

vRealize Log Insight 시작

2022년 5월 24일

vRealize Log Insight 8.0

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

<https://docs.vmware.com/kr/>

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

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

목차

vRealize Log Insight 시작 4

1 vRealize Log Insight를 설치하기 전에 5

vRealize Log Insight에서 지원되는 로그 파일 및 아카이브 형식 5

보안 요구 사항 6

제품 호환성 6

최소 요구 사항 7

vRealize Log Insight 배포 계획 9

vRealize Log Insight 가상 장치 크기 조정 11

vRealize Log Insight와 vRealize Operations Manager 통합 12

2 이벤트 수명 주기 14

이벤트 수명 주기의 주요 측면 15

3 vRealize Log Insight 설치 17

vRealize Log Insight 가상 장치 배포 17

새 vRealize Log Insight 배포 시작 20

기존 배포에 참여 22

4 고객 환경 향상 프로그램 24

vRealize Log Insight 시작

vRealize Log Insight용 "시작하기"에서는 로그 메시지를 수신하기 위해 vRealize Log Insight 가상 장치의 크기를 지정하는 방법을 포함하여 VMware® vRealize™ Log Insight™를 배포하고 구성하는 방법에 대한 정보를 제공합니다.

배포를 계획하거나 설치하려는 경우 이 정보를 사용하십시오. 이 정보는 가상 시스템 기술과 데이터 센터 운영에 대해 잘 알고 있는 숙련된 Linux 및 Windows 시스템 관리자를 대상으로 작성되었습니다.

vRealize Log Insight를 설치하기 전에

1

사용자 환경에서 vRealize Log Insight를 사용하려면 먼저 vRealize Log Insight 가상 장치를 배포하고 몇 가지 기본 구성을 적용해야 합니다.

본 장은 다음 항목을 포함합니다.

- vRealize Log Insight에서 지원되는 로그 파일 및 아카이브 형식
- 보안 요구 사항
- 제품 호환성
- 최소 요구 사항
- vRealize Log Insight 배포 계획
- vRealize Log Insight 가상 장치 크기 조정
- vRealize Log Insight와 vRealize Operations Manager 통합

vRealize Log Insight에서 지원되는 로그 파일 및 아카이브 형식

vRealize Log Insight를 사용하여 비구조화된 또는 구조화된 로그 데이터를 분석할 수 있습니다.

vRealize Log Insight는 다음 소스에서 데이터를 수락합니다.

- syslog 프로토콜을 통해 로그 스트림 전송을 지원하는 소스.
- 로그 파일을 쓰고 vRealize Log Insight 에이전트를 실행할 수 있는 소스.
- REST API를 통해 HTTP 또는 HTTPS로 로그 데이터를 게시할 수 있는 소스. API 설명서는 vRealize Log Insight 인터페이스(https://<vRLI_host>/rest-api)에서 사용할 수 있습니다.
- vRealize Log Insight에 의해 아카이브된 기록 데이터.

vSphere 로그 구문 분석기를 사용하면 vRealize Log Insight의 vSphere 로그 번들을 가져올 수 있습니다.

참고 vRealize Log Insight이 기존 데이터와 실시간 데이터를 동시에 처리할 수 있더라도 vRealize Log Insight의 개별 인스턴스를 배포하여 가져온 로그 파일을 처리하는 것이 좋습니다.

"vRealize Log Insight 관리"의 [Log Insight 아카이브를 vRealize Log Insight로 가져오기](#)를 참조하십시오.

보안 요구 사항

가상 환경을 외부 공격으로부터 보호하기 위해 지켜야 하는 몇 가지 규칙이 있습니다.

- vRealize Log Insight를 항상 신뢰할 수 있는 네트워크에 설치합니다.
- vRealize Log Insight 지원 번들을 항상 안전한 위치에 저장합니다.

vRealize Log Insight의 보안 구성 요소에 대해 잘 알고 있어야 하는 IT 의사 결정권자, 설계자, 관리자 등은 "vRealize Log Insight 관리"의 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.

가상 환경의 보안에 대한 자세한 내용은 "VMware vSphere 보안 가이드" 및 VMware 웹 사이트의 보안 센터를 참조하십시오.

제품 호환성

vRealize Log Insight는 syslog 프로토콜과 HTTP를 통해 데이터를 수집하며, vCenter Server에 연결하여 이벤트, 작업 및 경고 데이터를 수집할 수 있으며, vRealize Operations Manager와 통합되어 알림 이벤트를 전송하고 컨텍스트에서 실행 기능을 사용하도록 설정할 수 있습니다. 지원되는 제품 버전에 대한 최신 업데이트는 "VMware vRealize Log Insight 릴리스 정보"를 참조하십시오.

가상 장치 배포

vSphere를 사용하여 vRealize Log Insight 가상 장치를 배포해야 합니다. 항상 vSphere Client를 사용하여 vCenter Server에 연결하십시오. vRealize Log Insight 가상 장치는 vCenter Server 버전 5.0 이상으로 관리되는 ESX/ESXi 호스트 버전 5.0 이상에 배포됩니다.

Syslog 피드

vRealize Log Insight는 다음 포트 및 프로토콜을 통해 syslog 데이터를 수집하고 분석합니다.

- 514/UDP
- 514/TCP
- 1514/TCP(SSL)

운영 체제, 애플리케이션, 스토리지, 방화벽 및 네트워크 디바이스와 같은 환경 구성 요소가 자체 syslog 피드를 vRealize Log Insight로 푸시하도록 구성해야 합니다.

API 피드

vRealize Log Insight 수집 API는 다음 포트 및 프로토콜을 통해 데이터를 수집합니다.

- 9000/TCP
- 9543/TCP(SSL)

vSphere 통합

하나 이상의 vCenter Server 인스턴스에서 발생한 작업, 이벤트 및 경보에 대한 데이터를 가져오도록 vRealize Log Insight를 구성할 수 있습니다. vRealize Log Insight는 vSphere API를 사용하여 vCenter Server 시스템에 연결하고 데이터를 수집합니다.

syslog 데이터를 vRealize Log Insight에 전달하도록 ESXi 호스트를 구성할 수 있습니다.

