name	세션을 모니터링한 관리되는 디바이스의 이름입니다.

표 7-2 connection_log 필드(계속)

필드	설명
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 sensor_name이 null인 경우 0입니다.
source_device	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
src_device_ip	버전 5.2에서 사용 중단된 필드입니다. 이전 버전과의 호환성 때문에 이 필드의 값은 null로 설정되지 않으나, 신뢰할 수 없습니다.
src_device_ipaddr	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> 연결 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소를 이진수로 나타낸 값입니다. 0 - Cisco 관리되는 디바이스에서 연결을 탐지한 경우
src_device_ipv4	<ul style="list-style-type: none"> 버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
ssl_actual_action	SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다. <ul style="list-style-type: none"> Unknown Do Not Decrypt Block Block With Reset Decrypt (Known Key) Decrypt (Replace Key) Decrypt (Resign)
ssl_cipher_suite	SSL 연결에서 사용되는 암호화 그룹입니다. 이 값은 십진법 형식으로 저장됩니다. 참조: www.iana.org/assignments/tls-parameters/tls-parameters.xhtml 은 값에서 지정한 암호 그룹에 사용됩니다.
ssl_expected_action	SSL 규칙에 기반한 연결에서 수행해야 하는 작업입니다. 가능한 값은 다음과 같습니다. <ul style="list-style-type: none"> Unknown Do Not Decrypt Block Block With Reset Decrypt (Known Key) Decrypt (Replace Key) Decrypt (Resign)

표 7-2 connection_log 필드(계속)

필드	설명
ssl_flow_flags	<p>암호화된 연결에 대한 디버깅 레벨 플래그입니다. 가능한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> 0x00000001 — NSE_FLOW__VALID — 유효해야 하는 기타 필드에 설정해야 함 0x00000002 — NSE_FLOW__INITIALIZED — 처리 준비가 완료된 내부 구조 0x00000004 — NSE_FLOW__INTERCEPT — SSL 세션이 중단됨
ssl_flow_messages	<p>SSL 핸드셰이크 도중 클라이언트와 서버 간에 교환된 메시지입니다. 자세한 내용은 http://tools.ietf.org/html/rfc5246 을 참조하십시오.</p> <ul style="list-style-type: none"> 0x00000001 — NSE_MT__HELLO_REQUEST 0x00000002 — NSE_MT__CLIENT_ALERT 0x00000004 — NSE_MT__SERVER_ALERT 0x00000008 — NSE_MT__CLIENT_HELLO 0x00000010 — NSE_MT__SERVER_HELLO 0x00000020 — NSE_MT__SERVER_CERTIFICATE 0x00000040 — NSE_MT__SERVER_KEY_EXCHANGE 0x00000080 — NSE_MT__CERTIFICATE_REQUEST 0x00000100 — NSE_MT__SERVER_HELLO_DONE 0x00000200 — NSE_MT__CLIENT_CERTIFICATE 0x00000400 — NSE_MT__CLIENT_KEY_EXCHANGE 0x00000800 — NSE_MT__CERTIFICATE_VERIFY 0x00001000 — NSE_MT__CLIENT_CHANGE_CIPHER_SPEC 0x00002000 — NSE_MT__CLIENT_FINISHED 0x00004000 — NSE_MT__SERVER_CHANGE_CIPHER_SPEC 0x00008000 — NSE_MT__SERVER_FINISHED 0x00010000 — NSE_MT__NEW_SESSION_TICKET 0x00020000 — NSE_MT__HANDSHAKE_OTHER 0x00040000 — NSE_MT__APP_DATA_FROM_CLIENT 0x00080000 — NSE_MT__APP_DATA_FROM_SERVER

표 7-2 connection_log 필드(계속)

필드	설명
ssl_flow_status	<p>SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 'Unknown' • 'No Match' • 'Success' • 'Uncached Session' • 'Unknown Cipher Suite' • 'Unsupported Cipher Suite' • 'Unsupported SSL Version' • 'SSL Compression Used' • 'Session Undecryptable in Passive Mode' • 'Handshake Error' • 'Decryption Error' • 'Pending Server Name Category Lookup' • 'Pending Common Name Category Lookup' • 'Internal Error' • 'Network Parameters Unavailable' • 'Invalid Server Certificate Handle' • 'Server Certificate Fingerprint Unavailable' • 'Cannot Cache Subject DN' • 'Cannot Cache Issuer DN' • 'Unknown SSL Version' • 'External Certificate List Unavailable' • 'External Certificate Fingerprint Unavailable' • 'Internal Certificate List Invalid' • 'Internal Certificate List Unavailable' • 'Internal Certificate Unavailable' • 'Internal Certificate Fingerprint Unavailable' • 'Server Certificate Validation Unavailable' • 'Server Certificate Validation Failure' • 'Invalid Action'
ssl_issuer_common_name	SSL 인증서의 발급자 일반 이름입니다. 이는 일반적으로 인증서 발급자의 호스트 및 도메인 이름이지만, 다른 정보가 포함될 수도 있습니다.
ssl_issuer_country	SSL 인증서 발급자의 국가입니다.
ssl_issuer_organization	SSL 인증서 발급자의 조직입니다.
ssl_issuer_organization_unit	SSL 인증서 발급자의 조직 부서입니다.

표 7-2 connection_log 필드(계속)

필드	설명
ssl_policy_action	일치하는 규칙이 없을 경우 정책에 구성되는 기본 작업입니다.
ssl_policy_name	연결을 처리한 SSL 정책의 ID 번호입니다.
ssl_policy_reason	SSL 정책이 SSL 세션을 로깅한 이유입니다.
ssl_rule_action	SSL 규칙(allow, block 등)의 사용자 인터페이스에서 선택한 작업입니다.
ssl_rule_name	연결을 처리한 SSL 규칙 또는 기본 동작의 ID 번호입니다.
ssl_serial_number	발급 CA가 할당한 SSL 인증서의 일련 번호입니다.
ssl_server_name	SSL Client Hello의 서버 이름 표시에서 제공된 이름입니다.
ssl_subject_common_name	SSL 인증서의 주체 일반 이름입니다. 이는 일반적으로 인증서 주체의 호스트 및 도메인 이름이지만, 다른 정보가 포함될 수도 있습니다.
ssl_subject_country	SSL 인증서 주체의 국가입니다.
ssl_subject_organization	SSL 인증서 주체의 조직입니다.
ssl_subject_organization_unit	SSL 인증서 주체의 조직 부서입니다.
ssl_url_category	서버 이름 및 인증서 일반 이름에서 확인된 플로우의 카테고리입니다.
ssl_version	연결을 암호화하는 데 사용된 SSL 또는 TLS 프로토콜 버전입니다.
tcp_flags	세션에서 탐지된 TCP 플래그입니다.
url	제공되는 경우, 세션 도중 모니터링된 호스트에서 요청한 URL입니다.
url_category	모니터링된 호스트에서 요청한 URL의 카테고리입니다.
url_reputation	모니터링된 호스트에서 요청한 URL의 평판입니다. 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 1 - 매우 위험 • 2 - 의심스러운 사이트 • 3 - 보안 위험이 있는 정상적인 사이트 • 4 - 정상적인 사이트 • 5 - 유명함
web_application_id	웹 애플리케이션의 내부 ID 번호입니다.
web_application_name	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • web browsing - HTTP의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 식별하지 못하는 경우 • 연결에 HTTP 트래픽이 없는 경우 비어 있음

connection_log 조인

다음 표에는 `connection_log` 테이블을 사용하여 수행할 수 있는 조인이 설명되어 있습니다.

표 7-3 `connection_log` 조인

다음에 대해 이 테이블 조인 가능	추가
<code>application_protocol_id</code> 또는 <code>client_application_id</code> 또는 <code>web_application_id</code>	<code>application_info.application_id</code> <code>application_host_map.application_id</code> <code>application_tag_map.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>initiator_ipaddr</code> 또는 <code>responder_ipaddr</code>	<code>rna_host_ip_map.ipaddr</code> <code>user_ipaddr_history.ipaddr</code>

connection_log 샘플 쿼리

다음 쿼리는 `connection_log` 테이블에서 최대 25개의 연결 이벤트 레코드를 반환하며, 패킷 타임스탬프를 기준으로 내림차순으로 정렬합니다.

```
SELECT first_packet_sec, last_packet_sec, initiator_ipaddr, responder_ipaddr,
security_zone_ingress_name, security_zone_egress_name, initiator_port, protocol_name,
responder_port, application_protocol_id, client_application_id, web_application_id, url,
url_category, url_reputation
FROM connection_log
WHERE first_packet_sec <= UNIX_TIMESTAMP("2011-10-01 00:00:00" ) ORDER BY
first_packet_sec
DESC, last_packet_sec DESC LIMIT 0, 25;
```

connection_summary

`connection_summary` 테이블에는 연결 요약 또는 취합된 연결에 대한 정보가 포함됩니다. FireSIGHT System에서는 5분 간격으로 연결을 취합합니다. 연결을 취합하려면 연결의 조건은 다음을 충족해야 합니다.

- 동일한 소스 및 목적지 IP 주소가 있어야 함
- 동일한 프로토콜을 사용함
- 동일한 애플리케이션을 사용함
- 동일한 관리되는 디바이스에서 탐지되거나(FireSIGHT를 통해 관리되는 디바이스에서 탐지된 세션의 경우), 동일한 NetFlow 지원 디바이스에서 내보내고 동일한 관리되는 디바이스에서 처리됨

연결 요약의 취합된 데이터에는 개시자 및 응답자 호스트가 보낸 총 패킷 및 바이트 수는 물론 요약의 연결 수가 포함됩니다.

