

vRealize Log Insight 사용

2017년 9월 8일

vRealize Log Insight 4.5



vmware®

VMware 웹 사이트 (<https://docs.vmware.com/kr/>) 에서 최신 기술 문서를 확인할 수 있습니다.
이 문서에 대한 의견이 있으면 docfeedback@vmware.com으로 사용자 의견을 보내주십시오.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2018 VMware, Inc. 판권 소유. [저작권 및 상표 정보](#).

목차

vRealize Log Insight 사용 정보 5

1 vRealize Log Insight 기능 사용 6

vRealize Log Insight 웹 사용자 인터페이스 개요 8

로그 이벤트 검색 및 필터링 9

이벤트 유형 그룹화 9

로그 이벤트의 정보 10

시간 범위 기준으로 로그 이벤트 필터링 11

전체 키워드가 포함된 로그 이벤트 검색 11

필드 연산 기준으로 로그 이벤트 검색 12

이벤트 전, 후 또는 그쯤에 발생한 이벤트 검색 13

컨텍스트에서 이벤트 보기 14

이벤트 추세 분석 14

모든 필터링 규칙 지우기 15

검색 쿼리의 예 15

정규식의 예 17

대화형 분석 차트를 사용하여 로그 분석 20

차트 유형 20

다중 함수 차트 20

집계 함수 20

차트 사용 21

대화형 분석 차트 유형 변경 22

동적 필드 추출 23

한 번 클릭 추출을 사용하여 필드 추출 23

추출된 필드 수정 24

추출된 필드 복제 25

추출된 필드 삭제 26

검색 쿼리 관리 27

vRealize Log Insight 에서 쿼리 저장 27

vRealize Log Insight 에서 쿼리 이름 바꾸기 27

vRealize Log Insight 에서 쿼리 로드 28

vRealize Log Insight 에서 쿼리 삭제 28

현재 쿼리 공유 29

현재 쿼리 내보내기 29

쿼리 스냅샷 작성 30

대시보드 사용 30

대시보드 관리 32

대시보드에 쿼리 목록 위젯 추가 33

대시보드의 쿼리 목록 위젯에 쿼리 추가	34
대시보드에 필드 테이블 위젯 추가	34
대시보드에 이벤트 유형 위젯 추가	35
대시보드에 이벤트 추세 위젯 추가	35
차트의 필드 값을 사용하는 필터	36
컨텐츠 팩 사용	36
컨텐츠 팩 마켓플레이스의 컨텐츠 팩 설치	37
컨텐츠 팩 마켓플레이스에서 설치한 컨텐츠 팩 업데이트	38
컨텐츠 팩 가져오기	38
컨텐츠 팩 내보내기	40
컨텐츠 팩 요소에 대한 세부 정보 보기	41
컨텐츠 팩 제거	41
컨텐츠 팩 생성	42
컨텐츠 팩 용어	42
쿼리	44
대시보드 모범 사례	49
컨텐츠 팩 가져오기 오류	51
컨텐츠 팩 게시에 대한 요구 사항	52
컨텐츠 팩 제출	53
vRealize Log Insight 의 경고 쿼리	54
이메일 알림을 보내도록 경고 쿼리 추가	56
Webhook을 사용하여 타사 제품에 경고 보내기 정보	57
경고 쿼리 보기	61
경고 쿼리 수정	62
경고 쿼리 사용	64
경고 쿼리 삭제	66

vRealize Log Insight 사용 정보

vRealize Log Insight 사용 항목에서는 로그 메시지 필터링과 검색, 분석 수행과 검색 결과 시각화, 경고 쿼리 작업 및 사용자 지정된 쿼리를 기반으로 로그 메시지에서 동적으로 필드를 추출하는 방법에 대한 절차를 포함하여 웹 사용자 인터페이스 사용에 대한 정보를 제공합니다.

vRealize Log Insight 기능 사용

vRealize Log Insight는 거의 실시간 검색 및 분석 기능과 함께 모든 버전의 vSphere를 포함하여 vCloud Suite의 확장 가능한 로그 집계 및 인덱싱 기능을 제공합니다.

vRealize Log Insight는 로그 수집, 가져오기 및 분석을 거쳐 시스템, 서비스 및 애플리케이션 관련 문제에 대한 실시간 답변을 제공하고, 중요하고 의미 있는 정보를 도출합니다.

고성능 수집

vRealize Log Insight에서는 모든 유형의 로그 생성 또는 시스템 생성 데이터를 처리할 수 있습니다. 높은 처리율 및 낮은 대기 시간을 지원하고 syslog 및 수집 API를 통한 데이터를 허용합니다.

확장성

vRealize Log Insight은 여러 가상 장치 인스턴스를 사용하여 수평 확장될 수 있습니다. 이를 통해 수집 처리량의 선형 확장이 가능하며 쿼리 성능이 향상되고 수집 고가용성이 실현됩니다. 클러스터 모드에서 vRealize Log Insight은 마스터 및 작업자 노드를 제공합니다. 마스터 노드와 작업자 노드는 데이터의 하위 집합을 담당합니다. 마스터 노드 및 쿼리 노드는 데이터의 모든 하위 집합을 쿼리하고 결과를 집계할 수 있습니다.

거의 실시간 검색

vRealize Log Insight로 수집된 데이터를 몇 초 내에 검색할 수 있습니다. 또한 기간별 데이터를 동일한 인터페이스에서 똑같이 낮은 지연 시간으로 검색할 수 있습니다.

vRealize Log Insight는 완벽한 키워드 쿼리를 지원합니다. 키워드는 영숫자, 하이픈 또는 밑줄 문자로 정의됩니다. 완벽한 키워드 쿼리와 더불어 vRealize Log Insight는 glob 쿼리(예: erro? 또는 vm*) 및 필드 기반 필터링(예: test*와 일치하지 않는 호스트 이름, “10.64”를 포함하는 ip)을 지원합니다. 게다가 숫자 값을 포함하는 로그 메시지 필드는 선택 필터를 정의하는 데 사용될 수 있습니다(예: CPU>80, 10<스레드 수<100 등).

검색 결과는 개별 이벤트로 제공됩니다. 각 이벤트는 단일 소스에서 제공되지만 검색 결과는 여러 소스에서 제공될 수 있습니다. vRealize Log Insight를 사용하여 시간, 요청 식별자 등 하나 이상의 차원과 데이터의 상관 관계를 지정하여 스택 전체를 논리적으로 표현할 수 있습니다. 이런 방식으로 근본 원인 분석이 더 용이해집니다.

Windows 및 Linux 에이전트

vRealize Log Insight에는 Linux 및 Windows 시스템에서 이벤트 및 파일을 수집하는 에이전트가 포함되어 있습니다.

지능형 그룹화

vRealize Log Insight는 새로운 시스템 학습 기술을 사용합니다. 지능형 그룹화 기능은 수신 비정형 데이터를 검사한 후 문제 유형별로 메시지를 그룹화하여 물리, 가상 및 하이브리드 클라우드 환경 전체에 만연할 수 있는 문제를 빠르게 파악할 수 있도록 지원합니다.

집계

로그 데이터에서 추출된 필드를 집계에 사용할 수 있습니다. 이는 Microsoft Excel의 피벗 테이블 또는 관계형 데이터베이스에서 GROUP-BY 쿼리가 제공하는 기능과 유사합니다. 차이점은 ETL(Extract, Transform, and Load)이라는 추출, 변형 및 로드 프로세스가 필요하지 않고 vRealize Log Insight는 모든 크기의 데이터로 확장된다는 점입니다.

데이터를 집계한 보기를 생성하고 여러 시스템과 애플리케이션에 액세스하지 않고도 특정 이벤트 또는 오류를 식별할 수 있습니다. 예를 들어 분당 오류 수와 같은 중요 시스템 메트릭을 표시하면서 특정 시간 범위의 이벤트로 드릴다운하여 환경에 발생한 오류를 검사할 수 있습니다.

런타임 필드 추출

원시 로그 데이터는 항상 이해하기 쉽지 않으며, 검색 및 집계에 필요한 필드를 식별하기 위해 일부 데이터를 처리해야 할 수도 있습니다. vRealize Log Insight는 이 문제를 해결하기 위해 런타임 필드 추출을 제공합니다. 정규식을 제공하여 데이터에서 필드를 동적으로 추출할 수 있습니다. 추출된 필드는 구문 분석 시점에 추출된 필드가 사용되는 방식과 마찬가지로 선택, 예상 및 집계에 사용될 수 있습니다.

대시보드

면밀히 모니터링하려는 유용한 메트릭의 대시보드를 생성할 수 있습니다. 모든 쿼리는 대시보드 위젯으로 변환되어 원하는 특정 시간에 대해 요약될 수 있습니다. 지난 5분, 지난 1시간, 지난 1일 동안의 시스템 성능을 확인할 수 있습니다. 오류를 시간별로 분류하여 표시하고 로그 이벤트의 추세를 확인할 수 있습니다.

보안 고려 사항

vRealize Log Insight의 보안 구성 요소에 대해 잘 알고 있어야 하는 IT 의사 결정권자, 설계자, 관리자 등은 vRealize Log Insight 관리의 보안 항목을 읽어야 합니다.

이러한 항목에서는 vRealize Log Insight의 보안 기능에 대한 간단한 참조를 제공합니다. 항목으로는 제품 외부 인터페이스, 포트, 인증 메커니즘을 비롯하여 보안 기능의 구성 및 관리를 위한 옵션 등이 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [vRealize Log Insight 웹 사용자 인터페이스 개요](#)
- [로그 이벤트 검색 및 필터링](#)
- [대화형 분석 차트를 사용하여 로그 분석](#)
- [동적 필드 추출](#)
- [검색 쿼리 관리](#)
- [대시보드 사용](#)
- [컨텐츠 팩 사용](#)
- [컨텐츠 팩 생성](#)
- [vRealize Log Insight의 경고 쿼리](#)

vRealize Log Insight 웹 사용자 인터페이스 개요

액세스할 수 있는 기능은 vRealize Log Insight 웹 사용자 인터페이스에 로그인하는 데 사용하는 사용자 계정에 따라 다릅니다.

대시보드 탭

대시보드 탭에는 사용자 지정 대시보드 및 컨텐츠 팩 대시보드가 포함되어 있습니다. **대시보드** 탭에서 사용자 환경의 로그 이벤트 그래프를 보거나, 위젯의 사용자 지정 집합을 생성하여 가장 중요한 정보에 액세스할 수 있습니다.

대화형 분석 탭

대화형 분석 탭에서 로그 이벤트를 검색 및 필터링하고, 로그 이벤트의 타임스탬프, 텍스트, 소스 및 필드를 기준으로 이벤트를 추출하기 위한 쿼리를 생성할 수 있습니다. vRealize Log Insight는 쿼리 결과 차트를 표시합니다. **대시보드** 탭에서 나중에 조회할 수 있도록 해당 차트를 저장할 수 있습니다.

컨텐츠 팩

컨텐츠 팩에는 대시보드, 추출된 필드, 저장된 쿼리 및 특정 제품이나 로그 집합과 관련된 경고가 포함되어 있습니다. vRealize Log Insight 웹 사용자 인터페이스의 오른쪽 상단에 있는 드롭다운 메뉴에서 컨텐츠 팩을 액세스합니다.

컨텐츠 팩은 vRealize Log Insight 사용자가 가져오거나 생성할 수 있습니다. [컨텐츠 팩 사용](#)를 참조하십시오.

관리자 인터페이스

vRealize Log Insight 관리자는 사용자 계정을 관리하고, 스토리지 위치 및 아카이브를 구성하고, 이메일 알림에 대한 보내는 SMTP 서버를 구성하고, 다른 여러 매개 변수를 변경할 수 있습니다. 관리 UI의 URL 형식은 `https://log_insight-host/admin/`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

로그 이벤트 검색 및 필터링

대화형 분석 탭에서 로그 이벤트를 검색하고 필터링할 수 있습니다.

검색 텍스트 상자에 전체 키워드, glob 또는 구를 입력하고 **검색**을 클릭하여 지정된 키워드가 포함된 이벤트만 찾을 수 있습니다.

웹 사용자 인터페이스의 **대시보드** 또는 **대화형 분석** 페이지에서 시간 범위를 지정할 수 있습니다. 필터링 시 시간 범위가 포함됩니다.

구체적 필드의 특정 값과 일치하는 로그 이벤트를 검색할 수 있습니다. 기본 검색 필드에서 따옴표 붙은 텍스트를 사용하면 정확한 구와 일치됩니다. 기본 검색 필드에서 공백 입력은 논리적 AND 연산자입니다. 검색은 전체 토큰만 사용합니다. "err"를 검색하면 "error"를 일치 항목으로 찾지 못합니다.

드롭다운 메뉴 및 로그 이벤트 목록 위의 텍스트 상자를 사용하여 필드 검색 조건 또는 필터를 지정할 수 있습니다.

단일 행 필터 내에서 쉼표로 구분된 값을 사용하여 OR 필터를 나열할 수 있습니다. 예를 들어, **hostname contains**를 선택하고 **127.0.0.1**, **127.0.0.2**를 입력합니다. 검색에서 호스트 이름이 127.0.0.1 또는 127.0.0.2인 이벤트를 반환합니다.

참고 **text contains** 필터는 쉼표로 구분된 각 값을 완전한 키워드로 처리합니다.

from 또는 in 같은 내부 쿼리 언어 구문 이름을 사용하는 필드가 포함된 쿼리는 처리될 수 없으므로 사용하지 않아야 합니다.

각 필드에 대한 새 필터 행을 생성하여 여러 필드 필터를 결합할 수 있습니다. 여러 행 필터에 적용되는 연산자를 토글할 수 있습니다.

- AND 연산자를 적용하려면 **all**을 선택합니다.
- OR 연산자를 적용하려면 **any**를 선택합니다.

참고 토글 값에 관계없이, 단일 필터 행 내에서 쉼표로 구분된 값에 대한 연산자는 항상 OR입니다.

검색어에서 glob를 사용할 수 있습니다. 예: vm* or vmw?re.

- 0개 이상의 문자에는 *를 사용합니다.
- 하나의 문자에는 ?를 사용합니다.

참고 Glob는 검색어의 첫 번째 문자로 사용할 수 없습니다. 예를 들어, 192.168.0.*를 사용할 수 있지만, 필터링 쿼리에서 *.168.0.0을 사용할 수는 없습니다.

이벤트 유형 그룹화

Log Insight는 시스템 학습을 사용하여 유사한 이벤트를 함께 그룹화합니다. 이벤트 유형 그룹화를 통해 문제 해결과 근본 원인 분석을 훨씬 더 쉽게 할 수 있습니다.

Log Insight에서 쿼리를 실행하는 경우 결과 수는 쿼리 및 시간 범위에 따라 다릅니다. 종종 쿼리가 수많은 결과를 반환합니다. 시스템 학습은 Log Insight로 오는 이벤트에서 패턴을 동적으로 배우고 조정합니다.

이벤트 유형 탭은 대화형 분석 페이지에서 검색 창 아래에 있습니다. **이벤트 유형** 탭을 클릭하면 함께 그룹화된 유사한 이벤트 목록이 표시됩니다.

시스템 학습은 이벤트를 분석하고 유사한 로그 메시지가 포함하고 있는 필드 유형을 검색합니다. 예를 들어, 타임스탬프, 문자열, 정수, 16진수 등의 유형이 있을 수 있습니다. 검색된 유형은 **이벤트 유형** 목록 내에서 하이퍼링크로 나타납니다.

시스템 학습에서 검색하는 각 유형은 스마트 필드라는 새로운 필드 유형을 나타냅니다. 스마트 필드의 기본 이름은 스마트 필드 - 유형 번호 [event_type] 형식을 따릅니다. 스마트 필드의 기본 이름을 변경할 수 있습니다. 스마트 필드 이름을 지정한 후 다른 필드와 같이 필드 섹션에 이 이름이 나타납니다. 스마트 필드 이름을 바꾸거나 이 필드를 삭제할 수 있지만 정의는 수정할 수 없습니다.

시스템 학습에서는 event_type이라는 새로운 정적 필드를 도입합니다. event_type을 필터로 사용하여 쿼리에서 특정 이벤트 유형을 포함 또는 제외할 수 있습니다.

로그 이벤트의 정보

vRealize Log Insight는 애플리케이션 로그, 네트워크 추적, 구성 파일, 메시지, 성능 데이터, 시스템 상태 덤프 등 시스템에서 생성된 모든 유형의 로그 데이터를 수집하고 분석합니다.

vRealize Log Insight를 운영 체제, 애플리케이션, 스토리지, 방화벽, 네트워크 디바이스 등 환경 내의 모든 대상에 연결하여 로그 분석을 통해 전사적인 통찰력을 갖출 수 있습니다.

vRealize Log Insight가 구성되어 로그를 수집할 준비가 되었으면 다음을 포함한 몇 가지 방법으로 로그 데이터를 수집할 수 있습니다.

- vSphere 통합 - vRealize Log Insight를 vSphere와 통합하여 vCenter 서버의 이벤트와 ESXi 호스트의 로그를 자동으로 수집할 수 있습니다.
- vRealize Operations Manager 통합 - vRealize Log Insight를 vRealize Operations Manager와 통합하여 vRealize Operations Manager에서 알람 이벤트를 보내고 관리자에게 e-메일을 보내도록 다양한 경고를 사용하도록 설정할 수 있습니다.
- 에이전트 - vRealize Log Insight에는 Linux 또는 Windows에서 파일 및 이벤트 로그를 vRealize Log Insight로 보낼 수 있는 수집 에이전트가 포함되어 있습니다.
- Syslog - vRealize Log Insight는 syslog를 통해 모든 소스의 데이터를 수집할 수 있습니다. vRealize Log Insight 서버를 syslog 대상으로 설정하기만 하면 됩니다.
- CFAPI - cfapi를 사용하여 이벤트를 원래 형식으로 vRealize Log Insight에 보낼 수 있습니다. cfapi를 통해 보낸 이벤트는 syslog 이벤트에 대한 지침을 따를 필요가 없으며 syslog RFC를 준수하기 위해 수정되지 않습니다.

각 이벤트에는 다음 정보가 포함되어 있습니다.

유형	설명
타임 스탬프	이벤트가 발생한 시간
소스	이벤트가 발생한 위치입니다. ESXi 호스트와 같은 syslog 메시지의 송신자 또는 syslog 집계와 같은 전달자일 수 있습니다.
텍스트	이벤트의 원시 텍스트입니다.
필드	이벤트에서 추출된 이름-값 쌍입니다. 에이전트가 CFAPI 프로토콜을 사용하는 경우에만 필드가 정적 필드로 서버에 전송됩니다.

참고 vRealize Log Insight는 다른 VMware 제품의 로그 메시지 콘텐츠를 담당하지 않습니다. 로그 콘텐츠에 대한 질문이 있는 경우 로그 메시지를 생성한 제품 팀에 문의하십시오.

시간 범위 기준으로 로그 이벤트 필터링

로그 이벤트를 필터링하여 특정 기간 동안의 이벤트만 볼 수 있습니다.

웹 사용자 인터페이스의 **대시보드** 또는 **대화형 분석** 페이지에서 시간 범위를 지정할 수 있습니다. 필터링 시 시간 범위가 포함됩니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 **검색** 버튼 왼쪽의 드롭다운 메뉴에서 사전 정의된 기간 중 하나를 선택합니다.
- 2 (선택 사항) 시간 범위의 시작 지점과 끝 지점을 설정하려면 **사용자 지정 시간 범위**를 선택합니다.

전체 키워드가 포함된 로그 이벤트 검색

전체 키워드가 포함된 로그 이벤트를 검색할 수 있습니다. 키워드에는 영숫자, 하이픈 및 밑줄 문자가 포함됩니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 **대화형 분석** 탭으로 이동합니다.
- 2 검색 텍스트 상자에 로그 이벤트에서 검색하려는 전체 키워드를 입력하고 **검색** 버튼을 클릭합니다.

지정된 전체 키워드가 포함된 로그 이벤트가 목록에 나타납니다.