특정 버전의 vCenter Server 및 ESXi와의 호환성 정보에 대해서는 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

vSphere 환경에 연결하는 방법에 대한 자세한 내용은 [vRealize Log Insight를 vSphere 환경에 연결](#)을 참조하십시오.

vRealize Operations Manager 통합

vRealize Log Insight와 vRealize Operations Manager vApp 또는 Installable은 두 가지 독립적인 방법으로 통합할 수 있습니다.

지원되는 모든 버전의 vCenter Operations Manager에서는 컨텍스트에서 실행뿐 아니라 알림도 지원합니다.

- vRealize Log Insight는 vRealize Operations Manager로 알림 이벤트를 전송할 수 있습니다.
[vRealize Operations Manager에 알림 이벤트를 전송하도록 vRealize Log Insight 구성](#)을 참조하십시오.
- vRealize Operations Manager의 컨텍스트에서 실행 메뉴에 vRealize Log Insight에 관련된 작업을 표시할 수 있습니다.
[vRealize Operations Manager에서 vRealize Log Insight에 대해 컨텍스트에서 실행 사용](#)을 참조하십시오.

최소 요구 사항

VMware는 vRealize Log Insight를 OVA 파일 형식의 가상 장치로 배포합니다. 가상 장치를 실행하려면 다양한 리소스 및 애플리케이션을 사용할 수 있어야 합니다. 요구 사항에 대한 최신 정보는 최신 릴리스 정보를 확인하십시오.

가상 하드웨어

vRealize Log Insight 가상 장치를 배포하는 동안 환경의 수집 요구 사항에 따라 사전 설정된 구성 크기 중에서 선택할 수 있습니다. 이러한 사전 설정은 계산 및 디스크 리소스 크기를 조합한 인증된 크기이지만, 나중에 리소스를 더 추가할 수 있습니다. 다음 표에 설명된 소형 구성은 지원되는 상태를 유지하면서 최소 리소스를 소비합니다. 매우 작은 구성도 사용할 수 있지만 데모용으로만 적합합니다.

수집 요구 사항별로 필요한 전체 리소스 요구 사항은 [vRealize Log Insight 가상 장치 크기 조정](#)(을) 참조하십시오.

표 1-1. 소형 구성에 대한 사전 설정된 값

리소스	최소 요구 사항
메모리	8GB
vCPU	4
스토리지 공간	530GB

지원되는 브라우저

다음 브라우저 중 하나를 사용하여 vRealize Log Insight 웹 사용자 인터페이스에 연결할 수 있습니다. 더 최신 브라우저 버전에서도 vRealize Log Insight가 작동할 수 있지만 검증되지는 않았습니다.

중요 브라우저에서 쿠키를 사용하도록 설정해야 합니다.

- Mozilla Firefox 45.0 이상
- Google Chrome 51.0 이상
- Safari 9.1 이상
- Internet Explorer 11.0 이상

참고

- Internet Explorer 문서 모드는 **표준 모드**로 설정해야 합니다. 기타 모드는 지원되지 않습니다.
- **브라우저 모드:** 호환성 보기가 지원되지 않습니다.
- vRealize Log Insight 웹 클라이언트에서 Internet Explorer를 사용하려면 Windows 로컬 스토리지 무결성 수준을 낮춤으로 구성해야 합니다.

계정 암호

유형	요구 사항
루트	<p>OVA를 배포하는 동안 루트 암호를 지정하거나 게스트 사용자 지정을 사용하지 않으면 vRealize Log Insight 가상 장치의 루트 사용자에게 대한 기본 자격 증명은 root/<blank>입니다. vRealize Log Insight 가상 장치 콘솔에 처음 액세스하면 루트 계정 암호를 변경하라는 메시지가 표시됩니다.</p> <p>참고 SSH는 루트 암호를 설정할 때까지 사용할 수 없습니다.</p>
사용자 계정	<p>vRealize Log Insight 3.3 이상에서 만든 사용자 계정에는 강력한 암호가 필요합니다. 암호는 8자 이상이어야 하며 대문자, 소문자, 숫자 및 특수 문자를 각각 하나씩 포함해야 합니다.</p>

통합 요구 사항

제품	요구 사항
vCenter Server	vCenter Server에서 이벤트, 작업 및 경보 데이터를 가져오려면 해당 vCenter Server에 대한 일련의 사용자 자격 증명을 제공해야 합니다. vCenter Server를 사용하여 vRealize Log Insight를 등록 및 등록 취소하기 위해 필요한 최소 역할은 읽기 전용 입니다. 역할은 vCenter Server 수준에서 설정되고 하위 개체로 전파되어야 합니다. vCenter Server가 관리하는 ESXi 호스트를 구성하려면 vRealize Log Insight에 추가적인 권한이 필요합니다.
vSphere ESXi	vRealize Log Insight에 SSL 연결을 설정하려면 vSphere ESXi 6.0 업데이트 1 이상이 필요합니다.
vRealize Operations Manager	vRealize Operations Manager 인스턴스에서 알림 이벤트 및 컨텍스트에서 실행 기능을 사용하려면 해당 vRealize Operations Manager 인스턴스에 사용자 자격 증명을 제공해야 합니다.

네트워크 포트 요구 사항

다음 네트워크 포트를 외부에서 액세스할 수 있어야 합니다.

포트	프로토콜
22/TCP	SSH
80/TCP	HTTP
443/TCP	HTTPS
514/UDP, 514/TCP	Syslog
1514/TCP	SSL을 통한 Syslog 수집만
9000/TCP	vRealize Log Insight 수집 API
9543/TCP	vRealize Log Insight 수집 API(SSL)

vRealize Log Insight 배포 계획

단일 노드, 단일 클러스터 또는 전달자가 있는 클러스터로 vRealize Log Insight를 배포할 수 있습니다.

