

vRealize Automation 관리

2021년 7월 21일

vRealize Automation 7.6

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

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

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

목차

1 vRealize Automation 구성 요소와 옵션 유지 보수 및 사용자 지정	5
모든 사용자에게 메시지 브로드캐스트	5
메시지 보드 URL 허용 목록 생성	7
vRealize Automation 시작 및 종료	8
vRealize Automation 시작	8
vRealize Automation 다시 시작	9
vRealize Automation 종료	11
vRealize Automation 인증서 업데이트	11
인증서 및 개인 키 추출	13
vRealize Automation 장치에서 인증서 바꾸기	13
Infrastructure as a Service 인증서 바꾸기	16
IaaS Manager Service 인증서 바꾸기	17
vRealize Automation 인증서를 신뢰하도록 포함된 vRealize Orchestrator 업데이트	19
vRealize Automation 인증서를 신뢰하도록 외부 vRealize Orchestrator 업데이트	22
vRealize Automation 장치 관리 사이트 인증서 업데이트	22
관리 에이전트 인증서 바꾸기	26
인증서에 대한 폴링 방법 변경	29
vRealize Automation Postgres 장치 데이터베이스 관리	29
장치 데이터베이스 구성	31
3개 노드 장치 데이터베이스 자동 페일오버 시나리오	32
시나리오: 수동 장치 데이터베이스 페일오버 수행	35
시나리오: 유지 보수 데이터베이스 페일오버 수행	36
심각한 오류로부터 수동으로 장치 데이터베이스 복구	37
vRealize Automation 설치에 대한 백업 및 복구	40
고객 환경 향상 프로그램	40
vRealize Automation에 대한 고객 환경 향상 프로그램 참여 또는 탈퇴	40
데이터 수집 시간 구성	40
시스템 설정 조정	41
서비스 카탈로그에서 모든 서비스 아이콘 수정	41
데이터 롤오버 설정 사용자 지정	43
Manager Service 구성 파일의 설정 조정	45
vRealize Automation 모니터링	50
워크플로 모니터링 및 로그 보기	50
이벤트 로그 및 서비스 모니터링	50
vRealize Automation 감사 로깅 사용	52
분산 배포의 클러스터에 대한 호스트 정보 보기	54

vRealize Automation 상태 모니터링	55
vRealize Automation에 대한 시스템 테스트 구성	56
vRealize Automation에 대한 테넌트 테스트 구성	58
vRealize Orchestrator에 대한 테스트 구성	60
사용자 지정 테스트 집합	61
vRealize Automation 상태 서비스 테스트 집합 결과 보기	63
상태 서비스 문제 해결	64
SNMP를 사용하여 vRealize Automation 환경 리소스 모니터링	65
리소스 모니터링 및 관리	65
리소스 모니터링 선택 시나리오	65
리소스 사용량 용어	66
클라우드 시스템에 연결	67
소모를 통해 예약 사용률 줄이기	69
스토리지 경로 서비스 해제	70
데이터 수집	71
vCenter Server 끝점에 대한 vSwap 할당 확인 이해	74
데이터 센터 위치 제거	75
컨테이너 모니터링	75
가상 시스템 대량 가져오기, 업데이트 또는 마이그레이션	75
vRealize Automation 환경으로 가상 시스템 가져오기	76
vRealize Automation 환경에서 가상 시스템 업데이트	80
다른 vRealize Automation 환경으로 가상 시스템 마이그레이션	82

vRealize Automation 구성 요소와 옵션 유지 보수 및 사용자 지정

1

vRealize Automation 배포의 프로비저닝된 시스템 및 기타 측면을 관리할 수 있습니다.

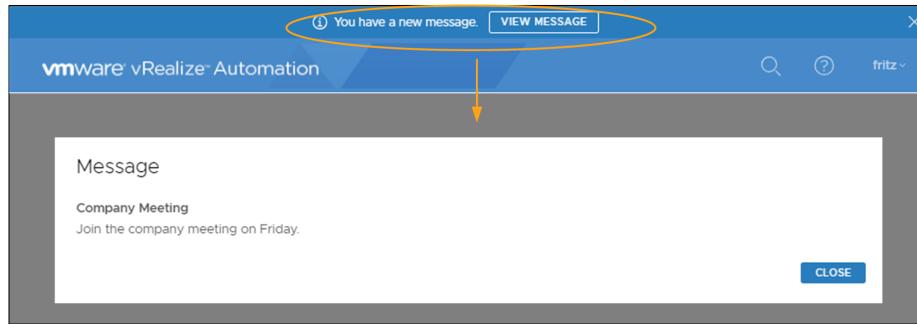
본 장은 다음 항목을 포함합니다.

- 모든 사용자에게 메시지 브로드캐스트
- vRealize Automation 시작 및 종료
- vRealize Automation 인증서 업데이트
- vRealize Automation Postgres 장치 데이터베이스 관리
- vRealize Automation 설치에 대한 백업 및 복구
- 고객 환경 향상 프로그램
- 시스템 설정 조정
- vRealize Automation 모니터링
- vRealize Automation 상태 모니터링
- SNMP를 사용하여 vRealize Automation 환경 리소스 모니터링
- 리소스 모니터링 및 관리
- 컨테이너 모니터링
- 가상 시스템 대량 가져오기, 업데이트 또는 마이그레이션

모든 사용자에게 메시지 브로드캐스트

테넌트 관리자는 모든 사용자에게 메시지를 브로드캐스트할 수 있습니다. 메시지 알림은 브라우저 페이지의 맨 위에 나타납니다. 사용자는 알림을 클릭하여 메시지를 볼 수 있습니다.

사용자는 배너에서 메시지에 액세스하거나 머리글의 사용자 드롭다운 메뉴에서 메시지에 액세스할 수 있습니다.



메시지 보드를 사용하여 텍스트 메시지 또는 웹 페이지를 브로드캐스트합니다. 웹 페이지에 따라 사용자는 메시지 보드의 웹 사이트를 탐색할 수 있습니다.

메시지 보드에는 다음과 같은 제한 사항이 있습니다.

표 1-1. 메시지 보드 제한 사항

옵션	제한 사항
URL 메시지 제한 사항	<ul style="list-style-type: none"> ■ 대상 URL을 메시지 보드 허용 목록에 포함해야 합니다. 메시지 보드 URL 허용 목록 생성 항목을 참조하십시오. ■ https 사이트에서 호스팅되는 콘텐츠를 게시하는 것만 가능합니다. ■ 자체 서명된 인증서를 사용할 수 없습니다. 인증서를 수락하는 옵션이 메시지 보드에 표시되지 않습니다. ■ 메시지 보드 URL이 iframe에 포함되어 있습니다. 일부 웹 사이트는 iframe에서 작동하지 않으며 오류가 표시됩니다. 오류의 한 가지 원인은 대상 웹 사이트의 머리글에 있는 X-Frame-Options DENY 또는 SAMEORIGIN입니다. 대상 웹 사이트가 제어 대상인 경우 X-Frame-Options 머리글을 X-Frame-Options: ALLOW-FROM https://<vRealizeAutomationApplianceURL>로 설정할 수 있습니다. ■ 일부 웹 사이트에는 전체 vRealize Automation 페이지를 새로 고칠 수 있는 최상위 페이지로의 리디렉션이 있습니다. 이 웹 사이트 유형은 메시지 보드에서 작동하지 않습니다. 새로 고침이 억제되었으며 "로드 중..." 메시지가 메시지 보드에 표시됩니다. ■ 내부 HTML 페이지를 표시하는 경우 페이지가 vRealize Automation 호스트를 URL로 포함할 수 없습니다.
사용자 지정 메시지 제한 사항	<ul style="list-style-type: none"> ■ 사용자 지정 메시지는 단순 마크업을 사용할 수 있지만 보안 유지를 위해 HTML 코드는 지원되지 않습니다. 예를 들어 <href>를 사용하여 웹 사이트에 연결할 수 없습니다. URL 메시지 옵션을 사용해야 합니다.

사전 요구 사항

테넌트 관리자로 vRealize Automation에 로그인합니다.

절차

- 1 **관리** 탭을 클릭합니다.
- 2 **알림 > 메시지 보드**를 선택합니다.
- 3 **유형** 드롭다운 메뉴에서 메시지 유형을 선택합니다.

옵션	설명
없음	메시지 알림을 제거합니다.
사용자 지정 메시지	일반 텍스트 메시지를 입력합니다.
URL	<p>페이지 URL을 입력합니다.</p> <p>URL을 메시지 보드 허용 목록에 포함해야 합니다. 메시지 보드 URL 허용 목록 생성 항목을 참조하십시오.</p> <p>사용자가 vRealize Automation 사용자 ID를 사용하여 웹 사이트(대부분의 경우 회사의 내부 웹 사이트)에 로그인하도록 하려면 사용자 ID 포함을 선택합니다. 웹 사이트에 전달되는 URL은 <code>http://company.com/internal/message?userID=richard_dawson@company.com</code>과 유사합니다. 이 방법을 사용하면 웹 사이트에서 <code>window.location.search</code> JavaScript 속성을 사용하여 현재 사용자 ID를 웹 사이트에 제공할 수 있습니다.</p>

- 4 **확인**을 클릭합니다.

결과

메시지가 배너 형태로 모든 테넌트 사용자에게 브로드캐스트됩니다.

메시지를 변경하거나 제거하려면 테넌트 관리자로 로그인해야 합니다. 메시지를 변경하려면 동일한 단계를 반복합니다. 메시지를 제거하려면 [유형]으로 [없음]을 선택하고 **확인**을 클릭합니다.

메시지 보드 URL 허용 목록 생성

보안 관리자는 메시지 보드에 사용할 수 있는 URL의 허용 목록을 구성합니다. 이러한 허용 목록은 보안을 강화합니다.

사전 요구 사항

보안 관리자로 vRealize Automation에 로그인합니다.

절차

- 1 **관리 > 메시지 보드 허용 목록**을 선택합니다.
- 2 **새로 만들기**를 클릭합니다.
- 3 URL을 추가하고 **확인**을 클릭합니다.

URL 항목에는 다음 콘텐츠가 포함될 수 있습니다.

- 사이트의 IP 주소 또는 FQDN. 예를 들어 `https://docs.vmware.com`입니다.
- `https`를 포함합니다.

- 허용되는 포트를 포함할 수 있습니다. 포트가 지정되지 않는 경우 허용되는 포트는 80 및 443입니다.

4 각 추가 항목에 대해 반복합니다.

결과

테넌트 관리자는 이 목록에 포함되어 있지 않은 URL을 메시지 보드에 추가할 수 없습니다.

다음에 수행할 작업

메시지 보드를 사용하여 허용 목록에 포함된 URL을 추가하고 브로드캐스트할 수 있는지 확인합니다. [모든 사용자에게 메시지 브로드캐스트](#) 항목을 참조하십시오.

vRealize Automation 시작 및 종료

시스템 관리자가 시스템 및 데이터 무결성을 유지하도록 vRealize Automation에 대한 제어된 종료 또는 시작을 수행합니다.

잘못된 초기 시작으로 인해 발생할 수 있는 성능 또는 제품 동작 문제를 해결하기 위해 제어된 종료 및 시작을 사용할 수도 있습니다. 배포의 일부 구성 요소가 실패하는 경우에만 다시 시작 절차를 사용하십시오.

vRealize Automation 시작

예상하거나 예상치 못한 이유로 전원이 꺼진 후 vRealize Automation을 시작하는 경우, 지정한 순서대로 구성 요소를 시작해야 합니다.

vCenter Server에서 배포 구성 요소를 관리하는 경우 여기에서 게스트 운영 체제를 시작할 수 있습니다.

사전 요구 사항

배포에서 사용하는 로드 밸런서가 실행 중인지 확인합니다.

절차

- 1 기존 독립형 PostgreSQL 데이터베이스를 사용 중인 경우 해당 서버를 시작합니다.
- 2 순서에 관계없이, 독립형 vRealize Automation MS SQL Server를 시작합니다.
- 3 상태 점검과 함께 로드 밸런서를 사용하는 배포에서 ping을 제외한 모든 상태 점검을 비활성화합니다.
- 4 기본 vRealize Automation 장치를 시작합니다.
- 5 기본 vRealize Automation 장치 관리 인터페이스에서 **클러스터** 탭을 살펴보고 시스템이 동기 또는 비동기 모드인지 확인합니다. 단일 장치 배포는 항상 비동기식입니다.
 - 배포가 동기식이면 나머지 vRealize Automation 장치를 시작합니다.
 - 배포가 비동기식이면 기본 vRealize Automation 장치 관리 인터페이스로 이동하여 라이선싱 서비스가 실행되고 등록될 때까지 기다립니다.

그런 다음 나머지 vRealize Automation 장치를 시작합니다.

- 6 모든 장치가 시작된 후 관리 인터페이스를 사용하여 서비스가 실행되고 등록되었는지 확인합니다.
장치가 시작하는 데 15분 이상 소요될 수 있습니다.
- 7 모든 IaaS 웹 노드를 시작하고 5분 동안 기다립니다.
- 8 기본 Manager Service 노드를 시작하고 2~5분을 기다립니다.
- 9 Manager Service 노드가 여러 개 있는 분산 배포에서 보조 Manager Service 노드를 시작하고 2~5분 동안 기다립니다.
보조 시스템에서, 자동 Manager Service 페일오버에 대해 구성된 경우가 아니면 Windows 서비스를 시작하거나 실행하지 마십시오.
- 10 순서에 관계없이, DEM Orchestrator, DEM 작업자 및 모든 vRealize Automation 프록시 에이전트를 시작합니다.
한 항목의 시작이 완료될 때까지 기다렸다가 다른 항목을 시작할 필요는 없습니다.
- 11 로드 밸런서 상태 점검을 비활성화해야 했다면 다시 활성화합니다.
- 12 시작된 서비스가 실행 중이고 등록되었는지 확인합니다.
 - a 브라우저에서 기본 vRealize Automation 장치 관리 인터페이스에 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
 - b **서비스** 탭을 클릭합니다.
 - c **새로 고침**을 클릭하여 서비스 시작 진행률을 모니터링합니다.

결과

모든 서비스가 등록되면 배포가 준비됩니다.

vRealize Automation 다시 시작

vRealize Automation 구성 요소를 다시 시작하면 문제 해결에 도움이 될 수 있습니다. 구성 요소는 지정된 순서대로 다시 시작해야 합니다.

vCenter Server에서 배포 구성 요소를 관리하는 경우 여기에서 게스트 운영 체제를 다시 시작할 수 있습니다.

다시 시작할 수 없는 경우 **vRealize Automation 종료** 및 **vRealize Automation 시작**의 지침을 대신 시도하십시오.

사전 요구 사항

- 배포에서 사용하는 모든 로드 밸런서가 실행 중인지 확인합니다.

절차

- 1 vRealize Automation 장치 데이터베이스가 비동기 모드로 설정되어 있는지 확인합니다. 필요한 경우 관리 인터페이스를 사용하여 비동기 모드로 변경합니다.

전체 절차를 완료한 후 동기 모드로 돌아갈 수 있습니다. 자세한 내용은 [vRealize Automation Postgres 장치 데이터베이스 관리](#)를 참조하십시오.

- 2 기본 vRealize Automation 장치를 다시 시작하고 시작이 완료될 때까지 기다립니다.
- 3 기본 vRealize Automation 장치 관리 인터페이스를 사용하여 라이선싱 서비스가 실행 중이고 등록되었는지 확인합니다.
- 4 나머지 vRealize Automation 장치를 동시에 다시 시작합니다.
- 5 장치가 다시 시작될 때까지 기다린 후 해당 관리 인터페이스를 사용하여 서비스가 실행 중이고 등록되었는지 확인합니다.
장치를 다시 시작하는 데 15분 이상 소요될 수 있습니다.
- 6 기본 웹 노드를 다시 시작하고 시작이 완료될 때까지 기다립니다.
- 7 여러 웹 노드가 있는 분산 배포를 실행 중인 경우 보조 웹 노드를 다시 시작하고 시작이 완료될 때까지 기다립니다.
- 8 Manager Service 노드를 다시 시작하고 시작이 완료될 때까지 기다립니다.

자동 Manager Service 페일오버를 실행 중이고 액티브 노드와 패시브 노드를 동일하게 유지하려는 경우 다음 순서로 다시 시작합니다.

- a 패시브 Manager Service 노드를 다시 시작하지 않고 중지합니다.
- b 액티브 Manager Service 노드를 완전하게 다시 시작합니다.
- c 패시브 Manager Service 노드를 시작합니다.

- 9 순서에 관계없이, DEM Orchestrator, DEM 작업자 및 모든 vRealize Automation 프록시 에이전트를 다시 시작합니다. 모든 시작이 완료될 때까지 기다립니다.

한 항목의 다시 시작이 완료될 때까지 기다렸다가 다른 항목을 다시 시작할 필요는 없습니다.

- 10 다시 시작된 서비스가 실행 중이고 등록되었는지 확인합니다.
 - a 브라우저에서 기본 vRealize Automation 장치 관리 인터페이스에 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
 - b **서비스** 탭을 클릭합니다.
 - c **새로 고침**을 클릭하여 서비스 시작 진행률을 모니터링합니다.

결과

모든 서비스가 등록되면 배포가 준비됩니다.

vRealize Automation 종료

데이터 무결성을 유지하려면 지정된 순서로 vRealize Automation을 종료해야 합니다.

vCenter Server에서 배포 구성 요소를 관리하는 경우 여기에서 게스트 운영 체제를 종료할 수 있습니다.

절차

- 1 순서에 관계없이, DEM Orchestrator, DEM 작업자 및 모든 vRealize Automation 프록시 에이전트를 종료합니다. 종료가 완료될 때까지 기다립니다.
- 2 Manager Service 노드를 종료하고 종료가 완료될 때까지 기다립니다.
- 3 여러 웹 노드가 있는 분산 배포에서 보조 웹 노드를 종료하고 종료가 완료될 때까지 기다립니다.
- 4 기본 웹 노드를 종료하고 종료가 완료될 때까지 기다립니다.
- 5 동기 모드의 여러 vRealize Automation 장치를 사용하는 분산 배포에서 vRealize Automation 장치 관리 인터페이스를 사용하여 비동기 모드로 변경합니다.
- 6 여러 vRealize Automation 장치를 사용하는 분산 배포에서 보조 장치를 종료하고 종료가 완료될 때까지 기다립니다.
- 7 기본 vRealize Automation 장치를 종료하고 종료가 완료될 때까지 기다립니다.
기본 vRealize Automation 장치는 기본 또는 쓰기 가능한 장치 데이터베이스를 포함하는 장치입니다. 올바른 순서로 백업을 시작할 수 있도록 어떤 장치가 기본 장치인지 기록해둡니다.
- 8 순서에 관계없이, 독립형 vRealize Automation MS SQL Server를 종료하고 종료가 완료될 때까지 기다립니다.
- 9 기존 독립형 PostgreSQL 데이터베이스를 사용 중인 경우 해당 서버를 종료합니다.

vRealize Automation 인증서 업데이트

시스템 관리자는 vRealize Automation 구성 요소에 대한 인증서를 업데이트하거나 교체할 수 있습니다.

vRealize Automation에는 서로 간의 원활한 보안 통신을 위해 SSL 인증서를 사용하는 세 가지 주요 구성 요소가 포함되어 있습니다.

- vRealize Automation 장치
- IaaS 웹 사이트 구성 요소
- IaaS Manager Service 구성 요소

또한 배포에는 vRealize Automation 장치 관리 인터페이스 웹 사이트에 대한 인증서가 포함될 수 있습니다. 이 외에도 각 IaaS 시스템은 인증서를 사용하는 관리 에이전트를 실행합니다.

참고 vRealize Automation은 Rabbit MQ와 같은 여러 타사 제품을 사용하여 다양한 기능을 지원합니다. 이러한 제품 중 일부는 기본 vRealize Automation 인증서를 CA에서 제공하는 인증서로 바꾸는 경우에도 유지되는 자체 서명된 고유 인증서를 사용합니다. 이러한 상황 때문에 사용자는 내부 통신을 위해 RabbitMQ에 사용되는 5671과 같은 특정 포트에 대한 인증서 사용을 효과적으로 제어할 수 없습니다.

한 가지 예외를 제외하고, 이 목록의 이후 구성 요소를 변경하더라도 이전 구성 요소에는 영향을 미치지 않습니다. 하지만 예외적으로 IaaS 구성 요소의 업데이트된 인증서는 vRealize Automation 장치에 등록해야 합니다.

일반적으로 자체 서명된 인증서는 제품 설치 중에 생성되어 이러한 구성 요소에 적용됩니다. 자체 서명된 인증서를 인증 기관이 제공한 인증서로 전환하기 위해 또는 인증서가 만료되었을 때 인증서를 교체해야 할 수 있습니다. vRealize Automation 구성 요소에 대한 인증서를 교체할 때 다른 vRealize Automation 구성 요소에 대한 신뢰 관계는 자동으로 업데이트됩니다.

예를 들어 vRealize Automation 장치의 여러 인스턴스가 있는 분산 시스템에서, 한 vRealize Automation 장치의 인증서를 업데이트하면 다른 관련 인증서가 자동으로 업데이트됩니다.

참고 vRealize Automation는 SHA2 인증서를 지원합니다. 시스템에 의해 생성되는 자체 서명된 인증서는 RSA 암호화가 적용된 SHA-256을 사용합니다. 운영 체제 또는 브라우저 요구 사항 때문에 SHA2 인증서로 업데이트해야 할 수 있습니다.

vRealize Automation 장치 관리 인터페이스는 인증서를 업데이트하거나 교체하는 옵션을 제공합니다.

클러스터링된 배포에서는 기본 노드 인터페이스에서 변경을 시작해야 합니다.

- **인증서 생성** — vRealize Automation에서 자체 서명된 인증서가 생성됩니다.
- **인증서 가져오기** — 사용자가 지정한 인증서를 사용합니다.
- **인증서 지문 제공** — 인증서 지문을 제공하여 IaaS Windows Server의 인증서 저장소에 이미 있는 인증서를 사용합니다.

이 옵션은 vRealize Automation 장치의 인증서를 IaaS Windows Server로 전송하지 않습니다. 이 옵션을 사용하면 vRealize Automation 장치 관리 인터페이스에서 인증서를 업로드하지 않고 IaaS Windows Server에 이미 있는 기존 인증서를 사용자가 배포할 수 있습니다.

- **기존 유지** — 현재 인증서를 계속 사용합니다.

vRealize Automation 장치 관리 인터페이스 웹 사이트의 인증서에는 등록 요구 사항이 없습니다.

참고 인증서의 암호화를 위해 암호가 사용되는 경우 장치에서 인증서를 교체할 때 암호를 입력하지 못하면, 인증서 교체가 실패하고 **Unable to load private key** 메시지가 나타납니다.

가상 시스템 템플릿

vRealize Automation 장치 또는 IaaS Windows Server 인증서를 변경한 후에는 템플릿이 vRealize Automation에서 다시 작동하도록 가상 시스템 템플릿에서 vRealize Automation 게스트 및 소프트웨어 에이전트를 업데이트해야 합니다. 에이전트를 업데이트하지 않으면 소프트웨어 구성 요소와 관련된 배포 요청이 실패하고 다음 예와 유사한 오류가 표시됩니다.

```
The following component requests failed: Linux. Request failed: Machine VM-001:
InstallSoftwareWorkflow. Install software work item timeout.
```

vRealize Orchestrator

vRealize Automation 인증서를 변경한 후에는 새 인증서를 신뢰하도록 vRealize Orchestrator를 업데이트해야 합니다.

vRealize Automation 배포에 연결된 vRealize Orchestrator 구성 요소에는 고유한 인증서가 있지만, 이러한 구성 요소도 vRealize Automation 인증서를 신뢰해야 합니다. 기본적으로 vRealize Orchestrator 구성 요소가 vRealize Automation에 내장되어 있지만 외부 vRealize Orchestrator를 사용하도록 선택하는 사용자도 있을 수 있습니다. 두 경우 모두 vRealize Orchestrator 인증서 업데이트에 대한 자세한 내용은 vRealize Orchestrator 설명서를 참조하십시오.

로드 밸런서 뒤에 다중 노드 vRealize Orchestrator 배포를 실행하는 경우 모든 vRealize Orchestrator 노드에서 동일한 인증서를 사용해야 합니다.

자세한 내용

인증서 문제 해결, 지원 가능성 및 신뢰 요구 사항에 대한 자세한 내용은 [VMware 기술 자료 문서 2106583](#)을 참조하십시오.

인증서 및 개인 키 추출

가상 장치와 함께 사용하는 인증서는 PEM 파일 형식이어야 합니다.

다음 테이블의 예는 Gnu openssl 명령을 사용하여 가상 장치를 구성하는 데 필요한 인증서 정보를 추출합니다.

표 1-2. 샘플 인증서 값 및 명령(openssl)

인증 기관 제공	명령	가상 장치 항목
RSA 개인 키	openssl pkcs12 -in <i>path_to_.pfx</i> <i>certificate_file</i> -nocerts -out key.pem	RSA 개인 키
PEM 파일	openssl pkcs12 -in <i>path_to_.pfx</i> <i>certificate_file</i> -clcerts -nokeys -out cert.pem	인증서 체인
(선택 사항) 암호	없음	암호

vRealize Automation 장치에서 인증서 바꾸기

시스템 관리자는 자체 서명된 인증서를 인증 기관의 신뢰할 수 있는 인증서로 업데이트하거나 바꿀 수 있습니다. 신뢰 요구 사항을 충족하는 한 SAN(주체 대체 이름) 인증서, 와일드카드 인증서 또는 환경에 적합한 다른 다용도 인증 방식을 사용할 수 있습니다.

vRealize Automation 장치 인증서를 업데이트하거나 바꿀 때 관련 구성 요소에 대한 신뢰가 자동으로 다시 시작됩니다. 인증서 업데이트에 대한 자세한 내용은 [vRealize Automation 인증서 업데이트](#) 항목을 참조하십시오.

절차

- 1 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

- 2 **vRA > 인증서**를 선택합니다.
- 3 인증서를 업데이트하는 vRealize Automation 구성 요소를 선택합니다.
- 4 **인증서 작업** 메뉴에서 적절한 작업을 선택합니다.

PEM 형식의 인코딩된 인증서를 사용하는 경우(예: 분산된 환경)에는 **가져오기**를 선택합니다.