FireSIGHT System 버전 5.0부터 사용 중단된 `rna_flow_summary` 테이블은 `connection_summary` 테이블로 대체됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [connection_summary 필드, 페이지 7-12](#)
- [connection_summary 조인, 페이지 7-14](#)
- [connection_summary 샘플 쿼리, 페이지 7-14](#)

connection_summary 필드

다음 표에는 `connection_summary` 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 7-4 connection_summary 필드

필드	설명
<code>application_protocol_id</code>	애플리케이션 프로토콜의 내부 ID 번호입니다.
<code>application_protocol_name</code>	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • <code>unknown</code> - 알려진 서버 지문을 기반으로 서버를 식별할 수 없는 경우 • <code>pending</code> - 시스템에 추가 데이터가 필요한 경우 • 연결에 애플리케이션 정보가 없는 경우 비어 있음
<code>bytes_recv</code>	세션 응답자가 전송한 총 바이트 수입니다.
<code>bytes_sent</code>	세션 개시자가 전송한 총 바이트 수입니다.
<code>connection_type</code>	연결 정보의 탐지 소스입니다. 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • <code>rna</code> - Cisco 디바이스에서 탐지된 경우 • <code>netflow</code> - NetFlow 지원 디바이스에서 내보낸 경우
<code>flow_type</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>id</code>	연결 요약의 내부 ID 번호입니다.
<code>initiator_ip_address</code>	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>initiator_ipaddr</code>	세션을 개시한 호스트의 IP 주소를 이진수로 나타낸 값입니다.
<code>initiator_user_dept</code>	개시자 호스트에 마지막으로 로그인한 사용자의 부서입니다.
<code>initiator_user_email</code>	개시자 호스트에 마지막으로 로그인한 사용자의 이메일 주소입니다.
<code>initiator_user_first_name</code>	개시자 호스트에 마지막으로 로그인한 사용자의 이름입니다.
<code>initiator_user_id</code>	개시자 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
<code>initiator_user_last_name</code>	개시자 호스트에 마지막으로 로그인한 사용자의 성입니다.
<code>initiator_user_last_seen_sec</code>	개시자 호스트에 마지막으로 로그인한 사용자의 사용자 활동을 FireSIGHT System에서 마지막으로 탐지한 날짜 및 시간의 UNIX 타임스탬프입니다.

표 7-4 connection_summary 필드(계속)

필드	설명
initiator_user_last_updated_sec	개시자 호스트에 마지막으로 로그인한 사용자의 사용자 레코드를 FireSIGHT System에서 마지막으로 업데이트한 날짜 및 시간의 UNIX 타임스탬프입니다.
initiator_user_name	개시자 호스트에 마지막으로 로그인한 사용자 이름입니다.
initiator_user_phone	개시자 호스트에 마지막으로 로그인한 사용자의 전화 번호입니다.
interface_egress_name	연결과 관련된 이그레스 인터페이스.
interface_ingress_name	연결과 관련된 이그레스 인터페이스.
num_connections	요약의 연결 개수입니다. 여러 연결 요약 간격에 걸쳐 있는 Long-Running 연결의 경우, 첫 번째 연결 요약 간격만 증가합니다.
packets_recv	세션 응답자가 전송한 총 패킷 수입니다.
packets_sent	세션 개시자가 전송한 총 패킷 수입니다.
protocol_name	취합된 세션에서 사용된 프로토콜의 이름입니다.
protocol_num	프로토콜의 IANA 번호는 다음 사이트에 나와 있습니다. http://www.iana.org/assignments/protocol-numbers .
responder_ip_address	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
responder_ipaddr	취합된 세션의 개시자에게 응답한 호스트의 IP 주소를 이진수로 나타낸 값입니다.
responder_port	취합된 세션의 응답자가 사용한 포트입니다.
responder_user_dept	취합된 세션의 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 부서입니다.
responder_user_email	취합된 세션의 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 이메일 주소입니다.
responder_user_first_name	취합된 세션의 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 이름입니다.
responder_user_id	취합된 세션의 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
responder_user_last_name	취합된 세션의 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 성입니다.
responder_user_last_seen_sec	취합된 세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 사용자 활동을 FireSIGHT System에서 마지막으로 탐지한 날짜 및 시간의 UNIX 타임스탬프입니다.
responder_user_last_updated_sec	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 사용자 활동을 에서 마지막으로 업데이트한 날짜 및 시간의 UNIX 타임스탬프입니다.
responder_user_name	취합된 세션의 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 사용자 이름입니다.
responder_user_phone	취합된 세션의 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 전화 번호입니다.
security_zone_egress_name	연결 이벤트의 이그레스 보안 영역입니다.
security_zone_ingress_name	연결 이벤트의 이그레스 보안 영역입니다.

표 7-4 connection_summary 필드(계속)

필드	설명
sensor_address	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
sensor_name	취합된 세션을 모니터링한 관리되는 디바이스의 이름입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 <code>sensor_name</code> 이 null인 경우 0입니다.
source_device	소스 디바이스의 ID이며, 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소 • FireSIGHT Cisco 관리되는 디바이스에서 연결을 탐지한 경우
start_time_sec	시작된 요약에서 세션을 취합하는 데 사용되는 5분 간격으로 된 날짜 및 시간의 UNIX 타임스탬프입니다.

connection_summary 조인

다음 표에는 `connection_summary` 테이블을 사용하여 수행할 수 있는 조인이 설명되어 있습니다.

표 7-5 connection_summary 조인

다음에 대해 이 테이블 조인 가능	추가
application_protocol_id	<code>application_info.application_id</code> <code>application_host_map.application_id</code> <code>application_tag_map.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>
initiator_ipaddr 또는 responder_ipaddr	<code>rna_host_ip_map.ipaddr</code> <code>user_ipaddr_history.ipaddr</code>

connection_summary 샘플 쿼리

다음 쿼리는 선택한 디바이스에서 탐지된 연결 이벤트 요약 레코드를 최대 5개까지 반환합니다.

```
SELECT initiator_ipaddr, responder_ipaddr, protocol_name, application_protocol_id,
source_device, sensor_name, sensor_address, packets_recv, packets_sent, bytes_recv,
bytes_sent, connection_type, num_connections
FROM connection_summary
WHERE sensor_name='linden' limit 5;
```

si_connection_log

si_connection_log 테이블에는 보안 인텔리전스 이벤트에 대한 정보가 포함됩니다. FireSIGHT System에서는 보안 인텔리전스에서 연결을 차단 목록에 올리거나 모니터링할 경우 보안 인텔리전스 이벤트를 생성합니다. 해당 이벤트에는 모니터링된 트래픽에 대한 자세한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- si_connection_log 필드, 페이지 7-15
- si_connection_log 조인, 페이지 7-24
- si_connection_log 샘플 쿼리, 페이지 7-24

si_connection_log 필드

다음 표에는 si_connection_log 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 7-6 si_connection_log 필드

필드	설명
access_control_policy_name	연결을 로깅하는 액세스 제어 규칙(또는 기본 작업)이 포함된 액세스 제어 정책입니다.
access_control_policy_UUID	연결을 로깅하는 액세스 제어 규칙(또는 기본 작업)이 포함된 액세스 제어 정책의 UUID입니다.
access_control_reason	액세스 제어 규칙이 연결을 로깅한 이유입니다. 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • User Bypass • IP Block • IP Monitor • File Monitor • File Block • File Resume • Intrusion Block • 연결을 로깅하지 않은 경우 비어 있음
access_control_rule_action	액세스 제어 규칙(또는 기본 작업)인 allow, block 등과 관련된 작업
access_control_rule_id	규칙의 내부 ID 번호입니다.
access_control_rule_name	연결을 로깅한 액세스 제어 규칙(또는 기본 작업)입니다.
application_protocol_id	애플리케이션 프로토콜의 내부 ID 번호입니다.
application_protocol_name	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • unknown - 알려진 서버 지문을 기반으로 서버를 식별할 수 없는 경우 • pending - 시스템에 추가 데이터가 필요한 경우 • 연결에 애플리케이션 정보가 없는 경우 비어 있음

표 7-6 si_connection_log 필드(계속)

필드	설명
bytes_recv	세션 응답자가 전송한 총 바이트 수입니다.
bytes_sent	세션 개시자가 전송한 총 바이트 수입니다.
cert_valid_end_date	연결에 사용된 SSL 인증서의 유효 기간이 만료되는 날짜에 대한 Unix 타임스탬프입니다.
cert_valid_start_date	연결에 사용된 SSL 인증서가 발행된 날짜에 대한 Unix 타임스탬프입니다.
client_application_id	침입 이벤트에 사용된 클라이언트 애플리케이션의 내부 ID 번호입니다.
client_application_name	침입 이벤트에 사용된 클라이언트 애플리케이션(사용 가능한 경우)입니다. 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • 일반 클라이언트 이름 - 시스템에서 클라이언트 애플리케이션을 탐지했으나 특정한 애플리케이션을 식별하지는 못한 경우 • 연결에 클라이언트 애플리케이션 정보가 없는 경우 비어 있음
client_application_version	클라이언트 애플리케이션의 버전입니다.
connection_type	연결 정보의 탐지 소스입니다. 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • rna - Cisco 디바이스에서 탐지된 경우 • netflow - NetFlow 지원 디바이스에서 내보낸 경우
counter	연결 이벤트와 관련된 침입 이벤트의 카운터입니다.
file_count	한 세션에서 Snort에 의해 식별된 파일의 수입니다. 세션에서 식별된 각 파일당 레코드가 생성됩니다.
first_packet_sec	세션의 첫 번째 패킷이 표시된 날짜 및 시간의 UNIX 타임스탬프입니다.
icmp_code	ICMP 코드 - 이벤트가 ICMP 트래픽인 경우 또는 null - 이벤트가 ICMP 트래픽에서 생성되지 않은 경우
icmp_type	ICMP 유형 - 이벤트가 ICMP 트래픽인 경우 또는 null - 이벤트가 ICMP 트래픽에서 생성되지 않은 경우
initiator_continent_name	세션을 개시한 호스트의 대륙 이름입니다. <ul style="list-style-type: none"> ** - 알 수 없음 na - 북미 as - 아시아 af - 아프리카 eu - 유럽 sa - 남미 au - 호주 an - 남극 대륙
initiator_country_id	세션을 개시한 호스트의 국가 코드입니다.
initiator_country_name	세션을 개시한 호스트의 국가 이름입니다.
initiator_ipaddr	세션을 개시한 호스트의 IP 주소를 이진수로 나타낸 값입니다.
initiator_port	세션 개시자가 사용한 포트입니다.

