

vRealize Automation 구성

2018년 3월 15일

vRealize Automation 7.3



vmware®

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

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

Copyright © 2015 – 2018 VMware, Inc. 판권 소유. [저작권 및 상표 정보](#).

목차

vRealize Automation 구성 6

업데이트된 정보 7

1 Blueprint 프로비저닝을 위한 외부적 준비 8

vRealize Automation 관리를 위해 환경 준비 8

NSX 네트워크 및 보안 구성 준비를 위한 검사 목록 9

타사 IPAM 제공자 지원을 제공하기 위한 검사 목록 13

vRealize Automation의 컨테이너 구성을 위한 검사 목록 17

vRealize Automation 을 위해 vCloud Director 환경 준비 18

vRealize Automation 을 위해 vCloud Air 환경 준비 18

Amazon AWS 환경 준비 19

Red Hat OpenStack 네트워크 및 보안 기능 준비 25

SCVMM 환경 준비 26

네트워크에서 Azure로 VPC 연결 구성 27

시스템 프로비저닝 준비 28

준비할 시스템 프로비저닝 방법 선택 28

프로비저닝 중 Visual Basic 스크립트 실행을 위한 검사 목록 31

프로비저닝에서 vRealize Automation 게스트 에이전트 사용 32

복제를 통한 프로비저닝 준비를 위한 검사 목록 39

vCloud Air 및 vCloud Director 프로비저닝 준비 52

Linux Kickstart 프로비저닝을 위한 준비 53

SCCM 프로비저닝 준비 55

WIM 프로비저닝 준비 57

가상 시스템 이미지 프로비저닝 준비 64

Amazon 시스템 이미지 프로비저닝 준비 64

시나리오: Rainpole에서의 시스템 프로비저닝을 위한 vSphere 리소스 준비 67

Software 프로비저닝 준비 69

Software 를 사용하여 시스템 프로비저닝 준비 70

시나리오: 시스템 복제 및 소프트웨어 구성 요소 Blueprint를 위해 vSphere CentOS 템플릿 준비 74

시나리오: vSphere 샘플 애플리케이션 Blueprint용 Dukes Bank 가져오기 준비 77

2 Blueprint 프로비저닝을 위한 테넌트 및 리소스 준비 82

테넌트 설정 구성 82

디렉토리 관리 구성 옵션 선택 83

디렉토리 관리용 외부 커넥터 업그레이드 140

시나리오: 고가용성 vRealize Automation 에 대해 Active Directory 링크 구성 148

vRealize Automation 에서 스마트 카드 및 타사 ID 제공자 인증을 위한 외부 커넥터 구성	150
다중 도메인 또는 다중 포리스트 Active Directory 링크 생성	157
그룹 및 사용자 역할 구성	159
추가 테넌트 생성	164
테넌트 삭제	166
사용자 지정 브랜딩 구성	166
알림 구성을 위한 검사 목록	169
프로비저닝된 시스템에 대한 RDP 연결 지원을 위해 사용자 지정 RDP 파일 생성	180
시나리오: 영역 간 배포를 위한 데이터 센터 위치 추가	180
vRealize Orchestrator 구성	181
리소스 구성	186
IaaS 리소스 구성을 위한 검사 목록	186
XaaS 리소스 구성	299
컨테이너 생성 및 구성	310
기본 vRealize Orchestrator 서버에 추가적인 플러그인 설치	330
Active Directory 정책 사용	330
3 사용자에게 서비스 Blueprint 제공	334
Blueprint 설계	334
Blueprint와 콘텐츠 내보내기 및 가져오기	336
시나리오: vSphere 샘플 애플리케이션용 Dukes Bank 가져오기 및 환경 구성	338
시나리오: Dukes Bank 샘플 애플리케이션 테스트	341
설계 라이브러리 구축	343
시스템 Blueprint 설계	344
Software 구성 요소 설계	420
XaaS Blueprint 및 리소스 작업 설계	432
Blueprint 게시	490
복합 Blueprint 구성	491
중첩된 Blueprint 동작 이해	493
Software 구성 요소를 지원하는 시스템 구성 요소 선택	496
Blueprint 구성 요소 간 속성 바인딩 생성	496
명시적 종속성 생성 및 프로비저닝 순서 제어	497
서비스 카탈로그 관리	498
서비스 카탈로그 구성을 위한 검사 목록	499
서비스 생성	500
카탈로그 항목 및 작업 사용	502
사용 권한 생성	505
승인 정책 사용	511
매개 변수화된 Blueprint를 사용하여 시스템 프로비저닝 요청	534
시나리오: 서비스 카탈로그에서 MySQL이 설치된 CentOS 애플리케이션 Blueprint를 사용할 수 있도록 설정	536

배포된 카탈로그 항목 관리	540
프로비저닝된 리소스에 대한 작업 실행	540
재구성에 대한 시스템 재구성 설정 및 고려 사항 지정	561
배포에서 로드 밸런서 재구성	568
배포에서 NAT 규칙 변경	569
배포에서 보안 항목 추가 또는 제거	570
기존 NSX Edge의 모든 NAT 규칙 표시	571

vRealize Automation 구성

vRealize Automation 구성에서는 vRealize Automation 프로비저닝과 카탈로그 관리 준비를 위해 vRealize Automation 및 외부 환경을 구성하는 것에 대한 정보를 제공합니다.

대상 사용자

이 정보는 vRealize Automation 환경 구성을 담당하는 IT 전문가, vRealize Automation 프로비저닝에 사용하기 위해 기존 인프라에서 요소 준비를 담당하는 인프라 관리자를 대상으로 합니다. 이 정보는 가상 시스템 기술과 데이터 센터 작업에 많은 경험을 가진 숙련된 Windows 및 Linux 시스템 관리자를 대상으로 작성되었습니다.

VMware 기술 자료 용어집

VMware 기술 자료 사이트에서는 새로운 용어를 정리한 용어집을 제공하고 있습니다. VMware 기술 설명서에 사용된 용어에 대한 정의를 보려면 <http://www.vmware.com/support/pubs>를 참조하십시오.

업데이트된 정보

다음 표에는 이 제품 릴리스의 vRealize Automation 구성에 대한 변경 내용이 나열되어 있습니다.

개정	설명
2018년 3월 15일	<ul style="list-style-type: none"> 로그 파일 이름을 포함하도록 워크로드 배치 문제 해결 항목이 업데이트되었습니다. Software 지원을 위해 Windows 참조 시스템 준비 및 Software 지원을 위해 Linux 참조 시스템 준비의 다운로드 가능한 스크립트가 업데이트되었습니다. 실패한 제거 요청 후 배포 강제 제거 섹션을 업데이트했습니다. LDAP/IWA를 통한 Active Directory 링크 구성 항목이 부분적으로 업데이트되었습니다.
2018년 1월 18일	<ul style="list-style-type: none"> 보다 일반적인 정보를 제공하도록 vRealize Automation에서 스마트 카드 및 타사 ID 제공자 인증을 위한 외부 커넥터 구성 항목이 업데이트되었습니다.
2017년 12월 4일	부분적 업데이트.
2017년 8월 30일	<ul style="list-style-type: none"> NSX 범용 개체 프로비저닝을 위한 관리자 요구 사항 Windows 참조 시스템에 게스트 에이전트 설치 항목을 업데이트했습니다. vRealize Orchestrator에서 타사 IPAM 제공자 패키지 얻기 및 가져오기 섹션을 업데이트했습니다. vRealize Automation에 필요한 Amazon AWS 사용자 역할 및 자격 증명
KO-002417-02	<ul style="list-style-type: none"> vRealize Orchestrator에 NSX 플러그인 설치 섹션을 업데이트했습니다. LDAP/IWA를 통한 Active Directory 링크 구성 섹션을 업데이트했습니다.
KO-002417-01	<ul style="list-style-type: none"> 외부 vRealize Orchestrator 서버 구성 섹션을 업데이트했습니다. 업그레이드 또는 마이그레이션된 끝점 사용 시 고려 사항 항목에서 KB 문서 링크를 업데이트 및 추가했습니다. 대/소문자 구분 문제 해결을 위해 시나리오: vSphere 샘플 애플리케이션용 Dukes Bank 가져오기 항목을 업데이트했습니다. 배포에서 로드 밸런서 재구성 항목에 KB 문서 링크를 추가했습니다. NAT 규칙 생성 및 사용 항목에 외부 참조를 추가했습니다. NSX 끝점을 생성하고 vSphere 끝점에 연결 항목에 외부 참조를 추가했습니다. Blueprint의 컨테이너 속성 및 속성 그룹 사용 섹션을 업데이트했습니다.
KO-002417-00	최초 설명서 릴리스입니다.