가져오는 인증서는 신뢰할 수 있어야 할 뿐 아니라 **SAN**(주체 대체 이름) 인증서를 통해 vRealize Automation 장치의 모든 인스턴스와 모든 로드 밸런서에 적용 가능해야 합니다.

인증 기관에 제출할 수 있는 새 인증서 **CSR** 요청을 생성하려면 **서명 요청 생성**을 선택합니다. CA는 CSR을 통해 올바른 값을 사용하여 사용자가 가져올 수 있는 인증서를 생성할 수 있습니다.

참고 인증서 체인을 사용하는 경우 다음 순서로 인증서를 지정합니다.

- a 중간 CA 인증서에 의해 서명된 클라이언트/서버 인증서
- b 하나 이상의 중간 인증서
- c 루트 CA 인증서

옵션	작업
기존 유지	현재 SSL 구성을 그대로 둡니다. 이 옵션은 변경 사항을 취소할 때 선택합니다.
인증서 생성	<ol style="list-style-type: none"> a 일반 이름 텍스트 상자에 표시되는 값은 페이지 위쪽 부분에 나타나는 호스트 이름입니다. vRealize Automation 장치의 추가 인스턴스를 사용할 수 있는 경우 FQDN이 인증서의 SAN 특성에 포함됩니다. b 조직 이름(예: 회사 이름)을 조직 텍스트 상자에 입력합니다. c 조직 구성 단위(예: 부서 이름 또는 위치)를 조직 구성 단위 텍스트 상자에 입력합니다. d 두 글자의 ISO 3166 국가 코드(예: KO)를 국가 텍스트 상자에 입력합니다.

옵션	작업
서명 요청 생성	<ul style="list-style-type: none"> a 서명 요청 생성을 선택합니다. b 조직, 조직 구성 단위, 국가 코드 및 일반 이름 텍스트 상자의 내용을 검토합니다. 이러한 항목은 기존 인증서로부터 채워집니다. 필요한 경우 이러한 항목을 편집할 수 있습니다. c CSR 생성을 클릭하여 인증서 서명 요청을 생성한 후 생성된 CSR을 여기에 다운로드 링크를 클릭하여, 인증 기관에 보낼 수 있는 위치에 CSR을 저장하기 위한 대화상자를 엽니다. d 준비된 인증서를 받으면 가져오기를 클릭한 후 지침을 따라 인증서를 vRealize Automation에 가져옵니다.
가져오기	<ul style="list-style-type: none"> a 머리글 및 바닥글을 포함하여 BEGIN PRIVATE KEY에서 END PRIVATE KEY까지 인증서 값을 복사한 후 RSA 개인 키 텍스트 상자에 붙여 넣습니다. b 머리글 및 바닥글을 포함하여 BEGIN CERTIFICATE에서 END CERTIFICATE까지 인증서 값을 복사한 후 인증서 체인 텍스트 상자에 붙여 넣습니다. 인증서 값이 여러 개인 경우, 각 인증서에 대해 BEGIN CERTIFICATE 머리글과 END CERTIFICATE 바닥글을 포함합니다. <p>참고 체인 인증서의 경우 추가 특성이 사용 가능할 수 있습니다.</p> <ul style="list-style-type: none"> c (선택 사항) 인증서의 인증서 키가 암호를 사용하여 암호화된 경우에는 해당 암호를 복사하여 암호 텍스트 상자에 붙여 넣습니다.

5 설정 저장을 클릭합니다.

vRealize Automation 장치 인증서를 업데이트하려면 vRealize Automation 서비스가 정상적으로 다시 시작되어야 합니다. 사용자 환경의 vRealize Automation 장치 수에 따라서, 다시 시작하는 데 15분에서 1시간 정도까지 걸릴 수 있습니다.

다시 시작한 후 vRealize Automation 장치의 해당되는 모든 인스턴스에 대한 인증서 세부 정보가 페이지에 나타납니다.

6 네트워크 또는 로드 밸런서에 필요한 경우, 가져온 또는 새로 생성된 인증서를 가상 장치 로드 밸런서에 복사합니다.

인증서를 내보내려면 루트 SSH 액세스를 사용하도록 설정해야 합니다.

- a 이미 로그인되어 있지 않은 경우 vRealize Automation 장치 관리 콘솔에 root로 로그인합니다.
- b **관리** 탭을 클릭합니다.
- c **관리** 하위 메뉴를 클릭합니다.
- d **SSH 서비스 사용** 확인란을 선택합니다.
완료되었을 때 SSH를 비활성화하려면 확인란을 선택 해제합니다.
- e **관리자 SSH 로그인 사용** 확인란을 선택합니다.
완료되었을 때 SSH를 비활성화하려면 확인란을 선택 해제합니다.
- f **설정 저장**을 클릭합니다.

7 vRealize Automation 콘솔에 로그인할 수 있는지 확인합니다.

- a 브라우저를 열고 <https://vcac-hostname.domain.name/vcac/>로 이동합니다.
로드 밸런서를 사용 중인 경우 호스트 이름은 로드 밸런서의 정규화된 도메인 이름이어야 합니다.
- b 인증서 경고가 나타나는 경우 무시하고 계속합니다.
- c 디렉토리 관리를 구성할 때 지정한 암호 및 **administrator@vsphere.local**을 사용하여 로그인합니다.
콘솔의 **테넌트** 페이지에서 **관리** 탭이 열립니다. 이름이 **vsphere.local**인 테넌트 하나가 목록에 표시됩니다.

8 로드 밸런서를 사용하는 경우 해당하는 상태 점검을 구성하고 사용하도록 설정합니다.

결과

인증서가 업데이트되었습니다.

Infrastructure as a Service 인증서 바꾸기

시스템 관리자는 분산 배포 환경의 보안을 보장하기 위해 만료된 인증서 또는 자체 서명된 인증서를 인증 기관이 발급한 인증서로 바꿀 수 있습니다.

SAN(주체 대체 이름) 인증서를 여러 시스템에 사용할 수 있습니다. IaaS 구성 요소(웹 사이트 및 Manager Service)에 사용되는 인증서는 해당 구성 요소가 설치되는 모든 Windows 호스트의 FQDN을 포함하는 SAN 값 그리고 동일한 구성 요소에 대한 로드 밸런서 FQDN과 함께 발급되어야 합니다.

절차

- 1 vRealize Automation 장치 관리 인터페이스에 root로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

- 2 **vRA > 인증서**를 선택합니다.
- 3 **구성 요소 유형** 메뉴에서 **IaaS 웹**을 클릭합니다.
- 4 **IaaS 웹 인증서** 창으로 이동합니다.
- 5 **인증서 작업** 메뉴에서 인증서 교체 옵션을 선택합니다.

PEM 형식의 인코딩된 인증서를 사용하는 경우(예: 분산된 환경)에는 **가져오기**를 선택합니다.

가져오는 인증서는 신뢰할 수 있어야 할 뿐 아니라 **SAN**(주체 대체 이름) 인증서를 통해 vRealize Automation 장치의 모든 인스턴스와 모든 로드 밸런서에 적용 가능해야 합니다.

참고 인증서 체인을 사용하는 경우 다음 순서로 인증서를 지정합니다.

- a 중간 CA 인증서에 의해 서명된 클라이언트/서버 인증서
- b 하나 이상의 중간 인증서
- c 루트 CA 인증서

옵션	설명
기존 유지	현재 SSL 구성을 그대로 둡니다. 이 옵션을 선택하면 변경 내용이 취소됩니다.
인증서 생성	<ul style="list-style-type: none"> a 일반 이름 텍스트 상자에 표시되는 값은 페이지 위쪽 부분에 나타나는 호스트 이름입니다. vRealize Automation 장치의 추가 인스턴스를 사용할 수 있는 경우 FQDN이 인증서의 SAN 특성에 포함됩니다. b 조직 이름(예: 회사 이름)을 조직 텍스트 상자에 입력합니다. c 조직 구성 단위(예: 부서 이름 또는 위치)를 조직 구성 단위 텍스트 상자에 입력합니다. d 두 글자의 ISO 3166 국가 코드(예: KO)를 국가 텍스트 상자에 입력합니다.
가져오기	<ul style="list-style-type: none"> a 머리글 및 바닥글을 포함하여 BEGIN PRIVATE KEY에서 END PRIVATE KEY 까지 인증서 값을 복사한 후 RSA 개인 키 텍스트 상자에 붙여 넣습니다. b 머리글 및 바닥글을 포함하여 BEGIN CERTIFICATE에서 END CERTIFICATE까지 인증서 값을 복사한 후 인증서 체인 텍스트 상자에 붙여 넣습니다. 인증서 값이 여러 개인 경우, 각 인증서에 대해 BEGIN CERTIFICATE 머리글과 END CERTIFICATE 바닥글을 포함합니다. <p>참고 체인 인증서의 경우 추가 특성이 사용 가능할 수 있습니다.</p> <ul style="list-style-type: none"> c (선택 사항) 인증서의 인증서 키가 암호를 사용하여 암호화된 경우에는 해당 암호를 복사하여 암호 텍스트 상자에 붙여 넣습니다.
인증서 지문 제공	<p>IaaS 서버의 인증서 저장소에 이미 배포된 인증서를 사용하기 위해 인증서 지문을 제공하려면 이 옵션을 사용합니다. 이 옵션을 사용하면 가상 장치에서 IaaS 서버로 인증서가 전송되지 않습니다. 이 옵션은 사용자가 기존 인증서를 관리 인터페이스에 업로드하지 않고 IaaS 서버에 배포할 수 있도록 합니다.</p>

6 설정 저장을 클릭합니다.

IaaS Windows Server 인증서를 업데이트하려면 vRealize Automation 서비스가 정상적으로 다시 시작되어야 합니다. 사용자 환경의 vRealize Automation 장치 수에 따라서, 다시 시작하는 데 15분에서 1시간 정도까지 걸릴 수 있습니다.

다시 시작하면 인증서 세부 정보가 페이지에 표시됩니다.

IaaS Manager Service 인증서 바꾸기

시스템 관리자는 분산 배포 환경의 보안을 보장하기 위해 만료된 인증서 또는 자체 서명된 인증서를 인증 기관이 발급한 인증서로 바꿀 수 있습니다.

SAN(주체 대체 이름) 인증서를 여러 시스템에 사용할 수 있습니다. IaaS 구성 요소(웹 사이트 및 Manager Service)에 사용되는 인증서는 해당 구성 요소가 설치되는 모든 Windows 호스트의 FQDN을 포함하는 SAN 값 그리고 동일한 구성 요소에 대한 로드 밸런서 FQDN과 함께 발급되어야 합니다.

IaaS Manager Service 및 IaaS Web Service는 하나의 인증서를 공유합니다.

절차

- 1 웹 브라우저를 열고 vRealize Automation 장치 관리 인터페이스 URL로 이동합니다.
- 2 사용자 이름 **root**와 vRealize Automation 장치 배포 시 지정한 암호를 사용하여 로그인합니다.
- 3 **vRA > 인증서**를 선택합니다.
- 4 **구성 요소 유형** 메뉴에서 **Manager Service**를 클릭합니다.
- 5 **인증서 작업** 메뉴에서 인증서 유형을 선택합니다.

PEM 형식의 인코딩된 인증서를 사용하는 경우(예: 분산된 환경)에는 **가져오기**를 선택합니다.

가져오는 인증서는 신뢰할 수 있어야 할 뿐 아니라 SAN(주체 대체 이름) 인증서를 통해 vRealize Automation 장치의 모든 인스턴스와 모든 로드 밸런서에 적용 가능해야 합니다.

참고 인증서 체인을 사용하는 경우 다음 순서로 인증서를 지정합니다.

- a 중간 CA 인증서에 의해 서명된 클라이언트/서버 인증서
- b 하나 이상의 중간 인증서
- c 루트 CA 인증서

옵션	설명
기존 유지	현재 SSL 구성을 그대로 둡니다. 이 옵션을 선택하면 변경 내용이 취소됩니다.
인증서 생성	<ol style="list-style-type: none"> a 일반 이름 텍스트 상자에 표시되는 값은 페이지 위쪽 부분에 나타나는 호스트 이름입니다. vRealize Automation 장치의 추가 인스턴스를 사용할 수 있는 경우 FQDN이 인증서의 SAN 특성에 포함됩니다. b 조직 이름(예: 회사 이름)을 조직 텍스트 상자에 입력합니다. c 조직 구성 단위(예: 부서 이름 또는 위치)를 조직 구성 단위 텍스트 상자에 입력합니다. d 두 글자의 ISO 3166 국가 코드(예: KO)를 국가 텍스트 상자에 입력합니다.

옵션	설명
가져오기	<p>a 머리글 및 바닥글을 포함하여 BEGIN PRIVATE KEY에서 END PRIVATE KEY 까지 인증서 값을 복사한 후 RSA 개인 키 텍스트 상자에 붙여 넣습니다.</p> <p>b 머리글 및 바닥글을 포함하여 BEGIN CERTIFICATE에서 END CERTIFICATE까지 인증서 값을 복사한 후 인증서 체인 텍스트 상자에 붙여 넣습니다. 인증서 값이 여러 개인 경우, 각 인증서에 대해 BEGIN CERTIFICATE 머리글과 END CERTIFICATE 바닥글을 포함합니다.</p> <hr/> <p>참고 체인 인증서의 경우 추가 특성이 사용 가능할 수 있습니다.</p> <p>c (선택 사항) 인증서의 인증서 키가 암호를 사용하여 암호화된 경우에는 해당 암호를 복사하여 암호 텍스트 상자에 붙여 넣습니다.</p>
인증서 지문 제공	<p>laaS 서버의 인증서 저장소에 이미 배포된 인증서를 사용하기 위해 인증서 지문을 제공하려면 이 옵션을 사용합니다. 이 옵션을 사용하면 가상 장치에서 laaS 서버로 인증서가 전송되지 않습니다. 이 옵션은 사용자가 기존 인증서를 관리 인터페이스에 업로드하지 않고 laaS 서버에 배포할 수 있도록 합니다.</p>

6 설정 저장을 클릭합니다.

몇 분 후에 인증서 세부 정보가 페이지에 표시됩니다.

7 네트워크 또는 로드 밸런서에 필요한 경우 가져온 인증서 또는 새로 생성한 인증서를 로드 밸런서에 복사합니다.

8 DEM 작업자 또는 에이전트를 실행하는 서버에서 브라우저를 열고 <https://managerServiceAddress/vmpsProvision/>으로 이동합니다.

로드 밸런서를 사용 중인 경우 호스트 이름은 로드 밸런서의 정규화된 도메인 이름이어야 합니다.

9 인증서 경고가 나타나는 경우 무시하고 계속합니다.

10 새 인증서가 제공되었고 신뢰되는지 검증합니다.

11 로드 밸런서를 사용하는 경우 해당하는 상태 점검을 구성하고 사용하도록 설정합니다.

vRealize Automation 인증서를 신뢰하도록 포함된 vRealize Orchestrator 업데이트

vRealize Automation 장치 또는 laaS 인증서를 업데이트하거나 교체하는 경우 새 인증서 또는 업데이트된 인증서를 신뢰하도록 vRealize Orchestrator를 업데이트해야 합니다.

이 절차는 포함된 vRealize Orchestrator 인스턴스를 사용하는 모든 vRealize Automation 배포에 적용됩니다. 외부 vRealize Orchestrator 인스턴스를 사용하는 경우 [vRealize Automation 인증서를 신뢰하도록 외부 vRealize Orchestrator 업데이트](#) 항목을 참조하십시오.

참고 이 절차는 테넌트 및 그룹 인증을 다시 기본 설정으로 재설정합니다. 인증 구성을 사용자 지정한 경우 절차를 완료한 후에 인증을 다시 구성할 수 있도록 변경 내용을 기록해 두십시오.

vRealize Orchestrator 인증서 업데이트 및 교체에 대한 자세한 내용은 vRealize Orchestrator 설명서를 참조하십시오.

클러스터링된 구성에서는 기본 vRealize Automation 장치 노드에서 이 절차를 완료한 다음, 각 복제 vRealize Automation 장치 노드에서 기본 노드에 대해 `join-cluster`를 수행해야 합니다.

참고 클러스터에서 필요하지 않은 자동 제어 센터 동기화를 방지하기 위해 절차가 완료될 때까지 모든 복제 노드에서 `vco-configurator` 서비스를 중지합니다.

이 절차를 완료하지 않고 vRealize Automation 인증서를 교체 또는 업데이트하는 경우 vRealize Orchestrator 제어 센터에 액세스하지 못할 수 있으며, `vco-server` 및 `vco-configurator` 로그 파일에 오류가 표시될 수 있습니다.

vRealize Orchestrator가 vRealize Automation 이외의 다른 테넌트 및 그룹에 대해 인증하도록 구성되어 있는 경우 인증서 업데이트와 관련한 문제가 발생할 수도 있습니다. 자세한 내용은 VMware 기술 자료 문서 [예외: vRA 인증서를 교체한 후 신뢰할 수 없는 인증서 체인\(2147612\)](#)을 참조하십시오.

여기에 나와 있는 신뢰 명령 구문은 최종 구문이 아니라 대표적인 구문입니다. 대부분의 일반적인 배포에는 적합하지만 명령에 대한 변형을 실험해야 하는 상황이 있을 수 있습니다.

- `--certificate`를 지정하면 PEM 형식의 유효한 인증서 파일에 대한 경로를 제공해야 합니다.
- `--uri`를 지정하면 명령이 신뢰할 수 있는 인증서를 가져올 수 있는 URI를 제공해야 합니다.
- `--registry-certificate` 옵션을 지정하면 요청된 인증서가 구성 요소 레지스트리의 인증서로 처리되어야 하고 신뢰할 수 있는 인증서가 구성 요소 레지스트리 인증서에 사용되는 특정 별칭으로 신뢰 저장소에 추가되어야 함을 나타냅니다.

vRealize Orchestrator에서 SSL 신뢰 관리자 워크플로 사용하여 인증서를 관리할 수도 있습니다. 자세한 내용은 [vRealize Orchestrator 설명서](#)에서 "Orchestrator 인증서 관리"를 참조하십시오.

절차

- 1 vRealize Orchestrator 서버와 제어 센터 서비스를 중지합니다.

```
service vco-server stop
service vco-configurator stop
```

- 2 다음 명령을 실행하여 vRealize Orchestrator 인증 제공자를 재설정합니다.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
ls -l /etc/vco/app-server/
mv /etc/vco/app-server/vco-registration-id /etc/vco/app-server/vco-registration-id.old
vcac-vami vco-service-reconfigure
```

- 3 다음 명령과 함께 `/var/lib/vco/tools/configuration-cli/bin`에 있는 명령줄 인터페이스 유틸리티를 사용하여 vRealize Orchestrator 신뢰 저장소에 대한 신뢰할 수 있는 인증서를 확인합니다.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

- 다음 별칭이 있는 인증서를 확인합니다. `vco.cafe.component-registry.ssl.certificate`. 이 인증서는 vRealize Orchestrator 인스턴스가 인증 제공자로 사용하는 vRealize Automation 인증서여야 합니다.

- 이 인증서는 새로 구성된 vRealize Automation 인증서와 일치해야 합니다. 일치하지 않는 경우 다음과 같이 변경할 수 있습니다.

- 1 vRealize Automation 서명된 장치 인증서 PEM 파일을 장치의 /tmp 폴더에 복사합니다.
- 2 다음 명령을 실행하여 적절한 인증서 경로를 추가합니다.

```
./vro-configure.sh trust --certificate path-to-the-certificate-file-in-PEM-format--registry-certificate
```

다음 명령 예시를 참조하십시오.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --certificate /var/tmp/test.pem --registry-certificate
```

- 4 인증서를 신뢰하기 위해 다음 명령을 실행해야 할 수도 있습니다.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --uri https://vra.domain.com  
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --registry-certificate --uri https://vra.domain.com
```

- 5 다음 명령을 사용하여 vRealize Automation 인증서가 vRealize Orchestrator 신뢰 저장소에 주입되었는지 확인합니다.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

- 6 vRealize Orchestrator 서버와 제어 센터 서비스를 시작합니다.

```
service vco-server start  
service vco-configurator start
```

다음에 수행할 작업

클러스터링된 시스템에서 신뢰가 업데이트 되었는지 확인할 수 있습니다.

- 1 가상 장치 관리 인터페이스에 root로 로그인합니다.
- 2 [서비스] 페이지를 선택합니다.
- 3 중복된 vco 서비스가 나열되지 않아야 합니다.
vco 서비스의 중복이 표시되면 **등록 취소**를 클릭하여 **Registered** 상태가 아닌 서비스를 제거합니다.
- 4 모든 가상 장치 노드에서 vco-configurator가 시작되었는지 확인합니다.
- 5 vRealize Orchestrator 제어 센터에 로그인하고 [구성 검증] 페이지로 이동하여 구성을 검증합니다.
- 6 [인증 제공자] 페이지로 이동하여 인증 설정이 올바른지 확인합니다.
이 페이지에서 로그인 자격 증명을 테스트할 수도 있습니다.

vRealize Automation 인증서를 신뢰하도록 외부 vRealize Orchestrator 업데이트

vRealize Automation 장치 또는 IaaS 인증서를 업데이트하거나 교체하는 경우 새 인증서 또는 업데이트된 인증서를 신뢰하도록 vRealize Orchestrator를 업데이트해야 합니다.

이 절차는 외부 vRealize Orchestrator 인스턴스를 사용하는 vRealize Automation 배포에 적용됩니다.

참고 이 절차는 테넌트 및 그룹 인증을 다시 기본 설정으로 재설정합니다. 인증 구성을 사용자 지정한 경우 절차를 완료한 후에 인증을 다시 구성할 수 있도록 변경 내용을 기록해 두십시오.

vRealize Orchestrator 인증서 업데이트 및 교체에 대한 자세한 내용은 vRealize Orchestrator 설명서를 참조하십시오.

이 절차를 완료하지 않고 vRealize Automation 인증서를 교체 또는 업데이트하는 경우 vRealize Orchestrator 제어 센터에 액세스하지 못할 수 있으며, vco-server 및 vco-configurator 로그 파일에 오류가 표시될 수 있습니다.

vRealize Orchestrator가 vRealize Automation 이외의 다른 테넌트 및 그룹에 대해 인증하도록 구성되어 있는 경우 인증서 업데이트와 관련한 문제가 발생할 수도 있습니다. [기술 자료 문서 2147612](#)를 참조하십시오.

절차

- 1 vRealize Orchestrator 서버와 제어 센터 서비스를 중지합니다.

```
service vco-configurator stop
```

- 2 vRealize Orchestrator 인증 제공자를 재설정합니다.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
```

- 3 vRealize Orchestrator 제어 센터 서비스를 시작합니다.

```
service vco-configurator start
```

- 4 가상 장치 관리 인터페이스 루트 자격 증명을 사용하여 제어 센터에 로그인합니다.

- 5 인증 제공자를 등록 취소한 다음 다시 등록합니다.

vRealize Automation 장치 관리 사이트 인증서 업데이트

시스템 관리자는 관리 사이트 서비스의 SSL 인증서가 만료되었을 경우 또는 자체 서명된 인증서를 인증 기관이 발행한 인증서로 교체하려는 경우 관리 사이트 서비스의 SSL 인증서를 교체할 수 있습니다. 관리 사이트 서비스는 포트 5480에서 보호할 수 있습니다.

vRealize Automation 장치는 lighttpd를 사용하여 고유한 관리 사이트를 실행합니다. 관리 사이트 인증서를 교체할 때는 모든 관리 에이전트가 새 인증서를 인식하도록 구성해야 합니다.

분산 배포를 실행 중인 경우 관리 에이전트를 자동으로 업데이트하거나 수동으로 업데이트할 수 있습니다. 최소 배포를 실행 중인 경우 관리 에이전트를 수동으로 업데이트해야 합니다.

자세한 내용은 수동으로 관리 에이전트 인증서 인식 업데이트 를 참조하십시오.

절차

1 관리 에이전트 식별자 찾기

새 관리 사이트 서버 인증서를 생성하고 등록할 때 관리 에이전트 식별자를 사용합니다.

2 vRealize Automation 장치 관리 사이트 인증서 바꾸기

관리 사이트 서비스의 SSL 인증서가 만료되었거나 자체 서명된 인증서로 시작했으며 사이트 정책에 따라 다른 인증서가 필요한 경우 해당 인증서를 바꿀 수 있습니다.

3 관리 에이전트 인증서 인식 업데이트

vRealize Automation 장치 관리 사이트 인증서를 교체한 후에는 새 인증서를 인식하고 가상 장치 관리 사이트와 IaaS 호스트의 관리 에이전트 사이에 신뢰할 수 있는 통신을 다시 설정하도록 모든 관리 에이전트를 업데이트해야 합니다.

관리 에이전트 식별자 찾기

새 관리 사이트 서버 인증서를 생성하고 등록할 때 관리 에이전트 식별자를 사용합니다.

절차

- 1 `<vra-installation-dir>\Management Agent\VMware.IaaS.Management.Agent.exe.config`에 위치한 관리 에이전트 구성 파일을 엽니다.

- 2 agentConfiguration 요소의 ID 특성 값을 기록합니다.

```
<agentConfiguration id="0E22046B-9D71-4A2B-BB5D-70817F901B27">
```

vRealize Automation 장치 관리 사이트 인증서 바꾸기

관리 사이트 서비스의 SSL 인증서가 만료되었거나 자체 서명된 인증서로 시작했으며 사이트 정책에 따라 다른 인증서가 필요한 경우 해당 인증서를 바꿀 수 있습니다.

포트 443에서 vRealize Automation 서비스에 사용되는 인증서를 재사용하거나 다른 인증서를 사용할 수 있습니다. 기존 인증서를 업데이트하기 위한 새 CA 발급 인증서를 요청하는 경우 기존 인증서의 일반 이름을 재사용하는 것이 가장 좋습니다.

참고 vRealize Automation 장치는 lighttpd를 사용하여 고유한 관리 사이트를 실행합니다. 관리 사이트 서비스는 포트 5480에서 보호할 수 있습니다.

사전 요구 사항

- 인증서는 PEM 형식이어야 합니다.
- 인증서는 다음 항목을 둘 다 순서대로 함께 한 파일에 포함해야 합니다.
 - a RSA 개인 키
 - b 인증서 체인
- 개인 키는 암호화할 수 없습니다.

- 기본 위치 및 파일 이름은 `/opt/vmware/etc/lighttpd/server.pem`입니다.

Java keystore에서 인증서와 개인 키를 PEM 파일에 내보내기에 대한 자세한 내용은 [인증서 및 개인 키 추출](#) 항목을 참조하십시오.