검색한 문자열이 노란색으로 강조 표시됩니다.

후속 작업

현재 쿼리를 저장해 두었다가 이후 단계에서 해당 쿼리를 로드할 수 있습니다.

필드 연산 기준으로 로그 이벤트 검색

기존 필드 목록을 사용하여 필드에 대한 특정 값으로 로그 이벤트를 검색할 수 있습니다.

중요 vRealize Log Insight가 전체, 영숫자, 하이픈 및 밑줄 문자를 인덱싱합니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭으로 이동합니다.
- 2 필터 추가를 클릭합니다.
- 3 검색 텍스트 상자 아래의 필터 행에서 첫 번째 드롭다운 메뉴를 사용하여 vRealize Log Insight 내에서 정의된 필드를 선택합니다.

예: **hostname**.

목록에는 콘텐츠 팩 및 사용자 지정 콘텐츠에서 통계적으로 사용 가능한 정의된 필드 모두가 포함되어 있습니다. **text** 필드를 제외하고 필드는 이름별로 정렬됩니다. **text**는 메시지 텍스트를 나타내는 특수 필드이므로, **text**가 목록 상단에 나타나고 기본적으로 선택되어 있습니다.

참고 숫자 필드에는 문자열 필드가 포함하지 않는 추가 연산자(=, >, <, >=, <=)가 포함되어 있습니다. 이러한 연산자는 숫자 비교를 수행하며 해당 연산자를 사용하면 문자열 연산자를 사용하는 것과 다른 결과가 제공됩니다. 예를 들어, 필터 **response_time = 02**는 값이 2인 **response_time** 필드를 포함하는 이벤트와 일치합니다. 필터 **response_time contains 02**는 같은 일치 항목이 없습니다.

- 4 검색 텍스트 상자 아래의 필터 행에서 두 번째 드롭다운 메뉴를 사용하여 첫 번째 드롭다운 메뉴에서 선택된 필드에 적용할 연산을 선택합니다.

예를 들어, **contains**를 선택합니다. **contains** 필터는 전체 토큰과 일치합니다. "err"를 검색하면 "error"를 일치 항목으로 찾지 못합니다.

- 5 필터 드롭다운 메뉴 오른쪽의 텍스트 상자에서 필터로 사용할 값을 입력합니다.
 쉼표로 구분된 여러 값을 나열할 수 있습니다. 이러한 값 사이 연산자는 OR입니다.

참고 두 번째 드롭다운 메뉴에서 **exists** 연산자를 선택하는 경우 텍스트 상자를 사용할 수 없습니다.

- 6 (선택 사항) 필터를 더 추가하려면 **필터 추가**를 클릭합니다.
 필터 행 위에 토글 버튼이 나타납니다.
- 7 (선택 사항) 여러 필터 행의 경우 필터 간 연산자를 선택합니다.

옵션	설명
모두	필터 행 간에 AND 연산을 적용하려면 선택
임의	필터 행 간에 OR 연산을 적용하려면 선택

기본적으로, **all**이 선택되어 있습니다.

- 8 **검색** 버튼을 클릭합니다.

예: 이름에 공통 문자열이 있는 호스트 그룹 검색

한 호스트 이름은 w1-stvc-205-prod3이고 다른 호스트 이름은 w1-stvc-206-prod5인 여러 호스트가 있다고 가정합니다.

두 호스트에 대한 모든 로그를 찾으려면 다음 쿼리를 생성하십시오.

1. 검색 텍스트 상자를 비워 둡니다.
2. 필터를 정의합니다.
 - a 필드 드롭다운 메뉴에서 **hostname**을 선택합니다.
 - b 연산자 드롭다운 메뉴에서 **starts with**를 선택합니다.
 - c 값 텍스트 상자에 **w1-stvc**를 입력합니다.

contains 연산자를 사용할 수도 있지만, 이 경우 검색 값에 glob를 사용해야 합니다. 이 예에서 값 텍스트 상자에 **w1-stvc-***를 입력해야 합니다.

- 3 **검색** 버튼을 클릭합니다.

후속 작업

현재 쿼리를 저장해 두었다가 이후 단계에서 해당 쿼리를 로드할 수 있습니다.

이벤트 전, 후 또는 그쯤에 발생한 이벤트 검색


목록에서 이벤트 전, 후 또는 그쯤에 발생한 이벤트에 대한 로그 이벤트 목록을 검색할 수 있습니다.

이벤트 전후 환경 상태에 대해 자세히 알아보려면 주변 이벤트를 확인할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 **대화형 분석** 탭의 목록에서 이벤트를 찾습니다.
- 2 이벤트 행 왼쪽에서  을 클릭하고 **이 이벤트에서 시간 범위 설정**을 선택합니다.
- 3 이벤트에서 시간 범위 설정 대화상자에서 드롭다운 메뉴를 사용하여 시간 범위의 기간과 방향을 선택합니다.
1초에서 10분까지 사전 정의된 기간 목록에서 선택할 수 있습니다.
- 4 **범위 설정**을 클릭합니다.

선택된 이벤트 주변의 이벤트가 목록에 나타납니다.

참고 이 작업은 이전에 지정한 모든 검색 매개 변수 및 필터를 지웁니다.

컨텍스트에서 이벤트 보기



로그 이벤트의 컨텍스트를 보고 이전 및 이후에 도착한 로그 이벤트를 찾아볼 수 있습니다.

이벤트 전후 환경 상태에 대해 자세히 알아보려면 주변 이벤트를 확인할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 **대화형 분석** 탭의 목록에서 이벤트를 찾습니다.
- 2 이벤트 행 왼쪽에서  을 클릭하고 **컨텍스트에서 이벤트 보기**를 선택합니다.
- 3 (선택 사항) 더 많은 이벤트를 로드하도록 창의 가장자리까지 위로 또는 아래로 스크롤합니다.
- 4 (선택 사항) 자주색 타임 스탬프를 클릭하여 강조 표시된 메시지로 다시 스크롤합니다.
- 5 (선택 사항) 필터를 추가하려면 맨 위의 **필터 추가**를 클릭하거나 강조 표시된 이벤트 내부의 필드를 클릭합니다.
- 6 (선택 사항) 이벤트를 가리키고  을 클릭하여 특정 이벤트 유형을 추가하거나 제거합니다.

이벤트 추세 분석

로그 이벤트의 추세 및 이상 징후를 분석할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭으로 이동합니다.
- 2 검색 텍스트 상자를 사용하고 필터를 적용하여 쿼리를 작성 및 실행합니다.
- 3 이벤트에서 시간 범위 설정 대화상자에서 드롭다운 메뉴를 사용하여 시간 범위의 기간과 방향을 선택합니다.
- 4 이벤트 추세 탭을 클릭합니다.

vRealize Log Insight는 바로 직전의 동일 기간 쿼리와 사용자 쿼리를 비교하여 결과를 표시합니다.

모든 필터링 규칙 지우기

필터링 및 검색 결과를 지워 모든 로그 이벤트 목록을 볼 수 있습니다.

이벤트 목록에서 검색을 수행한 후에는 모든 쿼리를 지울 때까지 검색 결과가 화면에 계속 표시됩니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭에서 모든 필터를 제거합니다.
- 2 텍스트가 검색 텍스트 상자에 나타나는 경우 이 텍스트를 삭제합니다.
- 3 검색 버튼을 클릭합니다.

검색 쿼리의 예

vRealize Log Insight의 대화형 분석 탭에서 쿼리를 작성할 때 다음 예를 사용할 수 있습니다.

예: 어제 오전 9-10시 사이 ESX/ESXi hostd 프로세스에서 보고한 모든 하트비트 이벤트에 대한 쿼리

중요 vRealize Log Insight가 전체, 영숫자, 하이픈 및 밑줄 문자를 인덱싱합니다.

ESX/ESXi hostd 프로세스에서 보고한 모든 하트비트 이벤트에 대해 쿼리하려면:

- 1 검색 텍스트 상자에 `heart beat*`를 입력합니다.

- 2 필터를 정의합니다.
 - a 첫 번째 드롭다운 메뉴에서 **appname**을 선택합니다.
 - b 두 번째 드롭다운 메뉴에서 **contains**를 선택합니다.
 - c 값 텍스트 상자에 **hostd**를 입력합니다.
- 3 시간 범위를 저장합니다.
 - a **시간 범위** 드롭다운 메뉴에서 **사용자 지정**을 선택합니다.
 - b 첫 번째 텍스트 상자에서 어제 날짜와 오전 9시를 입력합니다.
 - c 두 번째 텍스트 상자에서 어제 날짜와 오전 10시를 입력합니다.
- 4 **검색** 버튼을 클릭합니다.

예: 이름에 공통 문자열이 있는 호스트 그룹 검색

한 호스트 이름은 w1-stvc-205-prod3이고 다른 호스트 이름은 w1-stvc-206-prod5인 여러 호스트가 있다고 가정합니다.

두 호스트에 대한 모든 로그를 찾으려면 다음 쿼리를 생성하십시오.

- 1 1. 검색 텍스트 상자를 비워 둡니다.
- 2 필터를 정의합니다.
 - a 필드 드롭다운 메뉴에서 **hostname**을 선택합니다.
 - b 연산자 드롭다운 메뉴에서 **starts with**를 선택합니다.
 - c 값 텍스트 상자에 **w1-stvc**를 입력합니다.

contains 연산자를 사용할 수도 있지만, 이 경우 검색 값에 glob를 사용해야 합니다. 이 예에서 값 텍스트 상자에 **w1-stvc-***를 입력해야 합니다.
- 3 **검색** 버튼을 클릭합니다.

예: vCenter Server 작업, 이벤트 및 정보에서 보고한 모든 오류에 대한 쿼리

vCenter Server 작업, 이벤트 및 정보에서 보고한 모든 오류를 쿼리하려면:

- 1 검색 텍스트 상자에 **error**를 입력합니다.
- 2 필터를 정의합니다.
 - a 첫 번째 드롭다운 메뉴에서 **vc_event_type**을 선택합니다.
 - b 두 번째 드롭다운 메뉴에서 **exists** 연산자를 선택합니다.
- 3 **검색** 버튼을 클릭합니다.

예: ESX/ESXi의 보고에 따라 1분 이상 SCSI 대기 시간에 대한 쿼리

ESX/ESXi의 보고에 따라 1분 이상 SCSI 대기 시간에 대해 쿼리하려면:

- 1 검색 텍스트 상자에 **scsi latency "performance has"**를 입력합니다.

2 필터를 정의합니다.

- a 첫 번째 드롭다운 메뉴에서 **vmw_vob_component**를 선택합니다.
- b 두 번째 드롭다운 메뉴에서 **contains** 연산자를 선택합니다.
- c 텍스트 상자에 **scsiCorrelator**를 입력합니다.

3 두 번째 필터를 정의합니다.

- a 첫 번째 드롭다운 메뉴에서 **vmw_latency_in_micros**를 선택합니다.
- b 두 번째 드롭다운 메뉴에서 **>** 연산자를 선택합니다.
- c 텍스트 상자에 **1000000**을 입력합니다.

4 검색 버튼을 클릭합니다.

정규식의 예

필드 값에 대한 정규식을 텍스트 상자에 입력하여 로그 이벤트에서 필드를 추출할 수 있습니다.

입력하는 식은 Java 정규식 구문을 사용해야 합니다.

표 1-1. 문자 연산자

정규식	설명
\	특수 문자 이스케이프
\b	단어 경계
\B	단어 경계 아님
\d	숫자 하나
\D	숫자 이외 하나
\n	줄 바꿈
\r	줄 바꿈 기호
\s	공백 하나
\S	공백을 제외한 모든 문자
\t	탭
\w	영숫자 또는 밑줄 문자 하나
\W	영숫자 또는 밑줄 이외 문자 하나

예를 들어, 문자열 1234-5678이 있고 다음 정규식을 적용하는 경우

정규식	결과
\d	1
\d+	1234
\w+	1234
\S	1234-5678

표 1-2. 수량사 연산자

정규식	설명
.	줄 바꿈을 제외한 모든 문자
*	0개 이상의 문자, 최대한 길게
?	0개 이상의 문자 또는 최대한 짧게
+	하나 이상
{<n>}	정확히 <n>번
{<n>,<m>}	<n> ~ <m>번

예를 들어, 문자열 aaaaa가 있고 다음 정규식을 적용하는 경우

정규식	결과
.	a
*	aaaaa
.*?	aaaaa
.{1}	a
.{1,2}	aa

표 1-3. 조합 연산자

정규식	설명
.	모두
.*?	모두, 앞에 최대한 짧게

예를 들어, 문자열 a b 3 hi d hi가 있고 다음 정규식을 적용하는 경우

정규식	결과
a.* hi	b 3 hi d
a .*? hi	b 3

표 1-4. 논리 연산자

정규식	설명
^	줄의 시작 또는 대괄호에 있지 않음
\$	줄의 끝
()	캡슐화
[]	대괄호의 문자 하나
	OR
-	범위
\A	문자열 시작
\Z	문자열 끝

예를 들어, 다음 정규식을 적용하는 경우

정규식	결과
(hello)?	hello를 포함하거나 hello를 포함하지 않음
(a b c)	a 또는 b 또는 c
[a-cp]	a 또는 b 또는 c 또는 p
world\$	world로 끝나고 뒤에 아무 것도 없음

표 1-5. Lookahead 연산자

정규식	설명
?=	양의 lookahead(포함)
?!=	음의 lookahead(포함 안 됨)

예를 들어, 다음 정규식을 적용하는 경우

정규식	결과
is (?=\w+)\w{2} primary	is FT primary? false
opid=(?!WFU-1fecf8f9)\S+	WFU-3c9bb994

표 1-6. 정규식의 추가적인 예

정규식	설명
[xyz]	x, y 또는 z
(info warn error)	info, warn 또는 error
[a-z]	소문자
[^a-z]	소문자 아님
[a-z] +	소문자 하나 이상
[a-z]*	소문자 0개 이상
[a-z]?	소문자 0개 또는 1개
[a-z] {3}	정확히 3개의 소문자
[\d]	숫자 하나
\d+\$	하나 이상의 숫자 다음에 메시지 끝이 나옴
[0-5]	0에서 5까지의 숫자
\w	단어 문자(문자, 숫자 또는 밑줄)
\s	공백
\S	공백을 제외한 모든 문자
[a-zA-Z0-9] +	하나 이상의 영숫자 문자
([a-z] {2,} [0-9] {3,5})	2개 이상의 문자 다음에 3-5개의 숫자가 나옴

대화형 분석 차트를 사용하여 로그 분석

대화형 분석 페이지 상단의 차트를 통해 쿼리 결과에 대한 시각적 분석을 수행할 수 있습니다.

차트는 로그 검색 쿼리의 그래픽 스냅샷을 나타냅니다. 차트 아래의 드롭다운 메뉴를 사용하여 차트 유형을 변경할 수 있습니다.

왼쪽의 첫 번째 드롭다운 메뉴를 사용하여 차트의 집계 수준을 제어할 수 있습니다. **Count** 함수가 기본적으로 선택되어 있습니다.

차트 유형

여러 차트 유형을 선택하여 대화형 분석 페이지에서 데이터가 시각화되는 방식을 변경할 수 있습니다.

다양한 차트 유형을 사용하려면 다양한 집계 함수, 시계열 사용 및 그룹화 기준 필드가 필요합니다. 차트 표시는 2,000개의 가장 최근 결과로 제한됩니다.

차트 유형	집계 함수	시계열 요구 사항	그룹화 기준 필드 요구 사항
열	임의	시계열	해당 없음
행	임의	시계열	해당 없음
영역	임의	시계열	해당 없음
막대형	임의	비시계열	하나 이상의 필드
원형	개수 또는 고유한 개수	비시계열	하나 이상의 필드
거품형	임의	비시계열	두 개의 필드
게이지	개수	비시계열	해당 없음
스칼라	개수	비시계열	해당 없음
표	임의	임의	해당 없음

다중 함수 차트

다중 함수 차트를 사용하여 범위가 다른 변수를 비교할 수 있습니다.

다중 함수 차트에서는 각 시리즈에 대한 Y축 또는 X축을 할당하여 서로 다른 범주의 데이터 집합을 비교할 수 있습니다. 각 축은 차트의 오른쪽 또는 왼쪽에 배치할 수 있습니다. 함수를 전환하여 함수가 표시된 Y축을 오른쪽에서 왼쪽으로 바꿀 수 있습니다.

예를 들어 채널 및 수준으로 그룹화된 작업의 평균에 더해 채널 및 수준으로 그룹화된 이벤트 수를 차트로 만들 수 있습니다.

집계 함수

vRealize Log Insight는 여러 가지 집계 함수를 제공합니다.

유형	필드	설명
개수	이벤트만	특정 쿼리에 대한 이벤트 수 차트를 생성합니다.
고유한 개수	모든 필드	필드에 대한 고유한 값 수 차트를 생성합니다.



유형	필드	설명
최소값	숫자 필드만	필드에 대한 최소값 차트를 생성합니다.
최대값	숫자 필드만	필드에 대한 최대값 차트를 생성합니다.
평균	숫자 필드만	필드에 대한 평균 값 차트를 생성합니다.
표준 편차	숫자 필드만	필드 값에 대한 표준 편차 차트를 생성합니다.
합계	숫자 필드만	필드에 대한 값 합계 차트를 생성합니다.
편차	숫자 필드만	필드 값에 대한 편차 차트를 생성합니다.

쿼리 결과가 표시되는 보기를 수정할 수 있습니다.

보기	설명
특정 필드 값으로 쿼리 결과를 그룹화	차트 아래 두 번째 드롭다운 메뉴를 사용하여 시계열 이외의 또는 시계열과 함께 특정 필드 값으로 쿼리 결과를 그룹화합니다.
필드에 대한 이벤트 수 보기	예를 들어 호스트당 이벤트 수를 보려면 시계열 확인란을 선택 취소하고 해당 필드의 확인란을 선택합니다.
필드에 대한 누적 막대형 차트와 시간대별 그룹화 보기	시계열 확인란과 필드 확인란을 모두 선택합니다.

차트 사용

대화형 분석 탭에서 차트가 표시되는 방법을 변경하고, 사용자 지정 대시보드에 차트를 추가하고, 대시보드 차트를 관리할 수 있습니다.

작업	프로시저
차트의 시간 범위 변경	대화형 분석 탭에서 검색 버튼 왼쪽의 드롭다운 메뉴를 사용하여 차트에 표시되는 기간을 바꿉니다.
차트의 세분성 변경	대화형 분석 탭에서 오른쪽 상단의 버튼을 사용하여 차트에 나타난 각 포인트에 대한 여러 시간 범위 간에 전환합니다. 사용 가능한 범위는 쿼리에 대해 지정된 시간 범위에 따라 다릅니다.
대화형 분석 탭에서 대시보드 차트 로드	대시보드 탭에서 차트를 찾고 대화형 분석 에서 열기 아이콘  을 클릭합니다. 시간 범위는 대시보드의 현재 시간 범위로 설정되어 있습니다. 필요한 경우 시간 범위를 수정할 수 있습니다.
사용자 지정 대시보드에 차트 저장	<ol style="list-style-type: none"> 대화형 분석 탭의 왼쪽 위에서 대시보드에 추가를 클릭합니다. 또는 검색 버튼의 오른쪽에 있는 메뉴에서 대시보드에 현재 쿼리 추가를 선택합니다. 이름을 입력하고 드롭다운 메뉴에서 대상 대시보드를 선택하고 위젯 유형을 선택하고 위젯에 대한 정보를 추가한 후 추가를 클릭합니다.
사용자 지정 대시보드에 차트로 쿼리 저장	<ol style="list-style-type: none"> 검색 버튼 옆에 있는 현재 쿼리를 대시보드에 추가를 클릭합니다. 이름을 입력하고, 드롭다운 메뉴에서 대상 대시보드를 선택하고, 위젯 유형이 차트로 설정되어 있는지 확인하고, 위젯에 대한 정보를 추가하고, 추가를 클릭합니다.
사용자 지정 대시보드에 필드 테이블로 쿼리 저장	<ol style="list-style-type: none"> 검색 버튼 옆에 있는 현재 쿼리를 대시보드에 추가를 클릭합니다. 이름을 입력하고, 드롭다운 메뉴에서 대상 대시보드를 선택하고, 위젯 유형이 필드 테이블로 설정되어 있는지 확인하고, 위젯에 대한 정보를 추가하고, 추가를 클릭합니다.
사용자 지정 대시보드에서 위젯 삭제	<ol style="list-style-type: none"> 대시보드 탭에서 삭제할 위젯이 포함된 사용자 지정 대시보드를 선택합니다. 위젯의 오른쪽 맨 위에서 기타 작업 아이콘  을 클릭하고 삭제를 선택합니다. 위젯 삭제 대화상자에서 삭제를 클릭하여 확인합니다.

