

vRealize Log Insight 관리

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

Copyright © 2022 VMware, Inc. All rights reserved. 저작권 및 상표 정보

목차

vRealize Log Insight 관리 7

1 vRealize Log Insight 업그레이드 8

vRealize Log Insight 업그레이드 경로 8

Photon에서 vRealize Log Insight 8.0으로 업그레이드 8

vRealize Log Insight 4.0 이상으로 업그레이드 9

vRealize Log Insight 3.6으로 업그레이드 10

2 vRealize Log Insight 사용자 계정 관리 12

사용자 관리 개요 12

역할 기반 액세스 제어 13

필터링을 사용하여 사용자 계정 관리 13

vRealize Log Insight에서 새 사용자 계정 생성 14

vRealize Log Insight의 한 Active Directory 그룹에 대한 VMware Identity Manager 액세스 구성 15

vRealize Log Insight로 Active Directory 그룹 가져오기 17

크로스-도메인 그룹 멤버 자격으로 사용자 인증 18

데이터 집합 정의 18

역할 생성 및 수정 19

vRealize Log Insight에서 사용자 계정 또는 그룹 삭제 20

3 인증 구성 22

VMware Identity Manager를 통해 사용자 인증 사용 22

Active Directory를 통해 사용자 인증 활성화 24

Active Directory에 사용할 프로토콜 구성 25

4 vRealize Log Insight 구성 27

vRealize Log Insight 구성 제한 27

데이터 보존 구성 28

가상 장치 설정 구성 29

vRealize Log Insight 가상 장치에 대한 루트 SSH 암호 구성 29

vRealize Log Insight 가상 장치의 네트워크 설정 변경 30

vRealize Log Insight 가상 장치의 스토리지 용량 늘리기 31

vRealize Log Insight 가상 장치에 메모리 및 CPU 추가 32

vRealize Log Insight에 라이선스 할당 33

로그 저장 정책 34

시스템 알림 관리 34

시스템 알림	35
vRealize Log Insight 시스템 알림에 대한 대상 구성	39
vRealize Log Insight 이벤트 전달 대상 추가	42
대화형 분석에서 이벤트 전달 필터 사용	45
vRealize Log Insight 가상 장치의 시간 동기화	45
vRealize Log Insight에 대한 SMTP 서버 구성	46
사용자 지정 SSL 인증서 설치	47
자체 서명된 인증서 생성	49
인증서 서명 요청 생성	50
인증 기관의 서명 요청	51
인증서 파일 연결	51
서명된 인증서 업로드	52
vRealize Log Insight 서버 및 Log Insight Agents 간 SSL 연결 구성	52
SSL 인증서 보기 및 제거	56
vRealize Log Insight 웹 세션에 대한 기본 시간 초과 기간 변경	57
아카이브	57
vRealize Log Insight에서 데이터 아카이브 활성화 또는 비활성화	57
vRealize Log Insight 아카이브 파일 형식	59
vRealize Log Insight로 vRealize Log Insight 아카이브 가져오기	59
Log Insight 아카이브를 원시 텍스트 파일 또는 JSON으로 내보내기	60
vRealize Log Insight 서비스 다시 시작	61
vRealize Log Insight 가상 장치의 전원 끄기	62
vRealize Log Insight 지원 번들 다운로드	62
VMware 고객 환경 개선 프로그램 가입 또는 탈퇴	64
5 vRealize Log Insight 클러스터 관리	65
vRealize Log Insight 클러스터에 작업자 노드 추가	65
vRealize Log Insight 가상 장치 배포	65
기존 배포에 참여	68
vRealize Log Insight 클러스터에서 작업자 노드 제거	69
통합된 로드 밸런서 사용	70
통합된 로드 밸런서 사용	71
운영 환경 내 클러스터 검사의 결과 쿼리	72
6 포트 및 외부 인터페이스	73
7 vRealize Log Insight 에이전트의 상태 모니터링	77
8 서버에서 에이전트 자동 업데이트 사용	79

9	중앙 집중식 에이전트 구성 및 에이전트 그룹	80
	에이전트 그룹 구성 병합	81
	에이전트 그룹 생성	81
	에이전트 그룹 편집	83
	컨텐츠 팩 에이전트 그룹을 에이전트 그룹으로 추가	84
	에이전트 그룹 삭제	85
10	vRealize Log Insight 모니터링	86
	vRealize Log Insight 가상 장치의 상태 확인	86
	로그 이벤트를 전송하는 호스트 모니터링	87
	비활성 호스트를 보고하도록 시스템 알림 구성	88
11	vRealize Log Insight와 VMware 제품 통합	90
	vSphere 환경에 vRealize Log Insight 연결	91
	Syslog 서버 역할의 vRealize Log Insight	93
	로그 이벤트를 vRealize Log Insight으로 전달하도록 ESXi 호스트 구성	93
	vRealize Log Insight에 로그 이벤트를 전달하기 위해 ESXi 호스트 구성 수정	95
	vRealize Operations Manager의 vRealize Log Insight 알림 이벤트	96
	vCenter Server 인스턴스에서 이벤트, 작업 및 정보를 풀(pull)하도록 vRealize Log Insight 구성	97
	vRealize Log Insight에서 vRealize Operations Manager 사용	98
	vRealize Operations Manager와의 통합을 위한 요구 사항	98
	vRealize Operations Manager에 알림 이벤트를 전송하도록 vRealize Log Insight 구성	100
	vRealize Operations Manager에서 vRealize Log Insight에 대한 컨텍스트에서 실행 기능 활성화	101
	vRealize Operations Manager에서 vRealize Log Insight에 대한 컨텍스트에서 실행 기능 비활성화	106
	DNS 검색 경로 및 도메인 추가	106
	vRealize Log Insight 어댑터 제거	107
	vRealize Log Insight용 vRealize Operations Manager 컨텐츠 팩	108
12	vRealize Log Insight에 대한 보안 고려 사항	110
	포트 및 외부 인터페이스	110
	vRealize Log Insight 구성 파일	113
	vRealize Log Insight 공용 키, 인증서 및 키 저장소	114
	vRealize Log Insight 라이선스 및 EULA 파일	114
	vRealize Log Insight 로그 파일	115
	사용자 감사 로그 메시지에 디버그 수준 사용 설정	117
	vRealize Log Insight의 감사 로그	118
	vRealize Log Insight 사용자 계정	118
	vRealize Log Insight 방화벽 권장 사항	119

보안 업데이트 및 패치 120

13 백업, 복원 및 재해 복구 121

백업, 복원 및 재해 복구 개요 121

정적 IP 주소 및 FQDN 사용 122

계획 및 준비 123

노드 및 클러스터 백업 124

Linux 또는 Windows 에이전트 백업 125

노드 및 클러스터 복원 125

복원 후 구성 변경 126

동일한 호스트로 복원 126

다른 호스트로 복원 127

복원 확인 130

재해 복구 131

14 vRealize Log Insight 문제 해결 132

Internet Explorer에서 vRealize Log Insight에 로그인할 수 없음 132

vRealize Log Insight의 디스크 공간 부족 133

아카이브된 데이터 가져오기가 실패할 수 있음 133

가상 장치 콘솔을 사용하여 vRealize Log Insight의 지원 번들 생성 134

관리자 암호 재설정 134

루트 사용자 암호 재설정 135

경고를 vRealize Operations Manager로 전달할 수 없음 137

Active Directory 자격 증명을 사용하여 로그인할 수 없음 137

STARTTLS 옵션이 활성화된 경우 SMTP가 작동하지 않음 138

.pak 파일의 서명을 검증할 수 없어서 업그레이드가 실패함 139

내부 서버 오류와 함께 업그레이드 실패 140

VMware 제품과 통합한 후 첫 번째 로그 메시지에서 vmw_object_id 필드가 누락됨 140

vRealize Log Insight 관리

"vRealize Log Insight 관리"에서는 사용자 계정 관리 방법 및 다른 VMware 제품과의 통합을 구성하는 방법을 포함하여 VMware® vRealize™ Log Insight™ 관리에 대한 정보를 제공합니다. 또한 제품 보안 관리 및 배포 업그레이드에 대한 정보도 포함됩니다.

이 정보는 가상 시스템 기술과 데이터 센터 운영에 대해 잘 알고 있는 숙련된 Windows 또는 Linux 시스템 관리자를 대상으로 작성되었습니다.

vRealize Log Insight 업그레이드

1

중분 업그레이드 경로에 따라 vRealize Log Insight를 버전 8.0로 업그레이드할 수 있습니다. 업그레이드에는 클러스터의 자동 업그레이드가 포함됩니다.

vRealize Log Insight를 위해 PAK 파일을 다운로드하려면 [VMware vRealize Log Insight 다운로드 페이지](#)로 이동합니다.

본 장은 다음 항목을 포함합니다.

- vRealize Log Insight 업그레이드 경로
- Photon에서 vRealize Log Insight 8.0으로 업그레이드
- vRealize Log Insight 4.0 이상으로 업그레이드
- vRealize Log Insight 3.6으로 업그레이드

vRealize Log Insight 업그레이드 경로

따라야 하는 업그레이드 경로는 업그레이드하려는 설치된 vRealize Log Insight 버전에 따라 다릅니다.

vRealize Log Insight 업그레이드는 중분 방식으로 수행되어야 합니다. 예를 들어 버전 4.5에서 버전 4.7로 업그레이드하려면 4.6 업그레이드를 4.5에 적용한 후 4.6에서 4.7로 업그레이드합니다. 각 중간 릴리스로 업그레이드해야 합니다.

[VMware 제품 상호 운용성 매트릭스](#) 사이트에서 지원되는 업그레이드 경로를 확인할 수도 있습니다.

Photon에서 vRealize Log Insight 8.0으로 업그레이드

SLES 운영 체제의 vRealize Log Insight 4.8에서 Photon 운영 체제의 vRealize Log Insight 8.0으로 업그레이드할 수 있습니다.

vRealize Log Insight 8.0으로 업그레이드하는 방법에 대한 자세한 내용은 [업그레이드 참고](#)를 참조하십시오.

업그레이드

SLES 기반 vRealize Log Insight 4.8에서 Photon 기반 vRealize Log Insight 8.0으로 업그레이드하는 것은 기본 운영 체제가 변경되므로 이전 업그레이드와는 다릅니다. 이 업그레이드는 vRealize Log Insight 가상 장치에 있는 각 가상 시스템의 아키텍처를 변경합니다.

예를 들어, 부팅(SDA1), 스왑(SDA2) 및 루트(SDA3)용 파티션 3개를 포함하는 디스크 SDA가 있는 가상 시스템을 고려해 보십시오. 파티션 SDA3의 크기는 약 16GB이며 SLES에 대한 정보를 포함합니다. SLES 기반 vRealize Log Insight 4.8에서 Photon 기반 vRealize Log Insight 8.0으로 업그레이드하면 SDA3에 또 다른 파티션이 생성되고 각각 약 8GB 크기의 두 부분, 즉 SLES용 1개(SDA3)와 Photon용 1개(SDA4)로 동일하게 분할됩니다. SDA4가 활성 파티션이 됩니다. SDA3는 비활성 상태로 유지되지만 SLES에 대한 유효한 vRealize Log Insight 정보를 포함합니다. 가상 시스템을 부팅할 때 수동으로 선택하여 SDA3를 부팅할 수 있습니다.

참고 SLES 기반 vRealize Log Insight 4.8에서 Photon 기반 vRealize Log Insight 8.0으로 업그레이드하기 전에 루트 파티션에 업그레이드를 위한 충분한 공간이 있는지 확인합니다. 루트 파티션의 크기가 더 작은 경우(예: 8GB) 디스크 크기를 20GB로 늘려 루트 파티션 크기를 16GB로 늘립니다. 공간이 적은 루트 파티션이 있는 각 노드에 대한 디스크 크기를 늘려야 합니다. 루트 파티션 크기를 늘리는 방법에 대한 자세한 내용은 <https://kb.vmware.com/s/article/76304> 항목을 참조하십시오.

Photon 기반 vRealize Log Insight 8.0으로 업그레이드한 후:

- 사용자 인터페이스 또는 REST API는 변경되지 않습니다.
- 명령줄에서 vRealize Log Insight 8.0 가상 시스템에 연결하여 작업하는 경우 SLES는 `initd`를 기준으로 하지만 Photon은 `systemd`를 기준으로 하므로 `systemd` 기반 정보가 표시됩니다.

롤백

SLES 기반 vRealize Log Insight 4.8에서 Photon 기반 vRealize Log Insight 8.0으로 업그레이드하지 못하는 경우 자동화된 롤백이 발생하지 않습니다. 그러나 수동 롤백하여 SLES 기반 vRealize Log Insight로 되돌릴 수 있습니다. 자세한 내용은 <https://kb.vmware.com/s/article/75150> 항목을 참조하십시오.

vRealize Log Insight 4.0 이상으로 업그레이드

클러스터를 vRealize Log Insight 4.0 이상의 점점 높은 버전으로 업그레이드할 수 있습니다. 예를 들어 버전 3.6에서 버전 4.3으로 업그레이드하려면 4.0 업그레이드를 3.6에 적용한 후 4.0에서 4.3으로 업그레이드합니다.

vRealize Log Insight 업그레이드 작업은 기본 노드의 FQDN에서 수행해야 합니다. 통합된 로드 밸런서 IP 주소를 사용한 업그레이드는 지원되지 않습니다.

업그레이드 중에 기본 노드가 먼저 업그레이드된 후 다시 시작됩니다. 각 클러스터 노드가 순차적으로 업그레이드됩니다. **관리 > 클러스터** 페이지에서 롤링 업그레이드의 상태를 확인할 수 있습니다. 통합된 로드 밸런서가 구성되면 해당 IP가 클러스터 노드 간에 마이그레이션되므로 롤링 업그레이드가 진행되는 동안 수신 이벤트의 UI, API 및 수집을 비롯한 클러스터 서비스를 계속 사용할 수 있습니다. 하위 수준 세부 정보는 개별 노드의 `/storage/core/loginsight/var/upgrade.log` 파일에 기록됩니다. 업그레이드가 성공적으로 완료되면 시스템 알림이 전송됩니다.


업그레이드 프로세스 동안 하나 이상의 노드에 영향을 미치는 문제가 발생하는 경우 전체 클러스터가 원래의 작업 버전으로 롤백됩니다. 업그레이드가 시작된 후에 수행된 구성 변경 사항이 일관되지 않거나 유효하지 않을 수 있으므로 구성이 업그레이드 이전에 캡처된 잘 알려진 정상 상태로 되돌아갑니다. 수집된 이벤트는 손실되지 않습니다. 진행률은 개별 노드의 `/storage/core/loginsight/var/rollback.log` 파일에 기록됩니다. 롤백이 완료되면 시스템 알림이 전송됩니다. 문제를 조사하여 수정한 후에 업그레이드를 다시 시도할 수 있습니다.

업그레이드 후에 모든 노드는 연결된 상태가 되고, 업그레이드 전에 유지 보수 모드였더라도 온라인 상태가 됩니다.

사전 요구 사항

- 버전 vRealize Log Insight에 올바른 업그레이드를 적용하려는 것인지 확인합니다. 지원되는 업그레이드 경로에 대한 자세한 내용은 [vRealize Log Insight 업그레이드 경로](#)를 참조하십시오.
- vRealize Log Insight 가상 장치의 스냅샷 또는 백업 복사본을 생성합니다.
- 업그레이드하려는 릴리스에 대한 vRealize Log Insight 업그레이드 번들 .pak 파일의 복사본을 받습니다.
- 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.
- 유지 보수 모드에 있는 업그레이드하는 노드를 모두 적어둡니다. 업그레이드가 완료되면 연결된 상태에서 유지 보수 모드로 전환해야 합니다.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **클러스터**를 클릭합니다.
- 3 **PAK에서 업그레이드**를 클릭하여 .pak 파일을 업로드합니다.
- 4 새로운 EULA를 수락하여 업그레이드 절차를 완료합니다.

다음에 수행할 작업

마스터 노드 업그레이드 프로세스가 완료되면 자동으로 수행되는 남은 업그레이드 프로세스를 볼 수 있습니다.

관리자에게 전송된 이메일을 확인하여 업그레이드가 성공적으로 완료되었는지 확인합니다.

업그레이드 후 모든 노드는 업그레이드 전에 유지 보수 모드였더라도 온라인 상태가 됩니다. 필요한 경우 이러한 노드를 다시 유지 보수 모드로 전환합니다.

vRealize Log Insight 3.6으로 업그레이드

클러스터를 vRealize Log Insight 3.6으로 자동으로 업그레이드할 수 있습니다.

vRealize Log Insight 업그레이드 작업은 기본 노드의 FQDN에서 수행해야 합니다. 통합된 로드 밸런서 IP 주소를 사용한 업그레이드는 지원되지 않습니다.


업그레이드 중에 기본 노드가 먼저 업그레이드된 후 다시 시작됩니다. 그런 다음 각 클러스터 노드가 순차적으로 업그레이드됩니다. **관리 > 클러스터** 페이지에서 롤링 업그레이드의 현재 상태를 확인할 수 있습니다. 통합된 로드 밸런서가 구성되면 해당 IP가 클러스터 노드 간에 마이그레이션되므로 롤링 업그레이드가 진행되는 동안 수신 이벤트의 UI, API 및 수집을 비롯한 클러스터 서비스를 계속 사용할 수 있습니다. 각 개별 노드의 upgrade.log 파일에 자세한 정보가 기록됩니다. 업그레이드가 성공적으로 완료되면 시스템 알림이 전송됩니다.

업그레이드 프로세스 동안 하나 이상의 노드에 영향을 미치는 문제가 발생하는 경우 전체 클러스터가 원래의 작업 버전으로 자동으로 롤백됩니다. 업그레이드가 시작된 후에 수행된 구성 변경 사항이 일관되지 않거나 유효하지 않을 수 있으므로 구성이 업그레이드 이전에 캡처된 잘 알려진 정상 상태로 되돌아갑니다. 수집된 이벤트는 손실되지 않습니다. 각 개별 노드의 rollback.log 파일에 진행 사항이 기록됩니다. 롤백이 완료되면 시스템 알림이 전송됩니다. 문제를 조사하여 수정한 후에 업그레이드를 다시 시도할 수 있습니다.

사전 요구 사항

- 지원되는 업그레이드 경로에 대해 업그레이드를 적용하는지 확인합니다. [vRealize Log Insight 업그레이드 경로](#) 항목을 참조하십시오.
- vRealize Log Insight 가상 장치의 스냅샷 또는 백업 복사본을 생성합니다.
- 업그레이드하려는 릴리스에 대한 vRealize Log Insight 업그레이드 번들 .pak 파일의 복사본을 받습니다.
- 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.

절차

- 1 구성 드롭다운 메뉴 아이콘  을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **클러스터**를 클릭합니다.
- 3 **PAK에서 업그레이드**를 클릭하여 .pak 파일을 업로드합니다.
- 4 새로운 EULA를 수락하여 업그레이드 절차를 완료합니다.

다음에 수행할 작업

기본 노드 업그레이드 프로세스가 완료되면 자동으로 수행되는 남은 업그레이드 프로세스를 볼 수 있습니다.

관리자에게 전송된 이메일을 확인하여 업그레이드가 성공적으로 완료되었는지 확인합니다.

vRealize Log Insight 사용자 계정 관리

2

관리자는 사용자 계정 및 역할을 생성하여 vRealize Log Insight 웹 인터페이스에 대한 액세스를 제공할 수 있습니다.

관리 편집 권한을 가진 사용자만 사용자 계정을 생성하고 편집할 수 있습니다. 하지만 사용자는 관리 편집 권한 없이 자신의 고유한 이메일 및 계정 암호를 변경할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 사용자 관리 개요
- 역할 기반 액세스 제어
- 필터링을 사용하여 사용자 계정 관리
- vRealize Log Insight에서 새 사용자 계정 생성
- vRealize Log Insight의 한 Active Directory 그룹에 대한 VMware Identity Manager 액세스 구성
- vRealize Log Insight로 Active Directory 그룹 가져오기
- 크로스-도메인 그룹 멤버 자격으로 사용자 인증
- 데이터 집합 정의
- 역할 생성 및 수정
- vRealize Log Insight에서 사용자 계정 또는 그룹 삭제

사용자 관리 개요

시스템 관리자는 사용자 로그인, 역할 기반 액세스 제어, 사용 권한, 데이터 집합 등을 결합 사용하여 vRealize Log Insight 사용자를 관리할 수 있습니다. 역할 기반 액세스 제어를 통해 관리자는 사용자와 해당 사용자가 수행할 수 있는 작업을 관리할 수 있습니다.

역할은 특정 작업을 수행하는 데 필요한 사용 권한의 집합입니다. 시스템 관리자는 보안 정책을 정의하는 과정에서 역할을 정의하고 역할을 사용자에게 부여합니다. 특정 역할에 연결된 사용 권한 및 작업을 변경하려면 시스템 관리자가 역할 설정을 업데이트합니다. 업데이트된 설정은 해당 역할에 연결된 모든 사용자에게 적용됩니다.

- 사용자가 작업을 수행할 수 있도록 허용하려면 시스템 관리자가 사용자에게 역할을 부여합니다.
- 사용자가 작업을 수행하지 못하게 차단하려면 시스템 관리자가 사용자의 역할을 해지합니다.

각 사용자의 액세스 권한, 역할 및 사용 권한은 사용자 로그인 계정에 기반하여 관리할 수 있습니다. 개별 사용자에게 여러 역할 및 사용 권한이 부여될 수 있습니다.

특정 개체를 보거나 액세스할 수 없는 사용자 또는 특정 작업을 수행할 수 없는 사용자는 해당 작업을 수행할 사용 권한을 부여받지 않은 것입니다.

역할 기반 액세스 제어

시스템 관리자는 역할 기반 액세스 제어를 사용하여 특정 사용자에게 대한 로그 액세스 권한을 제한하고 로그인 후 이러한 사용자가 수행할 수 있는 작업을 제어할 수 있습니다. 시스템 관리자는 사용자 로그인 계정에 사용 권한 및 역할을 연결하거나 해제할 수 있습니다. 사용자는 액세스 권한이 있는 모든 대시보드를 볼 수 있지만 대시보드 및 대화형 분석의 데이터가 해당 사용자 역할이 액세스할 수 있는 데이터 집합을 기준으로 필터링됩니다.

사용자

시스템 관리자는 사용자의 로그인 계정에 사용 권한 및 역할을 부여하거나 해제하여 각 사용자의 액세스 권한과 작업을 제어할 수 있습니다.

사용 권한

사용 권한은 vRealize Log Insight에서 허용되는 작업을 제어합니다. 사용 권한은 vRealize Log Insight에서 특정 관리 작업 또는 사용자 작업에 적용됩니다. 예를 들어 **관리 보기** 사용 권한을 부여하면 사용자가 vRealize Log Insight 관리 설정을 볼 수 있습니다.

데이터 집합


데이터 집합은 일련의 필터로 구성되어 있습니다. 데이터 집합을 사용하면 데이터 집합을 역할에 연결하여 사용자에게 특정 콘텐츠에 대한 액세스 권한을 제공할 수 있습니다.

역할

역할은 사용자에게 연결될 수 있는 사용 권한 및 데이터 집합의 모음입니다. 역할은 작업을 수행하는데 필요한 모든 사용 권한을 패키지화할 수 있는 편리한 방법을 제공합니다. 한 사용자에게 여러 역할을 할당할 수 있습니다.

필터링을 사용하여 사용자 계정 관리

검색 필터를 지정하여 사용자 또는 사용자 집합을 검색할 수 있습니다.

액세스 제어 페이지의 **사용자 및 그룹** 탭에서 필터링이 완료됩니다. 페이지로 돌아가려면 드롭다운 메뉴 아이콘 에서 **관리**를 클릭하고, **관리** 메뉴에서 **액세스 제어**를 클릭한 후 **사용자 및 그룹** 탭을 선택합니다.

검색 텍스트 상자는 페이지 위쪽에 있으며 사용자 이름별 필터링을 포함합니다.

검색 기능은 사용자가 입력하면 결과를 필터링하고, 입력 패턴을 포함하는 사용자 이름을 반환합니다. 예를 들어, 사용자 이름이 John_Smith, John_Doe 및 Helen_Jonson인 경우 문자 **J**를 입력하는 경우 검색 기능은 해당 문자를 포함하는 모든 사용자 이름을 반환합니다. 이 예제에서는 John_Smith, John_Doe 및 Helen_Jonson이 반환됩니다. 문자를 계속 입력하면 정확한 패턴에 일치하도록 검색 결과 범위가 좁아집니다. 이 예에서는 **John_**를 입력하는 경우 검색 기능은 John_Smith 및 John_Doe를 반환합니다.

도메인, 인증, 역할, 이메일 또는 UPN 필드를 기준으로 검색 결과를 정렬할 수 있습니다. 또한 검색 결과에서 여러 사용자를 삭제하는 것과 같은 대량 작업을 수행할 수 있습니다.

vRealize Log Insight에서 새 사용자 계정 생성


수퍼 관리자 역할을 부여받은 사용자는 사용자 계정을 생성하여 vRealize Log Insight 웹 사용자 인터페이스에 대한 액세스 권한을 제공할 수 있습니다.

사전 요구 사항

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.

이러한 유형의 인증을 사용하는 사용자 계정을 생성하는 경우 VMware Identity Manager 또는 Active Directory 지원을 구성했는지 확인하십시오. [VMware Identity Manager](#)를 통해 사용자 인증 사용 및 [Active Directory](#)를 통해 사용자 인증 활성화 항목을 참조하십시오.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **액세스 제어**를 클릭합니다.
- 3 **사용자/사용자 및 그룹**을 클릭합니다.
- 4 **새 사용자**를 클릭합니다.
- 5 **인증** 드롭다운 메뉴에서 항목을 선택합니다.
 - 기본 제공 인증을 사용하는 경우 사용자 이름, 암호를 입력하고 선택 사항으로 이메일 주소를 입력합니다. **암호** 텍스트 상자의 암호를 복사하여 사용자에게 제공합니다.
 - Active Directory 또는 VMware Identity Manager 인증을 사용하는 경우 사용자가 속하는 도메인, 사용자 이름을 입력하고 선택 사항으로 사용자 이름 계정의 이메일 주소를 입력합니다.

- 6 오른쪽의 **역할** 목록에서 하나 이상의 사전 정의된 사용자 역할 또는 사용자 지정 사용자 역할을 선택합니다.

옵션	설명
사용자	사용자는 vRealize Log Insight의 전체 기능에 액세스할 수 있습니다. 사용자는 로그 이벤트를 보고, 쿼리를 실행하여 로그를 검색 및 필터링하고, 콘텐츠 팩을 자신의 사용자 공간으로 가져오고, 경고 쿼리를 추가하고, 암호 또는 이메일 주소를 변경하는 등 자신의 사용자 계정을 관리할 수 있습니다. 사용자는 관리 옵션에 대한 액세스 권한이 없고, 다른 사용자와 콘텐츠를 공유할 수 없으며, 다른 사용자의 계정을 수정할 수 없고, 마켓플레이스에서 콘텐츠 팩을 설치할 수 없습니다. 하지만 사용자 자신에게만 보이는 사용자 공간으로 콘텐츠 팩을 가져올 수는 있습니다.
대시보드 사용자	대시보드 사용자는 vRealize Log Insight의 대시보드 페이지만 사용할 수 있습니다.
보기 전용 관리자	View 관리 사용자는 관리 정보를 볼 수 있으며, 전체 사용자 액세스 권한을 보유하고, 공유 콘텐츠를 편집할 수 있습니다.
수퍼 관리자	수퍼 관리자는 vRealize Log Insight의 전체 기능에 액세스할 수 있으며, vRealize Log Insight를 관리할 수 있고, 다른 모든 사용자의 계정을 관리할 수 있습니다.

- 7 **저장**을 클릭합니다.

- 기본 제공 인증의 경우 이 정보는 로컬로 저장됩니다.
- VMware Identity Manager를 사용한 인증의 경우 vRealize Log Insight는 VMware Identity Manager가 지정된 그룹 및 해당 도메인과 동기화되는지 확인합니다. 그룹을 찾을 수 없으면 vRealize Log Insight에서 해당 그룹을 확인할 수 없다는 내용의 대화상자가 나타납니다. 확인 없이 그룹을 저장하거나, 취소하여 그룹 이름 또는 도메인을 수정할 수 있습니다.

vRealize Log Insight의 한 Active Directory 그룹에 대한 VMware Identity Manager 액세스 구성

VMware Identity Manager Single Sign-On 인증을 통해 vRealize Log Insight에서 Active Directory 그룹을 사용할 수 있습니다. 사이트는 Active Directory 지원이 설정된 VMware Identity Manager 인증에 대해 구성되어야 하고 서버 동기화가 설정되어야 합니다.

또한 그룹 정보를 vRealize Log Insight로 가져와야 합니다

VMware Identity Manager 사용자는 개별 사용자에게 할당된 역할 이외에 사용자가 속한 모든 그룹에 할당된 역할도 상속합니다. 예를 들어 관리자가 GroupA를 **관리 보기** 역할에 할당하고 사용자 Bob을 **사용자** 역할에 할당할 수 있습니다. 또한 Bob을 GroupA에 할당할 수 있습니다. 이 경우 Bob이 로그인하면 Bob은 그룹 역할을 상속하며 **관리 보기** 및 **사용자** 역할 모두에 대한 권한을 가집니다.


해당 그룹은 VMware Identity Manager 로컬 그룹이 아니고 VMware Identity Manager와 동기화된 Active Directory 그룹입니다.

사전 요구 사항

- UPN 특성(userPrincipalName)을 구성했는지 확인합니다. **ID 및 액세스 관리 > 사용자 특성**에서 VMware Identity Manager 관리자 인터페이스를 통해 구성할 수 있습니다.

- 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.
- vRealize Log Insight에서 VMware Identity Manager 지원을 구성했는지 확인합니다. **VMware Identity Manager**를 통해 **사용자 인증 사용** 항목을 참조하십시오.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **액세스 제어**를 클릭합니다.
- 3 **사용자 및 그룹**을 클릭합니다.
- 4 Directory 그룹 테이블로 스크롤한 후 **새 그룹**을 클릭합니다.
- 5 **유형** 드롭다운 메뉴에서 **VMware Identity Manager**를 선택합니다.

VMware Identity Manager 지원을 구성했을 때 지정한 기본 도메인 이름이 **도메인** 텍스트 상자에 표시됩니다.

- 6 도메인 이름을 그룹의 Active Directory 이름으로 변경합니다.
- 7 추가할 그룹의 이름을 입력합니다.
- 8 오른쪽의 **역할** 목록에서 하나 이상의 사전 정의된 사용자 역할 또는 사용자 지정 사용자 역할을 선택합니다.

옵션	설명
사용자	사용자는 vRealize Log Insight의 전체 기능에 액세스할 수 있습니다. 사용자는 로그 이벤트를 보고, 쿼리를 실행하여 로그를 검색 및 필터링하고, 콘텐츠 팩을 자신의 사용자 공간으로 가져오고, 경고 쿼리를 추가하고, 암호 또는 이메일 주소를 변경하는 등 자신의 사용자 계정을 관리할 수 있습니다. 사용자는 관리 옵션에 대한 액세스 권한이 없고, 다른 사용자와 콘텐츠를 공유할 수 없으며, 다른 사용자의 계정을 수정할 수 없고, 마켓플레이스에서 콘텐츠 팩을 설치할 수 없습니다. 하지만 사용자 자신에게만 보이는 사용자 공간으로 콘텐츠 팩을 가져올 수는 있습니다.
대시보드 사용자	대시보드 사용자는 vRealize Log Insight의 대시보드 페이지만 사용할 수 있습니다.
보기 전용 관리자	View 관리 사용자는 관리 정보를 볼 수 있으며, 전체 사용자 액세스 권한을 보유하고, 공유 콘텐츠를 편집할 수 있습니다.
수퍼 관리자	수퍼 관리자는 vRealize Log Insight의 전체 기능에 액세스할 수 있으며, vRealize Log Insight를 관리할 수 있고, 다른 모든 사용자의 계정을 관리할 수 있습니다.

- 9 **저장**을 클릭합니다.

vRealize Log Insight는 VMware Identity Manager가 지정된 그룹 및 해당 도메인과 동기화되는지 확인합니다. 그룹을 찾을 수 없으면 vRealize Log Insight에서 해당 그룹을 확인할 수 없다는 내용의 대화상자가 나타납니다. 확인 없이 그룹을 저장하거나, 취소하여 그룹 이름 또는 도메인을 수정할 수 있습니다.

결과

추가한 그룹에 속하는 사용자는 자신의 VMware Identity Manager 계정을 사용하여 vRealize Log Insight에 로그인하고, 자신이 속한 그룹과 동일한 수준의 사용 권한을 보유할 수 있습니다.

vRealize Log Insight로 Active Directory 그룹 가져오기

개별 도메인 사용자를 추가하지 않고 도메인 그룹을 추가하여 사용자가 vRealize Log Insight에 로그인하도록 허용할 수 있습니다.

vRealize Log Insight에서 AD 지원을 사용하도록 설정하는 경우 도메인 이름을 구성하고 해당 도메인에 속한 바인딩 사용자를 제공합니다. vRealize Log Insight는 바인딩 사용자를 사용하여 AD 도메인에 대한 연결을 확인하고 AD 사용자 및 그룹의 존재를 확인합니다.


vRealize Log Insight에 추가하는 Active Director 그룹은 바인딩 사용자의 도메인에 속하거나 바인딩 사용자의 도메인에서 신뢰하는 도메인에 속해야 합니다.

Active Directory 사용자는 개별 사용자에게 할당된 역할 이외에 사용자가 속한 모든 그룹에 할당된 역할도 상속합니다. 예를 들어 관리자가 GroupA를 **관리 보기** 역할에 할당하고 사용자 Bob을 **사용자** 역할에 할당할 수 있습니다. 또한 Bob을 GroupA에 할당할 수 있습니다. 이 경우 Bob이 로그인하면 Bob은 그룹 역할을 상속하며 **관리 보기** 및 **사용자** 역할 모두에 대한 권한을 가집니다.

사전 요구 사항

- 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.
- 구성된 AD 지원을 확인합니다. **Active Directory**를 통해 **사용자 인증 활성화** 항목을 참조하십시오.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **액세스 제어**를 클릭합니다.
- 3 **사용자 및 그룹**을 클릭합니다.
- 4 Directory 그룹 아래에서 **새 그룹**을 클릭합니다.
- 5 **유형** 드롭다운 메뉴에서 **Active Directory**를 클릭합니다.
Active Directory 지원을 구성했을 때 지정한 기본 도메인 이름이 **도메인** 텍스트 상자에 표시됩니다. 기본 도메인에서 그룹을 추가하는 경우 도메인 이름을 수정하지 마십시오.
- 6 (선택 사항) 기본 도메인을 신뢰하는 도메인에서 그룹을 추가하려는 경우 **도메인** 텍스트 상자에 신뢰하는 도메인의 이름을 입력합니다.
- 7 추가할 그룹의 이름을 입력합니다.

- 8 오른쪽의 **역할** 목록에서 하나 이상의 사전 정의된 사용자 역할 또는 사용자 지정 사용자 역할을 선택합니다.

옵션	설명
사용자	사용자는 vRealize Log Insight의 전체 기능에 액세스할 수 있습니다. 사용자는 로그 이벤트를 보고, 쿼리를 실행하여 로그를 검색 및 필터링하고, 콘텐츠 팩을 자신의 사용자 공간으로 가져오고, 경고 쿼리를 추가하고, 암호 또는 이메일 주소를 변경하는 등 자신의 사용자 계정을 관리할 수 있습니다. 사용자는 관리 옵션에 대한 액세스 권한이 없고, 다른 사용자와 콘텐츠를 공유할 수 없으며, 다른 사용자의 계정을 수정할 수 없고, 마켓플레이스에서 콘텐츠 팩을 설치할 수 없습니다. 하지만 사용자 자신에게만 보이는 사용자 공간으로 콘텐츠 팩을 가져올 수는 있습니다.
대시보드 사용자	대시보드 사용자는 vRealize Log Insight의 대시보드 페이지만 사용할 수 있습니다.
보기 전용 관리자	View 관리 사용자는 관리 정보를 볼 수 있으며, 전체 사용자 액세스 권한을 보유하고, 공유 콘텐츠를 편집할 수 있습니다.
수퍼 관리자	수퍼 관리자는 vRealize Log Insight의 전체 기능에 액세스할 수 있으며, vRealize Log Insight를 관리할 수 있고, 다른 모든 사용자의 계정을 관리할 수 있습니다.

- 9 **저장**을 클릭합니다.

vRealize Log Insight는 AD 그룹이 사용자가 지정한 도메인 또는 신뢰하는 도메인에 있는지 확인합니다. 그룹을 찾을 수 없으면 vRealize Log Insight에서 해당 그룹을 확인할 수 없다는 내용의 대화상자가 나타납니다. 확인 없이 그룹을 저장하거나, 취소하고 그룹 이름을 수정할 수 있습니다.