절차

- 1 장치 콘솔 또는 SSH를 사용하여 로그인합니다.
- 2 현재 인증서 파일을 백업합니다.

```
cp /opt/vmware/etc/lighttpd/server.pem /opt/vmware/etc/lighttpd/server.pem-bak
```

- 3 파일 `/opt/vmware/etc/lighttpd/server.pem`의 콘텐츠를 새 인증서 정보로 교체하여 장치에 새 인증서를 복사합니다.

- 4 다음 명령을 실행하여 lighttpd 서버를 다시 시작합니다.

```
service vami-lighttpd restart
```

- 5 다음 명령을 실행하여 haproxy 서비스를 다시 시작합니다.

```
service haproxy restart
```

- 6 관리 콘솔에 로그인하고 인증서가 교체되었는지 확인합니다. 브라우저를 다시 시작해야 할 수 있습니다.

다음에 수행할 작업

새 인증서를 인식하도록 모든 관리 에이전트를 업데이트합니다.

분산 배포 환경의 경우 관리 에이전트를 수동 또는 자동으로 업데이트할 수 있습니다. 최소 설치의 경우 에이전트를 수동으로 업데이트해야 합니다.

- 자동 업데이트에 대한 자세한 내용은 [vRealize Automation 장치 관리 사이트 인증서를 인식하도록 분산 환경에서 관리 에이전트를 자동으로 업데이트](#) 항목을 참조하십시오.
- 수동 업데이트에 대한 자세한 내용은 [수동으로 관리 에이전트 인증서 인식 업데이트](#) 항목을 참조하십시오.

관리 에이전트 인증서 인식 업데이트

vRealize Automation 장치 관리 사이트 인증서를 교체한 후에는 새 인증서를 인식하고 가상 장치 관리 사이트와 IaaS 호스트의 관리 에이전트 사이에 신뢰할 수 있는 통신을 다시 설정하도록 모든 관리 에이전트를 업데이트해야 합니다.

각 IaaS 호스트에서 관리 에이전트가 실행되며, 각 관리 에이전트를 업데이트해야 합니다. 최소 배포는 수동으로 업데이트해야 하지만 분산 배포는 수동으로 업데이트하거나 자동화 프로세스를 사용하여 업데이트할 수 있습니다.

■ 수동으로 관리 에이전트 인증서 인식 업데이트

vRealize Automation 장치 관리 사이트 인증서를 교체한 후에는 새 인증서를 인식하고 가상 장치 관리 사이트와 IaaS 호스트의 관리 에이전트 사이에 신뢰할 수 있는 통신을 다시 설정하도록 관리 에이전트를 수동으로 업데이트해야 합니다.

■ vRealize Automation 장치 관리 사이트 인증서를 인식하도록 분산 환경에서 관리 에이전트를 자동으로 업데이트

고가용성 배포에서 관리 사이트 인증서를 업그레이드한 후에는 새 인증서를 인식하고 신뢰할 수 있는 통신을 다시 설정하도록 관리 에이전트 구성도 업데이트해야 합니다.

수동으로 관리 에이전트 인증서 인식 업데이트

vRealize Automation 장치 관리 사이트 인증서를 교체한 후에는 새 인증서를 인식하고 가상 장치 관리 사이트와 IaaS 호스트의 관리 에이전트 사이에 신뢰할 수 있는 통신을 다시 설정하도록 관리 에이전트를 수동으로 업데이트해야 합니다.

vRealize Automation 장치 관리 사이트에 대한 인증서를 교체한 후 배포 환경의 각 관리 에이전트에 대해 이 단계를 수행하십시오.

분산 배포 환경의 경우 관리 에이전트를 수동 또는 자동으로 업데이트할 수 있습니다. 자동 업데이트에 대한 자세한 내용은 [vRealize Automation 장치 관리 사이트 인증서를 인식하도록 분산 환경에서 관리 에이전트를 자동으로 업데이트](#) 항목을 참조하십시오.

사전 요구 사항

새 vRealize Automation 장치 관리 사이트 인증서의 SHA1 지문을 가져옵니다.

절차

- 1 VMware vCloud Automation Center Management Agent 서비스를 중지합니다.
- 2 `[vcac_installation_folder]\Management Agent\VMware.IaaS.Management.Agent.exe.Config`에 있는 관리 에이전트 구성 파일(일반적으로 `C:\Program Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`)로 이동합니다.
- 3 파일을 편집용으로 열고 이전 관리 사이트 인증서에 대한 끝점 구성 설정을 찾습니다. 이 설정은 끝점 주소를 통해 식별할 수 있습니다.

예:

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
```

```
<endpoint address="https://vra-vd.local:5480"
thumbprint="D1542471C30A9CE694A512C5F0F19E45E6FA32E6" />
</managementEndpoints>
</agentConfiguration>
```

- 4 지문을 새 인증서의 SHA1 지문으로 변경합니다.

예:

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
<managementEndpoints>
<endpoint address="https://vra-vd.local:5480"
thumbprint="8598B073359BAE7597F04D988AD2F083259F1201" />
</managementEndpoints>
</agentConfiguration>
```

- 5 VMware vCloud Automation Center Management Agent 서비스를 시작합니다.
- 6 가상 장치 관리 사이트에 로그인하고 **클러스터** 탭을 선택합니다.
- 7 분산 배포 정보 테이블에서 IaaS 서버가 최근 가상 장치에 연결했는지 확인합니다. 연결을 했으면 업데이트가 성공한 것입니다.

vRealize Automation 장치 관리 사이트 인증서를 인식하도록 분산 환경에서 관리 에이전트를 자동으로 업데이트

고가용성 배포에서 관리 사이트 인증서를 업그레이드한 후에는 새 인증서를 인식하고 신뢰할 수 있는 통신을 다시 설정하도록 관리 에이전트 구성도 업데이트해야 합니다.

분산 시스템에 대한 vRealize Automation 장치 관리 사이트 인증서를 수동 또는 자동으로 업데이트할 수 있습니다. 관리 에이전트 수동 업데이트에 대한 자세한 내용은 [수동으로 관리 에이전트 인증서 인식 업데이트](#) 항목을 참조하십시오.

인증서 정보를 자동으로 업데이트하려면 다음 절차를 사용하십시오.

절차

- 1 관리 에이전트가 실행 중일 때 배포에서 단일 vRealize Automation 장치 관리 사이트의 인증서를 교체합니다.
- 2 관리 에이전트가 새 vRealize Automation 장치 관리 사이트 인증서와 동기화될 때까지 15분 동안 기다립니다.
- 3 배포에서 다른 vRealize Automation 장치 관리 사이트의 인증서를 교체합니다.

관리 에이전트가 자동으로 새 인증서 정보로 업데이트됩니다.

관리 에이전트 인증서 바꾸기

시스템 관리자는 관리 에이전트 인증서가 만료되었을 때 해당 인증서를 바꾸거나, 자체 서명된 인증서를 인증 기관이 발급한 인증서로 바꿀 수 있습니다.

IaaS 호스트마다 고유한 관리 에이전트를 실행합니다. 관리 에이전트를 업데이트하려는 IaaS 노드 각각에 대해 이 절차를 반복합니다.

사전 요구 사항

- 레코드를 제거하기 전에 [노드 ID] 열에 있는 관리 에이전트 식별자를 복사합니다. 이 식별자는 새 관리 에이전트 인증서를 생성할 때와 인증서를 등록할 때 사용해야 합니다.
- 새 인증서를 요청할 때는 새 인증서의 인증서 제목 필드에 CN(일반 이름) 특성을 다음과 같은 형식으로 입력해야 합니다.

```
VMware Management Agent 00000000-0000-0000-0000-000000000000
```

VMware Management Agent라는 문자열 다음에 공백 하나를 입력하고, 그 다음에 관리 에이전트의 GUID를 위와 같은 숫자 형식으로 입력해야 합니다.

절차

- 1 Windows 서비스 스냅인에서 관리 에이전트 서비스를 중지합니다.
 - a Windows 시스템에서 **시작**을 클릭합니다.
 - b Windows 시작 메뉴의 검색 상자에 **services.msc**를 입력하고 Enter 키를 누릅니다.
 - c **VMware vCloud Automation Center Management Agent** 서비스를 마우스 오른쪽 버튼으로 클릭하고 **중지**를 클릭하여 서비스를 중지합니다.
- 2 현재 인증서를 시스템에서 제거합니다. Windows Server 2008 R2에서 인증서를 관리하는 데 대한 자세한 내용은 Microsoft 기술 자료 문서(<http://technet.microsoft.com/en-us/library/cc772354.aspx>) 또는 Microsoft 위키 문서(<http://social.technet.microsoft.com/wiki/contents/articles/2167.how-to-use-the-certificates-console.aspx>)를 참조하십시오.
 - a **mmc.exe** 명령을 입력하여 Microsoft 관리 콘솔을 엽니다.
 - b Ctrl + M 키를 눌러 콘솔에 새 스냅인을 추가하거나 [파일] 드롭다운 메뉴에서 옵션을 선택합니다.
 - c **인증서**를 선택하고 **추가**를 클릭합니다.
 - d **컴퓨터 계정**을 선택하고 **다음**을 클릭합니다.
 - e **로컬 컴퓨터: (이 콘솔을 실행 중인 컴퓨터)**를 선택합니다.
 - f **확인**을 클릭합니다.
 - g 콘솔 왼쪽에서 **인증서(로컬 컴퓨터)**를 확장합니다.
 - h **개인**을 확장하고 Certificates 폴더를 선택합니다.
 - i 현재 관리 에이전트 인증서를 선택하고 **삭제**를 클릭합니다.
 - j 삭제 작업을 확인하려면 **예**를 클릭합니다.
- 3 새로 생성된 인증서를 로컬 **computer.personal** 저장소에 가져오거나, 시스템에서 새로운 자체 서명 인증서를 자동으로 생성하게 하려면 아무 것도 가져오지 않습니다.

4 vRealize Automation 장치 관리 사이트에 관리 에이전트 인증서를 등록합니다.

- a 관리자 권한으로 명령 프롬프트를 열고, 관리 에이전트가 설치되어 있는 시스템의 Cafe 디렉토리인 `<vra-installation-dir>\Management Agent\Tools\Cafe`(일반적으로 `C:\Program Files (x86)\VMware\vCAC\Management Agent\Tools\Cafe`)로 이동합니다.
- b `Vcac-Config.exe RegisterNode` 명령을 옵션과 함께 입력하여 관리 에이전트 식별자와 인증서를 하나의 단계로 등록합니다. 앞에서 기록한 관리 에이전트 식별자를 `-nd` 옵션에 대한 값으로 포함합니다.

표 1-3. Vcac-Config.exe RegisterNode의 필수 옵션 및 인수

[illegible]

다음 예에서는 명령 형식을 보여 줍니다.

```
Vcac-Config.exe RegisterNode -v -vamih "vra-vr-hostname.domain.name:5480"  
-cu "root" -cp "password" -hn "machine-hostname.domain.name"  
-nd "00000000-0000-0000-0000-000000000000"  
-tp "000000000000000000000000000000000000000000000000"
```

5 관리 에이전트를 다시 시작합니다.

예제: 관리 에이전트 인증서를 등록하는 명령

```
Vcac-Config.exe RegisterNode -v -vamih "vra-va.eng.mycompany:5480" -cu "root" -cp "secret" -hn "iaas.eng.mycompany" -nd "C816CFBX-4830-4FD2-8951-C17429CEA291" -tp "70928851D5B72B206E4B1CF9F6ED953EE1103DED"
```

인증서에 대한 폴링 방법 변경

IaaS 인증서의 OU 섹션에 쉼표가 있는 경우 Manager Service 로그 파일에 STOMP WebSocket 오류가 발생할 수 있습니다. 또한 가상 시스템 프로비저닝이 실패할 수 있습니다. 쉼표를 제거하거나 폴링 방법을 WebSocket에서 HTTP로 변경할 수 있습니다.

폴링 방법을 변경하려면 다음 단계를 수행합니다.

절차

- 1 텍스트 편집기에서 다음 파일을 엽니다.

C:\Program Files (x86)\VMware\VCAC\Server\Manager Service.exe.config.

- 2 <appSettings> 섹션 내부에 다음 줄을 추가합니다.

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```

- 3 Manager Service.exe.config를 저장하고 닫습니다.

- 4 Manager Service를 다시 시작합니다.

결과

Manager Service에 대한 자세한 내용은 "vRealize Automation 설치" 항목을 참조하십시오.

vRealize Automation Postgres 장치 데이터베이스 관리

vRealize Automation에는 시스템 작업을 위한 장치 데이터베이스가 필요합니다. vRealize Automation Appliance 가상 장치 관리 인터페이스를 통해 장치 데이터베이스를 관리할 수 있습니다.

참고 이 정보는 포함된 장치 데이터베이스를 사용하는 배포에만 적용됩니다. 외부 Postgres 데이터베이스를 사용하는 배포에는 적용되지 않습니다.

데이터베이스를 단일 노드로 구성하거나 페일오버를 통해 고가용성을 원활하게 지원하기 위해 여러 노드로 구성할 수 있습니다. vRealize Automation 설치 관리자는 각 vRealize Automation 장치 설치에 하나의 데이터베이스 노드를 포함시킵니다. 따라서 vRealize Automation 장치 인스턴스를 3개 설치할 경우에는 데이터베이스 노드가 3개입니다. 적용 가능한 배포에 자동 페일오버가 구현됩니다. 시스템 구성이 변경되지 않는 한 또는 클러스터링된 구성을 사용하는 경우 다른 노드를 기본 노드로 승격하는 경우 이외에는 장치 데이터베이스를 유지 보수할 필요가 없습니다.

참고 데이터베이스 클러스터링 구성은 [클러스터에 가입] 작업을 사용하여 가상 장치를 클러스터에 가입시킬 때 자동으로 설정됩니다. 데이터베이스 클러스터가 가상 장치 클러스터에 직접적으로 종속되는 것은 아닙니다. 예를 들어 포함된 장치 데이터베이스가 시작되지 않거나 실패한 경우에도 클러스터에 가입된 가상 시스템이 정상적으로 작동할 수 있습니다.

고가용성의 경우 vRealize Automation은 PostgreSQLprimary-replica 모델을 사용하여 데이터 복제를 지원합니다. 따라서 모든 데이터베이스 노드는 기본 노드라고 하는 하나의 선행 노드와 복제라고 하는 여러 복제 노드가 포함된 클러스터에서 작동합니다. 기본 노드는 모든 데이터베이스 요청을 처리하고 복제 노드는 로컬에서 기본 노드의 트랜잭션을 스트리밍하고 재생합니다.

클러스터링된 구성에는 하나의 기본 노드와 하나 이상의 복제 노드가 포함됩니다. 기본 노드는 시스템 기능을 지원하는 기본 데이터베이스가 있는 vRealize Automation 장치 노드입니다. 복제 노드에는 기본 노드에 장애가 발생할 경우 서비스로 끌어올 수 있는 데이터베이스의 복사본이 포함됩니다.

고가용성 장치 데이터베이스 옵션에는 몇 가지가 있습니다. 가장 중요한 데이터베이스 구성 옵션은 복제 모드를 선택하는 것입니다. 복제 모드는 vRealize Automation 배포에서 데이터 무결성을 유지하는 방법 및 고가용성 구성의 경우 기본 노드에 장애가 발생할 경우 페일오버하는 방법을 결정합니다. 복제 모드에는 동기식과 비동기식의 두 가지가 있습니다.

두 복제 모드는 모두 데이터베이스 페일오버를 지원하지만 각각 장단점이 있습니다. 고가용성 데이터베이스 페일오버를 지원하려면 비동기식 모드의 경우 2개, 동기식 모드의 경우 3개의 노드가 필요합니다. 동기식 모드도 자동 페일오버를 호출합니다.

복제 모드	장점	단점
동기식	<ul style="list-style-type: none"> ■ 데이터 손실 가능성을 최소화합니다. ■ 자동 페일오버를 호출합니다. 	<ul style="list-style-type: none"> ■ 시스템 성능에 영향을 줄 수 있습니다. ■ 3개의 노드가 필요합니다.
비동기식	<ul style="list-style-type: none"> ■ 두 개의 노드만 필요합니다. ■ 동기식 모드보다 시스템 성능에 미치는 영향이 적습니다. 	<ul style="list-style-type: none"> ■ 데이터 손실 방지 성능이 동기식 모드에 비해 떨어집니다.

vRealize Automation은 두 모드를 다 지원하지만 기본적으로 비동기 모드에서 작동하며 장치 데이터베이스 노드가 두 개 이상 있는 경우에만 고가용성을 제공합니다. 가상 장치 관리 인터페이스의 **클러스터** 탭을 사용하면 동기화 모드로 전환할 수 있으며 필요에 따라 데이터베이스 노드를 추가할 수 있습니다.

동기식 모드에서 작동하는 경우 vRealize Automation이 자동 페일오버를 호출합니다.

고가용성이 아닌 구성에서 노드 하나로 시작하는 경우, 고가용성 향상을 위해 필요에 따라 나중에 노드를 추가할 수 있습니다. 적절한 하드웨어가 있고 데이터 손실이 발생하지 않도록 최대한 보호해야 하는 경우에는 동기식 모드에서 작동하도록 배포를 구성하는 것을 고려하십시오.

장치 데이터베이스 페일오버

고가용성 구성에서 기본 노드는 트랜잭션을 복제 서버로 계속 스트리밍합니다. 기본 노드에 장애가 발생하면 활성 및 작동 중인 복제 노드는 읽기 전용 요청을 진행할 준비가 됩니다. 새 기본 노드가 승격되면, 수동으로 또는 자동으로, 예정된 모든 요청이 함께 이동됩니다.

장치 데이터베이스 구성

가상 장치 관리 인터페이스 데이터베이스 페이지를 사용하여 장치 데이터베이스의 구성을 모니터링하거나 업데이트할 수 있습니다. 또한 기본 노드 지정 및 데이터베이스에서 사용하는 동기화 모드를 변경할 수도 있습니다.

장치 데이터베이스는 vRealize Automation 시스템이 설치되고 구성되는 동안 설치 및 구성되지만 가상 장치 관리 인터페이스의 **데이터베이스** 탭에서 구성을 모니터링하고 변경할 수 있습니다.

연결 상태 텍스트 상자는 데이터베이스가 vRealize Automation 시스템에 연결되어 있는지 그리고 제대로 작동하는지 여부를 나타냅니다.

장치 데이터베이스에서 페일오버를 지원하는 여러 노드를 사용하는 경우 페이지 맨 아래의 테이블은 노드와 그 상태를 표시하고 어떤 노드가 기본 노드인지 알려 줍니다. **복제 모드** 텍스트 상자는 시스템에 현재 구성된 작동 모드가 동기인지 아니면 비동기인지 보여 줍니다. 장치 데이터베이스 구성을 업데이트하려면 이 페이지를 사용합니다.

데이터베이스 노드 테이블의 [동기화 상태*] 열은 클러스터에 대한 동기화 방법을 보여 줍니다. 이 열은 [상태] 열과 함께 클러스터 노드의 상태를 보여 줍니다. 잠재적 상태는 클러스터에서 사용하는 복제가 비동기적인지 아니면 동기적인지에 따라 다릅니다.

표 1-4. 장치 데이터베이스 복제 모드의 동기화 상태

모드	동기화 상태 메시지
동기적 복제	기본 노드 - 상태 없음 복제 노드 - 동기화 기타 노드 - 잠재적
비동기적 복제	기본 노드 - 상태 없음 기타 노드 - 잠재적

[유효] 열은 복제본이 기본 노드와 동기화되었는지 여부를 나타냅니다. 기본 노드는 항상 유효합니다.

[우선 순위] 열은 기본 노드와 비교하여 복제본 노드의 위치를 보여줍니다. 기본 노드에는 우선 순위 값이 없습니다. 복제 노드를 기본 노드로 승격시키는 경우 우선 순위 값이 가장 낮은 노드를 선택합니다.

동기식 모드에서 작동하는 경우 vRealize Automation이 자동 페일오버를 호출합니다. 기본 노드에서 장애가 발생할 경우, 다음으로 사용 가능한 복제 노드가 자동으로 새 기본 노드가 됩니다. 일반적인 vRealize Automation 배포의 경우 페일오버 작업은 10~30초 소요됩니다.

사전 요구 사항

- "vRealize Automation 설치"의 해당 지침에 따라 vRealize Automation을 설치 및 구성합니다.
- vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **루트**로 vRealize Automation 장치 관리에 로그인합니다.
- vRealize Automation 배포의 일부로 포함된 Postgres 장치 데이터베이스 클러스터를 적절하게 구성합니다.

절차

- 1 가상 장치 관리 인터페이스에서 **vRA 설정 > 데이터베이스**를 선택합니다.
- 2 데이터베이스에서 여러 노드를 사용하고 있는 경우 페이지 맨 아래의 테이블을 검토하여 시스템이 제대로 작동 중인지 확인합니다.
 - 모든 노드가 나열되어 있는지 확인합니다.
 - 적절한 노드가 기본 노드로 지정되어 있는지 확인합니다.

참고 데이터가 안전하다는 확신이 있는 경우가 아니면 데이터베이스의 동기화 모드 변경을 위해 **동기화 모드**를 클릭하지 마십시오. 준비 없이 동기화 모드를 변경하면 데이터 손실이 발생할 수 있습니다.

- 3 노드 중 하나를 기본 노드로 승격시키려면 해당 열에서 **승격**을 클릭합니다.
- 4 내용을 변경한 경우 구성을 저장하려면 **설정 저장**을 클릭합니다.

3개 노드 장치 데이터베이스 자동 페일오버 시나리오

장치 데이터베이스고가용성 페일오버 시나리오에는 여러 가지가 있으며, 장치 데이터베이스 구성 및 실패한 노드 수에 따라 vRealize Automation 동작이 달라집니다.

단일 노드 장애 시나리오

노드 세 개 중 하나에 장애가 발생하면 vRealize Automation이 자동 페일오버를 시작합니다. 노드 세 개 모두 복원될 때까지 추가적인 자동 페일오버 작업이 수행될 수 없습니다.

다음 표에는고가용성 배포에서 기본 노드 장애와 관련된 동작 및 작업이 설명되어 있습니다.

표 1-5. 기본 노드에서 장애 발생

예상 동작	<ul style="list-style-type: none"> ■ 구성된 동기화 복제 노드가 기본 노드가 되어 장치 데이터베이스 기능을 자동으로 수행합니다. ■ 잠재적 동기화 복제 노드가 동기화 대기 노드가 됩니다. ■ 자동 페일오버가 완료될 때까지 vRealize Automation 배포가 기능 읽기 전용 모드로 유지됩니다.
추가적인 작업	<ul style="list-style-type: none"> ■ 이전 기본 노드가 복구되면 페일오버 에이전트 복구 논리에 따라 자동으로 복제본으로 재설정됩니다. 어떠한 수동 작업도 필요하지 않습니다. ■ 이전 기본 노드를 복구할 수 없는 경우, 수동으로 장치 데이터베이스를 비동기식 모드로 설정합니다.

다음 표에는 고가용성 배포에서 동기화 복제 노드 장애와 관련된 동작 및 작업이 설명되어 있습니다.

표 1-6. 동기화 복제본에서 장애 발생

예상 동작	<ul style="list-style-type: none"> ■ vRealize Automation 배포에서 다운타임이 발생하지 않습니다. 잠재적 복제본이 새로운 동기화 복제본이 될 때까지 데이터베이스 요청이 몇 초 간 지연될 수 있습니다. 장치 데이터베이스가 이 작업을 자동으로 수행합니다.
추가적인 작업	<ul style="list-style-type: none"> ■ 이전 동기화 복제본이 온라인 상태가 되면 이 복제본이 자동으로 잠재적 복제본이 됩니다. 어떠한 수동 작업도 필요하지 않습니다. ■ 이전 동기화 복제본을 복구할 수 없는 경우, 수동으로 장치 데이터베이스를 비동기식 모드로 설정합니다.

다음 표에는 고가용성 배포에서 기본 노드 장애와 관련된 동작 및 작업이 설명되어 있습니다.

표 1-7. 잠재적 복제본에서 장애 발생

예상 동작	배포 다운타임이 발생하지 않습니다.
추가적인 작업	<ul style="list-style-type: none"> ■ 이전의 잠재적 복제본이 온라인 상태가 되면 이 복제본이 자동으로 잠재적 복제본이 됩니다. 어떠한 수동 작업도 필요하지 않습니다. ■ 이전의 잠재적 복제본을 복구할 수 없는 경우, 장치 데이터베이스를 비동기식 모드로 설정합니다.

2개 노드 장애 시나리오

노드 세 개 중 두 개에서 동시에 장애가 발생하면 vRealize Automation은 수동 복구가 수행될 때까지 읽기 전용 모드로 전환됩니다.

다음 표에는 고가용성 배포에서 기본 노드와 잠재적 복제 노드 장애와 관련된 동작 및 작업이 설명되어 있습니다.

표 1-8. 기본 노드 및 잠재적 복제본에서 장애 발생

예상 동작	<ul style="list-style-type: none"> ■ 동기화 복제본이 기본 노드로 자동 승격되지 않습니다. vRealize Automation은 수동 승격이 수행될 때까지 읽기 전용 트랜잭션을 처리할 수 있기 때문에 읽기 전용 모드로 작동합니다.
추가적인 작업	<ul style="list-style-type: none"> ■ 수동 승격이 필요합니다. 장치 데이터베이스를 비동기식 모드로 설정합니다. ■ 기본 노드 및 잠재적 복제본이 복구되면 새 기본 노드를 기준으로 동기화되도록 수동으로 설정합니다. 이때 vRealize Automation을 다시 동기식 모드로 전환할 수 있습니다. ■ 노드 세 개 중 두 개가 동시에 다운되면 vRealize Automation은 사용자가 수동 복구를 수행할 때까지 읽기 전용 모드로 전환됩니다. 하나의 데이터베이스 노드만 사용 가능한 경우에는 배포를 비동기식 모드로 전환합니다.

다음 표에는 고가용성 배포에서 동기화 및 잠재적 노드 장애와 관련된 동작 및 작업이 설명되어 있습니다.