참고 외부 로드 밸런서는 vRealize Log Insight 클러스터를 포함하는 vRealize Log Insight에서 사용되도록 지원되지 않습니다.

vRealize Suite Lifecycle Manager를 통해 설치

vRealize Suite Lifecycle Manager는 제품군 제품의 설치, 구성, 업그레이드, 패치, 구성 관리, 드리프트 수정 및 상태를 자동화합니다. vRealize Log Insight 설치 대안으로 vRealize Suite Lifecycle Manager를 통해 vRealize Log Insight를 설치할 수 있습니다. vRealize Suite Lifecycle Manager 1.2 이상 및 vRealize Log Insight 4.5.1 이상을 사용해야 합니다. 자세한 내용은 [vRealize Suite Lifecycle Manager 설명서](#)를 참조하십시오.

단일 노드

기본 vRealize Log Insight 구성에는 단일 노드가 포함됩니다. 로그 소스는 애플리케이션, OS 로그, 가상 시스템 로그, 호스트, vCenter Server, 가상 또는 물리적 스위치 및 라우터, 스토리지 하드웨어 등이 될 수 있습니다. 로그 스트림은 syslog (UDP, TCP, TCP+SSL) 또는 CFAPI(HTTP 또는 HTTPS를 통한 vRealize Log Insight 네이티브 수집 프로토콜)를 사용하여 소스에 설치된 vRealize Log Insight 에이전트에 의해 또는 직접 애플리케이션, syslog 집중 장치에 의해 vRealize Log Insight 노드로 전송됩니다.

단일 노드 배포에서 vRealize Log Insight ILB(통합된 로드 밸런서)를 사용하고 쿼리 및 수집 트래픽을 ILB로 전송하는 것이 가장 좋습니다. 이렇게 하면 향후 노드를 추가하여 배포용 클러스터를 생성하려는 경우 오버헤드가 발생하지 않고 구성이 간소화됩니다.

운영 환경에서는 단일 노드를 사용하지 않는 것이 가장 좋습니다.

클러스터

운영 환경에서는 일반적으로 클러스터를 사용해야 합니다. 클러스터는 다음 요구 사항을 충족해야 합니다.

- 클러스터의 노드는 모두 크기가 같고 동일한 데이터 센터에 있어야 합니다.
- 클러스터와 함께 사용되는 ILB의 경우 노드가 동일한 L2 네트워크에 있어야 합니다.
- vRealize Log Insight 가상 시스템은 VMware NSX 분산 방화벽 보호에서 제외해야 합니다.

이는 클러스터의 가상 IP가 로드 밸런싱을 위해 직접 서버 반환 모드(LVS-DR)에서 Linux 가상 서버를 사용하기 때문입니다. 직접 서버 반환은 모든 응답 트래픽이 단일 클러스터 멤버를 통과하도록 라우팅하는 것보다 좀 더 효율적입니다. 그러나 NSX 분산 방화벽에 의해 차단되는 스푸핑된 트래픽과도 유사합니다.

클러스터 크기 조정

vRealize Log Insight 단일 클러스터 구성에서는 3~12개의 노드를 포함할 수 있으며 ILB를 사용합니다. 클러스터가 제대로 작동하려면 최소 3개의 정상 노드가 있어야 합니다.

운영 환경에서는 노드가 적어도 중간 크기여야 합니다. 경고를 포함하여 많은 수의 동시 쿼리로 작업할 것이 예상되는 경우, 대규모 노드를 사용하는 것이 좋습니다. 크기 조정에 대한 자세한 내용은 [vRealize Log Insight 가상 장치 크기 조정](#)을 참조하십시오.

vRealize Log Insight 클러스터의 최소 노드 수가 세 개이나 해당 노드에 오류가 있는 경우, 세 개 미만의 정상 노드를 포함한 클러스터가 제대로 작동하지 않게 됩니다. 또한 클러스터의 정상 노드 수는 클러스터 노드 총 수의 절반 이상이어야 합니다. 예를 들어 사용자에게 6노드 클러스터가 있는 경우 그 중 3개 노드를 사용할 수 없게 된다면, 클러스터에서 작동하지 않는 노드를 제거하지 전까지 해당 클러스터가 제대로 작동하지 않게 됩니다. 클러스터 노드의 제거 및 재도입은 지원되지 않습니다.

전달자가 있는 클러스터

전달자가 있는 vRealize Log Insight 클러스터 구성에는 기본 인덱싱, 스토리지, ILB를 활용하는 3~12개 노드의 쿼리 클러스터가 포함됩니다. 단일 로그 메시지는 단일 클러스터에서와 마찬가지로 기본 클러스터 내 하나의 위치에만 있습니다.

설계는 원격 사이트 또는 클러스터에서 여러 개의 전달자 클러스터를 추가하여 확장됩니다. 각 전달자 클러스터는 해당하는 모든 로그 메시지를 기본 클러스터에 전달하도록 구성되어 있으며 사용자는 기본 클러스터에 연결하여 전달 경로의 압축과 복원을 위해 CFAPI를 활용합니다. TOR(Top-of-Rack)로 구성된 전달자 클러스터는 더 큰 로컬 보존 항목으로 구성되어 있을 수 있습니다.

이중화를 위한 교차 전달

이 vRealize Log Insight 배포 시나리오에는 확장 및 미러링된 전달자가 있는 클러스터가 포함되어 있습니다. 두 개의 기본 클러스터는 인덱싱, 스토리지 및 쿼리에 사용됩니다. 각 데이터 센터에는 하나의 기본 클러스터가 있으며, 각각 전용 전달자 클러스터 쌍으로 프런트 엔드화되어 있습니다. 모든 TOR(Top-of-Rack) 집계의 모든 로그 소스는 전달자 클러스터에 집중됩니다. 두 보존 클러스터 모두에서 동일한 로그를 독립적으로 쿼리할 수 있습니다.

vRealize Log Insight 통합된 로드 밸런서

클러스터의 노드 간에 트래픽을 적절히 유지하고 관리 오버헤드를 최소화하려면 모든 배포에 ILB(통합된 로드 밸런서)를 사용하십시오. 이렇게 하면 일부 vRealize Log Insight 노드를 사용할 수 없게 된 경우에도 수신 수집 트래픽이 수락될 수 있습니다.

vRealize Log Insight 가상 장치 크기 조정

기본적으로, vRealize Log Insight 가상 장치는 소규모 구성에 대한 사전 설정 값을 사용합니다.