Blueprint 프로비저닝을 위한 외부적 준비

1

카탈로그 항목 프로비저닝을 지원하기 위해 일부 요소를 vRealize Automation 외부에서 생성하거나 준비해야 할 수 있습니다. 예를 들어 복제 시스템을 프로비저닝하기 위한 카탈로그 항목을 제공하려면 복제 원본으로 사용할 템플릿을 하이퍼바이저에 생성해야 합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- vRealize Automation 관리를 위해 환경 준비
- 네트워크에서 Azure로 VPC 연결 구성
- 시스템 프로비저닝 준비
- Software 프로비저닝 준비

vRealize Automation 관리를 위해 환경 준비

통합 플랫폼에 따라, 환경을 vRealize Automation 관리로 가져오거나 특정 기능을 활용할 수 있으면 우선 몇 가지 구성을 변경해야 합니다.

표 1-1. vRealize Automation 통합을 위해 환경 준비







환경	준비
 NSX	NSX를 활용하여 vRealize Automation로 프로비저닝된 시스템의 네트워킹 및 보안 기능을 관리하려면 통합을 위해 NSX 인스턴스를 준비합니다. NSX 네트워크 및 보안 구성 준비를 위한 검사 목록 항목을 참조하십시오.
 vCloud Director	vCloud Director 인스턴스를 설치 및 구성하고, vSphere 및 클라우드 리소스를 설정하고, 적절한 자격 증명을 식별하거나 생성하여 vCloud Director 환경에 대한 액세스 권한을 vRealize Automation에 제공해야 합니다. vRealize Automation을 위해 vCloud Director 환경 준비 항목을 참조하십시오.

표 1-1. vRealize Automation 통합을 위해 환경 준비 (계속)

환경	준비
 vCloud Air	vCloud Air 계정을 등록하고, vCloud Air 환경을 설정하고, 적절한 자격 증명을 식별하거나 생성하여 해당 환경에 대한 액세스 권한을 vRealize Automation에 제공해야 합니다. vCloud Air 및 vCloud Director 프로비저닝 준비 항목을 참조하십시오.
 Amazon AWS	vRealize Automation에서 사용할 수 있도록 Amazon AWS 환경의 요소 및 사용자 역할을 준비하고, Amazon AWS 기능이 vRealize Automation 기능에 매핑되는 방법을 이해합니다. Amazon AWS 환경 준비 항목을 참조하십시오.
Microsoft Azure	Azure Blueprint의 소프트웨어 구성 요소를 지원하기 위해 VPN 터널링을 사용하도록 네트워킹을 구성합니다. 네트워크에서 Azure로 VPC 연결 구성 항목을 참조하십시오.
 Red Hat OpenStack	Red Hat OpenStack를 활용하여 vRealize Automation로 프로비저닝된 시스템의 네트워킹 및 보안 기능을 관리하려면 통합을 위해 Red Hat OpenStack 인스턴스를 준비합니다. Red Hat OpenStack 네트워크 및 보안 기능 준비 항목을 참조하십시오.
 SCVMM	스토리지, 네트워킹을 구성하고 템플릿 및 하드웨어 프로파일 이름 지정 제한을 이해합니다. SCVMM 환경 준비 항목을 참조하십시오.
외부 IPAM 제공자	외부 IPAM 제공자 패키지 또는 플러그인을 등록하고, 구성 워크플로를 실행하고, IPAM 솔루션을 새 vRealize Automation 끝점으로 등록합니다. 타사 IPAM 제공자 지원을 제공하기 위한 검사 목록 항목을 참조하십시오.
기타 모든 환경	환경을 변경할 필요가 없습니다. 템플릿, 부팅 환경 또는 시스템 이미지를 생성하여 시스템 프로비저닝을 위한 준비를 시작할 수 있습니다. 시스템 프로비저닝 준비 항목을 참조하십시오.

NSX 네트워크 및 보안 구성 준비를 위한 검사 목록

vRealize Automation에서 NSX 네트워크 및 보안 옵션을 사용할 수 있으려면 사용하고자 하는 외부 NSX 네트워크 및 보안 환경을 먼저 구성해야 합니다.

vRealize Automation 7.3부터 통합 NSX 기능을 얻기 위해 NSX 플러그인을 설치할 필요가 없습니다. 이제 모든 통합 NSX 기능은 NSX 플러그인이 아닌 NSX API를 통해 직접 받습니다. 하지만 XaaS를 사용하여 vRealize Automation 및 NSX 통합을 확장하려는 경우 여기에 설명된 대로 vRealize Orchestrator에 NSX 플러그인을 설치해야 합니다.

vRealize Automation에서 NSX 네트워크, 보안 및 로드 밸런싱 기능 사용을 준비하는 과정에서, NSX Manager 자격 증명을 사용할 때에는 NSX Manager 관리자 계정을 사용해야 합니다.

NSX에 대한 관련 정보는 NSX 설명서

(https://www.vmware.com/support/pubs/nsx_pubs.html)와 [Integrating NSX with vRealize Automation](#) 등의 공개 블로그 및 기사를 참조하십시오.

Blueprint 및 예약에 지정하는 네트워크 및 보안 구성에 대한 vRealize Automation 지원 대부분은 외부에서 구성하며, 계산 리소스에서 데이터 수집을 실행한 이후에 vRealize Automation에서 사용할 수 있습니다.

vRealize Automation Blueprint에 구성할 수 있는 NSX 설정에 대한 자세한 내용은 [네트워크 및 보안 구성 요소 설정 구성](#) 항목을 참조하십시오.

표 1-2. NSX 네트워킹 및 보안 준비를 위한 검사 목록

작업	위치	세부 정보
<input type="checkbox"/> 게이트웨이 및 전송 영역 설정을 포함하는 NSX 네트워크 설정을 구성합니다.	네트워크 설정은 NSX에서 구성합니다.	NSX 관리 가이드를 참조하십시오.
<input type="checkbox"/> NSX 보안 정책, 태그 및 그룹을 생성합니다.	보안 설정은 NSX에서 구성합니다.	NSX 관리 가이드를 참조하십시오.
<input type="checkbox"/> NSX 로드 밸런서 설정을 구성합니다.	vRealize Automation과 함께 작동하도록 NSX 로드 밸런서를 구성합니다.	NSX 관리 가이드를 참조하십시오. 사용자 지정 속성 참조 자료에서 네트워킹에 대한 사용자 지정 속성도 참조하십시오.
<input type="checkbox"/> 크로스 가상 센터 배포의 경우 계산 NSX Manager가 기본 NSX Manager 역할을 가지고 있는지 확인합니다.	vRealize Automation 프로비저닝을 수행하려면 시스템이 상주하는 영역의 계산 NSX Manager가 기본 NSX Manager 역할을 가지고 있어야 합니다.	NSX 범용 개체 프로비저닝을 위한 관리자 요구 사항 항목을 참조하십시오. 크로스 가상 센터 배포, 범용 개체 및 기본 NSX Manager 역할에 대한 자세한 내용은 NSX 설치 가이드 및 NSX 관리 가이드를 참조하십시오.

vRealize Orchestrator 에 NSX 플러그인 설치

NSX 플러그인을 설치하려면 vRealize Orchestrator 설치 관리자 파일을 다운로드하고 vRealize Orchestrator 구성 인터페이스를 사용하여 플러그인 파일을 업로드한 후 플러그인을 vRealize Orchestrator 서버에 설치해야 합니다.

일반적인 플러그인 업데이트 및 문제 해결 정보를 보려면 vRealize Orchestrator [설명서](#)를 참조하십시오.

필수 조건

vRealize Automation 7.3부터 통합 NSX 기능을 얻기 위해 NSX 플러그인을 설치할 필요가 없습니다. 이제 모든 통합 NSX 기능은 NSX 플러그인이 아닌 NSX API를 통해 직접 받습니다. 하지만 XaaS를 사용하여 vRealize Automation 및 NSX 통합을 확장하려는 경우 여기에 설명된 대로 vRealize Orchestrator에 NSX 플러그인을 설치해야 합니다.

NSX 플러그인이 이미 설치되어 있는 포함된 vRealize Orchestrator를 사용 중인 경우 이 절차를 건너뛸 수 있습니다.