표 1-9. 동기화 및 잠재적 복제본에서 장애 발생

예상 동작	<ul style="list-style-type: none"> ■ vRealize Automation은 수동 복구가 수행될 때까지 읽기 전용 트랜잭션을 처리할 수 있기 때문에 읽기 전용 모드로 작동합니다.
추가적인 작업	<ul style="list-style-type: none"> ■ 수동 승격이 필요합니다. 장치 데이터베이스를 비동기식 모드로 설정합니다. ■ 동기화 및 잠재적 복제본이 복구되면 기본 노드를 기준으로 동기화되도록 동기화 및 잠재적 복제본을 수동으로 재설정해야 합니다. 이때 vRealize Automation을 다시 동기식 모드로 전환할 수 있습니다. ■ 노드 세 개 중 두 개가 동시에 다운되면 vRealize Automation은 사용자가 수동 복구를 수행할 때까지 읽기 전용 모드로 전환됩니다. 하나의 데이터베이스 노드만 사용 가능한 경우에는 배포를 비동기식 모드로 전환합니다.

노드 간에 링크 장애 발생

분산된 배포에서 노드 간에 링크 장애가 발생할 경우 자동 페일오버 에이전트는 구성을 복구하려고 시도합니다.

다음 표에는 모든 노드가 작동 중이고 온라인 상태인 경우, 지정된 구성을 사용하는 고가용성 배포의 두 사이트 간 링크 장애와 관련된 동작 및 작업이 설명되어 있습니다.

사이트 A: 기본 노드 및 잠재적 복제본

사이트 B: 동기화 복제본

표 1-10. 모든 노드가 작동 중이고 온라인 상태일 때 두 사이트 간에 링크 장애 발생

예상 동작	vRealize Automation 배포에 대해 다운타임이 발생하지 않습니다. 잠재적 복제본이 자동으로 동기화 복제본이 됩니다.
추가적인 작업	어떠한 수동 작업도 필요하지 않습니다.

다음 표에는 모든 노드가 작동 중이고 온라인 상태인 경우, 지정된 구성을 사용하는 고가용성 배포의 두 사이트 간 링크 장애와 관련된 동작 및 작업이 설명되어 있습니다.

사이트 A: 기본 노드

사이트 B: 동기화 및 잠재적 복제본

표 1-11. 모든 노드가 작동 중이고 온라인 상태일 때 두 사이트 간에 링크 장애 발생 - 대체 구성

예상 동작	동기화 복제본이 기본 노드가 되어 장치 데이터베이스 기능을 자동으로 수행합니다. 자동 페일오버 에이전트가 잠재적 복제본을 새 동기화 복제본으로 승격시킵니다. 이 승격이 완료되기 전까지 vRealize Automation 배포가 읽기 전용 모드로 작동합니다.
추가적인 작업	어떠한 수동 작업도 필요하지 않습니다. 링크가 복구되면 자동 페일오버 에이전트가 이전 기본 노드를 복제본으로 재설정합니다.

시나리오: 수동 vRealize Automation 장치 데이터베이스 페일오버 수행

vRealize Automation 장치 Postgres 데이터베이스에 문제가 있는 경우 클러스터의 복제 vRealize Automation 장치 노드에 수동으로 페일오버를 수행할 수 있습니다.

기본 vRealize Automation 장치 노드의 Postgres 데이터베이스가 실패하거나 실행 중지되면 다음 단계를 수행합니다.

참고 노드가 비정상 상태가 되면 페일오버를 포함한 모든 작업에 가상 장치 관리 인터페이스를 사용하지 마십시오.

사전 요구 사항

- vRealize Automation 장치 노드의 클러스터를 구성합니다. 각 노드는 포함된 Postgres 장치 데이터베이스의 사본을 호스팅합니다.

절차

- 1 기본 노드 IP 주소를 외부 로드 밸런서에서 제거합니다.
- 2 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.
`https://vrealize-automation-appliance-FQDN:5480`
- 3 **클러스터**를 선택합니다.
- 4 데이터베이스 노드 목록에서 우선 순위가 가장 낮은 복제 노드를 찾습니다.
복제 노드는 우선 순위가 오름차순으로 표시됩니다.
- 5 **승격**을 클릭하고 작업이 완료될 때까지 기다립니다.
완료되면 복제 노드가 새 기본 노드로 나열됩니다.
- 6 이전 기본 노드의 문제를 수정하고 클러스터에 다시 추가합니다.
 - a 이전 기본 노드를 격리합니다.

현재 네트워크(나머지 vRealize Automation 장치 노드로 라우팅하는 네트워크)에서 노드의 연결을 끊습니다. 관리를 위해 다른 NIC를 선택하거나 가상 시스템 관리 콘솔에서 직접 관리합니다.

- b 이전 기본 노드를 복구합니다.

노드의 전원을 켜거나 문제를 수정합니다. 예를 들어 가상 시스템이 반응이 없으면 시스템을 재설정합니다.

- c 콘솔 세션에 루트로 로그인하고 vPostgres 서비스를 중지합니다.

```
service vpostgres stop
```

- d 이전 기본 노드를 원래 네트워크(다른 vRealize Automation 장치 노드로 라우팅하는 네트워크)에 다시 추가합니다.

- e 콘솔 세션에 루트로 로그인하고 haproxy 서비스를 다시 시작합니다.

```
service haproxy restart
```

- f 새 vRealize Automation 장치 기본 노드 관리 인터페이스에 루트로 로그인합니다.

- g 클러스터를 선택합니다.

- h 이전 기본 노드를 찾아서 **재설정**을 클릭합니다.

- i 재설정이 완료된 후 이전 기본 노드를 다시 시작합니다.

- j 이전 기본 노드의 전원이 켜진 상태에서 다음 서비스가 실행 중인지 확인합니다.

```
haproxy horizon-workspace rabbitmq-server vami-lighttpd vcac-server vco-server
```

- k 이전 기본 노드를 외부 로드 밸런서에 다시 추가합니다.

참고 복제로 강등된 기본 노드가 아직 기본 노드로 나열되면 문제를 수정하기 위해 해당 노드를 클러스터에 수동으로 다시 가입해야 할 수 있습니다.

시나리오: 유지 보수 데이터베이스 페일오버 수행

vRealize Automation 시스템 관리자로서, 장치 데이터베이스 유지 보수 페일오버 작업을 수행해야 합니다.

이 시나리오에서는 현재 기본 노드가 정상적으로 가동되어 실행 중이라고 가정합니다. 데이터베이스 페일오버 유지 보수 단계에는 기본 노드의 유지 보수와 복제 노드의 유지 보수 두 가지가 있습니다. 기본 노드가 대체되어 복제 노드가 되었다면 필요한 경우 다시 기본 노드가 되기에 적절하도록 이 노드에 대한 유지 보수를 수행해야 합니다.

참고 유지 보수 페일오버를 수행하는 동안 해당 호스트 시스템에서 HAProxy 서비스를 중지하거나 다시 시작하지 마십시오.

사전 요구 사항

- vRealize Automation을 "vRealize Automation 설치"의 해당 지침에 따라 설치하고 구성합니다.
- vRealize Automation 장치를 배포할 때 입력한 암호를 사용하여 **루트**로 vRealize Automation 장치 관리에 로그인합니다.

- 적절한 포함된 Postgres 장치 데이터베이스 클러스터를 설치하고 구성합니다.
- 데이터베이스에서 동기적 복제 모드를 사용하는 경우 클러스터에 3개의 활성 노드가 있는지 확인합니다.

절차

1 기본 노드 IP 주소를 외부 로드 밸런서에서 제거합니다.

2 기본 노드를 격리합니다.

현재 네트워크에서 노드의 연결을 끊습니다. 이 네트워크는 나머지 vRealize Automation 장치 노드에 라우팅하는 네트워크여야 합니다.

3 관리를 위해 다른 NIC를 선택하거나 가상 시스템 관리 인터페이스에서 직접 관리합니다.

4 가상 장치 관리 인터페이스에서 **클러스터**를 선택합니다.

5 기본 노드로 승격하는 우선 순위가 가장 낮은 복제 노드를 선택하고 **승격**을 클릭합니다.

복제 노드는 우선 순위가 오름차순으로 표시됩니다.

이전 기본 노드가 복제 상태로 강등되고 새 기본 노드가 승격됩니다.

6 적절한 복제 유지 보수를 수행합니다.

7 유지 보수가 완료되면 가상 장치가 네트워크 연결과 함께 실행 중인지 그리고 해당 HAProxy 서비스가 실행 중인지 확인합니다.

a **root**로 vRealize Automation 관리 콘솔에 로그인합니다.

b 가상 장치 관리 인터페이스의 **클러스터** 탭에서 복제 노드가 최신 상태인지, 복제 노드에 대해 ping을 수행할 수 있는지 및 복제 노드 이름을 확인할 수 있는지 확인합니다.

8 복제 노드에 대해 **재설정**을 클릭합니다.

이 작업은 데이터베이스를 재설정하여 데이터베이스가 현재 기본 노드로 복제되도록 구성하고 복제 노드를 기본 노드의 최신 haproxy 구성과 다시 동기화합니다.

9 성공적으로 재설정되었으면 복제 가상 장치 노드 IP 주소를 외부 가상 장치 로드 밸런서 IP 주소 풀에 반환합니다.

10 복제 노드가 데이터베이스 테이블에 정상 상태로 표시되는지, ping을 수행할 수 있는지, 이름을 확인할 수 있는지 확인합니다.

다음에 수행할 작업

이전 기본 노드의 문제를 수정하고 클러스터에 다시 추가합니다.

심각한 오류로부터 수동으로 장치 데이터베이스 복구

장치 데이터베이스가 실패한 후 데이터베이스 노드가 시작되어 실행되지 않거나, 기본 노드가 실패할 때 모든 복제 노드가 동기화되지 않는 경우 다음 절차를 사용하여 데이터베이스 복구를 시도하십시오.

이 절차는 비동기 모드로 실행 중인 클러스터에서 작업 중인 데이터베이스 노드가 없는 상황에 적용됩니다. 이 시나리오에서, 일반적으로 페이지를 로드하거나 새로 고치려고 시도하면 가상 장치 관리 인터페이스 페이지에 다음과 유사한 오류가 표시됩니다.

데이터베이스 서비스를 초기화하는 중 오류가 발생했습니다. 트랜잭션을 위해 JDBC 연결을 열 수 없습니다. 중첩된 예외는 `org.postgresql.util.PSQLException`입니다. 연결 시도가 실패했습니다.

절차

- 1 데이터베이스 노드 중 하나에서 가상 장치 관리 인터페이스를 사용하여 데이터베이스 복구를 시도합니다.
 - a 가능한 경우 가장 최근 상태인 노드의 가상 장치 관리 인터페이스 **클러스터** 페이지를 엽니다. 일반적으로 이 노드는 데이터베이스가 실패하기 전에 기본 노드였던 노드입니다.
 - b 기본 노드의 가상 장치 관리 인터페이스가 열리지 않으면 다른 복제 노드의 인터페이스를 열려고 시도합니다.
 - c 작동하는 가상 장치 관리 인터페이스가 있는 데이터베이스 노드를 찾을 수 있다면 수동 페일오버를 수행하여 복구를 시도합니다.

시나리오: 수동 vRealize Automation 장치 데이터베이스 페일오버 수행 항목을 참조하십시오.

- 2 1단계의 절차가 실패하면 셸 세션을 시작하고 가장 최근 상태인 노드의 확인을 시도합니다. 사용 가능한 모든 클러스터 노드에 대한 셸 세션을 시작하고 다음 셸 명령을 실행하여 데이터베이스를 시작하려고 시도합니다. `service vpostgres start`

- 3 가장 최근 상태인 노드를 확인하려면 실행 중인 로컬 데이터베이스가 있는 각 노드에 대해 다음 절차를 사용합니다.

- a 다음 명령을 실행하여 가장 최근 상태인 노드를 확인합니다. 명령이 **f**를 반환하면 이것이 가장 최근 상태인 노드이므로 4단계로 진행할 수 있습니다.

```
su - postgres
psql vcac
vcac=# select pg_is_in_recovery();
pg_is_in_recovery
```

- 이 명령이 **f**를 반환하면 이 노드가 가장 최근 상태인 노드입니다.
- 노드가 **t**를 반환하는 경우 해당 노드에서 다음 명령을 실행합니다.

```
SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location() as
replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
```

이 명령은 다음과 비슷한 결과를 반환합니다.

```
vcac=# SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location()
as replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
receive_loc | replay_loc | replay_timestamp
-----+-----+-----
0/200000000 | 0/203228A0 | 1491577215.68858
(1 row)
```

- 4 각 노드에 대한 결과를 비교하여 가장 최근 상태인 노드가 무엇인지 확인합니다.

receive_loc 열 아래에서 가장 큰 값이 있는 노드를 선택하고, 값이 같은 경우 **replay_loc** 열에서 가장 큰 값을 선택하고, 이 값도 같은 경우 **replay_timestamp**의 가장 큰 값이 있는 노드를 선택합니다.

- 5 가장 최근 상태인 노드에서 다음 명령을 실행합니다. **vcac-vami psql-promote-master -force**
- 6 텍스트 편집기에서 **/etc/haproxy/conf.d/10-psql.cfg** 파일을 열고 다음 줄을 업데이트합니다.

```
server masterserver sc-rdops-vm06-dhcp-170-156.eng.vmware.com:5432 check on-marked-up shutdown-
backup-sessions
```

현재 노드 FQDN을 사용하여 다음과 같이 변경합니다.

```
server masterserver current-node-fqdn:5432 check on-marked-up shutdown-backup-sessions
```

- 7 파일을 저장합니다.
- 8 **service haproxy restart** 명령을 실행합니다.
- 9 가장 최근 노드에 대한 가상 장치 관리 인터페이스 **클러스터** 페이지를 엽니다.

이 노드는 기본 노드로 나타나야 하며 다른 노드는 잘못된 복제본으로 나타나야 합니다. 또한 해당 복제본에 대한 **재설정** 버튼이 사용되도록 설정됩니다.

- 10 클러스터 상태가 복구됨일 때까지 계속해서 각 복제본에 대해 **재설정**을 클릭합니다.

vRealize Automation 설치에 대한 백업 및 복구

실패 시 데이터 손실 및 시스템 다운타임을 최소화하기 위해 관리자는 정기적으로 전체 vRealize Automation 설치를 백업합니다. 시스템이 실패하는 경우 마지막으로 알려진 작업 백업을 복원하거나 일부 구성 요소를 다시 설치하여 복구할 수 있습니다.

vRealize Automation을 백업 및 복원하려면 [vRealize Suite 설명서](#)에서 다음 항목을 참조하십시오.

- vRealize Automation 백업 준비
- vRealize Automation 시스템 복구

고객 환경 향상 프로그램

이 제품은 VMware의 CEIP(고객 환경 향상 프로그램)에 참여합니다. CEIP는 VMware에 VMware가 제품과 서비스를 향상하고 문제를 해결하고 제품을 가장 효과적으로 배포 및 사용하는 방법에 대해 조언할 수 있게 해 주는 정보를 제공합니다. 언제든지 vRealize Automation에 대한 CEIP에 참여하거나 탈퇴할 수 있습니다.

CEIP를 통해 수집된 데이터에 대한 세부 정보 및 VMware에서 CEIP를 사용하는 목적이 Trust & Assurance Center의 <http://www.vmware.com/trustvmware/ceip.html>에 기술되어 있습니다.

vRealize Automation에 대한 고객 환경 향상 프로그램 참여 또는 탈퇴

vRealize Automation에 대한 고객 환경 향상 프로그램(CEIP)에 언제든지 참여하거나 탈퇴할 수 있습니다.

vRealize Automation은 처음에 제품을 설치하고 구성할 때 고객 환경 향상 프로그램(CEIP)에 참여할 수 있는 기회를 제공합니다. 설치 후에는 아래 단계에 따라 CEIP에 참여하거나 탈퇴할 수 있습니다.

절차

- 1 vRealize Automation 장치 관리 인터페이스에 루트로 로그인합니다.

<https://vrealize-automation-appliance-FQDN:5480>

- 2 **원격 분석** 탭을 클릭합니다.

- 3 **VMware 고객 환경 향상 프로그램에 참여** 옵션을 선택하거나 선택을 해제합니다.

옵션을 선택하면 프로그램이 활성화되고 <https://vmware.com>으로 데이터가 전송됩니다.

- 4 **설정 저장**을 클릭합니다.

데이터 수집 시간 구성

CEIP(고객 환경 향상 프로그램)가 VMware로 데이터를 보내는 요일과 시간을 설정할 수 있습니다.

절차

- 1 vRealize Automation 장치의 콘솔 세션에 루트로 로그인합니다.

- 2 텍스트 편집기에서 다음 파일을 엽니다.

`/etc/telemetry/telemetry-collector-vami.properties`

- 3 요일(dow)과 시간(hod)의 속성을 편집합니다.

속성	설명
<code>frequency.dow=<요일></code>	데이터 수집을 수행하는 요일.
<code>frequency.hod=<시간></code>	데이터 수집을 수행하는 현지 시간. 가능한 값은 0-23입니다.

- 4 `telemetry-collector-vami.properties`를 저장하고 닫습니다.

- 5 다음 명령을 입력하여 설정을 적용합니다.

```
vcac-config telemetry-config-update --update-info
```

변경 내용이 배포에 포함된 모든 노드에 적용됩니다.

시스템 설정 조정

시스템 관리자는 로깅을 조정하고 IaaS 이메일 템플릿을 사용자 지정합니다. 각 테넌트에 대해 기본값으로 나타나는 설정도 관리할 수 있습니다. 예를 들어 알림을 처리하도록 이메일 서버를 구성합니다. 테넌트 관리자는 해당 테넌트에 다른 설정이 필요한 경우 이러한 기본값을 재정의하도록 선택할 수 있습니다.

서비스 카탈로그에서 모든 서비스 아이콘 수정

서비스 카탈로그에서 기본 아이콘을 수정하여 사용자 지정 이미지를 표시할 수 있습니다. 아이콘을 수정하면 모든 테넌트에서 아이콘이 변경됩니다. 카탈로그에 테넌트별 아이콘을 구성할 수는 없습니다.

모든 운영 체제에서 cURL 명령을 실행할 수 있도록 Linux, Mac 및 Windows에 대한 명령이 제공됩니다.

사전 요구 사항

- 이미지를 base64로 인코딩된 문자열로 변환합니다.
- 명령을 실행하는 시스템에 cURL이 설치되어 있어야 합니다.
- 시스템 관리자 역할을 맡은 vRealize Automation 사용자에게 대한 자격 증명이 있어야 합니다.

절차

- 1 터미널 세션에서 cURL 명령에 대해 VCAC 변수를 설정합니다.

운영 체제	명령
Linux/Mac	<code>export VCAC=<VA URL></code>
Windows	<code>set VCAC=<VA URL></code>

2 시스템 관리자 사용자를 위한 인증 토큰을 검색합니다.

운영 체제	명령
Linux/Mac	<pre>curl https://\$VCAC/identity/api/tokens --insecure -H "Accept: application/json" -H 'Content-Type: application/json' --data '{"username":"<Catalog Administrator User>","password":"<password>","tenant":"vsphere.local"}'</pre>
Windows	<pre>curl https://\$VCAC/identity/api/tokens --insecure -H "Accept:application/json" -H "Content-Type:application/json" --data "{\"username\":\"<Catalog Administrator User>\",\"password\":\"<password>\",\"tenant\":\"<vsphere.local>\"}"</pre>

인증 토큰이 생성됩니다.

3 <Auth Token>을 이전 단계에서 생성한 토큰 문자열로 대체하여 인증 토큰 변수를 설정합니다.

운영 체제	명령
Linux/Mac	<pre>export AUTH="Bearer <Auth Token>"</pre>
Windows	<pre>set AUTH=Bearer <Auth Token></pre>

4 이미지에 대한 Base64로 인코딩된 문자열을 추가합니다.

운영 체제	명령
Linux/Mac	<pre>curl https://\$VCAC/catalog-service/api/icons --insecure -H "Accept: application/json" -H 'Content-Type: application/json' -H "Authorization: \$AUTH" --data '{"id":"cafe_default_icon_genericAllServices","fileName":"<filename>","contentType":"image/png","image":"<IMAGE DATA as base64 string>"}</pre>
Windows	<pre>curl https://\$VCAC/catalog-service/api/icons --insecure -H "Accept: application/json" -H "Content-Type: application/json" -H "Authorization: %AUTH%" --data "{\"id\":\"cafe_default_icon_genericAllServices\",\"fileName\":\"<filename>\",\"contentType\":\"image/png\",\"image\":\"<IMAGE DATA as base64 string>\"}"</pre>

결과

약 5분이 지나면 새 서비스 아이콘이 서비스 카탈로그에 나타납니다.

기본 아이콘으로 되돌리고 싶다면 1-3단계를 수행한 후에 다음 명령을 실행할 수 있습니다.

운영 체제	명령
Linux/Mac	<pre>curl https://\$VCAC/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: \$AUTH" --request DELETE</pre>
Windows	<pre>curl https://\$VCAC/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: %AUTH%" --request DELETE</pre>

데이터 롤오버 설정 사용자 지정

vRealize Automation 데이터 롤오버 설정을 구성하여 시스템에서 기존 데이터를 보존, 아카이브 및 삭제하는 방식을 제어할 수 있습니다.

데이터 롤오버 기능을 사용하여 롤오버를 사용하도록 설정하고, vRealize Automation이 IaaS SQL Server 데이터베이스의 데이터를 아카이브 또는 삭제하기 전에 해당 데이터를 보존할 최대 일수 및 기타 데이터 롤오버 컨트롤을 설정합니다.

기본적으로 데이터 롤오버 기능은 비활성화됩니다.

vRealize Automation **글로벌 설정** 페이지에서 데이터 롤오버 설정을 구성합니다. 활성화되면, 이 기능은 다음 SQL Server 데이터베이스 테이블에서 데이터를 쿼리하고 제거합니다.

- UserLog
- Audit
- CategoryLog
- VirtualMachineHistory
- VirtualMachineHistoryProp
- AuditLogItems
- AuditLogItemsProperties
- TrackingLogItems
- WorkflowHistoryInstances
- WorkflowHistoryResults

DataRolloverIsArchiveEnabled를 True로 설정하면 dbo 스키마에서 테이블의 아카이브 버전이 생성됩니다. 예를 들어 UserLog의 아카이브 버전은 UserLogArchive, VirtualMachineHistory의 아카이브 버전은 VirtualMachineHistoryArchive가 됩니다.

사용하도록 설정한 경우, 데이터 롤오버 기능은 vRealize Automation 장치 표준 시간대 구성에 따라 사전 지정된 시간(오전 3시)에 하루 한 번 실행됩니다. DataRollover MaximumAgeInDays 설정을 사용하여 데이터를 보존할 최대 일수를 설정할 수 있습니다. 이 프로세스는 일반적으로 몇 분에서 한 시간 이내로 빠르게 실행됩니다. 하지만 이 기능을 처음 사용하도록 설정하면 아카이브/삭제할 데이터가 많아 완료하는 데 훨씬 더 오랜 시간이 걸릴 수 있습니다. 이 프로세스는 완료될 때까지 실행됩니다. 동시 실행 문제를 일으키지 않도록 이 작업은 작고 간단한 배치 크기의 트랜잭션 체크 단위로 수행됩니다. 아래 설명된 대로 이 프로세스는 정상적으로 중지할 수 있습니다.



참고 DataRollover Status 설정을 [실행 중]에서 [사용 안 함] 또는 [사용]으로 변경하여 DataRollover 프로세스를 중지할 수 있습니다. 그러면 현재 실행 중인 프로세스가 정상적으로 종료됩니다. 손실되는 작업이 없습니다. 프로세스를 중지하기까지 아카이브되거나 삭제된 모든 데이터가 저장됩니다.

DataRollover IsArchiveEnabled를 **True**로 설정하면 **DataRollover MaximumAgeInDays** 설정에 지정된 기간보다 오래된 데이터가 아카이브 테이블로 이동합니다. **DataRollover IsArchiveEnabled**를 **False**로 설정하면 데이터가 영구적으로 삭제되고 데이터가 아카이브되지 않습니다. 삭제된 데이터는 복구할 수 없습니다.

절차

- 1 **시스템 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 2 **인프라 > 관리 > 글로벌 설정**을 선택합니다.
- 3 **글로벌 설정** 페이지에서 테이블의 **데이터 롤오버** 섹션을 찾아 설정을 검토 및 구성합니다.

설정	설명
DataRollover BatchSize	기본값은 2000이며 대개 변경할 필요가 없습니다. 하지만 성능에 미치는 영향이 있을 것으로 생각되면 더 작은 BatchSize를 사용하는 것이 좋습니다. 더 큰 BatchSize를 사용하면 작업이 더 빠르게 완료될 수 있지만 동시 실행 처리 시 부담이 가중됩니다. 유효한 범위는 100~20000입니다.
DataRollover IsArchiveEnabled	최대 일수에 도달한 이후 롤오버 데이터를 아카이브 테이블로 이동할지 지정합니다. 기본적으로 이 값은 True 로 설정되어 있습니다. 이 값을 False 로 설정하면 DataRollover MaximumAgeInDays 설정에 지정된 기간보다 오래된 모든 데이터가 영구적으로 삭제됩니다.
DataRollover MaximumAgeInDays	데이터베이스의 데이터를 아카이브로 이동하거나 영구적으로 삭제하기 전에 시스템에서 보존할 최대 일수를 지정합니다. 기본적으로 이 값은 90일로 설정되어 있습니다.
DataRollover Status	데이터 롤오버를 사용하도록 설정할지 지정합니다. 기본적으로 이 값은 [사용 안 함]으로 설정되어 있습니다. 데이터 롤오버를 사용하도록 설정하려면 값을 [사용]으로 설정합니다.
DataRollover VirtualMachineHistory BatchSize	VirtualMachineHistory 테이블에서 1~5 레코드 범위로 배치 크기를 지정합니다. 기본값은 1입니다.
DataRollover UpdateStatistics	UpdateStatistics 는 기본적으로 사용되지 않도록 설정되어 있지만 통계를 업데이트하면 쿼리 성능이 향상되므로 사용하도록 설정(1로 설정)하는 것이 좋습니다. 이렇게 하면 아카이브 프로세스가 실행된 후 [dbo].[usp_DataRollover] 저장 프로시저가 테이블에 대해 통계 업데이트 명령을 수행합니다.

- 4 설정을 편집하려면 첫 번째 테이블 열에서 **편집** 아이콘()을 클릭합니다.
적용 가능한 설정에 대한 **값** 영역을 편집할 수 있습니다.
- 5 변경 내용을 저장하려면 첫 번째 테이블 열에서 **저장** 아이콘()을 클릭합니다.