대화형 분석 차트 유형 변경

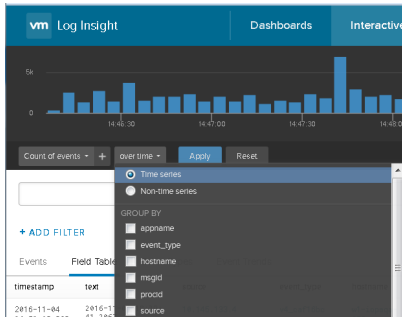
차트에 표시된 쿼리 결과의 집계와 그룹화를 변경하여 그래픽으로 로그 이벤트를 분석할 수 있습니다. 차트 아래에 표시되는 드롭다운 메뉴 수는 선택된 집계 함수에 따라 다릅니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 차트 아래의 드롭다운 메뉴를 사용하여 집계 함수와 그룹화 유형을 변경합니다.



- 시간 경과에 따른 이벤트 수를 보려면 **시계열** 버튼을 선택합니다.
- 이벤트 값만 보려면 **시계열 아님** 버튼을 선택하고 하나 이상의 필드를 선택합니다.

- 2 업데이트를 클릭합니다.

예: 대화형 분석 차트의 집계 및 그룹화

다음 테이블에는 vRealize Log Insight 차트의 집계 및 그룹화를 설명하는 예가 포함되어 있습니다.

표 1-7. 대화형 분석 차트의 집계 및 그룹화 예

첫 번째 드롭다운 메뉴에서의 선택	두 번째 드롭다운 메뉴에서의 선택	시계열 선택	화면에 표시된 텍스트	결과
개수	시계열	시계열	시간 경과에 따른 이벤트 개수	이 차트는 시간 경과에 따른 현재 쿼리에 대한 이벤트 수와 함께 막대형 차트를 표시합니다.
평균	vmw_op_latency (VMware - vSphere)	시계열	시간 경과에 따른 vmw_op_latency (VMware - vSphere)의 평균	이 차트는 시간 경과에 따른 연산 대기 시간의 평균 값과 함께 꺾은선형 차트를 표시합니다.

표 1-7. 대화형 분석 차트의 집계 및 그룹화 예 (계속)

첫 번째 드롭다운 메뉴에서의 선택	두 번째 드롭다운 메뉴에서의 선택	시계열 선택	화면에 표시된 텍스트	결과
개수	vmw_esx_problem 참고 기본적으로 vmw_esx_problem 필드는 나타나지 않습니다. vmw_esx_problem이 드롭다운 메뉴에 나타나도록 vmw_esx_problem 필드를 추출하고 쿼리를 저장해야 합니다.	비시계열	vmw_esx_problem으로 그룹화된 이벤트의 개수	이 차트는 vmw_esx_problem 필드를 포함한 이벤트 수의 막대형 차트를 표시합니다.
개수	시계열, vmw_esx_problem	시계열	시간 경과에 따라 vmw_esx_problem으로 그룹화된 이벤트의 개수	이 차트는 시간 경과에 따라 vmw_esx_problem으로 그룹화된 누적 막대형 차트를 표시합니다.

동적 필드 추출

수많은 로그 이벤트가 있는 대규모 환경에서는 사용자에게 중요한 데이터 필드를 찾을 수 없는 경우도 있습니다.

vRealize Log Insight는 이 문제를 해결하기 위해 런타임 필드 추출을 제공합니다. 정규식을 제공하여 데이터에서 동적으로 필드를 추출할 수 있습니다. [정규식의 예](#)를 참조하십시오.

참고 일반 쿼리는 매우 느릴 수 있습니다. 예를 들어, W(Wd+W) 식을 사용하여 필드를 추출하려고 시도하는 경우 쿼리가 괄호에 숫자가 포함된 모든 로그 이벤트를 반환합니다. 쿼리에 최대한 많은 텍스트 콘텐츠가 포함되어 있는지 확인하십시오. 예를 들어, Event for vmW(Wd+W)가 더 나은 필드 추출 쿼리일 것입니다.

추출된 필드를 사용하여 로그 이벤트 목록을 검색 및 필터링하거나 대화형 분석 차트의 이벤트를 집계할 수 있습니다.

한 번 클릭 추출을 사용하여 필드 추출

동적으로 필드를 추출하기 위해 컨텍스트 값을 입력하는 대신 한 번 클릭 추출 기능을 사용할 수 있습니다.

한 번 클릭 추출은 로그 이벤트에서 선택하는 필드에 해당되는 모든 콘텐츠 값을 채웁니다.

참고 한 번 클릭 추출 옵션은 이벤트 탭에서만 사용 가능합니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

1 대화형 분석 탭으로 이동합니다.

2 로그 이벤트 목록에서 추출할 필드를 나타내는 텍스트를 강조 표시합니다.

작업 메뉴가 해당 이벤트에 있는 필드 이름 집합 위에 나타납니다.

3 필드 추출을 클릭합니다.

필드 창의 전/후 컨텍스트 값은 강조 표시된 필드를 추출하는 데 필요한 컨텍스트로 자동으로 채워집니다.

4 (선택 사항) 필드 창에서 추출된 값 정규식을 수정합니다.

5 (선택 사항) 필드 창에서 전/후 컨텍스트 정규식을 수정합니다.

6 (선택 사항) **+** 다른 컨텍스트 추가를 클릭하여 키워드 및 필터를 더 추가합니다.

하나 이상의 키워드를 추가하고 단일 정적 필드를 필터로 사용할 수 있습니다.

7 관리자인 경우 드롭다운 메뉴에서 필드에 액세스할 수 있는 사용자를 선택합니다.

옵션	설명
모든 사용자	모든 사용자가 이벤트 및 필터 드롭다운 메뉴에서 필드를 볼 수 있습니다.
나만	필드를 생성한 사용자만 이벤트 및 필터 드롭다운 메뉴에서 필드를 볼 수 있습니다.

8 (선택 사항) 필드 창의 **i**를 클릭한 다음 편집을 클릭하여 이 필드에 노트를 추가합니다. 노트 편집 창에서 노트를 추가하고 확인을 클릭합니다.

9 저장을 클릭합니다.

후속 작업

추출된 필드를 사용하여 로그 이벤트 목록을 검색 및 필터링하거나 대화형 분석 차트의 이벤트를 집계할 수 있습니다.

저장된 필드 정의를 수정하거나 이러한 필드 정의가 더 이상 필요하지 않으면 삭제할 수 있습니다.

추출된 필드 수정

추출된 필드 정의를 수정할 수 있습니다.

vRealize Log Insight는 사용자가 차트, 쿼리 또는 경고를 생성할 때 사용하는 필드 복사본을 생성합니다. 필드 정의를 수정하는 경우 수정된 필드를 사용하는 모든 차트, 쿼리 및 경고가 업데이트되어 새로운 정의를 반영합니다.


일반 사용자는 자신의 콘텐츠만 수정할 수 있습니다. 관리자는 자신의 콘텐츠 및 공유 콘텐츠를 수정할 수 있습니다.

콘텐츠 팩 필드는 읽기 전용입니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭으로 이동합니다.
- 2 필드 창의 맨 위에서 **추출된 필드 관리**  를 클릭하고 목록에서 추출된 필드를 선택합니다.
- 3 값을 수정하고 **업데이트**를 클릭합니다.
대화상자에 업데이트된 필드로 인해 영향을 받게 되는 콘텐츠 목록이 표시됩니다. 해당 필드가 여러 사용자 사이에 공유되는 경우 영향을 받는 사용자 목록도 표시됩니다.
- 4 (선택 사항) 필드 창의 **i** 을 클릭한 다음 **편집**을 클릭하여 이 필드에 노트를 추가합니다. **노트 편집** 창에서 노트를 추가하고 **확인**을 클릭합니다.
- 5 **업데이트**를 클릭하여 변경 내용을 확인합니다.

vRealize Log Insight는 수정한 필드를 사용하는 모든 쿼리, 경고 및 차트를 업데이트합니다.

추출된 필드 복제

추출된 필드를 복제할 수 있습니다.


이벤트에서 두 개 이상이 필드를 추출하려는 경우 복제 옵션을 사용하면 두 필드가 유사한 컨텍스트에서 나타납니다. 필드를 추출하고 저장한 후 추출된 필드 정의를 열고 복제 옵션을 사용합니다. 복제된 필드에는 원래 추출된 필드와 동일한 정의가 있습니다. 관심이 있는 이벤트의 다른 값과 일치하도록 복제된 필드의 정의를 수정할 수 있습니다.

일반 사용자는 자신의 콘텐츠만 복제할 수 있습니다. 관리자는 자신의 콘텐츠 및 공유 콘텐츠를 수정할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭으로 이동합니다.
- 2 필드 창의 맨 위에서 **추출된 필드 관리**  를 클릭하고 목록에서 추출된 필드를 선택합니다.

- 3 **복제**를 클릭하여 필드 복사본을 생성합니다.
- 4 (선택 사항) 필드 창에서 추출된 값 정규식을 수정합니다.
- 5 (선택 사항) 필드 창에서 전/후 컨텍스트 정규식을 수정합니다.
- 6 (선택 사항) **+ 다른 컨텍스트 추가**를 클릭하여 키워드 및 필터를 더 추가합니다.
하나 이상의 키워드를 추가하고 단일 정적 필드를 필터로 사용할 수 있습니다.
- 7 관리자인 경우 드롭다운 메뉴에서 필드에 액세스할 수 있는 사용자를 선택합니다.

옵션	설명
모든 사용자	모든 사용자가 이벤트 및 필터 드롭다운 메뉴에서 필드를 볼 수 있습니다.
나만	필드를 생성한 사용자만 이벤트 및 필터 드롭다운 메뉴에서 필드를 볼 수 있습니다.

- 8 **저장**을 클릭합니다.

후속 작업


추출된 필드를 사용하여 로그 이벤트 목록을 검색 및 필터링하거나 대화형 분석 차트의 이벤트를 집계할 수 있습니다.

저장된 필드 정의를 수정하거나 이러한 필드 정의가 더 이상 필요하지 않으면 삭제할 수 있습니다.

추출된 필드 삭제

더 이상 필요하지 않은 추출된 필드를 삭제할 수 있습니다.

vRealize Log Insight는 사용자가 위젯, 쿼리 또는 경고를 생성할 때 사용하는 필드 복사본을 생성합니다. 위젯, 쿼리 또는 경고에서 사용되는 필드를 삭제하는 경우 vRealize Log Insight는 해당 필드를 사용하는 각 위젯, 쿼리 또는 경고에 대한 삭제된 필드의 임시 복사본을 생성합니다.


이름 옆에 **이 필드 편집** 아이콘 이 있는 필드만 삭제할 수 있습니다. 일반 사용자는 자신의 콘텐츠만 삭제할 수 있습니다. 관리자는 자신의 콘텐츠 및 공유 콘텐츠를 삭제할 수 있습니다.

콘텐츠 팩 필드는 읽기 전용입니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 **대화형 분석** 탭으로 이동합니다.
- 2 필드 창의 맨 위에서 **추출된 필드 관리** 를 클릭하고 목록에서 추출된 필드 위로 마우스를 이동합니다.

3 을 클릭합니다.

대화상자에 삭제하려는 필드를 사용하는 콘텐츠 목록이 표시됩니다. 관리자이고 해당 필드가 여러 사용자에게 의해 공유되는 경우 영향을 받는 사용자 목록도 표시됩니다.

4 삭제를 클릭하여 확인합니다.

삭제된 필드가 기존 쿼리에서 사용되는 경우 vRealize Log Insight는 필드의 임시 복사본을 생성하고 사용자가 삭제된 필드를 사용하는 쿼리를 로드하는 경우 이 복사본을 표시합니다.

임시 필드가 포함된 콘텐츠를 내보내는 경우 vRealize Log Insight는 내보낸 콘텐츠 팩에서 필드를 생성하여 임시 필드를 방지합니다.

검색 쿼리 관리

쿼리 결과를 내보내고, 다른 사용자와 쿼리를 공유하고, 기존 쿼리를 저장, 삭제, 이름 바꾸기 및 로드할 수 있습니다. 쿼리의 스냅샷을 작성하여 대시보드에 저장할 수 있습니다.


vRealize Log Insight 에서 쿼리 저장

vRealize Log Insight에서 현재 쿼리 및 시간 범위를 저장하고 나중에 볼 수 있습니다. 저장된 쿼리는 **대화형 분석** 페이지에서만 로드할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 **대화형 분석** 탭에서 저장할 쿼리를 수행합니다.
- 2 현재 쿼리를 즐겨찾기에 추가 아이콘을 클릭합니다 .
- 3 이름을 입력하고 **저장**을 클릭합니다.

참고 저장된 쿼리는 고정된 시간 범위를 포함하며 업데이트되지 않습니다. 쿼리를 저장하면, 저장하는 순간에 시간 범위 내에서 사용할 수 있는 로그 메시지의 스냅샷이 만들어집니다.

쿼리가 즐겨찾기 쿼리 목록에 추가됩니다.

관리자를 포함한 모든 사용자에게는 저장된 쿼리의 개별 목록이 있습니다.


vRealize Log Insight 에서 쿼리 이름 바꾸기

vRealize Log Insight에서 저장된 쿼리 이름을 변경할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭으로 이동합니다.
- 2 즐겨찾기 쿼리 아이콘 ★을 클릭합니다.
- 3 이름을 바꿀 쿼리를 가리키고 저장된 쿼리 편집 아이콘  을 클릭합니다.
- 4 새로운 이름을 입력하고 저장을 클릭합니다.

vRealize Log Insight 에서 쿼리 로드

컨텐츠 팩의 쿼리 또는 저장된 쿼리를 로드하여 대화형 분석 탭에 표시할 수 있습니다.

저장된 쿼리는 대시보드 항목과 구분됩니다. 저장된 쿼리는 사용자 지정 대시보드에 나타나지 않습니다. 저장된 쿼리를 보려면 해당 쿼리를 로드해야 합니다.

관리자를 포함한 모든 사용자에게는 저장된 쿼리의 개별 목록이 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭으로 이동합니다.
- 2 즐겨찾기 쿼리 아이콘 ★을 클릭합니다.
- 3 대화형 분석 탭에서 볼 쿼리를 즐겨찾기 쿼리 목록에서 클릭합니다.

이 쿼리가 대화형 분석 탭에 로드됩니다. 쿼리의 시간 범위는 이벤트 목록 위에 표시됩니다.

후속 작업

대시보드에 쿼리를 추가하거나, 차트의 세분성을 변경하거나, 쿼리 결과에 추가 필터링을 적용할 수 있습니다.

vRealize Log Insight 에서 쿼리 삭제

vRealize Log Insight에서 저장된 쿼리를 삭제할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭으로 이동합니다.
- 2 검색 버튼 오른쪽의 드롭다운 메뉴에서 **쿼리 로드**를 선택합니다.
- 3 즐겨찾기 쿼리 아이콘 ★을 클릭합니다.
- 4 즐겨찾기 목록에서 삭제할 쿼리 옆에 있는 ✕을 클릭합니다.
- 5 삭제를 클릭하여 확인합니다.


현재 쿼리 공유

현재 쿼리의 링크를 동료에게 보낼 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭에서 공유할 쿼리를 수행합니다.
- 2  아이콘을 클릭하고 **쿼리 공유**를 선택합니다.
vRealize Log Insight에서 쿼리에 대한 단축 URL을 만들고 표시합니다. URL은 삭제되기 전 마지막 사용 후 93일 동안 유지됩니다.
- 3 URL을 복사하고 공유할 사람에게 이 URL을 보냅니다.


현재 쿼리 내보내기

로그 쿼리 결과를 내보내서 이 결과를 다른 시스템과 공유하거나 지원 담당자에게 전달할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭에서 내보낼 쿼리를 수행합니다.
- 2 그런 다음 을 클릭하고 **이벤트 결과 내보내기**를 선택합니다.

3 쿼리를 저장할 형식을 선택하고 **내보내기**를 클릭합니다.

옵션	설명
원시 이벤트	TXT 형식으로 결과를 저장하려면 선택
JSON	JSON 형식으로 결과를 저장하려면 선택
XML	XML 형식으로 결과를 저장하려면 선택

쿼리 스냅샷 작성



빠르게 보거나 대시보드에 저장하기 위해 vRealize Log Insight에서 현재 및 특정 시간 범위의 쿼리에 대해 스냅샷을 작성할 수 있습니다. 스냅샷은 [대화형 분석] 페이지에서 작성할 수 있습니다.

스냅샷에는 스냅샷을 작성할 당시의 시간 범위 내에서 사용할 수 있는 로그 메시지가 저장됩니다. 스냅샷을 작성한 후 스냅샷을 클릭하면 스냅샷을 작성한 시점의 쿼리로 되돌아갑니다. 하나 이상의 스냅샷을 저장하려는 경우 기존 대시보드에 추가하거나 새 대시보드를 생성합니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 **대화형 분석** 탭에서 스냅샷으로 저장할 쿼리를 수행합니다.
- 2 [스냅샷] 아이콘을 클릭합니다.
스냅샷이 화면의 맨 아래에 나타납니다.
- 3 (선택 사항) 쿼리를 변경하고 추가 스냅샷을 작성합니다.
모든 스냅샷이 화면의 맨 아래에 나타납니다.
- 4 (선택 사항) 화면의 맨 아래에서  을 클릭하고 **대시보드에 모두 저장**을 선택합니다.
 - a 기존 대시보드를 선택하거나 새 대시보드를 생성합니다.
 - b **추가**를 클릭합니다.
선택한 대시보드 또는 새 대시보드에 스냅샷이 추가됩니다.
- 5 (선택 사항) 스냅샷을 삭제하려면 스냅샷에서 "X"를 클릭합니다.
- 6 (선택 사항)  을 클릭하고 **모두 삭제**를 선택하여 스냅샷을 삭제합니다.

대시보드 사용

vRealize Log Insight의 대시보드는 차트, 필드, 테이블 및 쿼리 목록 위젯의 모음입니다.

사용자 지정 대시보드

사용자 지정 대시보드는 vRealize Log Insight의 현재 인스턴스 사용자가 생성합니다. 사용자 대시보드는 내 대시보드와 공유 대시보드라는 두 가지 범주로 구성되어 있습니다. 공유 대시보드는 vRealize Log Insight 인스턴스의 모든 사용자에게 표시됩니다.

내 대시보드는 사용자별로 특정합니다.

일반 사용자는 내 대시보드 섹션의 대시보드만 수정할 수 있습니다.

관리자는 내 대시보드 섹션의 대시보드 및 공유 대시보드 섹션에서 생성한 대시보드를 수정할 수 있습니다.