- 지원되는 vRealize Orchestrator 인스턴스를 실행 중인지 확인합니다.
vRealize Orchestrator를 설정하는 데 대한 자세한 내용은 VMware vRealize Orchestrator 설치 및 구성을 참조하십시오.
- vRealize Orchestrator 플러그인을 설치하고 vCenter Single Sign-On을 통해 인증할 수 있는 사용 권한을 가진 계정의 자격 증명이 있는지 확인합니다.
- vRealize Orchestrator 클라이언트를 설치했으며, 관리자 자격 증명을 사용하여 로그인할 수 있는지 확인합니다.
- vRealize Automation [지원 매트릭스](#)에서 NSX 플러그인의 올바른 버전을 확인합니다.

프로시저

- 1 vRealize Orchestrator 서버에서 액세스할 수 있는 위치에 플러그인 파일을 다운로드합니다.
적절한 버전 값이 포함된 플러그인 설치 관리자 파일 이름 형식은 o11nplugin-nsx-1.n.n.vmoapp입니다. NSX 네트워킹 및 보안 제품용 플러그인 설치 파일은 VMware 제품 다운로드 사이트 (<http://vmware.com/web/vmware/downloads>)에 있습니다.
- 2 브라우저를 열고 vRealize Orchestrator 구성 인터페이스를 시작합니다.
URL 형식의 예: https://orchestrator_server.com:8283
- 3 왼쪽 창에서 **플러그인**을 클릭한 다음 아래쪽의 [새 플러그인 설치] 섹션으로 스크롤합니다.
- 4 **플러그인 파일** 텍스트 상자에서 플러그인 설치 관리자 파일을 찾은 후 **업로드 및 설치**를 클릭합니다.
파일은 .vmoapp 형식이어야 합니다.
- 5 메시지가 표시되면 플러그인 설치 창에서 라이선스 계약을 수락합니다.
- 6 사용하도록 설정된 플러그인 설치 상태 섹션에서 올바른 NSX 플러그인 이름이 지정되었는지 확인합니다.
버전 정보는 vRealize Automation 지원 매트릭스 항목을 참조하십시오.
상태가 다음에 서버를 시작할 때 플러그인이 설치됨으로 표시됩니다.
- 7 vRealize Orchestrator 서버 서비스를 다시 시작합니다.
- 8 vRealize Orchestrator 구성 인터페이스를 다시 시작합니다.
- 9 **플러그인**을 클릭하고, 상태가 설치 확인으로 변경되었는지 확인합니다.

10 vRealize Orchestrator 클라이언트 애플리케이션을 시작하여 로그인한 후 **워크플로** 탭을 사용하여 라이브러리에서 NSX 폴더로 이동합니다.

NSX 플러그인이 제공하는 워크플로를 검색할 수 있습니다.

후속 작업

vRealize Automation에서 vRealize Orchestrator 끝점을 생성하여 워크플로를 실행하는 데 사용할 수 있습니다. [vRealize Orchestrator 끝점 생성](#) 항목을 참조하십시오.

vRealize Orchestrator 및 NSX 보안 워크플로 실행

vRealize Automation에서 NSX 보안 정책 기능을 사용하기 전에 관리자가 vRealize Orchestrator에서 Enable security policy support for overlapping subnets 워크플로를 실행해야 합니다.

접치는 서브넷에 대한 보안 정책 지원 워크플로는 NSX 6.1 이상 끝점에 적용할 수 있습니다. 이 지원을 사용하려면 이 워크플로를 한 번만 실행합니다.

필수 조건

- vSphere 끝점이 NSX 끝점에 등록되어 있는지 확인합니다. [vSphere 끝점 생성](#) 항목을 참조하십시오.
- vRealize Orchestrator 클라이언트에 관리자로 로그인합니다.
- Create NSX endpoint vRO 워크플로를 실행했는지 확인합니다.

프로시저

- 1** 워크플로 탭을 클릭하고 **NSX > VCAC에 대한 NSX 워크플로**를 선택합니다.
- 2** **NSX 끝점 생성** 워크플로를 실행하고 프롬프트에 응답합니다.
- 3** **접치는 서브넷에 대한 보안 정책 지원 사용** 워크플로를 실행합니다.
- 4** NSX 끝점을 워크플로에 대한 입력 매개 변수로 선택합니다.

vSphere 끝점을 생성했을 때 지정한 IP 주소를 사용하여 NSX 인스턴스를 등록합니다.

이 워크플로를 실행한 후 보안 정책에 정의된 분산 방화벽 규칙이 이 보안 정책이 적용되는 보안 그룹 구성원의 vNIC에만 적용됩니다.

후속 작업

Blueprint에 대해 적용 가능한 보안 기능을 적용합니다.

NSX 범용 개체 프로비저닝을 위한 관리자 요구 사항

NSX 범용 개체를 사용할 경우 크로스 vCenter NSX 환경에서 시스템을 프로비저닝하려면 NSX 계산 관리자가 기본 역할을 가진 vCenter에 프로비저닝해야 합니다.

크로스 vCenter NSX 환경에 여러 vCenter Server가 있을 수 있는데, 각각은 고유한 NSX Manager와 쌍을 이루어야 합니다. 하나의 NSX Manager에 기본 NSX Manager 역할이 할당되고, 다른 NSX Manager에는 보조 NSX Manager 역할이 할당됩니다.

기본 NSX Manager는 범용 논리적 스위치 같은 범용 개체를 생성할 수 있습니다. 이러한 개체는 보조 NSX Manager와 동기화됩니다. 보조 NSX Manager에서 이러한 개체를 볼 수 있지만 보조 NSX Manager에서 편집할 수는 없습니다. 범용 개체를 관리하려면 기본 NSX Manager를 사용해야 합니다. 기본 NSX Manager를 사용하여 환경 내의 모든 보조 NSX Manager를 구성할 수 있습니다.

NSX 크로스 vCenter 환경에 대한 자세한 내용은 [NSX 제품 설명서](#)에서 NSX 관리 가이드의 크로스 vCenter 네트워킹 및 보안 개요를 참조하십시오.

기본 NSX Manager의 NSX 끝점에 연결되어 있는 vSphere(vCenter) 끝점의 경우, vRealize Automation에서 로컬 논리적 스위치, 로컬 Edge Gateway, 로컬 로드 밸런서, 보안 그룹, 보안 태그와 같은 NSX 로컬 개체를 지원합니다. 또한 범용 전송 영역이 있는 NAT 일대일 및 일대다 네트워크, 범용 전송 영역과 범용 DLR(논리적 분산 라우터)이 있는 라우팅된 네트워크, 그리고 모든 유형의 네트워크가 있는 로드 밸런서도 지원합니다.

vRealize Automation은 NSX의 기존 및 요청 시 범용 보안 그룹 또는 태그를 지원하지 않습니다.

로컬 요청 시 네트워크를 기본 NSX Manager로 프로비저닝하려면 vCenter 특정 로컬 전송 영역을 사용합니다. 해당 로컬 vCenter에서 배포를 위해 로컬 전송 영역 및 가상 선을 사용하도록 vRealize Automation 예약을 구성할 수 있습니다.

vSphere(vCenter) 끝점을 해당하는 보조 NSX Manager 끝점에 연결하는 경우 로컬 개체만 프로비저닝 및 사용할 수 있습니다.

NSX 끝점은 하나의 vSphere 끝점에만 연결할 수 있습니다. 이러한 연결 제약 조건은 범용 요청 시 네트워크를 프로비저닝하여 다른 vCenter에서 프로비저닝된 vSphere 시스템에 이 네트워크를 연결할 수 없다는 것을 의미합니다.

vRealize Automation에서는 NSX 범용 논리적 스위치를 외부 네트워크로 사용할 수 있습니다. 범용 스위치가 있는 경우 수집된 데이터가 해당 범용 스위치에 연결되거나, 배포 내의 각 시스템에 해당 범용 스위치를 사용합니다.

- 요청 시 네트워크를 범용 전송 영역에 프로비저닝하면 새로운 범용 논리적 스위치를 생성할 수 있습니다.
- 요청 시 네트워크를 기본 NSX Manager의 범용 전송 영역에 프로비저닝하면 범용 논리적 스위치가 생성됩니다.
- 요청 시 네트워크를 보조 NSX Manager의 범용 전송 영역에 프로비저닝하는 작업은 실패합니다. NSX는 보조 NSX Manager에서 범용 논리적 스위치를 생성할 수 없기 때문입니다.

NSX 범용 개체에 대한 자세한 내용은 VMware 기술 자료 문서 NSX 개체를 포함한 vRealize Automation Blueprint의 배포 실패(2147240)(<http://kb.vmware.com/kb/2147240>)를 참조하십시오.