표 7-6 si_connection_log 필드(계속)

필드	설명
initiator_user_dept	개시자 호스트에 마지막으로 로그인한 사용자의 부서입니다.
initiator_user_email	개시자 호스트에 마지막으로 로그인한 사용자의 이메일 주소입니다.
initiator_user_first_name	개시자 호스트에 마지막으로 로그인한 사용자의 이름입니다.
initiator_user_id	개시자 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
initiator_user_last_name	개시자 호스트에 마지막으로 로그인한 사용자의 성입니다.
initiator_user_last_seen_sec	개시자 호스트에 마지막으로 로그인한 사용자의 사용자 활동을 FireSIGHT System에서 마지막으로 탐지한 날짜 및 시간의 UNIX 타임스탬프입니다.
initiator_user_last_updated_sec	개시자 호스트에 마지막으로 로그인한 사용자의 사용자 레코드를 FireSIGHT System에서 마지막으로 업데이트한 날짜 및 시간의 UNIX 타임스탬프입니다.
initiator_user_name	개시자 호스트에 마지막으로 로그인한 사용자 이름입니다.
initiator_user_phone	개시자 호스트에 마지막으로 로그인한 사용자의 전화 번호입니다.
instance_id	이벤트를 생성한 관리되는 디바이스의 Snort 인스턴스의 숫자 ID입니다.
interface_egress_name	연결과 관련된 이그레스 인터페이스.
interface_ingress_name	연결과 관련된 이그레스 인터페이스.
ioc_count	연결에서 발견된 IoC(Indications of Compromise: 보안침해지표)의 개수입니다.
ips_event_count	침입 이벤트 임계값 이전에 연결에서 생성된 침입 이벤트의 개수입니다.
last_packet_sec	세션의 마지막 패킷이 표시된 날짜 및 시간의 UNIX 타임스탬프입니다.
monitor_rule_id_1	연결과 관련된 첫 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_1에 저장된 이름과 연결됩니다.
monitor_rule_id_2	연결과 관련된 두 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_2에 저장된 이름과 연결됩니다.
monitor_rule_id_3	연결과 관련된 세 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_3에 저장된 이름과 연결됩니다.
monitor_rule_id_4	연결과 관련된 네 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_4에 저장된 이름과 연결됩니다.
monitor_rule_id_5	연결과 관련된 다섯 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_5에 저장된 이름과 연결됩니다.
monitor_rule_id_6	연결과 관련된 여섯 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_6에 저장된 이름과 연결됩니다.
monitor_rule_id_7	연결과 관련된 일곱 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_7에 저장된 이름과 연결됩니다.
monitor_rule_id_8	연결과 관련된 여덟 번째 모니터 규칙의 ID입니다. 이 ID는 monitor_rule_name_8에 저장된 이름과 연결됩니다.
monitor_rule_name_1	연결과 관련된 첫 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_1에 저장된 이름과 연결됩니다.
monitor_rule_name_2	연결과 관련된 두 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_2에 저장된 ID와 연결됩니다.

표 7-6 si_connection_log 필드(계속)

필드	설명
monitor_rule_name_3	연결과 관련된 세 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_3에 저장된 ID와 연결됩니다.
monitor_rule_name_4	연결과 관련된 네 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_4에 저장된 ID와 연결됩니다.
monitor_rule_name_5	연결과 관련된 다섯 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_5에 저장된 ID와 연결됩니다.
monitor_rule_name_6	연결과 관련된 여섯 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_6에 저장된 ID와 연결됩니다.
monitor_rule_name_7	연결과 관련된 일곱 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_7에 저장된 ID와 연결됩니다.
monitor_rule_name_8	연결과 관련된 여덟 번째 모니터 규칙의 이름입니다. 이 이름은 monitor_rule_id_8에 저장된 ID와 연결됩니다.
netbios_domain	연결에 사용된 NetBIOS 도메인입니다.
netflow_dst_as	목적지(원본 또는 피어)의 Netflow 자동 시스템 수입입니다.
netflow_dst_mask	NetFlow 목적지 주소 접두사 마스크입니다.
netflow_dst_tos	패킷이 목적지에서 소스로 전달될 경우 IP 헤더의 서비스 유형입니다.
netflow_snmp_in	소스에서 목적지로 전달되는 패킷에서 사용된 인터페이스의 ID입니다.
netflow_snmp_out	목적지에서 소스로 전달되는 패킷에서 사용된 인터페이스의 ID입니다.
netflow_src_as	소스(원본 또는 피어)의 Netflow 자동 시스템 수입입니다.
netflow_src_mask	NetFlow 소스 주소 접두사 마스크입니다.
netflow_src_tos	패킷이 소스에서 목적지로 전달될 경우 IP 헤더의 서비스 유형입니다.
network_analysis_policy_name	침입 이벤트를 생성한 침입 정책과 관련된 네트워크 분석 정책입니다.
network_analysis_policy_UUID	침입 이벤트를 생성한 침입 정책과 관련된 네트워크 분석 정책의 UUID입니다.
packets_recv	세션을 개시한 호스트에서 수신한 총 패킷 수입입니다.
packets_sent	세션을 개시한 호스트에서 전송한 총 패킷 수입입니다.
protocol_name	연결에 사용된 프로토콜의 이름입니다.
protocol_num	프로토콜의 IANA 번호는 다음 사이트에 나와 있습니다. http://www.iana.org/assignments/protocol-numbers .
responder_continent_name	세션 개시자에게 응답한 호스트의 대륙 이름입니다. ** — 알 수 없음 na — 북미 as — 아시아 af — 아프리카 eu — 유럽 sa — 남미 au — 호주 an — 남극 대륙

표 7-6 si_connection_log 필드(계속)

필드	설명
responder_country_id	세션 개시자에게 응답한 호스트의 국가 코드입니다.
responder_country_name	세션 개시자에게 응답한 호스트의 국가 이름입니다.
responder_ipaddr	세션 개시자에게 응답한 호스트의 IPv4 또는 IPv6 주소를 이진수로 나타낸 값입니다.
responder_port	세션 응답자가 사용한 포트입니다.
responder_user_dept	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 부서입니다.
responder_user_email	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 이메일 주소입니다.
responder_user_first_name	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 이름입니다.
responder_user_id	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
responder_user_last_name	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 성입니다.
responder_user_last_seen_sec	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 사용자 활동을 FireSIGHT System에서 마지막으로 탐지한 날짜 및 시간의 UNIX 타임스탬프입니다.
responder_user_last_updated_sec	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 사용자 활동을 에서 마지막으로 업데이트한 날짜 및 시간의 UNIX 타임스탬프입니다.
responder_user_name	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 사용자 이름입니다.
responder_user_phone	세션 개시자에게 응답한 호스트에 마지막으로 로그인한 사용자의 전화번호입니다.
security_context	트래픽이 통과한 보안 컨텍스트(가상 방화벽)에 대한 설명입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
security_intelligence_category	연결과 관련된 보안 인텔리전스 카테고리입니다.
security_intelligence_ip	연결과 관련된 보안 인텔리전스 모니터링 IP 주소가 소스 IP(src)인지 또는 목적지 IP(dst)인지 나타냅니다.
security_zone_egress_name	연결 이벤트의 이그레스 보안 영역입니다.
security_zone_ingress_name	연결 이벤트의 인그레스 보안 영역입니다.
sensor_address	이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 ipv4 address, ipv6 address입니다.
sensor_name	세션을 모니터링한 관리되는 디바이스의 이름입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 sensor_name이 null인 경우 0입니다.

표 7-6 si_connection_log 필드(계속)

필드	설명
src_device_ipaddr	<p>다음 중 하나에 해당합니다.</p> <ul style="list-style-type: none"> • 연결 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소를 이진수로 나타낸 값입니다. • 0 - Cisco 관리되는 디바이스에서 연결을 탐지한 경우
ssl_actual_action	<p>SSL 규칙에 기반한 연결에서 수행된 작업입니다. 규칙에 명시된 작업이 가능하지 않을 수도 있으므로, 이는 예상 작업과 다를 수 있습니다. 가능한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 'Unknown' • 'Do Not Decrypt' • 'Block' • 'Block With Reset' • 'Decrypt (Known Key)' • 'Decrypt (Replace Key)' • 'Decrypt (Resign)'
ssl_cipher_suite	<p>SSL 연결에서 사용되는 암호화 그룹입니다. 이 값은 십진법 형식으로 저장됩니다. 참조: www.iana.org/assignments/tls-parameters/tls-parameters.xhtml은 값에서 지정한 암호 그룹에 사용됩니다.</p>
ssl_expected_action	<p>SSL 규칙에 기반한 연결에서 수행해야 하는 작업입니다. 가능한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 'Unknown' • 'Do Not Decrypt' • 'Block' • 'Block With Reset' • 'Decrypt (Known Key)' • 'Decrypt (Replace Key)' • 'Decrypt (Resign)'
ssl_flow_flags	<p>암호화된 연결에 대한 디버깅 레벨 플래그입니다. 가능한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 0x00000001 — NSE_FLOW__VALID — 유효해야 하는 기타 필드에 설정해야 함 • 0x00000002 — NSE_FLOW__INITIALIZED — 처리 준비가 완료된 내부 구조 • 0x00000004 — NSE_FLOW__INTERCEPT — SSL 세션이 중단됨

표 7-6 si_connection_log 필드(계속)

필드	설명
ssl_flow_messages	<p>SSL 핸드셰이크 도중 클라이언트와 서버 간에 교환된 메시지입니다. 자세한 내용은 http://tools.ietf.org/html/rfc5246 을 참조하십시오.</p> <ul style="list-style-type: none"> • 0x00000001 — NSE_MT__HELLO_REQUEST • 0x00000002 — NSE_MT__CLIENT_ALERT • 0x00000004 — NSE_MT__SERVER_ALERT • 0x00000008 — NSE_MT__CLIENT_HELLO • 0x00000010 — NSE_MT__SERVER_HELLO • 0x00000020 — NSE_MT__SERVER_CERTIFICATE • 0x00000040 — NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 — NSE_MT__CERTIFICATE_REQUEST • 0x00000100 — NSE_MT__SERVER_HELLO_DONE • 0x00000200 — NSE_MT__CLIENT_CERTIFICATE • 0x00000400 — NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 — NSE_MT__CERTIFICATE_VERIFY • 0x00001000 — NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 — NSE_MT__CLIENT_FINISHED • 0x00004000 — NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 — NSE_MT__SERVER_FINISHED • 0x00010000 — NSE_MT__NEW_SESSION_TICKET • 0x00020000 — NSE_MT__HANDSHAKE_OTHER • 0x00040000 — NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 — NSE_MT__APP_DATA_FROM_SERVER

표 7-6 si_connection_log 필드(계속)