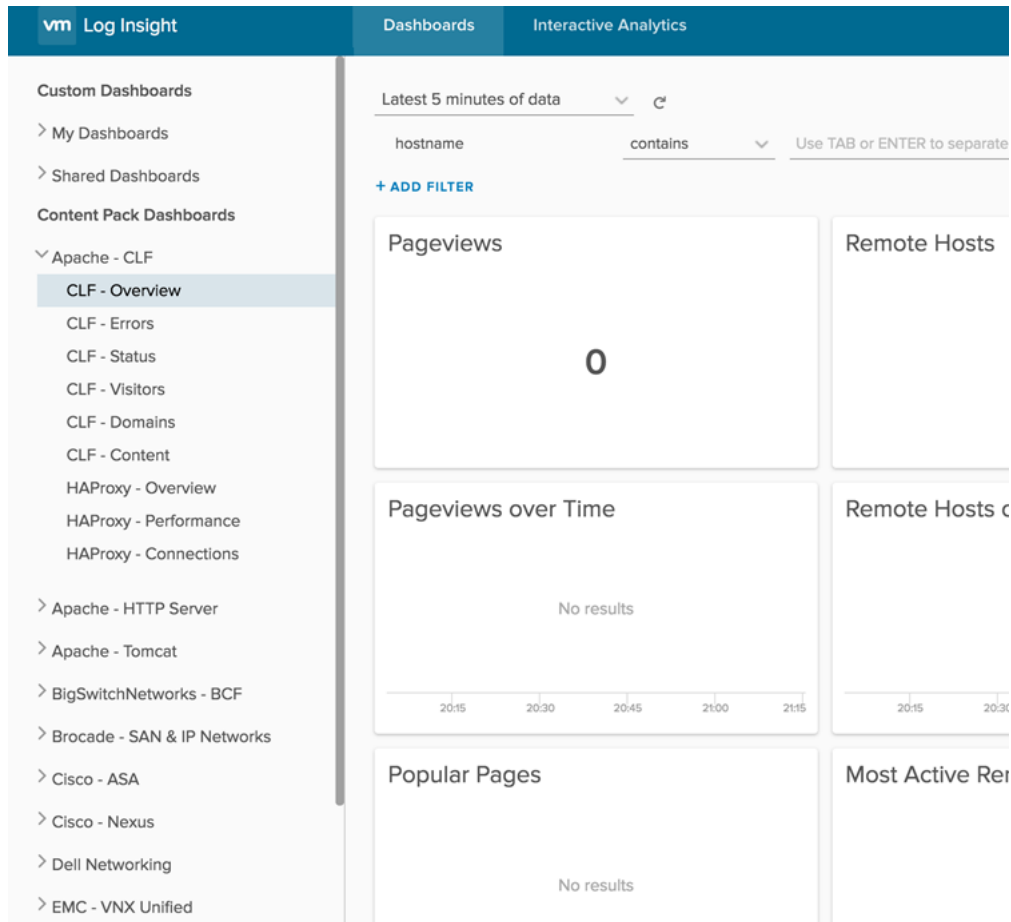
컨텐츠 팩 대시보드

컨텐츠 팩 대시보드는 컨텐츠 팩과 함께 가져오며 vRealize Log Insight 인스턴스의 모든 사용자에게 표시됩니다.

참고 컨텐츠 팩 대시보드는 읽기 전용입니다. 삭제하거나 이름을 변경할 수 없습니다. 그러나 컨텐츠 팩 대시보드를 사용자 지정 대시보드로 복제할 수 있습니다. 전체 대시보드 또는 개별 위젯을 복제할 수 있습니다.

vRealize Log Insight의 인스턴스에서 사용 가능한 대시보드를 보려면 vRealize Log Insight 사용자 인터페이스의 왼쪽 상단 모서리에 있는 **대시보드**를 클릭하십시오. 나타나는 왼쪽 창에는 사용자에게 액세스 권한이 있는 모든 대시보드가 사용자 지정 대시보드 및 컨텐츠 팩 대시보드별로 그룹화되어 표시됩니다. 각 하위 그룹 옆에 있는 >를 클릭하면 관련 대시보드가 표시됩니다. 그룹 이름 옆에 있는 >를 클릭하면 대시보드 그룹을 한 번에 하나씩 열 수 있습니다. 새 그룹을 열고 이전 그룹을 닫으려면 다른 그룹 이름 옆에 있는 >를 클릭합니다. 한 번에 하나의 그룹만 열 수 있습니다.

대시보드의 컨텐츠를 보려면 왼쪽의 목록에서 대시보드 이름을 클릭하십시오.



대시보드 관리

사용자 지정 대시보드 공간에서 대시보드를 추가, 수정 및 삭제할 수 있습니다.

컨텐츠 팩 대시보드는 수정할 수 없지만, 이러한 대시보드를 사용자 지정 대시보드 공간에 복제하고 복제본을 수정할 수 있습니다.

중요 vRealize Log Insight는 사용자가 저장하거나 복제하는 대시보드, 쿼리 및 경고의 중복 이름에 대한 검사를 수행하지 않습니다. vRealize Log Insight에서 쿼리를 저장할 때 표시 이름은 고유한 식별자가 아닙니다. 따라서 여러 차트, 경고 및 대시보드를 같은 이름으로 저장할 수 있습니다. 데이터 검색이 용이하도록 차트, 경고 또는 대시보드를 저장할 때 중복 이름을 사용하지 마십시오.

표 1-8. 사용자 지정 대시보드 사용

작업	프로시저
새로운 사용자 지정 대시보드 생성	대시보드 탭에서 내 대시보드 를 선택하고 왼쪽 하단에서 새 대시보드 를 클릭합니다.
사용자 지정 대시보드 이름 편집	대시보드 탭에서 대시보드 이름을 마우스로 가리키고 메뉴 아이콘  을 클릭한 후 이름 바꾸기 를 선택합니다. 새로운 이름을 입력하고 저장 을 클릭합니다.

표 1-8. 사용자 지정 대시보드 사용 (계속)

작업	프로시저
사용자 지정 대시보드 삭제	대시보드 탭에서 대시보드 이름을 마우스로 가리키고 메뉴 아이콘  을 클릭한 후 삭제 를 선택합니다. 확인 대화상자에서 삭제 를 선택합니다.
컨텐츠 팩에서 사용자 지정 대시보드로 대시보드 복제	<ol style="list-style-type: none"> 대시보드 탭에서 컨텐츠 팩을 선택하고 복제할 대시보드를 마우스로 가리킵니다. 메뉴 아이콘  을 클릭하고 드롭다운 메뉴에서 복제를 선택합니다. 이름을 입력하고 저장을 클릭합니다. <p>관리자인 경우 다른 사용자와 대시보드를 공유할지 여부를 선택할 수 있습니다.</p>
대시보드에 차트 위젯 추가	<ol style="list-style-type: none"> 대화형 분석 탭의 왼쪽 위에서 대시보드에 추가를 클릭합니다. 또는 검색 버튼의 오른쪽에 있는 메뉴에서 대시보드에 현재 쿼리 추가를 선택합니다. 이름을 입력하고 드롭다운 메뉴에서 대상 대시보드를 선택하고 위젯 유형을 선택하고 위젯에 대한 정보를 추가한 후 추가를 클릭합니다.
대시보드에 쿼리 목록 위젯 추가	대시보드에 쿼리 목록 위젯 추가 항목을 참조하십시오.
대시보드의 쿼리 목록 위젯에 쿼리 추가	대시보드의 쿼리 목록 위젯에 쿼리 추가 항목을 참조하십시오.
대시보드의 필드 테이블 위젯에 쿼리 추가	대시보드에 필드 테이블 위젯 추가 항목을 참조하십시오.
대시보드에 이벤트 유형 위젯 추가	대시보드에 이벤트 유형 위젯 추가
대시보드에 이벤트 추세 위젯 추가	대시보드에 이벤트 추세 위젯 추가
대시보드에서 위젯 삭제	<ol style="list-style-type: none"> 대시보드 탭에서 삭제할 위젯이 포함된 사용자 지정 대시보드를 선택합니다. 위젯의 오른쪽 맨 위에서 기타 작업 아이콘  을 클릭하고 삭제를 선택합니다. 위젯 삭제 대화상자에서 삭제를 클릭하여 확인합니다.


대시보드에 쿼리 목록 위젯 추가

쿼리 목록 위젯을 생성하여 사용자 지정 대시보드에 검색 쿼리 목록을 저장할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 대화형 분석** 탭에서 대시보드에 추가할 쿼리를 실행합니다.
- 현재 쿼리를 대시보드에 추가** 아이콘  을 클릭합니다.
- 대시보드** 드롭다운 메뉴에서 쿼리를 추가할 대시보드를 선택합니다.

- 4 **위젯 유형** 드롭다운 메뉴에서 **쿼리 목록**을 선택합니다.
- 5 **쿼리 목록** 드롭다운 메뉴에서 **새로운 쿼리 목록**을 선택하고 목록 이름을 입력하고 **저장**을 클릭합니다.
- 6 **추가**를 클릭합니다.

지정한 대시보드에 쿼리 목록 위젯이 나타납니다.

후속 작업

생성한 쿼리 목록 위젯에 쿼리를 추가할 수 있습니다. [대시보드의 쿼리 목록 위젯에 쿼리 추가](#)를 참조하십시오.

대시보드의 쿼리 목록 위젯에 쿼리 추가


쿼리 목록 위젯은 대시보드에서 하나 이상의 저장된 쿼리에 대한 빠른 액세스를 제공합니다.

사용자 지정 쿼리 목록 위젯을 수정하여 새 쿼리를 추가할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 **대화형 분석** 탭에서 쿼리 목록 위젯에 추가할 쿼리를 실행합니다.
- 2 **현재 쿼리를 대시보드에 추가** 아이콘  을 클릭합니다.
- 3 **대시보드** 드롭다운 메뉴에서 쿼리 목록 위젯이 포함된 대시보드를 선택합니다.
- 4 **위젯 유형** 드롭다운 메뉴에서 **쿼리 목록**을 선택합니다.
- 5 **쿼리 목록** 드롭다운 메뉴에서 쿼리를 추가할 위젯의 이름을 선택하고 **저장**을 클릭합니다.
- 6 **추가**를 클릭합니다.

vRealize Log Insight는 사용자가 선택한 위젯에 쿼리를 추가합니다.

참고 쿼리 목록 위젯은 메시지 쿼리를 사용합니다. 차트 위젯에서 동일한 메시지 쿼리를 사용하고 메시지에 존재하지 않는 그룹화 기준 필드를 선택하는 경우 차트에 결과가 표시되지 않습니다.


대시보드에 필드 테이블 위젯 추가

필드 테이블 위젯은 대시보드에서 하나 이상의 저장된 필드에 대한 빠른 액세스를 제공합니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭에서 필드 테이블 위젯에 추가할 쿼리를 실행합니다.
- 2 현재 쿼리를 대시보드에 추가 아이콘  을 클릭합니다.
- 3 대시보드 드롭다운 메뉴에서 필드 테이블을 추가할 대시보드를 선택합니다.
- 4 위젯 유형 드롭다운 메뉴에서 필드 테이블을 선택합니다.
- 5 필드 테이블에서 포함시킬 필드를 선택합니다.
- 6 추가를 클릭합니다.

지정한 대시보드에 필드 테이블 위젯이 나타납니다.


대시보드에 이벤트 유형 위젯 추가

이벤트 유형 위젯에서는 시스템 학습을 통해 생성되는 이벤트 유형 그룹에 액세스하여 비슷한 이벤트를 함께 그룹화할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭에서 위젯에 추가할 쿼리를 실행합니다.
- 2 현재 쿼리를 대시보드에 추가 아이콘  을 클릭합니다.
- 3 대시보드 드롭다운 메뉴에서 위젯을 추가할 대시보드를 선택합니다.
- 4 위젯 유형 드롭다운 메뉴에서 [이벤트 유형]을 선택합니다.
- 5 추가를 클릭합니다.

지정한 대시보드에 위젯이 나타납니다.

대시보드에 이벤트 추세 위젯 추가


이벤트 추세 위젯에서는 지정된 기간의 추세를 분석하는 이벤트 추세에 대한 정보에 액세스할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭에서 위젯에 추가할 쿼리를 실행합니다.

- 2 현재 쿼리를 대시보드에 추가 아이콘  을 클릭합니다.
- 3 대시보드 드롭다운 메뉴에서 위젯을 추가할 대시보드를 선택합니다.
- 4 위젯 유형 드롭다운 메뉴에서 [이벤트 추세]를 선택합니다.
- 5 추가를 클릭합니다.

지정한 대시보드에 위젯이 나타납니다.

차트의 필드 값을 사용하는 필터

차트가 포함된 대시보드, 필드를 사용하는 다른 대시보드 및 대화형 분석에서 차트의 필드 값을 필터로 사용할 수 있습니다.

차트의 필드 값에 문제가 있는 경우 빠르게 이 필드 값을 입력으로 사용하고 해당 필드를 사용하는 다른 대시보드로 이동할 수 있습니다. 다른 대시보드가 이 필드를 사용하지 않는 경우 같은 대시보드에서 필드 값을 필터로 사용하거나 대화형 분석에서 이 필드 값을 실행할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대시보드 드롭다운 메뉴에서 차트 위젯이 포함된 대시보드를 선택합니다.
- 2 차트 위젯에서 차트 데이터를 마우스로 가리키고 도구 설명으로 나타나는 필드 값을 봅니다.
- 3 필터로 사용할 필드 값을 클릭합니다.
값을 필터로 추가 메뉴가 나타납니다.
- 4 필드 값을 필터로 사용할 위치를 선택합니다.

옵션	작업
대화형 분석	대화형 분석 페이지가 열리고 차트 쿼리 결과가 표시됩니다. 3단계에서 선택한 필드 값이 필터로 사용됩니다.
이 대시보드	3단계에서 선택한 필드 값이 같은 대시보드에서 필터로 사용됩니다.
다른 대시보드	3단계에서 선택한 필드 값이 이 필드가 포함된 다른 대시보드에서 필터로 사용됩니다.

컨텐츠 팩 사용

컨텐츠 팩에는 대시보드, 추출된 필드, 저장된 쿼리 및 특정 제품이나 로그 집합과 관련된 경고가 포함되어 있습니다.

시스템에 로드된 컨텐츠 팩을 보려면 vRealize Log Insight 사용자 인터페이스의 오른쪽 상단 모서리에 있는 드롭다운 메뉴에서 **컨텐츠 팩**을 선택합니다.

컨텐츠 팩의 컨텐츠를 보려면 왼쪽의 목록에서 컨텐츠 팩을 클릭합니다.

컨텐츠 팩

컨텐츠 팩 범주에는 가져온 대시보드 집합, 추출된 필드, 쿼리 및 경고가 포함되어 있습니다. 기본적으로 일반 및 VMware - vSphere 컨텐츠 팩을 가져옵니다.

참고 컨텐츠 팩 대시보드는 읽기 전용입니다. 삭제하거나 이름을 변경할 수 없습니다. 그러나 컨텐츠 팩 대시보드를 사용자 지정 대시보드로 복제할 수 있습니다. 전체 대시보드 또는 개별 위젯을 복제할 수 있습니다.

사용자 지정 컨텐츠

사용자 지정 컨텐츠 범주에는 대시보드, 추출된 필드 및 vRealize Log Insight의 현재 인스턴스에서 생성된 쿼리가 포함되어 있습니다. 내 컨텐츠 섹션에는 현재 로그인된 사용자의 사용자 지정 컨텐츠가 포함되어 있습니다. 공유 컨텐츠 섹션에는 vRealize Log Insight의 모든 사용자 간에 공유되는 컨텐츠가 포함되어 있습니다.

관리자만이 다른 사용자와 컨텐츠를 공유할 수 있습니다. 관리자만이 공유 컨텐츠를 관리할 수 있습니다.

참고 사용자 지정 컨텐츠 섹션에서 컨텐츠를 제거할 수 없습니다. 사용자 지정 컨텐츠 섹션에서 저장된 정보를 제거하려는 경우 대시보드, 쿼리, 경고 및 필드와 같은 개별 요소를 삭제해야 합니다.

컨텐츠 팩 마켓플레이스의 컨텐츠 팩 설치

vRealize Log Insight UI에서 벗어나지 않고도 컨텐츠 팩 마켓플레이스의 컨텐츠 팩을 설치할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 **관리자 편집** 권한을 가진 사용자로 로그인했는지 확인합니다. URL 형식은 `https://log-insight-host`이며 여기서 `log-insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 오른쪽 상단의 드롭다운 메뉴에서 **컨텐츠 팩**을 선택합니다.
- 2 왼쪽의 **컨텐츠 팩 마켓플레이스**에서 **마켓플레이스**를 클릭합니다.
- 3 설치하려는 컨텐츠 팩을 클릭합니다.
- 4 라이선스 계약 조항에 동의하기 위한 확인란을 선택합니다.
- 5 **설치**를 클릭합니다.

설치가 완료되면 왼쪽의 [설치된 컨텐츠 팩] 목록에 컨텐츠 팩이 나타납니다.

컨텐츠 팩 마켓플레이스에서 설치한 컨텐츠 팩 업데이트

vRealize Log Insight에서 나가지 않고도 이전에 컨텐츠 팩 마켓플레이스에서 설치한 컨텐츠 팩을 업데이트할 수 있습니다.

참고 컨텐츠 팩의 경고가 사용되도록 설정되면 경고가 사용자의 프로파일에 복사됩니다. 사용자는 복사본의 설명 또는 조건을 수정할 수 있습니다. 4.0에서 인스턴스화된 경고 정의부터 컨텐츠 팩을 업데이트하고 경고 정의를 확장하면 향상된 컨텐츠 팩에 맞게 복사본이 업데이트되거나 제거됩니다. 사용자가 수정한 내용을 유지하려면 먼저 이를 컨텐츠 팩으로 내보내고 업데이트 후 다시 사용자 프로파일로 가져옵니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 **관리자 편집** 권한을 가진 사용자로 로그인했는지 확인합니다. URL 형식은 `https://log-insight-host`이며 여기서 `log-insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 오른쪽 상단의 드롭다운 메뉴에서 **컨텐츠 팩**을 선택합니다.
- 왼쪽에 있는 메뉴에서 **업데이트**를 선택하여 업데이트가 가능한 컨텐츠 팩 목록을 확인합니다.
 - 단일 컨텐츠 팩을 업데이트하려면 해당 아이콘을 클릭하여 정보 창을 엽니다. **업데이트**를 클릭하여 가져오기를 시작합니다. 컨텐츠 팩에 따라 가져오기가 완료된 후 추가 지침이 표시될 수 있습니다. 이러한 팝업이 나타나면 구성 단계에 따라 업그레이드를 완료합니다.
 - 보류 중인 업데이트와 함께 모든 컨텐츠 팩을 자동으로 업데이트하려면 **모두 업데이트**를 클릭합니다. 정보 팝업의 지침을 읽고 **업데이트**를 클릭하여 진행합니다. 업그레이드한 다음 각 컨텐츠 팩을 클릭하여 가져오기 후 업그레이드를 성공적으로 완료할 수 있도록 향후 구성 단계를 확인합니다. 사용자가 수정한 내용을 유지하기 위해 컨텐츠 팩을 내보낸 경우 다시 사용자 프로파일로 가져옵니다.

업데이트된 컨텐츠 팩이 왼쪽의 설치된 컨텐츠 팩 목록에 나타납니다.

컨텐츠 팩 가져오기

컨텐츠 팩을 가져와 사용자 정의 정보를 다른 vRealize Log Insight 인스턴스와 교환하거나, 이전 버전의 컨텐츠 팩을 최신 버전으로 업그레이드할 수 있습니다.

VLCP(vRealize vRealize Log Insight 컨텐츠 팩) 파일만 가져올 수 있습니다.

참고 이미 존재하는 컨텐츠 팩의 새 버전을 가져오는 경우 새 버전에 수정된 필드 정의가 포함되어 있으면 새 정의를 반영하도록 해당 수정된 필드를 사용하는 모든 쿼리, 경고 및 차트가 업데이트됩니다. 현재 컨텐츠 팩 버전에 있는 필드가 가져오는 새 버전에는 없는 경우 vRealize Log Insight가 삭제된 필드를 사용하는 각 쿼리, 차트 또는 경고의 필드에 대해 임시 복사본을 생성합니다.