타사 IPAM 제공자 지원을 제공하기 위한 검사 목록

지원되는 타사 IPAM 제공자(예: Infoblox)로부터 네트워크 프로파일 정의에 사용할 IP 주소와 범위를 구할 수 있습니다.

vRealize Automation 네트워크 프로파일에서 외부 IPAM 제공자 끝점을 생성하고 사용할 수 있다면 vRealize Orchestrator IPAM 제공자 플러그인 또는 패키지를 다운로드하거나 다른 방법으로 구한 후 플러그인 또는 패키지를 가져와서 vRealize Orchestrator에서 필요한 워크플로를 실행하고 IPAM 솔루션을 vRealize Automation 끝점으로 등록해야 합니다.

외부 IPAM 제공자를 사용하여 가능한 IP 주소 범위를 제공하기 위한 프로비저닝 프로세스 개요는 [타사 IPAM 제공자를 사용하여 vRealize Automation 배포 프로비저닝](#) 항목을 참조하십시오.

표 1-3. 외부 IPAM 제공자 지원 검사 목록 준비

작업	설명	세부 정보
<input type="checkbox"/> 지원되는 외부 IPAM 제공자 vRealize Orchestrator 플러그인 얻고 가져옵니다.	<p>VMware Solution Exchange(https://solutionexchange.vmware.com/store/category_groups/cloud-management)에서 IPAM 제공자 플러그인 또는 패키지(예: The Infoblox IPAM Plug-in for vRealize Orchestrator 플러그인 및 지원 설명서)를 다운로드하고 플러그인 또는 패키지를 vRealize Orchestrator에 가져옵니다.</p> <p>VMware Solution Exchange에 필요한 IPAM 제공자 패키지가 없으면 타사 IPAM 솔루션 제공자 SDK 및 지원 설명서를 사용하여 고유한 패키지를 생성할 수 있습니다.</p> <p>https://code.vmware.com/sdks 또는 https://code.vmware.com/samples에서 vRealize Automation 버전별 타사 IPAM 솔루션 제공자 SDK, 지원 설명서, 그리고 vRealize Orchestrator 및 vRealize Automation에 대한 관련 스타터 패키지를 사용할 수 있습니다.</p>	<p>vRealize Orchestrator에서 타사 IPAM 제공자 패키지 얻기 및 가져오기 항목을 참조하십시오.</p>
<input type="checkbox"/> 필요한 구성 워크플로를 실행하고 외부 IPAM 솔루션을 vRealize Automation 끝점으로 등록합니다.	<p>vRealize Orchestrator 구성 워크플로를 실행하고 vRealize Orchestrator에서 IPAM 제공자 끝점 유형을 등록합니다.</p>	<p>vRealize Orchestrator에서 타사 IPAM 끝점 유형을 등록하도록 워크플로 실행 항목을 참조하십시오.</p>

vRealize Orchestrator 에서 타사 IPAM 제공자 패키지 얻기 및 가져오기

타사 IPAM 제공자 끝점을 정의하고 사용할 준비를 하려면 먼저 타사 IPAM 제공자 패키지를 얻고 vRealize Orchestrator에 이 패키지를 가져와야 합니다.

기존의 타사 IP 주소 관리 제공자 플러그인(예: Infoblox IPAM)을 다운로드하고 사용할 수 있습니다. VMware 제공 스타터 패키지 및 함께 제공된 SDK 설명서를 사용하여 다른 타사 IPAM 솔루션 제공자(예: Bluecat)와 사용할 고유한 타사 IPAM 플러그인 또는 패키지를 생성할 수도 있습니다.

- marketplace.vmware.com에서 기존 [Infoblox IPAM Plug-in for vRealize Orchestrator](#) 플러그인 및 지원 설명서를 가져옵니다. 다운로드에는 이 플러그인의 설치 및 사용에 대한 설명서도 포함되어 있습니다.

- code.vmware.com/web/sdk의 **vRealize Automation Third-Party IPAM Integration SDK 7.3** 페이지에서 타사 IPAM 솔루션 제공자 SDK, 지원 설명서 그리고 vRealize Orchestrator 및 vRealize Automation에 대한 관련 스타터 패키지를 가져오고 사용하여 고유한 타사 IPAM 솔루션을 생성합니다.

vRealize Orchestrator에서 타사 IPAM 제공자 플러그인 또는 패키지를 가져온 후에는 필요한 워크플로를 실행하고 vRealize Orchestrator에 IPAM 끝점 유형을 등록해야 합니다.

플러그인 및 패키지 가져오기 및 vRealize Orchestrator 워크플로 실행에 대한 자세한 내용은 VMware vRealize Orchestrator 클라이언트 사용을 참조하십시오. vRealize Orchestrator 플러그인, 패키지 및 워크플로로 vRealize Automation 확장에 대한 자세한 내용은 수명 주기 확장성 항목을 참조하십시오.

이 단계 순서에서는 Infoblox IPAM 플러그인을 예로 사용합니다. 사용 중인 vRealize Automation 또는 플러그인 버전에 따라 단계 순서가 다를 수 있습니다.

필수 조건

- marketplace.vmware.com에서 패키지 또는 플러그인을 다운로드합니다.
- vRealize Orchestrator 플러그인 또는 패키지를 가져오고 구성하고 등록하려면 vRealize Orchestrator에 관리자 권한으로 로그인합니다.

프로시저

- 1 marketplace.vmware.com 사이트를 엽니다.
- 2 플러그인 또는 패키지를 찾아서 다운로드합니다.

예를 들어 vRealize Orchestrator 및 vRealize Automation 7.1 이상에서 Infoblox 타사 IPAM 끝점을 지원하는 Infoblox 플러그인을 가져옵니다.

- a **게시자** 범주에서 **Infoblox**를 선택하고 **적용**을 클릭합니다.
- b **Infoblox Plug-in for vRealize Orchestrator**를 선택합니다.
- c **Tech Specs**를 클릭하여 사전 요구 사항을 검토합니다.
- d **시도**를 클릭하여 추가 정보를 얻거나 다운로드 링크가 포함되어 있는 이메일을 받습니다.
- e 이메일에 지정되어 있는 지침에 따라 zip 파일을 다운로드합니다.

플러그인 버전 4.0 이상은 vRealize Automation 7.1 이상을 지원합니다. zip 파일에는 플러그인에 대한 설명서도 포함되어 있습니다.

- 3 vRealize Orchestrator에서 **관리자** 탭을 클릭하고 **패키지 가져오기**를 클릭합니다.
- 4 가져올 패키지를 선택합니다.
- 5 모든 워크플로와 아티팩트를 선택하고 **선택한 요소 가져오기**를 클릭합니다.

후속 작업

vRealize Orchestrator에서 타사 IPAM 끝점 유형을 등록하도록 워크플로 실행.

vRealize Orchestrator 에서 타사 IPAM 끝점 유형을 등록하도록 워크플로 실행

vRealize Automation에서 타사 IPAM 제공자를 사용할 수 있도록 지원하고

vRealize Automation에서 사용할 IPAM 끝점 유형을 등록하려면 vRealize Orchestrator에서 등록 워크플로를 실행합니다.

vRealize Orchestrator에서 IPAM 끝점 유형을 등록하기 위해 vRealize Automation vRA 관리자 자격 증명을 제공하라는 메시지가 표시됩니다.

패키지 가져오기 및 vRealize Orchestrator 워크플로 실행에 대한 자세한 내용은 VMware vRealize Orchestrator 클라이언트 사용을 참조하십시오. vRealize Orchestrator 패키지 및 워크플로로 vRealize Automation 확장에 대한 자세한 내용은 수명 주기 확장성 항목을 참조하십시오.

필수 조건

- vRealize Orchestrator에서 타사 IPAM 제공자 패키지 얻기 및 가져오기
- 워크플로 실행 권한을 가진 사용자로 vRealize Orchestrator(vRealize Automation 포함)에 로그인한 상태인지 확인합니다.
- 메시지가 표시되면 vRealize Automation vRealize Automation 관리자 자격 증명을 제공할 준비를 하십시오.

프로시저

- 1 vRealize Orchestrator에서 **설계** 탭을 클릭하고 **관리자 > 라이브러리**를 선택한 후 **IPAM 서비스 패키지 SDK**를 선택합니다.

각 IPAM 제공자 패키지에는 고유한 이름이 지정되고 고유 워크플로가 포함되어 있습니다. 각 제공자는 고유의 등록 워크플로를 제공합니다. 워크플로 이름은 제공자 패키지 간에 유사할 수 있지만 vRealize Orchestrator에서 워크플로의 위치는 제공자별로 다릅니다.