필드	설명
ssl_flow_status	<p>SSL 플로우의 상태입니다. 이 값은 작업을 수행한 이유 또는 오류 메시지가 표시된 이유를 설명합니다. 가능한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • 'Unknown' • 'No Match' • 'Success' • 'Uncached Session' • 'Unknown Cipher Suite' • 'Unsupported Cipher Suite' • 'Unsupported SSL Version' • 'SSL Compression Used' • 'Session Undecryptable in Passive Mode' • 'Handshake Error' • 'Decryption Error' • 'Pending Server Name Category Lookup' • 'Pending Common Name Category Lookup' • 'Internal Error' • 'Network Parameters Unavailable' • 'Invalid Server Certificate Handle' • 'Server Certificate Fingerprint Unavailable' • 'Cannot Cache Subject DN' • 'Cannot Cache Issuer DN' • 'Unknown SSL Version' • 'External Certificate List Unavailable' • 'External Certificate Fingerprint Unavailable' • 'Internal Certificate List Invalid' • 'Internal Certificate List Unavailable' • 'Internal Certificate Unavailable' • 'Internal Certificate Fingerprint Unavailable' • 'Server Certificate Validation Unavailable' • 'Server Certificate Validation Failure' • 'Invalid Action'
ssl_issuer_common_name	SSL 인증서의 발급자 일반 이름입니다. 이는 일반적으로 인증서 발급자의 호스트 및 도메인 이름이지만, 다른 정보가 포함될 수도 있습니다.
ssl_issuer_country	SSL 인증서 발급자의 국가입니다.
ssl_issuer_organization	SSL 인증서 발급자의 조직입니다.
ssl_issuer_organization_unit	SSL 인증서 발급자의 조직 부서입니다.

표 7-6 si_connection_log 필드(계속)

필드	설명
ssl_policy_action	일치하는 규칙이 없을 경우 정책에 구성되는 기본 작업입니다.
ssl_policy_name	연결을 처리한 SSL 정책의 ID 번호입니다.
ssl_policy_reason	SSL 정책이 SSL 세션을 로깅한 이유입니다.
ssl_rule_action	SSL 규칙(allow, block 등)의 사용자 인터페이스에서 선택한 작업입니다.
ssl_rule_name	연결을 처리한 SSL 규칙 또는 기본 동작의 ID 번호입니다.
ssl_serial_number	발급 CA가 할당한 SSL 인증서의 일련 번호입니다.
ssl_server_name	SSL Client Hello의 서버 이름 표시에서 제공된 이름입니다.
ssl_subject_common_name	SSL 인증서의 주체 일반 이름입니다. 이는 일반적으로 인증서 주체의 호스트 및 도메인 이름이지만, 다른 정보가 포함될 수도 있습니다.
ssl_subject_country	SSL 인증서 주체의 국가입니다.
ssl_subject_organization	SSL 인증서 주체의 조직입니다.
ssl_subject_organization_unit	SSL 인증서 주체의 조직 부서입니다.
ssl_url_category	서버 이름 및 인증서 일반 이름에서 확인된 플로우의 카테고리입니다.
ssl_version	연결을 암호화하는 데 사용된 SSL 또는 TLS 프로토콜 버전입니다.
tcp_flags	세션에서 탐지된 TCP 플래그입니다.
url	제공되는 경우, 세션 도중 모니터링된 호스트에서 요청한 URL입니다.
url_category	모니터링된 호스트에서 요청한 URL의 카테고리입니다.
url_reputation	모니터링된 호스트에서 요청한 URL의 평판입니다. 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 1 - 매우 위험 • 2 - 의심스러운 사이트 • 3 - 보안 위험이 있는 정상적인 사이트 • 4 - 정상적인 사이트 • 5 - 유명함
web_application_id	웹 애플리케이션의 내부 ID 번호입니다.
web_application_name	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 애플리케이션의 이름 - 올바른 식별이 이루어진 경우 • web browsing - HTTP의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 식별하지 못하는 경우 • 연결에 HTTP 트래픽이 없는 경우 비어 있음

si_connection_log 조인

다음 표에는 `si_connection_log` 테이블을 사용하여 수행할 수 있는 조인이 설명되어 있습니다.

표 7-7 *si_connection_log* 조인

다음에 대해 이 테이블 조인 가능	추가
application_protocol_name 또는 application_id 또는 client_application_id 또는 web_application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id
initiator_ipaddr 또는 responder_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

si_connection_log 샘플 쿼리

다음 쿼리는 `si_connection_log` 테이블에서 최대 25개의 연결 이벤트 레코드를 반환하며, 패킷 타임스탬프를 기준으로 내림차순으로 정렬합니다.

```
SELECT first_packet_sec, last_packet_sec, initiator_ipaddr, responder_ipaddr,
security_zone_ingress_name, security_zone_egress_name, initiator_port, protocol_name,
responder_port, application_protocol_id, client_application_id, web_application_id, url,
url_category, url_reputation
FROM si_connection_log
WHERE first_packet_sec <= UNIX_TIMESTAMP("2011-10-01 00:00:00") ORDER BY
first_packet_sec
DESC, last_packet_sec DESC LIMIT 0, 25;
```




스키마: 사용자 작업 테이블

이 장에는 사용자 작업 및 ID 이벤트의 스키마 및 지원되는 조인에 대한 정보가 포함되어 있습니다. FireSIGHT System은 LDAP, POP3, IMAP, SMTP, AIM, SIP를 비롯한 다양한 유형의 사용자 로그인을 추적하여 네트워크상의 사용자 작업을 탐지할 수 있습니다.

자세한 내용은 아래 표에 나열된 섹션을 참조하십시오.

표 8-1 사용자 ID 테이블의 스키마

참조	다음에 대한 정보가 저장되는 테이블	버전
discovered_users, 페이지 8-1	탐지된 사용자에 대한 정보	5.0+
user_discovery_event, 페이지 8-2	사용자 검색 이벤트 - 네트워크상의 사용자 활동에 대한 상세 정보 전달	5.0+

discovered_users

`discovered_users` 테이블에는 탐지된 각 사용자에 대한 자세한 정보가 포함됩니다.

FireSIGHT System 버전 5.0부터 사용 중단된 `rua_users` 테이블은 `discovered_users` 테이블로 대체됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [discovered_users 필드, 페이지 8-1](#)
- [discovered_users 조인, 페이지 8-2](#)
- [discovered_users 샘플 쿼리, 페이지 8-2](#)

discovered_users 필드

다음 표에는 `discovered_users` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 8-2 `discovered_users` 필드

필드	설명
<code>dept</code>	사용자의 부서입니다.
<code>email</code>	사용자의 이메일 주소입니다.
<code>first_name</code>	사용자의 이름입니다.

표 8-2 discovered_users 필드(계속)

필드	설명
ip_address	이 필드는 사용이 중단되었으며 모든 쿼리에 null을 반환합니다.
ipaddr	사용자 로그인이 탐지되었을 때 호스트의 IPv4 또는 IPv6 주소를 이진수로 나타낸 값입니다.
last_name	사용자의 성입니다.
last_seen_sec	사용자의 마지막 로그인이 보고된 날짜 및 시간의 UNIX 타임스탬프입니다.
last_updated_sec	사용자의 정보가 마지막으로 업데이트된 날짜 및 시간의 UNIX 타임스탬프입니다.
name	사용자의 이름입니다.
phone	사용자의 전화 번호입니다.
rna_service	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
user_id	호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.

discovered_users 조인

다음 표에는 `rua_user` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 8-3 discovered_users 조인

Left 조인을 수행할 수 있는 테이블	조인 유형이 포함된 기타 테이블
user_id	<code>user_discovery_event.user_id</code> <code>user_ipaddr_history.user_id</code>

discovered_users 샘플 쿼리

다음 쿼리는 지정된 날짜 및 시간 이후에 생성된 사용자 레코드를 검색하여 최대 25개까지 반환합니다.

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

user_discovery_event

`user_discovery_event` 테이블에는 각 사용자 검색 이벤트에 대한 레코드가 포함됩니다.

버전 5.0부터는 더 이상 탐지 엔진이 아니라 FireSIGHT System이 관리되는 디바이스 레벨에서 사용자 활동의 탐지를 기록합니다. 이 테이블의 `detection_engine_name` 및 `detection_engine_uuid` 필드는 각각 `sensor_name` 및 `sensor_uuid` 필드로 교체되었습니다. 이러한 필드의 쿼리는 사용자 검색 이벤트를 생성한 관리되는 디바이스에 대한 정보를 반환합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [user_discovery_event 필드, 페이지 8-3](#)
- [user_discovery_event 조인, 페이지 8-4](#)
- [user_discovery_event 샘플 쿼리, 페이지 8-4](#)

user_discovery_event 필드

다음 표에는 `user_discovery_event` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 8-4 user_discovery_event 필드

필드	설명
application_protocol_id	탐지된 애플리케이션 프로토콜의 내부 식별자입니다.
application_protocol_name	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 연결에 사용된 애플리케이션의 이름: LDAP, POP3 등 • pending - 여러 이유 중 하나로 인해 애플리케이션 프로토콜을 식별할 수 없는 경우 • 연결에 애플리케이션 정보가 없는 경우 비어 있음
description	검색 이벤트 유형이 Delete User Identity 또는 User Identity Dropped일 때의 사용자 이름입니다. 그렇지 않은 경우에는 비어 있습니다.
event_id	검색 이벤트의 내부 ID 번호입니다.
event_time_sec	검색 이벤트에 대한 날짜 및 시간의 UNIX 타임스탬프입니다.
event_type	검색 이벤트의 유형입니다. 예를 들어, New User Identity 또는 User Login입니다.
ip_address	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
ipaddr	사용자 활동이 탐지되었을 때 호스트 IP 주소를 이진수로 나타낸 값입니다.
reported_by	사용자 로그인을 보고하는 Active Directory 서버의 IPv4 주소, IPv6 주소 또는 NetBIOS 이름입니다.
sensor_address	사용자 검색 이벤트를 탐지한 관리되는 디바이스의 IP 주소입니다. 형식은 <code>ipv4_address</code> , <code>ipv6_address</code> 입니다.
sensor_name	사용자 검색 이벤트를 탐지한 관리되는 디바이스의 텍스트 이름입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 <code>sensor_name</code> 이 null인 경우 0입니다.
user_dept	호스트에 마지막으로 로그인한 사용자의 부서입니다.
user_email	호스트에 마지막으로 로그인한 사용자의 이메일 주소입니다.
user_first_name	사용자의 이름입니다.
user_id	호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
user_last_name	사용자의 성입니다.
user_last_seen_sec	사용자의 마지막 로그인이 보고된 날짜 및 시간의 UNIX 타임스탬프입니다.
user_last_updated_sec	사용자의 정보가 마지막으로 업데이트된 날짜 및 시간의 UNIX 타임스탬프입니다.