결과

추가한 Active Directory 그룹에 속하는 사용자는 자신의 도메인 계정을 사용하여 vRealize Log Insight에 로그인하고, 자신이 속한 그룹과 동일한 수준의 사용 권한을 보유할 수 있습니다.

크로스-도메인 그룹 멤버 자격으로 사용자 인증

관리자가 다른 신뢰할 수 있는 도메인의 사용자를 vRealize Log Insight에 대해 인증하는 방법에는 2가지가 있습니다.

- 각 사용자를 수동으로 추가합니다.
- 사용자가 속하는 동일한 도메인에 그룹을 구성하고 해당 그룹을 추가합니다.

데이터 집합 정의


데이터 집합을 정의하여 특정 콘텐츠에 대한 사용자 액세스 권한을 제공할 수 있습니다.

텍스트 기반 제약 조건은 데이터 집합에 대해 지원되지 않습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘  을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **액세스 제어**를 클릭합니다.
- 3 **데이터 집합**을 클릭합니다.
- 4 **새 데이터 집합**을 클릭합니다.
- 5 **필터 추가**를 클릭합니다.
- 6 첫 번째 드롭다운 메뉴를 사용하여 필터링할 vRealize Log Insight에 정의된 필드를 선택합니다.

예: **hostname**.

목록에는 정적 필드만 포함되며, 추출된 필드, 사용자 공유 필드 및 텍스트 필드와 event_type 필터를 통해 생성된 필드는 제외됩니다.

참고 숫자 필드에는 문자열 필드가 포함하지 않는 추가 연산자(=, >, <, >= 및 <=)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_timecontains02**에는 같은 일치 항목이 없습니다.

- 7 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 문자열을 검색하면 결과에 error가 일치 항목으로 나타나지 않습니다.

- 8 필터 드롭다운 메뉴 오른쪽의 필터 상자에서 필터로 사용할 값을 입력합니다.

여러 값을 사용할 수 있습니다. 이러한 값 사이 연산자는 OR입니다.

참고 두 번째 드롭다운 메뉴에서 **exists** 연산자를 선택하는 경우 이 확인란을 사용할 수 없습니다.

- 9 (선택 사항) 필터를 더 추가하려면 **필터 추가**를 클릭합니다.
- 10 (선택 사항) 필터 동작이 원하는 동작인지 확인하려면 **대화형 분석에서 실행**을 클릭합니다. 그러면 필터와 일치하는 데이터를 포함하는 대화형 분석 창이 열립니다.
- 11 **저장**을 클릭합니다.

다음에 수행할 작업

데이터 집합을 사용자 역할에 연결합니다. [역할 생성 및 수정](#) 항목을 참조하십시오.



역할 생성 및 수정

사용자 지정 역할을 생성하거나 미리 정의된 역할을 수정하여 사용자가 특정 작업을 수행하고 특정 콘텐츠에 액세스하도록 허용할 수 있습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘  을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **액세스 제어**를 클릭합니다.
- 3 **역할**을 클릭합니다.
- 4 **새 역할**을 클릭하거나,  을 클릭하여 기존 역할을 편집합니다.
역할을 편집하려면 먼저 슈퍼 관리자 및 사용자 역할을 복제해야 합니다.
- 5 **이름** 및 **설명** 텍스트 상자를 수정합니다.
- 6 사용 권한 목록에서 하나 이상의 사용 권한을 선택합니다.

옵션	설명
관리 편집	관리 정보 및 설정 편집 가능
관리 보기	관리 정보 및 설정 보기 가능
공유 콘텐츠 편집	공유 콘텐츠 편집 가능
분석	대화형 분석 사용 가능
대시보드	대시보드 보기 가능

- 7 (선택 사항) 오른쪽의 **데이터 집합** 목록에서 사용자 역할에 연결할 데이터 집합을 선택합니다.
- 8 **저장**을 클릭합니다.

vRealize Log Insight에서 사용자 계정 또는 그룹 삭제


vRealize Log Insight 관리 사용자 인터페이스에서 사용자 계정 또는 그룹을 삭제할 수 있습니다.

사용자 계정 및 그룹은 [액세스 제어] 페이지의 별도 표에 나열됩니다. 검색 필터를 사용하여 특정 사용자 계정을 찾을 수 있습니다. 그룹을 삭제하면 그룹에 속하는 모든 사용자는 그룹에 의해 부여된 권한을 잃습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘  을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **액세스 제어**를 클릭합니다.
- 3 **사용자 및 그룹**을 클릭합니다.
- 4 삭제할 사용자 이름 또는 그룹 옆의 확인란을 선택합니다.
- 5 계정 또는 그룹을 제거하려면 사용자 계정 또는 그룹 포 맨 위에 있는 **X 삭제**를 클릭합니다.

배포에서 몇 가지 인증 방법을 사용할 수 있습니다.

인증 방법에는 로컬 인증, VMware Identity Manager 인증 및 Active Directory 인증이 포함됩니다. 동일한 배포에서 둘 이상의 방법을 사용할 수 있으며, 사용자가 로그인 시 사용할 인증 유형을 선택합니다.

vRealize Log Insight에 대한 다운로드 페이지에는 VMware Identity Manager의 해당 버전에 대한 다운로드 링크가 포함되어 있습니다. VMware Identity Manager에는 다음과 같은 기능이 포함되어 있습니다.

- Active Directory 또는 LDAP와 같은 기존 디렉토리에 대해 사용자를 인증하기 위한 디렉토리 통합.
- Single Sign-On 기능도 지원하는 다른 VMware 제품과의 Single Sign-On 통합.
- ADFS, Ping Federate 등의 일부 타사 ID 제공자를 통한 Single Sign-On.
- RSA SecurID, Entrust 등과 같은 타사 소프트웨어와의 통합을 통한 2단계 인증. VMware Verify를 통한 2단계 인증도 포함됩니다.

로컬 인증은 vRealize Log Insight의 구성 요소입니다. 이를 사용하려면 vRealize Log Insight 서버에 저장되는 로컬 사용자 및 암호를 생성합니다. 제품 관리자는 vRealize Log Insight 및 Active Directory를 사용하도록 설정해야 합니다.

본 장은 다음 항목을 포함합니다.

- [VMware Identity Manager를 통해 사용자 인증 사용](#)
- [Active Directory를 통해 사용자 인증 활성화](#)

VMware Identity Manager를 통해 사용자 인증 사용

관리자가 사용하도록 설정한 경우 vRealize Log Insight에서 VMware Identity Manager 인증을 사용할 수 있습니다.

VMware Identity Manager 인증을 사용하면 동일한 Identity Manager를 사용하는 모든 VMware 제품에 대해 Single Sign-On을 사용할 수 있습니다.


또한 Active Directory 사용자는 VMware Identity Manager Active Directory 및 VMware Identity Manager 서버가 동기화될 때를 통해 인증을 받을 수 있습니다. 동기화에 대한 자세한 내용은 VMware Identity Manager 설명서를 참조하십시오.

VMware Identity Manager 통합은 로컬 사용자만 수행할 수 있습니다. VMware Identity Manager에서 테넌트 관리자 역할이 할당된 Active Directory 사용자는 vRealize Log Insight 통합에 대해 적격하지 않습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 구성 아래에서 **인증**을 클릭합니다.
- 3 **Single Sign-On 사용**을 선택합니다.
- 4 **호스트** 텍스트 상자에 VMware Identity Manager 인스턴스가 사용자를 인증하는 데 사용할 호스트 식별자를 입력합니다.
예를 들면 `company-name.vmwareidentity.com`입니다.
- 5 **API 포트** 텍스트 상자에 VMware Identity Manager 인스턴스에 연결하는 데 사용할 포트를 지정합니다. 기본 포트는 443입니다.
- 6 선택적으로 VMware Identity Manager 테넌트를 입력합니다. 이 테넌트는 테넌트 모드가 VMware Identity Manager에서 `tenant-in-path`로 구성된 경우에만 필요합니다.
- 7 **사용자 이름 및 암호** 텍스트 상자에 VMware Identity Manager 사용자 자격 증명을 지정합니다.
이 정보는 VMware Identity Manager에서 vRealize Log Insight 클라이언트를 생성하도록 구성하는 동안에 한 번만 사용되며 vRealize Log Insight에 로컬로 저장되지 않습니다. 사용자는 테넌트에 대해 API 명령을 실행할 권한이 있어야 합니다.
- 8 **연결 테스트**를 클릭하여 연결되었는지 확인합니다.
- 9 VMware Identity Manager 인스턴스가 신뢰할 수 없는 SSL 인증서를 제공하는 경우 인증서의 세부 정보가 포함된 대화상자가 나타납니다. **수락**을 클릭하여 vRealize Log Insight 클러스터에 있는 모든 노드의 신뢰 저장소에 인증서를 추가합니다.
취소를 클릭하면 인증서가 신뢰 저장소에 추가되지 않고, VMware Identity Manager 인스턴스와의 연결이 실패합니다. 연결에 성공하려면 인증서를 수락해야 합니다.
- 10 **리디렉션 URL 호스트** 드롭다운 메뉴에서 VMware Identity Manager에 등록하기 위해 리디렉션 URL에서 사용할 호스트 이름 또는 IP를 선택합니다.
통합 로드 밸런서에 대해 하나 이상의 가상 IP가 정의된 경우 VMware Identity Manager는 선택된 VIP로 리디렉션됩니다. 통합 로드 밸런서가 구성되어 있지 않으면 기본 노드의 IP 주소가 대신 사용됩니다.

- 11 VMware Identity Manager를 통한 Active Directory 사용자에게 대한 로그인 지원을 허용할지 여부를 선택합니다.

VMware Identity Manager가 Active Directory 인스턴스와 동기화될 때 Active Directory 사용자에게 대해 이 옵션을 사용할 수 있습니다.

- 12 **저장**을 클릭합니다.

연결을 테스트하지 않았으며, VMware Identity Manager 인스턴스에서 신뢰할 수 없는 인증서를 제공하는 경우 9단계의 지침을 따르십시오.

Active Directory를 통해 사용자 인증 활성화


Active Directory 통해 사용자를 인증하면 사용자는 여러 용도에서 공통 암호를 사용할 수 있으므로 로그인 프로세스가 간소화될 수 있습니다.

하위 도메인 액세스는 Active Directory를 통해 지원되지 않습니다. 이러한 유형의 액세스는 VMware Identity Manager를 통해서만 지원됩니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 구성 아래에서 **인증**을 클릭합니다.
- 3 **Active Directory 지원 사용**을 선택합니다.
- 4 **기본 도메인** 텍스트 상자에서 도메인 이름을 입력합니다.

예를 들면 **company-name.com**입니다.

참고 기본 도메인 텍스트 상자에서 여러 도메인을 나열할 수 없습니다. 지정하는 기본 도메인을 다른 도메인이 신뢰하는 경우 vRealize Log Insight는 기본 도메인과 바인딩 사용자를 사용하여 신뢰하는 도메인의 Active Directory 사용자 및 그룹을 확인합니다. Active Directory를 통한 하위 도메인 액세스는 지원되지 않습니다.

사용자 및 그룹이 이미 포함된 다른 도메인으로 전환하는 경우 기존 사용자 및 그룹에 대해 인증이 실패하며 기존 사용자가 저장한 데이터는 손실됩니다.

- 5 위치 정보를 찾았거나 보안이 제한된 도메인 컨트롤러가 있는 경우 이 vRealize Log Insight 인스턴스에 가장 가까운 도메인 컨트롤러를 수동으로 지정합니다.

참고 로드 밸런싱된 Active Directory 인증 서버는 지원되지 않습니다.

- 6 기본 도메인에 속하는 바인딩 사용자의 자격 증명을 입력합니다.

vRealize Log Insight은 기본 도메인과 바인딩 사용자를 사용하여 기본 도메인과 기본 도메인을 신뢰하는 도메인의 AD 사용자 및 그룹을 확인합니다.

- 7 연결 유형에 대한 값을 지정합니다.

이 연결은 Active Directory 인증에 사용됩니다.

- 8 **연결 테스트**를 클릭하여 연결되었는지 확인합니다.

- 9 Active Directory 서버가 신뢰할 수 없는 SSL 인증서를 제공하는 경우 인증서의 세부 정보가 포함된 대화상자가 나타납니다. **수락**을 클릭하여 vRealize Log Insight 클러스터에 있는 모든 노드의 신뢰 저장소에 인증서를 추가합니다.

취소를 클릭하면 인증서가 신뢰 저장소에 추가되지 않고, Active Directory 서버와의 연결이 실패합니다. 연결에 성공하려면 인증서를 수락해야 합니다.

- 10 **저장**을 클릭합니다.

연결을 테스트하지 않았으며, Active Directory 서버에서 신뢰할 수 없는 인증서를 제공하는 경우 9단계의 지점을 따르십시오.

다음에 수행할 작업

Active Directory 사용자 및 그룹에 vRealize Log Insight의 현재 인스턴스에 액세스할 수 있는 권한을 부여합니다.

Active Directory에 사용할 프로토콜 구성

Active Directory에 연결할 때 사용할 프로토콜을 구성할 수 있습니다. 기본적으로 vRealize Log Insight는 Active Directory에 연결될 때 먼저 SSL LDAP를 사용한 다음 필요한 경우 SSL LDAP 이외의 방법을 사용합니다.

Active Directory 통신을 하나의 특정 프로토콜로 제한하거나 시도되는 프로토콜의 순서를 변경하려면 vRealize Log Insight 가상 장치에서 추가 구성을 적용해야 합니다.

사전 요구 사항

- vRealize Log Insight 가상 장치에 로그인하기 위한 루트 사용자 자격 증명을 가지고 있는지 확인합니다.
- SSH 연결을 활성화하려면 TCP 포트 22가 열려 있는지 확인합니다.

절차

- 1 vRealize Log Insight 가상 장치에 대한 SSH 연결을 설정하고 루트 사용자로 로그인합니다.
- 2 다음 위치로 이동합니다. `/storage/core/loginsight/config`
- 3 `[number]`가 가장 큰 최신 구성 파일 `/storage/core/loginsight/config/loginsight-config.xml#[number]`를 찾습니다.

- 4 최신 구성 파일 `/storage/core/loginsight/config/loginsight-config.xml#[number]`를 복사합니다.
- 5 `[Number]`를 증가시키고 다음 위치에 저장합니다. `/storage/core/loginsight/config/loginsight-config.xml#[number + 1]`
- 6 편집할 파일을 엽니다.
- 7 Authentication 섹션에서 적용할 구성에 해당하는 라인을 추가합니다.

옵션	설명
<code><ad-protocols value="LDAP" /></code>	특별히 SSL이 포함되지 않은 LDAP를 사용하기 위한 용도
<code><ad-protocols value="LDAPS" /></code>	특별히 SSL만 포함된 LDAP를 사용하기 위한 용도
<code><ad-protocols value="LDAP,LDAPS" /></code>	특별히 먼저 LDAP를 사용한 다음 SSL이 포함된 LDAP를 사용하기 위한 용도.
<code><ad-protocols value="LDAPS,LDAP" /></code>	특별히 먼저 LDAPS를 사용한 다음 SSL이 포함되지 않은 LDAP를 사용하기 위한 용도

프로토콜을 선택하지 않는 경우 vRealize Log Insight은 먼저 LDAP 사용을 시도한 다음 SSL이 포함된 LDAP를 사용합니다.

- 8 파일을 저장한 후 닫습니다.
- 9 `service loginsight restart` 명령을 실행합니다.

vRealize Log Insight 구성

4

vRealize Log Insight를 구성하고 사용자 지정하여 기본 설정, 네트워크 설정을 변경하고 스토리지 리소스를 수정할 수 있습니다. 또한 시스템 알림을 구성할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- vRealize Log Insight 구성 제한
- 데이터 보존 구성
- 가상 장치 설정 구성
- vRealize Log Insight에 라이선스 할당
- 로그 저장 정책
- 시스템 알림 관리
- vRealize Log Insight 이벤트 전달 대상 추가
- vRealize Log Insight 가상 장치의 시간 동기화
- vRealize Log Insight에 대한 SMTP 서버 구성
- 사용자 지정 SSL 인증서 설치
- SSL 인증서 보기 및 제거
- vRealize Log Insight 웹 세션에 대한 기본 시간 초과 기간 변경
- 아카이브
- vRealize Log Insight 서비스 다시 시작
- vRealize Log Insight 가상 장치의 전원 끄기
- vRealize Log Insight 지원 번들 다운로드
- VMware 고객 환경 개선 프로그램 가입 또는 탈퇴

vRealize Log Insight 구성 제한

vRealize Log Insight를 구성할 때는 지원되는 최대값 이하를 유지해야 합니다.

표 4-1. vRealize Log Insight 구성 최대값

항목	최대값
노드 구성	
CPU	16vCPU
메모리	32GB
스토리지 디바이스(vmdk)	2TB - 512바이트
주소 지정이 가능한 총 스토리지	4TB(+ OS 드라이브) 최대 크기가 각각 2TB인 VMDK에 있는 최대 4TB의 주소 지정 가능 로그 스토리지입니다. 2개의 2TB VMDK 또는 4개의 1TB VMDK를 사용할 수 있습니다. 최대 제한에 도달하면 기존 VM에 디스크를 더 추가하는 대신 더 큰 클러스터 크기로 확장해야 합니다.
Syslog 연결	750
클러스터 구성	
노드	12개(기본 + 작업자 11개)
노드당 수집 수	
초당 이벤트 수	15,000eps
Syslog 메시지 길이	10KB(텍스트 필드)
수집 API HTTP POST 요청	16KB(텍스트 필드), HTTP Post 요청당 4MB
통합	
vRealize Operations Manager	1
vSphere vCenter Server	노드당 15개
Active Directory 도메인	1
이메일 서버	1
DNS 서버	2
NTP 서버	4
전달자	10

데이터 보존 구성

데이터 보존 기능을 구성하여 특정 날짜 또는 기간보다 오래된 데이터를 제거하는 기능을 사용하도록 설정할 수 있습니다. 데이터 보존 옵션은 기본적으로 사용되지 않도록 설정되어 있습니다.

사전 요구 사항

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.

절차

- 1 웹 사용자 인터페이스에서 구성 드롭다운 메뉴 아이콘을 클릭하고 **관리**를 선택합니다.
- 2 구성 아래에서 **일반**을 클릭합니다.
- 3 **데이터 보존** 확인란을 선택하고 보존 기간을 지정하여 데이터 보존 기능을 사용하도록 설정합니다.

참고

- 기본 데이터 보존 기간은 12개월이며, 여기서 1개월은 30일입니다.
- 보존 기간은 노드 스토리지에만 적용되며 NFS 아카이브는 그대로 유지됩니다.

- 4 **저장**을 클릭합니다.

결과

일단 사용하도록 설정하면 데이터 보존은 1시간 후에 시작되고 하루에 한 번 제거할 데이터를 확인합니다.

참고 수집 속도가 느린 경우 구성된 보존 기간과 클러스터에서 가장 오래된 데이터의 타임 스탬프 간에 약간의 차이가 발생할 수 있습니다.

가상 장치 설정 구성

스토리지 용량 및 메모리 또는 CPU 용량을 비롯한 가상 장치 설정을 수정할 수 있습니다.

vRealize Log Insight 가상 장치에 대한 루트 SSH 암호 구성

기본적으로 가상 장치에 대한 SSH 연결은 비활성화되어 있습니다. vRealize Log Insight 가상 장치를 배포할 때 또는 VMware Remote Console에서 루트 SSH 암호를 구성할 수 있습니다.

vRealize Log Insight .ova 파일을 배포할 때 루트 SSH 암호를 설정하는 것이 가장 좋은 방법입니다. 자세한 내용은 [vRealize Log Insight 가상 장치 배포](#) 항목을 참조하십시오.

SSH를 사용하도록 설정하고 VMware Remote Console에서 루트 암호를 설정할 수도 있습니다.

사전 요구 사항

vRealize Log Insight 가상 장치가 배포되었고 실행 중인지 확인합니다.

절차

- 1 vSphere Client 인벤토리에서 vRealize Log Insight 가상 장치를 클릭하고 **콘솔** 탭을 엽니다.
- 2 시작 화면에 지정된 키 조합에 따라 명령줄로 이동합니다.

- 3 콘솔에서 **root**를 입력하고 Enter 키를 누릅니다. 암호를 비워둔 후 Enter 키를 누릅니다.
다음 메시지가 콘솔에 표시됩니다. 암호 변경이 요청되었습니다. 새 암호를 선택하십시오.
- 4 기존 암호를 비워둔 후 Enter 키를 누릅니다.
- 5 루트 사용자에게 대한 새 암호를 입력한 후 Enter 키를 누르고 루트 사용자에게 대한 새 암호를 다시 입력한 후 Enter 키를 누릅니다.
암호는 8자 이상으로 구성되어야 하며 하나 이상의 대문자, 하나 이상의 소문자, 하나 이상의 숫자 및 하나 이상의 특수 문자를 포함해야 합니다. 동일한 문자를 4번 넘게 반복할 수 없습니다.

결과

다음 메시지가 표시됩니다. 암호가 변경되었습니다.

다음에 수행할 작업

루트 암호를 사용하여 vRealize Log Insight 가상 장치에 대한 SSH 연결을 설정할 수 있습니다.

vRealize Log Insight 가상 장치의 네트워크 설정 변경

vSphere Client에서 vApp 속성을 편집하여 vRealize Log Insight 가상 장치의 네트워크 설정을 변경할 수 있습니다.

vApps 구성에 대한 자세한 내용은 <https://docs.vmware.com/kr/VMware-vSphere/index.html> 항목을 참조하십시오.

사전 요구 사항

vApp 속성을 편집할 수 있는 권한을 가지고 있는지 확인합니다.

절차

- 1 vRealize Log Insight 가상 장치의 전원을 끕니다.
- 2 인벤토리에서 vRealize Log Insight 가상 장치를 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 클릭합니다.
- 3 **옵션** 탭을 클릭하고 **vApp 옵션 > IP 할당 정책**을 선택합니다.
- 4 IP 할당 옵션을 선택합니다.

옵션	설명
고정	IP 주소를 수동으로 구성합니다. 이 경우 주소가 자동으로 할당되지 않습니다.
임시	vApp 전원을 켜면 지정한 범위의 IP 풀을 사용하여 IP 주소를 자동으로 할당합니다. 장치의 전원이 꺼지면 IP 주소가 할당 해제됩니다.
DHCP	DHCP 서버는 IP 주소를 할당하는 데 사용됩니다. DHCP 서버에서 할당한 주소를 vApp에서 시작된 가상 시스템의 OVF 환경에서 볼 수 있습니다.

- 5 (선택 사항) **고정**을 선택하는 경우 **vApp 옵션 > 속성**을 클릭하고 vRealize Log Insight vApp에 대한 IP 주소, 넷마스크, 게이트웨이, DNS 및 호스트 이름을 할당합니다.

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.

- 6 vRealize Log Insight vApp의 전원을 끕니다.

vRealize Log Insight 가상 장치의 스토리지 용량 늘리기

확장이 필요하면 그에 따라 vRealize Log Insight에 할당되는 스토리지 리소스를 늘릴 수 있습니다.

vRealize Log Insight 가상 장치에 새 가상 디스크를 추가하는 방식으로 스토리지 공간을 늘립니다. 필요한 만큼 디스크를 추가하여 주소 지정이 가능한 스토리지를 최대 4TB(+ OS 드라이브)까지 확장할 수 있습니다. 총 2개의 2TB 디스크 또는 4개의 1TB 디스크 등의 조합이 될 수 있습니다. [vRealize Log Insight 구성 제한](#) 항목을 참조하십시오.

vRealize Log Insight 클러스터에서 클러스터의 각 노드에 동일한 양의 스토리지를 추가해야 합니다.

사전 요구 사항

- 환경에 있는 가상 시스템의 하드웨어를 수정할 수 있는 권한이 있는 사용자로 vSphere Client에 로그인합니다.
- vRealize Log Insight 가상 장치를 안전하게 종료합니다. [vRealize Log Insight 가상 장치의 전원 끄기](#) 항목을 참조하십시오.

절차

- 1 vSphere Client 인벤토리에서 vRealize Log Insight 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 2 **하드웨어** 탭에서 **추가**를 클릭합니다.
- 3 **하드 디스크**를 선택하고 나서 **다음**을 클릭합니다.

4 새 가상 디스크 생성을 선택하고 다음을 클릭합니다.

a 디스크 용량을 입력합니다.

vRealize Log Insight는 2TB의 가상 하드 디스크를 지원합니다. 더 많은 용량이 필요하다면 둘 이상의 가상 하드 디스크를 추가합니다.

b 디스크 포맷을 선택합니다.

옵션	설명
느리게 비워지는 썸 프로비저닝	기본 썸 형식의 가상 디스크를 생성합니다. 가상 디스크에 필요한 공간은 가상 디스크 생성 중에 할당됩니다. 물리적 디바이스에 상주하는 데이터는 가상 디스크를 생성하는 동안에는 지워지지 않지만 나중에 가상 장치에서 처음으로 쓴 후 요구에 따라 0으로 설정됩니다.
빠르게 비워지는 썸 프로비저닝	Fault Tolerance와 같은 클러스터 기능을 지원하는 썸 가상 디스크 유형을 생성합니다. 가상 디스크에 필요한 공간은 디스크 생성 시에 할당됩니다. 플랫 형식과 반대로 물리적 디바이스에 상주하는 데이터는 가상 디스크를 생성하는 동안 0으로 설정됩니다. 다른 유형의 디스크를 생성하는 것보다 이 형식의 디스크를 생성하는 것이 더 오래 걸릴 수 있습니다. vRealize Log Insight 가상 장치의 더 나은 성능과 운영을 위해 가능하면 빠르게 비워지는 썸 프로비저닝된 디스크를 생성합니다.
Thin Provision	썸 형식의 디스크를 생성합니다. 스토리지 공간을 저장하려면 이 형식을 사용합니다.

c (필수 사항) 데이터스토어를 선택하려면 데이터스토어 위치를 지정한 후 다음을 클릭합니다.

5 기본 가상 디바이스 노드를 수락하고 다음을 클릭합니다.

6 정보를 검토하고 마침을 클릭합니다.

7 확인을 클릭하여 변경 내용을 저장하고 대화상자를 닫습니다.

결과

vRealize Log Insight 가상 장치의 전원을 켜 경우 가상 시스템이 새 가상 디스크를 검색하고 자동으로 기본 데이터 볼륨에 추가합니다. 먼저 가상 시스템의 전원을 완전히 끕니다. 가상 장치의 전원에 대한 내용은 <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html> 항목을 참조하십시오.

경고 가상 장치에 디스크를 추가한 후에는 디스크를 안전하게 제거할 수 없습니다. vRealize Log Insight 가상 장치에서 디스크를 제거하면 데이터가 완전히 손실될 수 있습니다.

vRealize Log Insight 가상 장치에 메모리 및 CPU 추가

배포 후 vRealize Log Insight 가상 장치에 할당되는 메모리와 CPU의 양을 변경할 수 있습니다.

예를 들어 환경의 이벤트 수가 증가하는 경우 리소스 할당을 조정해야 할 수 있습니다.

사전 요구 사항

- 환경에 있는 가상 시스템의 하드웨어를 수정할 수 있는 권한이 있는 사용자로 vSphere Client에 로그인합니다.
- vRealize Log Insight 가상 장치를 안전하게 종료합니다. [vRealize Log Insight 가상 장치의 전원 끄기 항목](#)을 참조하십시오.

절차

- 1 vSphere Client 인벤토리에서 vRealize Log Insight 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 2 **하드웨어** 탭에서 **추가**를 클릭합니다.
- 3 필요에 따라 CPU 및 메모리의 양을 조정합니다.
- 4 정보를 검토하고 **마침**을 클릭합니다.
- 5 **확인**을 클릭하여 변경 내용을 저장하고 대화상자를 닫습니다.

결과

vRealize Log Insight 가상 장치의 전원을 켜면 가상 시스템이 새 리소스를 활용하기 시작합니다.

vRealize Log Insight에 라이선스 할당

vRealize Log Insight은 올바른 라이선스 키가 있어야 사용할 수 있습니다.

VMware 웹 사이트에서 vRealize Log Insight를 다운로드할 때 평가판 라이선스를 획득합니다. 이 라이선스는 60일 동안 유효합니다. 평가판 라이선스가 만료되면 vRealize Log Insight을 계속해서 사용하기 위해 영구 라이선스를 할당해야 합니다.

vRealize Log Insight OSI(운영 체제 인스턴스) 라이선스 모델은 가상화되지 않은 물리적 서버 또는 가상 시스템의 운영 체제 단일 설치로 OSI를 정의합니다. vRealize Log Insight의 경우 OSI는 가상화된 물리적 서버, 스토리지 어레이 또는 로그 메시지를 생성할 수 있는 네트워크 디바이스와 같이 IP 주소로 식별되는 단일 시스템일 수도 있습니다.

호스트, 서버 또는 다른 소스가 vRealize Log Insight로의 로그 전송을 중지하면 [라이선스] 페이지의 OSI 수가 보존 기간 동안 변경되지 않습니다. 보존 기간은 지난 3개월 동안 OSI 수의 평균으로 계산된 라이선스 사용량을 기준으로 합니다.

vRealize Log Insight 웹 사용자 인터페이스의 관리 섹션을 사용하여 vRealize Log Insight 라이선싱 상태를 확인하고 라이선스를 관리합니다.


솔루션 상호 운용성의 일부로, Standard, Advanced 또는 Enterprise Edition의 VMware NSX 사용자는 해당 NSX 라이선스 키로 vRealize Log Insight의 사용을 허가할 수 있습니다. 자세한 내용은 VMware NSX 설명서를 참조하십시오.

사전 요구 사항

- My VMware™에서 올바른 라이선스 키를 획득합니다.

- 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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **라이선스**를 선택합니다.
- 3 **라이선스 키** 텍스트 상자에서 라이선스 키를 입력하고 **키 설정**을 클릭합니다. VMware NSX 라이선스 키가 있으면 여기에 입력하십시오.
- 4 라이선스 상태가 활성화고 라이선스 유형 및 만료일이 올바른지 확인합니다.

로그 저장 정책

vRealize Log Insight 가상 장치는 들어오는 로그에 대해 최소 100GB의 스토리지를 사용합니다.

vRealize Log Insight로 가져오는 로그의 볼륨이 스토리지 제한에 도달하면 오래된 순서대로 로그 메시지가 주기적으로 자동 폐기됩니다. vRealize Log Insight 가상 장치에 더 많은 스토리지를 추가하여 스토리지 제한을 늘릴 수 있습니다. [vRealize Log Insight 가상 장치의 스토리지 용량 늘리기](#) 항목을 참조하십시오.

오래된 메시지를 보존하려면 vRealize Log Insight의 아카이브 기능을 활성화합니다. [vRealize Log Insight에서 데이터 아카이브 활성화 또는 비활성화](#) 항목을 참조하십시오.

vRealize Log Insight을 통해 저장된 데이터는 변경할 수 없습니다. 로그를 가져온 후에는 로그가 자동으로 폐기될 때까지 로그를 제거할 수 없습니다.

시스템 알림 관리

vRealize Log Insight는 디스크 공간이 거의 소모되고 오래된 로그 파일이 삭제되려는 경우 등의 vRealize Log Insight 상태와 관련된 활동에 대해 기본 제공 시스템 알림을 제공합니다. 관리자는 시스템 알림 전송의 빈도와 대상을 구성할 수 있습니다.

시스템 알림은 즉각적인 주의가 필요한 위험한 문제를 알리며 대응이 필요할 수 있는 경고를 제공하고 일반적인 시스템 활동을 알립니다. 시스템 알림은 업그레이드하는 동안 일시 중단되지만 다른 경우에는 항상 적용됩니다.

관리자는 트리거되는 경우 전송되는 알림의 빈도와 이메일 주소를 지정할 수 있습니다. vRealize Log Insight와 관련된 시스템 알림이 타사 애플리케이션에 전송될 수도 있습니다.

시스템 알림은 경고 쿼리와 구별되며 사용자 정의됩니다. 경고 쿼리에 대한 자세한 내용은 [Log Insight에서 경고 쿼리를 추가하여 이메일 알림 보내기](#)를 참조하십시오.

vRealize Log Insight 시스템 알림

vRealize Log Insight는 시스템 상태에 대해 2가지 알림 집합 즉, 모든 제품 구성에 적용 가능한 일반 알림과 클러스터 기반 배포의 클러스터와 관련된 알림을 제공합니다.

다음 표에서는 vRealize Log Insight에 대한 시스템 알림을 나열하고 설명합니다.

일반 시스템 알림

vRealize Log Insight는 아카이브 실패 또는 경고 스케줄 지연을 포함하여 관리 작업이 필요할 수 있는 상황에서 알림을 실행합니다.