독립형 배포

배포 중에 로그를 수집하려는 환경의 요구 사항에 맞게 장치 설정을 변경할 수 있습니다.

vRealize Log Insight에서는 미리 설정된 VM(가상 시스템) 크기를 제공합니다. 따라서 환경의 수집 요구 사항에 맞는 VM 크기를 선택할 수 있습니다. 이러한 사전 설정은 계산 및 디스크 리소스 크기를 조합한 인증된 크기입니다. 또한 나중에 리소스를 더 추가할 수 있습니다. 소규모 구성에서는 최소 리소스만 사용하지만 나머지도 지원됩니다. 매우 작은 구성은 데모용으로만 사용할 수 있습니다.

미리 설정된 크기	로그 수집 비율	가상 CPU	메모리	IOPS	Syslog 연결(활성 TCP 연결)	초당 이벤트 수
매우 작음	6GB/일	2	4GB	75	20	400
작음	30GB/일	4	8GB	500	100	2000
중간	75GB/일	8	16GB	1000	250	5000
큼	225GB/일	16	32GB	1500	750	15,000

Syslog 집계기를 사용하여 vRealize Log Insight에 이벤트를 전송하는 Syslog 연결의 수를 늘릴 수 있습니다. 하지만 초당 최대 이벤트 수는 고정되어 있으며 Syslog 집계자의 사용에 영향을 받지 않습니다.

vRealize Log Insight 인스턴스는 Syslog 집계자로 사용할 수 없습니다.

크기 조정은 다음 가정을 기반으로 합니다.

- 각 가상 CPU는 최소 2GHz입니다.

- 각 ESXi 호스트는 메시지 당 170바이트의 평균 메시지 크기로 초당 최대 10개의 메시지를 전송하고, 이는 대략적으로 150MB/일/호스트에 해당합니다.

참고 대규모 설치에서는 vRealize Log Insight 가상 시스템의 가상 하드웨어 버전을 업그레이드해야 합니다. vRealize Log Insight는 가상 하드웨어 버전 7 이상을 지원합니다. 가상 하드웨어 버전 7은 최대 8개의 가상 CPU를 지원할 수 있습니다. 그러므로 16개의 가상 CPU를 프로비저닝하려면 ESXi 5.x 가상 하드웨어 버전 8 이상으로 업그레이드해야 합니다. vSphere Client를 사용하여 가상 하드웨어를 업데이트하십시오. 가상 하드웨어를 최신 버전으로 업그레이드하려는 경우, VMware 기술 자료 문서 [가상 시스템을 최신 하드웨어 버전으로 업그레이드\(1010675\)](#)의 정보를 숙지하십시오.

클러스터 배포

vRealize Log Insight 클러스터의 기본 및 작업자 노드에 대해서는 중간 구성 또는 더 큰 구성을 사용하십시오. 초당 이벤트 수는 노드 수에 따라 선형으로 증가합니다. 예를 들어 3~12개 노드를 가진 클러스터(클러스터는 최소 3개의 노드를 보유해야 함)에서 12노드 클러스터의 인터넷은 180,000 EPS(초당 이벤트 수)이거나 일별 이벤트 수가 2.7TB입니다.

메모리 크기 줄이기

랩톱의 메모리가 충분하지 않은 경우 **매우 작음** 버전의 장치를 랩톱에서 사용하려면 메모리 크기를 2GB로 줄일 수 있습니다.

vRealize Log Insight 크기 조정 계산기

vRealize Log Insight에 대한 크기 조정 및 네트워크 및 스토리지 활용률을 결정하는 데 도움이 되는 계산기를 사용할 수 있습니다. 이 계산기는 지침 전용으로만 제공됩니다. 많은 환경 정보가 현장에 특정적이므로 계산기는 일부 지역에서 필수적으로 추정값을 사용합니다. <https://www.vmware.com/go/loginsight/calculator> 항목을 참조하십시오.

참고 텍스트 필드에 대해 정규식(예: “**text=~ “Deleting the machine”**”)을 포함하는 복합 또는 다중 조건을 사용하여 전달자를 정의하면 vRealize Log Insight의 전반적인 성능이 저하될 수 있습니다. 그러면 특히 클러스터의 전체 로드가 높은 경우에는 클러스터의 각 노드에서 성능이 지연되고 디스크 블록이 누적될 수 있습니다.

vRealize Log Insight와 vRealize Operations Manager 통합

vRealize Log Insight와 vRealize Operations Manager 간에 통합을 사용하도록 설정하려면 두 제품 모두에서 구성을 수행해야 합니다.

절차

- 1 vRealize Log Insight Management Pack을 vRealize Operations Manager에 설치합니다.

두 제품 간에 컨텍스트에서 실행 기능을 사용하려면 vRealize Log Insight Management Pack이 필요합니다. vRealize Log Insight Management Pack은 vRealize Operations Manager 다운로드 파일 또는 VMware Solution Exchange 웹 사이트를 통해 제공됩니다.

- 2 vRealize Operations Manager에 연결하도록 vRealize Log Insight를 구성합니다.
- 3 vRealize Operations Manager에 정보를 전달하도록 vRealize Log Insight 경고를 구성합니다.
"vRealize Log Insight 관리"에서 [vRealize Operations Manager에 알림 이벤트를 전송하도록 vRealize Log Insight 구성](#)을 참조하십시오.
- 4 vRealize Operations 컨텍스트에서 실행을 사용하여 로그를 vRealize Log Insight에 쿼리합니다.
"vRealize Log Insight 관리"에서 [vRealize Operations Manager에서 vRealize Log Insight에 대해 컨텍스트에서 실행 사용](#)을 참조하십시오.

이벤트 수명 주기

2

vRealize Log Insight를 효과적으로 사용하려면 vRealize Log Insight가 메시지 및 이벤트를 처리하는 방식을 반드시 이해해야 합니다.