- 2 이 예의 경우 Register IPAM Endpoint 등록 워크플로를 실행하고 IPAM Infoblox 끝점 유형을 지정합니다.
- 3 vRealize Automation 자격 증명을 묻는 메시지가 나타나면 vRealize Automation vRA 관리자 자격 증명을 입력합니다.

이 패키지는 vRealize Automation 끝점 서비스에서 Infoblox를 새 IPAM 끝점 유형으로 등록하고, vRealize Automation에 끝점을 정의할 때 끝점 유형을 사용할 수 있도록 만듭니다.

참고 vRealize Orchestrator 제어 센터에서 vRealize Orchestrator 서버를 다시 시작한 후 Infoblox IPAM 연결이 vRealize Orchestrator **인벤토리** 탭에서 사라지는 경우가 발생할 수 있습니다. 이런 문제를 해결하려면 **vRO관리자 > 라이브러리 > Infoblox > vRA > 도우미** 메뉴 순으로 이동하여 Create IPAM Connection 워크플로를 실행합니다. 그런 다음 vRealize Orchestrator **인벤토리** 탭으로 이동하여 **Infoblox IPAM**을 선택하고 페이지를 새로 고쳐서 Infoblox IPAM 연결이 표시되도록 합니다.

후속 작업

이제 vRealize Automation에서 IPAM Infloblox 유형 끝점을 생성하거나 등록한 타사 패키지 또는 플러그인에 대한 끝점을 생성할 수 있습니다. [타사 IPAM 제공자 끝점 생성](#) 항목을 참조하십시오.

vRealize Automation의 컨테이너 구성을 위한 검사 목록

컨테이너를 시작하려면 vRealize Automation 사용자 역할을 지원하도록 이 기능을 구성해야 합니다.

컨테이너에서 컨테이너 정의를 구성한 후 Blueprint에서 컨테이너 구성 요소를 추가하고 구성할 수 있습니다.

표 1-4. vRealize Automation의 컨테이너 구성을 위한 검사 목록

작업	세부 정보
컨테이너 관리자와 컨테이너 설계자 역할을 할당합니다.	기초 및 개념에 있는 컨테이너 역할 정보를 참조하십시오.
컨테이너 상황에 맞는 도움말 시스템을 표시합니다.	기초 및 개념에 있는 컨테이너 도움말 정보를 참조하십시오.
vRealize Automation의 컨테이너 탭에서 컨테이너 정의를 정의합니다.	vRealize Automation 구성의 내용을 참조하십시오.
vRealize Automation의 설계 탭에서 컨테이너 구성 요소와 컨테이너 네트워킹 구성 요소를 Blueprint에 추가합니다.	vRealize Automation 구성의 내용을 참조하십시오.

vRealize Automation 장치를 사용하여 컨테이너 구성

vRealize Automation vRealize Automation 장치(**vRA 설정 > Xenon**)에서 Xenon 서비스 정보에 액세스할 수 있습니다.

Xenon 호스트 VM, 수신 대기 포트 및 서비스 상태에 대한 정보가 포함됩니다. 클러스터된 Xenon 노드에 대한 정보도 표시합니다.

vRealize Automation 장치에서 다음 CLI 명령으로 Xenon Linux 서비스를 관리할 수 있습니다.

명령	설명
<code>service xenon-service status</code>	서비스의 상태를 "실행 중" 또는 "중지됨"으로 표시합니다.
<code>service xenon-service start</code>	서비스를 시작합니다.
<code>service xenon-service stop</code>	서비스를 중지합니다.
<code>service xenon-service restart</code>	서비스를 다시 시작합니다.
<code>service xenon-service get_host</code>	서비스가 실행 중인 호스트 이름을 표시합니다.
<code>service xenon-service get_port</code>	서비스 포트를 표시합니다.
<code>service xenon-service status_cluster</code>	클러스터된 모든 노드에 대한 정보를 JSON 형식으로 표시합니다.
<code>service xenon-service reset</code>	Xenon이 모든 구성 파일을 유지하는 디렉토리를 삭제하고 서비스를 다시 시작합니다.

컨테이너 클러스터링

vRealize Automation의 컨테이너와 함께 Xenon 서비스를 사용하여 노드를 클러스터에 연결할 수 있습니다. 노드가 클러스터되는 경우 Xenon 서비스는 시작 시 다른 노드를 자동으로 연결합니다.

vRealize Automation 장치의 **Xenon** 탭에서 클러스터 상태를 모니터링하거나 CLI에서 다음 명령을 실행하여 클러스터 상태를 모니터링할 수 있습니다.

```
service xenon-service status_cluster
```

Xenon은 쿼럼 기반 클러스터링에서 작동합니다. 쿼럼은 $(\text{number of nodes} / 2) + 1$ 공식을 사용하여 계산됩니다.

vRealize Automation 을 위해 vCloud Director 환경 준비

vCloud Director를 vRealize Automation에 통합하려면 먼저 vCloud Director 인스턴스를 설치 및 구성하고, vSphere 및 클라우드 리소스를 설정하고, 적절한 자격 증명을 식별하거나 생성하여 vCloud Director 환경에 대한 액세스 권한을 vRealize Automation에 제공해야 합니다.

환경 구성

가상 데이터 센터와 네트워크를 포함하여, vSphere 리소스와 클라우드 리소스를 구성합니다. 자세한 내용은 vCloud Director 설명서를 참조하십시오.

통합에 필요한 자격 증명

vRealize Automation IaaS 관리자가 vCloud Director 환경을 vRealize Automation에서 끝점으로 관리하도록 설정하는 데 사용할 수 있는 조직 관리자 또는 시스템 관리자의 자격 증명을 생성하거나 식별합니다.

사용자 역할 고려 사항

조직 내의 vCloud Director 사용자 역할이 vRealize Automation 비즈니스 그룹의 역할에 대응할 필요는 없습니다. 사용자 계정이 vCloud Director에 없으면 vCloud Director에서는 연결된 LDAP 나 Active Directory를 조회하고, 사용자가 ID 저장소에 있으면 사용자 계정을 생성합니다. 사용자 계정을 생성할 수 없는 경우 경고를 로깅하지만 프로비저닝 프로세스가 실패하지는 않습니다. 그런 다음 프로비저닝된 시스템이 vCloud Director 끝점을 구성하는 데 사용된 계정에 할당됩니다.

vCloud Director 사용자 관리에 대한 관련 내용은 vCloud Director 설명서를 참조하십시오.

vRealize Automation 을 위해 vCloud Air 환경 준비

vCloud Air를 vRealize Automation에 통합하려면 먼저 vCloud Air 계정을 등록하고, vCloud Air 환경을 설정하고, 적절한 자격 증명을 식별하거나 생성하여 해당 환경에 대한 액세스 권한을 vRealize Automation에 제공해야 합니다.

환경 구성

vCloud Air 설명서에 나와 있는 지침에 따라 환경을 구성합니다.

통합에 필요한 자격 증명

vRealize Automation IaaS 관리자가 vCloud Air 환경을 vRealize Automation에서 끝점으로 관리하도록 설정하는 데 사용할 수 있는 가상 인프라 관리자 또는 계정 관리자 자격 증명을 생성하거나 식별합니다.

사용자 역할 고려 사항

조직 내의 vCloud Air 사용자 역할이 vRealize Automation 비즈니스 그룹의 역할에 대응할 필요는 없습니다. vCloud Air 사용자 관리에 대한 관련 내용은 vCloud Air 설명서를 참조하십시오.

Amazon AWS 환경 준비

Amazon AWS 환경에서 요소와 사용자 역할을 준비하고, 게스트 에이전트 및 Software 부트스트랩 에이전트와 통신하도록 Amazon AWS를 준비하고 Amazon AWS 기능이 vRealize Automation 기능에 매핑하는 방법을 이해합니다.

vRealize Automation에 필요한 Amazon AWS 사용자 역할 및 자격 증명

vRealize Automation이 환경을 관리하는 데 필요한 사용 권한과 함께 Amazon AWS의 자격 증명을 구성해야 합니다.

vRealize Automation에서는 끝점 자격 증명에 대한 액세스 키를 요구하며 사용자 이름 및 암호를 지원하지 않습니다.