알림 이름	설명
가장 오래된 데이터를 곧 검색할 수 없게 됨	<p>vRealize Log Insight는 검색 가능한 데이터의 예상 크기, 스토리지 공간 및 현재 수집 속도를 기준으로 가상 장치 스토리지에서 오래된 데이터를 서비스 해제하기 시작할 것으로 예상됩니다. 시스템에서 교체된 데이터는 아카이브를 구성한 경우에는 아카이브되고 아카이브를 구성하지 않은 경우에는 삭제됩니다.</p> <p>이 문제를 해결하려면 스토리지를 추가하거나 보존 알림 임계값을 조정합니다. 자세한 내용은 상태 알림을 전송하도록 vRealize Log Insight 구성 항목을 참조하십시오.</p> <p>이 알림은 vRealize Log Insight 서비스가 다시 시작될 때마다 전송됩니다.</p>
저장소 보존 시간	<p>보존 기간은 데이터가 vRealize Log Insight 인스턴스의 로컬 디스크에 보존되는 기간입니다. 보존 기간은 시스템이 보유할 수 있는 데이터 양과 현재 수집 속도에 따라 결정됩니다. 예를 들어 하루에 10GB의 데이터를 수신하며(인덱싱 후) 300GB의 공간이 있는 경우 보존 기간은 30일입니다. 스토리지 제한에 도달하면 새로 수집된 데이터를 위해 이전 데이터가 제거됩니다. 이 알림은 vRealize Log Insight가 현재 수집 비율로 저장할 수 있는 검색 가능한 데이터 양이 가상 장치에서 사용 가능한 스토리지 공간을 초과할 수 있는 시기를 알려 줍니다.</p> <p>보존 알림 임계값으로 설정한 기간이 되기 전에 스토리지가 고갈될 수 있습니다. 스토리지를 추가하거나 보존 알림 임계값을 조정합니다.</p>
삭제된 이벤트	<p>vRealize Log Insight가 수신 로그 메시지를 모두 수집하지 못했습니다.</p> <ul style="list-style-type: none"> ■ vRealize Log Insight 서버에 의해 추적된 대로 TCP 메시지가 삭제될 경우 다음과 같이 시스템 알림이 전송됩니다. <ul style="list-style-type: none"> ■ 하루에 한 번 ■ vRealize Log Insight 서비스가 수동으로 또는 자동으로 다시 시작될 때마다. ■ 이메일에는 마지막 알림 이메일이 전송된 이후 삭제된 메시지 수와 vRealize Log Insight의 마지막 다시 시작 이후 총 메시지 삭제 수가 포함되어 있습니다. <p>참고 전송 라인의 시간은 이메일 클라이언트에 의해 제어되고 현지 표준 시간대에 속하지만 이메일 본문은 UTC 시간을 표시합니다.</p>

알림 이름	설명
손상된 인덱스 버킷	<p>온디스크 인덱스의 일부가 손상되었습니다. 손상된 인덱스는 대개 기본 스토리지 시스템의 심각한 문제를 나타냅니다. 인덱스의 손상된 부분은 쿼리 처리에서 제외됩니다. 손상된 인덱스는 새 데이터의 수집에 영향을 미칩니다. vRealize Log Insight은 서비스 시작 시 인덱스의 무결성을 확인합니다. 손상이 감지될 경우 vRealize Log Insight는 다음과 같이 시스템 알림을 전송합니다.</p> <ul style="list-style-type: none"> ■ 하루에 한 번 ■ vRealize Log Insight 서비스가 수동으로 또는 자동으로 다시 시작될 때마다.
디스크 공간 부족	vRealize Log Insight에서 할당된 디스크 공간이 부족합니다. vRealize Log Insight에서 스토리지 관련 문제가 발생할 가능성이 높습니다.
아카이브 공간이 가득 차게 됨	vRealize Log Insight 데이터를 아카이브하는 데 사용되는 NFS 서버의 디스크 공간이 곧 모두 소진됩니다.
총 디스크 공간 변경	<p>vRealize Log Insight 데이터 스토리지에 대한 파티션의 총 크기가 감소했습니다. 이 알림은 대개 기본 스토리지 시스템의 심각한 문제를 암시합니다. vRealize Log Insight는 해당 상태를 감지할 때 다음과 같이 이 알림을 전송합니다.</p> <ul style="list-style-type: none"> ■ 즉시 ■ 하루에 한 번
보류 중인 아카이브	vRealize Log Insight에서 예상대로 데이터를 아카이브할 수 없습니다. 이 알림은 대개 데이터 아카이브를 위해 구성된 NFS 스토리지의 문제를 나타냅니다.
라이선스 만료 예정	vRealize Log Insight의 라이선스가 곧 만료되려고 합니다.
라이선스가 만료됨	vRealize Log Insight의 라이선스가 만료되었습니다.
AD 서버에 연결할 수 없음	vRealize Log Insight에서 구성된 Active Directory 서버에 연결할 수 없습니다.
이미 다른 시스템이 보유하고 있어서 고가용성 IP 주소[IP 주소]를 인수할 수 없음	<p>vRealize Log Insight 클러스터가 ILB(통합된 로드 밸런서)에 대해 구성된 IP 주소를 가져올 수 없습니다. 가장 일반적으로 이 알림은 동일한 네트워크 내의 다른 호스트가 IP 주소를 보유하고 있어서 클러스터가 해당 IP 주소를 가져올 수 없을 때 발생합니다.</p> <p>현재 IP 주소를 보유한 호스트의 IP 주소 할당을 해제하거나 Log Insight 통합된 로드 밸런서를 네트워크에서 사용 가능한 정적 IP 주소로 구성하여 이 충돌을 해결할 수 있습니다. ILB IP 주소를 변경할 때는 새 IP 주소 또는 이 IP 주소로 확인되는 FQDN/URL로 로그를 전송하도록 모든 클라이언트를 재구성해야 합니다. 또한 vSphere 통합 페이지에서 vRealize Log Insight와 통합된 모든 vCenter Server의 구성을 해제한 후 다시 구성해야 합니다.</p>

알림 이름	설명
노드 장애가 너무 많아 고가용성 IP 주소[IP 주소]를 사용할 수 없음	<p>ILB(통합 로드 밸런서)에 대해 구성된 IP 주소를 사용할 수 없습니다. ILB IP 주소 또는 이 IP 주소로 확인되는 FQDN/URL을 통해 vRealize Log Insight 클러스터로 로그를 전송하려는 클라이언트에 해당 IP 주소가 사용할 수 없는 것으로 표시됩니다. 가장 일반적으로 이 알림은 vRealize Log Insight 클러스터의 노드 대부분이 비정상이거나 사용할 수 없거나 기본 노드에서 연결할 수 없는 경우 발생합니다. NTP 시간 동기화가 사용되지 않았거나 구성된 NTP 서버 간의 시간 이동이 큰 경우에도 이 알림이 발생합니다. 가능한 경우 IP 주소를 ping해서 연결할 수 없는지 확인하여 문제가 계속되고 있는지를 확인할 수 있습니다.</p> <p>대부분의 클러스터 노드를 정상적이고 연결 가능한 상태로 만들고 NTP 시간 동기화를 사용하여 NTP 서버의 시간을 정확하게 하면 이 문제를 해결할 수 있습니다.</p>
vRealize Log Insight 노드 간 고가용성 IP 주소[사용자 IP 주소] 마이그레이션이 너무 많음	<p>ILB(통합된 로드 밸런서)에 대해 구성된 IP 주소가 지난 10분 동안 너무 많이 마이그레이션되었습니다.</p> <p>정상 작동 시에는 vRealize Log Insight 클러스터 노드 간에 IP 주소가 거의 이동하지 않습니다. 그러나 현재 소유자 노드가 다시 시작되거나 유지 보수 모드로 전환된 경우 IP 주소가 이동할 수 있습니다. Log Insight 클러스터 노드 간의 시간이 동기화되지 않아 클러스터가 올바르게 작동하지 못하는 경우에도 IP 주소가 이동할 수 있습니다. 후자의 경우에는 NTP 시간 동기화를 사용하여 NTP 서버의 시간을 정확하게 맞추으로써 문제를 해결할 수 있습니다.</p>
SSL 인증서 오류	<p>syslog 소스에서 SSL을 통해 vRealize Log Insight에 대한 연결을 시작했지만 연결이 비정상적으로 끊어졌습니다. 이 알림은 SSL 인증서의 유효성을 확인하는 데 syslog 소스를 사용할 수 없음을 나타낼 수 있습니다.</p> <p>vRealize Log Insight에서 SSL을 통해 syslog 메시지를 수락하기 위해서는 클라이언트의 확인을 거친 인증서가 필요하며 시스템의 클럭이 동기화되어야 합니다. SSL 인증서 또는 네트워크 시간 서비스에 문제가 있을 수 있습니다.</p> <p>syslog 소스에서 SSL 인증서를 신뢰함을 확인하거나, SSL을 사용하지 않도록 소스를 재구성하거나, SSL 인증서를 다시 설치할 수 있습니다.</p> <p>vRealize Log Insight 에이전트 SSL 매개 변수 구성 및 사용자 지정 SSL 인증서 설치 항목을 참조하십시오.</p>
vCenter 수집 실패	<p>vRealize Log Insight에서 vCenter 이벤트, 작업 및 정보를 수집할 수 없습니다. 수집 실패의 원인이 된 정확한 오류를 확인하고 현재 수집 작업이 작동 중인지 보려면 <code>/storage/var/loginsight/plugins/vsphere/li-vsphere.log</code> 파일을 확인하십시오.</p>

알림 이름	설명
이벤트 전달자 이벤트가 삭제됨	<p>전달자가 연결 또는 오버로드 문제로 인해 이벤트를 삭제합니다.</p> <p>예:</p> <pre>Log Insight Admin Alert: Event Forwarder Events Dropped This alert is about your Log Insight installation on https://<your_url> Event Forwarder Events Dropped triggered at 2016-08-02T18:41:06.972Z Log Insight just dropped 670 events for forwarder target 'Test', reason: Pending queue is full.</pre>
일정보다 늦은 경고 쿼리	vRealize Log Insight에서 구성된 시간에 사용자 정의 경고를 실행할 수 없습니다. 지연 이유는 하나 이상의 사용자 정의 경고가 비효율적이거나 시스템이 수집 및 쿼리 로드에서 적절한 크기가 아니기 때문일 수 있습니다.
경고 자동 사용 안 함 설정	사용자 정의 경고가 10번 이상 실행되고 평균 실행 시간이 1시간이 넘는 경우 경고는 비효율적인 것으로 간주하며 다른 사용자 정의 경고에 영향을 주지 않도록 사용 안 함으로 설정됩니다.
비효율적인 경고 쿼리	경고를 완료하는 데 1시간이 넘게 소요되는 경우 사용자 정의 경고는 비효율적인 것으로 간주합니다.

클러스터에 대한 시스템 알림

vRealize Log Insight는 새 클러스터 멤버 추가 또는 일시적인 노드 통신 문제를 포함하여 클러스터 토폴로지 변경에 관한 알림을 전송합니다.

보낸 사람	알림 이름	설명
기본 노드	새 작업자 노드에 대한 승인이 필요함	Worker 노드가 클러스터에 가입하기 위한 요청을 전송하고 있습니다. 관리자는 해당 요청을 승인하거나 거부해야 합니다.
기본 노드	새 작업자 노드가 승인됨	관리자가 vRealize Log Insight 클러스터에 참여하기 위한 작업자 노드의 멤버 자격 요청을 승인했습니다.
기본 노드	새 작업자 노드가 거부됨	관리자가 vRealize Log Insight 클러스터에 참여하기 위한 작업자 노드의 멤버 자격 요청을 거부했습니다. 요청이 실수로 거부된 경우 관리자는 작업자에서 해당 요청을 다시 배치한 다음, 기본 노드에서 이를 승인할 수 있습니다.
기본 노드	작업자 노드로 인해 지원되는 최대 노드가 초과됨	새 작업자 노드로 인해 Log Insight 클러스터의 작업자 노드 수가 지원되는 최대 수를 초과했습니다.
기본 노드	허용되는 노드가 초과됨, 새 작업자 노드가 거부됨	관리자가 클러스터에 허용되는 최대 노드 수보다 많은 노드를 추가하려고 했으며 해당 노드가 거부되었습니다.

보낸 사람	알림 이름	설명
기본 노드	작업자 노드의 연결이 끊김	이전에 연결된 worker 노드가 vRealize Log Insight 클러스터에서 연결이 끊어졌습니다.
기본 노드	작업자 노드가 다시 연결됨	worker 노드가 vRealize Log Insight 클러스터에 다시 연결되었습니다.
기본 노드	작업자 노드가 관리자에 의해 취소됨	관리자가 작업자 노드 멤버 자격을 취소했으며 노드가 더는 vRealize Log Insight 클러스터의 일부가 아닙니다.
기본 노드	알 수 없는 작업자 노드가 거부됨	작업자 노드가 기본 노드에 알려지지 않았기 때문에 vRealize Log Insight 기본 노드가 작업자 노드의 요청을 거부했습니다. 작업자가 올바른 노드이며 클러스터에 추가되어야 하는 경우 작업자 노드에 로그인하고 <code>/storage/core/loginsight/config/</code> 에서 해당 토큰 파일과 사용자 구성을 제거한 후 작업자 노드에서 <code>restart loginsight service</code> 를 실행합니다.
기본 노드	작업자 노드가 유지 보수 모드로 전환됨	작업자 노드가 유지 보수 모드로 전환되었으며 관리자가 해당 작업자 노드를 유지 보수 모드에서 제거해야 구성 변경 사항을 수신하고 쿼리를 지원할 수 있습니다.
기본 노드	작업자 노드가 서비스를 시작함	worker 노드가 유지 보수 모드를 종료하고 서비스 상태로 돌아왔습니다.
작업자 노드	기본 노드가 실패했거나 작업자 노드와 연결이 끊김	알림을 전송하는 작업자 노드가 vRealize Log Insight 기본 노드에 연결할 수 없습니다. 이 알림은 기본 노드가 실패했을 수 있으며 다시 시작해야 할 수 있음을 나타냅니다. 기본 노드가 실패한 경우 마스터 노드가 다시 온라인 상태가 될 때까지 클러스터를 구성하고 쿼리를 제출할 수 없습니다. 작업자 노드가 계속해서 메시지를 수집합니다. 참고 많은 작업자가 별도로 기본 노드 실패를 감지하고 알림을 생성할 수 있기 때문에 이러한 알림을 많이 수신할 수도 있습니다.
작업자 노드	기본 노드가 작업자 노드에 연결됨	알림을 전송하는 작업자 노드가 vRealize Log Insight 기본 노드에 다시 연결되었습니다.

vRealize Log Insight 시스템 알림에 대한 대상 구성

관리자는 시스템 알림이 트리거될 때 vRealize Log Insight가 수행하는 작업을 구성할 수 있습니다.

vRealize Log Insight는 디스크 공간이 거의 소비되어 vRealize Log Insight가 오래된 로그 파일을 삭제 또는 아카이브하기 시작해야 하는 것과 같은 중요한 시스템 이벤트가 발생할 때 시스템 알림을 생성합니다.

관리자는 이러한 이벤트에 대한 이메일 알림을 보내도록 vRealize Log Insight를 구성할 수 있습니다. 시스템 알림 이메일의 보낸 사람 주소는 관리 UI의 SMTP 구성 페이지에 있는 **보낸 사람** 텍스트 상자를 사용하여 관리자가 구성합니다. [vRealize Log Insight에 대한 SMTP 서버 구성](#) 항목을 참조하십시오.

관리자 사용자는 알림을 타사 애플리케이션에 전송할 수도 있습니다. [webhook을 사용하여 타사 제품에 시스템 알림 보내기 정보](#) 항목을 참조하십시오.

상태 알림을 전송하도록 vRealize Log Insight 구성


관리자는 자체 상태와 관련된 알림을 전송하도록 vRealize Log Insight를 구성할 수 있습니다.

이메일 메시지를 전달할 수 없는 경우 웹 인터페이스에 오류 알림이 표시됩니다.

사전 요구 사항

- 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.
- SMTP 서버가 vRealize Log Insight에 대해 구성되어 있는지 확인합니다. 자세한 내용은 [vRealize Log Insight에 대한 SMTP 서버 구성](#) 항목을 참조하십시오.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 구성 아래에서 **일반**을 클릭합니다.
- 3 경고 머리글 아래에서 시스템 알림을 설정합니다.
 - a **다음 이메일 주소로 시스템 알림 전송** 텍스트 상자에서 알림을 받을 이메일 주소를 입력합니다.
쉼표를 사용하여 여러 이메일 주소를 구분합니다.
 - b **알림 보존기간 임계값** 확인란을 선택하고 알림을 트리거하는 임계값을 설정합니다.
시스템에서 보관할 수 있는 데이터 양이 지정된 기간에 대해 충분하지 않은 경우 알림이 전송됩니다. 이 값은 현재 수집 속도에 따라 계산됩니다.
- 4 **저장**을 클릭합니다.
- 5 **Log Insight 다시 시작**을 클릭하여 변경 내용을 적용합니다.

타사 제품에 대한 vRealize Log Insight 시스템 알림 구성


관리자는 자체 상태와 관련된 알림을 타사 애플리케이션에 전송하도록 vRealize Log Insight를 구성할 수 있습니다.

vRealize Log Insight는 디스크 공간이 거의 소비되어 vRealize Log Insight가 오래된 로그 파일을 삭제하기 시작해야 하는 것과 같은 중요한 시스템 이벤트가 발생할 때 이러한 알림을 생성합니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘  을 클릭하고 **관리**를 선택합니다.
- 2 구성 아래에서 **일반**을 클릭합니다.
- 3 경고 머리글 아래에서 시스템 알림을 설정합니다.
 - a **HTTP Post 시스템 알림 전송 대상** 텍스트 상자에 알림을 받을 이메일 주소를 입력합니다.
 - b (선택 사항) **용량이 다음 값 이하로 떨어질 때 알림 보내기** 확인란 및 관련 임계값이 환경에 맞게 구성되어 있는지 확인합니다.
- 4 **저장**을 클릭합니다.

다음에 수행할 작업

알림에 대한 webhook 출력 작업을 통해 vRealize Log Insight webhook 형식을 타사 애플리케이션에 사용되는 형식으로 매핑하는 shim을 생성합니다.

webhook을 사용하여 타사 제품에 시스템 알림 보내기 정보

webhook을 사용하여 타사 제품에 vRealize Log Insight 시스템 알림을 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.

vRealize Log Insight webhook 구현에서는 원격 서버에 대한 아웃바운드 HTTP 요청을 수행합니다. 서버는 성공 또는 실패와 실패 시 vRealize Log Insight 재시도 횟수를 보고할 수 있습니다. 모든 HTTP/2xx 상태 코드 응답은 성공으로 처리되며 다른 모든 응답(시간 초과 또는 연결 거부 포함)은 나중에 다시 시도될 수 있도록 실패로 처리됩니다.

메시지 쿼리와 함께 생성된 경고, 집계 쿼리와 함께 생성된 경고 및 시스템 알림은 각각 고유한 webhook 형식을 갖습니다.

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

시스템 알림에 대한 webhook 형식

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

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

시스템 알림에 대한 webhook 형식

다음 예는 시스템 알림에 대한 vRealize Log Insight webhook 형식을 보여 줍니다.

```
{
  "AlertName": " Admin Alert: Worker node has returned to service  (Host =
127.0.0.2)",
  "messages": [
    {
      "text": "This notification was generated from Log Insight node (Host =
127.0.0.2,
      Node Identifier = a31cad22-65c2-4131-8e6c-27790892alf9).
      A worker node has returned to service after having been in maintenance mode.
      The Log Insight master node reports that worker node has finished maintenance
      and exited maintenance mode. The node will resume receiving configuration
      changes and
      serving queries. The node is also now ready to start receiving incoming log
      messages."

      "timestamp": 1458665320514, "fields": []
    }
  ]
}
```

vRealize Log Insight 이벤트 전달 대상 추가

syslog 또는 수집 API 대상으로 수신 이벤트를 전달하도록 vRealize Log Insight 서버를 구성할 수 있습니다.

이벤트 전달을 사용하여 vRealize Log Insight, syslog 또는 둘 모두 등 하나 이상의 원격 대상에 필터링되거나 태그가 지정된 이벤트를 전송합니다. 이벤트 전달은 SIEM 등의 기존 로깅 도구를 지원하고 DMZ 또는 WAN 등의 다양한 네트워크에서 로깅을 통합하는 데 사용할 수 있습니다.

이벤트 전달자는 독립형이거나 클러스터 방식일 수 있지만 이벤트 전달자는 원격 대상과는 별도의 인스턴스입니다. 또한 이벤트 전달에 구성된 인스턴스는 로컬로 이벤트를 저장하고 데이터를 쿼리하는 데 사용할 수 있습니다.


[전달된 이벤트] 페이지에서 필터를 생성하는 데 사용하는 연산자는 대화형 분석 페이지에서 사용하는 필터와 다릅니다. **대화형 분석에서 실행** 메뉴 항목을 사용하여 이벤트 필터의 결과를 미리 보는 방법에 대한 자세한 내용은 **대화형 분석에서 이벤트 전달 필터 사용** 항목을 참조하십시오.

사전 요구 사항

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.

전달된 이벤트 수를 대상에서 처리할 수 있는지 확인합니다. 대상 클러스터가 전달 인스턴스보다 훨씬 더 작은 경우 일부 이벤트가 삭제될 수 있습니다.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **이벤트 전달**을 클릭합니다.
- 3 **+새 대상**을 클릭하고 다음 정보를 제공합니다.

옵션	설명
이름	새 대상의 고유 이름입니다.
호스트	IP 주소 또는 정규화된 도메인 이름입니다.
	<p>경고 전달 루프는 vRealize Log Insight 클러스터가 이벤트를 자기 자신에게 전달하거나, 이벤트를 다른 클러스터에 전달하면 이 클러스터에서 이를 다시 원래 클러스터로 전달하는 구성입니다. 이러한 루프는 전달된 각 이벤트 복사본을 무한 개수만큼 생성할 수 있습니다. vRealize Log Insight 웹 인터페이스는 이벤트가 자체 전달되도록 구성하는 것을 허용하지 않습니다. 그렇지만 vRealize Log Insight는 vRealize Log Insight 클러스터 A에서 클러스터 B로 전달하고 B에서 A에 동일한 이벤트를 다시 전달하는 것과 같은 간접 전달 루프를 방지할 수 없습니다. 전달 대상을 생성할 때는 간접 전달 루프를 생성하지 않도록 주의하십시오.</p>
프로토콜	<p>수집 API, syslog 또는 RAW. 기본값은 수집 API(CFAPI)입니다.</p> <p>수집 API를 사용하여 이벤트가 전달되는 경우 이벤트의 원래 소스가 소스 필드에 보존됩니다. 이벤트가 syslog를 사용하여 전달되는 경우 이벤트의 원래 소스가 손실되고 메시지 소스가 vRealize Log Insight 전달자의 IP 주소 또는 호스트 이름으로 수신기에 기록될 수 있습니다. RAW를 사용하여 이벤트가 전달되면 이 동작은 syslog와 유사하지만 syslog RFC 준수가 보장되지 않습니다. RAW는 vRealize Log Insight에 의해 추가된 사용자 지정 syslog 헤더 없이, 이벤트를 수신된 방식과 정확하게 동일한 방식으로 전달합니다. 이 프로토콜은 원래 형식의 syslog 이벤트를 필요로 하므로 타사 대상에 유용합니다.</p> <p>참고 이벤트 전달자에서 선택된 프로토콜에 따라 소스 필드가 다른 값을 가질 수 있습니다.</p> <ul style="list-style-type: none"> a 수집 API의 경우 소스는 처음 보낸 사람(이벤트 발신자)의 IP 주소입니다. b syslog 및 RAW의 경우 소스는 이벤트 전달자의 vRealize Log Insight 인스턴스 IP 주소입니다. 또한 메시지 텍스트에는 처음 보낸 사람의 IP 주소를 가리키는 <code>_li_source_path</code>가 포함되어 있습니다.
SSL 사용	수집 API에 대해 SSL과의 연결을 선택적으로 보안을 할 수 있습니다. 전달 대상에서 제공한 SSL 인증서를 신뢰할 수 없는 경우 이 구성을 테스트하거나 저장할 때 인증서를 수락할 수 있습니다.

옵션	설명
태그	미리 정의된 값으로 태그 쌍을 선택적으로 추가할 수 있습니다. 태그는 더 쉽게 이벤트를 쿼리할 수 있도록 해줍니다. 선택으로 구분된 태그는 여러 개 추가할 수 있습니다.
보조 태그 전달	syslog에 대한 보조 태그를 전달할지 여부를 선택할 수 있습니다. 보조 태그는 'vc_username' 또는 'vc_vmname'과 같이 클러스터 자체에 의해 추가되는 태그로, 소스에서 직접 가져온 태그와 함께 전달될 수 있습니다. 보조 태그는 수집 API가 사용될 때 항상 전달됩니다.
전송	syslog에 대한 전송 프로토콜을 선택합니다. UDP 또는 TCP를 선택할 수 있습니다.

4 (선택 사항) 전달할 이벤트를 제어하려면 **+** 필터 추가를 클릭합니다.

원하는 이벤트를 정의하려면 필드와 제약 조건을 선택합니다. 정적 필드만 필터로 사용할 수 있습니다. 필터를 선택하지 않으면 모든 이벤트가 전달됩니다. **대화형 분석에서 실행**을 클릭하여 작성 중인 필터의 결과를 확인할 수 있습니다.

연산자	설명
일치	문자열 및 와일드카드 규칙과 일치하는 문자열을 찾습니다. 여기서 *는 0개 이상의 문자를 의미하고 ?는 0개 또는 1개의 문자를 의미합니다. 전위 및 후위 와일드카드 사용이 지원됩니다. 예를 들어, *test*는 test123 또는 my-test-run과 같은 문자열과 일치합니다.
일치하지 않음	문자열 및 와일드카드 규칙과 일치하는 문자열을 제외합니다. 여기서 *는 0개 이상의 문자를 의미하고 ?는 0개 또는 1개의 문자를 의미합니다. 전위 및 후위 와일드카드 사용이 지원됩니다. 예를 들어 test*는 test123을 제외하지만 mytest123은 제외하지 않습니다. ?test*는 test123 및 xtest123을 제외하지만 mytest123은 제외하지 않습니다.
다음으로 시작	지정된 문자 또는 문자열로 시작하는 문자열을 찾습니다. 예를 들어 test는 test123 또는 test는 찾지만 my-test123은 찾지 않습니다.
다음으로 시작하지 않음	지정된 문자 또는 문자열로 시작하는 문자열을 제외합니다. 예를 들어 test는 test123을 필터링하여 제외하지만 my-test123은 제외하지 않습니다.

5 (선택 사항) 다음 전달 정보를 수정하려면 **고급 설정 표시**를 클릭합니다.

옵션	설명
포트	원격 대상에서 이벤트가 전송될 포트입니다. 기본값은 프로토콜에 따라 설정됩니다. 원격 대상이 다른 포트에서 수신하는 경우를 제외하고 이를 변경하지 마십시오.
작업자 수	사용할 동시 나가는 연결 수입니다. 전달되는 대상으로의 네트워크 지연 시간이 길수록, 전달 중인 해당 이벤트 수가 많을수록 작업자 수를 높게 설정하십시오. 기본값은 8입니다.

6 구성을 확인하고 **테스트**를 클릭합니다.

- 7 전달 대상이 신뢰할 수 없는 SSL 인증서를 제공하는 경우 인증서의 세부 정보가 포함된 대화상자가 나타납니다. **수락**을 클릭하여 vRealize Log Insight 클러스터에 있는 모든 노드의 신뢰 저장소에 인증서를 추가합니다.

취소를 클릭하면 인증서가 신뢰 저장소에 추가되지 않고, 전달 대상과의 연결이 실패합니다. 연결에 성공하려면 인증서를 수락해야 합니다.

- 8 **저장**을 클릭합니다.

구성을 테스트하지 않았으며, 대상에서 신뢰할 수 없는 인증서를 제공하는 경우 7단계의 지침을 따르십시오.

다음에 수행할 작업

이벤트 전달 대상을 편집 또는 복제할 수 있습니다. 대상을 편집하여 이벤트 전달자 이름을 변경하는 경우에는 모든 통계가 재설정됩니다.

대화형 분석에서 이벤트 전달 필터 사용

이벤트 필터에서 사용되는 연산자와 대화형 분석의 필터에 사용되는 연산자는 이름이 일대일로 대응되지 않습니다. 하지만 두 형식에서 비슷한 결과를 생성하는 연산자를 선택할 수 있습니다.

이러한 차이는 **이벤트 전달** 페이지에서 **대화형 분석에서 실행** 메뉴 항목을 사용하는 경우에 중요합니다. 예를 들어, 이벤트 전달 필터 **matches*foo***를 사용하고 이벤트 필터 페이지에서 **대화형 분석에서 실행** 메뉴 항목을 선택하면 대화형 분석 쿼리는 이벤트 전달 필터를 동일한 모든 이벤트를 일치시키지는 못할 수 있는 **match regexp^.*foo.*\$**와 동일하게 취급합니다.

또 다른 예로 **matchesfoo**가 있습니다. 대화형 분석에서 실행하면 **foo**와 동일하게 취급됩니다. 이 대화형 분석 함수는 키워드 쿼리도 검색하므로 **containsfoo**는 **matchesfoo**보다 더 많은 이벤트를 일치시킬 수 있습니다.

대화형 분석에서 사용되는 연산자를 변경하여 이러한 차이를 해결할 수 있습니다.

- **contains** 연산자는 **matches regex**로 변경합니다.
- 이벤트 전달 필터에서 *****가 나오는 모든 경우를 **.***과 **.***이 있는 점두사 필터 용어로 변경합니다. 예를 들어 이벤트 필터 표현식 **matches*foo***를 대화형 분석의 경우 **matches regex.*foo.***로 변경합니다.
- 이벤트 필터의 **does not match** 연산자의 경우 정규식 look ahead 값과 함께 **matches regex** 연산자를 사용할 수 있습니다. 예를 들어, **does not match*foo***는 **matches regex .*(?!foo).***와 같습니다.

vRealize Log Insight 가상 장치의 시간 동기화

vRealize Log Insight 가상 장치의 시간을 해당 가상 장치를 배포한 ESX/ESXi 호스트와 동기화하거나 NTP 서버와 동기화해야 합니다.


시간은 vRealize Log Insight의 핵심 기능에 중요합니다.

기본적으로 vRealize Log Insight는 시간을 미리 정의된 공용 NTP 서버 목록과 동기화합니다. 방화벽으로 인해 공용 NTP 서버에 액세스할 수 없는 경우 회사의 내부 NTP 서버를 사용할 수 있습니다. NTP 서버를 사용할 수 없는 경우 vRealize Log Insight 가상 장치를 배포한 ESX/ESXi 호스트와 시간을 동기화할 수 있습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 구성 아래에서 **시간**을 클릭합니다.
- 3 **시간 동기화 대상** 드롭다운 메뉴에서 시간 소스를 선택합니다.

옵션	설명
NTP 서버	vRealize Log Insight 가상 장치의 시간을 나열된 NTP 서버 중 하나와 동기화합니다.
ESX/ESXi 호스트	vRealize Log Insight 가상 장치의 시간을 해당 가상 장치를 배포한 ESX/ESXi 호스트와 동기화합니다.

- 4 (선택 사항) NTP 서버 동기화를 선택한 경우 NTP 서버 주소를 나열한 후 **테스트**를 클릭합니다.

참고 NTP 서버에 대한 연결 테스트에는 서버당 최대 20초가 걸릴 수 있습니다.

- 5 **저장**을 클릭합니다.

vRealize Log Insight에 대한 SMTP 서버 구성


vRealize Log Insight가 이메일 알림을 전송할 수 있도록 SMTP를 구성할 수 있습니다.

시스템 알림은 vRealize Log Insight가 가상 장치의 스토리지 용량이 사용자가 설정한 임계값에 도달하는 등의 중요한 시스템 이벤트를 감지할 때 생성됩니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 구성 아래에서 **SMTP**를 클릭합니다.

3 SMTP 서버 주소 및 포트 번호를 입력합니다.

4 SMTP 서버가 암호화된 연결을 사용하는 경우 암호화 프로토콜을 선택합니다.

5 **보낸 사람** 텍스트 상자에 시스템 알림을 전송할 때 사용할 이메일 주소를 입력합니다.

보낸 사람 주소는 시스템 알림 이메일에서 보낸 사람 주소로 표시됩니다. 이 주소는 실제 주소일 필요가 없으며 vRealize Log Insight의 특정 인스턴스를 나타내는 정보일 수 있습니다. 예를 들어, **loginsight@example.com**과 같습니다.

6 시스템 알림을 전송할 때 SMTP 서버를 통해 인증하기 위한 사용자 이름과 암호를 입력합니다.

7 대상 이메일을 입력하고 **테스트 이메일 보내기**를 클릭하여 연결을 확인합니다.

8 SMTP 서버가 신뢰할 수 없는 SSL 인증서를 제공하는 경우 인증서의 세부 정보가 포함된 대화상자가 나타납니다. **수락**을 클릭하여 vRealize Log Insight 클러스터에 있는 모든 노드의 신뢰 저장소에 인증서를 추가합니다.

취소를 클릭하면 인증서가 신뢰 저장소에 추가되지 않고, SMTP 서버와의 연결이 실패합니다. 연결에 성공하려면 인증서를 수락해야 합니다.

9 **저장**을 클릭합니다.

연결을 테스트하지 않았으며, SMTP 서버에서 신뢰할 수 없는 인증서를 제공하는 경우 8단계의 지침을 따르십시오.

사용자 지정 SSL 인증서 설치

기본적으로 vRealize Log Insight는 가상 장치에 자체 서명된 SSL 인증서를 설치합니다.

vRealize Log Insight 웹 사용자 인터페이스에 연결하면 자체 서명된 인증서가 보안 경고를 생성합니다. 자체 서명된 보안 인증서를 사용하지 않으려는 경우 사용자 지정 SSL 인증서를 설치할 수 있습니다. 사용자 지정 SSL 인증서가 필요한 유일한 기능은 SSL을 통한 이벤트 전달 기능입니다. ILB가 사용되도록 설정된 클러스터가 있는 경우 **통합된 로드 밸런서 사용** 항목을 참조하여 사용자 지정 SSL 인증서 관련 요구 사항을 확인하십시오.

참고 vRealize Log Insight 웹 사용자 인터페이스 및 Log Insight Ingestion 프로토콜 cfapi는 동일한 인증서를 사용하여 인증합니다.

사전 요구 사항

- 사용자 지정 SSL 인증서가 다음 요구 사항을 충족하는지 확인합니다.
 - CommonName에는 가상 IP 주소의 마스터 노드 또는 FQDN에 대한 와일드카드 또는 정확한 일치 항목이 포함됩니다. 경우에 따라 다른 모든 IP 주소 및 FQDN이 subjectAltName으로 나열됩니다.
 - 인증서 파일에 올바른 개인 키와 올바른 인증서 체인이 모두 포함되어 있어야 합니다.
 - 개인 키가 RSA 또는 DSA 알고리즘을 통해 생성되어야 합니다.

- 개인 키가 암호를 통해 암호화되지 않아야 합니다.
- 인증서가 다른 인증서 체인을 통해 서명되는 경우 가져올 인증서 파일에 다른 모든 인증서가 포함되어 있어야 합니다.
- 인증서 파일에 포함된 개인 키 및 모든 인증서가 PEM으로 인코딩되어야 합니다. vRealize Log Insight는 DER로 인코딩된 인증서 및 개인 키를 지원하지 않습니다.
- 인증서 파일에 포함된 개인 키 및 모든 인증서가 PEM 형식이어야 합니다. vRealize Log Insight는 PFX, PKCS12, PKCS7 또는 다른 형식의 인증서를 지원하지 않습니다.
- 다음 순서로 각 인증서의 전체 본문을 단일 텍스트 파일 내에 연결해야 합니다.
 - a 개인 키 - `your_domain_name.key`
 - b 기본 인증서 - `your_domain_name.crt`
 - c 중간 인증서 - `DigiCertCA.crt`
 - d 루트 인증서 - `TrustedRoot.crt`
- 각 인증서의 시작 및 끝 태그를 다음 형식으로 포함했는지 확인합니다.

```

-----BEGIN PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----

```

- 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.

절차

1 자체 서명된 인증서 생성

OpenSSL 도구를 사용하여 Windows 또는 Linux에 대한 자체 서명된 인증서를 생성할 수 있습니다.

2 인증서 서명 요청 생성

Windows용 OpenSSL 도구를 사용하여 인증서 서명 요청을 생성합니다.

3 인증 기관의 서명 요청

원하는 인증 기관에 인증서 서명 요청을 전송하고 서명을 요청합니다.

4 인증서 파일 연결

키 및 인증서 파일을 PEM 파일에 결합합니다.

5 서명된 인증서 업로드

서명된 SSL 인증서를 업로드할 수 있습니다.

6 vRealize Log Insight 서버 및 Log Insight Agents 간 SSL 연결 구성

SSL 기능을 사용하면 수집 API의 보안 흐름을 통해 Log Insight Agents 및 vRealize Log Insight 서버 간에 SSL 전용 연결을 제공할 수 있습니다. 또한 Log Insight Agents의 다양한 SSL 매개 변수를 구성할 수 있습니다.

자체 서명된 인증서 생성

OpenSSL 도구를 사용하여 Windows 또는 Linux에 대한 자체 서명된 인증서를 생성할 수 있습니다.

사전 요구 사항

- <https://www.openssl.org/community/binaries.html>에서 OpenSSL을 위한 적절한 설치 관리자를 다운로드합니다. 다운로드한 OpenSSL 설치 관리자를 사용하여 Windows에 OpenSSL을 설치합니다.
- openssl.cfg 파일을 편집하여 필수 매개 변수를 더 추가합니다. [req] 섹션에 req_extensions 매개 변수가 정의되어 있는지 확인합니다.

```
[req]
.
.
req_extensions=v3_req #
```

- 서버의 호스트 이름 또는 IP 주소에 대해 적합한 주체 대체 이름(예: *server-01.loginsight.domain*)을 추가합니다. 호스트 이름의 패턴을 지정할 수 없습니다.

```
[v3_req]
.
.
subjectAltName=DNS:server-01.loginsight.domain
#subjectAltName=IP:10.27.74.215
```

절차

- 1 인증서 파일을 저장할 폴더(예: C:\Certs\LogInsight)를 생성합니다.
- 2 명령 프롬프트를 열고 다음 명령을 실행합니다.

```
C:\Certs\LogInsight>openssl req -x509 -nodes -newkey 2048 -keyout server.key -out server.crt -days 3650
```

OpenSSL에서는 국가, 조직 등을 포함한 인증서 속성을 제공하라는 메시지를 표시합니다.

- 3 vRealize Log Insight 서버의 정확한 IP 주소나 호스트 이름 또는 로드 밸런싱이 사용되는 경우 vRealize Log Insight 클러스터 주소를 입력합니다.

이 속성은 값을 반드시 지정해야 하는 유일한 속성입니다.

결과

2개의 파일 `server.key` 및 `server.crt`가 생성됩니다.

- `server.key`는 새로운 PEM 인코딩 개인 키입니다.
- `server.crt`는 `server.key`로 서명된 새로운 PEM 인코딩 인증서입니다.

인증서 서명 요청 생성

Windows용 OpenSSL 도구를 사용하여 인증서 서명 요청을 생성합니다.

사전 요구 사항

- OpenSSL 도구를 설치합니다. OpenSSL 도구를 가져오는 방법에 대한 내용은 <http://www.openssl.org>를 참조하십시오.
- `openssl.cfg` 파일을 편집하여 필수 매개 변수를 더 추가합니다. `[req]` 섹션에 `req_extensions` 매개 변수가 정의되어 있는지 확인합니다.

```
[req]
.
.
req_extensions=v3_req #
```

- 서버의 호스트 이름 또는 IP 주소에 대해 적합한 주제 대체 이름(예: `server-01.loginsight.domain`)을 추가합니다. 호스트 이름의 패턴을 지정할 수 없습니다.

```
[v3_req]
.
.
subjectAltName=DNS:server-01.loginsight.domain
#subjectAltName=IP:10.27.74.215
```

절차

- 1 인증서 파일을 저장할 폴더(예: `C:\Certs\LogInsight`)를 생성합니다.
- 2 명령 프롬프트를 열고 다음 명령을 실행하여 개인 키를 생성합니다.

```
C:\Certs\LogInsight>openssl genrsa -out server.key 2048
```

- 3 다음 명령을 실행하여 인증서 서명 요청을 생성합니다.

```
C:\Certs\LogInsight>openssl req -new -key server.key -out server.csr
```

참고 이 명령은 대화식으로 실행되고 많은 질문을 합니다. 인증 기관에서는 답변을 비교 검토합니다. 답변은 회사 등록에 관한 법적 문서와 일치해야 합니다.

- 4 화면상의 지침을 따르고 인증서 요청에 통합될 정보를 입력합니다.

중요 일반 이름 필드에서 서버의 호스트 이름 또는 IP 주소(예: **mail.your.domain**)를 입력합니다. 모든 하위 도메인을 포함하려면 ***your.domain**을 입력합니다.

결과

인증서 서명 요청 파일 `server.csr`이 생성 및 저장됩니다.

인증 기관의 서명 요청

원하는 인증 기관에 인증서 서명 요청을 전송하고 서명을 요청합니다.