로그 메시지 또는 이벤트의 수명 주기는 읽기, 구문 분석, 수집, 인덱싱, 경고, 쿼리 적용, 보관 및 삭제를 포함한 여러 단계로 구성됩니다.

이벤트 및 메시지는 다음 단계를 거쳐 전환됩니다.

- 1 디바이스에서 생성됩니다(vRealize Log Insight 외부).
- 2 다음 방법 중 하나를 사용하여 선택된 후 vRealize Log Insight로 전송됩니다.
 - 수집 API 또는 syslog를 사용하여 vRealize Log Insight 에이전트에 의해
 - syslog를 사용하여 rsyslog, syslog-ng 또는 log4j와 같은 타사 에이전트를 통해
 - 수집 API로의 사용자 지정 쓰기에 의해(예: log4j 어펜더)
 - syslog로의 사용자 지정 쓰기에 의해(예: log4j 어펜더)
- 3 vRealize Log Insight는 이벤트를 수신합니다.
 - ILB(통합된 로드 밸런서)를 사용하는 경우 이벤트는 이벤트 처리를 담당하는 단일 노드로 전송됩니다.
 - 이벤트가 거부되면 클라이언트는 UDP 삭제, 프로토콜 설정을 포함하는 TCP 또는 디스크 백업 대기열을 포함하는 CFAPI를 통해 이러한 거부를 처리합니다.
 - 이벤트가 수락되면 클라이언트에게 알림이 전송됩니다.
- 4 이벤트는 vRealize Log Insight 수집 파이프라인을 통해 전달되며 여기서 다음 단계가 발생합니다.
 - 키워드 인덱스가 생성되거나 업데이트됩니다. 인덱스가 로컬 디스크에 전용 형식으로 저장됩니다.
 - 클러스터 이벤트에 시스템 학습이 적용됩니다.
 - 이벤트가 압축된 전용 형식으로 버킷의 로컬 디스크에 저장됩니다.
- 5 이벤트가 쿼리됩니다.
 - 키워드 및 glob 쿼리를 키워드 인덱스와 비교하여 일치시킵니다.
 - 정규식을 압축된 이벤트와 비교하여 일치시킵니다.

- 6 이벤트가 버킷으로 이동된 후 아카이브됩니다.
 - 버킷은 0.5GB에 도달하면 봉인되고 아카이브됩니다.
- 7 이벤트가 삭제됩니다.
 - 버킷은 FIFO 순서로 삭제됩니다.

추가 정보

자세한 내용은 다음 VMware 기술 자료 비디오를 참조하십시오.



vRealize Log Insight에서 로그 이벤트의 수명 주기

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_horp849x/uiConfId/50138843/)

본 장은 다음 항목을 포함합니다.

- 이벤트 수명 주기의 주요 측면

이벤트 수명 주기의 주요 측면

이벤트에 수명이 있기 때문에 이벤트 스토리지 및 관리에서 이벤트 수명 주기 동안 유의해야 하는 주요 측면이 있습니다.

이벤트 스토리지

각 이벤트는 단일의 디스크 버킷에 저장됩니다. 버킷을 사용할 때는 다음과 같은 동작과 특성을 이해해야 합니다.

- 버킷은 최대 0.5 GB 크기에 도달할 수 있습니다. 버킷이 0.5GB에 도달하면 봉인되고 아카이브를 위해 대기열에 추가됩니다. 봉인된 버킷이 아카이브되면 아카이브된 것으로 표시됩니다. 이벤트는 로컬에 보존되는 동시에 아카이브에도 보존될 수 있습니다.
- 버킷이 vRealize Log Insight 노드 전체에 복제되지 않습니다. 노드가 손실되면 해당 노드의 데이터도 손실됩니다.
- 모든 버킷이 /storage/core 파티션에 저장됩니다.
- vRealize Log Insight는 /storage/core 파티션의 사용 가능한 공간이 3% 미만이 되면 오래된 버킷을 삭제합니다. 삭제는 FIFO 모델을 따릅니다.

참고 일반적으로 /storage/core 파티션은 거의 가득 찬 상태를 유지합니다. 이 파티션은 vRealize Log Insight가 해당 파티션을 관리하므로 절대 100%에 도달하지 않습니다. 그러나 오래된 버킷의 삭제를 방해할 수 있으므로 해당 파티션에 데이터를 저장하지 마십시오.

이벤트 관리

제품을 설치하고 구성할 때 vRealize Log Insight 이벤트 및 이벤트 관리의 다음과 같은 특성 및 동작을 숙지하면 도움이 됩니다.

- 로컬에서 삭제된 이벤트는 명령줄 인터페이스를 사용하여 아카이브에서 가져오지 않는 한 쿼리되지 않습니다.
- 시스템 학습 클러스터에 대한 모든 이벤트가 vRealize Log Insight에서 삭제되면 클러스터가 제거됩니다.
- vRealize Log Insight는 수신되는 모든 이벤트를 자동으로 클러스터의 노드 전체에 균등하게 재조정합니다. 예를 들어 한 노드가 명시적으로 이벤트로 송신되더라도 반드시 해당 노드가 이벤트를 수집하는 것은 아닙니다.
- 이벤트 메타데이터는 데이터베이스가 아닌 단일 vRealize Log Insight 노드에 독점적 형식으로 저장됩니다.
- 이벤트는 노드 및 아카이브에 로컬로 존재할 수 있습니다.

vRealize Log Insight 설치

3

vRealize Log Insight는 vSphere 환경에 배포하는 가상 장치로 제공됩니다.

vRealize Log Insight 가상 장치 크기 조정을 검토한 후 vRealize Log Insight 가상 장치 배포로 이동하십시오. 단일 노드 배포인지 클러스터 방식 배포인지에 관계 없이 이 섹션에서 설명하는 표준 OVF 배포 절차를 따르십시오.