Manager Service 구성 파일의 설정 조정

Manager Service 구성 파일(managerService.exe.config)을 사용하여 시스템 배포를 위한 공통 설정을 조정할 수 있습니다.

managerService.exe.config 파일은 일반적으로 %System-Drive%\Program Files x86\VMware\vCAC\Server 디렉토리에 있습니다. 파일을 편집하기 전에 항상 파일의 복사본을 만들어야 합니다.

다음 managerService.exe.config 파일 설정을 사용하여 시스템 배포의 다양한 측면을 제어할 수 있습니다. 기본값은 다음과 같습니다.

- <add key="ProcessLeaseWorkflowTimerCallbackIntervalMilliseconds" value="3600000"/>
- <add key="BulkRequestWorkflowTimerCallbackMilliseconds" value="10000"/>
- <add key="MachineRequestTimerCallbackMilliseconds" value="10000"/>
- <add key="MachineWorkflowCreationTimerCallbackMilliseconds" value="10000"/>
- <add key="RepositoryConnectionMaxRetryCount" value="100"/>
- <add key="MachineCatalogRegistrationRetryTimerCallbackMilliseconds" value="120000"/>
- <add key="MachineCatalogUnregistrationRetryTimerCallbackMilliseconds" value="120000"/>
- <add key="MachineCatalogUpdateMaxRetryCount" value="15"/>

리소스를 많이 사용하는 동시성 제한 설정

vRealize Automation에서는 리소스를 절약하기 위해 동시에 실행되는 시스템 프로비저닝 및 데이터 수집 인스턴스의 수를 제한합니다. 이 제한은 변경할 수 있습니다.

동시 시스템 프로비저닝 구성

시스템 프로비저닝을 위한 여러 개의 동시 요청은 vRealize Automation의 성능에 영향을 줄 수 있습니다. 프록시 에이전트와 워크플로 작업에 설정된 제한을 일부 변경하여 성능을 바꿀 수 있습니다.

사이트의 시스템 소유자 요구에 따라, vRealize Automation Server에서 시스템 프로비저닝을 위한 여러 개의 동시 요청을 받을 수 있습니다. 이것은 다음과 같은 상황에서 발생할 수 있습니다.

- 단일 사용자가 여러 시스템에 대해 요청을 제출한 경우
- 여러 사용자가 동시에 시스템을 요청한 경우
- 한 명 이상의 그룹 관리자가 짧은 시간 차이로 보류 중인 여러 개의 시스템 요청을 연속하여 승인한 경우

vRealize Automation에서 시스템을 프로비저닝하는 데 필요한 시간은 보통 동시 요청의 수가 많을수록 증가합니다. 프로비저닝 시간의 증가는 다음의 세 가지 중요한 요인에 종속됩니다.

- SetupOS 작업(WIM 기반 프로비저닝에서와 같이 가상 플랫폼 내에 생성된 시스템의 경우)과 복제 작업(가상 플랫폼 내에서 복제된 시스템의 경우)을 포함하여, 리소스를 많이 사용하는 동시 vRealize Automation 워크플로 작업의 성능에 대한 영향.

- 동시에 실행될 수 있는, 리소스를 많이 사용하는(보통 시간이 오래 걸리는) 프로비저닝 작업의 수에 대해 구성된 vRealize Automation 제한. 기본값은 8개입니다. 구성된 제한을 초과하는 동시 작업은 대기열에 들어갑니다.
- 동시에 실행될 수 있는 vRealize Automation 작업 항목(리소스를 많이 사용하는지 여부에 관계없음)의 수에 대한 가상 플랫폼 또는 클라우드 서비스 계정 내 모든 제한. 예를 들어, vCenter Server의 기본 제한은 4개이며 이 제한을 초과하는 작업 항목은 대기열에 들어갑니다.

기본적으로, vRealize Automation는 프록시 에이전트를 사용하는 하이퍼바이저에 대해 동시 가상 프로비저닝 작업을 끝점당 8개로 제한합니다. 이를 통해 특정 에이전트가 관리하는 가상 플랫폼은 다른 항목의 실행을 방해하는 다수의 리소스 집약적 작업 항목을 받지 않습니다. 제한을 변경하기 전에 제한 변경의 영향을 신중하게 테스트하도록 계획하십시오. 사이트에 대한 최적의 제한을 결정하려면 가상 플랫폼 내의 작업 항목 실행과 vRealize Automation 내의 워크플로 작업 실행을 조사해야 합니다.

구성된 vRealize Automation 에이전트당 제한을 늘리는 경우 vRealize Automation에서 다음과 같이 추가적으로 구성을 조정해야 할 수 있습니다.

- SetupOS 및 CloneWorkflow 작업에 대한 기본 실행 시간 제한 간격은 각각 2시간입니다. 이러한 작업 중 하나를 실행하는 데 필요한 시간이 이 제한을 초과하는 경우 작업이 취소되고 프로비저닝이 실패합니다. 이와 같은 실패를 방지하려면 이러한 실행 시간 제한 간격 중 하나를 늘리거나 둘 다 늘리십시오.
- SetupOS 및 CloneWorkflow 작업에 대한 기본 배달 시간 제한 간격은 각각 20시간입니다. 일단 이러한 작업 중 하나가 시작된 경우 이 작업에 따라 시스템이 20시간 내에 프로비저닝되지 않으면 작업이 취소되고 프로비저닝이 실패합니다. 따라서 이러한 상황이 종종 발생하는 지점으로 제한을 늘렸다면 이러한 배달 시간 제한 간격 중 하나를 늘리거나 둘 다 늘려야 합니다.

동시 데이터 수집 구성

기본적으로 vRealize Automation는 동시 데이터 수집 작업을 제한합니다. 이 제한을 변경하는 경우 서로 다른 데이터 수집 유형에 대한 기본 실행 시간 제한 간격을 변경하여 불필요한 시간 제한을 피할 수 있습니다.

vRealize Automation는 해당 프록시 에이전트를 통해 알려진 가상화 계산 리소스로부터 그리고 해당 끝점을 통해 클라우드 서비스 계정 및 물리적 시스템으로부터 정기적으로 데이터를 수집합니다. 사이트의 끝점, 가상화 계산 리소스 및 에이전트의 수에 따라 동시 데이터 수집 작업이 자주 발생할 수 있습니다.

데이터 수집 실행 시간은 가상 시스템, 데이터 스토어, 템플릿 및 계산 리소스를 포함하여 끝점의 여러 개체에 따라 달라집니다. 여러 조건에 따라 단일 데이터 수집에 상당한 시간이 필요할 수 있습니다. 시스템 프로비저닝과 마찬가지로, 동시성은 데이터 수집을 완료하는 데 필요한 시간을 늘립니다.

기본적으로, 동시 데이터 수집 작업은 에이전트당 두 개로 제한되며 초과된 작업은 대기열에 들어갑니다. 이를 통해 각 데이터 수집 작업을 비교적 빨리 완료하고 동시 데이터 수집 작업에 따른 IaaS 성능 영향을 없앨 수 있습니다.

하지만 사이트의 리소스 및 상황에 따라 구성된 제한을 늘려 충분히 빠른 성능을 유지하면서도 프록시 데이터 수집의 동시성을 활용할 수 있습니다. 제한을 늘리면 단일 데이터 수집에 필요한 시간이 증가하지만, 더 많은 계산 리소스와 시스템으로부터 더 많은 정보를 한 번에 수집할 수 있으므로 단점을 충분히 보상할 수 있습니다.

구성된 에이전트당 제한을 늘리면 프록시 에이전트를 사용하는 서로 다른 데이터 수집 유형(인벤토리, 성능, 상태 및 WMI)에 대한 기본 실행 시간 제한 간격을 조정해야 할 수 있습니다. 이러한 작업 중 하나를 실행하는 데 필요한 시간이 구성된 시간 제한 간격을 초과하면 작업이 취소되고 다시 시작됩니다. 작업 취소를 방지하려면 이러한 실행 시간 제한 간격 중 하나 이상을 늘리십시오.

동시성 제한 및 시간 초과 간격 조정

동시 프로비저닝에 대한 에이전트별 제한, 데이터 수집 작업 및 기본 시간 초과 간격을 변경할 수 있습니다.

해당 변수에 대한 시간 값을 입력할 때 hh:mm:ss(hh=시간, mm=분, ss=초) 형식을 사용합니다.

사전 요구 사항

IaaS Manager Service를 호스팅하는 서버에 관리자 로 로그인합니다. 분산 설치의 경우 이 서버는 Manager Service가 설치된 서버입니다.

절차

- 1 편집기에서 **ManagerService.exe.config** 파일을 엽니다. 이 파일은 vRealize Automation 서버 설치 디렉토리(일반적으로 %SystemDrive%\Program Files x86\VMware\vCAC\Server)에 있습니다.
- 2 **workflowTimeoutConfigurationSection**이라는 섹션을 찾습니다.
- 3 필요에 따라 다음 변수를 업데이트합니다.

매개 변수	설명
MaxOutstandingResourceIntensive WorkItems	동시 프로비저닝 제한(기본값은 8임)
CloneExecutionTimeout	가상 프로비저닝 실행 시간 초과 간격
SetupOSExecutionTimeout	가상 프로비저닝 실행 시간 초과 간격
CloneTimeout	가상 프로비저닝 복제 배달 시간 초과 간격
SetupOSTimeout	가상 프로비저닝 설정 OS 배달 시간 초과 간격
CloudInitializeProvisioning	클라우드 프로비저닝 초기화 시간 초과 간격
MaxOutstandingDataCollection WorkItems	동시 데이터 수집 제한
InventoryTimeout	인벤토리 데이터 수집 실행 시간 초과 간격
PerformanceTimeout	성능 데이터 수집 실행 시간 초과 간격
StateTimeout	상태 데이터 수집 실행 시간 초과 간격

- 4 파일을 저장한 후 닫습니다.

5 시작 > 관리 도구 > 서비스를 선택합니다.

6 중지한 다음 vRealize Automation 서비스를 다시 시작합니다.

7 (선택 사항) vRealize Automation가고가용성 모드에서 실행되고 있는 경우 설치 후 `ManagerService.exe.config` 파일에서 변경된 내용 모두가 기본 서버와 페일오버 서버 둘 다에 적용되어야 합니다.

시스템 콜백의 실행 빈도 조정

vRealize Automation 콜백 프로시저가 변경된 시스템 리스에 대해 실행되는 빈도를 포함하여 여러 콜백 프로시저의 빈도를 변경할 수 있습니다.

vRealize Automation은 리스가 변경된 시스템을 검색하는

`ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds`와 같은 Model Manager 서비스에서 서로 다른 콜백 프로시저를 실행하기 위해 구성된 시간 간격을 사용합니다. 이러한 시간 간격을 변경하여 확인 빈도를 높이거나 낮출 수 있습니다.

이러한 변수에 대한 시간 값을 입력할 때 밀리초 단위로 값을 입력합니다. 예: 10000밀리초 = 10초, 3600000밀리초 = 60분 = 1시간.

사전 요구 사항

IaaS Manager Service를 호스팅하는 서버에 관리자 로 로그인합니다. 분산 설치의 경우 이 서버는 Manager Service가 설치된 서버입니다.

절차

- 1 편집기에서 `ManagerService.exe.config` 파일을 엽니다. 이 파일은 vRealize Automation 서버 설치 디렉토리(일반적으로 `%SystemDrive%\Program Files x86\VMware\VCAC\Server`)에 있습니다.
- 2 원하는 대로 다음 변수를 업데이트합니다.

매개 변수	설명
<code>RepositoryWorkflowTimerCallbackMiliSeconds</code>	작업을 위해 저장소 서비스 또는 Model Manager Web 서비스를 확인합니다. 기본 값은 10000입니다.
<code>ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds</code>	만료된 시스템 리스를 확인합니다. 기본 값은 3600000입니다.
<code>BulkRequestWorkflowTimerCallbackMiliSeconds</code>	대량 요청을 확인합니다. 기본 값은 10000입니다.
<code>MachineRequestTimerCallbackMiliSeconds</code>	시스템 요청을 확인합니다. 기본 값은 10000입니다.
<code>MachineWorkflowCreationTimerCallbackMiliSeconds</code>	새 시스템을 확인합니다. 기본 값은 10000입니다.

3 파일을 저장한 후 닫습니다.

4 시작 > 관리 도구 > 서비스를 선택합니다.

5 vCloud Automation Center 서비스를 중지한 후 다시 시작합니다.

- 6 (선택 사항) vRealize Automation가 고가용성 모드에서 실행되고 있는 경우 설치 후 **ManagerService.exe.config** 파일에서 변경된 내용 모두가 기본 서버와 페일오버 서버 둘 다에 적용되어야 합니다.

IaaS 로그 설정 조정

Manager Service 로그에서 보려는 정보만 로깅하도록 vRealize Automation을 조정할 수 있습니다.

vRealize Automation을 고가용성 모드에서 실행 중일 때 설치 후의 **ManagerService.exe.config** 파일을 변경하려면 기본 및 페일오버 vRealize Automation Server에서 이 파일 변경을 수행해야 합니다.

절차

- 1 관리자 액세스 권한이 있는 자격 증명을 사용하여 vRealize Automation Server에 로그인합니다.
- 2 %SystemDrive%\Program Files x86\VMware\vCAC\Server 또는 vRealize Automation Server 설치 디렉토리(위치가 다른 경우)에서 **ManagerService.exe.config** 파일을 편집합니다.
- 3 **RepositoryLogSeverity** 및 **RepositoryLogCategory** 키를 편집하여 로그 파일에 기록될 이벤트의 유형을 구성합니다.

옵션	설명
RepositoryLogSeverity	<p>심각도 수준을 지정합니다. 이 심각도 수준보다 낮은 심각도의 이벤트는 무시됩니다.</p> <ul style="list-style-type: none"> ■ 오류는 복구할 수 있는 오류와 그 이상만 로깅합니다. ■ 경고는 심각하지 않은 경고와 그 이상을 로깅합니다. ■ 정보는 모든 정보 메시지와 그 이상을 로깅합니다. ■ 세부 정보 표시는 디버깅 추적을 로깅하며 성능을 저하시킬 수 있습니다. <p>예: <add key="RepositoryLogSeverity" value="Warning" /></p>
RepositoryLogCategory	<p>심각도와 관계없이 해당 범주의 모든 이벤트를 로깅하는 범주를 지정합니다. 예를 들어, <add key="RepositoryLogCategory" value="MissingMachines,UnregisteredMachines,AcceptMachineRequest,RejectMachineRequest" />는 누락된 또는 등록되지 않은 시스템 그리고 수락 또는 거부된 모든 시스템 요청에 대한 모든 이벤트를 로깅합니다.</p>

- 4 파일을 저장한 후 닫습니다.
- 5 **시작 > 관리 도구 > 서비스**를 선택하고 vCloud Automation Center 서비스를 다시 시작합니다.

결과

Manager Service 설치 시스템에서 %SystemDrive%\Program Files (x86)\VMware\vCAC\Server\Logs 위치 또는 vRealize Automation 서버 설치 디렉토리(Manager Service를 다른 위치에 설치한 경우)에 있는 Manager Service 로그 파일을 확인하여 변경 내용이 로깅에 어떻게 영향을 미치는지 볼 수 있습니다.

vRealize Automation 모니터링

역할에 따라 워크플로 또는 서비스를 모니터링하거나, 이벤트 또는 감사 로그를 보거나, 분산 배포의 모든 호스트에 대한 로그를 수집할 수 있습니다.

워크플로 모니터링 및 로그 보기

자신의 역할에 따라 워크플로를 모니터링하고 작업 로그를 볼 수 있습니다.

표 1-12. 모니터링 및 로그 표시 옵션

목표	역할	메뉴 시퀀스 및 설명
발생한 작업에 대한 정보(예: 작업 종류, 작업의 날짜와 시간 등)를 표시합니다.	IaaS 관리자	기본 로그 정보를 표시하거나, 열 및 필터 옵션을 사용하여 표시 콘텐츠를 제어합니다. 인프라 > 모니터링 > 감사 로그 를 선택합니다. 감사 로그는 관리되는 가상 시스템의 상태 및 재구성 중 이러한 시스템에 수행된 작업에 대한 세부 정보를 제공합니다. 로그에는 시스템 프로비저닝, NSX, 회수 및 재구성 작업에 대한 정보가 포함됩니다.
예약 및 사용 가능한 Distributed Execution Manager와 기타 워크플로의 상태를 봅니다.	IaaS 관리자	워크플로 상태를 보고, 필요한 경우 특정 워크플로를 열어 해당하는 세부 정보를 표시합니다. 인프라 > 모니터링 > DEM 상태 를 선택합니다.
로그 데이터를 보고, 필요한 경우 내보냅니다.	IaaS 관리자	기본 로그 정보를 표시하거나, 열 및 필터 옵션을 사용하여 표시 콘텐츠를 제어합니다. 인프라 > 모니터링 > 로그 를 선택합니다.
실행된 Distributed Execution Manager 및 기타 워크플로의 상태와 기록을 봅니다.	IaaS 관리자	워크플로 기록을 표시하고, 필요한 경우 특정 워크플로를 열어 해당하는 실행 세부 정보를 표시합니다. 인프라 > 모니터링 > 워크플로 기록 을 선택합니다.
이벤트 유형, 시간, 사용자 ID 등을 포함한 이벤트 목록을 표시하고, 필요한 경우 이벤트 세부 정보 페이지를 표시합니다.	시스템 관리자	이벤트 및 이와 관련된 특성(예: 실행 시간, 이벤트 설명, 테넌트 이름, 대상 유형과 ID를 비롯한 기타 특성)의 목록을 봅니다. 관리 > 이벤트 > 이벤트 로그 를 선택합니다.
요청의 상태를 모니터링하고 요청 세부 정보를 봅니다.	테넌트 관리자 또는 비즈니스 그룹 관리자	자신이 책임지고 있거나 소유하고 있는 요청의 상태를 표시합니다. 요청 을 클릭합니다.
최근 이벤트에 대한 정보를 봅니다.	IaaS 관리자 또는 테넌트 관리자	현재 로그인된 사용자에게 대한 최근 이벤트를 표시합니다. 인프라 > 최근 이벤트 를 선택합니다.

이벤트 로그 및 서비스 모니터링

vRealize Automation 이벤트 로그 및 서비스를 모니터링하여 그 현재 상태와 기록 상태 확인할 수 있습니다.

이벤트 로그의 기본 보존 기간은 90일입니다. 이 기간은 `/etc/vcac/vcac.properties` 파일에서 변경할 수 있습니다.

데이터 롤오버 설정 사용자 지정을 통한 로그 지우기에 대한 자세한 내용은 "vRealize Automation 구성" 항목을 참조하십시오.

vRealize Automation 서비스

시스템 관리자는 시스템 관리자 콘솔의 이벤트 로그에서 vRealize Automation 서비스의 상태를 볼 수 있습니다.

서비스의 하위 집합은 개별 제품 구성 요소를 실행해야 합니다. 예를 들어 테넌트를 구성할 수 있으려면 먼저 ID 서비스와 UI 코어 서비스를 실행해야 합니다.

다음 테이블은 vRealize Automation 기능 영역과 연결된 서비스를 보여 줍니다.

표 1-13. ID 서비스 그룹

서비스	설명
management-service	ID 서비스 그룹
sts-service	Single Sign-On 장치
authorization	권한 부여 서비스
인증	인증
eventlog-service	이벤트 로그 서비스
licensing-service	라이선싱 서비스

표 1-14. UI 코어 서비스

서비스	설명
shel-ui-app	셸 서비스
branding-service	브랜딩 서비스
plugin-service	확장성(플러그인) 서비스
portal-service	포털 서비스

다음 서비스는 모두 IaaS 구성 요소를 실행해야 합니다.

표 1-15. 서비스 카탈로그 그룹(거버넌스 서비스)

서비스	설명
notification-service	알림 서비스
workitem-service	작업 항목 서비스
approval-service	승인 서비스
catalog-service	서비스 카탈로그

표 1-16. IaaS 서비스 그룹

서비스	설명
iaas-proxy-provider	IaaS 프록시
iaas-server	IaaS Windows 시스템

표 1-17. XaaS

서비스	설명
vco	vRealize Orchestrator
advanced-designer-service	XaaS Blueprint 및 리소스 작업

vRealize Automation 감사 로깅 사용

vRealize Automation은 중요 시스템 이벤트의 수집 및 보존을 지원하는 감사 로깅을 제공합니다.

현재 vRealize Automation은 이벤트 로깅의 확장 기능으로 감사 로깅을 지원합니다. 이 기능은 기본 감사 정보를 제공하며, 보존 설정은 적절한 vRealize Automation REST API 이벤트 브로커 서비스 호출을 사용해서만 구성할 수 있습니다. 현재 감사 로깅은 테넌트에 로그인할 수 있는 테넌트 관리자와 시스템 관리자가 사용할 수 있으며, 이벤트에 대한 검색 및 필터 기능을 제공합니다.

기본적으로 vRealize Automation은 워크플로 구독, 끝점 및 패브릭 그룹 생성, 업데이트 및 삭제 이벤트에 대한 감사 로깅을 지원합니다. 또한 vRealize Automation은 다양한 IaaS 이벤트에 대한 감사 로깅 사용자 지정도 지원합니다.

vRealize Automation 감사 로깅은 기본적으로 비활성화됩니다. 가상 장치 관리 인터페이스의 **vRA > 로그** 페이지에 있는 [감사 로그 통합] 섹션에서 **사용** 확인란을 전환하여 기능을 설정하거나 해제할 수 있습니다.

감사 로그 정보는 표준 [이벤트 로그] 페이지에 나타납니다. 테넌트 관리자인 경우 이 페이지를 보려면 **관리 > 이벤트 로그**를 선택합니다. 감사 이벤트는 이벤트 로그 테이블에서 [이벤트 유형] 필드의 [감사] 지정으로 식별됩니다. 각 항목은 각 이벤트에 대한 이벤트 설명을 비롯하여 테넌트, 시간, 사용자 및 관련된 서비스 이름을 표시합니다.

기타 IaaS 이벤트에 대해 감사 로깅을 사용하도록 설정하려면 사용자 지정 구성 파일이 필요하며 IaaS 호스트 시스템에서 적절한 명령을 실행해야 합니다. 지원이 필요한 경우 VMware 전문가 서비스에 문의하십시오.

이벤트를 외부 Syslog 서버, 특히 VMware Log Insight로 내보내도록 vRealize Automation을 구성할 수 있습니다.

Log Insight 감사 로깅을 위한 vRealize Automation 구성

감사 이벤트를 편리하게 볼 수 있도록 감사 이벤트를 VMware Log Insight로 내보내도록 vRealize Automation을 구성할 수 있습니다.

감사 로깅은 기본적으로 비활성화되어 있으므로 감사 로깅 이벤트를 생성하고 보려면 사용하도록 설정해야 합니다.

사용하는 경우 SSL이 Log Insight 에이전트가 상주하는 vRealize Automation 장치에 구성되고 Log Insight Syslog 서버에 대한 연결을 고려합니다. SSL을 사용하려면 vRealize Automation과 배포에 설치된 Log Insight 서버 간에 적절한 인증서 및 연결을 구성해야 합니다.

사전 요구 사항

vRealize Automation은 vRealize Automation 배포에 기본적으로 설치된 Log Insight 에이전트를 사용하여 Log Insight에서 볼 수 있도록 로그 항목을 읽습니다.

절차

- 1 가상 장치 관리 인터페이스에 시스템 관리자로 로그인합니다.
- 2 **vRA > 로그**를 선택합니다.
- 3 [감사 로그 통합] 머리글 아래에 감사 로깅에 대해 **사용** 확인란이 선택되어 있는지 확인합니다.
- 4 [Log Insight 에이전트 구성] 머리글 아래에 Log Insight 서버의 **호스트** 시스템 이름을 입력합니다.
 - a Log Insight 에이전트의 **호스트** 시스템 이름을 입력합니다.
 - b Log Insight 에이전트와의 통신에 사용할 **포트**를 입력합니다.
 - c 적절한 통신 프로토콜을 선택합니다.
 - d **SSL 사용** 확인란을 사용하여 SSL을 Log Insight 에이전트와 서버 간의 통신에 사용할지 여부를 지정합니다.

SSL을 사용하지 않도록 선택하면 페이지의 나머지 설정을 무시할 수 있습니다. SSL을 사용하는 경우 이러한 설정을 구성해야 합니다.

- 5 SSL을 사용하는 경우 [SSL 신뢰할 수 있는 루트 인증서] 섹션에서 적절한 선택을 하십시오.

기본적으로 vRealize Automation 장치는 자체 서명된 인증서를 사용합니다. 신뢰할 수 있는 루트 인증서를 사용하려는 경우 가져와야 합니다.

- a 새 인증서를 사용할지 또는 기존 인증서를 사용할지를 나타내는 적절한 확인란을 선택합니다.

자세한 내용은 가상 장치 관리 인터페이스의 [vRealize Automation 로깅 구성] 페이지의 참고 사항을 참조하십시오.

- 6 **설정 저장**을 클릭합니다.
- 7 [SSL 서버 인증서] 섹션에서 적절한 선택을 하십시오.
- 8 [에이전트 동작 구성] 섹션을 사용하여 에이전트가 로그 파일과 작동하는 방식을 구성합니다.

결과

vRealize Automation 감사 로그 이벤트가 Log Insight 인터페이스에 표시됩니다.

분산 배포의 클러스터에 대한 호스트 정보 보기

분산 배포에 클러스터된 모든 노드에 대한 로그를 vRealize Automation 장치 관리 콘솔에서 수집할 수 있습니다.

배포 환경 내의 각 호스트에 대한 정보를 볼 수도 있습니다. vRealize Automation 관리 콘솔의 **클러스터** 탭에는 다음과 같은 정보를 표시하는 분산 배포 정보 테이블이 포함되어 있습니다.

- 배포에 포함된 모든 노드의 목록
- 노드의 호스트 이름. 호스트 이름은 정규화된 도메인 이름으로 지정됨
- 호스트가 관리 콘솔에 마지막으로 응답한 후 경과한 시간. IaaS 구성 요소의 노드는 3분마다 가용성을 보고하고, 가상 장치 노드는 9분마다 가용성을 보고합니다.
- vRealize Automation 구성 요소 유형. 노드가 가상 장치인지 IaaS 서버인지 식별합니다.