절차

- ◆ `server.csr` 파일을 인증 기관에 제출합니다.

참고 파일을 PEM 형식으로 인코딩하도록 인증 기관에 요청합니다.

인증 기관은 요청을 처리한 후 PEM 형식으로 인코딩된 `server.crt` 파일을 다시 전송합니다.

인증서 파일 연결

키 및 인증서 파일을 PEM 파일에 결합합니다.

절차

- 1 새 `server.pem` 파일을 생성한 후 텍스트 편집기에서 엽니다.
- 2 `server.key` 파일의 콘텐츠를 복사한 후 다음 형식을 사용하여 `server.pem`에 붙여 넣습니다.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
```

- 3 CA(인증 기관)에서 받은 `server.crt` 파일의 콘텐츠를 복사하고 다음 형식을 사용하여 `server.pem`에 붙여넣습니다.

```
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
```

- 인증 기관에서 중간 또는 체인 인증서를 제공한 경우 해당 중간 또는 체인 인증서를 다음과 같은 형식으로 공용 인증서 파일의 끝에 추가합니다.


```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

- server.pem 파일을 저장합니다.

서명된 인증서 업로드

서명된 SSL 인증서를 업로드할 수 있습니다.

절차

- 구성 드롭다운 메뉴 아이콘  을 클릭하고 **관리**를 선택합니다.
- 구성 아래에서 **SSL 인증서**를 클릭합니다.
- 사용자 지정 SSL 인증서를 찾은 후 **열기**를 클릭합니다.
- 저장**을 클릭합니다.
- vRealize Log Insight을 다시 시작합니다.

다음에 수행할 작업

vRealize Log Insight를 다시 시작한 후 ESXi의 syslog 피드가 vRealize Log Insight에 계속 도착하는지 확인합니다.

vRealize Log Insight 서버 및 Log Insight Agents 간 SSL 연결 구성

SSL 기능을 사용하면 수집 API의 보안 흐름을 통해 Log Insight Agents 및 vRealize Log Insight 서버 간에 SSL 전용 연결을 제공할 수 있습니다. 또한 Log Insight Agents의 다양한 SSL 매개 변수를 구성할 수 있습니다.

vRealize Log Insight 에이전트는 TLSv.1.2를 통해 통신합니다. SSLv.3/TLSv.1.0은 보안 지침 준수를 위해 사용되지 않도록 설정됩니다.

기본 SSL 기능

기본 SSL 기능을 이해하면 Log Insight Agents를 제대로 구성하는 데 도움이 됩니다.

vRealize Log Insight Agent는 인증서를 저장하고, 특정 서버에 대한 첫 번째 연결을 제외하고 모든 연결 과정에서 서버 ID를 확인하는 데 해당 인증서를 사용합니다. 서버 ID가 확인되지 않으면 vRealize Log Insight Agent는 서버와의 연결을 거부하고 로그에 적합한 오류 메시지를 기록합니다. Agent에서 수신한 인증서는 cert 폴더에 저장됩니다.

- Windows의 경우 C:\ProgramData\VMware\Log Insight Agent\cert로 이동합니다.
- Linux의 경우 /var/lib/loginsight-agent/cert로 이동합니다.

vRealize Log Insight Agent가 vRealize Log Insight 서버와 보안 연결을 설정하는 경우 Agent는 유효성 검증을 위해 vRealize Log Insight 서버에서 수신한 인증서를 확인합니다. vRealize Log Insight Agent는 시스템에서 신뢰할 수 있는 루트 인증서를 사용합니다.

- Log Insight Linux Agent는 /etc/pki/tls/certs/ca-bundle.crt 또는 /etc/ssl/certs/ca-certificates.crt에서 신뢰할 수 있는 인증서를 로드합니다.
- Log Insight Windows Agent는 시스템 루트 인증서를 사용합니다.

자체 서명된 인증서가 로컬에 저장된 vRealize Log Insight Agent의 경우 동일한 공개 키를 사용하는 다른 유효 자체 서명된 인증서가 수신되면 해당 새 인증서를 수락합니다. 이는 자체 서명된 인증서가 동일한 개인 키를 사용하지만 다른 세부 정보(예: 새로운 만료 날짜)를 사용하여 재생성되는 경우에 발생할 수 있습니다. 그 외의 경우에는 연결이 거부됩니다.

자체 서명된 인증서가 로컬에 저장된 vRealize Log Insight Agent의 경우 CA 서명된 유효 인증서가 수신되면 vRealize Log Insight Agent는 자동으로 수락된 새 인증서를 바꿉니다.

CA 서명된 인증서를 보유한 vRealize Log Insight Agent에 자체 서명된 인증서가 수신되면 Log Insight Agent는 해당 인증서를 거부합니다. vRealize Log Insight Agent는 vRealize Log Insight 서버와 처음으로 연결하는 경우에만 해당 서버에서 수신된 자체 서명된 인증서를 수락합니다.

CA 서명된 인증서가 로컬에 저장된 vRealize Log Insight Agent의 경우 다른 신뢰할 수 있는 CA에서 서명한 유효 인증서가 수신되면 Agent는 해당 인증서를 거부합니다. 새 인증서를 수락하도록 vRealize Log Insight Agent의 구성 옵션을 수정할 수 있습니다. [vRealize Log Insight 에이전트 SSL 매개 변수 구성 항목](#)을 참조하십시오.

vRealize Log Insight 에이전트는 TLSv.1.2를 통해 통신합니다. SSLv.3/TLSv.1.0은 보안 지침 준수를 위해 사용되지 않도록 설정됩니다.

SSL 전용 연결 적용


vRealize Log Insight 웹 사용자 인터페이스를 사용하여 vRealize Log Insight Agents 및 Ingestion API가 서버로의 SSL 연결만 허용하도록 구성할 수 있습니다.

vRealize Log Insight API는 일반적으로 포트 9000의 HTTP 및 포트 9543의 HTTPS를 통해 연결할 수 있습니다. 두 포트는 vRealize Log Insight Agent 또는 사용자 지정 API 클라이언트에서 사용될 수 있습니다. 인증된 모든 요청에는 SSL이 필요하지만 vRealize Log Insight Agent 수집 트래픽을 비롯한 인증되지 않은 요청은 두 방법 중 하나를 통해 수행될 수 있습니다. 강제로 모든 API 요청에 SSL 연결이 사용되도록 할 수 있습니다. 이 옵션은 syslog 포트 514 트래픽을 제한하지 않으며 vRealize Log Insight 사용자 인터페이스에 영향을 미치지 않습니다. 이 인터페이스에서 HTTP 포트 80 요청은 HTTPS 포트 443으로 계속 리디렉션됩니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 구성 아래에서 **SSL**을 클릭합니다.
- 3 [API 서버 SSL]에서 **SSL 연결 필요**를 선택합니다.
- 4 **저장**을 클릭합니다.

결과

vRealize Log Insight API는 서버와의 SSL 연결만 허용합니다. SSL 이외의 연결은 거부됩니다.

vRealize Log Insight 에이전트 SSL 매개 변수 구성

vRealize Log Insight 에이전트 구성 파일을 편집하여 SSL 구성을 변경하고, 신뢰할 수 있는 루트 인증서에 대한 경로를 추가하고, 에이전트가 인증서를 수락하는지 여부를 지정할 수 있습니다.

이 절차는 Windows 및 Linux용 vRealize Log Insight 에이전트에 적용됩니다.

사전 요구 사항

vRealize Log Insight Linux 에이전트:

- **루트**로 로그인하거나 `sudo`를 사용하여 콘솔 명령을 실행합니다.
- vRealize Log Insight Linux 에이전트를 설치한 Linux 시스템에 로그인하고, 콘솔을 연 후 `pgrep liagent`를 실행하여 vRealize Log Insight Linux 에이전트가 설치되어 실행 중인지 확인합니다.

vRealize Log Insight Windows 에이전트:

- vRealize Log Insight Windows 에이전트가 설치된 Windows 시스템에 로그인하고 서비스 관리자를 시작하여 vRealize Log Insight 에이전트 서비스가 설치되었는지 확인합니다.

절차

- 1 `liagent.ini` 파일을 포함하는 폴더로 이동합니다.

운영 체제	경로
Linux	<code>/var/lib/loginsight-agent/</code>
Windows	<code>%ProgramData%\VMware\Log Insight Agent</code>

- 2 텍스트 편집기에서 `liagent.ini` 파일을 엽니다.
- 3 `liagent.ini` 파일의 `[server]` 섹션에 다음 키를 추가합니다.

키	설명
<code>ssl_ca_path</code>	<p>연결 피어 인증서를 확인하는 데 사용되는, 루트 CA(인증 기관)에서 서명한 인증서에 대한 기본 스토리지 경로를 재정의합니다.</p> <p><code>ssl_ca_path</code>에 대한 경로를 제공하는 경우 Linux 및 Windows 에이전트에 대한 기본값이 재정의됩니다. PEM 형식의 여러 인증서가 연결되거나 인증서를 포함하는 디렉토리가 PEM 형식이고 이름이 <code>hash.0</code> 형식인 경우 파일을 사용할 수 있습니다. (x509 유틸리티의 <code>-hash</code> 옵션을 참조하십시오.)</p> <p>Linux: 값을 지정하지 않으면 에이전트는 <code>LI_AGENT_SSL_CA_PATH</code> 환경 변수에 할당된 값을 사용합니다. 해당 값이 없으면 에이전트는 <code>/etc/pki/tls/certs/ca-bundle.crt</code> 파일 또는 <code>/etc/ssl/certs/ca-certificates.crt</code> 파일에서 신뢰할 수 있는 인증서 로드를 시도합니다.</p> <p>Windows: 값을 지정하지 않으면 에이전트는 <code>LI_AGENT_SSL_CA_PATH</code> 환경 변수로 지정된 값을 사용합니다. 해당 값이 없으면 vRealize Log Insight Windows 에이전트는 Windows 루트 인증서 스토어에서 인증서를 로드합니다.</p>
<code>ssl_accept_any</code>	<p>vRealize Log Insight 에이전트에서 인증서를 수락하는지 여부를 정의합니다. 가능한 값은 <code>yes</code>, <code>1</code>, <code>no</code> 또는 <code>0</code>입니다. 값을 <code>yes</code> 또는 <code>1</code>로 설정하면 에이전트가 서버의 인증서를 수락하고 데이터 전송을 위한 보안 연결을 설정합니다. 기본값은 <code>no</code>입니다.</p>

키	설명
ssl_accept_any_trusted	가능한 값은 yes, 1, no 또는 0입니다. 신뢰할 수 있는 CA(인증 기관)에서 서명한 인증서가 로컬에 저장된 vRealize Log Insight 에이전트의 경우 다른 신뢰할 수 있는 CA(인증 기관)에서 서명한 유효 인증서가 수신되면 구성 옵션을 확인합니다. 값이 yes 또는 1로 설정되어 있으면 에이전트는 유효한 새 인증서를 수락합니다. 값이 no 또는 0으로 설정되어 있으면 Agent는 인증서를 거부하고 연결을 종료합니다. 기본값은 no입니다.
ssl_cn	자체 서명된 인증서의 Common Name입니다. 기본값은 VMware vCenter Log Insight입니다. 인증서의 Common Name 필드와 비교하여 확인할 사용자 지정 Common Name을 정의할 수 있습니다. vRealize Log Insight 에이전트는 [server] 섹션의 hostname 키에 대해 지정된 호스트 이름과 수신된 인증서의 Common Name 필드를 비교합니다. 일치하지 않는 경우 에이전트는 liagent.ini 파일의 ssl_cn 키와 Common Name 텍스트 상자를 비교하여 확인합니다. 값이 일치하면 vRealize Log Insight 에이전트는 인증서를 수락합니다.

참고 이러한 키는 SSL이 사용되지 않도록 설정되면 무시됩니다.

4 liagent.ini 파일을 저장한 후 닫습니다.

예제: 구성

다음은 SSL 구성 예입니다.

```
proto=cfapi
port=9543
ssl=yes
ssl_ca_path=/etc/pki/tls/certs/ca-bundle.crt
ssl_accept_any=no
ssl_accept_any_trusted=yes
ssl_cn=LOGINSIGHT
```


SSL 인증서 보기 및 제거

수락된 후 vRealize Log Insight 클러스터에 있는 모든 노드에 대한 신뢰 인증서에 추가된 SSL 인증서를 볼 수 있습니다. 더 이상 필요하지 않은 인증서를 제거할 수도 있습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘  을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **인증서**를 선택합니다.
- 3 다음 중 하나를 수행합니다.
 - 인증서에 대한 정보를 보려면 인증서의 지문 오른쪽에 있는 정보 아이콘을 클릭합니다.
 - 인증서를 제거하려면 인증서를 선택하고 **삭제**를 클릭합니다. 필요한 경우 각 인증서의 지문 오른쪽에 있는 삭제 아이콘을 클릭할 수 있습니다.

팁 제공된 옵션을 사용하여 인증서를 정렬하고 필터링할 수 있습니다.

vRealize Log Insight 웹 세션에 대한 기본 시간 초과 기간 변경


기본적으로 환경을 안전하게 유지하기 위해 vRealize Log Insight 웹 세션이 30분 후에 만료됩니다. 시간 초과 기간을 늘리거나 줄일 수 있습니다.

참고 시간 초과 기간의 변경 사항은 새로 생성된 세션에만 적용됩니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘  을 클릭하고 **관리**를 선택합니다.
- 2 구성 아래에서 **일반**을 클릭합니다.
- 3 브라우저 세션 창에서 시간 제한 값을 분 단위로 지정합니다.
 - 1 값은 세션 시간 초과를 비활성화합니다.
- 4 **저장**을 클릭합니다.

아카이브

장시간 동안 로그를 유지하려는 경우 로그 데이터를 보관하도록 vRealize Log Insight를 구성합니다.

vRealize Log Insight에서 데이터 아카이브 활성화 또는 비활성화

데이터 아카이브는 스토리지 제약으로 인해 vRealize Log Insight 가상 장치에서 제거될 수도 있는 오래된 로그를 보존합니다. vRealize Log Insight은 아카이브된 데이터를 NFS 마운트에 저장할 수 있습니다.

vRealize Log Insight는 로그를 수집하여 일련의 0.5GB 버킷 단위로 디스크에 저장합니다. 버킷은 압축된 로그 파일 및 인덱스로 구성됩니다. 버킷에는 특정 시간 범위의 쿼리를 수행하는 데 필요한 모든 정보가 포함되어 있습니다. 버킷 크기가 0.5GB를 초과하면 vRealize Log Insight는 쓰기를 중지하고 버킷의 모든 파일을 닫은 후 버킷을 봉인합니다.

데이터를 아카이브할 경우 vRealize Log Insight가 버킷이 봉인될 때 버킷에서 압축된 원시 로그 파일을 NFS 마운트에 복사합니다. 데이터 아카이브를 사용하지 않도록 설정한 경우 봉인된 버킷은 소급적으로 아카이브되지 않습니다.

아카이브 내보내기 내에 생성된 경로는 `year/month/day/hour/bucketuuid/data.blob`와 같은 형식이며 버킷이 원래 생성된(UTC) 타임 스탬프를 사용합니다.


참고 vRealize Log Insight는 아카이브 목적으로 사용되는 NFS 마운트를 관리하지 않습니다. 시스템 알림이 활성화되어 있는 경우 vRealize Log Insight는 NFS 마운트의 공간이 곧 부족해지거나 NFS 마운트를 사용할 수 없을 때 이메일을 전송합니다. NFS 마운트에 충분한 사용 가능한 공간이 없거나 NFS 마운트를 가상 장치의 보존기간보다 오랜 시간 동안 사용할 수 없는 경우 vRealize Log Insight에서 새 데이터 수집을 중지합니다. NFS 마운트에 충분한 사용 가능한 공간이 있거나 NFS 마운트를 사용할 수 있거나 아카이브가 사용되지 않도록 설정된 경우 데이터 수집을 다시 시작합니다.

NFS를 영구적으로 마운트하거나 `/etc/fstab` 파일을 변경하지 마십시오. vRealize Log Insight에서 자체적으로 NFS 마운트를 수행합니다.

사전 요구 사항

- 다음과 같은 요구 사항을 충족하는 NFS 파티션에 대한 액세스 권한을 가지고 있는지 확인합니다.
 - NFS 파티션은 게스트 계정에 대해 읽기 및 쓰기 작업을 허용해야 합니다.
 - 마운트는 인증을 요구하면 안 됩니다.
 - NFS 서버는 NFS v3 또는 v4를 지원해야 합니다.
 - Windows NFS 서버를 사용하는 경우 매핑되지 않은 사용자 UNIX 액세스(UID/GID 사용)를 허용합니다.
- 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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 구성 아래에서 **아카이브**를 클릭합니다.
- 3 **데이터 아카이브 사용**을 선택하고 `nfs://servername<:port-number>/exportname` 형식으로 로그가 아카이브되는 NFS 파티션에 대한 경로를 입력합니다.
포트 번호 기본값은 2049입니다.
- 4 **테스트**를 클릭하여 연결을 확인합니다.

5 저장을 클릭합니다.

결과

참고 데이터 아카이브는 스토리지 제약으로 인해 vRealize Log Insight 가상 장치에서 제거된 이후의 로그 이벤트를 보존합니다. vRealize Log Insight 가상 장치에서 제거되었지만 아카이브된 로그 이벤트는 더 이상 검색할 수 없습니다. 아카이브된 로그를 검색하려면 vRealize Log Insight 인스턴스로 가져와야 합니다. 아카이브된 로그 파일 가져오기에 대한 자세한 내용은 [vRealize Log Insight로 vRealize Log Insight 아카이브 가져오기](#)를 참조하십시오.

다음에 수행할 작업

vRealize Log Insight를 다시 시작한 후 ESXi의 syslog 피드가 vRealize Log Insight에 계속 도착하는지 확인합니다.

vRealize Log Insight 아카이브 파일 형식

vRealize Log Insight는 데이터를 특정 형식으로 아카이브합니다.

vRealize Log Insight는 아카이브 파일을 NFS 서버에 저장하고 아카이브 시간에 기반하여 계층형 디렉토리로 구성합니다. 예를 들면 다음과 같습니다.

```
/backup/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49/data.blob
```

여기서 /backup은 NFS 위치이고, 2014/08/07/16은 아카이브 시간이며, bd234b2d-df98-44ae-991a-e0562f10a49는 버킷 ID이고, data.blob은 아카이브된 버킷 데이터입니다.

아카이브 데이터 data.blob은 vRealize Log Insight 내부 인코딩을 사용하는 압축 파일입니다. 여기에는 버킷에 저장된 모든 메시지의 원래 콘텐츠가 포함되며 timestamp, hostname, source, appname 등의 정적 필드도 함께 포함됩니다.

아카이브된 데이터를 vRealize Log Insight에 가져오고, 아카이브 데이터를 원시 텍스트 파일에 내보내며, 아카이브 데이터에서 메시지 콘텐츠를 추출할 수 있습니다. [Log Insight 아카이브를 원시 텍스트 파일 또는 JSON으로 내보내기](#) 및 [vRealize Log Insight로 vRealize Log Insight 아카이브 가져오기](#)를 참조하십시오.

vRealize Log Insight로 vRealize Log Insight 아카이브 가져오기

데이터 아카이브는 스토리지 제약으로 인해 vRealize Log Insight 가상 장치에서 제거될 수도 있는 오래된 로그를 보존합니다. [vRealize Log Insight에서 데이터 아카이브 활성화 또는 비활성화](#)를 참조하십시오. 명령줄을 사용하여 vRealize Log Insight에 아카이브된 로그를 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.

사전 요구 사항

- vRealize Log Insight 가상 장치에 로그인하기 위한 루트 사용자 자격 증명을 가지고 있는지 확인합니다.

- vRealize Log Insight 로그가 아카이브된 NFS 서버에 대한 액세스 권한이 있는지 확인합니다.
- vRealize Log Insight 가상 장치에 가져온 로그 파일을 수용할 수 있는 디스크 공간이 충분히 있는지 확인합니다.

가상 장치의 /storage/core 파티션에서 사용 가능한 최소 공간은 가져올 아카이브된 로그 크기의 약 10배여야 합니다.

절차

- 1 vRealize Log Insight vApp에 대한 SSH 연결을 설정하고 루트 사용자로 로그인합니다.
- 2 아카이브된 데이터가 상주하는 NFS 서버에 공유 폴더를 마운트합니다.
- 3 아카이브된 vRealize Log Insight 로그의 디렉토리를 가져오려면 다음 명령을 실행합니다.

```
/usr/lib/loginsight/application/bin/loginsight repository import Path-To-Archived-Log-Data-Folder.
```

참고 가져오는 폴더 크기에 따라 아카이브된 데이터를 가져오는 데 시간이 오래 걸릴 수 있습니다.

- 4 SSH 연결을 닫습니다.

다음에 수행할 작업

가져온 로그 이벤트를 검색, 필터링 및 분석할 수 있습니다.

Log Insight 아카이브를 원시 텍스트 파일 또는 JSON으로 내보내기

명령줄을 사용하여 vRealize Log Insight 아카이브를 원시 텍스트 파일 또는 JSON 형식으로 내보낼 수 있습니다.

참고 다음은 고급 절차입니다. 이전 버전과의 호환이 지원되지 않는 경우 명령 구문 및 출력 형식은 vRealize Log Insight 이후 릴리스에서 변경될 수 있습니다.

사전 요구 사항

- vRealize Log Insight 가상 장치에 로그인하기 위한 루트 사용자 자격 증명을 가지고 있는지 확인합니다.
- vRealize Log Insight 가상 장치에 내보낸 파일을 수용할 수 있는 디스크 공간이 충분히 있는지 확인합니다.

절차

- 1 vRealize Log Insight vApp에 대한 SSH 연결을 설정하고 루트 사용자로 로그인합니다.
- 2 vRealize Log Insight vApp에 아카이브 디렉토리를 생성합니다.

```
mkdir /archive
```

- 3 다음 명령을 실행하여 아카이브된 데이터가 상주하는 NFS 서버에 공유 폴더를 마운트합니다.

```
mount -t nfs
archive-fileshare:archive directory path /archive
```

- 4 vRealize Log Insight vApp에서 사용할 수 있는 스토리지 공간을 확인합니다.

```
df -h
```

- 5 vRealize Log Insight 아카이브를 원시 텍스트 파일로 내보냅니다.

```
/usr/lib/loginsight/application/sbin/repo-exporter -d archive-file-directory
output-file
```

예를 들면 다음과 같습니다.

```
/usr/lib/loginsight/application/sbin/repo-exporter -d /archive/2014/08/07/16/bd234b2d-
df98-44ae-991a-e0562f10a49 /tmp/output.txt
```

- 6 vRealize Log Insight 아카이브 메시지 콘텐츠를 JSON 형식으로 내보냅니다.

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d archive-file-directory output-
file.
```

예를 들면 다음과 같습니다.

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d /archive/2014/08/07/16/bd234b2d-
df98-44ae-991a-e0562f10a49 /tmp/output.json
```

- 7 SSH 연결을 닫습니다.

vRealize Log Insight 서비스 다시 시작


웹 사용자 인터페이스의 관리 페이지를 사용하여 vRealize Log Insight을 다시 시작할 수 있습니다.

경고 vRealize Log Insight을 다시 시작하면 모든 활성 사용자 세션이 종료됩니다. vRealize Log Insight 인스턴스의 사용자는 다시 로그인해야 합니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘  을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **클러스터**를 클릭합니다.
- 3 클러스터 노드를 선택합니다.
- 4 **마스터 다시 시작**을 클릭하고 **다시 시작**을 클릭합니다.

다음에 수행할 작업

vRealize Log Insight를 다시 시작한 후 ESXi의 syslog 피드가 vRealize Log Insight에 계속 도착하는지 확인합니다.

vRealize Log Insight 가상 장치의 전원 끄기

vRealize Log Insight 기본 또는 작업자 노드의 전원을 끌 때 데이터 손실을 방지하려면 엄격한 단계 순서에 따라 노드의 전원을 꺼야 합니다.

vRealize Log Insight 가상 장치의 전원을 끈 후 장치의 가상 하드웨어를 수정해야 합니다.

vSphere Client에서 **전원 > 게스트 종료** 메뉴 옵션을 사용하여 vRealize Log Insight 가상 장치의 전원을 끌 수 있습니다. 가상 장치 콘솔을 사용하거나 vRealize Log Insight 가상 장치에 대한 SSH 연결을 설정하고 명령을 실행할 수도 있습니다.

사전 요구 사항

- SSH를 사용하여 vRealize Log Insight 가상 장치에 연결할 계획인 경우 TCP 포트 22가 열렸는지 확인합니다.
- vRealize Log Insight 가상 장치에 로그인하기 위한 루트 사용자 자격 증명을 가지고 있는지 확인합니다.

절차

- 1 vRealize Log Insight vApp에 대한 SSH 연결을 설정하고 루트 사용자로 로그인합니다.
- 2 vRealize Log Insight 가상 장치의 전원을 끄려면 `shutdown -h now`를 실행합니다.

다음에 수행할 작업

vRealize Log Insight 가상 장치의 가상 하드웨어를 안전하게 수정할 수 있습니다.

vRealize Log Insight 지원 번들 다운로드

문제가 발생하여 vRealize Log Insight가 예상대로 작동하지 않으면 로그 및 구성 파일의 복사본을 지원 번들 형식으로 VMware 지원 서비스로 전송할 수 있습니다.

클러스터 전체 지원 번들은 VMware 지원 서비스에서 요구하는 경우에만 필요합니다. 번들을 정적으로 생성하여 노드의 디스크 공간을 사용하거나, 스트리밍하여 노드의 디스크 공간을 사용하지 않고 기본적으로 번들을 초기 시스템에 저장할 수 있습니다.


지원 번들의 스토리지 위치는 지원 번들을 가져오는 데 사용하는 옵션에 따라 다릅니다.

옵션	지원 번들 위치
API - POST appliance/vm-support-bundle	로컬 파일이 없는 스트리밍 버전입니다.
API - POST appliance/support-bundle	/tmp/ui-support/
웹 사용자 인터페이스 - 정적 지원 번들	/tmp/ui-support/
웹 사용자 인터페이스 - 스트리밍 지원 번들	로컬 파일이 없는 스트리밍 버전입니다.
명령줄 - scripts/loginsight-support	번들이 현재 디렉토리에 생성됩니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **클러스터**를 클릭합니다.
- 3 지원 머릿글 아래에서 **지원 번들 다운로드**를 클릭합니다.

vRealize Log Insight 시스템은 진단 정보를 수집하고 데이터를 압축된 tarball로 브라우저에 전송합니다.

- 4 번들을 생성하는 방법을 선택합니다.
 - 번들을 로컬로 생성하려면 **정적 지원 번들**을 선택합니다. 번들을 생성하면 노드의 디스크 공간이 사용됩니다.
 - 지원 번들 스트리밍을 즉시 시작하려면 **스트리밍 지원 번들**을 선택합니다. 이 방법은 노드의 디스크 공간을 사용하지 않습니다.
- 5 **계속**을 클릭합니다.
- 6 파일 다운로드 대화상자에서 **저장**을 클릭합니다.
- 7 타르볼 아카이브를 저장할 위치를 선택하고 **저장**을 클릭합니다.

다음에 수행할 작업

로그 파일의 콘텐츠에서 오류 메시지를 검토할 수 있습니다. 문제를 해결하거나 완료한 경우에는 디스크 공간 절약을 위해 오래된 지원 번들을 삭제합니다.

VMware 고객 환경 개선 프로그램 가입 또는 탈퇴


vRealize Log Insight를 배포한 후에 VMware 고객 환경 개선 프로그램에 가입 또는 탈퇴할 수 있습니다.

vRealize Log Insight를 설치할 때 고객 환경 개선 프로그램에 참여할지 여부를 선택합니다. 설치 후에는 다음 단계에 따라 이 프로그램에 가입하거나 탈퇴할 수 있습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 구성 아래에서 **일반**을 클릭합니다.
- 3 [고객 환경 개선 프로그램] 창에서 **VMware 고객 환경 개선 프로그램 참여** 확인란을 선택하거나 선택 취소합니다.

선택한 경우 프로그램이 활성화되고 데이터가 <https://vmware.com>으로 전송됩니다.

- 4 **저장**을 클릭합니다.

vRealize Log Insight 클러스터 관리

5

vRealize Log Insight 클러스터의 노드를 추가, 제거 및 업그레이드할 수 있습니다.

참고 vRealize Log Insight는 WAN 클러스터링을 지원하지 않습니다. 현재 버전의 vRealize Log Insight는 WAN 클러스터(지역 클러스터, 고가용성 클러스터 또는 원격 클러스터라고도 함)를 지원하지 않습니다. 클러스터의 모든 노드가 동일한 계층 2 LAN에 배포되어야 합니다. 또한 노드 간 통신이 원활하려면 [장 6 포트 및 외부 인터페이스](#)에 설명된 포트가 열려 있어야 합니다.

본 장은 다음 항목을 포함합니다.

- vRealize Log Insight 클러스터에 작업자 노드 추가
- vRealize Log Insight 클러스터에서 작업자 노드 제거
- 통합된 로드 밸런서 사용
- 운영 환경 내 클러스터 검사의 결과 쿼리

vRealize Log Insight 클러스터에 작업자 노드 추가

Log Insight 가상 장치의 새 인스턴스를 배포한 후 기존 Log Insight 기본 노드에 추가합니다.

절차

1 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.

2 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 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 집계자를 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 형식의 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 썸 프로비저닝:** Fault Tolerance와 같은 클러스터 기능을 지원하는 썸 가상 디스크 유형을 만듭니다. 가상 디스크에 필요한 공간은 디스크 생성 시에 할당됩니다. 플랫 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 썸 프로비저닝된 디스크가 포함된 vRealize Log Insight 가상 장치를 배포합니다.

- **썸 프로비저닝:** 썸 형식의 디스크를 만듭니다. 디스크는 저장되는 데이터가 늘어남에 따라 확장됩니다. 스토리지 디바이스가 썸 프로비저닝 디스크를 지원하지 않거나 vRealize Log Insight 가상 장치의 사용되지 않은 디스크 공간을 보존하려는 경우 썸 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 설정] 페이지에서 vRealize Log Insight 가상 장치에 대한 네트워킹 매개 변수를 설정합니다.

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.

쉽프로 구분된 목록을 사용하여 도메인 이름 서버를 지정합니다.

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

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.

vRealize Log Insight 클러스터에서 작업자 노드 제거



vRealize Log Insight 클러스터에서 더 이상 올바르게 작동하지 않는 작업자 노드는 제거할 수 있습니다. 클러스터에서 제대로 작동 중인 작업자 노드는 제거하지 마십시오.

경고 노드를 제거하면 데이터가 손실됩니다. 노드를 반드시 제거해야 하는 경우 그 전에 노드를 백업해야 합니다. 새 노드를 추가하고 30분 안에 노드를 제거하지 마십시오.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **클러스터**를 클릭합니다.
- 3 작업자 표에서 원하는 노드를 찾고 일시 중지 아이콘 을 클릭한 후 **계속**을 클릭합니다.
노드가 이제 유지 보수 모드에 있습니다.

참고 유지 보수 모드의 노드는 로그를 계속 수신합니다.

4 을 클릭하여 노드를 제거합니다.

vRealize Log Insight은 클러스터에서 노드를 제거하고 이메일 알림을 전송합니다.

5 제거되면 노드는 독립형 노드로 부트스트랩되거나 부트스트랩된 후 클러스터에 결합됩니다.

통합된 로드 밸런서 사용

vRealize Log Insight ILB(통합 로드 밸런서)는 vRealize Log Insight 클러스터를 지원하고, 일부 vRealize Log Insight 노드가 사용할 수 없는 상태가 된 경우에도 수신 수집 트래픽이 vRealize Log Insight에서 수락되도록 합니다. 가상 IP 주소를 여러 개 구성할 수도 있습니다.

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

단일 노드 인스턴스를 비롯한 모든 배포에 ILB를 포함하는 것이 가장 좋습니다. 향후 필요할 때 클러스터가 쉽게 지원될 수 있도록 쿼리 및 수집 트래픽을 ILB로 전송합니다. ILB는 클러스터의 노드 간에 트래픽을 분산하고 관리 오버헤드를 최소화합니다.

ILB를 사용하면 일부 vRealize Log Insight 노드가 사용할 수 없는 상태가 된 경우라도 수신 수집 트래픽이 vRealize Log Insight에서 수락됩니다. 또한 ILB를 통해 사용할 수 있는 vRealize Log Insight 노드 간에 수신 트래픽이 균등하게 분산됩니다. Syslog 또는 Ingestion API를 통해 웹 사용자 인터페이스 및 수집을 모두 사용하는 vRealize Log Insight 클라이언트는 ILB 주소를 통해 vRealize Log Insight에 연결됩니다.

ILB를 사용하려면 모든 vRealize Log Insight 노드가 동일한 계층 2 네트워크에 위치해야 합니다. 예를 들어, 동일한 스위치 뒤에 위치하거나 ARP 요청을 서로 주고 받을 수 있는 위치에 있어야 합니다. vRealize Log Insight 노드가 자체 IP 주소를 소유하고 해당 트래픽을 수신할 수 있도록 ILB IP 주소를 설정해야 합니다. 일반적으로 이는 ILB IP 주소가 vRealize Log Insight 노드의 물리적 주소로 동일한 서브넷에 위치하는 것을 의미합니다. ILB IP 주소를 구성한 후 다른 네트워크에서 ping하여 해당 주소에 연결할 수 있는지 확인합니다.

향후 변경 및 업그레이드를 간소화하기 위해 클라이언트가 ILB IP 주소를 직접 가리키지 않고 ILB IP 주소로 확인되는 FQDN을 가리키도록 할 수 있습니다.

Direct Server Return 구성 정보

vRealize Log Insight 로드 밸런서는 DSR(Direct Server Return) 구성을 사용합니다. DSR의 경우 모든 수신 트래픽은 현재 밸런서 노드인 vRealize Log Insight 노드를 통과합니다. 반환 트래픽은 로드 밸런서 노드를 거치지 않고 vRealize Log Insight 서버에서 클라이언트로 직접 전송됩니다.

여러 가상 IP 주소

통합된 로드 밸런서에서 사용할 vIP(가상 IP 주소)를 여러 개 구성할 수 있습니다. 또한 각 vIP에 대해 일련의 정적 태그를 구성하여 해당 vIP로부터 수신된 모든 로그 메시지에 구성된 태그가 달리도록 할 수 있습니다.

통합된 로드 밸런서 사용

vRealize Log Insight ILB(통합된 로드 밸런서)를 vRealize Log Insight 클러스터에서 사용하도록 설정하면 가상 IP 주소를 하나 이상 구성해야 합니다.


통합된 로드 밸런서는 하나 이상의 vIP(가상 IP 주소)를 지원합니다. 각 vIP는 들어오는 수집 및 쿼리 트래픽을 사용 가능한 vRealize Log Insight 노드 간에 분산합니다. 노드로 직접 연결되지 않고 vIP를 통해 모든 vRealize Log Insight 클라이언트에 연결하는 것이 가장 좋습니다.

향후 변경 및 업그레이드를 간소화하기 위해 클라이언트가 ILB IP 주소를 직접 가리키지 않고 ILB IP 주소로 확인되는 FQDN을 가리키도록 할 수 있습니다. 경고 메시지만 아니라 vSphere 및 vRealize Operations 통합에서도 FQDN을 사용합니다(제공되는 경우). 그렇지 않은 경우 ILB IP 주소를 사용합니다. vRealize Log Insight는 FQDN을 지정된 IP 주소로 확인할 수 있어야 합니다. 즉, 지정한 FQDN 값이 DNS에 정의된 값과 일치해야 합니다.

사전 요구 사항

- 모든 vRealize Log Insight 노드 및 지정된 통합 로드 밸런서 IP 주소가 동일한 네트워크에 있는지 확인합니다.
- NSX에서 vRealize Log Insight를 사용하는 경우 NSX 논리적 스위치에 대해 **IP 검색 사용** 옵션이 사용되지 않도록 설정되어 있는지 확인합니다.
- vRealize Log Insight 기본 및 작업자 노드에는 동일한 인증서가 있어야 합니다. 그렇지 않으면 SSL을 통해 연결하도록 구성된 vRealize Log Insight Agent가 연결을 거부합니다. CA 서명된 인증서를 vRealize Log Insight 기본 및 작업자 노드에 업로드할 때 인증서 생성 요청 도중 일반 이름을 ILB FQDN(또는 IP 주소)으로 설정하십시오. **인증서 서명 요청 생성** 항목을 참조하십시오.
- vRealize Log Insight 가상 장치의 시간을 NTP 서버의 시간과 동기화해야 합니다. **Log Insight 가상 장치의 시간 동기화**를 참조하십시오.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **클러스터**를 클릭합니다.
- 3 통합 로드 밸런서 섹션에서 **새 가상 IP 주소**를 선택하고 통합된 로드 밸런싱에 사용할 vIP(가상 IP) 주소를 입력합니다.
- 4 (선택 사항) 여러 가상 IP 주소를 구성하려면 **새 가상 IP 주소**를 클릭하고 IP 주소를 입력합니다. FQDN과 태그를 입력할 수도 있습니다.
 - 각 vIP는 각 노드에 있는 하나 이상의 네트워크 인터페이스와 동일한 서브넷에 속해 있어야 하며, 사용 가능한 상태(다른 시스템에서 사용 중이 아님)여야 합니다.
 - 태그를 사용하면 미리 정의된 값을 가진 필드를 이벤트에 추가할 수 있어 쿼리 작업이 더 쉬워집니다. 섹프로 구분된 태그는 여러 개 추가할 수 있습니다. vIP를 통해 시스템에 들어오는 모든 이벤트에는 vIP의 태그가 표시됩니다.