■ Amazon Web Services의 역할 및 사용 권한 부여

AWS의 고급 사용자 역할은 AWS Directory Service 사용자 또는 그룹에 AWS 서비스 및 리소스에 대한 전체 액세스 권한을 제공하지만 이것이 필수는 아닙니다. 낮은 권한의 사용자 역할도 지원됩니다. vRealize Automation 기능의 요구를 충족하는 AWS 보안 정책은 다음과 같습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeVolumes",

      "ec2:DescribeVpcAttribute",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImageAttribute",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeVolumeStatus",
```

```

        "ec2:DescribeVpnConnections",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",

        "ec2:DisassociateAddress",
        "ec2:GetPasswordData",

        "ec2:ImportKeyPair",
        "ec2:ImportVolume",

        "ec2:CreateVolume",
        "ec2:DeleteVolume",
        "ec2:AttachVolume",
        "ec2:ModifyVolumeAttribute",
        "ec2:DetachVolume",

        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses",

        "ec2:CreateKeyPair",
        "ec2:DeleteKeyPair",

        "ec2:CreateTags",
        "ec2:AssociateAddress",
        "ec2:ReportInstanceState",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:MonitorInstances",
        "ec2:RebootInstances",
        "ec2:RunInstances",
        "ec2:TerminateInstances",

        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth"
    ],
    "Resource": "*"
}
}}

```

■ Amazon Web Services의 인증 자격 증명

Amazon IAM(Identity and Access Management) 사용자 및 그룹의 관리를 위해서는 사용자가 AWS 전체 액세스 권한 관리자 자격 증명으로 구성되어야 합니다.

vRA에서 AWS 끝점을 생성할 때 키와 보안 키를 입력하라는 메시지가 표시됩니다. Amazon 끝점을 생성하는 데 필요한 액세스 키를 얻으려면 관리자가 AWS 전체 액세스 권한 관리자 정책으로 추가 구성되거나 AWS 전체 액세스 권한 관리자 자격 증명을 가진 사용자로부터 키를 요청해야 합니다.

[Amazon 끝점 생성](#) 항목을 참조하십시오.

정책 및 역할 사용에 대한 자세한 내용은 Amazon Web Services 제품 설명서의 AWS IAM(Identity and Access Management) 섹션을 참조하십시오.

Amazon AWS 가 Software 부트스트랩 에이전트 및 게스트 에이전트와 통신하도록 허용

Software가 포함된 애플리케이션 Blueprint를 프로비저닝하거나 게스트 에이전트를 사용하여 프로비저닝된 시스템을 추가적으로 사용자 지정하는 능력을 원하는 경우 시스템이 프로비저닝되는 Amazon AWS 환경과 에이전트가 패키지를 다운로드하고 지침을 수신하는 vRealize Automation 환경 간에 연결을 사용하도록 설정해야 합니다.

vRealize Automation을 사용하여 Amazon AWS 시스템을 vRealize Automation 게스트 에이전트 및 Software 부트스트랩 에이전트와 함께 프로비저닝하는 경우 프로비저닝된 시스템이 다시 vRealize Automation와 통신하여 시스템을 사용자 지정할 수 있도록 네트워크 및 Amazon VPC 간 연결을 설정해야 합니다.

Amazon AWS VPC 연결 옵션에 대한 자세한 내용은 Amazon AWS 설명서를 참조하십시오.

선택적 Amazon 기능 사용

vRealize Automation은 Amazon Virtual Private Cloud, Elastic Load Balancer, Elastic IP 주소 및 Elastic Block 스토리지를 포함한 몇 가지 Amazon 기능을 지원합니다.

Amazon 보안 그룹 사용

Amazon 예약을 생성할 때 최소 하나의 보안 그룹을 지정합니다. 사용 가능한 각 영역에는 보안 그룹을 하나 이상 지정해야 합니다.

보안 그룹은 방화벽처럼 작동하여 시스템에 대한 액세스를 제어합니다. 각 영역에는 기본 보안 그룹이 하나 이상 있습니다. 관리자는 Amazon Web Services Management Console을 사용하여 추가적인 보안 그룹을 생성하고, Microsoft Remote Desktop Protocol 또는 SSH에 대한 포트를 구성하고, Amazon VPN에 대한 가상 전용 네트워크를 설정합니다.

Amazon 예약을 생성하거나 Blueprint에서 시스템 구성 요소를 구성할 때는 지정된 Amazon 계정 영역에 사용 가능한 보안 그룹 목록 중에서 선택할 수 있습니다. 보안 그룹 가져오기는 데이터를 수집하는 동안 수행됩니다.

Amazon Web Services에서 보안 그룹을 생성하고 사용하는 방법에 대한 자세한 내용은 Amazon 설명서를 참조하십시오.

Amazon Web Services 영역 이해

각 Amazon Web Services 계정은 클라우드 끝점으로 표시됩니다. vRealize Automation에서 Amazon Elastic Cloud Computing 끝점을 생성하는 경우 영역은 계산 리소스로 수집됩니다. IaaS 관리자가 비즈니스 그룹에 대한 계산 리소스를 선택한 후 인벤토리 및 상태 데이터 수집이 자동으로 수행됩니다.

하루에 한 번 자동으로 수행되는 인벤토리 데이터 수집은 다음 데이터 등 계산 리소스에 있는 항목에 대한 데이터를 수집합니다.

- Elastic IP 주소
- Elastic Load Balancer
- Elastic Block 스토리지 볼륨

상태 데이터 수집은 기본적으로 15분마다 자동으로 수행됩니다. vRealize Automation에서 생성하는 인스턴스인 관리되는 인스턴스의 상태에 대한 정보를 수집합니다. 상태 데이터의 예는 다음과 같습니다.

- Windows 암호
- 로드 밸런서의 시스템 상태
- Elastic IP 주소

패브릭 관리자는 인벤토리 및 상태 데이터 수집을 시작하고 인벤토리 및 상태 데이터 수집의 빈도를 변경하거나 사용하지 않도록 설정할 수 있습니다.

Amazon Virtual Private Cloud 사용

Amazon Virtual Private Cloud를 사용하면 Amazon Web Services 클라우드의 사설 섹션에서 Amazon 시스템 인스턴스를 프로비저닝할 수 있습니다.

Amazon Web Services 사용자는 Amazon VPC를 사용하여 사양에 따라 가상 네트워크 토폴로지를 설계할 수 있습니다. vRealize Automation에서 Amazon VPC를 할당할 수 있습니다. 하지만 vRealize Automation에서는 Amazon VPC 사용 비용은 추적하지 않습니다.

Amazon VPC를 사용하여 프로비저닝할 때 vRealize Automation은 Amazon이 기본 IP 주소를 가져오는 VPC 서브넷이 있는 것으로 예측합니다. 이 주소는 인스턴스가 종료될 때까지 정적입니다. 또한 Elastic IP 풀을 사용하여 Elastic IP 주소를 vRealize Automation에서 인스턴스에 연결할 수도 있습니다. 이를 통해 Amazon Web Services에서 인스턴스를 지속적으로 프로비저닝 및 해체하는 사용자가 동일한 IP를 유지할 수 있습니다.

AWS Management Console을 사용하여 다음 요소를 생성합니다.

- 인터넷 게이트웨이, 라우팅 테이블, 보안 그룹과 서브넷 및 사용 가능한 IP 주소가 포함된 Amazon VPC
- 사용자가 AWS Management Console 외부에서 Amazon 시스템 인스턴스에 로그인해야 하는 경우 Amazon Virtual Private Network

vRealize Automation 사용자는 Amazon VPC로 작업할 때 다음 작업을 수행할 수 있습니다.

- 패브릭 관리자는 Amazon VPC를 클라우드 예약에 할당할 수 있습니다. [Amazon EC2 예약 생성](#) 항목을 참조하십시오.
- 시스템 소유자는 Amazon 시스템 인스턴스를 Amazon VPC에 할당할 수 있습니다.

Amazon VPC 생성에 대한 자세한 내용은 Amazon Web Services 설명서를 참조하십시오.

Amazon Web Services 용 Elastic Load Balancer 사용

Elastic Load Balancer는 들어오는 애플리케이션 트래픽을 여러 Amazon Web Services 인스턴스로 분배합니다. Amazon 로드 밸런싱은 무장애 기능과 성능을 향상시킵니다.

Amazon에서는 Amazon EC2 Blueprint를 사용하여 프로비저닝된 시스템에 Elastic 로드 밸런싱을 제공합니다.

Elastic Load Balancer는 Amazon Web Services, Amazon Virtual Private Network 및 프로비저닝 위치에서 사용 가능해야 합니다. 예를 들어 us-east1c에서 로드 밸런서를 사용 가능하고 시스템 위치가 us-east1b인 경우 시스템은 사용 가능한 로드 밸런서를 사용할 수 없습니다.

vRealize Automation에서는 Elastic Load Balancer를 생성, 관리 또는 모니터링하지 않습니다.

Amazon Web Services Management Console을 사용하여 Amazon Elastic Load Balancer를 생성하는 방법에 대한 자세한 내용은 Amazon Web Services 설명서를 참조하십시오.

Amazon Web Services 용 Elastic IP 주소 사용

Elastic IP 주소를 사용하면 동적 Amazon Web Services 클라우드 환경에서 신속하게 다른 시스템으로 패일오버할 수 있습니다. vRealize Automation에서 Elastic IP 주소는 영역에 대한 권한을 가진 모든 비즈니스 그룹이 사용할 수 있습니다.

관리자는 AWS Management Console을 사용하여 Elastic IP 주소를 Amazon Web Services 계정에 할당할 수 있습니다. 지정 영역에는 두 가지 그룹의 Elastic IP 주소가 있습니다. 하나의 범위는 비 Amazon VPC 인스턴스에 대해 할당되며 다른 범위는 Amazon VPC에 대해 할당됩니다. 비 Amazon VPC 영역에만 주소를 할당하는 경우 Amazon VPC에서는 해당 주소를 사용할 수 없습니다. 그 반대의 경우도 마찬가지입니다. Amazon VPC에만 주소를 할당하면 비-Amazon VPC 영역에서는 주소를 사용할 수 없습니다.

Elastic IP 주소는 특정 시스템이 아닌 Amazon Web Services 계정과 연결되어 있지만 한 번에 하나의 시스템에서만 주소를 사용할 수 있습니다. 주소는 해제를 선택할 때까지

Amazon Web Services 계정과 연결된 상태를 계속 유지합니다. 이 주소를 해제하여 특정 시스템 인스턴스에 매핑할 수 있습니다.

IaaS 설계자는 Blueprint에 사용자 지정 속성을 추가하여 프로비저닝 중에 Elastic IP 주소를 시스템에 할당할 수 있습니다. 시스템 소유자 및 관리자는 시스템에 할당된 Elastic IP 주소를 볼 수 있으며 시스템 편집 권한이 있는 관리자 또는 시스템 소유자는 프로비저닝 후 Elastic IP 주소를 할당할 수 있습니다. 하지만 주소가 이미 시스템 인스턴스에 연결되어 있고 인스턴스가

Amazon Virtual Private Cloud 배포의 일부인 경우에는 Amazon이 주소를 할당하지 않습니다.

Amazon Elastic IP 주소 생성 및 사용에 대한 자세한 내용은 Amazon Web Services 설명서를 참조하십시오.

Amazon Web Services 용 Elastic Block 스토리지 사용

Amazon Elastic Block 스토리지는 Amazon 시스템 인스턴스 및

Amazon Virtual Private Cloud에 사용하기 위한 블록 수준 스토리지 볼륨을 제공합니다. 스토리지 볼륨은 Amazon Web Services 클라우드 환경에서 해당 볼륨에 연결된 Amazon 시스템 인스턴스의 수명 이상으로 지속될 수 있습니다.

Amazon Elastic Block 스토리지 볼륨을 vRealize Automation과 함께 사용하는 경우 다음의 제한이 적용됩니다.

- 시스템 인스턴스를 프로비저닝할 때 기존 Elastic Block 스토리지 볼륨을 연결할 수 없습니다. 하지만 새 볼륨을 생성하고 한 번에 둘 이상의 시스템을 요청할 경우에는 볼륨이 생성되어 각 인스턴스에 연결됩니다. 예를 들어 volume_1이라는 이름의 볼륨 하나를 생성하고 세 개의 시스템을 요청하면 각 시스템별로 볼륨이 생성됩니다. 이름이 volume_1인 세 개의 볼륨이 생성되어 각 시스템에 연결됩니다. 각 볼륨은 고유한 볼륨 ID를 가집니다. 각 볼륨의 크기와 위치는 동일합니다.
- 볼륨은 동일한 운영 체제의 볼륨이어야 하며 해당 볼륨을 연결하는 시스템과 동일한 위치에 있어야 합니다.
- vRealize Automation은 Elastic Block 스토리지로 지원되는 인스턴스의 기본 볼륨을 관리하지 않습니다.

Amazon Elastic Block 스토리지에 대한 자세한 내용과

Amazon Web Services Management Console을 사용하여 이를 사용하도록 지정하는 자세한 방법은 Amazon Web Services 설명서를 참조하십시오.

시나리오: 개념 증명 환경을 위해 네트워크 및 Amazon VPC 간 연결 구성

vRealize Automation을 평가하기 위해 개념 증명 환경 설정 작업을 수행하는 IT 전문가로서, vRealize Automation Software 기능을 지원하는 네트워크 및 Amazon VPC 간 연결을 일시적으로 구성하려고 합니다.

네트워크 및 Amazon VPC 간 연결은 게스트 에이전트를 사용하여 프로비저닝된 시스템을 사용자 지정하거나 Blueprint에 Software 구성 요소를 포함하려는 경우에만 필요합니다. 운영 환경이라면 Amazon Web Services를 통해 공식적으로 이 연결을 구성하겠지만 개념 증명 환경에서 작업 중이므로 임시 네트워크 및 Amazon VPC 간 연결을 구성하려고 합니다. 터널을 통해 라우팅하도록 SSH 터널을 설정한 다음 vRealize Automation에서 Amazon 예약을 구성합니다.

필수 조건

- vRealize Automation을 설치하고 완전하게 구성합니다. Rainpole의 vRealize Automation 설치 및 구성 시나리오 항목을 참조하십시오.
- TunnelGroup이라는 Amazon AWS 보안 그룹을 생성하고 포트 22에서 액세스를 허용하도록 그룹을 구성합니다.
- Amazon AWS TunnelGroup 보안 그룹에서 CentOS 시스템을 생성 또는 식별하고 다음 구성을 기록해 둡니다.
 - 관리 사용자 자격 증명(예: root).
 - 공용 IP 주소.
 - 개인 IP 주소.
- vRealize Automation 설치와 동일한 로컬 네트워크에서 CentOS 시스템을 생성 또는 식별합니다.
- 두 터널 시스템 모두에 OpenSSH SSHD 서버를 설치합니다.

프로시저

- 1 Amazon AWS 터널 시스템에 루트 사용자 또는 이와 유사한 사용자로 로그인합니다.
- 2 iptables를 사용하지 않도록 설정합니다.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

- 3 /etc/ssh/sshd_config를 편집하여 AllowTCPForwarding과 GatewayPorts를 사용하도록 설정합니다.
- 4 서비스를 다시 시작합니다.