필수 조건

- [컨텐츠 팩으로 설치]를 가져오기 방법으로 사용하려는 경우 **관리 편집** 권한을 사용하여 vRealize Log Insight 웹 사용자 인터페이스에 로그인되어 있는지 확인하십시오. URL 형식은 `https://log-insight-host`이며 여기서 `log-insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.
- [내 컨텐츠로 가져오기]를 사용하려는 경우 임의 권한 수준으로 vRealize Log Insight 웹 사용자 인터페이스에 로그인할 수 있습니다.

프로시저

- 1 오른쪽 상단의 드롭다운 메뉴에서 **컨텐츠 팩**을 선택합니다.
- 2 왼쪽 아래에서 **컨텐츠 팩 가져오기**를 클릭합니다.
- 3 가져오기 방법을 선택합니다.

옵션	설명
컨텐츠 팩으로 설치	vRealize Log Insight 인스턴스의 모든 사용자에게 표시되는 읽기 전용 컨텐츠 팩으로 컨텐츠를 가져옵니다. 참고 컨텐츠 팩 대시보드는 읽기 전용입니다. 삭제하거나 이름을 변경할 수 없습니다. 그러나 컨텐츠 팩 대시보드를 사용자 지정 대시보드로 복제할 수 있습니다. 전체 대시보드 또는 개별 위젯을 복제할 수 있습니다.
내 컨텐츠로 가져오기	사용자 공간에 사용자 지정 컨텐츠로 컨텐츠를 가져오며 이는 해당 사용자에게만 표시됩니다. 가져온 컨텐츠는 복제하지 않고도 편집할 수 있습니다. 참고 이름, 작성자, 아이콘 등의 컨텐츠 팩 메타데이터는 이 모드에서 표시되지 않습니다. 내 컨텐츠로 가져온 컨텐츠 팩은 팩 단위로 제거할 수 없습니다. 내 컨텐츠에서 컨텐츠 팩을 제거하려면 대시보드, 쿼리, 경고 및 필드와 같은 각 요소를 개별적으로 제거해야 합니다.

일반 사용자는 자신의 사용자 공간에만 컨텐츠 팩을 가져올 수 있습니다.

- 4 가져올 컨텐츠 팩을 지정한 다음 **열기**를 클릭합니다.
- 5 **가져오기**를 클릭합니다.

사용자 지정 컨텐츠로 가져오는 옵션을 선택한 경우 가져올 컨텐츠를 사용자가 선택할 수 있도록 대화상자가 나타납니다.

- 6 (선택 사항) 사용자 지정 컨텐츠로 가져오는 옵션을 선택한 경우 확인란을 사용하여 가져올 항목을 선택하고 **가져오기**를 다시 클릭합니다.

참고 가져온 쿼리, 차트 및 경고에 사용되는 필드도 가져와집니다.

- 7 (선택 사항) 일부 컨텐츠 팩의 경우 컨텐츠 팩을 처음 가져올 때 가져오기가 완료된 후 설정 지침 팝업이 표시됩니다. 이러한 지침에 따라 컨텐츠 팩 설정을 완료합니다.
- 8 (선택 사항) 일부 컨텐츠 팩의 경우 컨텐츠 팩을 업그레이드로 가져올 때 가져오기가 완료된 후 업그레이드 지침 팝업이 표시됩니다. 이러한 지침에 따라 컨텐츠 팩 설정을 완료합니다.

가져온 콘텐츠 팩의 사용 준비가 완료되어 왼쪽의 콘텐츠 팩 또는 사용자 지정 콘텐츠 목록에 표시됩니다.

참고 가져온 경고는 기본적으로 사용하지 않도록 설정됩니다. [경고 쿼리 사용](#) 항목을 참조하십시오.

콘텐츠 팩 내보내기


사용자 지정 대시보드, 저장된 쿼리, 경고, 추출된 필드 등을 콘텐츠 팩으로 내보내고 콘텐츠를 vRealize Log Insight 인스턴스 간에 공유하거나 커뮤니티의 vRealize Log Insight 사용자와 공유할 수 있습니다.

콘텐츠 팩은 vCenter vRealize Log Insight 콘텐츠 팩(VLCP) 파일로 저장됩니다.

내보내는 쿼리, 차트 및 경고에 사용되는 모든 필드가 내보낸 콘텐츠 팩에 포함됩니다.

임시 필드가 포함된 콘텐츠를 내보내는 경우 vRealize Log Insight는 내보내는 동안 콘텐츠 팩 내에 이들 필드를 생성합니다.

프로시저

- 오른쪽 상단의 드롭다운 메뉴에서 **콘텐츠 팩**을 선택합니다.
- 내보낼 콘텐츠 팩을 클릭하고 콘텐츠 팩 이름 옆에 있는 드롭다운 메뉴 에서 **내보내기**를 선택합니다.
- (선택 사항) 콘텐츠 팩에 포함할 콘텐츠를 선택합니다.

참고 선택한 대시보드, 쿼리 또는 경고에 사용되는 필드를 내보내도록 선택 취소할 수는 없습니다.

- 오른쪽의 텍스트 필드에 콘텐츠 팩의 메타데이터를 입력합니다.

옵션	설명
이름	팩을 vRealize Log Insight 인스턴스로 가져올 때 이름이 표시됩니다. 콘텐츠 팩 파일 이름은 이름 텍스트 상자에서 파생됩니다. 권장 형식은 벤더 - 제품 (예: VMware - vSphere)입니다.
버전	이 콘텐츠 팩을 업그레이드할 계획이면 버전을 입력합니다. 사용자가 콘텐츠 팩 목록에 이미 있는 콘텐츠 팩을 설치하려 하면 vRealize Log Insight는 버전을 표시합니다.
네임스페이스	네임스페이스는 콘텐츠 팩에 대한 고유 식별자입니다. 역 DNS 이름 지정법 (예: <code>com.companyname.contentpackname</code>)을 사용합니다.
Author	필요에 따라 사용자 자신의 이름 또는 회사 이름을 입력할 수 있습니다.
웹 사이트	필요에 따라 콘텐츠 팩에 연결된 웹 사이트 링크를 제공할 수 있습니다. 콘텐츠 팩을 볼 수 있는 모든 사용자가 웹 사이트 링크도 볼 수 있습니다.

옵션	설명
설명	필요에 따라 콘텐츠 관련 정보 및 팩의 용도를 제공할 수 있습니다.
아이콘	필요에 따라 콘텐츠 팩 이름 옆에 표시할 아이콘을 지정할 수 있습니다. 참고 아이콘 파일 형식은 PNG 또는 JPG여야 하며 144 X 144 픽셀 크기로 확장됩니다.

참고 이 데이터는 **콘텐츠 팩으로 설치** 옵션을 사용하여 콘텐츠 팩을 가져오는 경우에만 표시됩니다. 사용자 지정 콘텐츠로 콘텐츠 팩을 가져오도록 선택하는 경우 이 정보를 볼 수 없습니다.

5 내보내기를 클릭하고, 파일을 저장할 위치를 지정한 다음 **저장**을 클릭합니다.

내보낸 VLCP 파일이 선택된 위치로 다운로드됩니다.

콘텐츠 팩 요소에 대한 세부 정보 보기

대시보드를 구성하는 쿼리를 열거나 콘텐츠 팩 보기에서 필드 정의, 쿼리 및 경고를 직접 열 수 있습니다.

사용자 지정 정의에 대한 템플릿으로 콘텐츠 팩 요소 정의를 사용하려고 할 수 있습니다.

프로시저

- 오른쪽 상단의 드롭다운 메뉴에서 **콘텐츠 팩**을 선택합니다.
- 검토하려는 요소가 포함된 콘텐츠 팩을 선택합니다.
- 검토하려는 요소 유형에 해당되는 버튼을 클릭합니다.

예를 들어 콘텐츠 팩에 포함된 모든 경고를 보려면 **경고**를 클릭합니다.

- 요소 목록에서 검토하려는 요소 이름을 클릭합니다.

대화형 분석 페이지가 열리고 선택된 요소에 해당되는 쿼리가 표시됩니다.

후속 작업

콘텐츠 팩 요소 정의나 쿼리를 수정하고 사용자 지정 콘텐츠에 저장할 수 있습니다.

콘텐츠 팩 제거

콘텐츠 팩을 제거할 수 있습니다. 콘텐츠 팩을 제거하면 사용자 지정 대시보드, 저장된 쿼리, 경고 및 추출된 필드가 제거됩니다.


콘텐츠 팩은 vCenter vRealize Log Insight 콘텐츠 팩(VLCP) 파일로 저장됩니다.

콘텐츠 팩을 제거하면 모든 사용자가 이를 영구적으로 사용할 수 없습니다. 먼저 콘텐츠 팩을 VLCP 파일로 내보내서 백업하십시오. [콘텐츠 팩 내보내기](#) 항목을 참조하십시오.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 **관리자 편집** 권한을 가진 사용자로 로그인했는지 확인합니다. URL 형식은 `https://log-insight-host`이며 여기서 `log-insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 오른쪽 상단의 드롭다운 메뉴에서 **컨텐츠 팩**을 선택합니다.
- 2 제거할 컨텐츠 팩을 클릭하고 컨텐츠 팩 이름 옆에 있는 드롭다운 메뉴 에서 **제거**를 선택합니다.
- 3 **제거**를 클릭합니다.

설치된 컨텐츠 팩 목록에서 컨텐츠 팩이 제거됩니다.

컨텐츠 팩 생성

모든 Log Insight 사용자는 비공개적 또는 공개적 사용을 위해 컨텐츠 팩을 생성할 수 있습니다.

컨텐츠 팩은 vRealize Log Insight에 대한 변경할 수 없거나 읽기 전용인 플러그인이며, 로그 메시지 등 특정 이벤트 유형에 대한 사전 정의된 지식을 제공합니다. 컨텐츠 팩의 목표는 관리자, 엔지니어, 모니터링 팀 및 임원들이 쉽게 이해할 수 있는 형식으로 특정 이벤트 집합에 대한 지식을 제공하는 것입니다.

컨텐츠 팩은 제품 또는 애플리케이션의 상태에 대한 정보를 제공합니다. 또한 컨텐츠 팩은 제품 또는 애플리케이션이 작동하는 방식을 이해하는 데 도움이 됩니다.

vRealize Log Insight에서 [대시보드] 또는 [대화형 분석] 페이지를 사용하여 컨텐츠 팩의 정보를 저장할 수 있습니다. 컨텐츠 팩의 정보에는 다음이 포함됩니다.

- 쿼리 - 일반적으로 컨텐츠 팩에는 각 대시보드에 대한 3개 이상의 쿼리와 3개의 차트 위젯이 포함되어 있습니다. 즉, 총 9개가 넘는 쿼리가 포함되어 있음을 의미합니다.
- 필드 - 컨텐츠 팩에는 20개 이상의 추출된 필드가 포함되어 있어야 합니다.
- 집계
- 경고 - 각 컨텐츠 팩에는 5개 이상의 경고가 포함되어 있습니다.
- 대시보드 - 각 컨텐츠 팩에 3개 이상의 대시보드가 있습니다.
- 대시보드 필터 - 참조: [로그 이벤트 검색 및 필터링](#)
- 시각화 - 참조: [대화형 분석 차트를 사용하여 로그 분석](#)

기본적으로, vRealize Log Insight에는 VMware - vSphere 컨텐츠 팩이 함께 제공됩니다. 필요한 경우 추가적인 컨텐츠 팩을 가져올 수 있습니다.

컨텐츠 팩 용어

컨텐츠 팩 생성 워크플로는 여러 개념과 용어를 기반으로 합니다. 컨텐츠 팩을 효율적으로 생성하고 유지 보수하려면 컨텐츠 팩에 대해 잘 알고 있어야 합니다.

인스턴스

vRealize Log Insight 관리자만이 콘텐츠 팩 파일을 콘텐츠 팩으로 가져올 수 있습니다. 콘텐츠 팩을 콘텐츠 팩으로 가져오는 경우 이 콘텐츠 팩을 편집할 수 없습니다.

모든 사용자는 콘텐츠 팩 파일을 사용자 공간에 가져올 수 있습니다. 콘텐츠 팩 파일을 사용자 공간에 가져오는 경우 이 작업에서는 선별적으로 내 콘텐츠 아래에 개체를 가져옵니다. 콘텐츠 팩을 사용자 공간에 가져오면 vRealize Log Insight 인스턴스에서 콘텐츠 팩을 편집할 수 있습니다. 콘텐츠 팩을 게시하거나 수정하려는 경우 내보낸 콘텐츠 팩이 필요합니다.

사용자

콘텐츠 팩은 사용자 공간이라고도 하는 사용자 지정 대시보드 또는 보다 구체적으로 대시보드 페이지의 내 대시보드 또는 공유 대시보드 아래에 저장되는 콘텐츠에서 일부 생성됩니다. 사용자 지정 대시보드의 개체는 선별적으로 내보낼 수 있지만, 콘텐츠 팩별로 클린 사용자 공간을 보장하기 위해 vRealize Log Insight에서 별도의 사용자 엔티티가 각각의 개별 콘텐츠 팩을 작성하는 것이 좋습니다.

vRealize Log Insight에서 사용자 생성에 대한 자세한 내용은 VMware vRealize Log Insight 관리 가이드를 참조하십시오.

생성하는 모든 콘텐츠 팩에 대해 vRealize Log Insight에서 별도 콘텐츠 팩 작성자 사용자를 사용하십시오.

이벤트

콘텐츠 팩이 제품 또는 애플리케이션에 대한 모든 관련 이벤트를 포함하도록 보장하기 위해 콘텐츠 팩 생성을 시도하기 전에 관련 이벤트를 수집해야 합니다. 관련 이벤트를 수집하는 일반적인 방법 하나는 품질 보증 및 지원 팀이 대개 일반 이벤트에 대한 액세스 권한과 지식을 가지고 있으므로 이 팀에 요청하는 것입니다.

콘텐츠 팩을 만들면서 이벤트를 생성하려는 시도는 시간 소모적이며 중요 이벤트를 놓치게 됩니다. QA 및 지원 팀이 이벤트를 공급할 수 없는 경우, 제품 또는 애플리케이션 이벤트가 알려져 있고 문서화되어 있으면 이벤트를 시뮬레이션하고 이 이벤트를 대신 사용할 수 있습니다.

해당 로그를 수집한 후에는 vRealize Log Insight에 이 로그가 수집됩니다.

작성자

콘텐츠 팩의 작성자는 다음과 같은 자격을 갖추어야 합니다.

- VMware vRealize Log Insight 사용 경험
- 제품 또는 애플리케이션에 대한 실질적인 운영 지식
- 최적화된 정규식 생성에 대한 이해 및 능력
- 로그를 사용하는 제품 또는 애플리케이션의 여러 문제 디버깅 경험
- 수많은 문제를 다룬 지원 경력
- 이전 syslog 환경에서의 시스템 관리자 경력

워크플로

컨텐츠 팩 생성에 대한 권장 접근 방식은 대화형 분석 페이지에서 시작하고 오류나 경고 등 특정 유형의 이벤트에 대한 쿼리를 시작하는 것입니다. 쿼리 결과를 살펴보고 적절하게 잠재적인 필드 후보를 분석하고 추출하십시오. 이벤트 유형에 대한 이해와 이벤트에서 제공되는 유용한 정보를 통해, 적절하게 관련 쿼리를 구성하고 저장하십시오. 신속한 조치가 필요한 문제를 강조하는 쿼리의 경우, 경고를 생성하고 저장하십시오. 쿼리를 저장하면, 필터를 사용하여 결과 목록에서 해당 쿼리를 제거하고 새로 저장된 쿼리에 대한 잠재적인 후보일 수 있는 다른 이벤트를 표시하십시오. 모든 관련 쿼리를 저장한 후에는, 대시보드 페이지에서 논리적 방식으로 이러한 쿼리를 구성하고 표시하십시오.

쿼리

vRealize Log Insight의 쿼리는 이벤트를 검색하고 요약할 수 있습니다.

대화형 분석 페이지에서 쿼리를 생성하고 저장할 수 있습니다. 쿼리는 다음 중 하나 이상으로 구성되어 있습니다.

키워드	전체 또는 전체 텍스트, 영숫자, 하이픈 및/또는 밑줄 일치 항목
Glob	전체 또는 전체 텍스트, 영숫자, 하이픈 및/또는 밑줄 일치 항목
정규식	Java 정규식을 기반으로 하는 정교한 문자열 패턴 일치
필드 연산	추출된 필드에 적용되는 키워드, 정규식 및 패턴 일치 항목
집계	결과의 하위 그룹 하나 이상에 적용되는 함수

vRealize Log Insight는 다음과 같은 쿼리 유형을 지원합니다.

- 메시지. 키워드, 정규식 및/또는 필드 연산으로 구성된 쿼리
- 정규식 또는 필드. 키워드 및/또는 정규식으로 구성된 쿼리
- 집계. 함수, 하나 이상의 그룹화 및 임의의 개수의 필드로 구성된 쿼리

vRealize Log Insight에서 사용자 지정 경고를 정의하고 모든 유형의 스케줄링된 쿼리에서 이러한 경고를 트리거할 수 있습니다.

메시지 쿼리 생성에 대한 모범 사례

메시지 쿼리 생성에 대한 기본 개념입니다.

검색 창을 사용하거나 필터를 입력하여 메시지 쿼리를 입력할 수 있습니다.

검색 창을 사용하여 vRealize Log Insight 인스턴스의 이벤트 결과를 구체화하십시오. 검색 창 대신 필터를 사용할 수 있지만, 동등 필터보다 검색 창을 이용하는 쿼리를 이해하기가 더 쉬운 경우가 종종 있습니다. 본 모범 사례는 가능한 경우 동등 필터 대신 검색 창을 사용하기 위한 것입니다.

필터를 통해 정규식, 필드, 논리적 OR 연산 또는 검색 창과 필터 쿼리의 조합을 사용하여 쿼리를 생성할 수 있습니다.

검색 창과 필터를 사용하여 쿼리를 생성할 때 다음과 같은 모범 사례가 적용됩니다.

- 쿼리가 특정 환경과 관련되지 않은지 확인하십시오. 공개 콘텐츠 팩은 모든 환경에 일반적이어야 하므로 환경별 정보에 의존할 필요가 없습니다. 환경 특정 정보의 예에는 소스, 호스트 이름 및 기능이 `local*`을 사용하는 경우 잠재적으로 기능이 포함됩니다.
- 쿼리 구성 시, 가능한 경우, 키워드가 glob 사용에 충분치 않은 경우 및 glob가 정규식 사용에 충분치 않은 경우 키워드를 사용하십시오. 키워드 쿼리는 리소스를 가장 적게 사용하는 쿼리 유형입니다. Glob는 정규식의 간소화된 버전이며 그 다음으로 리소스를 적게 사용하는 쿼리 유형입니다. 정규식은 가장 리소스를 많이 사용하는 쿼리 유형입니다.
- 정규식 또는 필드 사용 시 가능하면 많은 키워드를 제공하십시오. 정규식에 논리적 OR가 포함되는 경우(예: `this|that`) 키워드를 포함시키지 마십시오. vRealize Log Insight는 정규식 오버헤드를 최소화하기 위해 정규식 전에 키워드 쿼리를 수행하도록 최적화되어 있습니다.

필드 쿼리

필드는 구조화되지 않은 이벤트에 구조를 추가하고 데이터의 텍스트 및 시각적 표시 모두에 대한 조작을 허용하는 강력한 방법입니다.

필드는 집계 및 필터를 비롯하여 여러 가지 방법으로 사용할 수 있으므로 콘텐츠 팩에서 가장 중요한 항목 중 하나입니다. 집계를 사용하여 필드에 함수 및 그룹화를 적용할 수 있습니다. 필터를 사용하여 필드에 대해 연산을 수행할 수 있습니다.

쿼리 또는 집계에 적용할 수 있는 로그 메시지의 모든 부분을 추출해야 합니다. 필드는 정규식 쿼리 유형이며 복잡한 패턴 일치에 유용하므로 복잡한 정규식을 알거나 기억하거나 배울 필요가 없습니다.