그림 1-1. 분산 배포 정보 테이블

	Host / Node Name	Version	Last Connected	Type	State*	Valid*
▶	cava-n-80-175.eng.vmware.com	7.5.0.378	7 minutes ago	MASTER	Up	<button>Delete</button>
▶	cava-n-85-043.eng.vmware.com	7.5.0.14528	14 seconds ago	IAAS		<button>Delete</button>

이 테이블을 사용하여 배포에서의 작업을 모니터링할 수 있습니다. 예를 들어 호스트가 최근에 연결하지 않은 것으로 [최근 연결] 열에 나타나면 호스트 서버에 문제가 있음을 의미할 수 있습니다.

로그 수집

vRA > 로그 페이지에서 [지원 번들 생성] 버튼을 사용하여 배포의 모든 호스트에 대한 로그 파일을 포함하는 zip 파일을 생성할 수 있습니다. 자세한 내용은 [클러스터 및 분산 배포에 대한 로그 수집](#) 항목을 참조하십시오.

테이블에서 노드 제거

배포에서 호스트를 제거하는 경우, 분산 배포 정보 테이블에서 해당하는 노드를 제거하여 로그 수집 시간을 최적화해야 합니다. **삭제** 버튼을 클릭하여 테이블에서 노드를 제거합니다.

클러스터 및 분산 배포에 대한 로그 수집

문제 해결 및 기록 유지 작업을 지원하기 위해 배포의 서버에 대한 모든 로그 파일을 포함하는 zip 파일을 생성할 수 있습니다.

원격 가상 장치 관리 인터페이스의 [클러스터] 탭에 있는 [분산 배포 정보] 테이블에는 로그 파일이 수집되는 노드가 나열됩니다. 이 테이블에서 노드를 삭제할 수도 있습니다.

vRealize Automation 장치 배포 구성에 대한 관련 정보는 "vRealize Automation 설치" 를 참조하십시오.

절차

- 1 가상 장치 관리 인터페이스에 시스템 관리자로 로그인합니다.
- 2 **vRA > 로그**를 클릭합니다.
- 3 **지원 번들 생성**을 클릭합니다.

각 노드에 대한 로그 파일이 수집되고 Zip 파일로 복사됩니다.

분산 배포 정보 테이블에서 노드 제거

노드를 배포 클러스터에서 제거하려는 경우나 관리 에이전트 인증서를 바꾸는 경우에는 노드를 삭제합니다.

가상 장치 관리 인터페이스의 [클러스터] 탭에 있는 [분산 배포 정보] 테이블에 해당 클러스터에 대한 노드가 나열됩니다. 테이블에서 노드의 **삭제** 버튼을 클릭하면 클러스터에서 노드를 제거하거나 다음 절차를 사용할 수 있습니다.

절차

- 1 **root**라는 사용자 이름과 장치 배포 시 지정한 암호를 사용하여 vRealize Automation 장치에 로그인합니다.
 - 2 **클러스터** 탭을 클릭합니다.
- 분산 배포 정보 테이블에 분산 배포에 대한 노드 목록이 표시됩니다.
- 3 명령 프롬프트를 열고 다음 명령을 실행하여, 삭제할 노드의 노드 ID를 찾습니다.

```
/usr/sbin/vcac-config cluster-config-node --action list
```

- 4 JSON 출력에서 노드 ID(예: `cafe.node.46686239.17144`)를 찾습니다.
- 5 명령 프롬프트를 열고, 이전 단계에서 확인한 노드 ID를 사용하여 다음 형식의 명령을 입력합니다.

```
/usr/sbin/vcac-config cluster-config-node  
--action delete --id node-UID
```

예를 들어 예제 노드 ID `cafe.node.46686239.17144`에 대해 다음 명령을 입력합니다.

```
/usr/sbin/vcac-config cluster-config-node --action delete --id cafe.node.46686239.17144
```

- 6 **새로 고침**을 클릭합니다.

노드가 화면에 더 이상 표시되지 않습니다.

vRealize Automation 상태 모니터링

vRealize Automation 상태 서비스는 vRealize Automation 환경의 기능 상태를 평가합니다.

IaaS 관리자는 구성 요소가 등록되어 있고 필수 리소스를 사용할 수 있는지 확인하는 테스트 집합을 실행하도록 상태 서비스를 구성합니다. 이 테이블에서는 상태 서비스에서 제공하는 테스트 집합과 각 집합의 일부 예제 테스트를 보여 줍니다.

상태 서비스 테스트 집합	예제 테스트
vRealize Automation에 대한 시스템 테스트	<ul style="list-style-type: none"> ■ SSO/ID VA 연결 테스트 ■ vRealize Automation 라이선스 확인 - 라이선스가 만료되었는지 여부 ■ vRealize Automation 가상 장치 루트 암호 확인 - 암호가 끝 만료 예정인지 여부
vRealize Automation에 대한 테넌트 테스트	<ul style="list-style-type: none"> ■ vSphere 예약 스토리지 경로 확인 ■ 예약 할당에 대한 예약 정책 확인 ■ 포털 서비스 상태 확인
vRealize Orchestrator에 대한 테스트	<ul style="list-style-type: none"> ■ 활성 vRO 노드 수 확인 ■ vRO 노드에서 Java 메모리 힙의 활용도 확인 ■ vRO 노드에서 vro-server 서비스의 상태 확인

가상 시스템에서 테스트 집합을 실행하면 상태 서비스가 통과하거나 실패한 테스트 수를 보고합니다. 실패한 각 테스트에 대해 상태 서비스는 다음 링크를 제공합니다.

링크	컨텐츠
원인	테스트가 실패한 이유에 대한 설명.
업데이트 적용	문제를 해결하는 데 사용할 수 있는 정보.

스케줄에 따라 테스트를 실행하거나 필요할 때만 테스트를 실행하도록 상태 서비스를 구성할 수 있습니다.

Python을 사용하여 사용자 지정 테스트를 생성할 수도 있습니다. "vRealize Automation 상태 서비스 확장 가이드" 를 참조하십시오.

상태 소비자 역할을 가진 테넌트 관리자는 담당 테넌트에 대한 테스트 결과를 볼 수 있지만 테스트를 구성하거나 실행할 수는 없습니다.

vRealize Automation에 대한 시스템 테스트 구성

IaaS 관리자는 선택된 vRealize Automation 가상 장치에서 시스템 테스트를 실행하도록 상태 서비스를 구성합니다. 이러한 테스트는 vRealize Automation 라이선스 등의 구성 요소가 등록되어 있고 메모리 등의 필수 리소스를 가상 장치에서 사용할 수 있는지 확인합니다. 시스템 테스트를 구성하면 [상태] 페이지에 테스트가 테스트 카드로 표시됩니다.

vRealize Automation에 대한 시스템 테스트를 실행하도록 상태 서비스를 구성하려면 이 절차를 완료합니다.

사전 요구 사항

IaaS 관리자로 vRealize Automation에 로그인합니다.

절차

- 1 **관리 > 상태**를 선택합니다.
- 2 **새 구성**을 클릭합니다.
- 3 [구성 세부 정보] 페이지에 요청된 정보를 입력합니다.

옵션	설명
이름	이 구성의 제목입니다. 이 제목은 테스트 카드에 표시됩니다.
설명	테스트 집합에 대한 설명입니다.
제품	vRealize Automation을 선택합니다.
스케줄	테스트 집합의 실행 간격을 선택합니다.

- 4 **다음**을 클릭합니다.
- 5 [테스트 집합 선택] 페이지에서 **vRealize Automation에 대한 시스템 테스트**를 선택합니다.
- 6 **다음**을 클릭합니다.
- 7 [매개 변수 구성] 페이지에 요청된 정보를 입력합니다.

표 1-18. vRealize Automation 가상 장치

옵션	설명
공개 웹 서버 주소	<ul style="list-style-type: none"> ■ 최소 배포의 경우 vRealize Automation 장치 호스트에 대한 기본 URL입니다. 예: <code>https://va-host.domain/</code> ■ 고가용성 배포의 경우 vRealize Automation 로드 밸런서에 대한 기본 URL입니다. 예: <code>https://load-balancer-host.domain/</code>
SSH 콘솔 주소	vRealize Automation 장치의 정규화된 도메인 이름입니다. 예: <code>va-host.domain</code>
SSH 콘솔 사용자	root
SSH 콘솔 암호	루트 암호입니다.

표 1-19. vRealize Automation 시스템 테넌트

옵션	설명
시스템 테넌트 관리자	관리자
시스템 테넌트 암호	관리자 암호입니다.

표 1-20. vRealize Automation 디스크 공간 모니터링

옵션	설명
경고 임계값 백분율	경고 테스트가 실패하기 전까지 사용된 가상 장치 디스크 공간의 허용 가능한 백분율입니다.
위험 임계값 백분율	위험 테스트가 실패하기 전까지 사용된 가상 장치 디스크 공간의 허용 가능한 백분율입니다.

8 다음을 클릭합니다.

9 [요약] 페이지에서 정보를 검토합니다.

10 완료를 클릭합니다.

선택한 스케줄에 따라 테스트가 실행됩니다.

다음에 수행할 작업

[vRealize Automation 상태 서비스 테스트 집합 결과 보기](#)

vRealize Automation에 대한 테넌트 테스트 구성

IaaS 관리자는 선택된 vRealize Automation 가상 장치에서 테넌트 테스트를 실행하도록 상태 서비스를 구성합니다. 이러한 테스트는 **software-service** 등의 테넌트 관련 구성 요소가 등록되어 있고 가상 장치에서 vSphere 가상 시스템 등의 필수 리소스를 사용할 수 있는지 확인합니다. 테넌트 테스트를 구성하면 [상태] 페이지에 테스트가 테스트 카드로 표시됩니다.

vRealize Automation에 대한 테넌트 테스트를 실행하도록 상태 서비스를 구성하려면 이 절차를 완료합니다.

사전 요구 사항

IaaS 관리자로 vRealize Automation에 로그인합니다.

절차

1 **관리 > 상태**를 선택합니다.

2 **새 구성**을 클릭합니다.

3 [구성 세부 정보] 페이지에 요청된 정보를 입력합니다.

옵션	설명
이름	이 구성의 제목입니다. 이 제목은 테스트 카드에 표시됩니다.
설명	테스트에 대한 설명입니다.
제품	vRealize Automation을 선택합니다.
스케줄	이러한 테스트의 실행 간격을 선택합니다.

4 다음을 클릭합니다.

- 5 [테스트 집합 선택] 페이지에서 **vRealize Automation에 대한 테넌트 테스트**를 선택합니다.
- 6 다음을 클릭합니다.
- 7 [매개 변수 구성] 페이지에 요청된 정보를 입력합니다.

표 1-21. vRealize Automation 가상 장치

옵션	설명
vRealize Automation 웹 주소	<ul style="list-style-type: none"> ■ 최소 배포의 경우 vRealize Automation 장치 호스트에 대한 기본 URL입니다. 예: <code>https://va-host.domain/</code> ■ 고가용성 배포의 경우 vRealize Automation 로드 밸런서에 대한 기본 URL입니다. 예: <code>https://load-balancer-host.domain/</code>
SSH 콘솔 주소	SSH 호스트의 정규화된 도메인 이름입니다. 예: <code>ssh-host.domain</code>
SSH 콘솔 사용자	root
SSH 콘솔 암호	루트의 암호입니다.
최대 서비스 응답 시간(ms)	시스템이 응답을 기다리는 최대 시간(밀리초)입니다.

표 1-22. vRealize Automation 테넌트

옵션	설명
테스트 중인 테넌트	qe
패브릭 관리자 사용자 이름	패브릭 관리자 사용자 이름입니다. 참고 모든 테스트를 실행하려면 이 패브릭 관리자에게 테넌트 관리자 및 IaaS 관리자 역할도 있어야 합니다.
패브릭 관리자 암호	패브릭 관리자의 암호입니다.

표 1-23. vRealize Automation 시스템 테넌트

옵션	설명
시스템 테넌트 관리자	관리자
시스템 테넌트 암호	관리자의 암호입니다.

표 1-24. vRealize Automation 디스크 공간 모니터링

옵션	설명
위험 임계값 백분율	위험 테스트가 실패하기 전까지 사용된 가상 장치 디스크 공간의 허용 가능한 백분율입니다.

- 8 다음을 클릭합니다.
- 9 [요약] 페이지에서 정보를 검토합니다.

10 완료

선택한 스케줄에 따라 테스트가 실행됩니다.

다음에 수행할 작업

[vRealize Automation 상태 서비스 테스트 집합 결과 보기](#)

vRealize Orchestrator에 대한 테스트 구성

IaaS 관리자는 vRealize Orchestrator 호스트에서 vRealize Orchestrator에 대한 테스트를 실행하도록 상태 서비스를 구성합니다. 이러한 테스트는 vro-server 서비스 등의 구성 요소가 등록되어 있고 호스트 시스템에서 충분한 Java 메모리 힙 등의 필수 리소스를 사용할 수 있는지 확인합니다. vRealize Orchestrator 테스트를 구성하면 [상태] 페이지에 테스트가 테스트 카드로 표시됩니다.

사전 요구 사항

IaaS 관리자로 vRealize Automation에 로그인합니다.

절차

- 1 **관리 > 상태**를 선택합니다.
- 2 **새 구성**을 클릭합니다.
- 3 [구성 세부 정보] 페이지에 요청된 정보를 입력합니다.

옵션	설명
이름	이 구성의 제목입니다. 이 제목은 테스트 카드에 표시됩니다.
설명	테스트에 대한 설명입니다.
제품	vRealize Orchestrator을 선택합니다.
스케줄	테스트의 실행 간격을 선택합니다.

- 4 **다음**을 클릭합니다.
- 5 [테스트 집합 선택] 페이지에서 **vRealize Orchestrator에 대한 테스트**를 선택합니다.
- 6 **다음**을 클릭합니다.

7 [매개 변수 구성] 페이지에 요청된 정보를 입력합니다.

표 1-25. vRealize Orchestrator 호스트/로드 밸런서

옵션	설명
클라이언트 주소	<ul style="list-style-type: none"> ■ 최소 배포의 경우 vRealize Orchestrator 호스트의 FQDN(정규화된 도메인 이름)입니다. 예: <code>vro-host.domain</code> ■ 고가용성 배포의 경우 vRealize Orchestrator 로드 밸런서에 대한 기본 URL(<code>https://load-balancer-host.domain/</code>)입니다.
클라이언트 사용자 이름	관리자
클라이언트 암호	관리자 암호입니다.
SSH 콘솔 사용자 이름	root
SSH 콘솔 암호	루트 암호입니다.
힙 활용도 임계값	경고 테스트가 실패하기 전까지 사용된 힙 공간의 허용 가능한 백분율입니다.

표 1-26. 로드 밸런서 뒤에 있는 vRealize Orchestrator 인스턴스

옵션	설명
SSH 콘솔 주소	로드 밸런서 뒤에 있는 vRealize Orchestrator 인스턴스의 IP 주소 또는 URL입니다.
SSH 콘솔 사용자 이름	이 인스턴스에 액세스할 수 있는 사용자 이름입니다.
SSH 콘솔 암호	사용자 이름의 암호입니다.

- 목록에 다른 vRealize Orchestrator 인스턴스를 추가하려면 **추가**를 클릭합니다.
- 로드 밸런서 뒤에 있는 인스턴스 목록에서 선택한 vRealize Orchestrator 인스턴스를 제거하려면 **제거**를 클릭합니다.

8 다음을 클릭합니다.

9 [요약] 페이지에서 정보를 검토합니다.

10 완료를 클릭합니다.

선택한 스케줄에 따라 테스트가 실행됩니다.

다음에 수행할 작업

[vRealize Automation 상태 서비스 테스트 집합 결과 보기](#)

사용자 지정 테스트 집합

Python을 사용하여 vRealize Automation 상태 서비스에 대한 사용자 지정 테스트 집합을 생성할 수 있습니다.

사용자 지정 테스트 집합을 생성하면 추가 vRealize Automation 구성 요소의 상태를 확인하는 테스트 집합을 추가하여 상태 서비스에 대해 제공되는 테스트를 확장할 수 있습니다. 사용자 지정 테스트 집합 생성에 대한 자세한 내용은 "vRealize Automation 상태 서비스 확장성 가이드"를 참조하십시오.

사용자 지정 테스트 집합 추가

IaaS 관리자는 사용자 지정 테스트 집합을 vRealize Automation 상태 서비스에 추가한 후에 테스트 집합을 실행해야 합니다.

vRealize Automation 자산에 대한 사용자 지정 테스트 집합을 추가하려면 이 절차를 완료합니다.

사전 요구 사항

- 사용자 지정 테스트 집합 파일에 대한 Python 휠을 생성합니다. 자세한 내용은 "vRealize Automation 상태 서비스 확장성 가이드"를 참조하십시오.
- **IaaS 관리자**로 vRealize Automation에 로그인합니다.

절차

- 1 **관리 > 상태**를 클릭합니다.
- 2 오른쪽 상단에서 톱니바퀴 아이콘을 클릭하고 **확장성**을 선택합니다.
- 3 **새 자산**을 클릭합니다.
- 4 [자산 추가] 대화상자에 요청된 정보를 입력합니다.

옵션	설명
자산 제목	실행 중인 테스트 집합의 이름 및 버전 번호입니다(예: Infoblox 1.0).
자산 설명	Python 휠에 포함된 테스트에 대한 설명입니다.
자산 버전	테스트 집합 버전 번호입니다.
자산 파일	파일 선택 을 클릭하고 사용자 지정 테스트 집합 파일을 선택합니다.

- 5 **추가**를 클릭합니다.

새 행이 업로드된 상태로 자산 테이블에 추가되었습니다. 상태가 설치됨으로 변경되면 테스트 집합을 사용할 수 있습니다. 설치 프로세스가 실패하면 이유를 제공하는 팝업이 표시됩니다.

참고 페이지가 업데이트되지 않으면 새로 고침 아이콘을 클릭합니다.

다음에 수행할 작업

[사용자 지정 테스트 집합 실행](#).

사용자 지정 테스트 집합 실행

IaaS 관리자는 vRealize Automation 환경에서 사용자 지정 테스트 집합을 실행하도록 상태 서비스를 구성합니다. 사용자 지정 테스트 집합을 구성하면 [상태] 페이지에 테스트 집합이 테스트 카드로 표시됩니다.

vRealize Automation에 대한 사용자 지정 테스트 집합을 실행하도록 상태 서비스를 구성하려면 이 절차를 완료합니다.

사전 요구 사항

- 사용자 지정 테스트 집합 추가.
- IaaS 관리자로 vRealize Automation에 로그인합니다.

절차

- 1 관리 > 상태를 선택합니다.
- 2 새 구성을 클릭합니다.
- 3 [구성 세부 정보] 페이지에 요청된 정보를 입력합니다.

옵션	설명
이름	이 구성의 제목입니다. 이 제목은 테스트 카드에 표시됩니다.
설명	테스트 집합에 대한 설명입니다.
제품	제품 드롭다운 메뉴에서 테스트할 제품을 선택합니다.
스케줄	이 테스트 집합의 실행 간격을 선택합니다.

- 4 다음을 클릭합니다.
- 5 [테스트 집합 선택] 페이지에서 사용자 지정 테스트 집합을 선택하고 다음을 클릭합니다.
- 6 [매개 변수 구성] 페이지에 요청된 정보를 입력하고 다음을 클릭합니다.
- 7 [요약] 페이지에서 정보를 검토하고 완료를 클릭합니다.

선택한 스케줄에 따라 사용자 지정 테스트 집합이 실행됩니다.

다음에 수행할 작업

[vRealize Automation 상태 서비스 테스트 집합 결과 보기](#)

vRealize Automation 상태 서비스 테스트 집합 결과 보기

테스트를 실행한 후 상태 서비스 테스트 결과를 볼 수 있습니다.

구성된 각 테스트 집합이 [상태] 페이지에 테스트 카드로 표시됩니다. 테스트 집합이 실행되면 테스트 카드 가운데에 결과가 표시됩니다.

[상태] 페이지에 표시되는 테스트 카드는 사용자의 권한에 따라 필터링됩니다.

- IaaS 관리자는 모든 테스트 카드를 볼 수 있습니다.

- 상태 소비자 역할을 가진 테넌트 관리자는 자신이 담당하는 테넌트의 테스트 카드만 볼 수 있습니다.

사전 요구 사항

- 구성된 테스트 집합에 실행 중인 스케줄이 있습니다.
- **IaaS 관리자** 또는 **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

절차

- 1 **관리 > 상태**를 선택합니다.
- 2 테스트가 실행되도록 스케줄링되지 않은 경우 테스트 카드에서 **실행**을 클릭합니다.
- 3 테스트가 완료된 후 테스트 카드의 가운데를 클릭합니다.

각 테스트의 상태를 표시하는 페이지가 표시됩니다. 테스트가 실패한 이유를 보려면 **원인**을 클릭합니다. 문제를 해결하는 방법을 설명하는 항목을 열려면 사용 가능한 **업데이트 적용** 링크(있는 경우)를 클릭합니다.

상태 서비스 문제 해결

상태 서비스 문제 해결 항목에서는 상태 서비스를 사용할 때 발생할 수 있는 문제에 대한 해결 방법을 제공합니다.

서비스 상태 테스트 실패

실패한 서비스 테스트는 테스트 스케줄 설정을 변경하여 수정할 수 있습니다.

문제

서비스 상태 테스트가 실패한 경우 **원인**을 클릭하면 **SSH** 연결을 설정할 수 없습니다. 예외 메시지: **[Auth fail]** 메시지가 표시됩니다.

원인

15분마다 실행되도록 테스트 집합이 스케줄링된 경우, 시스템 로그인은 루트 사용자 계정에 잠금을 설정합니다.

해결책

- ◆ 테스트 스케줄을 **없음**으로 변경하고 15분 동안 기다린 후 테스트 집합을 다시 실행합니다.

업그레이드 후 장치 콘솔의 [상태] 페이지가 비어 있음

vRealize Automation 업그레이드 후 장치 콘솔의 [상태] 페이지가 비어 있습니다.

문제

업그레이드 후 상태 서비스가 시작되지 않습니다.

해결책

- ◆ 각 vRealize Automation 가상 장치에서 **root**로 명령 프롬프트를 열고 다음 명령을 실행합니다.

- a 자동으로 시작되도록 상태 서비스를 구성하려면 이 명령을 실행합니다.

```
chkconfig vrhb-service on
```

- b 이 가상 장치에서 상태 서비스를 시작하려면 이 명령을 실행합니다.

```
service vrhb-service start
```

SNMP를 사용하여 vRealize Automation 환경 리소스 모니터링

SNMP에 익숙한 시스템 관리자는 vSNMP용 vRealize Automation REST API를 사용하여 vRealize Automation 노드를 모니터링하는 방식을 개선할 수 있습니다. vSNMP를 사용하면 vRealize Automation에서 CPU, RAM, 디스크 공간이 부족해지려고 하면 SNMP를 사용하여 암호화된 조기 주의 시스템으로 작동하여 성능 저하를 방지할 수 있습니다.

SNMP OID를 수동으로 모니터링하거나 SNMP 트랩을 설정하여 리소스를 활발하게 모니터링할 수 있습니다.

예를 들어 vSNMP가 이벤트(예: "높은 CPU 사용량이 감지됨")를 전송하면 CPU를 사용하는 프로세스에 대한 정보 수집을 시작하고 과도한 리소스를 사용하는 프로세스를 확인할 수 있습니다. 그런 다음 CPU, 메모리 및 기타 사용량의 연관성을 확인하여 추가적인 문제를 해결할 수 있습니다.

vRealize Automation vSNMP를 사용하면 vRealize Automation 인스턴스에서 실행되는 vSNMPD 데몬을 사용하거나 REST API를 사용하여 데이터를 모니터링하고 검색하기 위해 전체 Linux 트리를 노출할 수 있습니다.

vRealize Automation SNMP에는 일반적인 사용 인터페이스가 없습니다. REST API 또는 데몬 명령을 사용해야 합니다.

자세한 내용은 vRealize Automation 프로그래밍 가이드에서 "SNMP를 사용하여 vRealize Automation 모니터링"을 참조하십시오. 프로그래밍 가이드를 찾으려면 [vRealize Automation API 설명서](#)를 참조하고 버전 링크를 선택하십시오.

리소스 모니터링 및 관리

vRealize Automation 역할마다 리소스 사용량을 모니터링하고 인프라를 관리하는 방법이 서로 다릅니다.

리소스 모니터링 선택 시나리오

패브릭 관리자, 테넌트 관리자 및 비즈니스 그룹 관리자가 리소스 모니터링과 관련하여 관심을 기울이는 사항은 서로 다릅니다. 이에 따라 vRealize Automation은 리소스 사용량의 다양한 패킷을 모니터링할 수 있게 합니다.

예를 들어 패브릭 관리자는 예약 및 계산 리소스의 리소스 사용 모니터링에 관심을 기울이지만, 테넌트 관리자는 테넌트 내 프로비저닝 그룹의 리소스 사용량에 관심을 기울입니다. 모니터링하려는 특정 리소스 사용량 및 역할에 따라 vRealize Automation는 리소스 사용을 추적하는 여러 방법을 허용합니다.

표 1-27. 리소스 모니터링 선택 시나리오

리소스 모니터링 시나리오	필요한 권한	위치
현재 사용되고 있는 계산 리소스에서 물리적 스토리지 및 메모리의 양을 모니터링하고 사용 가능한 상태로 유지되는 양을 확인합니다. 또한 각 계산 리소스에서 프로비저닝된 예약되고 할당된 시스템 수를 모니터링할 수 있습니다.	패브릭 관리자 (패브릭 그룹에서 계산 리소스의 리소스 사용량 모니터링)	인프라 > 계산 리소스 > 계산 리소스
현재 프로비저닝되고 vRealize Automation 관리 아래에 있는 시스템을 모니터링합니다.	패브릭 관리자	인프라 > 시스템 > 관리되는 시스템
현재 할당된 예약의 시스템 할당량, 메모리 및 스토리지의 양을 모니터링하고 예약에 사용 가능한 상태로 유지되는 용량을 확인합니다.	패브릭 관리자 (계산 리소스 및 물리적 시스템에서 예약에 대한 리소스 사용량 모니터링)	인프라 > 예약 > 예약
비즈니스 그룹이 현재 사용하고 있는 시스템 할당량, 메모리 및 스토리지의 양을 모니터링하고 이러한 그룹을 위해 예약된 상태로 유지되는 용량을 확인합니다.	<ul style="list-style-type: none"> ■ 테넌트 관리자(테넌트의 모든 그룹에 대한 리소스 사용량 모니터링) ■ 비즈니스 그룹 관리자(관리하는 그룹에 대한 리소스 사용량 모니터링) 	관리 > 사용자 및 그룹 > 비즈니스 그룹

리소스 사용량 용어

vRealize Automation에서는 사용할 수 있는 리소스, 특정 용도를 위해 구분해 둔 리소스 및 프로비저닝된 시스템에서 현재 사용 중인 리소스를 서로 구분하기 위한 명시적인 용어가 사용됩니다.