표 8-4 user_discovery_event 필드(계속)

필드	설명
user_name	호스트에 마지막으로 로그인한 사용자의 사용자 이름입니다.
user_phone	호스트에 마지막으로 로그인한 사용자의 전화 번호입니다.

user_discovery_event 조인

다음 표에는 user_discovery_event 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 8-5 user_discovery_event 조인

다음에 대해 이 테이블 조인 가능	추가
ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr
user_id	discovered_users.user_id user_ipaddr_history.user_id

user_discovery_event 샘플 쿼리

다음 쿼리는 선택한 관리되는 디바이스에서 특정 날짜 및 시간 이후에 생성한 사용자 이벤트 레코드를 최대 25개까지 반환합니다.

```
SELECT event_time_sec, ipaddr, sensor_name, event_type, user_name, user_last_seen_sec,
user_last_updated_sec
FROM user_discovery_event
WHERE sensor_name = sensor_name
AND user_last_seen_sec >= UNIX_TIMESTAMP("2011-10-01 00:00:00") ORDER BY event_type ASC
LIMIT 0, 25;
```



스키마: 상관관계 테이블

이 장에는 교정 상태 및 화이트리스트 이벤트를 비롯한 상관관계 관련 이벤트의 스키마 및 지원되는 조인에 대한 정보가 포함되어 있습니다. 자세한 내용은 아래 표에 나열된 섹션을 참조하십시오.

표 9-1 상관관계 테이블의 스키마

참조	다음에 대한 정보가 저장되는 테이블	버전
compliance_event , 페이지 9-1	상관관계 이벤트 - 활성화 상관관계 정책 내에서 상관관계 규칙이 트리거될 때 생성됩니다.	4.10.x+
remediation_status , 페이지 9-6	교정 상태 이벤트 - 활성화 상관관계 정책이 응답의 일환으로 교정을 트리거할 때 생성됩니다.	4.10.x+
white_list_event , 페이지 9-7	화이트리스트 이벤트 - 활성화 화이트리스트 규정준수 정책의 화이트리스트를 위반하는 호스트가 탐지될 때 생성됩니다.	4.10.x+
white_list_violation , 페이지 9-9	화이트리스트 위반 - 네트워크의 호스트가 활성화 규정준수 정책의 규정준수 화이트리스트를 위반하는 방식을 추적합니다.	4.10.x+

compliance_event

`compliance_event` 테이블에는 방어 센터에서 생성하는 상관관계 이벤트에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [compliance_event 필드](#), [페이지 9-1](#)
- [compliance_event 조인](#), [페이지 9-5](#)
- [compliance_event 샘플 쿼리](#), [페이지 9-5](#)

compliance_event 필드

상관관계 규칙을 트리거한 이벤트의 유형에 따라 테이블의 많은 필드가 비어 있을 수 있습니다. 예를 들어, 특정 애플리케이션 프로토콜이 탐지되거나 특정 포트에서 실행 중인 웹 애플리케이션이 탐지되어 방어 센터에서 상관관계 이벤트를 생성하는 경우, 이러한 상관관계 이벤트에는 침입 관련 정보가 포함되지 않습니다. 이 테이블의 필드는 FireSIGHT System 컨피그레이션에 따라서도 비어 있을 수 있습니다. 예를 들어, Control 라이선스가 없는 경우 상관관계 이벤트에는 사용자 ID 정보가 포함되지 않습니다.

버전 5.0부터는 탐지 엔진이 아니라 FireSIGHT System이 관리되는 디바이스 레벨에서 네트워크 및 사용자 활동의 탐지를 기록합니다. 이제 `compliance_event` 테이블의 `detection_engine_name` 및 `detection_engine_uuid` 필드는 빈칸만 반환하며, 해당 필드를 조인하는 쿼리는 제로 레코드를 반환합니다. 이벤트 탐지 위치에 대한 정보는 `detection_engine_uuid`가 아닌 `sensor_uuid` 필드에서 쿼리해야 합니다.

다음 표에는 `compliance_event` 테이블에서 액세스할 수 있는 필드가 설명되어 있습니다.

표 9-2 `compliance_event` 필드

필드	설명
<code>blocked</code>	침입 이벤트를 트리거한 패킷에 무슨 상황이 발생했는지 나타내는 값입니다. <ul style="list-style-type: none"> 0 — 패킷이 삭제되지 않음 1 — 패킷이 삭제됨(인라인, 스위치드 또는 라우티드 구축) 2 — 이벤트를 트리거한 패킷이 삭제되었을 수 있음(침입 정책이 인라인, 스위치드 또는 라우티드 구축의 디바이스에 적용된 경우)
<code>description</code>	상관관계 이벤트 및 트리거된 방식에 대한 정보
<code>detection_engine_name</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>detection_engine_uuid</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>dst_host_criticality</code>	상관관계 이벤트와 관련된 소스 또는 목적지 호스트에 대해 사용자가 할당하는 호스트 중요도(<code>None</code> , <code>Low</code> , <code>Medium</code> , <code>High</code>)입니다.
<code>dst_host_type</code>	목적지 호스트 유형(<code>Host</code> , <code>Router</code> , <code>Bridge</code> , <code>NAT Device</code> , <code>Load Balancer</code>)입니다.
<code>dst_ip_address</code>	버전 5.2에서 사용 중단된 필드입니다. 이전 버전과의 호환성 때문에 이 필드의 값은 <code>null</code> 로 설정되지 않으나, 신뢰할 수 없습니다.
<code>dst_ip_address_v6</code>	버전 5.2에서 사용 중단된 필드입니다. 이전 버전과의 호환성 때문에 이 필드의 값은 <code>null</code> 로 설정되지 않으나, 신뢰할 수 없습니다.
<code>dst_ipaddr</code>	이벤트 트리거와 관련된 목적지 호스트의 IPv4 또는 IPv6 주소를 이진수로 나타낸 값입니다.
<code>dst_os_product</code>	목적지 호스트의 운영 체제 이름입니다.
<code>dst_os_vendor</code>	목적지 호스트의 운영 체제 공급업체입니다.
<code>dst_os_version</code>	목적지 호스트의 운영 체제 버전 번호입니다.
<code>dst_port</code>	이벤트 프로토콜 유형이 TCP 또는 UDP인 경우 트래픽을 수신하는 호스트의 포트 번호입니다. 프로토콜 유형이 ICMP인 경우에는 ICMP 코드입니다.
<code>dst_rna_service</code>	식별된 경우, 이벤트 트리거와 관련된 소스 호스트의 애플리케이션 프로토콜입니다. 식별되지 않은 경우 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> <code>none</code> 또는 빈칸 - 애플리케이션 프로토콜 트래픽이 없음 <code>unknown</code> - 알려진 서버 지문을 기반으로 서버를 식별할 수 없음 <code>pending</code> - 추가 정보가 필요함
<code>dst_user_dept</code>	목적지 사용자의 부서입니다.
<code>dst_user_email</code>	목적지 사용자의 이메일 주소입니다.
<code>dst_user_first_name</code>	목적지 사용자의 이름입니다.
<code>dst_user_id</code>	목적지 사용자, 즉, 이벤트가 발생하기 전에 목적지 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
<code>dst_user_last_name</code>	목적지 사용자의 성입니다.

표 9-2 compliance_event 필드(계속)

필드	설명
dst_user_last_seen_sec	목적지 사용자의 마지막 로그인 이 보고된 날짜 및 시간의 UNIX 타임스탬프입니다.
dst_user_last_updated_sec	목적지 사용자의 정보가 마지막으로 업데이트된 날짜 및 시간의 UNIX 타임스탬프입니다.
dst_user_name	목적지 사용자의 사용자 이름입니다.
dst_user_phone	목적지 사용자의 전화 번호입니다.
dst_vlan_id	해당하는 경우, 목적지 호스트의 VLAN ID 번호입니다.
event_id	디바이스에서 생성된 침입 이벤트 트리거의 ID 번호입니다.
event_time_sec	이벤트 트리거에 대한 날짜 및 시간의 UNIX 타임스탬프입니다.
event_time_usec	이벤트 트리거 타임스탬프가 마이크로초 단위로 증가한 값입니다.
event_type	상관관계 규칙을 트리거했거나 방어 센터가 상관관계 이벤트를 생성하도록 유발한 기본 이벤트의 유형입니다. 값은 다음과 같습니다. <ul style="list-style-type: none"> ids - 침입 이벤트 트리거 rna - 검색 이벤트, 호스트 입력 이벤트, 연결 이벤트, 또는 트래픽 프로필 변경 트리거 rua - 사용자 검색 이벤트 트리거 whitelist - 규정준수 화이트리스트 위반 트리거
host_event_type	이벤트 유형(예: New Host 또는 Identity Conflict)입니다.
id	상관관계 이벤트의 내부 ID 번호입니다.
impact	이벤트의 영향 플래그 값입니다. 값은 다음과 같습니다. <ul style="list-style-type: none"> 1 - 빨간색(vulnerable) 2 - 주황색(potentially vulnerable) 3 - 노란색(currently not vulnerable) 4 - 파란색(unknown target) 5 - 회색(unknown impact) 상관관계 규칙이 침입 이벤트에 의해 트리거된 경우에만 설정됩니다.
interface_egress_name	연결과 관련된 이그레스 인터페이스입니다.
interface_ingress_name	연결과 관련된 이그레스 인터페이스입니다.
policy_name	위반된 상관관계 정책입니다.
policy_rule_name	정책 위반을 트리거한 상관관계 규칙입니다.
policy_rule_uuid	상관관계 규칙의 고유한 식별자입니다.
policy_time_sec	상관관계 이벤트가 생성된 날짜 및 시간의 UNIX 타임스탬프입니다.
policy_uuid	상관관계 정책의 고유한 식별자입니다.
priority	사용자 인터페이스에서 설정되는 상관관계 이벤트의 우선순위입니다. 트리거된 규칙 또는 위반된 상관관계 정책의 우선순위에 의해 결정되는 상관관계 이벤트의 우선순위를 지정합니다.
protocol_name	이벤트와 관련된 프로토콜입니다(제공되는 경우).