필드 컨텍스트	
값	정의
값 앞의 Regex	최대한 많은 키워드를 포함하십시오. 이 필드가 비어 있거나 특수 문자만 포함된 경우 값 뒤의 Regex에는 키워드가 포함되어야 합니다.
값 뒤의 Regex	최대한 많은 키워드를 포함하십시오. 이 필드가 비어 있거나 특수 문자만 포함된 경우 값 앞의 Regex에는 키워드가 포함되어야 합니다.
이름	영숫자 문자만 사용하십시오. 모든 문자가 소문자이고 공백 대신 밑줄을 사용하는지 확인하십시오. 그러면 필드를 보기가 더 쉬워집니다. 콘텐츠 팩 필드에는 필드 이름 오른쪽의 괄호에 네임스페이스가 있을 것이지만 콘텐츠 팩 필드 및 사용자 필드는 동일할 수 있음에 주의하십시오. 예를 들어 <code>vmw_</code> 과 같이 혼동을 피하기 위해 약어가 포함된 접두사 콘텐츠 팩 필드가 있습니다.
키워드 검색어	필드를 포함하는 이벤트 내에 나타나는 하나 이상의 키워드로, 이는 공백으로 구분됩니다.
필터	필드를 포함하는 이벤트 내에 나타나는 정적 필드, 연산자 및 잠재적 값입니다. 일반적으로 필터를 vRealize Log Insight 에이전트와 함께 사용하여 키워드를 포함하지 않는 이벤트에 태그를 지정합니다.
정보("i" 버튼)	필드에 대한 정보를 제공하는 데 사용됩니다. 여기에는 필드의 의미, 반환 가능한 잠재적 값이 제공되며 가능한 경우 값을 이해하기 쉬운 정보에 연결합니다.

모범 사례

필드를 이루는 다양한 구성 요소뿐만 아니라 여러 모범 사례가 적용됩니다.

- 정규식 패턴에 대한 필드만 생성하십시오. 키워드 쿼리를 사용하여 필드를 쿼리할 수 있거나 필드가 단일 값만 반환하는 경우 사전 정의된 필드 대신 키워드 쿼리를 사용하십시오. 필드가 두 개의 값만 반환하는 경우 필드를 추출하는 대신 개별 쿼리를 구성하는 것을 고려하십시오. 필드는 구조화되지 않은 데이터에 구조를 추가하기 위한 것일 뿐만 아니라 이벤트의 특정 부분에 대해 쿼리하는 방법을 제공하기도 합니다.
- 전체 이벤트의 일부를 반환하는 정규식 패턴에 대한 필드만 생성하십시오. 대부분의 이벤트와 일치하는 필드 및/또는 매우 많은 결과를 반환하는 필드는 필드 추출에 좋은 후보가 아닙니다. 정규식은 리소스 집약적인 연산이 되게 하는 많은 양의 이벤트에 적용되어야 합니다. 가능한 경우 키워드를 더 추가하여 반환되는 결과 수를 줄이고 쿼리를 최적화하십시오.
- 필드에 정규식 구문 내 키워드가 포함된 경우, 정규식 구문 없이 해당 키워드를 필터로 추가하십시오. 예를 들어, 필드의 값이나 컨텍스트에 `this|that`과 같은 정규식 구문 내 키워드가 포함된 경우, 해당 키워드를 텍스트 필터로 추가하여 `text contains this, that`과 같은 쿼리를 최적화하십시오.
- 복잡한 정규식의 경우 컨텍스트 전/후로 하나 이상의 키워드와 함께 추가 컨텍스트를 사용하는 것이 좋습니다.
- 쿼리 성능을 최적화하려면 모든 추출된 필드에 컨텍스트를 더 추가하십시오.

임시 필드

임시 필드는 쿼리의 일부로 존재하는 필드이지만, vRealize Log Insight 인스턴스 내에서 전역으로 또는 설치된 콘텐츠 팩의 일부로 저장되지 않습니다.

vRealize Log Insight는 수정 중인 필드를 사용하는 쿼리를 자동으로 업데이트하여 임시 필드를 생성하는 경우를 줄입니다.

참고 저장된 쿼리가 사용하는 필드를 삭제하는 경우 저장된 쿼리에 임시 필드가 포함됩니다.

대화형 분석 페이지에서 저장된 쿼리를 실행하면 임시 필드를 볼 수 있으며 저장된 쿼리에서 사용되는 필드에는 필드 이름 오른쪽에 네임스페이스 `Temporary`가 포함되어 있습니다.

쿼리 대상에는 하나 이상의 필드가 포함되어 있습니다. vRealize Log Insight의 저장된 쿼리의 경우 해당 필드가 수정되면 쿼리가 저장될 때 사용된 필드 정의가 수정됩니다. 필드 수정에는 다음이 포함됩니다.

- 필드 값 변경
- 값 앞의 regex 및 필드 값 뒤의 regex 변경
- 필드 이름 변경
- 필드 삭제

콘텐츠 팩을 내보내는 경우 vRealize Log Insight는 모든 임시 필드를 콘텐츠 팩 필드로 변환합니다. 콘텐츠 팩에서 임시 필드가 표시되는 경우, 임시 필드와 함께 내보낸 이전 제품 버전의 콘텐츠 팩이 표시되는 것이거나 콘텐츠 팩이 수동으로 편집된 것입니다.

추출된 기존 필드와 이름이 동일한 임시 필드가 있는 경우 임시 필드의 끝에 {n}이 표시됩니다. 예를 들어 product_test_field라는 필드가 있는 경우 내보내는 동안 product_test_field {2}도 표시될 수 있습니다. 이러한 동작이 나타나면 임시 필드가 있는 것입니다. 이 문제를 해결하려면 내보내기 대화상자의 맨 아래에서 **모두 선택 취소** 옵션을 선택하고 끝에 {n}이 있는 추출 필드가 선택될 때까지 각 대시보드 및/또는 경고를 선택합니다. 해당 대시보드 및/또는 경고로 이동하고 각 쿼리를 편집합니다. 추출된 필드를 사용하는 쿼리가 발견되면 끝에 {n} 없이 필드를 사용하도록 필터 또는 집계를 변경하고 쿼리를 실행한 후 쿼리를 저장합니다. 끝에 {n}이 있는 필드를 사용하는 모든 쿼리에 대해 이러한 단계를 완료하면 내보내는 동안 필드가 더 이상 표시되지 않습니다.

집계 쿼리

vRealize Log Insight에서 집계 쿼리를 사용하여 이벤트의 시각적 표시를 조작할 수 있습니다.

집계 쿼리는 다음 두 가지 특성으로 구성됩니다.

- 기능
- 그룹화

집계 쿼리에는 하나의 함수와 하나 이상의 그룹화가 필요합니다. 그룹화는 콘텐츠 팩의 중요한 부분입니다. 함수와 그룹화는 차트가 표시되는 방식에 영향을 미칩니다.

차트 표시는 2,000개의 가장 최근 결과로 제한됩니다.

막대형 차트

기본적으로, vRealize Log Insight의 대화형 분석 페이지에 있는 개요 차트는 시간 경과에 따른 이벤트 개수를 표시합니다. 시계열 그룹화와 함께 count 함수를 사용하는 경우 vRealize Log Insight는 막대형 차트를 생성합니다.

시계열 대신 단일 필드 그룹화와 함께 count 함수를 사용하는 경우 vRealize Log Insight는 최대 수부터 최소 수까지 차례대로 나열되는 막대형 차트를 생성합니다.

꺾은선형 차트

count 함수를 제외한 모든 함수는 수학입니다. 이러한 함수를 사용하려면 수식을 적용하는 필드가 필요합니다. 필드에서 수학 함수를 수행하고 시계열로 그룹화하는 경우, vRealize Log Insight는 꺾은선형 차트를 생성합니다.

누적형 차트

기본적으로, vRealize Log Insight의 대화형 분석 페이지에 있는 개요 차트는 시간 경과에 따른 이벤트 개수를 표시합니다. 시계열 그룹화에 필드 하나를 추가하면 vRealize Log Insight는 누적형 차트를 생성합니다.

시계열로 그룹화를 사용하고 필드를 더하고 count를 제외한 함수를 사용하면 vRealize Log Insight는 누적 꺾은선형 차트를 생성합니다. 개체에 대한 예외 사항을 찾으려고 시도할 때 누적형 차트는 강력한 기능을 발휘합니다.

집계 쿼리가 반환할 수 있는 개체 수를 기준으로, 사용할 누적형 차트 유형을 결정해야 합니다. 더 많은 개체를 표시하려면 구문 분석하고 정보를 표시하는 데 필요한 리소스가 더 많이 요구됩니다. 또한, 색상 수는 고정되어 있으므로, 반환되는 개체 수에 따라 개체 간 구분이 어려워질 수 있습니다. 일반적으로 다음 모범 사례가 적용됩니다.

- 각 막대에서 반환되는 개체 수가 10개 미만인 경우 누적형 차트를 사용할 수 있습니다.
- 각 막대에서 반환되는 개체 수가 10-20개 사이이거나 이 사이일 수 있는 경우 누적형 차트가 괜찮을 수 있습니다. 콘텐츠 팩에서 차트를 시각적으로 표시할 방법을 고려해야 합니다.
- 각 막대에서 반환되는 개체 수가 20개를 넘거나 넘을 수 있는 경우 누적형 차트를 사용하지 않는 것이 좋습니다.

여러 색상 차트

두 개 이상의 필드 및 시계열을 사용하여 그룹화를 생성하는 경우 vRealize Log Insight는 다중 색상 차트를 생성합니다. 차트는 교환 가능한 두 가지 색상으로 구성되어 있습니다. 각각의 교환은 새로운 시간 범위를 나타냅니다. 다중 색상 차트는 해석하기 어려울 수 있으므로 콘텐츠 팩에 이 차트를 포함시키기 전에 해당 차트의 값의 고려하십시오.

여러 필드로 그룹화를 만드는 경우 비시계열 사용을 고려하십시오. 시계열을 제거하면 막대형 차트를 이해하기가 훨씬 더 쉽습니다.

지정된 시간 범위에서 여러 필드가 중요한 경우, 시간 범위에서 개별적으로 각 필드에 대해 여러 차트를 생성할 수 있습니다. 그런 다음 콘텐츠 팩에서 대시보드 그룹의 동일한 열에 차트를 표시할 수 있습니다.

그 밖의 차트

원형, 거품형 및 표 차트를 비롯한 몇 가지 다른 차트 유형을 사용할 수 있습니다. 이러한 차트를 사용하려면 특정 쿼리 유형이 필요합니다. 이러한 차트 옵션을 사용할 수 있는 경우 정확한 쿼리가 이미 있다는 의미입니다. 이러한 차트 옵션을 사용할 수 없는 경우 사용할 차트 이름 위로 마우스 커서를 이동합니다. 팝업 메시지는 차트 유형에 필요한 쿼리 유형이 설명되어 있습니다.

메시지 쿼리

집계 쿼리 구성 시, 메시지 쿼리는 집계 쿼리와 관련된 결과만 반환해야 합니다. 그러면 분석하기가 더 쉽고 결과가 관련 필드만 표시하도록 보장됩니다. 메시지 쿼리가 집계 쿼리로 동일한 결과를 반환하도록 보장하려면, 집계 쿼리에 사용되는 각 필드에 대해 exists 연산자를 사용하여 필터를 추가해야 합니다.

차트 유형 변경

대시보드에서 위젯의 차트 유형을 변경하려는 경우 위젯의 톱니 바퀴 아이콘을 클릭하고 **차트 유형 편집**을 선택합니다. 위젯 유형을 변경하려는 경우 새 위젯을 저장하고 기존 위젯을 삭제하면 됩니다.

경고

경고는 특정 유형의 이벤트가 발생하는 경우 반응을 트리거하는 방법을 제공합니다.

vRealize Log Insight는 두 가지 유형의 경고를 지원합니다.

- 이메일

■ vRealize Operations Manager

사용자 공간에만 경고를 저장할 수 있습니다. 기본적으로 모든 콘텐츠 팩 경고는 사용하지 않도록 설정되어 있습니다. 사용하도록 설정된 경고를 생성하고 콘텐츠 팩의 일부로 이 경고를 내보내는 경우 콘텐츠 팩에서 해당 경고가 사용되지 않도록 설정됩니다.

콘텐츠 팩에는 이메일 및 vRealize Operations Manager 설정이 포함되지 않습니다. 그리고 이러한 설정을 콘텐츠 팩에 추가할 수 없습니다.

임계값

임계값은 트리거된 경고 수에 대한 제한을 설정합니다.

사용되는 경우 콘텐츠 팩 경고가 실수로 사용자에게 스팸을 보내지 않도록 임계값이 어떻게 작동하는지 이해해야 합니다. 임계값 사용을 고려할 때 주의해야 할 질문 두 가지가 있습니다.

- 경고를 얼마나 자주 트리거해야 합니까? Log Insight에는 사전 정의된 빈도가 제공됩니다. 경고는 지정된 임계값 기간 동안 한 번만 트리거됩니다.
- 경고 상태가 발생했는지 여부를 얼마나 자주 확인해야 합니까? 경고는 쿼리에 의해 트리거됩니다. 쿼리와 마찬가지로 경고는 현재 버전에서 실시간이 아닙니다. 각 임계값 기간 동안 사전 결정된 쿼리 빈도가 할당되어 있습니다. 임계값을 변경하면 쿼리 시간이 변경됩니다.

그룹화

이메일 경고를 생성할 때 경고 소스를 식별하는 필드별로 그룹화해야 합니다.

경고에서 전송하는 이메일에는 특정 집계 쿼리에 대한 결과 테이블이 포함되어 있습니다. 대화형 분석 페이지에서 쿼리의 시각적 표현을 볼 수 있습니다.

사용자가 그룹화한 고유 식별자가 없다면 결과가 환경에 있는 시스템 하나 또는 여러 개와 관련되어 있는지 알 수 없습니다. 소스 필드가 아닌 호스트 이름 필드를 기준으로 그룹화해야 합니다. 또한 이벤트 소스 위치를 고유하게 식별하는 필드를 원하는 대로 추가할 수도 있습니다.

대시보드 모범 사례

대시보드는 콘텐츠 팩의 일부입니다. 대시보드 생성 시 적용되는 몇 가지 모범 사례가 있습니다.

대시보드 생성 시 다음 모범 사례가 적용됩니다.

- 콘텐츠 팩에는 일반적으로 최소 3개의 대시보드가 포함되어 있습니다. 모범 사례는 개요 대시보드로 시작하여 특정 제품이나 애플리케이션의 이벤트에 대한 대략적인 정보를 제공하는 것입니다. 개요 대시보드 외에도, 이벤트의 논리적 그룹화를 기준으로 다른 대시보드도 생성해야 합니다. 논리적 그룹화는 제품과 관련되거나 애플리케이션과 관련되지만 몇 가지 일반적인 접근 방식은 성능, 오류 및 감사입니다. 또한 디스크 및 컨트롤러와 같은 구성 요소에 대한 대시보드를 생성하는 것도 일반적입니다. 구성 요소 접근 방식의 경우, 특정 구성 요소에서 결과를 반환하도록 쿼리를 구성할 수 있는 경우에만 유효하다는 점에 주의해야 합니다. 이것이 가능하지 않은 경우 논리적 접근 방식이 권장됩니다.
- 대시보드 이름 지정 시, 구성 요소와 관련된 방식으로 사용하고 있지 않은 경우 제품과 관련되거나 애플리케이션과 관련된 이름을 추가하지 말고 일반적인 제목을 지정하십시오. 예를 들어, VMware - vSphere 콘텐츠 팩에 VMware ESX/ESXi 대신 ESX/ESXi라는 대시보드 그룹이 있습니다.

- 대시보드에는 최소 3개, 최대 6개의 대시보드 위젯이 포함되어야 합니다. 대시보드 위젯이 3개 미만인 경우에는 대시보드를 통해 얻을 수 있는 지식의 양이 아주 적습니다. 또한 제한된 양의 대시보드 위젯만 있는 많은 대시보드를 갖게 되면 사용자가 여러 페이지 간에 전환해야 하며 일관된 방식으로 정보가 제공되지 않습니다.

반대로, 대시보드의 대시보드 위젯이 6개가 넘으면 부정적인 영향을 미칠 수 있습니다. 혼동스러울 수 있는 정보를 너무나 많이 갖게 될 수 있습니다. 각 위젯은 시스템에 대해 실행해야 하는 쿼리이므로, 위젯이 너무 많으면 시스템 리소스를 상당히 많이 사용하게 됩니다.

대시보드에서 6개가 넘는 대시보드 위젯을 포함하면, 정보를 구분하고 여러 대시보드를 생성해야 합니다. 대시보드 위젯이 하나 이상의 대시보드에 적용되는 경우, 적용되는 각 대시보드에서 위젯을 생성하십시오.

대시보드 필터

대시보드 필터는 특정 이벤트로 드릴다운하는 데 사용될 수 있습니다. 필터 기능은 [대화형 분석] 페이지의 필터와 유사하며, 드릴다운하는 데 필터가 사용됩니다. 모든 대시보드에는 주로 호스트 이름 필드와 함께 하나 이상의 대시보드 필터가 있어야 하며, 각 대시보드에는 최대 5개 필드만 추가될 수 있습니다.

추가된 필드는 해당 대시보드에 있는 대부분의 위젯에 사용되어야 합니다. 그래야 대시보드 필터가 사용되면 대부분의 위젯에서 결과를 반환합니다. 대시보드 필터의 예로는 심각도 필드, 사용자 필드, 심지어 구성 요소 필드도 포함될 수 있습니다.

참고 대시보드 필터에 사용되는 필드와 연산자는 내보낸 콘텐츠 팩에 저장됩니다. 대시보드 필터에 사용된 모든 값은 모든 환경에 대해 일반적인 값이 아니라 해당 환경에만 연관될 수 있으므로 내보내는 도중 저장되지 않습니다.

대시보드 위젯

대시보드 위젯은 정보를 시각화하는 데 유용합니다.

대시보드에 추가할 수 있는 여러 유형의 위젯이 vRealize Log Insight에 있습니다. 여기에는 다음이 포함됩니다.

- 저장된 쿼리에 대한 링크와 함께 이벤트의 시각적 표시가 포함된 차트 위젯
- 저장된 쿼리에 대한 제목 링크가 포함된 쿼리 목록 위젯
- 이벤트를 포함하는 필드 테이블 위젯(각 필드는 열을 나타냄)
- 단일 그룹에 결합된 비슷한 이벤트를 포함하는 단순화된 이벤트 유형 테이블 위젯
- 쿼리에서 확인된 이벤트 유형 목록을 발생 횟수별로 정렬하여 표시하는 단순화된 이벤트 추세 테이블 위젯 이러한 위젯에서는 쿼리에서 자주 발생하는 이벤트 종류를 빠르게 확인할 수 있습니다.

차트

대시보드 차트 위젯에는 이벤트의 시각적 표시가 포함되어 있습니다. 막대형 차트 또는 꺾은선형 차트로 차트를 나타내고 누적형으로 표시할 수 있습니다.

차트를 나타내는 여러 가지 방법이 있습니다.

- 차트에는 여러 가지 정보가 포함되어 있습니다. 단일 행에 차트 위젯이 두 개가 넘지 않게 하십시오. 드물게 세 개의 차트 위젯을 효과적으로 사용할 수 있는 경우가 있기는 하지만, 세 개가 넘게 사용하지 않는 것이 좋습니다. 차트 위젯을 읽을 수 있는지 여부를 확인할 때, vRealize Log Insight에서 지원하는 최소 해상도 1024 x 768픽셀을 사용해야 합니다.
- 마지막 행을 제외한 행에 단일 차트 위젯이 있는 경우 해당 위젯을 전체 너비로 만드십시오.
- 차트 위젯 이름 지정 시, 설명적인 제목을 사용하고 모호한 필드 이름은 피하십시오. 예를 들어, 추출된 필드를 `vmw_error_message`라고 합니다. 차트 이름을 `vmw_error_message`의 개수라고 하는 대신 오류 메시지 개수라고 지정하십시오.
- 유사한 차트를 저장하고 시각적인 비교를 위해 대시보드 그룹의 동일한 열에 이러한 차트를 누적할 수 있습니다. 예:
 - 시간 경과에 따른 이벤트의 평균 X + 시간 경과에 따른 이벤트의 최대 X. 사용되는 여러 함수를 고려하면 차트의 Y 축에 다른 배열이 있을 수 있습니다.
 - 시간 경과에 따라 X별로 그룹화된 이벤트 개수 + 시간 경과에 따라 Y별로 그룹화된 이벤트 개수.