참고 vRealize Suite Lifecycle Manager 1.2 이상을 사용하여 vRealize Log Insight 4.5.1 이상 릴리스를 설치할 수 있습니다. 자세한 내용은 [vRealize Suite 설명서](#)를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- vRealize Log Insight 가상 장치 배포
- 새 vRealize Log Insight 배포 시작
- 기존 배포에 참여

vRealize Log Insight 가상 장치 배포

vRealize Log Insight 가상 장치를 다운로드합니다. VMware는 vRealize Log Insight 가상 장치를 .ova 파일로 배포합니다. vSphere Client를 사용하여 vRealize Log Insight 가상 장치를 배포합니다.

사전 요구 사항

- vRealize Log Insight 가상 장치 .ova 파일의 사본을 가지고 있는지 확인합니다.
- 인벤토리에 OVF 템플릿을 배포할 수 있는 권한이 있는지 확인합니다.
- 환경에 vRealize Log Insight 가상 장치의 최소 요구 사항을 수용하기 위한 충분한 리소스가 있는지 확인합니다. [최소 요구 사항](#)을 참조하십시오.
- 가상 장치 크기 조정에 대한 권장 사항을 읽고 이해했는지 확인합니다. [Log Insight 가상 장치 크기 조정](#)을 참조하십시오.

절차

- 1 vSphere Client에서 **파일 > OVF 템플릿 배포**를 선택합니다.
- 2 **OVF 템플릿 배포** 마법사의 안내를 따릅니다.

- 3 [구성 선택] 페이지에서 로그를 수집할 환경의 크기를 기준으로 vRealize Log Insight 가상 장치의 크기를 선택합니다.

작음은 운영 환경에 대한 최소 요구 사항입니다.

vRealize Log Insight에서는 미리 설정된 VM(가상 시스템) 크기를 제공합니다. 따라서 환경의 수집 요구 사항에 맞는 VM 크기를 선택할 수 있습니다. 이러한 사전 설정은 계산 및 디스크 리소스 크기를 조합한 인증된 크기입니다. 또한 나중에 리소스를 더 추가할 수 있습니다. 소규모 구성에서는 최소 리소스만 사용하지만 나머지도 지원됩니다. 매우 작은 구성은 데모용으로만 사용할 수 있습니다.

미리 설정된 크기	로그 수집 비율	가상 CPU	메모리	IOPS	Syslog 연결(활성 TCP 연결)	초당 이벤트 수
매우 작음	6GB/일	2	4GB	75	20	400
작음	30GB/일	4	8GB	500	100	2000
중간	75GB/일	8	16GB	1000	250	5000
큼	225GB/일	16	32GB	1500	750	15,000

Syslog 집계기를 사용하여 vRealize Log Insight에 이벤트를 전송하는 Syslog 연결의 수를 늘릴 수 있습니다. 하지만 초당 최대 이벤트 수는 고정되어 있으며 Syslog 집계자의 사용에 영향을 받지 않습니다. vRealize Log Insight 인스턴스는 Syslog 집계자로 사용할 수 없습니다.

참고 **큼**을 선택하는 경우 배포 후 vRealize Log Insight 가상 시스템의 가상 하드웨어를 업그레이드해야 합니다.

- 4 [스토리지 선택] 페이지에서 디스크 형식을 선택합니다.

- **느리게 비워지는 썩 프로비저닝**: 기본 썩 포맷의 가상 디스크를 만듭니다. 가상 디스크에 필요한 공간은 가상 디스크 생성 중에 할당됩니다. 물리적 디바이스에 남아 있는 데이터는 가상 디스크를 생성하는 동안에는 지워지지 않지만 나중에 가상 장치에서 해당 데이터에 처음으로 쓰는 경우, 요구에 따라 0으로 설정됩니다.
- **빠르게 비워지는 썩 프로비저닝**: Fault Tolerance와 같은 클러스터링 기능을 지원하는 썩 가상 디스크 유형을 만듭니다. 가상 디스크에 필요한 공간은 디스크 생성 시에 할당됩니다. 플랫폼 형식과 반대로 물리적 디바이스에 남아 있는 데이터는 가상 디스크를 생성하는 동안 0으로 설정됩니다. 다른 유형의 디스크를 생성하는 것보다 이 형식의 디스크를 생성하는 것이 더 오래 걸릴 수 있습니다.

중요 가상 장치의 더 나은 성능과 운영을 위해 가능하면 빠르게 비워지는 썩 프로비저닝된 디스크가 포함된 vRealize Log Insight 가상 장치를 배포합니다.

- **썬 프로비저닝**: 썬 포맷의 디스크를 만듭니다. 디스크는 저장되는 데이터양이 늘어남에 따라 확장됩니다. 스토리지 디바이스가 썬 프로비저닝 디스크를 지원하지 않거나 vRealize Log Insight 가상 장치의 사용되지 않은 디스크 공간을 보존하려는 경우 썬 프로비저닝된 디스크가 포함된 가상 장치를 배포합니다.

참고 vRealize Log Insight 가상 장치에서 디스크 축소는 지원되지 않으며 이 경우 데이터 손상이나 데이터 손실로 이어질 수 있습니다.

- 5 (선택 사항) [네트워크 선택] 페이지에서 vRealize Log Insight 가상 장치에 대한 네트워킹 매개 변수를 설정합니다. IPv4 또는 IPv6 프로토콜을 선택할 수 있습니다.

IP 주소, DNS 서버 및 게이트웨이 정보와 같은 네트워크 설정을 제공하지 않는 경우 vRealize Log Insight에서 DHCP를 활용하여 이러한 설정을 설정합니다.

경고 도메인 이름 서버를 3개 이상 지정하지 마십시오. 도메인 이름 서버를 3개 이상 지정하는 경우 구성된 모든 도메인 이름 서버가 vRealize Log Insight 가상 장치에서 무시됩니다.

쉽포로 구분된 목록을 사용하여 도메인 이름 서버를 지정합니다.

- 6 (선택 사항) [템플릿 사용자 지정] 페이지에서 DHCP를 사용하고 있지 않은 경우 네트워크 속성을 설정합니다.

이중 스택 네트워크에서 가상 시스템을 실행하려면 [애플리케이션]에서 **IPv6 주소 선호** 확인란을 선택합니다.