표 9-2 compliance_event 필드(계속)

필드	설명
protocol_num	IANA 지정 프로토콜 번호입니다(제공되는 경우).
rna_event_type	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
rua_event_type	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
rule_generator_id	침입 이벤트 트리거를 생성한 구성 요소의 GID(Generator ID) 번호입니다.
rule_message	상관관계 규칙을 트리거한 침입 이벤트에 대한 설명 텍스트입니다. 규칙 기반 이벤트의 경우 규칙에서 메시지가 생성됩니다. 디코더 및 프리프로세서 기반 이벤트의 경우 이벤트 메시지가 하드 코딩됩니다.
rule_signature_id	이벤트의 서명 ID(SID)입니다. 침입 이벤트 트리거를 생성하도록 유발한 특정 규칙, 디코더 메시지 또는 프리프로세서 메시지를 식별합니다.
security_zone_egress_name	상관관계 이벤트의 이그레스 보안 영역입니다.
security_zone_ingress_name	상관관계 이벤트의 인그레스 보안 영역입니다.
sensor_address	규정준수 이벤트를 트리거한 기본 이벤트를 생성한 관리되는 디바이스의 IP 주소입니다. 형식은 <i>ipv4_address</i> , <i>ipv6_address</i> 입니다.
sensor_name	규정준수 이벤트를 트리거한 기본 이벤트를 생성한 관리되는 디바이스입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 <i>sensor_name</i> 이 null인 경우 0입니다.
src_host_criticality	규정준수 이벤트와 관련된 소스 호스트에 대해 사용자가 할당하는 소스 호스트 중요도(None, Low, Medium, High)입니다.
src_host_type	소스 호스트 유형(Host, Router, Bridge, NAT Device, Load Balancer)입니다.
src_ip_address	버전 5.2에서 사용 중단된 필드입니다. 이전 버전과의 호환성 때문에 이 필드의 값은 null로 설정되지 않으나, 신뢰할 수 없습니다.
src_ip_address_v6	버전 5.2에서 사용 중단된 필드입니다. 이전 버전과의 호환성 때문에 이 필드의 값은 null로 설정되지 않으나, 신뢰할 수 없습니다.
src_ipaddr	이벤트 트리거와 관련된 소스 호스트의 IPv4 또는 IPv6 주소를 이진수로 나타낸 값입니다.
src_os_product	소스 호스트의 운영 체제 이름입니다.
src_os_vendor	소스 호스트의 운영 체제 공급업체 이름입니다.
src_os_version	소스 호스트의 운영 체제 버전 번호입니다.
src_port	소스 호스트의 포트 번호입니다. ICMP 트래픽의 경우 ICMP 유형이 대신 표시됩니다.
src_rna_service	식별된 경우, 이벤트 트리거와 관련된 소스 호스트의 애플리케이션 프로토콜입니다. 식별되지 않은 경우 다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • none 또는 빈칸 - 애플리케이션 프로토콜 트래픽이 없음 • unknown - 알려진 서버 지문을 기반으로 서버 및 애플리케이션 프로토콜을 식별할 수 없음 • pending - 추가 정보가 필요함
src_user_dept	소스 사용자의 부서입니다.
src_user_email	소스 사용자의 이메일 주소입니다.
src_user_first_name	소스 사용자의 이름입니다.

표 9-2 compliance_event 필드(계속)

필드	설명
src_user_id	소스 사용자, 즉, 이벤트가 발생하기 전에 소스 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
src_user_last_name	소스 사용자의 성입니다.
src_user_last_seen_sec	소스 사용자의 로그인이 마지막으로 보고된 날짜 및 시간의 UNIX 타임스탬프입니다.
src_user_last_updated_sec	소스 사용자의 정보가 마지막으로 업데이트된 날짜 및 시간의 UNIX 타임스탬프입니다.
src_user_name	소스 사용자의 로그인 사용자 이름입니다.
src_user_phone	소스 사용자의 전화 번호입니다.
src_vlan_id	해당하는 경우, 소스 호스트의 VLAN ID 번호입니다.
user_event_type	사용자 이벤트 트리거 유형(예: New User Identity 또는 User Login)입니다.

compliance_event 조인

다음 표에는 `compliance_event` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 9-3 compliance_event 조인

다음에 대해 이 테이블 조인 가능	추가
dst_ipaddr 또는 src_ipaddr	<code>rna_host_ip_map.ipaddr</code> <code>user_ipaddr_history.ipaddr</code>

compliance_event 샘플 쿼리

다음 쿼리는 일주일간의 상관관계 이벤트 레코드를 최대 25개까지 반환하며 여기에는 이벤트 시간, 소스 및 목적지 IP 주소, 소스 및 목적지 포트, 정책 정보 등과 같은 이벤트 정보가 포함됩니다.

```
SELECT event_id, policy_time_sec, impact, blocked, src_ipaddr, dst_ipaddr, src_port,
dst_port, description, policy_name, policy_rule_name, priority, src_host_criticality,
dst_host_criticality, security_zone_egress_name, security_zone_ingress_name,
sensor_name, interface_egress_name, interface_ingress_name
FROM compliance_event WHERE event_type!="whitelist"
AND policy_time_sec
BETWEEN UNIX_TIMESTAMP("2011-10-01 00:00:00")
AND UNIX_TIMESTAMP("2011-10-07 23:59:59")
ORDER BY policy_time_sec
DESC LIMIT 0, 25;
```

remediation_status

remediation_status 테이블에는 방어 센터가 상관관계 정책 위반에 대응하여 생성한 교정 이벤트에 대한 정보가 포함됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- remediation_status 필드, 페이지 9-6
- remediation_status 조인, 페이지 9-6
- remediation_status 샘플 쿼리, 페이지 9-6

remediation_status 필드

다음 표에는 remediation_status 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 9-4 remediation_status 필드

필드	설명
id	위반되어 교정을 트리거한 정책의 ID 번호입니다.
policy_name	위반되어 교정을 트리거한 상관관계 정책입니다.
policy_rule_name	교정을 트리거한 특정 상관관계 규칙입니다.
policy_rule_uuid	상관관계 규칙의 고유한 식별자입니다.
policy_time_sec	교정을 트리거한 상관관계 이벤트가 생성된 날짜 및 시간의 UNIX 타임스탬프입니다.
policy_uuid	상관관계 이벤트를 트리거한 상관관계 정책의 고유한 식별자입니다.
remediation_name	실행된 교정입니다.
remediation_time_sec	방어 센터가 교정을 실행한 날짜 및 시간의 UNIX 타임스탬프입니다.
status_text	교정이 실행되었을 때 발생한 상황을 설명하는 메시지입니다(예: "successful completion of remediation").

remediation_status 조인

remediation_status 테이블에서는 조인을 수행할 수 없습니다.

remediation_status 샘플 쿼리

다음 쿼리는 지정된 날짜 이전에 생성된 레코드를 최대 25개까지 반환합니다. 이러한 레코드에는 교정 타임스탬프, 상태 메시지 등과 같은 교정 상태 정보가 포함됩니다.

```
SELECT policy_time_sec, remediation_time_sec, remediation_name, policy_name,
policy_rule_name, status_text
FROM remediation_status WHERE remediation_time_sec <= UNIX_TIMESTAMP("2011-10-01
00:00:00")
ORDER BY policy_time_sec
DESC LIMIT 0, 25;
```

white_list_event

`white_list_event` 테이블에는 활성 화이트리스트 규정준수 정책의 화이트리스트를 위반하는 호스트가 탐지될 때 생성된 화이트리스트 이벤트가 포함됩니다.

버전 5.0부터는 더 이상 탐지 엔진이 아니라 FireSIGHT System이 관리되는 디바이스 레벨에서 네트워크 및 사용자 활동의 탐지를 기록합니다. 이제 `white_list_event` 테이블의 `detection_engine_name` 및 `detection_engine_uuid` 필드는 `null`만 반환하며, 해당 필드를 조인하는 쿼리는 제로 레코드를 반환합니다. `detection_engine_uuid` 대신 `sensor_uuid` 필드에서 쿼리를 수행하면 동일한 정보가 제공됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [white_list_event 필드, 페이지 9-7](#)
- [white_list_event 조인, 페이지 9-8](#)
- [white_list_event 샘플 쿼리, 페이지 9-8](#)

white_list_event 필드

다음 표에는 `white_list_event` 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 9-5 `white_list_event` 필드

필드	설명
<code>description</code>	화이트리스트를 어떤 식으로 위반했는지 설명합니다.
<code>detection_engine_name</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>detection_engine_uuid</code>	버전 5.0에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>host_criticality</code>	화이트리스트를 준수하지 않는 호스트에 대해 사용자가 할당하는 호스트 중요도 (None, Low, Medium, High)입니다.
<code>host_type</code>	호스트 유형(Host, Router, Bridge, NAT Device, Load Balancer)입니다.
<code>id</code>	화이트리스트 이벤트의 내부 고유 식별자입니다.
<code>ip_address</code>	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>ip_address_v6</code>	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>ipaddr</code>	규정준수를 위반한 호스트의 IP 주소를 이진수로 나타낸 값입니다.
<code>os_product</code>	운영 체제의 제품 이름입니다.
<code>os_vendor</code>	운영 체제의 공급업체입니다.
<code>os_version</code>	운영 체제의 버전 번호입니다.
<code>policy_name</code>	화이트리스트를 포함하는 위반된 규정준수 정책입니다.
<code>policy_time_sec</code>	이벤트가 생성된 날짜 및 시간의 UNIX 타임스탬프입니다.
<code>policy_uuid</code>	화이트리스트 이벤트를 포함하는 규정준수 정책의 고유한 식별자입니다.
<code>port</code>	서비스 화이트리스트 위반을 트리거(즉, 규정준수 위반 서비스로 인해 위반이 발생한 경우)한 이벤트와 관련된 포트입니다. 다른 유형의 화이트리스트 위반의 경우, 이 필드는 빈칸으로 되어 있습니다.
<code>priority</code>	사용자 인터페이스에서 설정되는 화이트리스트 이벤트의 우선순위입니다.