리소스 사용량 용어 표에서는 vRealize Automation에서 리소스 사용량을 표시하기 위해 사용되는 용어에 대해 설명합니다.

표 1-28. 리소스 사용량 용어

용어	설명
물리적	계산 리소스의 실제 메모리 또는 스토리지 용량을 나타냅니다.
예약됨	예약을 위해 구분해 둔 시스템 할당량, 메모리 및 스토리지 용량을 나타냅니다. 예를 들어 계산 리소스의 물리적 용량이 600GB이고 100GB씩 세 개의 예약이 있는 경우 계산 리소스의 예약된 스토리지는 300GB이고 예약된 스토리지는 50%입니다.
관리됨	시스템이 프로비저닝되었고 현재 vRealize Automation에서 관리됨을 나타냅니다.
할당됨	프로비저닝된 시스템에서 현재 사용 중인 시스템 할당량, 메모리 또는 스토리지 리소스를 나타냅니다. 예를 들어 시스템 할당량이 10인 예약이 있다고 가정해 보겠습니다. 프로비저닝된 시스템이 15개이고 그 중 6개의 전원만 현재 켜져 있는 경우, 할당된 시스템 할당량은 60%입니다.

표 1-28. 리소스 사용량 용어 (계속)

용어	설명
사용됨	사용됨 열 값은 항상 할당됨 열 값과 같습니다.
사용 가능	스토리지 경로에서 사용되지 않은 물리적 용량을 나타냅니다.

클라우드 시스템에 연결

클라우드 시스템에 처음 연결하는 때에는 관리자로 로그인해야 합니다.

그런 다음 vRealize Automation 콘솔에 시스템의 사용자로 로그인할 때 사용할 자격 증명을 추가하고 해당 시점부터 vRealize Automation 자격 증명으로 로그인합니다.

중요 Amazon Web Services를 사용하는 경우 Amazon 시스템 인스턴스에서 RDP나 SSH를 사용하도록 설정해야 하며 시스템이 올바른 포트가 열려 있는 보안 그룹에 속해 있어야 합니다.

Amazon 시스템에 대한 사용자 자격 증명 수집

Amazon 시스템에 관리자로 로그인하려면 시스템의 관리자 암호를 알아야 합니다.

관리자 암호는 [시스템 세부 정보] 페이지에 있습니다. 시스템 프로비저닝에 사용된 Amazon 시스템 이미지가 부팅할 때마다 관리자 암호를 생성하도록 구성되어 있지 않은 경우 대체 기술을 사용하여 암호를 찾아야 합니다. 다른 방법으로 관리자 암호를 가져오는 것에 대한 자세한 내용은 Amazon 설명서에서 *Amazon EC2 인스턴스에 연결(Connect to Your Amazon EC2 Instance)* 항목을 검색하십시오.

필요한 경우 vRealize Automation 사용자 자격 증명을 생성할 수 있습니다. 이러한 사용자 자격 증명은 해당 시스템에 대한 후속 로그인에 유효합니다.

사전 요구 사항

- Amazon 시스템이 이미 프로비저닝되어 있어야 합니다.
- 시스템 소유자, **비즈니스 그룹 관리자** 또는 **지원 사용자**로 vRealize Automation에 로그인합니다.
- 프로비저닝에 사용될 Amazon 시스템 이미지에서 RDP 또는 SSH가 활성화되어 있어야 합니다.
- 시스템이 보안 그룹에 속해 있고 올바른 포트가 열려 있어야 합니다.

절차

- 1 **항목** 페이지로 이동하고 관리하는 그룹 또는 특정 그룹으로 필터링합니다.
- 2 시스템 목록에서 Amazon 시스템을 선택합니다.

작업 드롭다운 메뉴에서 **세부 정보 보기**를 클릭하여 시스템 유형과 같은 세부 정보를 표시할 수 있습니다.

- 3 **작업** 드롭다운 메뉴에서 **편집**을 선택합니다.

- 4 **관리자 암호 표시**를 클릭하여 시스템의 관리자 암호를 가져옵니다.

아니면 외부 Amazon 절차를 사용하여 암호를 가져올 수도 있습니다.

- 5 **작업** 드롭다운 메뉴에서 **RDP를 사용하여 연결**을 클릭합니다.
- 6 로그인 자격 증명을 묻는 메시지가 나타나면 **다른 계정 사용**을 클릭합니다.
- 7 사용자 이름을 묻는 메시지가 나타나면 **LOCAL\Administrator**를 입력합니다.
- 8 암호를 묻으면 관리자 암호를 입력합니다.
- 9 **확인**을 클릭합니다.

이제 관리자로 시스템에 로그인했습니다.

- 10 필요에 따라 vRealize Automation 자격 증명을 추가합니다. 예를 들어 Windows Server 시스템의 경우 Server Manager를 열고 **구성 > 로컬 사용자 및 그룹**을 선택하고 **DOMAIN\username** 형식으로 자격 증명을 **원격 데스크톱 사용자** 그룹에 추가합니다.

이제 vRealize Automation 사용자 이름과 암호는 이 시스템에 대한 후속 로그인에 유효한 자격 증명 이 되었습니다.

- 11 Amazon 시스템에서 로그아웃합니다.
- 12 **작업** 드롭다운 메뉴에서 **RDP를 사용하여 연결**을 클릭합니다.
- 13 로그인을 묻는 메시지가 나타나면 vRealize Automation 사용자 이름 및 암호 자격 증명을 사용하여 시스템에 로그인합니다.

결과

시스템 소유자는 이제 vRealize Automation 자격 증명을 사용하여 시스템에 로그인할 수 있습니다.

vCloud 시스템에 대한 사용자 자격 증명 수집

vCloud Air 또는 vCloud Director 시스템에 관리자로 로그인하려면 시스템의 관리자 암호를 알아야 합니다.

관리자 암호는 [시스템 세부 정보] 페이지에 있습니다. 시스템 프로비저닝에 사용된 시스템 이미지가 부팅 할 때마다 관리자 암호를 생성하도록 구성되어 있지 않은 경우 대체 기술을 사용하여 암호를 찾을 수 있습니다. 관리자 암호를 가져올 수 있는 다른 방법에 대한 자세한 내용은 vCloud Air 또는 vCloud Director 설명서를 참조하십시오.

필요한 경우 vRealize Automation 사용자 자격 증명을 생성할 수 있습니다. 이러한 사용자 자격 증명은 해당 시스템에 대한 후속 로그인에 유효합니다.

사전 요구 사항

- vCloud Air 또는 vCloud Director 시스템이 이미 프로비저닝되어 있어야 합니다.
- 시스템 소유자, **비즈니스 그룹 관리자** 또는 **지원 사용자**로 vRealize Automation에 로그인합니다.
- 프로비저닝에 사용될 vCloud Air 또는 vCloud Director 시스템 이미지에서 RDP 또는 SSH가 활성화 되어 있어야 합니다.
- 시스템이 보안 그룹에 속해 있고 올바른 포트가 열려 있어야 합니다.

절차

- 1 항목 페이지로 이동하고 관리하는 그룹 또는 특정 그룹으로 필터링합니다.
- 2 시스템 목록에서 vCloud Air 또는 vCloud Director 시스템을 선택합니다.
작업 드롭다운 메뉴에서 **세부 정보 보기**를 클릭하여 시스템 유형과 같은 세부 정보를 표시할 수 있습니다.
- 3 작업 드롭다운 메뉴에서 **편집**을 선택합니다.
- 4 관리자 암호 표시를 클릭하여 시스템의 관리자 암호를 가져옵니다.
아니면 외부 vCloud Air 또는 vCloud Director 절차를 사용하여 암호를 가져올 수도 있습니다.
- 5 작업 드롭다운 메뉴에서 **RDP를 사용하여 연결**을 클릭합니다.
- 6 로그인 자격 증명을 묻는 메시지가 나타나면 **다른 계정 사용**을 클릭합니다.
- 7 사용자 이름을 묻는 메시지가 나타나면 **LOCAL\Administrator**를 입력합니다.
- 8 암호를 물으면 관리자 암호를 입력합니다.
- 9 **확인**을 클릭합니다.
이제 관리자로 시스템에 로그인했습니다.
- 10 필요에 따라 vRealize Automation 자격 증명을 추가합니다. 예를 들어 Windows Server 시스템의 경우 Server Manager를 열고 **구성 > 로컬 사용자 및 그룹**을 선택하고 **DOMAIN\username** 형식으로 자격 증명을 **원격 데스크톱 사용자** 그룹에 추가합니다.
이제 vRealize Automation 사용자 이름과 암호는 이 시스템에 대한 후속 로그인에 유효한 자격 증명 이 되었습니다.
- 11 vCloud Air 또는 vCloud Director 시스템에서 로그아웃합니다.
- 12 작업 드롭다운 메뉴에서 **RDP를 사용하여 연결**을 클릭합니다.
- 13 로그인을 묻는 메시지가 나타나면 vRealize Automation 사용자 이름 및 암호 자격 증명을 사용하여 시스템에 로그인합니다.

결과

시스템 소유자는 이제 vRealize Automation 자격 증명을 사용하여 시스템에 로그인할 수 있습니다.

소모를 통해 예약 사용률 줄이기

패브릭 관리자는 예약 및 해당 예약에 프로비저닝된 기존 시스템은 활성 상태로 유지하면서 장기간에 걸쳐 특정 예약의 시스템 수를 줄일 수 있습니다.

가상 예약의 예약된 시스템 할당량, 메모리 및 스토리지를 현재 할당된 양보다 적게 줄일 수 있습니다. 이렇게 하면 기존 시스템은 변함 없이 그대로 관리하는 동시에, 새로 예약된 양 미만으로 할당량이 떨어질 때까지 새로운 시스템이 프로비저닝되지 않도록 방지할 수 있습니다.

참고 전원이 꺼진 가상 시스템은 총 시스템 할당량 및 할당된 메모리에 포함되지 않기 때문에 예약의 메모리 또는 시스템 할당을 줄이면 현재 전원이 꺼져 있는 시스템의 전원을 다시 켜지 못할 수 있습니다.

예를 들어 비즈니스 그룹에 대해 90일 이후 만료되도록 설정된 20개의 프로비저닝된 시스템을 포함하는 예약이 있다고 가정해 보겠습니다. 소모를 통해 이 예약의 시스템 수를 15개 이하로 줄으려면 예약을 편집하여 시스템 할당량을 20개에서 15개로 줄일 수 있습니다. 이렇게 하면 향후 만료를 통해 예약의 시스템 수가 자연적으로 줄어들 때까지 해당 예약에 시스템을 추가적으로 프로비저닝할 수 없습니다.

스토리지 경로 서비스 해제

스토리지 경로에 대한 서비스를 해제하고 시스템을 새 경로로 이동하려는 경우에는 패브릭 관리자가 vRealize Automation의 스토리지 경로를 비활성화해야 합니다.

다음은 스토리지 경로에 대한 서비스를 해제하는 데 필요한 단계 순서의 간략한 개요입니다.

- 1 패브릭 관리자가 특정 스토리지 경로를 사용하는 모든 예약에서 해당 스토리지 경로를 비활성화합니다. [스토리지 경로 비활성화](#) 항목을 참조하십시오.
- 2 시스템을 vRealize Automation 외부의 새로운 스토리지 경로로 이동합니다.
- 3 vRealize Automation에서 자동으로 인벤토리 데이터 수집을 실행하기를 대기하거나 수동으로 인벤토리 데이터 수집을 시작합니다. [계산 리소스 데이터 수집 구성](#) 항목을 참조하십시오.

스토리지 경로 비활성화


스토리지 경로가 서비스 해제되면 패브릭 관리자가 예약에서 해당 스토리지 경로를 비활성화할 수 있습니다.

참고 스토리지 경로를 비활성화하는 각 예약에 대해, 활성화된 다른 스토리지 경로에 충분한 공간이 남아 있는지 확인하십시오.

사전 요구 사항

패브릭 관리자로 vRealize Automation에 로그인합니다.

절차

- 1 **인프라 > 예약 > 예약**을 선택합니다.
- 2 서비스 해제 중인 스토리지 경로가 사용되고 있는 예약을 가리키고 **편집**을 클릭합니다.
- 3 **리소스** 탭을 클릭합니다.
- 4 서비스 해제 중인 스토리지 경로를 찾습니다.
- 5 **편집** 아이콘()을 클릭합니다.

- 6 사용 안 함 열의 확인란을 선택하여 이 스토리지 경로를 비활성화합니다.
- 7 **저장** 아이콘(📁)을 클릭합니다.
- 8 **확인**을 클릭합니다.
- 9 서비스 해제 중인 스토리지 경로를 사용하는 모든 예약에 대해 이 절차를 반복합니다.

데이터 수집

vRealize Automation는 인프라 소스 끝점과 해당 계산 리소스에서 데이터를 수집합니다.

데이터 수집은 정기적으로 수행됩니다. 각 데이터 수집 유형에는 재정의하거나 수정할 수 있는 기본 간격이 있습니다. 각 데이터 수집 유형에는 또한 재정의하거나 수정할 수 있는 기본 시간 초과 간격이 있습니다.

IaaS 관리자는 인프라 소스 끝점에 대해 데이터 수집을 수동으로 시작할 수 있으며 패브릭 관리자는 계산 리소스에 대해 데이터 수집을 수동으로 시작할 수 있습니다.

표 1-29. 데이터 수집 유형

데이터 수집 유형	설명
인프라 소스 끝점 데이터 수집	가상화 환경을 위한 가상화 호스트, 템플릿 및 ISO 이미지에 대한 정보를 업데이트합니다. vCloud Director를 위해 가상 데이터 센터 및 템플릿을 업데이트합니다. Amazon 영역 및 Amazon 영역에 프로비저닝된 시스템을 업데이트합니다. 끝점 데이터 수집은 4시간마다 실행됩니다.
인벤토리 데이터 수집	네트워크, 스토리지 및 가상 시스템에 대한 세부 정보를 포함하여 사용 리소스가 특정 계산 리소스와 연관되어 있는 가상 시스템의 레코드를 업데이트합니다. 이 레코드에는 관리되지 않는 가상 시스템, 즉 vRealize Automation 외부에서 프로비저닝된 시스템에 대한 정보도 포함됩니다. 인벤토리 데이터 수집은 24시간마다 실행됩니다. 인벤토리 데이터 수집의 기본 시간 초과 간격은 2시간입니다.
상태 데이터 수집	인벤토리 데이터 수집을 통해 검색된 각 시스템의 전원 상태 레코드를 업데이트합니다. 상태 데이터 수집에서는 vRealize Automation에서 관리하지만 가상화 계산 리소스나 클라우드 끝점에서는 감지할 수 없는 누락된 시스템도 기록합니다. 상태 데이터 수집은 15분마다 실행됩니다. 상태 데이터 수집의 기본 시간 초과 간격은 1시간입니다.
성능 데이터 수집(vSphere 계산 리소스 전용)	인벤토리 데이터 수집을 통해 검색된 각 가상 시스템의 평균 CPU, 스토리지, 메모리 및 네트워크 사용량 레코드를 업데이트합니다. 성능 데이터 수집은 24시간마다 실행됩니다. 성능 데이터 수집의 기본 시간 초과 간격은 2시간입니다.

표 1-29. 데이터 수집 유형 (계속)

데이터 수집 유형	설명
네트워크 및 보안 인벤토리 데이터 수집(vSphere 계산 리소스 전용)	인벤토리 데이터 수집 이후에 각 시스템에 대해 보안 그룹과 로드 밸런싱에 대한 정보를 포함하여 vCloud Networking and Security 및 NSX와 관련된 네트워크 및 보안 데이터 레코드를 업데이트합니다.
WMI 데이터 수집(Windows 계산 리소스 전용)	각 Windows 시스템의 관리 데이터 레코드를 업데이트합니다. 일반적으로 Manager Service 호스트에 WMI 에이전트가 설치되어 있고 Windows 시스템에서 데이터를 수집하는 기능이 사용하도록 설정되어 있어야 합니다.

끝점 데이터 수집 수동 시작

끝점 데이터 수집은 4시간마다 자동으로 실행되지만 IaaS 관리자는 프록시 에이전트가 필요하지 않은 끝점에 대해 언제라도 수동으로 끝점 데이터 수집을 시작할 수 있습니다.

데이터 수집 페이지에서는 데이터 수집의 상태 및 기간에 대한 정보를 제공하며 새 끝점 데이터 수집을 수동으로 시작할 수 있습니다.

사전 요구 사항

IaaS 관리자로 vRealize Automation에 로그인합니다.

절차

- 1 **인프라 > 끝점 > 끝점**을 선택합니다.
- 2 데이터를 수집할 끝점 행을 클릭합니다.
- 3 사용 가능한 데이터 수집 작업을 선택합니다.

계산 리소스 데이터 수집 구성

데이터 수집을 활성화 또는 비활성화하거나 데이터 수집 빈도를 구성하거나 데이터 수집을 수동으로 요청할 수 있습니다.

데이터 수집 페이지에서는 데이터 수집의 상태 및 기간에 대한 정보를 제공합니다. 또한 이 페이지에서는 계산 리소스에 대한 데이터 수집을 구성할 수도 있습니다.

사전 요구 사항

패브릭 관리자로 vRealize Automation에 로그인합니다.

절차

- 1 **인프라 > 계산 리소스 > 계산 리소스**를 선택합니다.
- 2 데이터 수집을 구성할 계산 리소스를 가리키고 **데이터 수집**을 클릭합니다.
- 3 **계산 리소스** 데이터 수집 규칙을 구성합니다.
 - 데이터 수집을 활성화하려면 **켜짐**을 선택합니다.

- 데이터 수집을 비활성화하려면 **꺼짐**을 선택합니다.

4 인벤토리 데이터 수집을 구성합니다.

- 데이터 수집을 활성화하려면 **켜짐**을 선택합니다.
- 데이터 수집을 비활성화하려면 **꺼짐**을 선택합니다.
- **빈도** 텍스트 상자에 숫자를 입력하여 인벤토리 데이터 수집 사이의 시간 간격(시간)을 구성합니다.
- **지금 요청**을 클릭하여 수동으로 데이터 수집을 시작합니다.

5 상태 데이터 수집을 구성합니다.

- 데이터 수집을 활성화하려면 **켜짐**을 선택합니다.
- 데이터 수집을 비활성화하려면 **꺼짐**을 선택합니다.
- **빈도** 텍스트 상자에 숫자를 입력하여 상태 데이터 수집 사이의 시간 간격(분)을 구성합니다.
- **지금 요청**을 클릭하여 수동으로 데이터 수집을 시작합니다.

6 성능 데이터 수집을 구성합니다.

이 옵션은 vSphere 통합에 대해서만 사용할 수 있습니다.

- 데이터 수집을 활성화하려면 **켜짐**을 선택합니다.
- 데이터 수집을 비활성화하려면 **꺼짐**을 선택합니다.
- **빈도** 텍스트 상자에 숫자를 입력하여 성능 데이터 수집 사이의 시간 간격(시간)을 구성합니다.
- **지금 요청**을 클릭하여 수동으로 데이터 수집을 시작합니다.

7 스냅샷 인벤토리 데이터 수집을 구성합니다.

이 옵션은 vRealize Business for Cloud에서 관리되는 계산 리소스에 대해 사용할 수 있습니다.

- 데이터 수집을 활성화하려면 **켜짐**을 선택합니다.
- 데이터 수집을 비활성화하려면 **꺼짐**을 선택합니다.
- **빈도** 텍스트 상자에 숫자를 입력하여 스냅샷 데이터 수집 사이의 시간 간격(시간)을 구성합니다.
- **지금 요청**을 클릭하여 수동으로 데이터 수집을 시작합니다.

8 확인을 클릭합니다.

모든 계산 리소스에 대한 비용 데이터 업데이트

패브릭 관리자는 vRealize Business for Cloud으로 관리되는 모든 계산 리소스에 대한 비용 정보를 수동으로 업데이트할 수 있습니다.

사전 요구 사항

패브릭 관리자로 vRealize Automation에 로그인합니다.

절차

1 인프라 > 계산 리소스 > 계산 리소스를 선택합니다.

2 비용 업데이트를 클릭합니다.

3 지금 요청을 클릭합니다.

결과

비용 업데이트가 완료되면 상태가 성공으로 바뀝니다.

vCenter Server 끝점에 대한 vSwap 할당 확인 이해

vSwap을 사용하여 대상 시스템에서 최대 크기 스왑 파일에 대한 스왑 공간 가용성을 확인할 수 있습니다. 사용자가 vRealize Automation에서 가상 시스템을 생성하거나 재구성하는 경우 vSwap 확인이 수행됩니다. vSwap 할당 확인은 vCenter Server 끝점에만 사용할 수 있습니다.

vRealize Automation 스토리지 할당은 생성 또는 재구성 요청 중에 가상 시스템 디스크를 수용하기에 충분한 여유 공간이 데이터스토어에 있는지 확인합니다. 하지만 시스템의 전원이 켜져 있는 경우, vCenter Server 끝점에서 스왑 파일을 생성하는 데 충분한 공간을 사용할 수 없으면 시스템의 전원을 켜지 못합니다. 전원 켜기 작업이 실패하는 경우 시스템에 의존하는 모든 사용자 지정도 실패합니다. 또한 시스템이 삭제될 수 있습니다. 요청의 크기에 따라 시스템의 전원이 켜져 있지 않거나 시스템이 프로비저닝 중이 아니라는 피드백이 즉각 명확하지는 않습니다.

vCenter Server 끝점에 대한 vRealize Automation 생성 및 재구성 프로세스의 일부로 최대 크기 스왑 파일에 대한 스왑 공간 가용성을 확인하여 이러한 제한을 해결하는 데 vSwap 할당 확인을 사용할 수 있습니다. vSwap 할당 확인을 사용하도록 설정하려면 시스템 구성 요소 또는 전체 Blueprint에서 사용자 지정 속성 `VirtualMachine.Storage.ReserveMemory`를 True로 설정합니다.

vSwap 할당 확인에 대해 다음과 같은 동작을 고려합니다.

- 스왑 파일은 가상 시스템이 포함된 데이터스토어에 있습니다. 전용 데이터스토어 또는 다른 데이터스토어에서 스왑 파일을 찾기 위한 대체 vCenter Server 구성은 지원되지 않습니다.
- 가상 시스템 생성 또는 재구성 시 스왑 크기가 고려됩니다. 최대 스왑 크기는 가상 시스템의 메모리 크기입니다.
- 호스트의 vRealize Automation 스토리지 예약에 대한 예약된 값은 계산 리소스의 물리적 용량을 초과해서는 안 됩니다.
- 예약 생성 시 예약된 값의 합계는 사용 가능한 스토리지 공간을 초과해서는 안 됩니다.
- vSphere의 리소스 풀 또는 호스트 수준이나 가상 시스템 수준 메모리 예약은 vSphere 끝점에서 수집되지 않으며 vRealize Automation에서 계산 중에 고려되지 않습니다.
- vSwap은 기존 시스템에 대한 전원 켜기 작업 중에 사용 가능한 스왑 공간을 검증하지 않습니다.
- 데이터 수집을 다시 실행하여 vSwap에 관하여 vSphere 끝점에서 변경된 사항을 캡처해야 합니다.

데이터 센터 위치 제거

데이터 센터 위치를 사용자 메뉴에서 제거하려면 시스템 관리자가 위치 파일에서 위치 정보를 제거하고, 패브릭 관리자가 계산 리소스에서 위치 정보를 제거해야 합니다.

예를 들어 위치 파일에 **London**을 추가하고, 이 위치에 10개의 계산 리소스를 연결한 다음 파일에서 **London**을 제거할 경우, 계산 리소스는 **London**이라는 위치에 계속 연결되어 있으며 **London**이 [시스템 요청 확인] 페이지의 위치 드롭다운 목록에도 계속 표시됩니다. 드롭다운 목록에서 이 위치를 제거하려면 패브릭 관리자가 계산 리소스를 편집하여 이 위치에 연결된 모든 계산 리소스에 대해 위치를 빈 상태로 재설정해야 합니다.

다음은 데이터 센터 위치를 제거하는 데 필요한 일련의 단계에 대한 개괄적인 개요입니다.

- 1 시스템 관리자가 위치 파일에서 데이터 센터 위치 정보를 제거합니다.
- 2 패브릭 관리자가 연결된 계산 리소스 각각의 위치를 편집하여, 해당 위치에 대한 모든 계산 리소스 연결을 제거합니다.

컨테이너 모니터링

vRealize Automation의 컨테이너에서 생성한 컨테이너의 상태를 모니터링할 수 있습니다.

템플릿을 기반으로 컨테이너를 생성한 후 상태를 모니터링할 수 있습니다. 컨테이너에서 **세부 정보**를 클릭하면 네트워크 대역폭, CPU 및 메모리 사용량, 로그 및 컨테이너의 속성을 모니터링할 수 있습니다.

가상 시스템 대량 가져오기, 업데이트 또는 마이그레이션

대량 가져오기 기능을 사용하여 가상 시스템을 vRealize Automation으로 가져오고 업데이트하거나 마이그레이션할 수 있습니다. 대량 가져오기는 여러 환경에서 여러 시스템 관리를 간소화합니다.

대량 가져오기는 예약, 스토리지 경로, **Blueprint**, 소유자 및 모든 사용자 지정 속성 같은 가상 시스템 정의 데이터가 포함되어 있는 **CSV** 파일을 생성합니다. 이 **CSV** 파일을 사용하여 vRealize Automation 환경에 가상 시스템을 가져옵니다. 대량 가져오기는 다음과 같은 관리 작업을 지원합니다.

- 하나 이상의 관리되지 않는 가상 시스템을 vRealize Automation 환경에서 관리할 수 있도록 가져옵니다.
- 가상 시스템 속성(예: 스토리지 경로)을 전체 변경합니다.
- 가상 시스템을 vRealize Automation 환경 하나에서 다른 환경으로 마이그레이션합니다.

참고 vCloud Director 및 vSphere만 대량 가져오기가 지원됩니다. 다른 끝점 유형으로 필터를 설정하면 CSV 파일 형식의 데이터가 생성되지 않습니다.