쿼리 목록

대시보드 쿼리 목록 위젯에는 사전 정의된 쿼리에 대한 하나 이상의 링크가 포함되어 있습니다.

다음과 같은 경우에 쿼리 목록 위젯을 사용할 수 있습니다.

- 차트 위젯은 중요한 값을 제공하지 않지만 기본 쿼리는 이러한 값을 제공하는 경우
- 정규식을 사용하는 쿼리 등 복잡한 쿼리를 저장하려는 경우
- 대시보드 그룹 내 동일한 기본 쿼리에 대해 여러 집계를 사용하려는 경우

필드 테이블

이벤트를 포함하는 필드 테이블로, 여기서 각 필드는 열을 나타냅니다.

대시보드 필드 테이블 위젯에는 지정된 쿼리에 대한 최신 이벤트가 테이블 형식으로 포함되어 있으며, 여기서 각 필드는 열을 나타냅니다.

다음과 같은 이유로 필드 테이블 위젯을 사용할 수 있습니다.

- 지정된 쿼리에 대한 최신 이벤트 보기. 이는 변경 관리 또는 보안 목적인 경우 유용할 수 있습니다.
- 지정된 쿼리에 대해 관심 있는 필드만 보기. 이는 이벤트 출력을 제한하는 데 유용할 수 있습니다.

컨텐츠 팩 가져오기 오류

컨텐츠 팩을 가져오는 경우 일부 경고 또는 오류 메시지가 표시될 수 있습니다.

업그레이드

업그레이드 메시지가 표시될 수 있습니다. 이는 다른 컨텐츠 팩이 동일한 네임스페이스가 있는 시스템에 설치되어 있음을 나타냅니다. 이러한 경우 업그레이드하고 기존 컨텐츠 팩을 교체하거나, 업그레이드 프로세스를 취소하고 기존 컨텐츠 팩을 유지할 수 있습니다.

잘못된 형식

형식이 잘못되었다고 나타내는 메시지가 표시될 수 있습니다. 즉, VLCP 파일이 수동으로 편집되었으며 구문 오류가 포함되었음을 나타냅니다. 콘텐츠 팩을 가져오기 전에 구문 오류를 해결해야 합니다.

최신 버전

이 유형의 메시지는 콘텐츠 팩이 최신 버전의 Log Insight에서 생성되었으며 이 버전에서만 지원됨을 나타냅니다. Log Insight 1.5 이후 제품 버전에서 이 유형의 메시지가 표시되면 VLCP 파일이 수동으로 편집되었음을 나타냅니다.

인식되지 않는 버전

VLCP 파일이 수동으로 편집되고 구문 오류가 포함된 경우 이 유형의 메시지가 표시될 수 있습니다. 콘텐츠 팩을 가져오려고 시도하기 전에 구문 오류를 해결해야 합니다.

참고 수동으로 VLCP 파일을 편집하지 않아야 합니다. 그러면 구문 오류를 찾고 수정하기가 어렵습니다.

콘텐츠 팩 게시에 대한 요구 사항

콘텐츠 팩을 생성하고 게시하려는 경우 콘텐츠 팩이 기본 게시 요구 사항을 충족하는지 확인하십시오.

콘텐츠 팩 요구 사항 및 게시 요구 사항 모두를 확인해야 합니다.

콘텐츠 팩 요구 사항

콘텐츠 팩은 콘텐츠, 품질 및 표준에 대한 몇 가지 요구 사항을 충족해야 합니다.

콘텐츠 요구 사항에는 다음이 포함됩니다.

- 최소 3개의 대시보드
- 대시보드당 최소 1개의 대시보드 필터(3개가 이상적이며, 최대는 5개)
- 대시보드당 최소 3개의 대시보드 위젯
- 대시보드당 최대 6개의 대시보드 위젯
- 행당 최대 3개의 대시보드 위젯
- 최소 5개의 경고
- 최소 20개의 추출된 필드

콘텐츠 팩에 대한 품질 요구 사항은 다음과 같습니다.

- 모든 쿼리에 최소 1개의 전체 텍스트 키워드가 있고, 3개 이상의 키워드가 있는 것이 좋습니다.
- 쿼리는 소스, 호스트 이름, 시설* 등의 환경 관련 특성을 기반으로 하지 않습니다.
- 모든 필드에 최소 1개의 전체 텍스트 키워드가 있고, 3개 이상의 키워드가 있는 것이 좋습니다.
- 필드는 제품/애플리케이션과 관련되며 다른 제품/애플리케이션 로그에 대한 결과는 반환하지 않습니다.

- 모든 대시보드 위젯에는 차트가 표시하는 내용 및 이 내용이 중요한 이유에 대한 정보/링크가 포함되어야 합니다.

컨텐츠 팩 생성에 대한 표준은 다음 규칙을 따릅니다.

컨텐츠 팩 부분	포맷
컨텐츠 팩 이름 형식	회사 - 제품
컨텐츠 팩 네임스페이스 형식(컨텐츠 팩은 네임스페이스와 함께 내보내야 합니다.)	외부.도메인.제품
추출된 필드 형식	접두사_필드_이름, 여기서 접두사는 회사 이름 또는 회사 약어입니다.

게시 요구 사항

컨텐츠 팩을 게시하기 전에 컨텐츠 팩이 게시 요구 사항을 충족하는지 확인하십시오. 권장할 컨텐츠 팩은 Developer Center의 컨텐츠 팩 게시자를 사용하고, 검토용 버전은 VMware에 업로드하십시오. <https://developercenter.vmware.com/web/loginsight>

게시 요구 사항	설명
컨텐츠 팩 파일 형식	VLCP 파일입니다.
이벤트	컨텐츠 팩을 검증하는 데 필요한 해당 이벤트입니다.
개요	컨텐츠 팩을 개괄적으로 설명하는 1~2개의 단락입니다.
강조 표시	컨텐츠 팩의 가치를 설명하는 3가지 주요 내용입니다.
설명	컨텐츠 팩과 그 가치를 설명하는 2~3개의 단락입니다.
기술 규격	제품 버전과 구성 그리고 Log Insight 버전과 구성을 포함하여 최소 시스템 요구 사항을 설명합니다. 또한 Log Insight에 로그를 기록하고 컨텐츠 팩을 채우도록 제품을 구성하는 데 필요한 모든 지침도 제공합니다.
스크린샷	실제 데이터가 있는 컨텐츠 팩을 보여주는 3개 이상 스크린샷입니다.
비디오(선택 사항)	컨텐츠 팩이 값을 가져오는 방법에 대한 예입니다.
백서(선택 사항)	제품 또는 애플리케이션이 로그를 vRealize Log Insight에 전달하도록 구성하는 방법입니다.

컨텐츠 팩 제출

VMware Solutions Exchange에서 생성한 컨텐츠 팩을 제출합니다.

필수 조건

- 컨텐츠 팩이 [컨텐츠 팩 게시에 대한 요구 사항](#)을 충족하는지 확인합니다.
- <http://solutionexchange.vmware.com>의 계정이 없는 경우 **등록**을 클릭하고 **파트너**를 선택합니다. 파트너 등록 요청 양식을 채우고 제출합니다. 로그인 요청이 승인되면 알림 이메일을 받게 됩니다.

프로시저

- 1 <http://solutionexchange.vmware.com>으로 이동하고 페이지 오른쪽 상단 모서리에서 **지금 로그인**을 클릭합니다.

- 2 사용자 이름과 암호를 입력하고 **지금 로그인**을 클릭합니다.
- 3 **관리**를 클릭하고 **솔루션 관리**를 선택하여 솔루션을 추가하거나 편집합니다.
- 4 **솔루션 추가**를 클릭하고 필수 정보를 채웁니다.

작업이 손실되지 않도록 자주 **초안 저장** 버튼을 사용하십시오.

- 5 **승인을 위해 제출**을 클릭합니다.

검토와 승인을 위해 솔루션이 VMware Solution Exchange 제휴 팀으로 전송됩니다.

솔루션의 승인 상태에 관한 이메일을 받게 됩니다.

후속 작업

솔루션 목록 작성에 대한 자세한 내용을 보려면 페이지 상단의 **파트너 코너** 링크를 클릭하십시오. 필요한 정보를 찾을 수 없는 경우 VSXAlliance@vmware.com으로 문의하십시오.

vRealize Log Insight 의 경고 쿼리

스케줄링된 간격으로 특정 쿼리를 실행하도록 vRealize Log Insight를 구성할 수 있습니다.

쿼리와 일치하는 이벤트 수가 설정한 임계값을 초과하는 경우 vRealize Log Insight가 이메일 또는 webhook 알림을 보내고 vRealize Operations Manager에서 알림 이벤트를 트리거할 수 있습니다.

사용 가능한 경고 목록을 보려면 대화형 분석 페이지로 이동하고 **검색** 필드 옆에 있는 **경고 만들기 또는 관리...** 드롭다운 메뉴에서 **경고 관리...**를 선택합니다. 각 경고 상태가 경고 이름 아래에 나타납니다.

참고 경고 쿼리는 사용자에게 따라 다릅니다. 자신의 경고만 관리할 수 있습니다.

vRealize Log Insight 에서 생성할 수 있는 경고 유형

경고 쿼리가 실행되는 간격 및 경고 유형 중 하나를 선택하여 vRealize Log Insight가 경고 알림을 보내는 조건을 제어할 수 있습니다.

모든 일치 항목에 대한 경고	5분마다 경고 쿼리가 자동으로 실행됩니다. 지난 5분 내에 하나 이상의 이벤트가 쿼리와 일치하는 경우 알림이 트리거됩니다.
이벤트 유형 기반 경고	5분마다 경고 쿼리가 자동으로 실행됩니다. 지정된 이벤트 유형이 확인되면 알림이 트리거됩니다.
사용자 지정 기간 내 이벤트 수에 기반한 경고	경고 쿼리 간격은 설정에 따라 다릅니다. 지난 Y분에 X개 정도 일치하는 이벤트가 발생하는 경우, 설정에 따라 알림이 트리거됩니다.

이 경고 유형이 트리거되는 경우 동일한 이벤트 집합에 대해 중복 경고가 발생하지 않도록 해당 기간 동안 경고가 일시 중지됩니다. 일시 중지된 동안 경고를 사용하도록 설정하려면, 사용되지 않도록 설정했다가 다시 사용하도록 설정할 수 있습니다.

집계 쿼리 기반 경고

집계 쿼리 경고는 그룹에 포함된 함수의 값이 사용자가 정의하는 값을 초과하는 경우 알림을 트리거합니다. 지정한 기간 내에 차트에서 하나 이상의 막대가 설정한 임계값보다 높거나 낮은 경우 차트에서 이러한 알림을 볼 수 있습니다.

이 경고 유형은 **시간 경과에 따른 이벤트 개수**를 시각화하지 않는 차트에 대해 설정할 수 있습니다.

컨텐츠 팩 경고

컨텐츠 팩은 경고 쿼리를 포함할 수 있습니다. 기본적으로 vRealize Log Insight에 포함된 vSphere 컨텐츠 팩은 여러 가지 사전 정의된 경고 쿼리를 포함합니다. ESXi 호스트가 syslog 데이터 전송을 중지하는 경우, vRealize Log Insight가 vCenter Server에서 이벤트, 작업 및 경고 데이터를 더 이상 수집하지 않는 경우 또는 경고 상태가 빨간색으로 변경되는 경우 이러한 쿼리가 경고를 트리거할 수 있습니다. 환경에 특정한 경고를 생성하기 위한 템플릿으로 이러한 경고 쿼리를 사용할 수 있습니다.

기본적으로 모든 컨텐츠 팩 경고는 사용되지 않도록 설정되어 있습니다.

vRealize Log Insight를 다시 시작할 때 특정 버전의 ESXi 호스트가 syslog 데이터 보내기를 중지할 수 있으므로 **vCenter Server: ESX/ESXi가 로깅을 중지함** 경고를 사용하도록 설정하는 것이 좋습니다. 이 경고는 vCenter Server 이벤트 esx.problem.vmsyslogd.remote.failure를 모니터링하여 syslog 보내기를 중지한 ESXi 호스트가 있는지 감지합니다. syslog 문제와 솔루션에 대한 자세한 내용은 [VMware ESXi 5.x 호스트가 원격 서버로의 syslog 전송 중지\(2003127\)](#)를 참조하십시오.

다음 필터를 경고 쿼리에 추가하고 새로운 경고로 저장하여 vRealize Log Insight의 인스턴스에 피드 전송을 중지하는 ESXi 호스트만을 감지할 수 있습니다. **vc_remote_host (VMware - vSphere) contains log-insight-hostname**.

컨텐츠 팩 경고 쿼리는 읽기 전용입니다. 컨텐츠 팩 경고에 대한 변경 내용을 저장하려면 사용자 지정 컨텐츠에 경고를 저장해야 합니다.

■ 이메일 알림을 보내도록 경고 쿼리 추가

특정 데이터가 로그에 나타나는 경우 이메일 알림을 보내도록 vRealize Log Insight에서 경고 쿼리를 구성할 수 있습니다.

■ Webhook을 사용하여 타사 제품에 경고 보내기 정보

webhook을 사용하여 타사 제품에 vRealize Log Insight 사용자 경고를 보낼 수 있습니다.

■ 경고 쿼리 보기

생성한 경고 쿼리를 보고 이러한 쿼리에 대한 알림이 사용되는지 확인할 수 있습니다.

■ 경고 쿼리 수정

경고 쿼리의 트리거를 변경하거나, 쿼리가 전송하는 알림을 사용 또는 사용하지 않도록 설정하거나, 알림 방법(이메일, webhook 또는 vRealize Operations Manager로 보내기)을 변경할 수 있습니다.

■ 경고 쿼리 사용

경고 쿼리가 사용하지 않도록 설정된 경우 vRealize Log Insight는 이메일 또는 webhook 알림을 보내지 않고 vRealize Operations Manager 알림 이벤트를 트리거하지 않습니다.

■ 경고 쿼리 삭제

더 이상 필요하지 않은 경우 경고 쿼리를 삭제할 수 있습니다.


이메일 알림을 보내도록 경고 쿼리 추가

특정 데이터가 로그에 나타나는 경우 이메일 알림을 보내도록 vRealize Log Insight에서 경고 쿼리를 구성할 수 있습니다.

필수 조건

- vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.
- 관리자가 이메일 알림을 사용하도록 SMTP를 구성했는지 확인합니다. [Log Insight에 대한 SMTP 서버 구성](#)을 참조하십시오.

프로시저

- 1 대화형 분석 탭에서 알림을 전송할 쿼리를 실행합니다.
- 2 검색 버튼 오른쪽에 있는 **경고 만들기 또는 관리** 메뉴에서  아이콘을 클릭하고 **쿼리에서 경고 만들기**를 선택합니다.
- 3 경고 추가 대화상자에서 경고 이름을 입력하고 경고를 트리거하는 이벤트에 대한 의미 있는 간단한 설명을 제공합니다.
경고 이름과 설명은 vRealize Log Insight가 보내는 이메일에 포함됩니다.
- 4 **이메일** 확인란을 선택하고 vRealize Log Insight에서 보내는 알림을 받을 이메일 주소를 입력합니다.
쉼표를 사용하여 여러 주소를 구분합니다.
- 5 경고 임계값을 설정합니다.

경고 유형	선택
모든 일치	일치 항목에서 옵션을 선택합니다. 쿼리는 5분마다 실행됩니다.
이벤트 유형 기반	새 이벤트 유형이 확인될 때 옵션을 선택합니다. 쿼리는 5분마다 실행됩니다.

경고 유형	선택
일정 기간 이내의 이벤트 수 기준	세 번째 옵션을 선택하고 드롭다운 메뉴를 사용하여 매개 변수를 설정합니다. 쿼리는 드롭다운 메뉴의 선택 항목을 기준으로 실행됩니다.
차트 값 기준	네 번째 옵션을 선택하고 드롭다운 메뉴를 사용하여 매개 변수를 구성합니다. 참고 이 경고 유형은 하나 이상의 필드에 따라 이벤트를 그룹화하도록 선택하는 경우에만 사용할 수 있습니다. 시계열만 시각화하는 차트에 대해서는 이 경고 유형을 생성할 수 없습니다. 쿼리는 두 번째 드롭다운 메뉴의 선택 항목을 기준으로 실행됩니다.

미리보기 차트의 주황색 라인은 현재 임계값을 보여 줍니다.

6 저장을 클릭합니다.

후속 작업

저장된 경고를 활성화, 비활성화 또는 삭제할 수 있습니다.

참고 경고 쿼리는 사용자에게 따라 다릅니다. 자신의 경고만 관리할 수 있습니다.

Webhook을 사용하여 타사 제품에 경고 보내기 정보

webhook을 사용하여 타사 제품에 vRealize Log Insight 사용자 경고를 보낼 수 있습니다.

vRealize Log Insight에서는 webhook을 사용하여 HTTP POST를 통해 다른 애플리케이션에 경고를 보냅니다. vRealize Log Insight에서는 webhook을 고유한 형식으로 전송하지만 타사 솔루션에서는 webhook을 자사의 고유한 형식으로 수신해야 합니다. vRealize Log Insight webhook을 통해 전송된 정보를 사용하려면 타사 애플리케이션에서 vRealize Log Insight 형식을 기본적으로 지원하거나, shim 형식을 사용하여 vRealize Log Insight 형식과 타사 제품에서 사용하는 형식 사이의 매핑을 생성해야 합니다. shim은 vRealize Log Insight 형식을 다른 형식으로 변환하거나 다른 형식에 매핑합니다.

시스템 알림, 메시지 쿼리로 생성되는 경고, 집계 쿼리로 생성되는 경고에서는 각각 고유한 webhook 형식을 사용합니다.

HTTP 기본 인증이 지원됩니다. {{https://username:password@hostname/path}} 형식을 사용해서 url에 자격 증명을 포함합니다.

시스템 알림을 생성하려면 vRealize Log Insight 관리자여야 합니다.

경고 쿼리를 추가하여 webhook 알림 보내기


로그에 특정 데이터가 나타나는 경우 원격 웹 서버에 webhook 알림을 보내도록 vRealize Log Insight에서 경고 쿼리를 구성할 수 있습니다. webhook은 HTTP POST를 통해 이벤트 알림을 제공합니다.

필수 조건

- vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 https://log_insight-host이고, 여기서 log_insight-host는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

- webhook 알림을 수신할 웹 서버가 구성되어 있는지 확인하십시오.

프로시저

- 대화형 분석 탭으로 이동합니다.
- 검색 버튼 오른쪽에 있는 **경고 만들기 또는 관리** 메뉴에서  아이콘을 클릭하고 **쿼리에서 경고 만들기**를 선택합니다.
- 경고 추가 대화상자에서 경고 이름을 입력하고 경고를 트리거하는 이벤트에 대한 의미 있는 간단한 설명을 제공합니다.
경고 이름과 설명은 vRealize Log Insight가 보내는 알림에 포함됩니다.
- Webhook** 확인란을 선택하고 vRealize Log Insight에서 알림을 보낼 URL을 입력합니다.
- 경고 임계값을 설정합니다.