경고 네트워크에서 지원되는 IPv6에도 순수 IPv4를 사용하려는 경우 **IPv6 주소 선호** 확인란을 선택하지 마십시오. 네트워크가 IPv6에 대해 이중 스택 또는 순수 스택을 지원하는 경우에만 이 확인란을 선택합니다.

- 7 (선택 사항) [템플릿 사용자 지정] 페이지에서 **기타 속성**을 선택하고 vRealize Log Insight 가상 장치에 대한 루트 암호를 설정합니다.

루트 암호는 SSH에 필요합니다. VMware Remote Console을 통해 이 암호를 설정할 수도 있습니다.

- 8 안내에 따라 배포를 완료합니다.

가상 장치 배포에 대한 자세한 내용은 "vApp 및 가상 장치 배포를 위한 사용자 가이드"를 참조하십시오.

가상 장치의 전원을 켜면 초기화 프로세스가 시작됩니다. 초기화 프로세스는 완료하는 데 몇 분이 소요됩니다. 프로세스가 완료되면 가상 장치가 다시 시작됩니다.

- 9 콘솔 탭으로 이동하여 vRealize Log Insight 가상 장치의 IP 주소를 확인합니다.

IP 주소 접두사	설명
https://	가상 장치의 DHCP 구성이 올바릅니다.
http://	가상 장치의 DHCP 구성이 실패했습니다. a vRealize Log Insight 가상 장치의 전원을 끕니다. b 가상 장치를 마우스 오른쪽 버튼으로 클릭하고 설정 편집 을 선택합니다. c 가상 장치의 정적 IP 주소를 설정합니다.

다음에 수행할 작업

- 독립형 vRealize Log Insight 배포를 구성하려면 새 **Log Insight 배포 구성**을 참조하십시오.

vRealize Log Insight 웹 인터페이스는 <https://log-insight-host/>에서 사용할 수 있습니다. 여기서 *log-insight-host*는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

새 vRealize Log Insight 배포 시작

가상 장치 배포 후 또는 클러스터에서 worker 노드 제거 후 처음으로 vRealize Log Insight 웹 인터페이스에 액세스할 때는 초기 구성 단계를 완료해야 합니다.

초기 구성 도중에 수정하는 모든 설정은 관리 웹 사용자 인터페이스에서도 사용할 수 있습니다.

고객 환경 향상 프로그램에 참가할 경우 vRealize Log Insight가 수집하여 VMware로 전송할 수 있는 추적 데이터에 대한 정보는 [장 4 고객 환경 향상 프로그램](#)을 참조하십시오.

사전 요구 사항

- vSphere Client에서 vRealize Log Insight 가상 장치의 IP 주소를 기록합니다. IP 주소 찾기에 대한 자세한 내용은 [vRealize Log Insight 가상 장치 배포](#)를 참조하십시오.
- 지원되는 브라우저를 사용하고 있는지 확인하려면 [최소 요구 사항](#)을 참조하십시오.
- 유효한 라이선스 키가 있는지 확인합니다. <https://my.vmware.com/>의 My VMware™에서 자신의 계정을 사용하여 평가판 또는 영구 라이선스 키를 요청할 수 있습니다.
- 로컬 vCenter Server 또는 Active Directory 자격 증명을 사용하여 vRealize Log Insight를 vRealize Operations Manager와 통합하려면 vRealize Operations Manager 사용자 지정 사용자 인터페이스에서 해당 사용자를 가져와야 합니다. LDAP 구성에 대한 지침은 [vRealize Operations Manager 설명서](#)를 참조하십시오.

절차

- 1 지원되는 브라우저를 사용하여 vRealize Log Insight의 웹 사용자 인터페이스로 이동합니다.
URL 형식은 https://log_insight-host/이며 여기서 *log_insight-host*는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.
초기 구성 마법사가 열립니다.
- 2 **새 배포 시작**을 클릭합니다.
- 3 관리자의 암호를 설정하고 **저장하고 계속**을 클릭합니다.
원하는 경우 관리자의 이메일 주소를 제공할 수 있습니다.
- 4 라이선스 키를 입력하고 **라이선스 키 추가**를 클릭한 후 **저장하고 계속**을 클릭합니다.
- 5 일반 구성 페이지에서 vRealize Log Insight가 전송하는 시스템 알림을 수신할 이메일 주소를 입력합니다.
- 6 webhook를 사용하여 vRealize Operations Manager 또는 타사 애플리케이션으로 알림을 전송하는 경우 **HTTP Post 시스템 알림 전송 대상** 텍스트 상자에 공백으로 구분된 URL 목록을 입력합니다.
- 7 (선택 사항) 고객 환경 향상 프로그램에서 탈퇴하려면 **VMware 고객 환경 향상 프로그램 참여** 옵션을 선택 취소합니다. **저장하고 계속**을 클릭합니다.

- 8 시간 구성 페이지에서 vRealize Log Insight 가상 장치의 시간을 동기화할 방법을 설정하고 **테스트**를 클릭합니다.

옵션	설명
NTP 서버(권장)	기본적으로 vRealize Log Insight는 공개 NTP 서버와 시간을 동기화하도록 구성됩니다. 방화벽 설정으로 인해 외부 NTP 서버에 액세스할 수 없는 경우에는 조직의 내부 NTP 서버를 사용할 수 있습니다. 여러 개의 NTP 서버를 입력할 때는 쉼표로 구분합니다.
ESX/ESXi 호스트	사용할 수 있는 NTP 서버가 없는 경우에는 vRealize Log Insight 가상 장치를 배포한 ESXi 호스트와 시간을 동기화할 수 있습니다.

- 9 **저장하고 계속**를 클릭합니다.

- 10 (선택 사항) 경고 및 시스템 알림 이메일 발송을 사용하도록 설정하려면 SMTP 서버의 속성을 지정합니다.

SMTP 구성이 올바른지 확인하려면 유효한 이메일 주소를 입력하고 **테스트**를 클릭합니다. 그러면 vRealize Log Insight가 지정된 주소로 테스트 이메일을 전송합니다.