표 9-5 white_list_event 필드(계속)

필드	설명
protocol_name	이벤트와 관련된 프로토콜입니다(제공되는 경우).
protocol_num	IANA 지정 프로토콜 번호입니다(제공되는 경우).
rna_service	화이트리스트 위반을 트리거한 서비스입니다(제공되는 경우).
sensor_address	트래픽을 탐지한 관리되는 디바이스의 IP 주소입니다. 형식은 <i>ipv4_address</i> , <i>ipv6_address</i> 입니다.
sensor_name	화이트리스트 이벤트를 생성한 디바이스입니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 <i>sensor_name</i> 이 null인 경우 0입니다.
user_dept	사용자의 부서입니다.
user_email	사용자의 이메일 주소입니다.
user_first_name	사용자의 이름입니다.
user_id	이벤트가 발생하기 전에 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
user_last_name	사용자의 성입니다.
user_last_seen_sec	사용자의 마지막 로그인이 보고된 날짜 및 시간의 UNIX 타임스탬프입니다.
user_last_updated_sec	사용자의 정보가 마지막으로 업데이트된 날짜 및 시간의 UNIX 타임스탬프입니다.
user_name	사용자의 로그인 사용자 이름입니다.
user_phone	사용자의 전화 번호입니다.
vlan_id	해당하는 경우, VLAN ID 번호입니다.
white_list_name	위반된 화이트리스트입니다.
white_list_uuid	화이트리스트의 고유한 식별자입니다.

white_list_event 조인

다음 표에는 `white_list_event` 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 9-6 white_list_event 조인

다음에 대해 이 테이블 조인 가능	추가
ipaddr	<code>rna_host_ip_map.ipaddr</code> <code>user_ipaddr_history.ipaddr</code>

white_list_event 샘플 쿼리

다음 쿼리는 지정된 시간 이전에 생성된 레코드를 최대 25개까지 반환합니다. 해당 레코드에는 규정준수 정책 이름, 이벤트가 생성된 타임스탬프, 화이트리스트 이름 등과 같은 화이트리스트 이벤트 정보가 포함됩니다.

```
SELECT policy_name, policy_time_sec, ipaddr, user_name, port, description,
white_list_name, priority, host_criticality, sensor_name
FROM white_list_event WHERE policy_time_sec <= UNIX_TIMESTAMP("2011-10-01 00:00:00")
ORDER BY policy_time_sec DESC LIMIT 0, 25;
```

white_list_violation

`white_list_violation` 테이블은 규정준수 화이트리스트 위반을 추적하며, 이는 네트워크의 호스트가 활성 규정준수 정책의 규정준수 화이트리스트를 위반하는 방식을 추적합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [white_list_violation 필드, 페이지 9-9](#)
- [white_list_violation 조인, 페이지 9-9](#)
- [white_list_violation 샘플 쿼리, 페이지 9-10](#)

white_list_violation 필드

다음 표에는 `white_list_violation` 테이블에서 액세스할 수 있는 데이터베이스 필드가 설명되어 있습니다.

표 9-7 `white_list_violation` 필드

필드	설명
<code>host_id</code>	화이트리스트를 위반한 호스트의 ID 번호입니다.
<code>info</code>	화이트리스트 위반과 관련하여 제공되는 모든 공급업체, 제품 또는 버전 정보입니다. 화이트리스트를 위반한 프로토콜의 경우, 이 필드에 해당 위반이 네트워크로 인한 것인지 전송 프로토콜로 인한 것인지 표시됩니다.
<code>ip_address</code>	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 <code>null</code> 을 반환합니다.
<code>port</code>	서비스 화이트리스트 위반을 트리거(즉, 규정준수 위반 서비스로 인해 위반이 발생한 경우)한 이벤트와 관련된 포트입니다. 다른 유형의 화이트리스트 위반의 경우, 이 필드는 빈 칸으로 되어 있습니다.
<code>protocol_name</code>	이벤트와 관련된 프로토콜입니다.
<code>type</code>	화이트리스트 위반의 유형으로, 해당 위반이 규정준수 위반으로 인해 발생한 것인지 나타냅니다. <ul style="list-style-type: none"> • 운영 체제(<code>os</code>) • 서비스(<code>service</code>) • 클라이언트 애플리케이션(<code>client app</code>) • 프로토콜(<code>protocol</code>)
<code>violation_time_sec</code>	위반이 로깅된 날짜 및 시간의 UNIX 타임스탬프입니다.
<code>white_list_name</code>	위반된 화이트리스트입니다.
<code>white_list_uuid</code>	화이트리스트의 고유한 식별자입니다.

white_list_violation 조인

`white_list_violation` 테이블에서는 조인을 수행할 수 없습니다.

white_list_violation 샘플 쿼리

다음 쿼리는 화이트리스트를 위반한 호스트 IP 주소, 위반된 화이트리스트 이름, 위반 수 같은 화이트리스트 위반 정보가 포함된 레코드를 최대 25개까지 반환합니다.

```
SELECT host_id, white_list_name, count(*)
FROM white_list_violation
GROUP BY white_list_name, host_id
ORDER BY white_list_name
DESC LIMIT 0, 25;
```



스키마: 파일 이벤트 테이블

이 장에는 파일 이벤트의 스키마 및 지원되는 조인에 대한 정보가 포함되어 있습니다. 자세한 내용은 아래 표에 나열된 섹션을 참조하십시오.

표 10-1 파일 이벤트 테이블의 스키마

참조	다음에 대한 정보가 저장되는 테이블	버전
file_event , 페이지 10-1	모니터링된 네트워크에서 파일 전송이 탐지되었을 때 생성된 파일 이벤트	5.1.1+

다음 테이블을 사용할 수 있는 동안 Cisco에서는 현재 해당 테이블에 대한 조회를 지원하지 않습니다.

- `file_categories`
- `file_rules`
- `file_types`
- `file_type_rule_map`
- `file_type_category_map`

file_event

`file_event` 테이블에는 방어 센터에서 생성하는 파일 이벤트에 대한 정보가 포함됩니다. 모니터링된 네트워크에서 파일 전송이 탐지될 때마다 새로운 파일 이벤트가 생성됩니다.

자세한 내용은 다음 섹션을 참조하십시오.

- [file_event 필드](#), [페이지 10-1](#)
- [file_event 조인](#), [페이지 10-6](#)
- [file_event 샘플 쿼리](#), [페이지 10-6](#)

file_event 필드

`file_event` 테이블에는 모니터링된 네트워크를 통과하는 탐지된 파일에 대한 정보가 포함됩니다. 각 파일 이벤트는 연결 이벤트와 상관관계가 있을 수 있습니다. 파일 및 파일 전송의 상세 정보가 기록되며 이러한 정보에는 이름, 크기, 소스, 목적지, 파일의 방향, 파일의 SHA256 해시, 파일을 탐지한 디바이스, 파일의 악성코드 여부가 포함됩니다.

표 10-2 file_event 필드

필드	설명
action	파일 유형을 기반으로 파일에 조취를 취합니다. 다음과 같은 값을 사용할 수 있습니다. <ul style="list-style-type: none"> • 1 — Detect • 2 — Block • 3 — Malware Cloud Lookup • 4 — Malware Block • 5 — Malware Whitelist • 6 — Cloud Lookup Timeout
application_id	파일 전송을 사용하여 애플리케이션에 매핑되는 ID 번호입니다.
application_name	다음 중 하나에 해당합니다. <ul style="list-style-type: none"> • 연결에 사용된 애플리케이션의 이름 • pending 또는 unknown - 애플리케이션을 식별하지 못할 경우 • 연결에 애플리케이션 정보가 없는 경우 비어 있음
archived	파일이 아카이브되었다는 것을 나타냅니다.
cert_valid_end_date	연결에 사용된 SSL 인증서의 유효 기간이 만료되는 날짜에 대한 Unix 타임스탬프입니다.
cert_valid_start_date	연결에 사용된 SSL 인증서가 발행된 날짜에 대한 Unix 타임스탬프입니다.
client_application_id	해당하는 경우, 클라이언트 애플리케이션의 내부 ID 번호입니다.
client_application_name	해당하는 경우, 클라이언트 애플리케이션의 이름입니다.
connection_sec	파일 이벤트와 관련된 연결 이벤트의 UNIX 타임스탬프(00:00:00 01/01/1970 이후의 초)입니다.
counter	동일한 초에 발생한 여러 개의 이벤트를 구분하기 위해 사용되는 특정 이벤트 카운터입니다.
direction	파일이 업로드되거나 다운로드되었는지 나타냅니다. 현재 이 값은 전적으로 프로토콜에 따라 좌우됩니다(예: 연결이 HTTP인 경우 다운로드임).
disposition	파일의 악성코드 상태입니다. 가능한 값은 다음과 같습니다. <ul style="list-style-type: none"> • CLEAN — 파일이 깨끗하고 악성코드가 포함되어 있지 않습니다. • UNKNOWN — 파일에 악성코드가 포함되어 있는지 알 수 없습니다. • MALWARE — 파일에 악성코드가 포함되어 있습니다. • UNAVAILABLE — 소프트웨어가 처리를 위한 요청을 Cisco 클라우드에 전송하지 못했거나, Cisco 클라우드 서비스가 요청에 응답하지 않았습니다. • CUSTOM SIGNATURE — 파일이 사용자가 정의한 해시와 일치하며, 사용자가 지정한 방식으로 처리됩니다.

표 10-2 file_event 필드(계속)

필드	설명
dst_continent_name	목적지 호스트의 대륙 이름입니다. ** — 알 수 없음 na — 북미 as — 아시아 af — 아프리카 eu — 유럽 sa — 남미 au — 호주 an — 남극 대륙
dst_country_id	목적지 호스트의 국가 코드입니다.
dst_country_name	목적지 호스트의 국가 이름입니다.
dst_ip_address_v6	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
dst_ipaddr	이벤트 트리거와 관련된 목적지 호스트의 IP 주소를 이진수로 나타낸 값입니다.
dst_port	연결 목적지에 대한 포트 번호입니다.
event_description	이벤트 유형과 관련된 추가 이벤트 정보입니다.
event_id	이벤트 ID 번호입니다.
file_name	탐지된 파일의 이름입니다. 이 이름에는 UTF-8 문자를 포함할 수 있습니다.
file_sha	파일의 SHA256 해시입니다.
file_size	탐지된 파일의 바이트 단위 크기입니다.
file_type	탐지 또는 격리된 파일의 파일 유형입니다.
file_type_category	파일 카테고리에 대한 설명입니다.
file_type_category_id	파일 카테고리의 숫자 식별자입니다.
file_type_id	파일 유형에 매핑되는 ID 번호입니다.
instance_id	이벤트를 생성한 관리되는 디바이스의 Snort 인스턴스의 숫자 ID입니다.
policy_uuid	이벤트를 트리거한 액세스 제어 정책의 고유한 식별자 역할을 하는 ID 번호입니다.