경고 유형	선택
모든 일치	일치 항목에서 옵션을 선택합니다. 쿼리는 5분마다 실행됩니다.
이벤트 유형 기반	새 이벤트 유형이 확인될 때 옵션을 선택합니다. 쿼리는 5분마다 실행됩니다.
일정 기간 이내의 이벤트 수 기준	세 번째 옵션을 선택하고 드롭다운 메뉴를 사용하여 매개 변수를 설정합니다. 쿼리는 드롭다운 메뉴의 선택 항목을 기준으로 실행됩니다.
차트 값 기준	네 번째 옵션을 선택하고 드롭다운 메뉴를 사용하여 매개 변수를 구성합니다. 참고 이 경고 유형은 하나 이상의 필드에 따라 이벤트를 그룹화하도록 선택하는 경우에만 사용할 수 있습니다. 시계열만 시각화하는 차트에 대해서는 이 경고 유형을 생성할 수 없습니다. 쿼리는 두 번째 드롭다운 메뉴의 선택 항목을 기준으로 실행됩니다.

미리보기 차트의 주황색 라인은 현재 임계값을 보여 줍니다.

- 저장을 클릭합니다.

후속 작업

저장된 경고를 활성화, 비활성화 또는 삭제할 수 있습니다.

참고 경고 쿼리는 사용자에게 따라 다릅니다. 자신의 경고만 관리할 수 있습니다.

vRealize Log Insight 경고를 위한 변환 Shim 쓰기 정보

Shim은 다양한 webhook 형식을 매핑하는 데 사용됩니다.

vRealize Log Insight에서는 webhook을 고유한 형식으로 전송하지만 타사 솔루션에서는 webhook을 자사의 고유한 형식으로 수신해야 합니다. 즉, 타사 솔루션에서 vRealize Log Insight 형식을 기본적으로 지원하거나 vRealize Log Insight와 타사 솔루션 사이에 vRealize Log Insight 형식을 타사 형식으로 변환하는 shim이 필요합니다.

다음 그림은 사용자 경고 쿼리와 해당 쿼리에 대해 생성되는 webhook을 보여 줍니다. 이 정보를 사용하면 shim을 지원하는 데 필요한 매핑을 보다 쉽게 이해할 수 있습니다.

그림 1-1. 사용자 정의 경고 쿼리

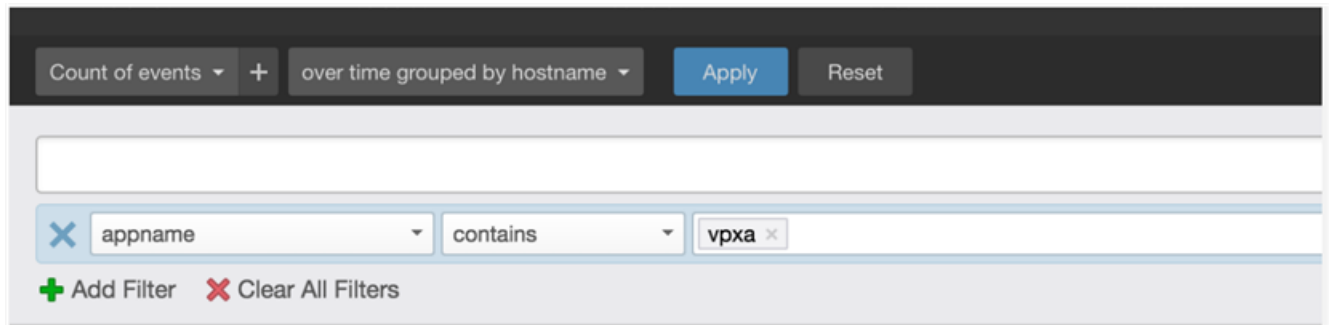


그림 1-2. 사용자 경고 집계 쿼리에 대한 webhook 출력

```
{
  "AlertType":1,
  "AlertName":"ESXi Vpxa Alert",
  "SearchPeriod":300000,
  "HitCount":0.0,
  "HitOperator":2,
  "messages":[
    {
      "text":"2016-06-24T15:42:42.055Z esx01 Vpxa: [4845FB90 verbose 'VpxaHalCnxHostagent' opID=WFU-dcfc2d3a]
[WaitForUpdatesDone] Starting next WaitForUpdates() call to hostd",
      "timestamp":1451940578545,
      "fields":[
        {
          "name":"hostname",
          "content":"esx01"
        },
        {
          "name":"appname",
          "content":"vpxa"
        }
      ]
    },
    {
      "text":"2016-06-24T15:42:42.055Z esx02 Vpxa: [4845FB90 verbose 'vpxavpxaInvtVm' opID=WFU-dcfc2d3a]
[VpxaInvtVmChangeListener] Guest DiskInfo Changed",
      "timestamp":1451940561008,
      "fields":[
        {
          "name":"hostname",
          "content":"esx02"
        },
        {
          "name":"appname",
          "content":"vpxa"
        }
      ]
    }
  ],
  "HasMoreResults":false,
  "Url":"https://10.11.12.13/s/8pgzq6",
}
```

```

"EditUrl":"https://10.11.12.13/s/56monr",
"Info":"This is an alert for all the 'ESXi Vpxa' messages",
"NumHits":2
}

```

사용자 경고 메시지 쿼리에 대한 webhook 형식

vRealize Log Insight webhook에 사용되는 형식은 생성되는 쿼리 유형에 따라 다릅니다. 시스템 알림, 사용자 경고 메시지 쿼리, 집계 사용자 쿼리에서 생성되는 경고는 서로 다른 webhook 형식을 사용합니다.

사용자 경고 메시지 쿼리에서 생성된 경고를 타사 프로그램에 전송할 때 타사 프로그램 형식으로 vRealize Log Insight 정보를 이해할 수 있도록 해주는 shim을 작성해야 합니다.

사용자 경고 메시지 쿼리 webhook 형식

다음 예에서는 사용자 경고 메시지 쿼리에 대한 vRealize Log Insight webhook 형식을 보여 줍니다.

```

{
  "AlertType":1,
  "AlertName":"Hello World Alert",
  "SearchPeriod":300000,
  "HitCount":0.0,
  "HitOperator":2,
  "messages":[
    {
      "text":"hello world 1",
      "timestamp":1451940578545,
      "fields":[
        {
          "name":"Field_1",
          "content":"Content 1"
        },
        {
          "name":"Field_2",
          "content":"Content 2"
        }
      ]
    },
    {
      "text":"hello world 2",
      "timestamp":1451940561008,
      "fields":[
        {
          "name":"Field_1",
          "content":"Content 1_2"
        },
        {
          "name":"Field_2",
          "content":"Content 2_2"
        }
      ]
    }
  ]
}

```

```

],
"HasMoreResults": false,
"Url": "https://10.11.12.13/s/8pgzq6",
"EditUrl": "https://10.11.12.13/s/56monr",
"Info": "This is an alert for all the 'Hello World' messages",
"NumHits": 2
}

```

사용자 경고 집계 쿼리에 대한 webhook 형식

vRealize Log Insight webhook에 사용되는 형식은 생성되는 쿼리 유형에 따라 다릅니다. 시스템 알림, 사용자 경고 메시지 쿼리, 집계 사용자 쿼리에서 생성되는 경고는 서로 다른 webhook 형식을 사용합니다.

타사 프로그램에 시스템 알림을 전송할 때 타사 프로그램 형식으로 vRealize Log Insight 정보를 이해할 수 있도록 해주는 shim을 작성해야 합니다.

사용자 경고 집계 쿼리에 대한 webhook 형식

```

{
  "AlertType": 2,
  "AlertName": "field_1 aggregated alert",
  "SearchPeriod": 300000,
  "HitCount": 2.0,
  "HitOperator": 2,
  "messages": [
    {
      "fields": [
        {
          "name": "Field_1",
          "content": "Content 1"
        }
      ]
    }
  ],
  "HasMoreResults": false,
  "Url": "https://10.11.12.13/s/r25g3s",
  "EditUrl": "https://10.11.12.13/s/n3gsed",
  "Info": null,
  "NumHits": 1
}

```

경고 쿼리 보기

생성한 경고 쿼리를 보고 이러한 쿼리에 대한 알림이 사용되는지 확인할 수 있습니다.

참고 경고 쿼리는 사용자에게 따라 다릅니다. 자신의 경고만 관리할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

1 대화형 분석 탭으로 이동합니다.

2 검색 버튼 오른쪽에 있는 메뉴에서  을 클릭하고 경고 관리를 선택합니다.

모든 경고 쿼리 목록이 표시됩니다. 경고 알림 상태가 경고 이름 아래에 표시됩니다.

후속 작업

목록의 경고 쿼리를 클릭하여 해당 매개 변수를 수정하거나 더 이상 필요하지 않은 쿼리를 삭제할 수 있습니다.

컨텐츠 팩 경고 쿼리는 읽기 전용입니다. 컨텐츠 팩 경고에 대한 변경 내용을 저장하려면 사용자 지정 컨텐츠에 경고를 저장해야 합니다.

경고 쿼리 수정

경고 쿼리의 트리거를 변경하거나, 쿼리가 전송하는 알림을 사용 또는 사용하지 않도록 설정하거나, 알림 방법(이메일, webhook 또는 vRealize Operations Manager로 보내기)을 변경할 수 있습니다.

참고 경고 쿼리는 사용자에 따라 다릅니다. 자신의 경고만 관리할 수 있습니다.


컨텐츠 팩 경고 쿼리는 읽기 전용입니다. 컨텐츠 팩 경고에 대한 변경 내용을 저장하려면 사용자 지정 컨텐츠에 경고를 저장해야 합니다.

변경 내용을 하나 이상의 경고에 동시에 적용할 수 있습니다.

필수 조건

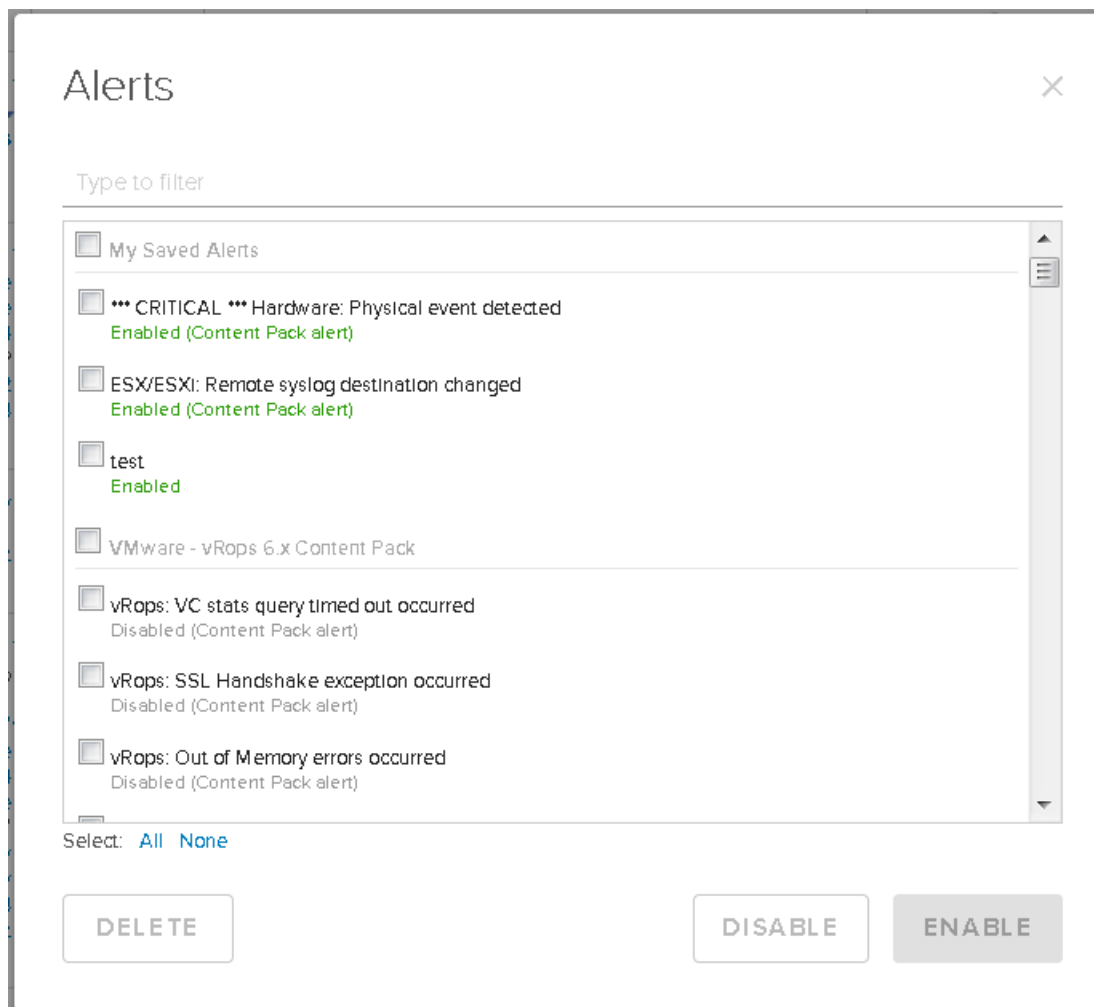
- vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.
- 관리자가 이메일 알림을 사용하도록 SMTP를 구성했는지 확인합니다. [Log Insight에 대한 SMTP 서버 구성](#)을 참조하십시오.
- 관리자가 경고 통합을 사용하도록 vRealize Log Insight 및 vRealize Operations Manager 간 연결을 구성했는지 확인합니다. [vRealize Operations Manager에 알림 이벤트를 전송하도록 Log Insight 구성](#)을 참조하십시오.
- Webhook를 사용하는 경우에는 webhook 알림을 수신할 웹 서버가 구성되어 있는지 확인하십시오.

프로시저

- 1 대화형 분석 탭으로 이동합니다.
- 2 검색 버튼 오른쪽에 있는 **경고 만들기 또는 관리** 메뉴에서  아이콘을 클릭하고 **경고 관리**를 선택합니다.
- 3 [경고] 목록에서 수정할 경고 쿼리를 하나 이상 선택하고 필요에 따라 쿼리 매개 변수를 변경합니다.

문자열을 필터로 입력하여 쿼리를 찾을 수 있습니다. 쿼리는 [사용] 또는 [사용 안 함]으로 레이블이 지정되고 콘텐츠 팩 쿼리인지 여부가 표시됩니다.

참고 모든 알림 옵션을 선택 취소하면 경고 쿼리가 사용되지 않도록 설정됩니다.



4 변경 내용을 저장합니다.

옵션	설명
저장	사용자의 고유한 경고를 수정할 때 이 버튼이 나타납니다.
내 경고에 저장	공유 경고 또는 콘텐츠 팩 경고를 수정할 때 이 버튼이 나타납니다. 원래 경고는 변경되지 않은 상태로 유지되지만 경고 복사본을 사용자 지정 콘텐츠에 저장합니다.

경고 쿼리 사용

경고 쿼리가 사용하지 않도록 설정된 경우 vRealize Log Insight는 이메일 또는 webhook 알림을 보내지 않고 vRealize Operations Manager 알림 이벤트를 트리거하지 않습니다.

참고 경고 쿼리는 사용자에게 따라 다릅니다. 자신의 경고만 관리할 수 있습니다.

경고 쿼리는 다음과 같은 조건에서 사용되지 않도록 설정됩니다.


- [경고 편집] 대화상자에서 모든 알림 옵션을 사용하지 않도록 설정한 경우
- 경고가 콘텐츠 팩의 일부인 경우

콘텐츠 팩 경고 쿼리는 읽기 전용입니다. 콘텐츠 팩 경고에 대한 변경 내용을 저장하려면 사용자 지정 콘텐츠에 경고를 저장해야 합니다.

필수 조건

- vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.
- 관리자가 이메일 알림을 사용하도록 SMTP를 구성했는지 확인합니다. [Log Insight에 대한 SMTP 서버 구성](#)을 참조하십시오.
- 관리자가 경고 통합을 사용하도록 vRealize Log Insight 및 vRealize Operations Manager 간 연결을 구성했는지 확인합니다. [vRealize Operations Manager에 알림 이벤트를 전송하도록 Log Insight 구성](#)을 참조하십시오.

프로시저

- 1 대화형 분석 탭으로 이동합니다.
- 2 검색 버튼 오른쪽에 있는 **경고 만들기 또는 관리** 메뉴에서  아이콘을 클릭하고 **경고 관리**를 선택합니다.
- 3 [경고] 목록에서 사용하도록 설정할 경고 쿼리를 하나 이상 클릭합니다.

4 사용하도록 설정하려는 알림 옵션을 선택하고 필요한 매개 변수를 제공합니다.

옵션	설명
이메일	텍스트 상자에 이메일 주소를 하나 이상 입력합니다. 쉼표를 사용하여 여러 주소를 구분합니다.
webhook	vRealize Log Insight에서 알림을 보낼 URL을 입력합니다.
vRealize Operations Manager로 보내기	vRealize Operations Manager 리소스를 선택하여 알림 이벤트와 연결하고 이벤트의 중요도 수준을 선택합니다.

5 변경 내용을 저장합니다.

옵션	설명
저장	사용자의 고유한 경고를 수정할 때 이 버튼이 나타납니다.
내 경고에 저장	공유 경고 또는 콘텐츠 팩 경고를 수정할 때 이 버튼이 나타납니다. 원래 경고는 변경되지 않은 상태로 유지되지만 경고 복사본을 사용자 지정 콘텐츠에 저장합니다.

경고 쿼리가 경고 조건과 일치하는 결과를 반환하는 경우 vRealize Log Insight는 구성에 따라 알림을 보냅니다.

예: VMware - vSphere 콘텐츠 팩에서 경고 사용

VMware - vSphere 콘텐츠 팩에는 **vCenter Server: ESX/ESXi가 로깅을 중지함** 경고를 비롯한 여러 가지 사전 정의된 경고 쿼리가 포함되어 있습니다.

vRealize Log Insight를 다시 시작할 때 특정 버전의 ESXi 호스트가 syslog 데이터 보내기를 중지할 수 있으므로 **vCenter Server: ESX/ESXi가 로깅을 중지함** 경고를 사용하도록 설정하는 것이 좋습니다. 이 경고는 vCenter Server 이벤트 esx.problem.vmsyslogd.remote.failure를 모니터링하여 syslog 보내기를 중지한 ESXi 호스트가 있는지 감지합니다.

- 1 대화형 분석 탭에서 검색 버튼 오른쪽의 드롭다운 메뉴를 확장하고 **경고 관리**를 선택합니다.
- 2 VMware - vSphere 콘텐츠 팩 아래에서 **vCenter Server: ESX/ESXi가 로깅을 중지함**을 클릭합니다.
- 3 이메일 알림, webhook 알림 또는 vRealize Operations Manager 알림 이벤트를 사용하도록 설정합니다.
- 4 **내 경고에 저장**을 클릭합니다.

vRealize Log Insight의 인스턴스에 피드 보내기를 중지하는 ESXi 호스트만 감지하려면 **vc_remote_host (VMware - vSphere) contains <log-insight-hostname>** 필터를 경고 쿼리에 추가하고 경고에 새 쿼리를 저장할 수 있습니다.

syslog 문제와 솔루션에 대한 자세한 내용은 <https://kb.vmware.com/kb/2003127>에 있는 기술 자료 문서 VMware ESXi 5.x 호스트가 원격 서버로의 syslog 전송 중지(2003127)를 참조하십시오.

경고 쿼리 삭제



더 이상 필요하지 않은 경우 경고 쿼리를 삭제할 수 있습니다.

참고 경고 쿼리는 사용자에게 따라 다릅니다. 자신의 경고만 관리할 수 있습니다.

필수 조건

vRealize Log Insight 웹 사용자 인터페이스에 로그인했는지 확인합니다. URL 형식은 `https://log_insight-host`이고, 여기서 `log_insight-host`는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

프로시저

- 1 대화형 분석 탭으로 이동합니다.
- 2 검색 버튼 오른쪽에 있는 메뉴에서  을 클릭하고 **경고 관리**를 선택합니다.
- 3 삭제할 경고를 하나 이상 선택하고 **삭제** 또는 삭제 아이콘  을 클릭합니다.
- 4 **경고 삭제** 대화상자에서 **삭제**를 선택하여 작업을 확인합니다.