- ILB VIP에 대해 정적 태그(키=값) 목록을 구성하여, 구성된 태그가 VIP에서 수신되는 각 로그 메시지에 주석으로 사용되도록 할 수 있습니다.

5 (선택 사항) vRealize Log Insight 사용자가 FQDN을 통해 클러스터에 액세스할 수 있게 하려면 클라이언트가 구성된 ILB IP 주소를 직접 가리키지 않고 FQDN을 가리키도록 설정합니다.

클라이언트가 IBM IP 주소로 확인되는 FQDN을 가리키도록 하여 향후 변경 및 업그레이드를 간소화할 수 있고, 클라이언트가 ILB IP 주소를 직접 가리키지 않고 FQDN을 가리키도록 할 수 있습니다.

6 저장을 클릭합니다.

통합된 로드 밸런서는 vRealize Log Insight 클러스터의 한 노드에 의해 관리되고 해당 서비스에 대해 리더로 선언됩니다. 현재의 리더는 노드 옆의 텍스트(ILB)로 표시됩니다.

운영 환경 내 클러스터 검사의 결과 쿼리

운영 환경 내 클러스터 검사 서비스는 각 노드에 대해 여러 가지 검사를 정기적으로 실행합니다. CLI를 통해 운영 환경 내 클러스터 검사의 최신 결과를 쿼리할 수 있습니다.

예를 들어 이 서비스는 클러스터가 예상한 대로 실행되고 구성되었는지 또는 다른 시스템과의 통합에 문제가 있는지 여부를 확인합니다. 그 외에 아래에 나열된 추가적인 검사도 실행합니다.

- NTP가 다중 호스트 배포 환경에 구성되었는지 여부
- Active Directory에 연결할 수 있는지 여부(현재 Active Directory가 구성되어 있는 경우)
- Active Directory 인증을 사용할 수 있는지 여부(현재 Active Directory가 구성되어 있는 경우)
- Active Directory 호스트 및 Kerberos 호스트에 연결할 수 있는지 여부(현재 Active Directory가 구성되어 있는 경우)
- 지원되지 않는 이중 호스트 배포 환경에서 시스템이 실행 중인지 여부
- 업그레이드를 수행하는 데 필요한 공간이 /tmp에 충분한지 여부
- 업그레이드를 수행하는 데 필요한 공간이 /storage/core에 충분한지 여부
- localhost가 /etc/hosts에 올바르게 배치되었는지 여부

절차

- 1 명령줄에서 vRealize Log Insight 가상 장치에 대한 SSH 연결을 설정하고 루트 사용자로 로그인합니다.
- 2 명령줄에 /usr/lib/loginsight/application/sbin/query-check-results.sh를 입력하고 **Enter** 키를 누릅니다.

포트 및 외부 인터페이스

6

vRealize Log Insight는 특정 필수 서비스, 포트 및 외부 인터페이스를 사용합니다.

vRealize Log Insight의 포트 및 프로토콜에 대한 자세한 내용은 [VMware Ports and Protocols](#)을 참조하십시오.

통신 포트

vRealize Log Insight는 이 항목에 나열된 통신 포트와 프로토콜을 사용합니다. 필수 포트는 소스, 사용자 인터페이스, 클러스터 간 또는 외부 서비스에 필요한지 여부 또는 방화벽으로 안전하게 차단될 수 있는지 여부에 따라 구성됩니다. 일부 포트는 해당하는 통합을 사용하도록 설정하는 경우에만 사용됩니다.

참고 vRealize Log Insight에서는 WAN 클러스터링(지역적 클러스터링, 고가용성 클러스터링 또는 원격 클러스터링이라고도 함)을 지원하지 않습니다. 클러스터의 모든 노드가 동일한 계층 2 LAN에 배포되어야 합니다. 또한 노드 간 통신이 원활하려면 이 섹션에 설명된 포트가 열려 있어야 합니다.

vRealize Log Insight 네트워크 트래픽에는 몇 개의 소스가 있습니다.

관리 워크스테이션

시스템 관리자가 원격으로 vRealize Log Insight 가상 장치를 관리하기 위해 사용하는 시스템입니다.

사용자 워크스테이션

vRealize Log Insight 사용자가 브라우저를 사용하여 vRealize Log Insight의 웹 인터페이스에 액세스하는 시스템입니다.

로그를 보내는 시스템

분석 및 검색을 위해 vRealize Log Insight에 로그를 보내는 끝점입니다. 예를 들어 끝점에는 ESXi 호스트, 가상 시스템 또는 IP 주소가 할당된 모든 시스템이 포함됩니다.

Log Insight Agents

Windows 또는 Linux 시스템에 있으며 API를 통해 vRealize Log Insight로 운영 체제 이벤트 및 로그를 보내는 에이전트입니다.

vRealize Log Insight 장치

vRealize Log Insight 서비스가 있는 모든 vRealize Log Insight 가상 장치, 기본 또는 작업자입니다. 장치의 기본 운영 체제는 SUSE 11 SP3입니다.

데이터를 보내는 소스에 필요한 포트

클러스터 외부에서의 연결 및 클러스터 노드 간 로드 밸런싱된 연결 둘 다에 대해 vRealize Log Insight로 데이터를 전송하는 소스의 네트워크 트래픽에 대해 다음 포트를 열어야 합니다.

소스	대상	포트	프로토콜	서비스 설명
로그를 보내는 시스템	vRealize Log Insight 장치	514	TCP, UDP	전달자 대상으로 구성되는 아웃바운드 syslog 트래픽
로그를 보내는 시스템	vRealize Log Insight 장치	1514, 6514	TCP	SSL을 통한 Syslog 데이터
vRealize Log Insight 에이전트	vRealize Log Insight 장치	9000	TCP	Log Insight 수집 API
vRealize Log Insight 에이전트	vRealize Log Insight 장치	9543	TCP	SSL을 통한 Log Insight 수집 API

사용자 인터페이스에 필요한 포트

클러스터 외부에서의 연결 및 클러스터 노드 간 로드 밸런싱된 연결 둘 다에 대해 vRealize Log Insight 사용자 인터페이스를 사용해야 하는 네트워크 트래픽에 대해 다음 포트를 열어야 합니다.

소스	대상	포트	프로토콜	서비스 설명
관리 워크스테이션	vRealize Log Insight 장치	22	TCP	SSH: 보안 셸(Secure Shell) 연결
사용자 워크스테이션	vRealize Log Insight 장치	80	TCP	HTTP: 웹 인터페이스
사용자 워크스테이션	vRealize Log Insight 장치	443	TCP	HTTPS: 웹 인터페이스

클러스터 노드 간에 필요한 포트

작업자 노드에서 네트워크에 액세스하는 경우 보안을 극대화하기 위해 다음 포트를 vRealize Log Insight 기본 노드에서만 열어야 합니다. 이러한 포트는 클러스터 노드 간에 로드 밸런싱된 소스 및 UI 트래픽에 사용되는 포트 외에 사용됩니다.

소스	대상	포트	프로토콜	서비스 설명
vRealize Log Insight 장치	vRealize Log Insight 장치	7000	TCP	Cassandra 복제 및 쿼리
vRealize Log Insight 장치	vRealize Log Insight 장치	9042	TCP	네이티브 프로토콜 클라이언트용 Cassandra 서비스
vRealize Log Insight 장치	vRealize Log Insight 장치	59778, 16520-16580	TCP	vRealize Log Insight Thrift 서비스

외부 서비스에 필요한 포트

vRealize Log Insight 클러스터 노드에서 원격 서비스로의 아웃바운드 네트워크 트래픽에 대해 다음 포트를 열어야 합니다.

소스	대상	포트	프로토콜	서비스 설명
vRealize Log Insight 장치	NTP 서버	123	UDP	NTPD: NTP 시간 동기화 제공 참고 포트는 NTP 시간 동기화를 사용하기로 선택한 경우에만 열립니다.
vRealize Log Insight 장치	메일 서버	25	TCP	SMTP: 아웃바운드 경고를 위한 메일 서비스
vRealize Log Insight 장치	메일 서버	465	TCP	SMTPS: 아웃바운드 경고를 위한 SSL을 통한 메일 서비스
vRealize Log Insight 장치	DNS 서버	53	TCP, UDP	DNS: 이름 확인 서비스
vRealize Log Insight 장치	AD 서버	389	TCP, UDP	Active Directory
vRealize Log Insight 장치	AD 서버	636	TCP	SSL을 통한 Active Directory
vRealize Log Insight 장치	AD 서버	3268	TCP	Active Directory 글로벌 카탈로그
vRealize Log Insight 장치	AD 서버	3269	TCP	Active Directory 글로벌 카탈로그 SSL
vRealize Log Insight 장치	AD 서버	88	TCP, UDP	Kerberos
vRealize Log Insight 장치	vCenter Server	443	TCP	vCenter Server 웹 서비스
vRealize Log Insight 장치	vRealize Operations Manager 장치	443	TCP	vRealize Operations 웹 서비스

소스	대상	포트	프로토콜	서비스 설명
vRealize Log Insight 장치	타사 로그 관리자	514	TCP, UDP	Syslog 데이터
vRealize Log Insight 장치	타사 로그 관리자	9000	CFAPI	전달자 대상으로 구성되는 아웃바운드 Log Insight 수집 API(CFAPI) 트래픽
vRealize Log Insight 장치	타사 로그 관리자	9543	CFAPI	암호화(SSL/TLS)를 통해 전달자 대상으로 구성되는 아웃바운드 Log Insight 수집 API(CFAPI) 트래픽

vRealize Log Insight 에이전트의 상태 모니터링

7

vRealize Log Insight Windows 및 Linux 에이전트의 상태를 모니터링하고 해당 작업의 현재 통계를 볼 수 있습니다.

CFAPI를 통해 데이터를 보내도록 구성된 에이전트만 에이전트 페이지에 나타납니다. 다른 Syslog 소스와 마찬가지로, Syslog를 통해 데이터를 보내도록 구성된 에이전트가 호스트 페이지에 나타납니다. 프로토콜을 CFAPI에서 Syslog로 변경하면 통계가 업데이트되지 않고 [통계] 페이지에 표시되지 않으며, 에이전트 상태는 “연결 끊김”으로 표시됩니다. 여기에 표시된 데이터는 30초마다 LI 에이전트에서 전송됩니다. vRealize Log Insight는 최대 15,000개 에이전트에 대한 정보를 표시할 수 있습니다.

프로토콜을 CFAPI에서 Syslog로 변경하면 통계 업데이트가 중단되고 [에이전트] 페이지에 더 이상 표시되지 않으며, 에이전트 상태는 중단됨으로 표시됩니다. 여기에 표시된 데이터는 30초마다 vRealize Log Insight 에이전트에서 전송됩니다.

참고 에이전트 구성에서 vRealize Log Insight 서버에 대한 호스트 IP를 변경하는 경우 에이전트는 페이지 통계를 0으로 재설정합니다.

사전 요구 사항

vRealize Log Insight 웹 사용자 인터페이스에 **관리 보기** 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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.

2 관리 아래에서 에이전트를 클릭합니다.

CFAPI 통해 데이터를 전송하는 각 에이전트에 대한 상태 정보가 표시됩니다.

The screenshot shows the 'Agents' page in vRealize Log Insight. The left sidebar has a 'Management' section with options: System Monitor, Cluster, Access Control, User Alerts, Hosts, **Agents**, Event Forwarding, and License. The main content area is titled 'Agents' and shows a dropdown for 'All Agents' and a toggle for 'Enable auto-updates'. Below this is an 'EXPORT' button and a checkbox for 'Configurable only'. A table lists agents with columns: IP Addr..., Hostna..., Version, OS, Last Act..., Events ..., Events ..., Events ..., Uptime, and Status. The first agent is highlighted with a blue row.

IP Addr...	Hostna...	Version	OS	Last Act...	Events ...	Events ...	Events ...	Uptime	Status
1...	...	4.3.0.5052904	SUSE Linux Enterprise Server 11	Less than 1 minute ago	117,012	10	0	2 hours	Active

다음에 수행할 작업

에이전트 페이지의 정보를 사용하여 설치된 vRealize Log Insight Windows 및 Linux 에이전트의 작업을 모니터링할 수 있습니다. 에이전트 호스트 이름을 클릭하여 해당 호스트에 대한 [대화형 분석] 페이지로 이동합니다. LI 에이전트에서 호스트 이름 매개 변수를 설정하고, 기본 CFAPI 프로토콜을 사용하여 Log Insight 인스턴스를 가리키는 경우 [에이전트 통계] 페이지를 열고 에이전트가 에이전트 목록에 나타나는지 확인하여 연결을 모니터링할 수 있습니다. 호스트 이름 열 아래에 있는 링크를 사용하여 [Insight Agent] 페이지로 이동하면 언급된 에이전트에서 가져온 로그를 확인할 수 있습니다.

서버에서 에이전트 자동 업데이트 사용

8

vRealize Log Insight 서버에서 모든 에이전트에 대해 자동 업데이트를 사용하도록 설정할 수 있습니다.


자동 업데이트는 서버에 연결된 모든 에이전트에 사용 가능한 최신 업데이트를 적용합니다. 에이전트의 `liagent.ini` 파일을 편집하여 개별 서버에 대한 자동 업데이트 기능을 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 "vRealize Log Insight Agent 작업" 항목을 참조하십시오.

자동 업데이트는 기본적으로 서버에 대해 사용되지 않도록 설정되어 있습니다.

사전 요구 사항

에이전트는 활성 상태여야 하며 버전 4.3 이상이어야 합니다.

절차

- 1 구성 드롭다운 메뉴 아이콘  을 클릭하고 **관리**를 선택합니다.
- 2 왼쪽의 메뉴에서 **에이전트**를 클릭합니다.
- 3 [에이전트] 페이지에서 **모든 에이전트에 대해 자동 업데이트가 사용되도록 설정** 토글 컨트롤을 클릭합니다.

결과

업데이트가 있는 경우 이 서버에 연결된 에이전트가 업데이트됩니다.

중앙 집중식 에이전트 구성 및 에이전트 그룹

9

vRealize Log Insight 서버를 사용하여 애플리케이션의 사용자 인터페이스 내에서 에이전트를 구성할 수 있습니다. 에이전트는 정기적으로 vRealize Log Insight 서버를 폴링하여 새 구성이 사용 가능한지 확인합니다.

동일한 구성이 필요한 에이전트를 그룹화할 수 있습니다. 예를 들어 vRealize Log Insight Linux 에이전트와 별도로 모든 vRealize Log Insight Windows 에이전트를 그룹화할 수 있습니다.

모든 에이전트 메뉴에서 콘텐츠 팩의 기존 에이전트 그룹이 자동으로 나열됩니다. 나열된 에이전트는 에이전트 그룹을 사용하는, 사용자가 이미 설치한 콘텐츠 팩(예: vSphere 콘텐츠 팩)과 관련이 있습니다. **내 콘텐츠** 또는 **공유 콘텐츠**를 클릭할 때 **콘텐츠 팩 > 사용자 지정 콘텐츠** 아래에 모든 사용자 생성 에이전트 그룹이 표시됩니다.

하나 이상의 보기 전용 관리자 역할이 있는 사용자는 에이전트 그룹 템플릿을 사용하여 콘텐츠 팩을 내보낼 수 있습니다.

참고

- 동일한 콘텐츠 팩 템플릿은 두 번 이상 사용할 수 없습니다.
- 콘텐츠 팩 그룹은 읽기 전용입니다.

[winlog], [filelog] 및 [parser]로 시작된 구성 섹션만 콘텐츠 팩에 사용됩니다. 추가 섹션을 콘텐츠 팩의 일부로 내보내지 않습니다. [winlog], [filelog] 및 [parser] 섹션 아래에서 한 줄의 주석(;로 시작된 줄)만 콘텐츠 팩에서 유지됩니다.

참고 단일 에이전트가 여러 에이전트 그룹에 속할 수 있으며 중앙 집중식 에이전트 구성의 모든 설정을 상속합니다.

에이전트 그룹 생성에 설명된 대로 "모든 에이전트" 그룹에 대한 구성을 생성할 수 있습니다. 에이전트가 중앙 집중식 에이전트 구성과 다른 구성의 조합으로 구성된 경우 에이전트 구성은 두 구성을 모두 병합한 결과입니다. 병합에 대한 자세한 내용은 [에이전트 그룹 구성 병합](#)을 참조하십시오.

참고 가능하면 항상 에이전트 그룹을 사용하고, 필요하지 않으면 "모든 에이전트" 구성을 사용하지 않도록 하십시오.

에이전트 구성과 로컬 및 서버 쪽 구성 병합에 대한 자세한 내용은 "vRealize Log Insight Agent 작업" 을 참조하십시오.

■ 에이전트 그룹 구성 병합

에이전트 그룹을 사용하면 에이전트가 여러 그룹의 일부가 되고, 기본 그룹인 "모든 에이전트"에 속할 수 있으므로 중앙 집중식 구성이 가능해집니다.

■ 에이전트 그룹 생성

동일한 매개 변수로 구성된 에이전트 그룹을 생성할 수 있습니다.

■ 에이전트 그룹 편집

에이전트 그룹의 이름과 설명을 편집하고, 필터를 변경하고, 구성을 편집할 수 있습니다.

■ 콘텐츠 팩 에이전트 그룹을 에이전트 그룹으로 추가

콘텐츠 팩의 일부로 정의된 에이전트 그룹을 활성 그룹에 추가하고 에이전트 구성을 이 그룹에 적용할 수 있습니다.

■ 에이전트 그룹 삭제

에이전트 그룹을 삭제하여 활성 그룹 목록에서 이 에이전트 그룹을 제거할 수 있습니다.

에이전트 그룹 구성 병합

에이전트 그룹을 사용하면 에이전트가 여러 그룹의 일부가 되고, 기본 그룹인 "모든 에이전트"에 속할 수 있으므로 중앙 집중식 구성이 가능해집니다.

병합은 서버 측에서 일어나며 그 결과로 인한 구성이 에이전트 측 구성과 병합됩니다. 병합된 구성은 다음 규칙의 결과입니다.

- 개별 그룹 구성은 모든 에이전트 그룹 구성보다 우선 순위가 높으며 모든 에이전트 그룹 설정을 재정의합니다.
- 모든 에이전트 그룹 구성은 로컬 구성을 재정의합니다.
- 모든 에이전트 그룹을 제외한 서로 다른 그룹에 동일한 이름의 섹션을 구성할 수 없습니다. 그러나 개별 그룹의 섹션이 더 높은 우선 순위를 가집니다.

참고 에이전트 손실을 방지하기 위해 에이전트 구성의 **호스트 이름** 및 **포트** 매개 변수를 서버에서 중앙 집중식으로 변경할 수 없습니다.

병합된 구성은 에이전트 측 liagent-effective.ini 파일에 저장됩니다. Windows 시스템의 경우 이 파일은 %ProgramData%\VMware\Log Insight Agent에 저장되고 Linux 시스템의 경우에는 /var/lib/loginsight-agent/에 저장됩니다.


에이전트 그룹 생성

동일한 매개 변수로 구성된 에이전트 그룹을 생성할 수 있습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **에이전트**를 클릭합니다.
- 3 **모든 에이전트** 메뉴에서 새로 고침 버튼 옆에 있는 에이전트 이름 필드에서 드롭다운 메뉴를 열고 **새 그룹**을 클릭합니다.
- 4 에이전트 그룹에 대한 고유한 이름과 설명을 제공하고 **새 그룹**을 클릭합니다.

에이전트 그룹이 생성되고 **모든 에이전트** 목록에 나타나지만 저장되지는 않습니다.

- 5 에이전트 그룹에 대해 하나 이상의 필터를 지정합니다. 필터를 생성하려면 필드 이름, 연산자 및 값을 지정합니다.

필터는 * 및 ?와 같은 와일드카드를 포함할 수 있습니다. 예를 들어 OS 필터 contains를 선택하고 구성에 대한 모든 Windows 에이전트를 식별하기 위한 값 windows를 지정할 수 있습니다.

- a 다음 필드 중에서 필터링 기준으로 사용할 필드를 하나 선택합니다.

- IP 주소
- 호스트 이름
- 버전
- 운영 체제

- b 드롭다운 메뉴에서 연산자를 선택하고 값을 지정합니다.

연산자	설명
일치	지정된 문자열 및 와일드카드 규격과 일치하는 문자열을 찾습니다. 여기서 *는 0개 이상의 문자를 의미하고 ?는 단일 문자를 의미합니다. 전위 및 후위 와일드카드 사용이 지원됩니다. 예를 들어, *test* 는 test123 또는 my-test-run 과 같은 문자열과 일치합니다.
일치하지 않음	지정된 문자열 및 와일드카드 규격과 일치하는 문자열을 제외합니다. 여기서 *는 0개 이상의 문자를 의미하고 ?는 단일 문자를 의미합니다. 전위 및 후위 와일드카드 사용이 지원됩니다. 예를 들어 test* 는 test123 을 필터링하여 제외하지만 mytest123 은 제외하지 않습니다. %test* 는 test123 을 필터링하여 제외하지 않지만 xtest123 은 제외합니다.
다음으로 시작	지정된 문자 또는 문자열로 시작하는 문자열을 찾습니다. 예를 들어 test 는 test123 또는 test 는 찾지만 my-test123 은 찾지 않습니다.
다음으로 시작하지 않음	지정된 문자 또는 문자열로 시작하는 문자열을 제외합니다. 예를 들어 test 는 test123 을 필터링하여 제외하지만 my-test123 은 제외하지 않습니다.

- 6 에이전트 구성 영역에서 에이전트 구성 값을 지정하고 **새 그룹 저장**을 클릭합니다.

결과

다음 폴링 간격 이후에 에이전트 구성이 적용됩니다.


에이전트 그룹 편집

에이전트 그룹의 이름과 설명을 편집하고, 필터를 변경하고, 구성을 편집할 수 있습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **에이전트**를 클릭합니다.
- 3 **모든 에이전트** 메뉴에서 적절한 에이전트 그룹의 이름을 선택하고 연필 아이콘을 클릭하여 이 그룹을 편집합니다.
- 4 원하는 내용을 변경합니다.

편집할 항목	작업
이름 또는 설명	필요한 내용을 변경하고 저장 을 클릭합니다.
필터 또는 구성	필요한 내용을 변경하고 그룹 저장 을 클릭합니다.


컨텐츠 팩 에이전트 그룹을 에이전트 그룹으로 추가

컨텐츠 팩의 일부로 정의된 에이전트 그룹을 활성 그룹에 추가하고 에이전트 구성을 이 그룹에 적용할 수 있습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **에이전트**를 클릭합니다.
- 3 **모든 에이전트** 메뉴에서, 사용할 수 있는 템플릿 목록에 대한 에이전트 템플릿을 선택합니다.
- 4 **템플릿 복사**를 클릭하여 활성 그룹에 컨텐츠 팩 에이전트 그룹을 복사합니다.
- 5 **복사**를 클릭합니다.
- 6 필수 필터를 선택하고 **새 그룹 저장**을 클릭합니다.

결과

컨텐츠 팩 에이전트 그룹이 활성 그룹에 추가되고 사용자가 지정한 필터에 따라 에이전트가 구성됩니다.


에이전트 그룹 삭제

에이전트 그룹을 삭제하여 활성 그룹 목록에서 이 에이전트 그룹을 제거할 수 있습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **에이전트**를 클릭합니다.
- 3 **모든 에이전트** 메뉴에서 에이전트 그룹 이름 옆의 X 아이콘을 클릭하여 삭제할 에이전트 그룹 이름을 선택합니다.
- 4 **삭제**를 클릭합니다.

결과

해당 에이전트 그룹이 활성 그룹에서 제거됩니다.

vRealize Log Insight 모니터링

10

vRealize Log Insight에 로그 이벤트를 보내는 호스트와 장치 및 vRealize Log Insight 가상 장치를 모니터링할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- vRealize Log Insight 가상 장치의 상태 확인
- 로그 이벤트를 전송하는 호스트 모니터링
- 비활성 호스트를 보고하도록 시스템 알림 구성


vRealize Log Insight 가상 장치의 상태 확인

vRealize Log Insight 가상 장치의 사용 가능한 리소스 및 활성 쿼리를 확인하고 vRealize Log Insight의 작업에 대한 현재 통계를 볼 수 있습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **시스템 모니터**를 클릭합니다.
- 3 vRealize Log Insight이 클러스터로 실행 중인 경우 **다음에 대한 리소스 표시**를 클릭하고 모니터링할 노드를 선택합니다.

4 시스템 모니터 페이지의 버튼을 클릭하여 필요한 정보를 봅니다.

옵션	설명
리소스	vRealize Log Insight 가상 장치의 CPU, 메모리, IOPS(읽기 및 쓰기 활동) 및 스토리지 사용량에 대한 정보를 봅니다. 오른쪽의 차트는 마지막 24시간 동안의 기존 데이터를 나타내며 5분 간격으로 새로 고침됩니다. 왼쪽의 차트는 마지막 5분 동안의 정보를 표시하며 3초마다 새로 고침됩니다.
활성 쿼리	vRealize Log Insight에서 현재 활성 상태인 쿼리에 대한 정보를 봅니다.
통계	로그 수집 작업 및 비율에 대한 통계를 봅니다. 보다 세부적인 통계를 보려면 고급 통계 표시 를 클릭합니다.

다음에 수행할 작업

시스템 모니터 페이지의 정보를 사용하여 vRealize Log Insight 가상 장치의 리소스를 관리할 수 있습니다.

로그 이벤트를 전송하는 호스트 모니터링


모니터링을 위해 로그 이벤트를 vRealize Log Insight에 전송하는 모든 호스트 및 디바이스 목록을 볼 수 있습니다.

호스트 테이블의 항목은 이벤트가 마지막으로 수집되고 3개월 후에 만료됩니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 관리 아래에서 **호스트**를 클릭합니다.

참고 이벤트 및 경보를 전송하도록 vCenter Server를 구성했지만 로그를 전송하도록 개별 ESXi 호스트를 구성하지 않은 경우, 호스트 이름 옆에 vCenter Server만 나열되는 것이 아닌 vCenter Server 및 개별 ESXi 호스트 모두가 소스로 나열됩니다.

다음에 수행할 작업

관리자 권한이 있는 사용자는 호스트가 비활성 상태일 때 전송되는 시스템 알림을 설정할 수 있습니다. 자세한 내용은 **비활성 호스트를 보고하도록 시스템 알림 구성** 항목을 참조하십시오.

비활성 호스트를 보고하도록 시스템 알림 구성

vRealize Log Insight에는 지정된 기간에 비활성 상태인 호스트를 알아보는 데 사용할 수 있는 기본 제공 알림이 포함되어 있습니다.

[호스트] 화면에서 알림을 사용하도록 설정하고 알림을 트리거하는 임계값을 지정합니다. 이 설정을 모든 호스트 또는 좀 더 작은 호스트 목록에 적용할 수 있습니다.

사전 요구 사항

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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리** 를 선택합니다.
- 2 관리 아래에서 **호스트** 를 클릭합니다.

참고 이벤트 및 경보를 전송하도록 vCenter Server를 구성했지만 로그를 전송하도록 개별 ESXi 호스트를 구성하지 않은 경우, 호스트 이름 옆에 vCenter Server만 나열되는 것이 아닌 vCenter Server 및 개별 ESXi 호스트 모두가 소스로 나열됩니다.

- 3 **호스트** 페이지에서 **비활성 호스트 알림** 을 선택하여 알림이 전송될 때와 알림이 전송되는 호스트를 구성하기 위한 양식을 표시합니다.
- 4 알림을 전송하기 전에 호스트가 비활성 상태를 유지하는 기간을 지정합니다.

값은 10분부터 최대 호스트 TTL(Time to Live) 기간까지 가능하며, 기본값은 3개월입니다. 예를 들면 다음과 같습니다.

Send alert listing hosts that are inactive for **8시간** of last received event.

- 5 **비활성 호스트 알림 화이트리스트** 설정을 사용하여 알림이 모니터링되는 호스트를 제어합니다. 이 설정을 선택하지 않으면 모든 비활성 호스트에 대해 알림이 전송됩니다.

- 모든 비활성 호스트에 대해 알림이 전송되도록 하려면 이 확인란의 선택을 취소합니다.

- 일부 비활성 호스트에 대해서만 알림이 전송되도록 하려면 **비활성 호스트 알림 화이트리스트**를 선택하고 호스트 이름을 선택으로 구분된 목록에 지정합니다.

6 저장을 클릭합니다.

결과

호스트가 지정된 제한보다 더 오래 비활성 상태가 되면 **구성>SMTP 서버** 페이지에 지정된 주소로 시스템 알림이 전송됩니다.

vRealize Log Insight와 VMware 제품 통합

11

vRealize Log Insight는 이벤트 및 로그 데이터를 사용하고 가상 환경에서 발생하는 이벤트에 대한 향상된 가시성을 제공하기 위해 다른 VMware 제품과 통합될 수 있습니다.

VMware vSphere와 통합

vRealize Log Insight 관리자는 2분 간격으로 vCenter Server 시스템에 연결하고 이러한 vCenter Server 시스템에서 이벤트, 경고 및 작업 데이터를 수집하도록 vRealize Log Insight를 설정할 수 있습니다. 또한 vRealize Log Insight는 vCenter Server를 통해 ESXi 호스트를 구성할 수 있습니다. [vSphere 환경에 vRealize Log Insight 연결](#) 항목을 참조하십시오.

VMware vRealize Operations Manager와 통합

vRealize Log Insight를 vRealize Operations Manager vApp 및 vRealize Operations Manager 설치 파일과 통합할 수 있습니다. 설치 파일 버전과 통합하려면 vRealize Operations Manager 구성에 대한 추가 변경이 필요합니다. vRealize Log Insight와 통합하도록 vRealize Operations Manager 설치 파일 구성에 대한 자세한 내용은 "Log Insight 시작 가이드"를 참조하십시오.

vRealize Log Insight 및 vRealize Operations Manager는 두 가지의 독립된 방식으로 통합될 수 있습니다.

알림 이벤트

vRealize Log Insight 관리자는 사용자가 생성하는 쿼리를 기준으로 vRealize Operations Manager에 알림 이벤트를 전송하도록 vRealize Log Insight를 설정할 수 있습니다. [vRealize Operations Manager에 알림 이벤트를 전송하도록 vRealize Log Insight 구성](#) 항목을 참조하십시오.

컨텍스트에서 실행

컨텍스트에서 실행은 특정 컨텍스트에서 URL을 통해 외부 애플리케이션을 시작할 수 있도록 해주는 vRealize Operations Manager의 기능입니다. 컨텍스트는 활성 UI 요소 및 개체 선택에 의해 정의됩니다. 컨텍스트에서 실행 기능을 통해 vRealize Log Insight 어댑터는 vRealize Operations Manager의 사용자 지정 사용자 인터페이스 및 vSphere 사용자 인터페이스 내의 여러 다른 보기에 메뉴 항목을

추가할 수 있습니다. **vRealize Operations Manager**에서 **vRealize Log Insight**에 대한 컨텍스트에서 실행 기능 활성화 항목을 참조하십시오.

참고 알람 이벤트는 컨텍스트에서 실행 구성에 따라 달라지지 않습니다. 컨텍스트에서 실행 기능을 활성화하지 않더라도 **vRealize Log Insight**에서 **vRealize Operations Manager**로 알람 이벤트를 전송할 수 있습니다.

환경이 변경되는 경우 **vRealize Log Insight** 관리자는 **vRealize Log Insight**에서 **vSphere** 시스템을 변경, 추가 또는 제거하고, 경고 알람이 전송되는 **vRealize Operations Manager**의 인스턴스를 변경하거나 제거하고, **vSphere** 시스템 및 **vRealize Operations Manager**에 연결하는 데 사용되는 암호를 변경할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- **vSphere** 환경에 **vRealize Log Insight** 연결
- **vCenter Server** 인스턴스에서 이벤트, 작업 및 경보를 풀(pull)하도록 **vRealize Log Insight** 구성
- **vRealize Log Insight**에서 **vRealize Operations Manager** 사용
- **vRealize Log Insight**용 **vRealize Operations Manager** 콘텐츠 팩

vSphere 환경에 vRealize Log Insight 연결

vSphere 환경에서 경고, 이벤트 및 작업 데이터를 수집하도록 **vRealize Log Insight**을 구성하기 전에 하나 이상의 **vCenter Server** 시스템에 **vRealize Log Insight**을 연결해야 합니다.

vRealize Log Insight은 **vCenter Server** 인스턴스와 이러한 인스턴스가 관리하는 **ESXi** 호스트에서 두 가지 유형의 데이터를 수집할 수 있습니다.

- 이벤트, 작업 및 경고는 특정 의미가 있는 구조화된 데이터입니다. 구성된 경우 **vRealize Log Insight**은 등록된 **vCenter Server** 인스턴스에서 이벤트, 작업 및 경고를 풀합니다.
- 로그에는 **vRealize Log Insight**에서 분석할 수 있는 구조화되지 않은 데이터가 포함되어 있습니다. **ESXi** 호스트 또는 **vCenter Server Appliance** 인스턴스는 syslog를 통해 로그를 **vRealize Log Insight**으로 푸시할 수 있습니다.

사전 요구 사항


- 달성할 통합 수준의 경우 vCenter Server 시스템과 ESXi 호스트에서 필요한 구성을 수행하기에 충분한 권한이 있는 사용자 자격 증명을 가지고 있는지 확인합니다.

통합 수준	필요한 권한
이벤트, 작업 및 정보 수집	<ul style="list-style-type: none"> ■ 시스템.보기 참고 시스템.보기는 시스템 정의 권한입니다. 사용자 지정 역할을 추가하고 해당 역할에 할당한 권한이 없으면 역할이 세 가지 시스템 정의 권한(시스템.익명, 시스템.보기 및 시스템.읽기)을 보유한 읽기 전용 역할로 생성됩니다.
ESXi 호스트에 대한 Syslog 구성	<ul style="list-style-type: none"> ■ 호스트.구성.설정 변경 ■ 호스트.구성.네트워크 구성 ■ 호스트.구성.고급 설정 ■ 호스트.구성.보안 프로파일 및 방화벽

참고 vCenter Server 인벤토리 내의 최상위 폴더에 대한 권한을 구성하고 **하위 항목으로 전파** 확인란이 선택되어 있는지 확인해야 합니다.

- vCenter Server 시스템의 IP 주소 또는 도메인 이름을 알고 있는지 확인합니다.
- 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.

절차

- 1 구성 드롭다운 메뉴 아이콘  을 클릭하고 **관리**를 선택합니다.
- 2 통합 아래에서 **vSphere**를 클릭합니다.
- 3 vCenter Server에 대한 IP 주소 및 서비스 계정 자격 증명을 입력한 후 **연결 테스트**를 클릭합니다.
- 4 vSphere 환경이 신뢰할 수 없는 SSL 인증서를 제공하는 경우 인증서의 세부 정보가 포함된 대화상자가 나타납니다. **수락**을 클릭하여 vRealize Log Insight 클러스터에 있는 모든 노드의 신뢰 저장소에 인증서를 추가합니다.

취소를 클릭하면 인증서가 신뢰 저장소에 추가되지 않고, vSphere 환경과의 연결이 실패합니다. 연결에 성공하려면 인증서를 수락해야 합니다.

- 5 (선택 사항) 다른 vCenter Server를 등록하려면 **vCenter Server 추가**를 클릭하고 3~5단계를 반복합니다.

참고 중복된 이름 또는 IP 주소를 사용하는 vCenter Server 시스템을 등록하지 마십시오. vRealize Log Insight은 중복된 vCenter Server 이름을 확인하지 않습니다. 등록된 vCenter Server 시스템의 목록에 중복된 항목이 포함되어 있지 않은지 확인해야 합니다.

6 저장을 클릭합니다.

연결을 테스트하지 않았으며, vSphere 환경에서 신뢰할 수 없는 인증서를 제공하는 경우 4단계의 지침을 따르십시오.

다음에 수행할 작업

- 등록한 vCenter Server 인스턴스에서 이벤트, 작업 및 경고 데이터를 수집합니다. [vCenter Server](#) 인스턴스에서 이벤트, 작업 및 경보를 풀(pull)하도록 [vRealize Log Insight](#) 구성 항목을 참조하십시오.
- vCenter Server가 관리하는 ESXi 호스트에서 syslog 피드를 수집합니다. [로그 이벤트를 vRealize Log Insight](#)으로 전달하도록 [ESXi 호스트](#) 구성 항목을 참조하십시오.