대량 가져오기 기능의 명령은 vRealize Automation 콘솔 또는 CloudUtil 명령줄 인터페이스를 사용하여 실행할 수 있습니다. CloudUtil 명령줄 인터페이스를 사용하는 데 대한 자세한 내용은 "수명 주기 확장성" 설명서를 참조하십시오.

참고 대량 시스템 가져오기는 정상적인 프로비저닝 단계를 우회하지 않습니다. 프로비저닝 중에 이벤트 브로커에 의해 트리거된 기존의 외부 워크플로는 가져온 시스템에 대해 실행됩니다. 다음 중 하나를 수행하여 가져온 시스템에 대해 워크플로를 일시적으로 비활성화할 수 있습니다.

- 모든 이벤트 브로커 구독을 비활성화합니다. 구독을 비활성화하려면 vRealize Automation 클러스터에 대한 서비스 중단을 스케줄링해야 합니다. 해당 기간 동안은 프로비저닝된 정상적인 시스템에 확장성이 적용되지 않기 때문입니다.
- 시스템을 가져올 때 트리거되지 않도록 이벤트 구독에 조건을 추가합니다. 이 조건을 추가하려면 이벤트 구독으로 이동한 후 비활성화할 구독을 선택하고 사용자 지정 속성 `VirtualMachine.Imported.ConvergedBlueprint` 값이 없음 <가져온 Blueprint의 ID>라는 조건을 추가합니다. 이 조건은 일반적으로 프로비저닝된 시스템에는 적용되지 않고 가져온 시스템에만 적용됩니다.

사전 요구 사항

- **패브릭 관리자 및 비즈니스 그룹 관리자**로 vRealize Automation에 로그인합니다.
- 정적 IP 주소를 사용하는 가상 시스템을 가져오는 경우에는 올바르게 구성된 주소 풀을 준비해야 합니다.

vRealize Automation 환경으로 가상 시스템 가져오기

관리되지 않는 가상 시스템을 vRealize Automation 환경으로 가져올 수 있습니다.

관리되지 않는 가상 시스템은 하이퍼바이저에 있지만 vRealize Automation 환경에서 관리되지 않으며 콘솔에 표시되지 않습니다. 관리되지 않는 가상 시스템을 가져온 후에는 vRealize Automation 관리 인터페이스를 사용하여 가상 시스템을 관리합니다. 권한에 따라 **관리되는 시스템** 탭 또는 **배포** 탭에서 가상 시스템을 볼 수 있습니다.

대량 가져오기 옵션은 NSX 네트워크 및 보안 구성 요소 또는 소프트웨어 구성 요소가 포함된 Blueprint에서 프로비저닝된 배포를 지원하지 않습니다.

사전 요구 사항

- **패브릭 관리자 및 비즈니스 그룹 관리자**로 vRealize Automation에 로그인합니다.
- 정적 IP 주소를 사용하는 가상 시스템을 가져오는 경우에는 올바르게 구성된 주소 풀을 준비해야 합니다. 네트워크 프로파일을 사용하여 IP 주소 범위를 제어하는 방법에 대한 자세한 내용은 "vRealize Automation 구성" 을 참조하십시오.
- 대량 가져오기를 사용하여 다른 가상 시스템에 할당된 정적 IP 주소를 사용하는 가상 시스템을 가져오는 경우 가져오기가 실패합니다.

절차

- 1 모든 이벤트 브로커 구독을 일시적으로 비활성화합니다.

참고 구독을 사용하지 않도록 설정하는 경우 vRealize Automation 클러스터에 대한 서비스 중단을 스케줄링해야 합니다. 이 프로세스 중에는 일반적으로 프로비저닝된 시스템에 확장성이 적용되지 않습니다. 구독을 비활성화하지 못하면 데이터가 손실되고 백업 인프라에서 시스템이 영구적으로 삭제될 수 있습니다.

- 2 가상 시스템 CSV 데이터 파일을 생성합니다.

- a **인프라 > 관리 > 대량 가져오기**를 선택합니다.
- b **CSV 파일 생성**을 클릭합니다.
- c **시스템** 드롭다운 메뉴에서 **관리되지 않음**을 선택합니다.
- d 드롭다운 메뉴에서 **비즈니스 그룹** 기본값을 선택합니다.
- e **소유자** 기본값을 입력합니다.
- f 드롭다운 메뉴에서 **Blueprint** 기본값을 선택합니다.

가져오기가 성공하려면 **Blueprint**를 게시하고 사용 권한에 추가해야 합니다.

- g 드롭다운 메뉴에서 **구성 요소 시스템** 기본값을 선택합니다.

비즈니스 그룹 및 **Blueprint**에 대한 값을 선택하는 경우 CSV 데이터 파일에서 다음 결과를 볼 수 있습니다.

■ Host Reservation (Name or ID) = INVALID_RESERVATION

■ Host To Storage (Name or ID) = INVALID_HOST_RESERVATION_TO_STORAGE

이러한 메시지는 관리되지 않는 가상 시스템도 호스팅하는 호스트 가상 시스템에 대한 예약이 선택한 비즈니스 그룹에 없는 경우에 발생합니다. 관리되지 않는 가상 시스템 호스트에 대한 예약이 비즈니스 그룹에 있는 경우에는 호스트 예약 및 스토리지 호스트 값이 제대로 채워집니다.

- h **리소스** 드롭다운 메뉴에서 사용 가능한 리소스 유형 하나를 선택합니다.

메뉴 항목	설명
끝점	가상 호스트에 액세스하는 데 필요한 정보입니다.
계산 리소스	서로 유사한 기능을 수행하는 가상 시스템 그룹에 액세스하는 데 필요한 정보입니다.

- i **이름** 드롭다운 메뉴에서 가상 시스템 리소스의 이름을 선택합니다.
- j **확인**을 클릭합니다.

3 가상 시스템 CSV 데이터 파일을 편집합니다.

- a CSV 파일을 열고 대상 vRealize Automation 환경의 기존 범주와 일치하도록 데이터 범주를 편집합니다.

CSV 데이터 파일에 포함되어 있는 가상 시스템을 가져오려면 각 가상 시스템이 다음 항목과 연결되어 있어야 합니다.

- 예약
- 스토리지 위치
- Blueprint
- 가상 시스템 구성 요소
- 대상 배포에 있는 소유자

각 가상 시스템의 모든 값이 대상 vRealize Automation 환경에 있어야 가져오기가 성공적으로 완료됩니다. CSV 파일을 편집하여 예약, 스토리지 위치, Blueprint 및 소유자의 값을 변경하거나 개별 가상 시스템에 정적 IP 주소 값을 추가할 수 있습니다.

머리글	설명
# Import—Yes or No	특정 가상 시스템을 가져오기 대상에서 제외하려면 [아니요]로 변경합니다.
가상 시스템 이름	변경하지 않습니다.
가상 시스템 ID	변경하지 않습니다.
호스트 예약(이름 또는 ID)	대상 vRealize Automation 환경에 있는 예약의 이름 또는 ID를 입력합니다.
스토리지 호스트(이름 또는 ID)	대상 vRealize Automation 환경에 있는 스토리지 위치의 이름 또는 ID를 입력합니다.
배포 이름	대상 vRealize Automation 환경에 생성하려는 배포의 새 이름을 입력합니다(예: 가상 시스템 이름).
	참고 각 가상 시스템은 해당 시스템에 고유한 배포로 가져와야 합니다. 단일 가상 시스템을 기존 배포로 가져올 수 없습니다. 여러 가상 시스템을 단일 배포로 가져올 수 없습니다.
Blueprint ID	대상 vRealize Automation 환경에 가상 시스템을 가져오기 위해 사용하는 Blueprint의 ID를 입력합니다.
	참고 Blueprint 이름이 아닌 Blueprint ID만 입력하십시오. 단일 가상 시스템 구성 요소만 포함된 Blueprint를 선택해야 합니다. Blueprint를 게시하고 사용 권한에 추가해야 합니다.
	가져온 가상 시스템의 경우 구성 요소 프로파일이 포함된 Blueprint를 연결하지 마십시오. 가져온 가상 시스템의 기존 설정(예: 메모리 또는 스토리지 크기)이 프로파일 제한 범위를 벗어날 수 있습니다. 이러한 문제가 발생하면 가상 시스템의 향후 Blueprint 기반 재구성에 대한 유효성 검사가 실패합니다.
구성 요소 시스템 ID	선택한 Blueprint에 포함된 가상 시스템 구성 요소의 이름을 입력합니다. 둘 이상의 구성 요소가 있는 Blueprint로 가상 시스템을 가져올 수 없습니다.
소유자 이름	대상 vRealize Automation 환경에서 Blueprint에 대한 사용 권한이 있는 사용자를 입력합니다.

사용자 지정 속성을 하나 이상 가진 가상 시스템을 가져오는 경우, 해당 시스템에 맞게 쉼표로 구분된 값 세 개를 줄에 추가하여 각 사용자 지정 속성을 식별합니다. 각 사용자 지정 속성에 다음 형식을 사용합니다.

,Custom.Property.Name, Value, FLAGS

FLAGS는 vRealize Automation에서 속성을 처리하는 방법을 설명하는 3개의 문자입니다. 플래그는 사용 순서에 따라 다음과 같습니다.

- 1 H 또는 N = 숨김 또는 숨김 아님
- 2 E 또는 O = 암호화됨 또는 암호화되지 않음
- 3 R 또는 P = 런타임 또는 런타임 아님

예를 들어 시스템의 정적 IP 주소를 구성하는 사용자 지정 속성을 추가할 수 있습니다. 다음 형식을 사용할 경우 이 사용자 지정 속성은 네트워크 프로파일에서 사용 가능한 정적 IP 주소를 할당합니다.

,VirtualMachine.Network#.Address, w.x.y.z, HOP

가상 시스템에 대한 적절한 정보로 변수를 변경합니다.

- #을 이 정적 IP 주소를 사용하여 구성되는 네트워크 인터페이스의 개수로 변경합니다. 예: `VirtualMachine.Network0.Address`

- w.x.y.z를 가상 시스템의 정적 IP 주소로 변경합니다. 예: `11.27.42.57`

HOP 플래그 문자열(숨김, 암호화되지 않음, 런타임 아님)은 속성의 가시성을 설정합니다. 이 특정 속성은 대량 가져오기에만 사용되기 때문에 가져오기가 완료된 후 가상 시스템에서 제거됩니다.

이 사용자 지정 속성이 작동하려면 IP 주소는 올바르게 구성된 주소 풀에서 사용할 수 있는 주소여야 합니다. 주소를 찾을 수 없거나, 주소가 이미 사용 중이면 정적 IP 주소 정의 없이 가져오기가 성공적으로 완료되고 오류가 기록됩니다.

b CSV 파일을 저장합니다.

- 4 vRealize Automation 관리 인터페이스를 사용하여 가상 시스템을 vRealize Automation 환경으로 가져옵니다.

a **인프라 > 관리 > 대량 가져오기**를 선택합니다.

b **새로 만들기**를 클릭합니다.

c **이름** 텍스트 상자에 이 작업에 대한 고유한 이름을 입력합니다. 예를 들어 `unmanaged import 10` 이라고 입력합니다.

d CSV 파일 이름을 찾은 후 **CSV 파일** 텍스트 상자에 입력합니다.

- e 가져오기 옵션을 선택합니다.

옵션	설명
시작 시간	항후 시작 날짜를 스케줄링합니다. 선택된 시작 시간은 사용자 Workstation의 로컬 시간이 아니라 로컬 서버 시간입니다.
지금	가져오기 프로세스를 즉시 시작합니다.
지연(초)	여러 가상 시스템을 가져오는 경우, 각 가상 시스템 등록을 지연할 시간을 초 단위로 선택합니다. 이 메뉴 항목을 선택하면 가져오기 프로세스 속도가 느려집니다. 지연을 선택하지 않으려면 값을 비워 둡니다.
배치 크기	여러 가상 시스템을 가져오는 경우, 지정된 시간에 등록할 총 가상 시스템 수를 선택합니다. 이 메뉴 항목을 선택하면 가져오기 프로세스 속도가 느려집니다. 제한하지 않으려면 값을 비워 둡니다.
관리되는 시스템 무시	선택되지 않은 상태로 둡니다.
사용자 검증 건너뛰기	이 메뉴 항목을 선택하면 사용자가 존재하는지 여부를 확인하지 않고 CSV 데이터 파일의 [소유자] 열에 나열된 값으로 가상 시스템 소유자를 설정합니다. 이 메뉴 항목을 선택하면 가져오기 시간을 단축할 수 있습니다.
가져오기 테스트	가상 시스템을 실제로 가져오지 않고 가져오기 프로세스를 테스트하여 CSV 파일에 오류가 있는지 테스트할 수 있습니다.

- f **확인**을 클릭합니다.

작업 진행률이 대량 가져오기 페이지에 나타납니다.

vRealize Automation 환경에서 가상 시스템 업데이트

스토리지 경로와 같은 가상 시스템 속성을 변경하여 vRealize Automation 환경의 관리되는 가상 시스템을 하나 이상 업데이트할 수 있습니다.

관리되는 가상 시스템은 vRealize Automation 환경에서 관리되는 시스템으로 콘솔에서 볼 수 있습니다.

사전 요구 사항

- **패브릭 관리자 및 비즈니스 그룹 관리자**로 vRealize Automation에 로그인합니다.

절차

- 1 가상 시스템 CSV 데이터 파일을 생성합니다.
 - a **인프라 > 관리 > 대량 가져오기**를 선택합니다.
 - b **CSV 파일 생성**을 클릭합니다.
 - c **시스템** 드롭다운 메뉴에서 **관리됨**을 선택합니다.

- d **리소스** 드롭다운 메뉴에서 사용 가능한 리소스 유형 하나를 선택합니다.

옵션	설명
끝점	가상 호스트에 액세스하는 데 필요한 정보입니다.
계산 리소스	서로 유사한 기능을 수행하는 가상 시스템 그룹에 액세스하는 데 필요한 정보입니다.

- e **이름** 드롭다운 메뉴에서 가상 시스템 리소스의 이름을 선택합니다.
- f (선택 사항) 가상 시스템 사용자 지정 속성을 마이그레이션하려는 경우 **사용자 지정 속성 포함**을 선택합니다.
- g **확인**을 클릭합니다.

2 가상 시스템 CSV 데이터 파일을 편집합니다.

- a 텍스트 편집기로 **CSV** 파일을 열고 전체적으로 변경하려는 데이터 범주를 편집합니다.

CSV 데이터 파일에 포함되어 있는 가상 시스템을 업데이트하려면 각 시스템이 다음 항목과 연결되어 있어야 합니다.

- 예약
- 스토리지 위치
- Blueprint
- 시스템 구성 요소
- 대상 배포에 있는 소유자

각 가상 시스템의 모든 값이 대상 vRealize Automation 환경에 있어야 업데이트가 성공적으로 완료됩니다. CSV 파일을 편집하여 예약, 스토리지 위치, Blueprint 및 소유자의 값을 변경하거나 개별 시스템에 정적 IP 주소 값을 추가할 수 있습니다.

- b 가상 시스템 정적 IP 주소를 변경하는 경우 다음과 같은 형식으로 CSV 파일에 명령을 추가합니다.

,VirtualMachine.Network#.Address, w.x.y.z, HOP

가상 시스템에 대한 적절한 정보로 명령을 구성합니다.

- #을 이 정적 IP 주소를 사용하여 구성되는 네트워크 인터페이스의 개수로 변경합니다. 예: VirtualMachineNetwork0.Address
- w.x.y.z를 가상 시스템의 정적 IP 주소로 변경합니다. 예: 11.27.42.57
- HOP 문자열(Hidden, Not encrypted, Not runtime)은 속성의 가시성을 설정합니다. 이 기본 속성은 가져오기가 성공적으로 완료되면 가상 시스템에서 제거됩니다.

업데이트가 성공하려면 올바르게 구성된 주소 풀에서 사용할 수 있는 IP 주소를 지정해야 합니다. 주소를 찾을 수 없거나, 주소가 이미 사용 중이면 정적 IP 주소 정의 없이 업데이트가 완료되고 오류가 기록됩니다.

- c CSV 파일을 저장하고 텍스트 편집기를 닫습니다.

3 vRealize Automation 관리 인터페이스를 사용하여 vRealize Automation 환경의 가상 시스템을 하나 이상 업데이트합니다.

- a **인프라 > 관리 > 대량 가져오기**를 선택합니다.
- b **새로 만들기**를 클릭합니다.
- c **이름** 텍스트 상자에 이 작업에 대한 고유한 이름을 입력합니다. 예를 들어 managed global update 10이라고 입력합니다.
- d CSV 파일 이름을 찾은 후 **CSV 파일** 텍스트 상자에 입력합니다.
- e 가져오기 옵션을 선택합니다.

옵션	설명
시작 시간	향후 시작 날짜를 스케줄링합니다. 지정된 시작 시간은 사용자 Workstation의 로컬 시간이 아니라 로컬 서버 시간입니다.
지금	가져오기 프로세스를 즉시 시작합니다.
지연(초)	가상 시스템을 대량으로 업데이트하는 경우, 각 가상 시스템 업데이트를 지연할 시간을 초 단위로 선택합니다. 이 옵션을 선택하면 업데이트 프로세스가 느려집니다. 지연을 적용하지 않으려면 값을 비워 둡니다.
배치 크기	가상 시스템을 대량으로 업데이트하는 경우, 지정된 시간에 업데이트할 가상 시스템의 총 개수를 선택합니다. 이 옵션을 선택하면 업데이트 프로세스가 느려집니다. 제한을 지정하지 않으려면 값을 비워 둡니다.
관리되는 시스템 무시	선택되지 않은 상태로 둡니다.
사용자 검증 건너뛰기	이 옵션을 선택하면 사용자가 존재하는지 여부를 확인하지 않고 CSV 데이터 파일의 [소유자] 열에 나열된 값으로 시스템 소유자를 설정합니다. 이 옵션을 선택하면 업데이트 시간을 단축할 수 있습니다.
가져오기 테스트	선택되지 않은 상태로 둡니다.

- f **확인**을 클릭합니다.

작업 진행률이 [대량 가져오기] 페이지에 나타납니다.

다른 vRealize Automation 환경으로 가상 시스템 마이그레이션

VMware vRealize™ Automation 환경의 관리되는 가상 시스템을 다른 vRealize Automation 환경으로 하나 이상 마이그레이션할 수 있습니다.

관리되는 가상 시스템은 vRealize Automation 환경에서 관리되는 가상 시스템으로 콘솔에서 볼 수 있습니다.

사전 요구 사항

- **패브릭 관리자 및 비즈니스 그룹 관리자**로 vRealize Automation에 로그인합니다.
- 정적 IP 주소를 사용하는 가상 시스템을 가져오는 경우에는 올바르게 구성된 주소 풀을 준비해야 합니다. 네트워크 프로파일을 사용하여 IP 주소 범위를 제어하는 방법에 대한 자세한 내용은 "vRealize Automation 구성"을 참조하십시오.

절차

1 가상 시스템 CSV 데이터 파일을 생성합니다.

- a **인프라 > 관리 > 대량 가져오기**를 선택합니다.
- b **CSV 파일 생성**을 클릭합니다.
- c **시스템** 드롭다운 메뉴에서 **관리됨**을 선택합니다.
- d **리소스** 드롭다운 메뉴에서 사용 가능한 리소스 유형 하나를 선택합니다.

옵션	설명
끝점	가상 호스트에 액세스하는 데 필요한 정보입니다.
계산 리소스	서로 유사한 기능을 수행하는 가상 시스템 그룹에 액세스하는 데 필요한 정보입니다.

- e **이름** 드롭다운 메뉴에서 가상 시스템 리소스의 이름을 선택합니다.
- f (선택 사항) **사용자 지정 속성 포함**을 선택합니다.
가상 시스템을 동일한 속성과 함께 새로운 배포로 가져올 때 사용자 지정 속성을 포함합니다.
- g **확인**을 클릭합니다.

2 가상 시스템 CSV 데이터 파일을 편집합니다.

CSV 데이터 파일을 편집해야 하는지 여부는 소스 및 대상 환경의 유사성에 따라 좌우됩니다. 소스 환경의 구성 값이 대상 환경의 값과 일치하지 않으면 마이그레이션을 시작하기 전에 값이 일치하도록 CSV 데이터 파일을 편집해야 합니다.

- a CSV 파일을 열고 대상 vRealize Automation 환경의 기존 범주와 일치하도록 데이터 범주를 편집합니다.

CSV 데이터 파일에 포함된 가상 시스템을 마이그레이션하려면 각 가상 시스템이 대상 vRealize Automation 환경에 있는 예약, 스토리지 위치, Blueprint, 시스템 구성 요소 및 소유자와 연결되어 있어야 합니다. 각 가상 시스템의 모든 값이 대상 vRealize Automation 환경에 있어야 마이그레이션이 성공적으로 완료됩니다. CSV 파일을 편집하여 예약, 스토리지 위치, Blueprint 및 소유자의 값을 변경하거나 개별 가상 시스템에 정적 IP 주소 값을 추가할 수 있습니다.

머리글	설명	예
# 가져오기--예 또는 아니요	특정 가상 시스템을 가져오기 대상에서 제외하려면 [아니요]로 변경합니다.	예
가상 시스템 이름	변경하지 않습니다.	MyMachine
가상 시스템 ID	변경하지 않습니다.	a6e05812-0b06-4d4e-a84a-fed242340426a
호스트 예약(이름 또는 ID)	대상 vRealize Automation 환경에 있는 예약의 이름 또는 ID를 입력합니다.	DevReservation
스토리지 호스트(이름 또는 ID)	대상 vRealize Automation 환경에 있는 스토리지 위치의 이름 또는 ID를 입력합니다.	ce-san-1:custom-nfs-2
배포 이름	대상 vRealize Automation 환경에 생성하려는 배포의 새 이름을 입력합니다. 각 가상 시스템은 해당 시스템에 고유한 배포로 마이그레이션해야 합니다. 단일 가상 시스템을 기존 배포로 가져올 수 없습니다. 여러 가상 시스템을 단일 환경으로 가져올 수 없습니다.	ImportedDeployment0001
융합형 Blueprint ID	대상 vRealize Automation 환경에 가상 시스템을 가져오기 위해 사용하는 Blueprint의 ID를 입력합니다. Blueprint ID만 입력해야 합니다. Blueprint 이름을 입력하지 마십시오. 단일 가상 시스템 구성 요소만 포함된 Blueprint를 선택해야 합니다. Blueprint를 게시하고 사용 권한에 추가해야 합니다.	ImportBlueprint
구성 요소 Blueprint ID	선택한 Blueprint에 포함된 가상 시스템 구성 요소의 이름을 입력합니다. 둘 이상의 구성 요소가 있는 Blueprint로 가상 시스템을 가져올 수 없습니다.	ImportedMachine
소유자 이름	대상 vRealize Automation 환경의 사용자를 입력합니다.	user@tenant

적절한 형식의 완전한 CSV 줄의 예: Yes, MyMachine, a6e05812-0b06-4d4e-a84a-fed242340426, DevReservation, ce-san-1:custom-nfs-2, Imported Deployment 0001, ImportBlueprint, ImportedMachine, user@tenant

- b 정적 IP 주소를 가진 가상 시스템을 마이그레이션하는 경우, 다음과 같은 형식으로 CSV 파일에 명령을 추가합니다.

`,VirtualMachine.Network#.Address, w.x.y.z, HOP`

가상 시스템에 대한 적절한 정보로 명령을 구성합니다.

- #을 이 정적 IP 주소를 사용하여 구성되는 네트워크 인터페이스의 개수로 변경합니다. 예: `VirtualMachineNetwork0.Address`
- `w.x.y.z`를 가상 시스템의 정적 IP 주소로 변경합니다. 예: `11.27.42.57`
- `HOP` 문자열(Hidden, Not encrypted, Not runtime)은 속성의 가시성을 설정합니다. 이 기본 속성은 가져오기가 성공적으로 완료되면 가상 시스템에서 제거됩니다.

마이그레이션이 성공하려면 올바르게 구성된 주소 풀에서 사용할 수 있는 IP 주소를 지정해야 합니다. 주소를 찾을 수 없거나, 주소가 이미 사용 중이면 정적 IP 주소 정의 없이 마이그레이션이 완료되고 오류가 기록됩니다.

- c CSV 파일을 저장합니다.

- 3 vRealize Automation 관리 인터페이스를 사용하여 가상 시스템을 vRealize Automation 환경으로 마이그레이션합니다.

- a 인프라 > 관리 > 대량 가져오기를 선택합니다.
- b 새로 만들기를 클릭합니다.
- c 이름 텍스트 상자에 이 작업에 대한 고유한 이름을 입력합니다. 예를 들어 managed migration 10 이라고 입력합니다.
- d CSV 파일 이름을 찾은 후 **CSV 파일** 텍스트 상자에 입력합니다.

e 가져오기 옵션을 선택합니다.

옵션	설명
시작 시간	향후 시작 날짜를 스케줄링합니다. 선택된 시작 시간은 사용자 Workstation의 로컬 시간이 아니라 로컬 서버 시간입니다.
지급	마이그레이션 프로세스를 즉시 시작합니다.
지연(초)	여러 가상 시스템을 마이그레이션하는 경우, 각 가상 시스템 등록을 지연할 시간을 초 단위로 선택합니다. 이 옵션을 선택하면 마이그레이션 프로세스가 느려집니다. 지연을 선택하지 않으려면 값을 비워 둡니다.
배치 크기	여러 가상 시스템을 마이그레이션하는 경우, 지정된 시간에 등록할 총 가상 시스템 수를 선택합니다. 이 옵션을 선택하면 마이그레이션 프로세스가 느려집니다. 제한하지 않으려면 값을 비워 둡니다.
관리되는 시스템 무시	선택되지 않은 상태로 둡니다.
사용자 검증 건너뛰기	이 옵션을 선택하면 사용자가 존재하는지 여부를 확인하지 않고 CSV 데이터 파일의 [소유자] 열에 나열된 값으로 가상 시스템 소유자를 설정합니다. 이 옵션을 선택하면 마이그레이션 시간을 단축할 수 있습니다.
가져오기 테스트	가상 시스템을 실제로 마이그레이션하지 않고 마이그레이션 프로세스를 테스트하여 CSV 파일에 오류가 있는지 테스트할 수 있습니다.

f **확인**을 클릭합니다.

작업 진행률이 [대량 가져오기] 페이지에 나타납니다.