```
/etc/init.d/sshd restart
```

- 5 vRealize Automation 설치와 동일한 로컬 네트워크의 CentOS 시스템에 루트 사용자로 로그인합니다.
- 6 로컬 네트워크 시스템에서 Amazon AWS 터널 시스템으로 SSH 터널을 호출합니다.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" W

-R 1442:vRealize_automation_appliance_fqdn:5480 W
-R 1443:vRealize_automation_appliance_fqdn:443 W
-R 1444:manager_service_fqdn:443 W
User of Amazon tunnel machine@Public IP Address of Amazon tunnel machine
```

Amazon AWS 터널 시스템에서 vRealize Automation 리소스에 액세스할 수 있도록 포트 전달을 구성했지만 SSH 터널은 터널을 통해 라우팅하도록 Amazon 예약을 구성할 때까지 작동하지 않습니다.

후속 작업

- 1 IaaS 설계자가 Blueprint를 생성하는 데 사용할 수 있는 Amazon 시스템 이미지를 생성하려면 Windows 또는 Linux 참조 시스템에 소프트웨어 부트스트랩 에이전트와 게스트 에이전트를 설치합니다. [Software 프로비저닝 준비](#) 항목을 참조하십시오.
- 2 SSH 터널을 통해 라우팅하도록 vRealize Automation에서 Amazon 예약을 구성합니다. [시나리오: 개념 증명 환경을 위해 Amazon 예약 생성](#) 항목을 참조하십시오.

Red Hat OpenStack 네트워크 및 보안 기능 준비

vRealize Automation은 보안 그룹 및 부동 IP 주소를 포함한 OpenStack의 몇 가지 기능을 지원합니다. 이러한 기능이 vRealize Automation과 작동하는 방식 및 환경에서 이를 구성하는 방법에 대해 알아보십시오.

OpenStack 보안 그룹 사용

보안 그룹을 사용하면 특정 포트를 통해 전송되는 네트워크 트래픽에 대한 제어 규칙을 지정할 수 있습니다.

시스템을 요청할 때 예약에 보안 그룹을 지정할 수 있습니다. 설계 캔버스에 기존 또는 요청 시 NSX 보안 그룹을 지정할 수도 있습니다.

보안 그룹 가져오기는 데이터를 수집하는 동안 수행됩니다.