Syslog 서버 역할의 vRealize Log Insight

vRealize Log Insight에는 vRealize Log Insight 서비스가 실행 중인 동안 계속 활성 상태를 유지하는 기본 제공 syslog 서버가 포함됩니다.

syslog 서버는 514/TCP, 1514/TCP 및 514/UDP 포트를 수신하고 다른 호스트에서 전송된 로그 메시지를 수집할 준비가 된 상태를 유지합니다. syslog 서버에서 수집된 메시지는 vRealize Log Insight 웹 사용자 인터페이스를 통해 거의 실시간으로 검색할 수 있게 됩니다. vRealize Log Insight에서 수락하는 최대 syslog 메시지 길이는 10KB입니다.

Syslog 형식 RFC-6587, RFC-5424 및 RFC-3164가 지원됩니다.

로그 이벤트를 vRealize Log Insight으로 전달하도록 ESXi 호스트 구성

ESXi 호스트 또는 vCenter Server Appliance 인스턴스가 vRealize Log Insight에서 분석될 수 있는 비구조화된 로그 데이터를 생성합니다.

vRealize Log Insight 관리 인터페이스를 사용하여 vRealize Log Insight에 syslog 데이터를 푸시하도록 ESXi 호스트를 등록된 vCenter Server에서 구성합니다.

경고 병렬 구성 작업을 실행하면 대상 ESXi 호스트의 syslog 설정이 잘못될 수 있습니다. 구성하려는 ESXi 호스트를 다른 관리자가 구성 중이지 않은지 확인합니다.

vRealize Log Insight 클러스터는 통합 로드 밸런서를 사용하여 클러스터의 개별 노드 간에 ESXi와 vCenter Server Appliance syslog 피드를 분산할 수 있습니다.

메시지가 vRealize Log Insight로 전송되기 전에 ESXi 호스트의 syslog 메시지를 필터링하는 방법에 대한 자세한 내용은 [vSphere 설치 및 설정](#) 가이드의 [ESXi 설정](#) 섹션에서 "ESXi 호스트의 로그 필터링 구성" 항목을 참조하십시오.

vCenter Server Appliance에서 수집하는 syslog 피드 구성에 대한 자세한 내용은 [로그 이벤트를 vRealize Log Insight](#)에 전달하도록 [vCenter Server](#) 구성을 참조하십시오.


참고 vRealize Log Insight는 ESXi 호스트 버전 5.5 이상의 syslog 데이터를 수신할 수 있습니다.

사전 요구 사항

- ESXi 호스트를 관리하는 vCenter Server가 vRealize Log Insight 인스턴스에 등록되어 있는지 확인합니다. 또는 한 번의 작업으로 ESXi 호스트 등록 및 vCenter Server 구성을 수행할 수 있습니다.
- ESXi 호스트에 대한 syslog를 구성하기에 충분한 권한이 있는 사용자 자격 증명을 가지고 있는지 확인합니다.
 - **호스트.구성.고급 설정**
 - **호스트.구성.보안 프로파일 및 방화벽**

참고 vCenter Server 인벤토리 내의 최상위 폴더에 대한 권한을 구성하고 **하위 항목으로 전파** 확인란이 선택되어 있는지 확인해야 합니다.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 통합 아래에서 **vSphere**를 클릭합니다.
- 3 vCenter Server 표에서 syslog 피드를 수신하려는 ESXi 호스트를 관리하는 vCenter Server 인스턴스를 찾은 후 **편집**을 클릭합니다.
- 4 열려 있는 편집 보기에서 **ESXi 호스트가 로그를 Log Insight에 전송하도록 구성** 확인란을 선택합니다.

기본적으로 vRealize Log Insight는 UDP를 통해 로그를 전송하도록 버전 5.5 이상의 모든 연결 가능한 ESXi 호스트를 구성합니다.

- 5 (선택 사항) 기본 구성 값을 수정하려면 **고급 옵션**을 클릭합니다.
 - 모든 ESXi 호스트에 대한 프로토콜을 변경하려면 **모든 ESXi 호스트 구성**을 선택하고 프로토콜을 선택한 다음 **확인**을 클릭합니다.
 - 특정 ESX 호스트 로깅만 설정하거나 선택한 ESXi 호스트에 대한 프로토콜을 변경하려면 다음 단계를 사용합니다.
 - a **특정 ESXi 호스트 구성**을 선택합니다.
 - b **호스트별 필터링** 목록에서 하나 이상의 호스트를 선택합니다.
 - c 프로토콜 값을 설정합니다.
 - d **확인**을 클릭합니다.
- 6 (선택 사항) 클러스터를 사용하는 경우 **대상** 텍스트 상자에 대한 드롭다운 메뉴를 열고 syslog 피드를 분산하는 로드 밸런서의 호스트 이름 또는 IP 주소를 선택합니다.
- 7 **저장**을 클릭합니다.

다음에 수행할 작업

ESXi 호스트 구성이 vCenter Server 포의 ESXi 호스트 구성 열에 표시됩니다. 호스트가 구성된 경우 호스트 구성 열에서 **세부 정보 보기**를 클릭하여 구성된 ESXi 호스트에 대한 세부 정보를 볼 수 있습니다.

vRealize Log Insight에 로그 이벤트를 전달하기 위해 ESXi 호스트 구성 수정

ESXi 호스트 또는 vCenter Server Appliance 인스턴스가 vRealize Log Insight에서 분석될 수 있는 비구조화된 로그 데이터를 생성합니다.

vRealize Log Insight 관리 인터페이스를 사용하여 vRealize Log Insight에 syslog 데이터를 푸시하도록 ESXi 호스트를 등록된 vCenter Server에서 구성합니다.

경고 병렬 구성 작업을 실행하면 대상 ESXi 호스트의 syslog 설정이 잘못될 수 있습니다. 구성하려는 ESXi 호스트를 다른 관리자가 구성 중이지 않은지 확인합니다.

초기 구성을 설정한 후에는 아직 구성되지 않은 기존 및 새로 추가된 vSphere ESXi 호스트를 주기적으로 확인하고 자동으로 구성하는 옵션을 사용하도록 설정할 수 있습니다. 현재 구성된 프로토콜은 ESXi 호스트를 자동으로 구성하는 데 사용됩니다.

vRealize Log Insight 클러스터는 통합 로드 밸런서를 사용하여 클러스터의 개별 노드 간에 ESXi와 vCenter Server Appliance syslog 피드를 분산할 수 있습니다.

구성된 메시지가 vRealize Log Insight로 전송되기 전에 ESXi 호스트의 syslog 메시지를 필터링하는 방법에 대한 자세한 내용은 **vSphere 설치 및 설정 가이드**의 **ESXi 설정** 섹션에서 "ESXi 호스트의 로그 필터링 구성" 항목을 참조하십시오.

vCenter Server Appliance에서 수집하는 syslog 피드 구성에 대한 자세한 내용은 **로그 이벤트를 vRealize Log Insight에 전달하도록 vCenter Server 구성**을 참조하십시오.

vRealize Log Insight는 ESXi 호스트 버전 5.5 이상의 syslog 데이터를 수신할 수 있습니다.

사전 요구 사항

- ESXi 호스트를 관리하는 vCenter Server가 vRealize Log Insight 인스턴스에 등록되어 있는지 확인합니다.
- ESXi 호스트에 대한 syslog를 구성하기에 충분한 권한이 있는 사용자 자격 증명을 가지고 있는지 확인합니다.
 - **호스트.구성.고급 설정**
 - **호스트.구성.보안 프로파일 및 방화벽**

참고 vCenter Server 인벤토리 내의 최상위 폴더에 대한 권한을 구성하고 **하위 항목으로 전파** 확인란이 선택되어 있는지 확인해야 합니다.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.

- 2 통합 아래에서 **vSphere**를 클릭합니다.
- 3 **ESXi 호스트가 로그를 Log Insight에 전송하도록 구성** 확인란을 선택합니다.
- 4 **고급 옵션**을 클릭합니다.
- 5 선택한 ESXi 호스트에 대한 프로토콜을 변경하려면 다음 단계를 사용합니다.
 - a **호스트별 필터링** 목록에서 하나 이상의 호스트를 선택합니다.
 - b 현재 프로토콜이 원하는 프로토콜인지 확인하고, 그렇지 않으면 다른 프로토콜을 선택합니다.
 - c 현재 구성된 프로토콜을 사용하여 ESXi 호스트의 자동 구성을 사용하도록 설정하려면 **모든 ESXi 호스트를 자동으로 구성**을 선택합니다. 이 옵션을 사용하도록 설정하면 vRealize Log Insight는 아직 구성되지 않은 기존 및 새로 추가된 vSphere ESXi 호스트를 주기적으로 찾아 구성합니다.
 - d **구성**을 클릭하여 선택한 호스트의 구성을 시작합니다. ESXi 대화상자가 닫힙니다.
 - e 메시지 대화상자에서 **확인**을 클릭합니다.
 - f 프로토콜 설정을 변경한 경우 **ESXi 구성** 대화 상자를 닫은 후 기본 창에서 **저장**을 클릭합니다.
- 6 (선택 사항) 클러스터를 사용하는 경우 **vSphere 통합** 페이지에서 **대상** 텍스트 상자에 대한 드롭다운 메뉴를 열고 로드 밸런서에 대한 호스트 이름 또는 IP 주소를 선택하여 로드 밸런서를 지정할 수 있습니다.

vRealize Operations Manager의 vRealize Log Insight 알림 이벤트

생성하는 경고 쿼리를 기준으로 vRealize Operations Manager에 알림 이벤트를 전송하도록 vRealize Log Insight을 구성할 수 있습니다.

vRealize Log Insight에서 알림 경고를 구성하는 경우 알림 이벤트와 관련된 vRealize Operations Manager에서 리소스를 선택합니다. **Log Insight**에서 경고 쿼리를 추가하여 **vRealize Operations Manager**에 알림 이벤트 보내기를 참조하십시오.

다음은 알림 이벤트가 나타나는 vRealize Operations Manager UI의 섹션입니다.

- 홈 > **권장 사항** 대시보드 > **하위 항목에 대한 주요 상태 경고** 위젯
- 홈 > **경고** 탭
- 알림 이벤트가 있는 위젯이 포함된 모든 사용자 지정 대시보드

알림 이벤트가 표시되는 위치에 대한 자세한 내용은 [VMware vRealize Operations Manager 설명서 센터](#)를 참조하십시오.

로그 이벤트를 vRealize Log Insight에 전달하도록 vCenter Server 구성

vSphere 통합은 vCenter Server에서 작업과 이벤트를 수집하지만 각 vCenter Server 구성 요소의 하위 수준 내부 로그는 수집하지 않습니다. 이러한 로그는 vSphere 컨테츠 팩에서 사용합니다.

vCenter Server 6.5 이상 릴리스 구성은 vCenter Server Appliance 관리 인터페이스를 통해 수행해야 합니다. vCenter Server에서 로그 이벤트를 전달하는 방법에 대한 자세한 내용은 vCenter Server Appliance 로그 파일을 다른 시스템으로 리디렉션하는 방법에 대한 vSphere 설명서를 참조하십시오.

이전 버전의 vSphere의 경우 로그를 라우팅하는 데 사용할 수 있는 syslog 데몬이 vCenter Server Appliance에 포함되어 있지만 선호되는 방법은 vRealize Log Insight 에이전트를 설치하는 것입니다.

vRealize Log Insight 에이전트를 설치하는 방법에 대한 내용은 "vRealize Log Insight Agent 작업" 을 참조하십시오.

vCenter Server 설치에서 수집할 특정 로그 파일을 정의하는 에이전트 그룹이 vSphere 컨텐츠 팩에 포함되어 있습니다. 구성은 `https://LogInsightServerFqdnOrIP/contentpack?contentPackId=com.vmware.vsphere`에서 볼 수 있습니다.

에이전트 그룹으로 작업하는 데 대한 자세한 내용은 [장 9 중앙 집중식 에이전트 구성 및 에이전트 그룹 항목](#)을 참조하십시오.

vCenter Server 로그 파일 위치에 대한 자세한 내용은 <http://kb.vmware.com/kb/1021804> 및 <http://kb.vmware.com/kb/1021806>을 참조하십시오.

vCenter Server 인스턴스에서 이벤트, 작업 및 경보를 풀(pull)하도록 vRealize Log Insight 구성

이벤트, 작업 및 경고는 특정 의미가 있는 구조화된 데이터입니다. 하나 이상의 vCenter Server 시스템에서 정보, 이벤트 및 작업 데이터를 수집하도록 vRealize Log Insight을 구성할 수 있습니다.

관리 UI를 사용하여 vCenter Server 시스템에 연결하도록 vRealize Log Insight을 구성합니다. vSphere Web Services API를 사용하여 정보가 vCenter Server 시스템에서 풀되고 vRealize Log Insight 웹 사용자 인터페이스에 vSphere 컨텐츠 팩으로 표시됩니다.

vSphere 6.5에는 새 네이티브 고가용성 솔루션이 있습니다. HA 및 로드 밸런서 사용에 대한 자세한 내용은 www.vmware.com에서 사용할 수 있는 "VMware vSphere 6.5의 새로운 기능" 백서를 참조하십시오.


참고 vRealize Log Insight은 vCenter Server 5.5 이상에서만 경고, 이벤트 및 작업 데이터를 풀할 수 있습니다.

사전 요구 사항

시스템.보기 권한이 있는 사용자 자격 증명을 가지고 있는지 확인합니다.

참고 vCenter Server 인벤토리 내의 최상위 폴더에 대한 권한을 구성하고 **하위 항목으로 전파** 확인란이 선택되어 있는지 확인해야 합니다.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 통합 아래에서 **vSphere**를 클릭합니다.
- 3 vCenter Server 표에서 데이터를 수집하려는 vCenter Server 인스턴스를 찾습니다.
- 4 열려 있는 편집 보기에서 **vCenter Server 이벤트, 작업 및 경고 수집** 확인란을 선택합니다.
- 5 **저장**을 클릭합니다.

결과

vRealize Log Insight은 vCenter Server에 2분마다 연결되며 마지막 폴링 성공 이후의 모든 새 정보를 수집합니다.

다음에 수행할 작업

- vSphere 컨텐츠 팩 또는 사용자 지정 쿼리를 사용하여 vSphere 이벤트를 분석합니다.
- vSphere 컨텐츠 팩 경고 또는 사용자 지정 경고를 활성화합니다.

vRealize Log Insight에서 vRealize Operations Manager 사용

vRealize Operations Manager와의 통합을 위한 요구 사항

vRealize Operations Manager와 vRealize Log Insight 통합의 일부로 vRealize Log Insight에 대한 자격 증명을 지정하여 vRealize Operations Manager에서 인증을 받아야 합니다.

vRealize Operations Manager는 로컬 사용자 계정 및 다중 LDAP 소스를 모두 지원합니다. vRealize Operations Manager 및 VMware Identity Manager 통합은 둘 다 vRealize Log Insight 관리자가 구성합니다.

배포가 vRealize Log Insight에서 VMware Identity Manager 통합을 사용하는 경우 VMware Identity Manager 폴백 URL(리디렉션 URL 호스트) 및 vRealize Operations Manager 통합 페이지의 대상 필드는 정확히 동일한 값이어야 합니다.

사전 요구 사항

통합 사용자 계정에 vRealize Operations Manager에서 개체를 조작할 수 있는 사용 권한이 있는지 확인합니다. 로컬 또는 [Active Directory](#) 사용자 계정의 필요한 최소 사용 권한 항목을 참조하십시오.

절차

- ◆ 로컬 사용자 계정의 사용자 이름을 확인하려면:
 - a vRealize Operations Manager 웹 인터페이스에서 **액세스 제어**를 선택합니다.
 - b 통합 사용자를 식별하거나 생성합니다. 소스 유형 필드는 **로컬 사용자**입니다.
 - c **사용자 이름** 필드의 값을 적어둡니다. vRealize Log Insight 관리 사용자 인터페이스에서 통합을 구성하는 경우 이 사용자 이름을 지정합니다.
- ◆ vRealize Log Insight에서 제공되어야 하는 LDAP 사용자 계정에 대한 사용자 이름 형식을 결정하려면 다음 지침을 따릅니다.
 - a vRealize Operations Manager 웹 인터페이스에서 **액세스 제어**를 선택합니다.
 - b 통합 사용자를 식별하거나 생성합니다. **사용자 이름** 및 **소스 유형** 필드를 메모합니다. 예를 들어 소스가 **Active Directory - ad**이고 이름이 **integration@example.com**인 사용자를 메모합니다.

- c 인증 소스를 선택합니다.
- d b단계에서 **소스 유형**에 해당하는 인증 소스를 식별합니다. **소스 표시 이름** 필드를 메모합니다. 예를 들어 "ad"를 메모합니다.
- e vRealize Log Insight 관리 사용자 인터페이스에서 입력해야 하는 사용자 이름은 `UserName@SourceDisplayName`과 같은 형식으로 3단계 및 5단계에서 결합됩니다. 예를 들면 `integration@example.com@ad`와 같습니다.

로컬 또는 Active Directory 사용자 계정의 필요한 최소 사용 권한

vRealize Log Insight를 vRealize Operations Manager와 통합하려면 vRealize Operations Manager에 대해 인증할 vRealize Log Insight의 자격 증명을 지정해야 합니다. vRealize Operations Manager에서 개체를 조작하려면 사용자 계정이 필수 사용 권한을 가지고 있어야 합니다.

컨텍스트에서 실행을 위해 사용자에게 사용 권한을 할당하는 경우 경고 통합을 구성할 수도 있습니다. 경고 통합 테이블의 정보는 경고 통합을 위한 사용 권한 할당에만 사용하십시오.

표 11-1. 경고 통합

작업	선택할 사용 권한 및 개체
나열된 사용 권한을 가진 사용자 지정 역할을 생성합니다.	<ol style="list-style-type: none"> 1 관리 -> Rest API <ol style="list-style-type: none"> a 다른 모든 읽기, 쓰기 API b API에 대한 읽기 액세스 권한
이전 역할을 로컬 또는 Active Directory 사용자(새 사용자 또는 기존 사용자)에게 할당하고, 할당할 개체 계층을 선택합니다.	<ol style="list-style-type: none"> 1 어댑터 인스턴스 -> vRealizeOpsMgrAPI[모두 선택] 2 vSphere 호스트 및 클러스터[모두 선택] 3 vSphere 네트워킹[모두 선택] 4 vSphere 스토리지[모두 선택]

표 11-2. 컨텍스트에서 실행 통합

작업	선택할 사용 권한 및 개체
나열된 사용 권한을 가진 사용자 지정 역할을 생성합니다.	<ol style="list-style-type: none"> 관리 -> Rest API <ol style="list-style-type: none"> 다른 모든 읽기, 쓰기 API API에 대한 읽기 액세스 권한 리소스 삭제 관리 -> 구성 -> 리소스 관계 관리 관리 -> 리소스 종류 관리 <ol style="list-style-type: none"> 생성 편집 관리 -> 리소스 관리 <ol style="list-style-type: none"> 생성 삭제 읽기 관리 -> 액세스 -> 액세스 제어 -> 역할 추가, 편집 또는 삭제 <p>참고 이 사용 권한은 vRealize Operations Manager 7.0 이하 버전에 필요합니다.</p>
이전 역할을 로컬 또는 Active Directory 사용자(새 사용자 또는 기존 사용자)에게 할당하고, 할당할 개체 계층을 선택합니다.	시스템 내의 모든 개체에 대한 액세스 허용을 선택합니다.

vRealize Operations Manager에 알림 이벤트를 전송하도록 vRealize Log Insight 구성

vRealize Operations Manager에 경고 알림을 전송하도록 vRealize Log Insight를 구성할 수 있습니다.

vRealize Log Insight를 vRealize Operations Manager vApp 및 vRealize Operations Manager 설치 파일과 통합할 수 있습니다. 설치 파일 버전과 통합하려면 vRealize Operations Manager 구성에 대한 추가 변경이 필요합니다. vRealize Log Insight와 통합하도록 vRealize Operations Manager 설치 파일 구성에 대한 자세한 내용은 "Log Insight 시작 가이드"를 참조하십시오.

vRealize Log Insight 경고를 vRealize Operations Manager와 통합하면 단일 사용자 인터페이스에서 환경에 대한 모든 정보를 볼 수 있습니다.

여러 vRealize Log Insight 인스턴스의 알림 이벤트를 단일 vRealize Operations Manager 인스턴스에 보낼 수 있습니다. vRealize Operations Manager 인스턴스별로 단일 vRealize Log Insight 인스턴스에 대해 컨텍스트에서 실행을 사용하도록 설정할 수 있습니다.

vRealize Log Insight는 컨텍스트에서 실행 어댑터 구성을 위해 vRealize Operations Manager에서 리소스 및 관계를 생성하는 데 vRealize Operations Manager REST API를 사용합니다.

사전 요구 사항

- vRealize Operations Manager에서 필요한 사용 권한을 가진 통합 사용자 계정을 생성합니다. 자세한 내용은 [vRealize Operations Manager와의 통합을 위한 요구 사항](#) 항목을 참조하십시오.

- 대상 vRealize Operations Manager 인스턴스의 IP 주소 또는 호스트 이름을 알고 있는지 확인합니다.
- 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.

참고 로드 밸런서가 구성된 vRealize Operations Manager 클러스터를 실행하는 환경에서는 로드 밸런서 IP 주소(제공되는 경우)를 사용할 수 있습니다.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 통합 아래에서 **vRealize Operations Manager**를 선택합니다.
- 3 기본 노드 또는 로드 밸런서(구성된 경우)의 IP 주소나 호스트 이름을 입력합니다. vRealize Operations Manager 사용자 자격 증명을 사용하고, **연결 테스트**를 클릭합니다. vRealize Log Insight는 자격 증명을 사용하여 알림 이벤트를 vRealize Operations Manager에 푸시합니다. 구성된 사용자가 통합에 필요한 최소 사용 권한을 가지고 있는지 확인합니다. 로컬 또는 **Active Directory** 사용자 계정의 필요한 **최소 사용 권한** 항목을 참조하십시오.
- 4 vRealize Operations Manager가 신뢰할 수 없는 SSL 인증서를 제공하는 경우 인증서의 세부 정보가 포함된 대화상자가 나타납니다. **수락**을 클릭하여 vRealize Log Insight 클러스터에 있는 모든 노드의 신뢰 저장소에 인증서를 추가합니다.

취소를 클릭하면 인증서가 신뢰 저장소에 추가되지 않고, vRealize Operations Manager와의 연결이 실패합니다. 연결에 성공하려면 인증서를 수락해야 합니다.

- 5 vRealize Operations Manager 창에서 **경고 통합 사용**을 선택합니다.
- 6 **저장**을 클릭합니다.

연결을 테스트하지 않았으며, vRealize Operations Manager에서 신뢰할 수 없는 인증서를 제공하는 경우 4단계의 지침을 따르십시오.

다음에 수행할 작업

- vRealize Log Insight가 전송하는 알림 이벤트를 보려면 vRealize Operations Manager UI에서 관련 페이지를 참조하십시오.

vRealize Operations Manager에서 vRealize Log Insight에 대한 컨텍스트에서 실행 기능 활성화

vRealize Log Insight와 관련된 메뉴 항목을 표시하고 개체별 쿼리를 사용하여 vRealize Log Insight를 시작하도록 vRealize Operations Manager를 구성할 수 있습니다.

vRealize Log Insight를 vRealize Operations Manager vApp 및 vRealize Operations Manager 설치 파일과 통합할 수 있습니다.

vApp 설치 및 Installable(Windows, Linux)과 통합하려면 vRealize Operations Manager 구성을 추가로 변경해야 합니다. [vRealize Log Insight 4.0 설명서 센터](#)에서 vRealize Operations Manager 6.x 이상 버전의 vRealize Log Insight Management Pack(어댑터) 설치에 대한 항목을 참조하십시오.

vRealize Log Insight Management Pack은 vRealize Operations Manager 6.0 이상에서 미리 설치되며 구성을 변경할 필요가 없습니다.


vRealize Operations Manager Installable(Windows 버전)은 vRealize Operations Manager 6.5 이상에서 더 이상 지원되지 않습니다.

중요 vRealize Operations Manager의 인스턴스 하나는 vRealize Log Insight의 인스턴스 하나에 대해서만 컨텍스트에서 실행 기능을 지원합니다. vRealize Log Insight은 다른 인스턴스가 vRealize Operations Manager에 이미 등록되어 있는지 여부를 확인하지 않기 때문에 다른 사용자의 설정을 재정의할 수도 있습니다.

사전 요구 사항

- 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.
- 대상 vRealize Operations Manager 인스턴스의 IP 주소 또는 호스트 이름을 알고 있는지 확인합니다.
- 필요한 사용자 자격 증명이 있는지 확인합니다. 로컬 또는 [Active Directory](#) 사용자 계정의 **필요한 최소 사용 권한** 항목을 참조하십시오.
- vRealize Operations Manager 6.5 이상을 사용하는 경우 [vRealize Operations Manager 6.5 정보 센터](#)에서 컨텍스트에서 실행을 사용하도록 설정하기 위한 절차를 참조하십시오.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 통합 아래에서 **vRealize Operations Manager**를 선택합니다.
- 3 vRealize Operations Manager 기본 노드 또는 로드 밸런서(구성된 경우)의 IP 주소나 FQDN을 입력하고 **연결 테스트**를 클릭합니다.

참고 컨텍스트에서 실행 기능의 경우, 관리자 권한이 있는 vRealize Operations Manager 사용자를 제공해야 합니다.

- 4 **저장**을 클릭합니다.

결과

vRealize Log Insight이 vRealize Operations Manager 인스턴스를 구성합니다. 이 작업에는 몇 분 정도 걸릴 수 있습니다.

vRealize Log Insight과 관련된 항목이 vRealize Operations Manager의 메뉴에 표시됩니다.

다음에 수행할 작업

vRealize Operations Manager 인스턴스에서 vRealize Log Insight 쿼리를 실행합니다. [vRealize Log Insight 컨텍스트에서 실행](#) 항목을 참조하십시오.

vRealize Log Insight 컨텍스트에서 실행

vRealize Log Insight에 대해 컨텍스트에서 실행을 사용하도록 설정하면 vRealize Operations Manager에 vRealize Log Insight 리소스가 생성됩니다.

리소스 식별자는 vRealize Log Insight 인스턴스의 IP 주소를 포함하며 vRealize Operations Manager가 vRealize Log Insight을 여는 데 사용됩니다.

vRealize Operations Manager 6.5 이상에서 컨텍스트에서 실행

컨텍스트에서 실행을 사용하도록 설정하는 방법에 대한 자세한 내용은 [vRealize Operations Manager 정보 센터](#)를 참조하십시오.

vRealize Operations Manager 6.4 이하 버전의 vSphere 사용자 인터페이스에서 컨텍스트에서 실행

vRealize Log Insight과 관련된 컨텍스트에서 실행 옵션은 vSphere 사용자 인터페이스의 **작업** 드롭다운 메뉴에 표시됩니다. 이러한 메뉴 항목을 사용하여 vRealize Log Insight을 열고 vRealize Operations Manager의 개체에서 로그 이벤트를 검색할 수 있습니다.

사용 가능한 컨텍스트에서 실행 작업은 vRealize Operations Manager 인벤토리에서 선택하는 개체에 따라 다릅니다. 쿼리의 시간 범위는 컨텍스트에서 실행 옵션을 클릭하기 60분 전으로 제한되어 있습니다.

표 11-3. vRealize Operations Manager UI의 개체와 해당 컨텍스트에서 실행 옵션 및 작업

vRealize Operations Manager에서 선택된 개체	작업 드롭다운 메뉴의 컨텍스트에서 실행 옵션	vRealize Operations Manager의 작업	vRealize Log Insight의 작업
월드	vRealize Log Insight 열기	vRealize Log Insight을 엽니다.	vRealize Log Insight은 대화형 분석 탭을 표시합니다.
vCenter Server	vRealize Log Insight 열기	vRealize Log Insight을 엽니다.	vRealize Log Insight은 대화형 분석 탭을 표시합니다.
데이터 센터	vRealize Log Insight에서 로그 검색	vRealize Log Insight를 열고 선택된 데이터 센터 개체 아래의 모든 호스트 시스템의 리소스 이름을 전달합니다.	vRealize Log Insight은 대화형 분석 탭을 표시하고 데이터 센터 내의 호스트 이름이 포함된 로그 이벤트를 찾기 위한 쿼리를 수행합니다.
클러스터	vRealize Log Insight에서 로그 검색	vRealize Log Insight을 열고 선택된 클러스터 개체 아래의 모든 호스트 시스템의 리소스 이름을 전달합니다.	vRealize Log Insight은 대화형 분석 탭을 표시하고 클러스터 내의 호스트 이름이 포함된 로그 이벤트를 찾기 위한 쿼리를 수행합니다.

표 11-3. vRealize Operations Manager UI의 개체와 해당 컨텍스트에서 실행 옵션 및 작업 (계속)


vRealize Operations Manager에서 선택된 개체	작업 드롭다운 메뉴의 컨텍스트에서 실행 옵션	vRealize Operations Manager의 작업	vRealize Log Insight의 작업
호스트 시스템	vRealize Log Insight에서 로그 검색	vRealize Log Insight을 열고 선택된 호스트 개체의 리소스 이름을 전달합니다.	vRealize Log Insight은 대화형 분석 탭을 표시하고 선택된 호스트 시스템의 이름이 포함된 로그 이벤트를 찾기 위한 쿼리를 수행합니다.
가상 시스템	vRealize Log Insight에서 로그 검색	vRealize Log Insight을 열고 선택된 가상 시스템의 IP 주소와 관련 호스트 시스템의 리소스 이름을 전달합니다.	vRealize Log Insight은 대화형 분석 탭을 표시하고 가상 시스템의 IP 주소와 가상 시스템이 상주하는 호스트의 이름이 포함된 로그 이벤트를 찾기 위한 쿼리를 수행합니다.

경고 탭에서 경고를 선택하고 컨텍스트 내 메뉴에서 **Log Insight에서 로그 검색**을 선택하는 경우 쿼리의 시간 범위는 경고가 트리거되기 1시간 전으로 제한됩니다. 예를 들어 경고가 오후 2시에 트리거된 경우 vRealize Log Insight의 쿼리는 오후 1시와 오후 2시 사이에 발생한 모든 로그 메시지를 표시합니다. 이를 통해 경고를 트리거했을 수 있는 이벤트를 식별할 수 있습니다.

vRealize Operations Manager의 메트릭 차트에서 vRealize Log Insight을 열 수 있습니다. vRealize Log Insight을 실행하는 쿼리의 시간 범위는 메트릭 차트의 시간 범위와 일치합니다.

참고 가상 장치의 시간 설정이 다른 경우 vRealize Log Insight 및 vRealize Operations Manager 메트릭 차트에서 보는 시간은 다를 수 있습니다.

vRealize Operations Manager 6.4 이하 버전의 사용자 인터페이스의 컨텍스트에서 실행

컨텍스트에서 실행 아이콘 이 사용자 인터페이스의 여러 페이지에 나타나지만 vRealize Log Insight 알림 이벤트가 표시되는 페이지에서만 vRealize Log Insight을 실행할 수 있습니다.

- 경고 개요 페이지.
- vRealize Log Insight 알림 경고의 경고 요약 페이지.
- 대시보드의 경고 위젯(vRealize Log Insight 알림 경고가 선택된 경우).

사용자 지정 사용자 인터페이스에서 vRealize Log Insight 알림 이벤트를 선택할 때 두 개의 컨텍스트에서 실행 작업 중에서 선택할 수 있습니다.

표 11-4. vRealize Operations Manager UI의 컨텍스트에서 실행 옵션 및 작업

vRealize Operations Manager의 컨텍스트에서 실행 옵션	vRealize Operations Manager의 작업	vRealize Log Insight의 작업
vRealize Log Insight 열기	vRealize Log Insight을 엽니다.	vRealize Log Insight은 대시보드 탭을 표시하고 vSphere 개요 대시보드를 로드합니다.
vRealize Log Insight에서 로그 검색	vRealize Log Insight을 열고 알림 이벤트를 트리거한 쿼리의 ID를 전달합니다.	vRealize Log Insight은 대화형 분석 탭을 표시하고 알림 이벤트를 트리거한 쿼리를 수행합니다.

vRealize Log Insight에서 발생하지 않은 경고를 선택하는 경우 컨텍스트에서 실행 메뉴에 **vRealize Log Insight에서 VM 및 호스트 로그 검색** 메뉴 항목이 포함됩니다. 이 메뉴 항목을 선택하는 경우 vRealize Operations Manager는 vRealize Log Insight을 열고 경고를 트리거한 개체의 식별자를 전달합니다. vRealize Log Insight은 리소스 식별자를 사용하여 사용 가능한 로그 이벤트에서 검색을 수행합니다.

양방향 컨텍스트에서 실행

vRealize Log Insight에서 vRealize Operations Manager로 컨텍스트에서 실행 기능을 사용할 수도 있습니다.

vRealize Log Insight를 vRealize Operations Manager와 통합하면 이벤트의 왼쪽에 있는 톱니 바퀴 아이콘을 선택한 후 vRealize Operations Manager에서 보려는 옵션을 선택하여 vRealize Log Insight 이벤트에서 컨텍스트에서 실행을 수행할 수 있습니다.

vRealize Operations Manager에서 vRealize Log Insight로의 컨텍스트에서 실행에 대한 자세한 내용은 [vRealize Log Insight 컨텍스트에서 실행](#) 항목을 참조하십시오.

절차

- 1 vRealize Log Insight에서 **대화형 분석** 탭으로 이동합니다.
- 2 인벤토리 매핑 필드가 포함된 이벤트를 찾아서 해당 이벤트 위로 마우스 커서를 이동합니다.
- 3 톱니 바퀴 아이콘을 클릭하고, 드롭다운 메뉴에서 vRealize Operations Manager에서 **분석 열기**를 선택합니다.

vRealize Log Insight와 통합된 vRealize Operations Manager 인스턴스로 연결되는 새 브라우저 탭이 열립니다. 인증을 마치면 개체가 선택된 상태로 vRealize Operations Manager의 **환경 > 분석** 섹션으로 이동됩니다.

참고 vRealize Operations Manager 인스턴스 하나에 vRealize Log Insight 인스턴스 여러 개가 연결되어 있으면 vRealize Operations Manager와 통합된 마지막 vRealize Log Insight 인스턴스에서만 컨텍스트에서 실행 기능을 사용할 수 있습니다. 즉, 이전에 다른 vRealize Log Insight 인스턴스와 통합되었던 vRealize Operations Manager 인스턴스에 vRealize Log Insight 인스턴스를 통합할 때마다 컨텍스트에서 실행 기능이 재정의된다는 의미입니다.

vRealize Operations Manager에서 vRealize Log Insight에 대한 컨텍스트에서 실행 기능 비활성화

vRealize Operations Manager 인스턴스에서 vRealize Log Insight을 제거하여 vRealize Operations Manager 사용자 인터페이스에서 vRealize Log Insight과 관련된 메뉴 항목을 제거할 수 있습니다.


vRealize Log Insight의 관리 UI를 사용하여 컨텍스트에서 실행 기능을 비활성화합니다. vRealize Log Insight에 대한 액세스 권한이 없거나 vRealize Log Insight 인스턴스가 vRealize Operations Manager와의 연결이 비활성화되기 전에 삭제된 경우 vRealize Operations Manager의 관리 UI에서 vRealize Log Insight을 등록 취소할 수 있습니다. vRealize Operations Manager 관리 포털의 도움말을 참조하십시오.

경고 vRealize Operations Manager의 인스턴스 하나는 vRealize Log Insight의 인스턴스 하나에 대해서만 컨텍스트에서 실행 기능을 지원합니다. 비활성화할 인스턴스를 등록한 후 vRealize Log Insight의 다른 인스턴스가 등록된 경우 두 번째 인스턴스는 알림 없이 첫 번째 인스턴스의 설정을 재정의합니다.

사전 요구 사항

- 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.

절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 통합 아래에서 **vRealize Operations Manager**를 선택합니다.
- 3 **컨텍스트에서 실행 사용** 확인란의 선택을 취소합니다.
- 4 **저장**을 클릭합니다.

결과

vRealize Log Insight은 vRealize Log Insight 어댑터를 제거하도록 vRealize Operations Manager 인스턴스를 구성합니다. 이 작업에는 몇 분이 소요될 수 있습니다.

DNS 검색 경로 및 도메인 추가

DNS 검색 경로와 도메인을 추가하여 일치하는 vRealize Operations Manager 인벤토리의 검색 성능을 높일 수 있습니다.

DNS 검색 경로 및 도메인을 추가하면 가상 시스템 레이블 및 검색 도메인이 IP 주소(vRealize Log Insight로 로그 메시지를 전송하는 호스트의 IP 주소)로 확인되는 경우 일치율을 높일 수 있습니다. 예를 들어 vRealize Operations Manager에 `linux_01`이라는 가상 시스템이 있고 호스트 이름 `linux_01.company.com`이 `192.168.10.10`으로 확인될 경우 검색 도메인을 추가하면 vRealize Log Insight에서 해당 리소스를 인식하고 일치시킬 수 있습니다.