표 10-2 file_event 필드(계속)

필드	설명
sandboxed	<p>동적 분석을 위해 파일이 제출되었는지 나타냅니다. 가능한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> • Sent for Analysis • Failed to Send • File Size is Too Small • File Size is Too Large • Sent for Analysis • Analysis Complete • Failure (Network Issue) • Failure (Rate Limit) • Failure (File Too Large) • Failure (File Read Error) • Failure (Internal Library Error) • File Not Sent, Disposition Unavailable • Failure (Cannot Run File) • Failure (Analysis Timeout) • File Not Supported
score	동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 0부터 100까지 나타낸 숫자 값입니다.
security_context	트래픽이 통과한 보안 컨텍스트(가상 방화벽)에 대한 설명입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
sensor_address	이벤트를 제공한 디바이스의 IP 주소를 이진수로 나타낸 값입니다.
sensor_id	이벤트를 제공한 디바이스의 ID입니다.
sensor_name	이벤트 레코드를 생성한 관리되는 디바이스의 텍스트 이름입니다. 이 필드는 이벤트가 참조하는 대상이 연결된 디바이스가 아닌 보고 디바이스 자체일 경우 null이 됩니다.
sensor_uuid	관리되는 디바이스의 고유한 식별자입니다. 또는 sensor_name이 null인 경우 0입니다.
signature_processed	파일의 서명이 처리되었는지 나타냅니다.

표 10-2 file_event 필드(계속)

필드	설명
src_continent_name	소스 호스트의 대륙 이름입니다. ** — 알 수 없음 na — 북미 as — 아시아 af — 아프리카 eu — 유럽 sa — 남미 au — 호주 an — 남극 대륙
src_country_id	소스 호스트의 국가 코드입니다.
src_country_name	소스 호스트의 국가 이름입니다.
src_ip_address_v6	버전 5.2에서 사용 중단된 필드입니다. 모든 쿼리에 null을 반환합니다.
src_ipaddr	이벤트 트리거와 관련된 소스 호스트의 IPv4 또는 IPv6 주소를 이진수로 나타낸 값입니다.
src_port	연결 소스의 포트 번호입니다.
ssl_issuer_common_name	SSL 인증서의 발급자 일반 이름입니다. 이는 일반적으로 인증서 발급자의 호스트 및 도메인 이름이지만, 다른 정보가 포함될 수도 있습니다.
ssl_issuer_country	SSL 인증서 발급자의 국가입니다.
ssl_issuer_organization	SSL 인증서 발급자의 조직입니다.
ssl_issuer_organization_unit	SSL 인증서 발급자의 조직 부서입니다.
ssl_serial_number	발급 CA가 할당한 SSL 인증서의 일련 번호입니다.
ssl_subject_common_name	SSL 인증서의 주체 일반 이름입니다. 이는 일반적으로 인증서 주체의 호스트 및 도메인 이름이지만, 다른 정보가 포함될 수도 있습니다.
ssl_subject_country	SSL 인증서 주체의 국가입니다.
ssl_subject_organization	SSL 인증서 주체의 조직입니다.
ssl_subject_organization_unit	SSL 인증서 주체의 조직 부서입니다.
storage	파일의 저장 상태입니다. 가능한 값은 다음과 같습니다. <ul style="list-style-type: none"> File Stored Unable to Store File File Size is Too Large File Size is Too Small Unable to Store File File Not Stored, Disposition Unavailable
threat_name	위협의 이름입니다.
timestamp	파일 유형을 식별하기 위한 파일이 충분히 전송되었을 때의 UNIX 타임스탬프입니다.
url	파일 소스의 URL입니다.

표 10-2 file_event 필드(계속)

필드	설명
user_id	목적지 사용자, 즉, 이벤트가 발생하기 전에 목적지 호스트에 마지막으로 로그인한 사용자의 내부 ID 번호입니다.
username	user_id와 관련된 이름입니다.
web_application_id	해당하는 경우, 웹 애플리케이션의 내부 ID 번호입니다.
web_application_name	해당하는 경우, 웹 애플리케이션의 이름입니다.

file_event 조인

다음 표에는 file_event 테이블에서 수행할 수 있는 조인이 설명되어 있습니다.

표 10-3 file_event 조인

다음에 대해 이 테이블 조인 가능	추가
application_id	<pre> application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id </pre>

file_event 샘플 쿼리

다음 쿼리는 애플리케이션 이름, 연결 정보, 파일 이름, 처리 상태가 CLEAN이 아닌 항목이 포함된 파일 이벤트를 최대 10개까지 반환합니다.

```

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

FROM file_event

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

```



사용 중단된 테이블

이 부록에는 이전 릴리스에서 사용되었으나 지금은 사용 중단된 테이블에 대한 정보가 포함되어 있습니다. 이러한 테이블에 대한 쿼리는 계속 수행할 수 있으나, 필드의 값은 올바르지 않을 수 있으며 대부분의 경우 null로 되어 있습니다. 이러한 테이블에는 지원되는 조인이 없습니다.

표 A-1 **사용 중단된 테이블**

표	다음으로 대체됨	최종 사용 버전
application_ip_map	application_host_map , 페이지 6-5	5.1.1
rna_ip_host	rna_host , 페이지 6-12	5.1.1
rna_ip_host_attribute	rna_host_attribute , 페이지 6-13	5.1.1
rna_ip_host_client_app	rna_host_client_app , 페이지 6-15	5.1.1
rna_ip_host_client_app_payload	rna_host_client_app_payload , 페이지 6-17	5.1.1
rna_ip_host_os	rna_host_os , 페이지 6-26	5.1.1
rna_ip_host_os_vulns	rna_host_os_vulns , 페이지 6-28	5.1.1
rna_ip_host_sensor	rna_host_sensor , 페이지 6-31	5.1.1
rna_ip_host_service	rna_host_service , 페이지 6-33	5.1.1
rna_ip_host_service_banner	rna_host_service_banner , 페이지 6-35	5.1.1
rna_ip_host_service_info	rna_host_service_info , 페이지 6-36	5.1.1
rna_ip_host_service_payload	rna_host_service_payload , 페이지 6-39	5.1.1
rna_ip_host_service_subtype	rna_host_service_subtype , 페이지 6-42	5.1.1
rna_ip_host_service_vulns	rna_host_service_vulns , 페이지 6-43	5.1.1
rna_ip_host_third_party_vuln	rna_host_third_party_vuln , 페이지 6-45	5.1.1
rna_ip_host_third_party_vuln_bugtraq_id	rna_host_third_party_vuln_bugtraq_id , 페이지 6-46	5.1.1
rna_ip_host_third_party_vuln_cve_id	rna_host_third_party_vuln_cve_id , 페이지 6-48	5.1.1
rna_ip_host_third_party_vuln_rna_id	rna_host_third_party_vuln_rna_id , 페이지 6-50	5.1.1
rna_ip_host_user_history	user_ipaddr_history , 페이지 6-57	5.1.1
rna_mac_host	rna_host_mac_map , 페이지 6-25	5.1.1
rna_mac_host_sensor	rna_host_mac_map , 페이지 6-25	5.1.1
rna_mac_ip_map	rna_host_ip_map , 페이지 6-24 rna_host_mac_map , 페이지 6-25	5.1.1



색인

A

app_ids_stats [5-4, 5-8, 5-10, 5-11, 5-12, 5-15, 5-16, 5-17](#)
app_stats [5-6](#)
application_info [6-7](#)
application_ip_map [6-5](#)
application_tag_map [6-9](#)
audit_log [3-1](#)

C

compliance_event [9-2](#)
connection_log [7-2, 7-15](#)
connection_summary [7-12](#)

D

DHCP [2-4](#)
DHCP 를 사용하는 네트워크 설정 [2-4](#)
discovered_users [8-1](#)

F

file_event [10-1](#)
fireamp_event [3-2](#)

H

health_event [3-9](#)

I

intrusion_event [4-2](#)
intrusion_event_packet [4-7](#)

N

network_discovery_event [6-10](#)

R

remediation_status [9-6](#)
rna_host_protocol [6-30](#)
rna_ip_host_attribute [6-14](#)
rna_ip_host_client_app [6-15](#)
rna_ip_host_client_app_payload [6-18](#)
rna_ip_host_os [6-27](#)
rna_ip_host_os_vulns [6-29](#)
rna_ip_host_sensor [6-32](#)
rna_ip_host_service [6-33](#)
rna_ip_host_service_banner [6-35](#)
rna_ip_host_service_info [6-37](#)
rna_ip_host_service_payload [6-39](#)
rna_ip_host_service_subtype [6-42](#)
rna_ip_host_service_vulns [6-43](#)
rna_ip_host_third_party_vuln [6-45, 6-46](#)
rna_ip_host_third_party_vuln_bugtraq_id [6-47](#)
rna_ip_host_third_party_vuln_cve_id [6-49](#)
rna_ip_host_third_party_vuln_rna_id [6-51](#)
rna_ip_host_user_history [6-58](#)
rna_mac_ip_map [6-21, 6-24, 6-25](#)
rna_vuln [6-53, 6-54](#)
rule_message [4-8, 4-9](#)

S

sru_import_log [3-10](#)

T

tag_info [6-55](#)

U

url_categories [6-56](#)

url_category_stats [5-18](#)

url_reputation_stats [5-20](#)

url_reputations [6-57](#)

user_discovery_event [8-3](#)

user_ids_stats [5-21](#)

user_stats [5-22](#)

W

white_list_event [9-7](#)

white_list_violation [9-9](#)

ㅂ

비밀번호

강도 검사 옵션 [2-3](#)

강제 재설정 [2-3](#)

비밀번호 옵션 [2-2](#)

실패한 로그인 [2-3](#)

ㅅ

사용자 어카운트 비밀번호 옵션 [2-2](#)

실패한 로그인 [2-3](#)