- 11 (선택 사항) 사용자 지정 SSL 인증서를 제공하려면 인증서 파일을 PEM 형식으로 클러스터에 업로드합니다. 기존 인증서의 세부 정보를 볼 수도 있습니다.

시스템은 클러스터의 모든 노드에 대한 신뢰 저장소에 인증서를 추가하고 나중에 사용할 수 있도록 저장합니다.

사용자 지정 SSL 인증서의 사전 요구 사항에 대한 자세한 내용은 [사용자 지정 SSL 인증서 설치](#)를 참조하십시오.

- 12 **저장하고 계속**를 클릭합니다.

결과

vRealize Log Insight 프로세스가 다시 시작되면 vRealize Log Insight의 **대시보드** 탭으로 리디렉션됩니다.

다음에 수행할 작업

- **관리** 탭으로 이동합니다. **vSphere 통합** 페이지의 vCenter Server 인스턴스에서 작업, 이벤트 및 경고를 가져오도록 vRealize Log Insight를 구성하고, vRealize Log Insight로 syslog 피드를 보내도록 ESXi 호스트를 구성합니다.
- vRealize Log Insight에 영구 라이선스를 할당합니다. "vRealize Log Insight 관리"에서 [Log Insight에 영구 라이선스 할당](#)을 참조하십시오.
- 컨텍스트에 따라 실행하도록 vRealize Operations Manager에서 vRealize Log Insight 어댑터를 구성하십시오. "vRealize Operations Manager 구성 가이드"에서 "vRealize Operations Manager로 vRealize Log Insight 구성"을 참조하십시오.

- Windows 이벤트 채널, Windows 디렉토리 및 일반 텍스트 로그 파일에서 이벤트를 수집하려면 vRealize Log Insight Windows 에이전트를 설치합니다. "vRealize Log Insight 에이전트 사용"에서 [Windows 에이전트 설치](#)를 참조하십시오.

기존 배포에 참여

독립형 vRealize Log Insight 노드를 배포 및 설정한 후 새 vRealize Log Insight 인스턴스를 배포하고 기존 노드에 추가하여 vRealize Log Insight 클러스터를 형성할 수 있습니다.

vRealize Log Insight는 클러스터에서 여러 가상 장치 인스턴스를 사용하여 수평 확장될 수 있습니다. 클러스터는 수집 처리량의 선형 확장이 가능하며, 쿼리 성능을 높이고, 고가용성 수집을 허용합니다. 클러스터 모드에서 vRealize Log Insight는 기본 및 작업자 노드를 제공합니다. 기본 노드와 작업자 노드는 데이터의 하위 집합을 담당합니다. 기본 노드는 데이터의 모든 하위 집합을 쿼리하고 결과를 집계할 수 있습니다. 사이트 요구를 지원하기 위해 노드가 더 필요할 수도 있습니다. 클러스터에서는 3~12개의 노드를 사용할 수 있습니다. 즉, 제대로 작동하는 클러스터에는 3개 이상의 정상 노드가 있어야 합니다. 더 큰 클러스터에서 대부분의 노드가 정상 상태여야 합니다. 예를 들어, 6노드 클러스터에서 세 개의 노드에 오류가 있는 경우 오류가 있는 노드가 제거될 때까지 모든 노드가 제대로 작동하지 않습니다.

사전 요구 사항

- vSphere Client에서 작업자 vRealize Log Insight 가상 장치의 IP 주소를 기록해 둡니다.
- 기본 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름을 가지고 있는지 확인합니다.
- 기본 vRealize Log Insight 가상 장치에 관리자 계정을 가지고 있는지 확인합니다.
- vRealize Log Insight 기본 및 작업자 노드의 버전이 동기화된 상태인지 확인합니다. 최신 버전의 vRealize Log Insight 기본 노드에 더 이전 버전의 vRealize Log Insight 작업자 노드를 추가하지 마십시오.
- vRealize Log Insight 가상 장치의 시간을 NTP 서버의 시간과 동기화해야 합니다. [Log Insight 가상 장치의 시간 동기화](#)를 참조하십시오.
- 지원되는 브라우저 버전에 대한 자세한 내용은 [vRealize Log Insight 릴리스 정보](#)를 참조하십시오.

절차

- 1 지원되는 브라우저를 사용하여 vRealize Log Insight 작업자의 웹 사용자 인터페이스로 이동합니다.
URL 형식은 `https://log_insight-host/`이고 여기서 `log_insight-host`는 vRealize Log Insight 작업자 가상 장치의 IP 주소 또는 호스트 이름입니다.
초기 구성 마법사가 열립니다.
- 2 **기존 배포에 참여**를 클릭합니다.
- 3 vRealize Log Insight 기본의 IP 주소 또는 호스트 이름을 입력하고 **이동**을 클릭합니다.
작업자는 기존 배포에 참여하기 위해 vRealize Log Insight 기본 노드에 요청을 전송합니다.
- 4 **클러스터 관리 페이지에 액세스하려면 여기를 클릭하십시오.**를 클릭합니다.

5 관리자로 로그인합니다.

클러스터 페이지가 로드됩니다.

6 **허용**을 클릭합니다.

작업자 노드는 기존 배포에 참여하고 vRealize Log Insight는 클러스터에서 작동하기 시작합니다.

다음에 수행할 작업

- 필요에 따라 작업자 노드를 더 추가합니다. 클러스터에 3개 이상의 노드가 있어야 합니다.

고객 환경 향상 프로그램

4

이 제품은 VMware의 CEIP(고객 환경 향상 프로그램)에 참여하는 제품입니다.

CEIP를 통해 수집되는 데이터와 VMware에서 이러한 데이터를 사용하는 목적과 관련된 세부 정보는 신뢰 및 보장 센터(<https://www.vmware.com/solutions/trustvmware/ceip.html>)에 명시되어 있습니다.

이 제품에 대한 CEIP에 참여하거나 참여를 중지하려면 "vRealize Log Insight 관리"의 "VMware 고객 환경 향상 프로그램 참여 또는 참여 중지"를 참조하십시오.