절차

- 1 vRealize Log Insight 가상 장치의 게스트 종료를 수행합니다.

2 가상 시스템의 전원이 꺼지면 **설정 편집**을 선택합니다.

3 **vApp 옵션** 탭을 선택합니다.

4 **vApp 옵션 > 인증**에서 **속성**을 클릭합니다.

5 `vami.searchpath.VMware_vCenter_Log_Insight` 및 `vami.domain.VMware_vCenter_Log_Insight` 키를 찾습니다.

이러한 키가 없는 경우 키를 생성합니다.

검색 경로 키에 다음 값을 사용합니다.

- 범주는 **네트워킹 속성**입니다.
- 레이블은 **DNS 검색 경로**입니다.
- 키 클래스 ID는 **vami**입니다.
- 키 인스턴스 ID는 **VMware_vCenter_Log_Insight**입니다.
- 유형은 **정적 속성**, 문자열 및 **사용자 구성 가능**입니다.

도메인 키의 경우 레이블에 **DNS 도메인**을 지정하고 키 ID에 **도메인**을 지정하여 같은 값을 사용합니다.

6 DNS 검색 경로와 도메인을 설정합니다. 예를 들면 `ny01.acme.local`입니다.

7 가상 장치의 전원을 켭니다.

다음에 수행할 작업

vRealize Log Insight가 부팅되면 로그인한 후 `/etc/resolv.conf` 파일의 콘텐츠를 확인하여 DNS 구성이 유효한지 확인할 수 있습니다. 파일의 끝 부분에서 검색 및 도메인 옵션을 볼 수 있습니다.

vRealize Log Insight 어댑터 제거

vRealize Operations Manager 6.2 이상 인스턴스에서 컨텍스트에서 실행을 사용하는 경우, vRealize Log Insight가 vRealize Operations Manager 인스턴스에 vRealize Log Insight 어댑터의 인스턴스를 생성합니다.

이 어댑터의 인스턴스는 vRealize Log Insight를 제거할 때 vRealize Operations Manager 인스턴스에 남아 있습니다. 결과적으로 컨텍스트에서 실행 메뉴 항목은 계속해서 작업 메뉴에 표시되며 더 이상 존재하지 않는 vRealize Log Insight 인스턴스를 가리킵니다.

vRealize Operations Manager에서 컨텍스트에서 실행 기능을 비활성화하려면 vRealize Operations Manager 인스턴스에서 vRealize Log Insight 어댑터를 제거해야 합니다.

명령줄 유틸리티 cURL을 사용하여 REST 호출을 vRealize Operations Manager로 전송할 수 있습니다.

참고 컨텍스트에서 실행이 사용된 경우에만 해당 단계가 필요합니다.

사전 요구 사항

- cURL이 시스템에 설치되어 있는지 확인합니다. 이 도구는 vRealize Operations Manager 가상 장치에 미리 설치되며 IP 주소 127.0.0.1을 사용하여 장치에서 해당 단계를 수행할 수 있습니다.
- 대상 vRealize Operations Manager 인스턴스의 IP 주소 또는 호스트 이름을 알고 있는지 확인합니다.
- 소유한 vRealize Operations Manager 라이선스에 따라 관리 팩을 제거하는 데 필요한 최소 자격 증명을 가지고 있는지 확인합니다. 로컬 또는 Active Directory 사용자 계정의 필요한 최소 사용 권한 항목을 참조하십시오.

절차

- 1 cURL에서 vRealize Operations Manager 가상 장치에 대한 다음 쿼리를 실행하여 vRealize Log Insight 어댑터를 찾습니다.

```
curl -k -u "admin" https://ipaddress/suite-api/api/adaptkinds/LogInsight/resourcekinds/LogInsightLogServer/resources
```

여기서 *admin*은 관리자 로그인 이름이고 *ipaddress*는 vRealize Operations Manager 인스턴스의 IP 주소(또는 호스트 이름)입니다. 사용자의 암호 *admin*을 입력하라는 메시지가 표시됩니다.

cURL 출력에서 <ops:resource creationTime="{TIMESTAMP}" identifier="{GUID}"> 식별자에 할당된 GUID 값을 찾습니다. 어댑터 인스턴스를 제거하는 아래 명령에서 이 GUID 값을 사용할 수 있습니다.

- 2 다음 명령을 실행하여 vRealize Log Insight 어댑터를 제거합니다.

```
curl -k -u "admin" -X DELETE https://ipaddress/suite-api/api/adapters/{GUID}
```

여기서 *admin*은 관리자 로그인 이름이고 *ipaddress*는 vRealize Operations Manager 인스턴스의 IP 주소(또는 호스트 이름)입니다. 사용자의 암호 *admin*을 입력하라는 메시지가 표시됩니다.

결과

vRealize Log Insight 컨텍스트에서 실행 항목이 vRealize Operations Manager의 메뉴에서 제거됩니다. 컨텍스트에서 실행에 대한 자세한 내용은 vRealize Log Insight 제품 내 도움말의 "vRealize Log Insight 컨텍스트에서 실행" 항목을 참조하십시오.

vRealize Log Insight용 vRealize Operations Manager 콘텐츠 팩

vRealize Log Insight용 vRealize Operations Manager 콘텐츠 팩에는 vRealize Operations Manager 인스턴스에서 리더렉션된 모든 로그를 분석하는 데 사용되는 대시보드, 추출된 필드, 저장된 쿼리 및 경고가 포함되어 있습니다.

vRealize Operations Manager 콘텐츠 팩은 vRealize Operations Manager 인스턴스에서 리디렉션된 모든 로그를 분석하기 위한 방법을 제공합니다. 콘텐츠 팩에는 vRealize Operations Manager 관리자에게 진단 및 문제 해결 기능을 제공하기 위한 대시보드, 쿼리 및 경고가 포함되어 있습니다. 대시보드는 향상된 관리 용이성을 제공하기 위해 분석, UI 및 어댑터와 같은 vRealize Operations Manager의 주요 구성 요소에 따라 그룹화됩니다. 다양한 경고를 사용하여 관리자에게 vRealize Operations Manager의 알림 이벤트와 이메일을 전송할 수 있습니다.

[https://solutionexchange.vmware.com/store/loginsight?](https://solutionexchange.vmware.com/store/loginsight?src=Product_Product_LogInsight_YES_US)

[src=Product_Product_LogInsight_YES_US](https://solutionexchange.vmware.com/store/loginsight?src=Product_Product_LogInsight_YES_US)에서 vRealize Operations Manager 콘텐츠 팩을 다운로드할 수 있습니다.

콘텐츠 팩을 사용하여 작업을 참조하십시오.

vRealize Log Insight에 대한 보안 고려 사항

12

vRealize Log Insight 기능을 사용하여 공격으로부터 환경을 보호합니다.

본 장은 다음 항목을 포함합니다.

- 포트 및 외부 인터페이스
- vRealize Log Insight 구성 파일
- vRealize Log Insight 공용 키, 인증서 및 키 저장소
- vRealize Log Insight 라이선스 및 EULA 파일
- vRealize Log Insight 로그 파일
- vRealize Log Insight 사용자 계정
- vRealize Log Insight 방화벽 권장 사항
- 보안 업데이트 및 패치

포트 및 외부 인터페이스

vRealize Log Insight는 특정 필수 서비스, 포트 및 외부 인터페이스를 사용합니다.

vRealize Log Insight의 포트 및 프로토콜에 대한 자세한 내용은 [VMware Ports and Protocols](#)를 참조하십시오.

통신 포트

vRealize Log Insight는 이 항목에 나열된 통신 포트와 프로토콜을 사용합니다. 필수 포트는 소스, 사용자 인터페이스, 클러스터 간 또는 외부 서비스에 필요한지 여부 또는 방화벽으로 안전하게 차단될 수 있는지에 따라 구성됩니다. 일부 포트는 해당하는 통합을 사용하도록 설정하는 경우에만 사용됩니다.

참고 vRealize Log Insight에서는 WAN 클러스터링(지역적 클러스터링,고가용성 클러스터링 또는 원격 클러스터링이라고도 함)을 지원하지 않습니다. 클러스터의 모든 노드가 동일한 계층 2 LAN에 배포되어야 합니다. 또한 노드 간 통신이 원활하려면 이 섹션에 설명된 포트가 열려 있어야 합니다.

vRealize Log Insight 네트워크 트래픽에는 몇 개의 소스가 있습니다.

관리 워크스테이션

시스템 관리자가 원격으로 vRealize Log Insight 가상 장치를 관리하기 위해 사용하는 시스템입니다.

사용자 워크스테이션

vRealize Log Insight 사용자가 브라우저를 사용하여 vRealize Log Insight의 웹 인터페이스에 액세스하는 시스템입니다.

로그를 보내는 시스템

분석 및 검색을 위해 vRealize Log Insight에 로그를 보내는 끝점입니다. 예를 들어 끝점에는 ESXi 호스트, 가상 시스템 또는 IP 주소가 할당된 모든 시스템이 포함됩니다.

Log Insight Agents

Windows 또는 Linux 시스템에 있으며 API를 통해 vRealize Log Insight로 운영 체제 이벤트 및 로그를 보내는 에이전트입니다.

vRealize Log Insight 장치

vRealize Log Insight 서비스가 있는 모든 vRealize Log Insight 가상 장치, 기본 또는 작업자입니다. 장치의 기본 운영 체제는 SUSE 11 SP3입니다.

데이터를 보내는 소스에 필요한 포트

클러스터 외부에서의 연결 및 클러스터 노드 간 로드 밸런싱된 연결 둘 다에 대해 vRealize Log Insight로 데이터를 전송하는 소스의 네트워크 트래픽에 대해 다음 포트를 열어야 합니다.

소스	대상	포트	프로토콜	서비스 설명
로그를 보내는 시스템	vRealize Log Insight 장치	514	TCP, UDP	전달자 대상으로 구성되는 아웃바운드 syslog 트래픽
로그를 보내는 시스템	vRealize Log Insight 장치	1514, 6514	TCP	SSL을 통한 Syslog 데이터
vRealize Log Insight 에이전트	vRealize Log Insight 장치	9000	TCP	Log Insight 수집 API
vRealize Log Insight 에이전트	vRealize Log Insight 장치	9543	TCP	SSL을 통한 Log Insight 수집 API

사용자 인터페이스에 필요한 포트

클러스터 외부에서의 연결 및 클러스터 노드 간 로드 밸런싱된 연결 둘 다에 대해 vRealize Log Insight 사용자 인터페이스를 사용해야 하는 네트워크 트래픽에 대해 다음 포트를 열어야 합니다.

소스	대상	포트	프로토콜	서비스 설명
관리 워크스테이션	vRealize Log Insight 장치	22	TCP	SSH: 보안 셸(Secure Shell) 연결
사용자 워크스테이션	vRealize Log Insight 장치	80	TCP	HTTP: 웹 인터페이스
사용자 워크스테이션	vRealize Log Insight 장치	443	TCP	HTTPS: 웹 인터페이스

클러스터 노드 간에 필요한 포트

작업자 노드에서 네트워크에 액세스하는 경우 보안을 극대화하기 위해 다음 포트를 vRealize Log Insight 기본 노드에서만 열어야 합니다. 이러한 포트는 클러스터 노드 간에 로드 밸런싱된 소스 및 UI 트래픽에 사용되는 포트 외에 사용됩니다.

소스	대상	포트	프로토콜	서비스 설명
vRealize Log Insight 장치	vRealize Log Insight 장치	7000	TCP	Cassandra 복제 및 쿼리
vRealize Log Insight 장치	vRealize Log Insight 장치	9042	TCP	네이티브 프로토콜 클라이언트용 Cassandra 서비스
vRealize Log Insight 장치	vRealize Log Insight 장치	59778, 16520-16580	TCP	vRealize Log Insight Thrift 서비스

외부 서비스에 필요한 포트

vRealize Log Insight 클러스터 노드에서 원격 서비스로의 아웃바운드 네트워크 트래픽에 대해 다음 포트를 열어야 합니다.

소스	대상	포트	프로토콜	서비스 설명
vRealize Log Insight 장치	NTP 서버	123	UDP	NTPD: NTP 시간 동기화 제공 참고 포트는 NTP 시간 동기화를 사용하기로 선택한 경우에만 열립니다.
vRealize Log Insight 장치	메일 서버	25	TCP	SMTP: 아웃바운드 경고를 위한 메일 서비스
vRealize Log Insight 장치	메일 서버	465	TCP	SMTPS: 아웃바운드 경고를 위한 SSL을 통한 메일 서비스
vRealize Log Insight 장치	DNS 서버	53	TCP, UDP	DNS: 이름 확인 서비스

소스	대상	포트	프로토콜	서비스 설명
vRealize Log Insight 장치	AD 서버	389	TCP, UDP	Active Directory
vRealize Log Insight 장치	AD 서버	636	TCP	SSL을 통한 Active Directory
vRealize Log Insight 장치	AD 서버	3268	TCP	Active Directory 글로벌 카탈로그
vRealize Log Insight 장치	AD 서버	3269	TCP	Active Directory 글로벌 카탈로그 SSL
vRealize Log Insight 장치	AD 서버	88	TCP, UDP	Kerberos
vRealize Log Insight 장치	vCenter Server	443	TCP	vCenter Server 웹 서비스
vRealize Log Insight 장치	vRealize Operations Manager 장치	443	TCP	vRealize Operations 웹 서비스
vRealize Log Insight 장치	타사 로그 관리자	514	TCP, UDP	Syslog 데이터
vRealize Log Insight 장치	타사 로그 관리자	9000	CFAPI	전달자 대상으로 구성되는 아웃바운드 Log Insight 수집 API(CFAPI) 트래픽
vRealize Log Insight 장치	타사 로그 관리자	9543	CFAPI	암호화(SSL/TLS)를 통해 전달자 대상으로 구성되는 아웃바운드 Log Insight 수집 API(CFAPI) 트래픽

vRealize Log Insight 구성 파일

일부 구성 파일에는 vRealize Log Insight 보안에 영향을 미치는 설정이 포함되어 있습니다.

참고 루트 계정은 모든 보안 관련 리소스에 액세스할 수 있습니다. 따라서 이 계정의 보호는 vRealize Log Insight의 보안에 매우 중요합니다.

표 12-1. Log Insight 구성 파일

파일	설명
/usr/lib/loginsight/application/etc/loginsight-config-base.xml	vRealize Log Insight의 기본 시스템 구성입니다.
/storage/core/loginsight/config/loginsight-config.xml#number	vRealize Log Insight의 수정된(기본값에서) 시스템 구성입니다.
/usr/lib/loginsight/application/etc/jaas.conf	Active Directory 통합에 대한 구성입니다.

표 12-1. Log Insight 구성 파일 (계속)

파일	설명
/usr/lib/loginsight/application/etc/3rd_config/server.xml	Apache Tomcat 서버에 대한 시스템 구성입니다.
/storage/var/loginsight/apache-tomcat/conf/tomcat-users.xml	Apache Tomcat 서버에 대한 시스템 구성입니다.
/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/server.xml	Apache Tomcat 서버에 대한 시스템 구성입니다.
/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/tomcat-users.xml	Apache Tomcat 서버에 대한 사용자 정보입니다.

vRealize Log Insight 공용 키, 인증서 및 키 저장소

vRealize Log Insight의 공용 키, 인증서 및 키 저장소는 vRealize Log Insight 가상 장치에 있습니다.

참고 루트 계정은 모든 보안 관련 리소스에 액세스할 수 있습니다. 따라서 이 계정의 보호는 vRealize Log Insight의 보안에 매우 중요합니다.

- /usr/lib/loginsight/application/etc/public.cert
- /usr/lib/loginsight/application/etc/loginsight.pub
- /usr/lib/loginsight/application/etc/3rd_config/keystore
- /usr/lib/loginsight/application/etc/truststore
- /usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/keystore

vRealize Log Insight 라이선스 및 EULA 파일

EULA(최종 사용자 라이선스 계약) 및 라이선스 파일은 vRealize Log Insight 가상 장치에 있습니다.

참고 루트 계정은 모든 보안 관련 리소스에 액세스할 수 있습니다. 따라서 이 계정의 보호는 vRealize Log Insight의 보안에 매우 중요합니다.

파일	위치
라이선스	/usr/lib/loginsight/application/etc/license/loginsight_dev.dlf
라이선스	/usr/lib/loginsight/application/etc/license/loginsight_cpu.dlf
라이선스	/usr/lib/loginsight/application/etc/license/loginsight_osi.dlf
라이선스 키 파일	/usr/lib/loginsight/application/etc/license/loginsight_license.bak
최종 사용자 라이선스 계약	/usr/lib/loginsight/application/etc/license/release/eula.txt

vRealize Log Insight 로그 파일

시스템 메시지가 포함된 파일은 vRealize Log Insight 가상 장치에 있습니다.

다음 표에는 각 파일 및 해당 용도가 나와 있습니다.

이러한 파일의 로그 순환 또는 로그 아카이브에 대한 정보가 필요한 경우 "vRealize Log Insight Agent 작업"의 [vRealize Log Insight 에이전트에서 지원하는 로그 순환 체계](#) 및 "vRealize Log Insight 관리"의 [vRealize Log Insight에서 데이터 아카이브 활성화 또는 비활성화](#)를 참조하십시오.

파일	설명
/storage/var/loginsight/alert.log	트리거된 사용자 정의 경고에 대한 정보를 추적하는 데 사용됩니다.
/storage/var/loginsight/apache-tomcat/logs/*.log	Apache Tomcat 서버의 이벤트를 추적하는 데 사용됩니다.
/storage/var/loginsight/cassandra.log	Apache Cassandra에서 클러스터 구성 저장 및 복제를 추적하는 데 사용됩니다.
/storage/var/loginsight/plugins/vsphere/li-vsphere.log	vSphere Web Client와의 통합에 관련된 이벤트를 추적하는 데 사용됩니다.
/storage/var/loginsight/loginsight_daemon_stdout.log	vRealize Log Insight 대몬의 표준 출력에 사용됩니다.
/storage/var/loginsight/phonehome.log	VMware로 전송된 추적 데이터 수집(사용하도록 설정한 경우)에 대한 정보를 추적하는 데 사용됩니다.
/storage/var/loginsight/pi.log	데이터베이스 시작 또는 중지 이벤트를 추적하는 데 사용됩니다.
/storage/var/loginsight/runtime.log	vRealize Log Insight에 관련된 모든 런타임 정보를 추적하는 데 사용됩니다.
/var/log/firstboot/stratavm.log	vRealize Log Insight 가상 장치의 최초 부팅 및 구성 시 발생하는 이벤트를 추적하는 데 사용됩니다.
/storage/var/loginsight/systemalert.log	vRealize Log Insight가 보내는 시스템 알림에 대한 정보를 추적하는 데 사용됩니다. 각 경고는 JSON 항목으로 나열됩니다.
/storage/var/loginsight/systemalert_worker.log	vRealize Log Insight 작업자 노드가 보내는 시스템 알림에 대한 정보를 추적하는 데 사용됩니다. 각 경고는 JSON 항목으로 나열됩니다.
/storage/var/loginsight/ui.log	vRealize Log Insight 사용자 인터페이스에 관련된 이벤트를 추적하는 데 사용됩니다.
/storage/var/loginsight/ui_runtime.log	vRealize Log Insight 사용자 인터페이스에 관련된 런타임 이벤트를 추적하는 데 사용됩니다.
/storage/var/loginsight/upgrade.log	vRealize Log Insight 업그레이드 도중 발생하는 이벤트를 추적하는 데 사용됩니다.
/storage/var/loginsight/usage.log	모든 쿼리를 추적하는 데 사용됩니다.
/storage/var/loginsight/vcenter_operations.log	vRealize Operations Manager 통합에 관련된 이벤트를 추적하는 데 사용됩니다.
/storage/var/loginsight/watchdog_log*	어떤 이유로 종료된 경우 vRealize Log Insight의 다시 시작을 담당하는 watchdog 프로세스의 런타임 이벤트를 추적하는 데 사용됩니다.
/storage/var/loginsight/api_audit.log	Log Insight에 대한 API 호출을 추적하는 데 사용됩니다.

파일	설명
/storage/var/loginsight/ pattern_matcher.log	필드 추출에 대한 패턴 일치 시간 및 시간 초과를 추적하는 데 사용됩니다.
/storage/var/loginsight/audit.log	vRealize Log Insight가 사용된 방식을 추적하는 데 사용됩니다. 자세한 내용은 vRealize Log Insight의 감사 로그 항목을 참조하십시오 .

보안에 관련된 로그 메시지

ui_runtime.log 파일에는 사용자 감사 로그 메시지가 다음과 같은 형식으로 포함되어 있습니다.

- [2019-05-10 11:28:29.709+0000] ["https-jsse-nio-443-exec-9"/10.153.234.136
DEBUG] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User
login success: vIDM: SAM=myusername, Domain=vmware.com,
UPN=myusername@vmware.com]
- [2019-05-10 11:28:45.812+0000] ["https-jsse-nio-443-exec-3"/10.153.234.136
INFO] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User
logged out: vIDM: SAM=myusername, Domain=vmware.com,
UPN=myusername@vmware.com]
- [2019-05-10 11:28:29.709+0000] ["https-jsse-nio-443-exec-9"/10.153.234.136
DEBUG] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User
login success: Active Directory User: SAM=myusername,
Domain=vmware.com,UPN=myusername@vmware.com]
- [2019-05-10 11:28:45.812+0000] ["https-jsse-nio-443-exec-3"/10.153.234.136
INFO] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User
logged out: Active Directory User: SAM=myusername,
Domain=vmware.com,UPN=myusername@vmware.com]
- [2019-05-10 11:29:28.330+0000] ["https-jsse-nio-443-exec-6"/10.153.234.136
DEBUG] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User
login success: Local User: Name=myusername]
- [2019-05-10 11:29:47.078+0000] ["https-jsse-nio-443-exec-10"/
10.153.234.136 INFO]
[com.vmware.loginsight.web.actions.misc.LoginActionBean] [User logged out:
Local User: Name=myusername]
- [2019-05-10 11:29:23.559+0000] ["https-jsse-nio-443-exec-7"/10.153.234.136
WARN] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User login
failure: Bad username/password attempt (username: incorrectUser)]
- [2019-05-10 11:45:37.795+0000] ["https-jsse-nio-443-exec-7"/10.153.234.136
INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean]
[Created new user: Local User: Name=myusername]

- [2019-05-10 11:09:50.493+0000] ["https-jsse-nio-443-exec-6"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: vidm: SAM=myusername, Domain=vmware.com, UPN=myusername@vmware.com]
- [2019-05-10 11:47:05.202+0000] ["https-jsse-nio-443-exec-10"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new group: (directoryType= VIDM, domain=vmware.com, group=vidm_admin)]
- [2019-05-10 11:58:11.902+0000] ["https-jsse-nio-443-exec-4"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed groups: [class com.vmware.loginsight.database.dao.RBACADGroupDO<vidm/vmware.com/vidm_admin>]]

참고

- 일부 로그는 디버그 수준에서 사용할 수 있습니다. 각 노드에 디버그 수준을 사용하도록 설정하는 방법에 대한 자세한 내용은 [사용자 감사 로그 메시지에 디버그 수준 사용 설정](#)을 참조하십시오.
- vRealize Log Insight 클러스터의 각 노드에는 고유한 ui_runtime 파일이 있습니다. 노드의 로그 파일을 검토하여 클러스터를 모니터링할 수 있습니다.

사용자 감사 로그 메시지에 디버그 수준 사용 설정

사용자 감사 로그 메시지에 디버그 수준을 사용하도록 설정하여 ui_runtime 파일에 로그 메시지를 포함할 수 있습니다.

사전 요구 사항

vRealize Log Insight 가상 장치에 로그인하기 위한 루트 사용자 자격 증명을 가지고 있는지 확인합니다.

절차

- 1 /usr/lib/loginsight/application/etc/로 이동한 후 임의 텍스트 편집기에서 구성 파일 loginsight-config-base를 엽니다.
- 2 이름이 UI_RUNTIME_FILE인 appender의 경우 Threshold 매개 변수 값을 DEBUG로 업데이트합니다.

```
<appenders>
  <appender name="UI_RUNTIME_FILE"
    class="com.vmware.loginsight.log4j.SafeRollingFileAppender">
    <param name="Threshold" value="DEBUG"/>
  </appender>
</appenders>
```

3 LoginActionBean의 새 로거를 DEBUG 로그인 수준으로 추가합니다.

```
<loggers>
  <logger name="com.vmware.loginsight.web.actions.misc.LoginActionBean" level="DEBUG"
    appender="UI_RUNTIME_FILE" additivity="false"/>
</loggers>
```

4 loginsight-config-base.xml 파일을 저장한 후 닫습니다.

5 service loginsight restart 명령을 실행하여 변경 내용을 적용합니다.

vRealize Log Insight의 감사 로그

감사 로그는 vRealize Log Insight가 사용된 방식을 추적합니다.

감사 로그 파일 audit.log는 /storage/var/loginsight/에 있습니다. 이 파일은 다음 작업을 기록합니다.

범주	로깅된 작업
사용자 인증	<ul style="list-style-type: none"> 로그인, 로그아웃 및 인증 실패.
액세스 제어	<ul style="list-style-type: none"> 사용자, 그룹, 역할 및 데이터 집합 생성, 제거 및 수정.
구성	<ul style="list-style-type: none"> 전달자, vSphere 및 vRealize Operations Manager 통합 등 생성 및 제거. 세션 시간 초과, SSL, SMTP 구성 등의 구성 값 변경.
컨텐츠 팩	<ul style="list-style-type: none"> 설치, 제거 및 업그레이드. 가져오기 및 내보내기.
대시보드 및 위젯	<ul style="list-style-type: none"> 생성, 제거 및 수정. 대시보드 공유.
관리	<ul style="list-style-type: none"> 에이전트 구성 및 자동 업데이트를 사용하도록 설정. 클러스터 업그레이드. 인증서 및 라이선스 추가 및 제거.
경고	<ul style="list-style-type: none"> 생성, 제거 및 수정.
대화형 분석	<ul style="list-style-type: none"> 스냅샷 및 추출된 필드 생성, 제거 및 수정.

vRealize Log Insight 사용자 계정

vRealize Log Insight를 관리하려면 시스템 및 루트 계정을 설정해야 합니다.

vRealize Log Insight 루트 사용자

vRealize Log Insight는 현재 루트 사용자 계정을 서비스 사용자로 사용합니다. 다른 사용자는 생성되지 않습니다.

배포하는 도중에 루트 암호 속성을 설정한 경우 이외에는 기본 루트 암호는 공백입니다. vRealize Log Insight 콘솔에 처음 로그인할 때 루트 암호를 변경해야 합니다.

기본 루트 암호가 설정될 때까지 SSH는 사용하지 않도록 설정됩니다.

루트 암호는 다음 요구 사항을 충족해야 합니다.

- 8자 이상이어야 합니다.
- 최소 하나의 대문자, 하나의 소문자, 하나의 숫자 및 하나의 특수 문자를 포함해야 합니다.
- 같은 문자가 네 번 이상 반복되지 않아야 합니다.

vRealize Log Insight 관리자

vRealize Log Insight 가상 장치를 처음 시작하면 vRealize Log Insight는 웹 사용자 인터페이스용 관리자 계정을 만듭니다.

관리자의 기본 암호는 공백입니다. vRealize Log Insight의 초기 구성 도중 웹 사용자 인터페이스에서 관리 암호를 변경해야 합니다.

Active Directory 지원

vRealize Log Insight는 Active Directory와의 통합을 지원합니다. 구성된 경우 vRealize Log Insight는 Active Directory에 대해 사용자를 인증하거나 권한 부여할 수 있습니다.

[Active Directory](#)를 통해 사용자 인증 사용을 참조하십시오.

기본 사용자에게 할당되는 권한

vRealize Log Insight 서비스 사용자에게는 루트 권한이 있습니다.

웹 사용자 인터페이스 관리자는 vRealize Log Insight 웹 사용자 인터페이스에 대해서만 관리자 권한을 가집니다.

vRealize Log Insight 방화벽 권장 사항

vRealize Log Insight가 수집하는 민감한 정보를 보호하기 위해, 내부 네트워크의 나머지 부분으로부터 방화벽으로 보호되는 관리 네트워크 세그먼트에 서버를 배치하십시오.

필요한 포트

vRealize Log Insight로 데이터를 전송하는 소스의 네트워크 트래픽에 대해 다음 포트를 열어야 합니다.

포트	프로토콜
514/UDP, 514/TCP	Syslog
1514/TCP, 6514/TCP	Syslog-TLS(SSL)
9000/TCP	vRealize Log Insight 수집 API
9543/TCP	vRealize Log Insight 수집 API - TLS(SSL)

vRealize Log Insight UI를 사용해야 하는 네트워크 트래픽에 대해 다음 포트를 열어야 합니다.

포트	프로토콜
80/TCP	HTTP
443/TCP	HTTPS

다음의 포트 집합은 최대의 보안을 위해 작업자 노드로부터의 네트워크 액세스에 대해 vRealize Log Insight 기본 노드에서만 열어야 합니다.

포트	프로토콜
16520:16580/TCP	Thrift RPC
59778/TCP	log4j 서버
12543/TCP	데이터베이스 서버

보안 업데이트 및 패치

vRealize Log Insight 가상 장치는 VMware Photon 3.0을 게스트 운영 체제로 사용합니다.

vRealize Log Insight 8.0 이상은 Photon 운영 체제와 함께 제공됩니다. Photon은 vRealize Log Insight 4.8 이하 버전을 수반하는 SLES 운영 체제보다 더 안전합니다.

VMware는 유지 보수 릴리스의 보안 문제를 해결하기 위한 패치를 릴리스합니다. 이러한 패치는 [vRealize Log Insight 다운로드 페이지](#)에서 다운로드할 수 있습니다.

게스트 운영 체제에 업그레이드나 패치를 적용하기 전에 종속성을 고려하십시오. [장 6 포트 및 외부 인터페이스](#) 항목을 참조하십시오.

백업, 복원 및 재해 복구

13

많은 비용을 초래하는 데이터 센터 다운타임을 방지하려면 이러한 모범 사례에 따라 vRealize Log Insight 백업, 복원 및 재해 복구 작업을 수행하십시오.

본 장은 다음 항목을 포함합니다.

- 백업, 복원 및 재해 복구 개요
- 정적 IP 주소 및 FQDN 사용
- 계획 및 준비
- 노드 및 클러스터 백업
- Linux 또는 Windows 에이전트 백업
- 노드 및 클러스터 복원
- 복원 후 구성 변경
- 복원 확인
- 재해 복구

백업, 복원 및 재해 복구 개요

VMware는고가용성, 데이터 보호 및 재해 복구를 위한 포괄적이고 통합된 BCDR(무중단 업무 운영 및 재해 복구) 솔루션 포트폴리오를 제공합니다.

기본 노드, 작업자 노드 및 전달자를 비롯한 vRealize Log Insight 구성 요소에 대해서는 이 문서의 백업, 복원 및 재해 복구 정보를 참조하십시오.

- 구성, 로그 데이터 및 사용자 지정을 비롯한 기본 및 작업자 클러스터 멤버에 대한 자세한 내용은 [노드 및 클러스터 백업](#)를 참조하십시오.
- Linux 또는 Windows 에이전트 로컬 구성에 대한 자세한 내용은 [Linux 또는 Windows 에이전트 백업](#)를 참조하십시오.

이 문서의 정보는 다음 도구 및 제품에 적용되지 않습니다. 이러한 도구 및 제품에 대한 정보는 여러 리소스를 통해 얻어야 합니다.

- 백업, 복원 및 재해 복구에 특별히 사용되는 타사 도구. 자세한 내용은 벤더 설명서를 참조하십시오.

- vSphere Data Protection, Site Recovery Manager, Symantec NetBackup, VMware BCDR 솔루션에 대한 추가 정보는 <https://www.vmware.com/solutions/business-continuity-disaster-recovery-draas.html>을 참조하십시오.
- vRealize Log Insight와 통합되는 제품의 백업, 복원 및 재해 복구 기능.
 - vRealize Operations Manager
 - vSphere Web Client 서버
 - ESXi 호스트

정적 IP 주소 및 FQDN 사용

정적 IP 주소 및 FQDN을 사용하여 백업, 복원 및 재해 복구 작업 동안 위험을 피할 수 있습니다.

vRealize Log Insight 클러스터 노드 및 로드 밸런서의 정적 IP 주소

vRealize Log Insight 클러스터의 모든 노드에 대해 정적 IP 주소를 사용하면 IP 주소가 변경되는 경우에도 클러스터 노드의 IP 주소를 업데이트하지 않아도 됩니다.

vRealize Log Insight에는 [기술 자료 문서 2123058](#)에 설명된 대로 각 클러스터 노드 구성 파일에 있는 모든 노드 IP 주소가 포함됩니다.

vRealize Log Insight와 통합된 모든 제품(ESXi, vSphere, vRealize Operations)은 클러스터 기본 노드의 FQDN(정규화된 도메인 이름) 또는 IP 주소를 syslog 대상으로 사용합니다. 그러한 제품은 로드 밸런서(구성된 경우)의 FQDN 또는 IP 주소를 syslog 대상으로 사용할 수 있습니다. 정적 IP 주소는 여러 위치의 syslog 대상 IP 주소를 지속적으로 업데이트해야 하는 위험을 줄여줍니다.

로드 밸런서에 대한 정적 IP 주소와 선택적 가상 IP 주소를 제공합니다. 통합된 로드 밸런서를 구성하는 경우 가상 IP 주소에 대한 FQDN(선택 사항)을 제공합니다. 어떠한 이유로 IP 주소에 연결할 수 없을 때 이 FQDN이 사용됩니다.

vRealize Log Insight 클러스터 노드 및 작업자 노드의 FQDN

vRealize Log Insight 클러스터의 모든 노드에 대해 FQDN을 사용하는 경우 복구 사이트에서 동일한 FQDN을 확인할 수 있다고 가정할 때 복원 및 복구 후 구성 변경 시 시간을 절약할 수 있습니다.

기본 노드(로드 밸런서를 사용하는 경우 로드 밸런서)의 경우 완벽하게 확인 가능한 FQDN이 필요합니다. 그렇지 않을 경우 ESXi 호스트가 syslog 메시지를 vRealize Log Insight 또는 원격 대상에 제공하지 못합니다.

시스템 알림에 대해 vRealize Log Insight는 IP 주소 대신 FQDN 호스트 이름(사용할 수 있는 경우)을 사용합니다.

백업, 복원 또는 재해 복구 작업 후 기본 IP 주소만 변경된다는 것을 합리적으로 가정할 수 있습니다. FQDN을 사용하면 로그를 vRealize Log Insight 클러스터에 제공하는 모든 외부 장치에서 syslog 대상 주소(기본 노드 FQDN 또는 내부 로드 밸런서 FQDN)를 변경하지 않아도 됩니다.

vRealize Log Insight 작업자 노드의 참여 요청에서 vRealize Log Insight 기본 노드의 FQDN을 사용하는지 확인합니다.

각 노드의 구성 파일에 있는 기본 노드 호스트 값은 조인 요청을 보내는 첫 번째 작업자 노드에서 사용하는 값을 기반으로 합니다. 조인 요청에 기본 노드의 FQDN을 사용하면 재해 복구 후에 기본 노드 호스트 값을 수동으로 변경하지 않아도 됩니다. 그렇지 않을 경우 기본 노드 호스트 이름을 복원된 모든 클러스터 노드의 구성 파일에 업데이트하기 전까지 작업자 노드가 기본 노드에 다시 가입할 수 없습니다.

계획 및 준비

백업, 복원 또는 재해 복구 절차를 구현하기 전에 이 항목의 계획 및 준비 정보를 검토하십시오.

백업, 복원 및 재해 복구 계획에 다음 권장 사항이 포함되어야 합니다.

백업 작업 테스트

실제 운영 설정에서 백업, 복원 및 재해 복구 작업을 수행하기 전에 테스트 또는 스테이징 환경에서 이러한 작업의 테스트 실행을 수행합니다.

전체 vRealize Log Insight 클러스터에 대한 전체 백업을 수행합니다. 개별 파일 및 구성 백업에 자동 절차를 사용하지 마십시오.

수정 사항 확인

백업, 복원 및 재해 복구 작업을 수행하기 전에 수정 사항이 구현되고 주의 및 오류가 해결되었는지 확인합니다. 백업, 복원 및 재해 복구 도구는 일반적으로 백업, 복원 및 재해 복구 구성이 성공적으로 생성되었는지 확인할 수 있는 시각적 검증 및 단계를 제공합니다.

백업 예약

클러스터 구성에 따라 첫 번째 백업 작업은 보통 전체 백업입니다. 첫 번째 백업을 완료하는 데에는 충분한 시간을 할당해야 합니다. 이후 백업은 증분 또는 전체 백업이 될 수 있으며 첫 번째 백업 작업과 비교하여 상대적으로 빠르게 완료됩니다.

추가 설명서 및 도구

설명서에 따라 vRealize Log Insight 백업, 복원 및 재해 복구 도구의 리소스를 할당 중인지 확인합니다.

도구별 모범 사례 및 권장 사항에 따라 타사 백업, 복원 및 재해 복구 도구를 사용 중인지 확인합니다.

VMware 제품을 사용하여 배포된 가상 시스템의 경우 백업, 복원 및 재해 복구를 지원하는 특수 기능과 구성을 제공할 수 있는 추가 도구를 사용합니다.

전달자 및 클러스터

전달자의 경우, 기본 vRealize Log Insight 클러스터에 대해 백업, 복원 및 재해 복구 단계를 적용합니다.

[노드 및 클러스터 복원](#) 항목을 참조하십시오.

고객 요구 사항을 기반으로 단일 또는 여러 개의 vRealize Log Insight 전달자를 구성할 수 있습니다. 또한 전달자를 독립형 노드 또는 클러스터로 설치할 수 있습니다. 백업, 복원 및 재해 복구 작업을 위해 vRealize Log Insight 전달자는 기본 vRealize Log Insight 클러스터 노드와 동일하고 같은 방식으로 처리됩니다.

노드 및 클러스터 백업

vRealize Log Insight 노드 및 클러스터에 대해서는 예약된 백업이나 복제를 설정하는 것이 가장 좋습니다.

사전 요구 사항

- 백업 또는 복제 작업을 수행하기 전에 소스 사이트와 대상 사이트에 구성 문제가 없는지 확인합니다.
- 클러스터 리소스 할당이 최대 용량에 도달하지 않았는지 확인합니다.

적절한 수집 및 쿼리 로드와 있는 구성에서, 백업 작업과 복제 작업 중 메모리 및 스왑 사용량이 거의 100% 용량에 도달할 수 있습니다. 실제 환경에서 메모리는 최대 용량의 근사치이므로 이 메모리 스파이크의 일부는 vRealize Log Insight 클러스터 사용량에서 비롯됩니다. 또한 예약된 백업 및 복제 작업이 메모리 스파이크에 큰 영향을 줄 수 있습니다.

경우에 따라, 높은 메모리 사용량으로 인해 작업자 노드가 기본 노드에 다시 가입하기 전에 1~3분 동안 일시적으로 연결이 끊길 수 있습니다.

- 다음 중 하나 또는 둘 다 수행하여 vRealize Log Insight 노드의 메모리 임계치 조절을 줄입니다.
 - vRealize Log Insight 권장 구성 이상의 추가 메모리를 할당합니다.
 - 작업량이 많지 않은 시간에 반복 백업을 예약합니다.

절차

- 1 vRealize Log Insight 서버에 대해 사용하는 것과 동일한 절차를 사용하여 vRealize Log Insight 전달자의 정기적인 백업 또는 복제를 사용하도록 설정합니다.
- 2 백업 빈도와 백업 유형을 사용 가능한 리소스 및 고객별 요구 사항에 따라 적절히 선택했는지 확인합니다.
- 3 리소스에 문제가 없고 도구에서 지원하는 경우 동시 클러스터 노드 백업을 사용하도록 설정하여 백업 프로세스의 속도를 높입니다.
- 4 모든 노드를 동시에 백업합니다.

다음에 수행할 작업

모니터링—백업이 진행되는 동안 vRealize Log Insight 설정에 환경 또는 성능 문제가 없는지 확인합니다. 대부분의 백업, 복원 및 재해 복구 도구는 모니터링 기능을 제공합니다.

사용자 인터페이스에 표시되지 않는 문제가 있을 수 있으므로 백업 프로세스 동안 운영 시스템에 대한 모든 관련 로그를 확인합니다.

Linux 또는 Windows 에이전트 백업

서버 측에서 설치 및 구성 정보를 백업하여 에이전트를 백업합니다. 별도의 에이전트 노드 백업은 필요하지 않습니다.

에이전트는 일반적으로 일부 다른 애플리케이션 또는 서비스에도 사용되고 기존 백업 절차에도 포함될 수 있는 Linux 또는 Windows 시스템에 설치됩니다. 전체 에이전트 설치 및 해당 구성을 포함하는 시스템의 전체 파일 수준 또는 블록 수준 백업만으로도 복구에 충분합니다. 에이전트는 로컬 및 서버 제공 구성 둘 모두를 지원합니다.

에이전트가 전적으로 vRealize Log Insight 서버에서 구성되면 liagent.ini 구성 파일을 로컬에서 변경하지 않고도 에이전트 설치의 백업이 전혀 생성되지 않도록 할 수 있습니다. 대신 에이전트를 새로 설치하고 서버 백업을 가져옵니다.

에이전트에 사용자 지정 로컬 구성이 있으면 liagent.ini 파일을 백업한 후 에이전트를 새로 설치하면서 함께 복원합니다. 에이전트 노드를 에이전트 소프트웨어 설치 이상의 용도로 사용하고 이러한 노드에 대한 전체 백업이 필요한 경우에는 다른 가상 시스템과 동일한 백업 절차를 따릅니다.

에이전트 구성이 클라이언트 측(에이전트)에서 완료되고 에이전트 노드를 vRealize Log Insight 에이전트 소프트웨어의 설치에만 사용하는 경우 에이전트 구성 파일의 백업을 만드는 것만으로도 충분합니다.

사전 요구 사항

vRealize Log Insight 서버 측에 에이전트 구성이 있는지 확인합니다.

절차

- 1 liagent.ini 파일을 백업합니다.
- 2 복구된 에이전트 또는 Linux/Windows 시스템의 파일을 백업 파일로 바꿉니다.

노드 및 클러스터 복원

노드는 특정 순서로 복원해야 하며 일부 복원 시나리오에는 수동 구성 변경이 필요할 수 있습니다.

복원에 사용한 도구에 따라 가상 시스템을 동일한 호스트로 복원하거나 동일한 데이터 센터의 다른 호스트로 복원하거나 대상 원격 데이터 센터의 다른 호스트로 복원할 수 있습니다. **복원 후 구성 변경** 항목을 참조하십시오.

사전 요구 사항

- 복원된 노드의 전원이 꺼진 상태인지 확인합니다.
- 클러스터를 새 사이트에 복원하기 전에 클러스터 인스턴스의 전원이 꺼져 있는지 확인합니다.
- 동일한 IP 주소 및 FQDN을 복구 사이트에 사용하는 경우 분할 브레인 동작이 발생하지 않는지 확인합니다.
- 기본 사이트에서 부분적으로 작동하는 클러스터가 실수로 사용되고 있지는 않은지 확인합니다.

절차

- 1 작업자 노드를 복원하기 전에 우선 기본 노드를 복원합니다.
- 2 순서에 관계없이 작업자 노드를 복원합니다.
- 3 (선택 사항) 전달자를 복원합니다(구성되어 있는 경우).

전달자를 복원하기 전에 vRealize Log Insight 서버(클러스터 설정의 기본 노드 및 모든 작업자 노드)를 복원해야 합니다.

- 4 복구된 에이전트를 복원합니다.

다음에 수행할 작업

- vRealize Log Insight 클러스터를 복원할 때 동일한 IP 주소를 사용하는 경우 복원된 모든 노드의 IP 주소 및 FQDN이 원래 노드에 연결되어 있는지 확인합니다.
예를 들어 다음 시나리오는 실패합니다. 노드 A, B, C가 있는 3노드 클러스터에서, 노드 A는 IP 주소 B로, 노드 B는 IP 주소 C로, 노드 C는 IP 주소 A로 복원됩니다.
- 복원된 노드 중 일부에만 동일한 IP 주소를 사용할 경우 이러한 노드의 모든 복원된 이미지가 원래 IP 주소에 연결되어 있는지 확인합니다.
- 대부분의 백업, 복원 및 재해 복구 도구는 복원 작업 진행 중 실패 또는 경고를 확인할 수 있도록 모니터링 보기를 제공합니다. 문제점이 확인되는 경우 적절한 조치를 취합니다.
- 사이트를 완벽히 복원하기 전에 수동 구성 변경이 필요한 경우 **복원 후 구성 변경**의 지침을 따릅니다.
- 복원이 완료되면 복원된 클러스터에 대해 빠른 부분 검사를 수행합니다.

복원 후 구성 변경

백업 구성 중에 적용되는 IP 사용자 지정과 복구 대상은 필요한 수동 구성 변경을 결정합니다. 복원된 사이트를 정상적으로 작동하려면 구성 변경을 하나 이상의 vRealize Log Insight 노드에 적용해야 합니다.

동일한 호스트로 복원

vRealize Log Insight 클러스터를 동일한 호스트로 복구하는 것은 간단하며 모든 도구를 사용하여 수행할 수 있습니다.

사전 요구 사항

[계획 및 준비](#)에 관한 중요 정보를 검토합니다.

절차

- 1 복원 작업을 시작하기 전에 기존 클러스터의 전원을 끕니다. 기본적으로, 복원된 클러스터 노드에는 동일한 IP 주소와 FQDN이 사용됩니다.

2 (선택 사항) 클러스터의 새 이름을 제공합니다.

복원 프로세스 중에 가상 시스템에 새 이름을 제공하지 않으면 복원된 버전이 클러스터의 원래 사본을 덮어씁니다.

3 (선택 사항) 가능한 경우 운영 환경에 사용된 모든 네트워크, IP 및 FQDN 설정이 복원 및 복구된 사이트에 보존되었는지 확인합니다.

다음에 수행할 작업

복원 완료 및 온전성 검사 후 이전 사본을 삭제하여 리소스를 보존하고 사용자가 이전 사본의 전원을 켜는 경우 분할 브레인 상황이 발생하는 사고를 방지합니다.

다른 호스트로 복원

다른 호스트로 복원을 수행할 때 vRealize Log Insight 클러스터에서 구성 변경을 수행해야 합니다.

vRealize Log Insight 3.0 이상 릴리스에서는 장치 콘솔에서 바로 구성 파일을 변경하는 것이 공식적으로 지원되지 않습니다. 웹 UI 인터페이스를 사용하여 이러한 변경을 수행하는 방법에 대한 자세한 내용은 [기술 자료 문서 2123058](#)을 참조하십시오.

이러한 구성 변경은 모든 백업 복구 도구와 함께 사용할 수 있는 vRealize Log Insight 빌드에만 해당합니다.

다른 호스트로 복구하려면 vRealize Log Insight 클러스터 구성을 수동으로 변경해야 합니다. 백업을 생성한 소스 노드와 다른 IP 주소 및 FQDN이 복원된 vRealize Log Insight 노드에 있는 것으로 가정할 수 있습니다.

사전 요구 사항

[계획 및 준비](#)에 관한 중요 정보를 검토합니다.

절차

1 각 vRealize Log Insight 노드에 할당된 새 IP 주소와 FQDN을 모두 나열합니다.

2 기술 자료 문서 2123058에 설명된 단계를 사용하여 기본 노드에서 다음 구성을 변경합니다.

a vRealize Log Insight 구성 섹션에서 다음 행과 유사한 행을 찾습니다.

```
<distributed overwrite-children="true">
  <daemon host="prod-es-vrli1.domain.com" port="16520" token="c4c4c6a7-f85c-4f28-
a48f-43aeea27cd0e">
    <service-group name="standalone" />
  </daemon>
  <daemon host="192.168.1.73" port="16520" token="a5c65b52-
aff5-43ea-8a6d-38807ebc6167">
    <service-group name="workernode" />
  </daemon>
  <daemon host="192.168.1.74" port="16520" token="a2b57cb5-
a6ac-48ee-8e10-17134e1e462e">
    <service-group name="workernode" />
  </daemon>
</distributed>
```

코드가 3개의 노드를 표시합니다. 첫 번째 노드는 기본 노드(<service-group name=standalone> 표시)이고 나머지 두 노드는 작업자 노드(<service-group name="workernode"> 표시)입니다.

b 복구 전 환경에 사용된 DNS 항목을 복구된 환경의 기본 노드에 재사용할 수 있는지 확인합니다.

- DNS 항목을 재사용할 수 있는 경우에는 기본 노드의 새 IP 주소를 가리키도록 DNS 항목만 업데이트하면 됩니다.
- DNS 항목을 재사용할 수 없다면 기본 노드 항목을 새 DNS 이름(새 IP 주소를 가리키는 DNS 이름)으로 바꿉니다.
- DNS 이름을 할당할 수 없는 경우 마지막 방법으로 구성 항목을 새 IP 주소로 업데이트합니다.

c 작업자 노드 IP 주소도 새 IP 주소를 반영하도록 업데이트합니다.

- d 동일한 구성 파일에서 **NTP**, **SMTP**, 데이터베이스 및 **appender** 섹션을 나타내는 항목이 있는지 확인합니다.

```
<ntp>
  <ntp-servers value="ntp1.domain.com, ntp2.domain.com" />
</ntp>

<smtp>
  <server value="smtp.domain.com" />
  <default-sender value="source.domain.com@domain.com" />
</smtp>

<database>
  <password value="xserttt" />
  <host value="vrli-node1.domain.com" />
  <port value="12543" />
</database>
```

- 구성된 **NTP** 서버 값이 새 환경에서 더 이상 유효하지 않은 경우 `<ntp>...</ntp>` 섹션에서 이 값을 업데이트합니다.
 - 구성된 **SMTP** 서버 값이 새 환경에서 더 이상 유효하지 않은 경우 `<smtp>...</smtp>` 섹션에서 이 값을 업데이트합니다.
 - 필요에 따라 **SMTP** 섹션에서 `default-sender` 값을 변경합니다. 어떤 값으로든 변경할 수 있지만 이메일을 전송하는 소스를 나타내는 것이 좋습니다.
 - `<database>...</database>` 섹션에서 기본 노드 **FQDN** 또는 **IP** 주소를 가리키도록 호스트 값을 변경합니다.
- e 동일한 구성 파일에서 vRealize Log Insight ILB 구성 섹션을 업데이트합니다.

```
<load-balancer>
<leadership-lease-renewal-secs value="5" />
<high-availability-enabled value="true" />
<high-availability-ip value="10.158.128.165" />
<high-availability-fqdn value="LB-FQDN.eng.vmware.com" />
<layer4-enabled value="true" />
<ui-balancing-enabled value="true" />
</load-balancer>
```

- f `<load-balancer>...</load-balancer>` 섹션에서, `high-availability-ip` 값이 현재 설정과 다른 경우 이를 업데이트합니다.
- g 로드 밸런서의 **FQDN**도 업데이트해야 합니다.

- h [관리] 페이지의 [클러스터] 탭을 통해 웹 UI에서 다시 시작합니다. 나열된 각 노드에 대해 호스트 이름 또는 IP 주소를 선택하여 세부 정보 패널을 열고 **Log Insight 다시 시작**을 클릭합니다.

구성 변경 사항이 모든 클러스터 노드에 자동으로 적용됩니다.

- i vRealize Log Insight 서비스가 시작한 후 2분을 기다려 다른 worker 노드를 온라인으로 전환하기 전에 Cassandra 서비스가 시작할 수 있는 충분한 시간을 허용합니다.

다음에 수행할 작업

백업을 생성한 소스 노드와 다른 IP 주소 및 FQDN이 복원된 vRealize Log Insight 노드에 할당되었는지 확인합니다.


복원 확인

복원된 모든 vRealize Log Insight 클러스터가 완벽하게 작동하는지 확인해야 합니다.

사전 요구 사항

노드 구성과 클러스터 구성을 확인하기 전에 백업 및 복원 프로세스가 완료되었는지 확인합니다.

절차

- 1 ILB(내부 로드 밸런서) IP 주소 또는 FQDN(구성된 경우)을 사용하여 vRealize Log Insight에 로그인합니다.
- 2 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 3 다음을 확인합니다.
 - a 각 IP 주소 또는 FQDN을 사용하여 모든 개별 클러스터 노드에 액세스할 수 있는지 확인합니다.
 - b 클러스터 페이지에서 클러스터 노드의 상태를 확인하고 ILB(구성된 경우)도 활성 상태에 있는지 확인합니다.
 - c vSphere 통합을 확인합니다. 필요한 경우 통합을 다시 구성합니다. 복구 후에 ILB 또는 기본 노드 IP 주소 또는 FQDN이 변경된 경우 재구성이 필요합니다.
 - d vRealize Operations Manager 통합을 확인하고 필요한 경우 다시 구성합니다.
 - e 모든 콘텐츠 팩 및 UI 기능이 올바르게 작동하는지 확인합니다.
 - f vRealize Log Insight 전달자 및 에이전트가 제대로 작동하는지 확인합니다(구성된 경우).
- 4 vRealize Log Insight의 다른 주요 기능이 예상대로 작동하는지 확인합니다.

다음에 수행할 작업

백업, 복원 및 확인 작업 중 식별된 문제점을 해결하기 위해 필요에 따라 백업 및 복구 계획을 조정합니다.

재해 복구

클러스터를 작동 상태로 신속하게 되돌리려면 제대로 문서화되고 적절한 테스트를 거친 복구 계획이 필수적입니다.

재해 복구를 위해 가상 시스템을 구성할 때에는 복제 유형의 선택이 매우 중요합니다. 복제 유형을 결정할 때에는 RPO(복구 시점 목표), RTO(복구 시간 목표), 비용 및 확장성을 고려하십시오.

재해 복구 시나리오에서, 기본 사이트가 완전히 정지된 경우 동일한 사이트로 복원할 수 없는 경우가 종종 있습니다. 하지만 선택하는 옵션에 따라 vRealize Log Insight 클러스터를 완전하게 복원하여 실행 상태로 되돌리려면 몇 가지 수동 단계가 필요합니다.

vRealize Log Insight 클러스터가 완전히 정지되고 액세스할 수 없는 상태가 아니라면 클러스터를 새 사이트에 복원하기 전에 클러스터 인스턴스의 전원이 꺼졌는지 확인해야 합니다.

운영 중단 또는 재해가 발생한 경우 vRealize Log Insight 클러스터를 가급적 빨리 복구하십시오.

vRealize Log Insight 문제 해결

14

VMware 지원 서비스에 연락하기 전에 vRealize Log Insight 관리와 관련된 일반 문제를 해결할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- Internet Explorer에서 vRealize Log Insight에 로그인할 수 없음
- vRealize Log Insight의 디스크 공간 부족
- 아카이브된 데이터 가져오기가 실패할 수 있음
- 가상 장치 콘솔을 사용하여 vRealize Log Insight의 지원 번들 생성
- 관리자 암호 재설정
- 루트 사용자 암호 재설정
- 경고를 vRealize Operations Manager로 전달할 수 없음
- Active Directory 자격 증명을 사용하여 로그인할 수 없음
- STARTTLS 옵션이 활성화된 경우 SMTP가 작동하지 않음
- .pak 파일의 서명을 검증할 수 없어서 업그레이드가 실패함
- 내부 서버 오류와 함께 업그레이드 실패
- VMware 제품과 통합한 후 첫 번째 로그 메시지에서 vmw_object_id 필드가 누락됨

Internet Explorer에서 vRealize Log Insight에 로그인할 수 없음

Internet Explorer에서 vRealize Log Insight 인증이 실패합니다.

문제

vRealize Log Insight 웹 클라이언트에는 LocalStorage 또는 DOM 스토리지 지원이 필요하지만 파일 시스템 무결성 수준 때문에 Internet Explorer에서 LocalStorage를 사용할 수 없습니다. 콘솔 및 디버거는 SCRIPT5: Access is Denied 오류를 표시합니다.

원인

vRealize Log Insight에서 LocalStorage 또는 DOM 스토리지 지원에 액세스할 수 없습니다. Internet Explorer는 CachePath 매개 변수로 설정된 폴더에 이 스토리지 데이터를 보관합니다. 이 폴더는 일반적으로 %USERPROFILE%\AppData\LocalLow\Microsoft\Internet Explorer\DOMstore입니다. 이 폴더의 무결성 수준이 낮음이 아니면 Internet Explorer는 LocalStorage를 사용할 수 없습니다.

해결책

다음 명령을 사용하여 사용자 계정의 무결성 수준을 설정할 수 있습니다.

```
icaccls %userprofile%\Appdata\LocalLow /t /setintegritylevel (OI)(CI)L
```

vRealize Log Insight의 디스크 공간 부족

작은 가상 디스크를 사용하고 아카이브가 활성화되어 있지 않은 경우 vRealize Log Insight 기본 또는 작업자 노드의 디스크 공간이 부족할 수 있습니다.

문제

들어오는 로그의 비율이 분당 스토리지 공간의 3%를 초과하는 경우 vRealize Log Insight의 디스크 공간이 부족하게 됩니다.

원인

일반적인 상황에서는 매분 사용 가능한 공간이 3% 미만인지 확인하기 때문에 vRealize Log Insight의 공간이 절대 부족하지 않습니다. vRealize Log Insight 가상 장치의 사용 가능한 공간이 3% 이하로 감소하는 경우 오래된 데이터 버킷이 폐기됩니다.

그러나 디스크가 작고 로그 수집 비율이 매우 높아 사용 가능한 공간(3%)이 1분 이내로 채워지는 경우 vRealize Log Insight의 디스크 공간이 부족하게 됩니다.

아카이브가 활성화된 경우 vRealize Log Insight은 폐기하기 전에 버킷을 아카이브합니다. 오래된 버킷이 아카이브 및 폐기되기 전에 사용 가능 공간이 채워지는 경우 vRealize Log Insight의 디스크 공간이 부족하게 됩니다.

해결책

- ◆ vRealize Log Insight 가상 장치의 스토리지 용량을 늘립니다. [vRealize Log Insight 가상 장치의 스토리지 용량 늘리기](#) 항목을 참조하십시오.

아카이브된 데이터 가져오기가 실패할 수 있음

vRealize Log Insight 가상 장치의 디스크 공간이 부족하면 아카이브된 데이터 가져오기가 실패할 수 있습니다.

문제

vRealize Log Insight 리포지토리 가져오기 유틸리티는 vRealize Log Insight 가상 장치에서 사용할 수 있는 디스크 공간을 확인하지 않습니다. 따라서 가상 장치의 디스크 공간이 부족하면 아카이브된 로그 가져오기에 실패할 수 있습니다.

해결책

vRealize Log Insight 가상 장치의 스토리지 용량을 늘리고 가져오기를 다시 시작하십시오. [vRealize Log Insight 가상 장치의 스토리지 용량 늘리기](#)를 참조하십시오. 실패하기 전에 성공적으로 가져온 정보는 중복될 수 있음에 유의하십시오.

가상 장치 콘솔을 사용하여 vRealize Log Insight의 지원 번들 생성

vRealize Log Insight 웹 사용자 인터페이스에 액세스할 수 없는 경우 가상 장치 콘솔을 사용하거나 vRealize Log Insight 가상 장치에 대한 SSH 연결을 설정한 후 지원 번들을 다운로드할 수 있습니다.

사전 요구 사항

- vRealize Log Insight 가상 장치에 로그인하기 위한 루트 사용자 자격 증명을 가지고 있는지 확인합니다.
- SSH를 사용하여 vRealize Log Insight 가상 장치에 연결할 계획인 경우 TCP 포트 22가 열렸는지 확인합니다.

절차

- 1 vRealize Log Insight vApp에 대한 SSH 연결을 설정하고 루트 사용자로 로그인합니다.
- 2 지원 번들을 생성하려면 `loginsight-support`를 실행합니다.

지원 번들을 생성하고 특정 기간 내 변경된 파일만 포함하려면 `--days` 제약 조건과 함께 `loginsight-support` 명령을 실행합니다. 예를 들어 `--days=1`은 1일 내에 변경된 파일만 포함합니다.

결과

지원 정보는 `loginsight-support-YYYY-MM-DD_HHMMSS.xxxxxx.tar.gz`와 같은 이름 지정 규칙이 있는 `*.tar.gz` 파일로 수집 및 저장됩니다. 여기서 `xxxxxx`는 `loginsight-support` 프로세스를 실행한 프로세스 ID입니다.

다음에 수행할 작업

요청에 따라 지원 번들을 VMware 지원 서비스로 전달합니다.

관리자 암호 재설정

관리자가 웹 사용자 인터페이스에 대한 암호를 잊어버리는 경우 계정에 연결할 수 없게 됩니다.

사전 요구 사항

- vRealize Log Insight 가상 장치에 로그인하기 위한 루트 사용자 자격 증명을 가지고 있는지 확인합니다.
- SSH 연결을 활성화하려면 TCP 포트 22가 열려 있는지 확인합니다.

문제

vRealize Log Insight에 관리자가 한 명뿐일 때 관리자가 암호를 잊어버린 경우 애플리케이션을 관리할 수 없습니다. 관리자가 vRealize Log Insight의 유일한 사용자인 경우 전체 웹 사용자 인터페이스에 액세스할 수 없게 됩니다.

원인

사용자가 현재 암호를 기억하지 못하는 경우 vRealize Log Insight는 관리자가 자신의 암호를 재설정할 수 있는 사용자 인터페이스를 제공하지 않습니다.

참고 로그인할 수 있는 관리자는 다른 관리자의 암호를 재설정할 수 있습니다. 모든 관리자 계정의 암호를 알 수 없는 경우에만 관리자 암호를 재설정합니다.

해결책

- 1 vRealize Log Insight 가상 장치에 대한 SSH 연결을 설정하고 루트 사용자로 로그인합니다.
- 2 관리자 암호를 재설정하는 스크립트를 실행합니다.

```
li-reset-admin-passwd.sh
```

스크립트는 관리자 암호를 재설정하고 새 암호를 생성한 후 화면에 표시합니다.

다음에 수행할 작업

새 암호를 사용하여 vRealize Log Insight 웹 사용자 인터페이스에 로그인한 후 관리자 암호를 변경합니다.

루트 사용자 암호 재설정

루트 사용자의 암호를 잊어버리는 경우 더 이상 SSH 연결을 설정하거나 vRealize Log Insight 가상 장치의 콘솔을 사용할 수 없습니다.

다음은 포함하여 다양한 이유로 인해 루트로 로그인하지 못할 수 있습니다.

- 기본 암호를 변경하지 않은 경우. 기본적으로 vRealize Log Insight에서는 루트 사용자에 대해 빈 암호를 설정하며 SSH 액세스를 사용하지 않도록 설정합니다. 암호를 설정한 후에는 루트 사용자에 대해 SSH 액세스를 사용하도록 설정됩니다.
- vRealize Log Insight 가상 장치를 배포하는 동안 SSH 키를 설정한 경우. OVF를 통해 SSH 키를 지정된 경우에는 암호 인증이 사용되지 않도록 설정됩니다. 설정된 SSH 키를 사용하여 로그인하거나 아래의 해결 단계를 참조하십시오.

- 암호를 여러 번 잘못 입력하여 현재 일시적으로 잠금 상태인 경우. 이 경우에는 잠금 기간이 경과하기 전까지는 올바른 암호를 입력해도 로그인할 수 없습니다. 잠금 기간이 경과할 때까지 기다리거나 가상 장치를 다시 시작할 수 있습니다.

vRealize Log Insight 가상 장치가 Photon OS에 상주하기 때문에 다음 단계에서는 Photon OS 시스템에서 루트 암호를 재설정하는 방법을 설명합니다.

문제

SSH 연결을 설정하거나 vRealize Log Insight 가상 장치의 콘솔을 사용할 수 없는 경우 관리 작업의 일부를 완수하거나 관리자의 암호를 재설정할 수 없습니다.

해결책

- 1 Photon OS를 실행 중인 vRealize Log Insight 가상 시스템을 다시 시작합니다.
- 2 Photon OS가 다시 시작되고 시작 화면이 나타나면 즉시 문자 e를 입력하여 GNU GRUB 편집 메뉴로 이동합니다.

참고 Photon OS가 재부팅되기 때문에 e를 입력하는 데 시간이 많이 걸리지 않습니다. vSphere 및 Workstation에서 키보드 입력을 수락하기 전에 콘솔 창을 클릭하여 콘솔을 포커스 상태로 전환해야 할 수 있습니다.

- 3 GNU GRUB 편집 메뉴의 linux로 시작하는 줄 끝에 공백을 입력하고 다음 코드를 추가합니다.

```
rw init=/bin/bash
```

- 4 F10 키를 눌러 명령 프롬프트를 엽니다.

- 5 다음 명령을 실행합니다.

```
passwd
```

- 6 지시에 따라 Photon OS의 암호 복잡성 규칙을 준수하는 새 루트 암호를 입력한 후 다시 입력합니다. 암호를 기억하는지 확인하십시오.

- 7 암호가 업데이트되었다는 메시지가 표시되면 다음 명령을 실행합니다.

```
umount /
```

- 8 다음 명령을 실행합니다.

```
reboot -f
```

참고 강제 재부팅하려면 -f 옵션을 포함해야 합니다. 그렇지 않으면 커널이 패닉 상태가 됩니다.

다음에 수행할 작업

vRealize Log Insight가 재부팅된 후, 새 루트 사용자 암호로 로그인할 수 있는지 확인합니다.

경고를 vRealize Operations Manager로 전달할 수 없음

vRealize Log Insight은 경고 이벤트를 vRealize Operations Manager로 전송할 수 없는 경우 사용자에게 알립니다. vRealize Log Insight은 문제가 해결될 때까지 매 분마다 경고 전송을 재시도합니다.

문제

경고를 vRealize Operations Manager로 전달할 수 없는 경우 느낌표가 있는 빨간색 기호가 vRealize Log Insight 도구 모음에 표시됩니다.

원인

연결 문제로 인해 vRealize Operations ManagervRealize Log Insight가 경고 알림을 vRealize Operations Manager로 전송할 수 없습니다.

해결책

- ◆ 빨간색 아이콘을 클릭하여 오류 메시지 목록을 열거나 아래로 스크롤하여 최근 메시지를 봅니다.
오류 메시지 목록을 열거나 문제가 해결된 경우 빨간색 기호가 도구 모음에서 사라집니다.
- ◆ vRealize Operations Manager의 연결 문제를 수정하려면 다음을 시도합니다.
 - vRealize Operations Manager vApp이 종료되지 않았는지 확인합니다.
 - vRealize Operations Manager 웹 사용자 인터페이스의 **관리** 페이지의 **vRealize Operations Manager** 섹션에 있는 **연결 테스트** 버튼을 통해 vRealize Log Insight에 연결할 수 있는지 확인합니다.
 - vRealize Operations Manager에 직접 로그인하여 올바른 자격 증명을 가지고 있는지 확인합니다.
 - vRealize Log Insight 및 vRealize Operations Manager 로그에서 연결 문제와 관련된 메시지를 확인합니다.
 - vRealize Operations Manager vSphere 사용자 인터페이스에서 경고가 필터링되지 않음을 확인합니다.

Active Directory 자격 증명을 사용하여 로그인할 수 없음

Active Directory 자격 증명을 사용할 경우 vRealize Log Insight 웹 사용자 인터페이스에 로그인할 수 없습니다.

문제

관리자가 Active Directory 계정을 vRealize Log Insight에 추가한 경우에도 Active Directory 도메인 사용자 자격 증명을 사용하여 vRealize Log Insight에 로그인할 수 없습니다.

원인

가장 일반적인 원인은 만료된 암호, 잘못된 자격 증명, 연결 문제 또는 vRealize Log Insight 가상 장치와 Active Directory 클럭 간의 동기화 부족입니다.

해결책

- 자격 증명이 올바르고 암호가 만료되지 않았으며 Active Directory 계정이 잠기지 않았는지 확인합니다.
- Active Directory 인증에 사용할 도메인을 지정하지 않은 경우 `/storage/core/loginsight/config/loginsight-config.xml#[number]`(여기서 `[number]`는 가장 큰 숫자)에서 최신 vRealize Log Insight 구성에 저장된 기본 도메인의 계정이 있는지 확인합니다.
- 최신 구성 파일을 찾습니다. `/storage/core/loginsight/config/loginsight-config.xml#[number]`(여기서 `[number]`는 가장 큰 숫자).
- vRealize Log Insight이 Active Directory 서버에 연결할 수 있는지 확인합니다.
 - vRealize Log Insight 웹 사용자 인터페이스의 **관리** 페이지에 있는 **인증** 섹션으로 이동한 후 사용자 자격 증명을 입력하고 **연결 테스트** 버튼을 클릭합니다.
 - vRealize Log Insight/storage/var/loginsight/runtime.log에서 DNS 문제와 관련된 메시지를 확인합니다.
- vRealize Log Insight과 Active Directory 클럭이 동기화 상태인지 확인합니다.
 - vRealize Log Insight/storage/var/loginsight/runtime.log에서 클럭 왜곡과 관련된 메시지를 확인합니다.
 - NTP 서버를 사용하여 vRealize Log Insight과 Active Directory 클럭을 동기화합니다.

STARTTLS 옵션이 활성화된 경우 SMTP가 작동하지 않음

STARTTLS 옵션을 활성화한 상태로 SMTP 서버를 구성하는 경우 테스트 이메일이 실패합니다. SMTP 서버를 위한 SSL 인증서를 Java 신뢰 저장소에 추가하여 문제를 해결합니다.

사전 요구 사항

- vRealize Log Insight 가상 장치에 로그인하기 위한 루트 사용자 자격 증명을 가지고 있는지 확인합니다.
- SSH를 사용하여 vRealize Log Insight 가상 장치에 연결할 계획인 경우 TCP 포트 22가 열렸는지 확인합니다.

절차

- 1 vRealize Log Insight vApp에 대한 SSH 연결을 설정하고 루트 사용자로 로그인합니다.
- 2 SMTP 서버를 위한 SSL 인증서를 vRealize Log Insight vApp으로 복사합니다.

3 다음 명령을 실행합니다.

```
`/usr/java/jre-vmware/bin/keytool -import -alias certificate_name -file
path_to_certificate -keystore /usr/java/jre-vmware/lib/security/cacerts`
```

참고 키보드의 물결표와 동일한 키에 있는 역따옴표를 사용하여 외부 따옴표를 삽입할 수 있습니다. 작은따옴표를 사용하지 마십시오.

4 기본 암호 **changeit**을 입력합니다.

5 `service loginsight restart` 명령을 실행합니다.

다음에 수행할 작업

관리 > Smtip로 이동하고 **테스트 이메일 전송**을 사용하여 설정을 테스트합니다. [vRealize Log Insight에 대한 SMTP 서버 구성](#) 항목을 참조하십시오.

.pak 파일의 서명을 검증할 수 없어서 업그레이드가 실패함

손상된 .pak 파일, 만료된 라이선스, 부족한 디스크 공간 등으로 인해 vRealize Log Insight 업그레이드가 실패했습니다.

문제

vRealize Log Insight 업그레이드가 실패하고 다음 오류 메시지가 표시됩니다. 업그레이드가 실패했습니다. PAK 파일의 서명을 검증할 수 없어서 업그레이드가 실패함.

원인

오류가 발생하는 원인은 다음과 같습니다.

- 업로드된 파일이 .pak 파일이 아닙니다.
- 업로드된 .pak 파일이 완전하지 않습니다.
- vRealize Log Insight의 라이선스가 만료되었습니다.
- vRealize Log Insight 가상 장치 루트 파일 시스템의 디스크 공간이 부족합니다.

해결책

- ◆ .pak 파일을 업로드하고 있는지 확인합니다.
- ◆ VMware 다운로드 사이트와 비교하여 .pak 파일의 md5sum을 확인합니다.
- ◆ 하나 이상의 유효한 라이선스가 vRealize Log Insight에 구성되어 있는지 확인합니다.
- ◆ vRealize Log Insight 가상 장치에 로그인한 후 `df -h`를 실행하여 사용 가능한 디스크 공간을 확인합니다.

참고 vRealize Log Insight 가상 장치 루트 파일 시스템에 파일을 배치하지 마십시오.

내부 서버 오류와 함께 업그레이드 실패

연결 문제로 인해 vRealize Log Insight 업그레이드가 내부 서버 오류와 함께 실패합니다.

문제

vRealize Log Insight 업그레이드가 실패하고 다음 오류 메시지가 표시됩니다. 업그레이드가 실패했습니다. 내부 서버 오류.

원인

클라이언트와 서버 간에 연결 문제가 발생했습니다. 예를 들어 WAN에 위치한 클라이언트에서 업그레이드하는 경우가 있습니다.

해결책

- ◆ 서버와 동일한 LAN에서 클라이언트의 IP를 업그레이드하십시오.

VMware 제품과 통합한 후 첫 번째 로그 메시지에서 vmw_object_id 필드가 누락됨

vRealize Log Insight를 VMware 제품과 통합한 후 첫 번째 로그 메시지에 vmw_object_id 필드가 포함되지 않습니다.

문제

vRealize Log Insight를 vCenter Server 및 vRealize Operations Manager에 통합한 후에 수신하는 첫 번째 로그 메시지는 연결된 vmw_object_id 필드가 포함되지 않습니다. 누락된 필드는 vRealize Operations Manager 개체가 경고 대상으로 지정된 경우 경고 전송 메커니즘에 영향을 줄 수 있습니다.

참고 vCenter Server가 vRealize Operations Manager와 통합되었는지도 확인하십시오.

해결책

2분 동안 기다립니다. 수신하는 다음 로그 메시지는 vmw_object_id 필드가 포함됩니다.