사용 가능한 각 영역에는 보안 그룹을 하나 이상 지정해야 합니다. 예약을 생성할 때 해당 영역에서 사용할 수 있는 보안 그룹이 표시됩니다. 각 영역에는 기본 보안 그룹이 하나 이상 있습니다.

추가적인 보안 그룹은 소스 리소스에서 관리해야 합니다. 다양한 시스템에서 보안 그룹을 관리하는 데 대한 자세한 내용은 OpenStack 설명서를 참조하십시오.

OpenStack과 함께 부동 소수점 IP 주소 사용

OpenStack의 실행 중인 가상 인스턴스에 부동 소수점 IP 주소를 할당할 수 있습니다.

부동 소수점 IP 주소의 할당을 사용하려면 IP 전달을 구성하고 Red Hat OpenStack에서 부동 소수점 IP 풀을 생성해야 합니다. 자세한 내용은 Red Hat OpenStack 설명서를 참조하십시오.

시스템 소유자에게 부동 소수점 IP 연결 및 부동 소수점 IP 연결 끊기 작업에 대한 사용 권한을 부여해야 합니다. 그런 다음 권한 있는 사용자가 부동 소수점 IP 주소 풀에서 사용 가능한 주소를 선택하여 시스템에 연결된 외부 네트워크에서 프로비저닝된 시스템에 부동 소수점 IP 주소를 연결할 수 있습니다. 부동 소수점 IP 주소가 시스템과 연결된 후 vRealize Automation 사용자가 부동 소수점 IP 연결 끊기 옵션을 선택하여 현재 할당된 부동 소수점 IP 주소를 확인하고 시스템에서 주소와의 연결을 끊을 수 있습니다.

SCVMM 환경 준비

vRealize Automation 시스템 프로비저닝에 사용할 SCVMM 템플릿과 하드웨어 프로파일의 생성을 시작하기 전에 템플릿과 하드웨어 프로파일 이름에 대한 이름 지정 제한 사항을 이해하고 SCVMM 네트워크 및 스토리지 설정을 구성해야 합니다.

환경을 준비하는 것과 관련된 자세한 내용은 vRealize Automation 7.3 설치에서 SCVMM 요구 사항을 참조하십시오.

시스템 프로비저닝과 관련된 자세한 내용은 [Hyper-V\(SCVMM\) 끝점 생성](#) 항목을 참조하십시오.

vRealize Automation은 SCVMM 사설 클라우드 구성을 사용하는 배포 환경을 지원하지 않습니다. vRealize Automation은 현재 SCVMM 사설 클라우드를 기반으로 수집, 할당 또는 프로비저닝할 수 없습니다.

템플릿 및 하드웨어 프로파일 이름 지정

SCVMM 및 vRealize Automation에서 템플릿 및 하드웨어 프로파일에 대해 사용하는 이름 지정 규칙에 따라 템플릿 또는 하드웨어 프로파일 이름은 temporary 또는 profile이라는 단어로 시작하면 안 됩니다. 예를 들어 다음과 같은 용어는 데이터를 수집할 때 무시됩니다.

- TemporaryTemplate
- Temporary Template
- TemporaryProfile
- Temporary Profile

■ Profile

SCVMM 클러스터의 필수 네트워크 구성

SCVMM 클러스터는 vRealize Automation에만 가상 네트워크를 노출하기 때문에 가상 네트워크와 논리적 네트워크 사이에 일대일 관계가 성립되어야 합니다. SCVMM 콘솔을 사용하여 각 논리적 네트워크를 가상 네트워크에 매핑하고, 가상 네트워크를 통해 시스템에 액세스하도록 SCVMM 클러스터를 구성합니다.

SCVMM 클러스터의 필수 스토리지 구성

SCVMM Hyper-V 클러스터에서 vRealize Automation은 공유 볼륨에서만 데이터를 수집하고 프로비저닝을 수행합니다. SCVMM 콘솔을 사용하여 공유 리소스 볼륨만 스토리지로 사용하도록 클러스터를 구성합니다.

독립형 SCVMM 호스트의 필수 스토리지 구성

독립형 SCVMM 호스트의 경우, vRealize Automation은 기본 가상 시스템 경로에서만 데이터를 수집하고 프로비저닝을 수행합니다. SCVMM 콘솔을 사용하여 독립형 호스트를 위한 기본 가상 시스템 경로를 구성합니다.

네트워크에서 Azure로 VPC 연결 구성

Azure Blueprint에서 소프트웨어 구성 요소를 사용하려면 네트워크에서 Azure로 연결을 구성해야 합니다.

필수 조건

- vRealize Automation을 설치하고 완전하게 구성합니다. Rainpole의 vRealize Automation 설치 및 구성 시나리오의 내용을 참조하십시오.
- TunnelGroup이라는 Azure 보안 그룹을 생성하고 포트 22에 대한 액세스를 허용하도록 해당 그룹을 구성합니다.
- Azure TunnelGroup 보안 그룹에서 CentOS 시스템을 생성 또는 식별하고 다음 구성을 기록해 둡니다.
 - 관리 사용자 자격 증명(예: root).
 - 공용 IP 주소.
 - 개인 IP 주소.
- vRealize Automation 설치와 동일한 로컬 네트워크에서 CentOS 시스템을 생성 또는 식별합니다.
- 두 터널 시스템 모두에 OpenSSH SSHD 서버를 설치합니다.

프로시저

- 1 Azure 터널 시스템에 루트 사용자 또는 이와 유사한 사용자로 로그인합니다.

2 iptables를 사용하지 않도록 설정합니다.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

3 /etc/ssh/sshd_config를 편집하여 AllowTCPForwarding과 GatewayPorts를 사용하도록 설정합니다.

4 서비스를 다시 시작합니다.

```
/etc/init.d/sshd restart
```

5 vRealize Automation 설치와 동일한 로컬 네트워크의 CentOS 시스템에 루트 사용자로 로그인합니다.

6 로컬 네트워크 시스템에서 Azure 터널 시스템으로 SSH 터널을 호출합니다.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" W

-R 1442:vRealize_automation_appliance_fqdn:5480 W
-R 1443:vRealize_automation_appliance_fqdn:443 W
-R 1444:manager_service_fqdn:443 W
Azure 터널 시스템의 사용자@Azure 터널 시스템의 공용 IP 주소
```

Azure 터널 시스템에서 vRealize Automation 리소스에 액세스할 수 있도록 포트 포워딩을 구성했지만 SSH 터널은 터널을 통해 라우팅하도록 Azure 예약을 구성할 때까지 작동하지 않습니다.

후속 작업

- 1 IaaS 설계자가 Blueprint를 생성하는 데 사용할 수 있는 Azure 시스템 이미지를 생성하려면 Windows 또는 Linux 참조 시스템에 소프트웨어 부트스트랩 에이전트와 게스트 에이전트를 설치합니다. [Software 프로비저닝 준비](#) 항목을 참조하십시오.
- 2 SSH 터널을 통해 라우팅하도록 vRealize Automation에서 Azure 예약을 구성합니다. [Microsoft Azure를 위한 예약 생성](#) 항목을 참조하십시오.

시스템 프로비저닝 준비

환경과 시스템 프로비저닝 방법에 따라 vRealize Automation 외부에 요소를 구성해야 할 수 있습니다.

예를 들어 시스템 템플릿이나 시스템 이미지를 구성해야 합니다. NSX 설정을 구성하거나 vRealize Orchestrator 워크플로를 실행해야 할 수도 있습니다.

시스템 프로비저닝을 준비할 때 포트 지정에 대한 관련 정보는 [VMware vRealize Automation 정보](#)의 보안 구성 가이드 및 참조 아키텍처 항목을 참조하십시오.

준비할 시스템 프로비저닝 방법 선택

시스템 프로비저닝 방법의 대부분은 일부 요소를 vRealize Automation 외부에서 준비해야 합니다.

표 1-5. 준비할 시스템 프로비저닝 방법 선택

시나리오	지원되는 끝 점	에이전트 지원	프로비저닝 방법	사전 프로비저닝 준비
시스템 프로비저닝 전 또는 후에 시스템 수명 주기 동안의 추가 단계로서 사용자 지정 Visual Basic 스크립트를 실행하도록 vRealize Automation을 구성합니다. 예를 들어 사전 프로비저닝 스크립트를 사용하여 프로비저닝 이전에 인증서 또는 보안 토큰을 생성한 다음 사후 프로비저닝 스크립트를 사용하여 시스템 프로비저닝 이후에 인증서 및 토큰을 사용할 수 있습니다.	Amazon AWS를 제외하고 지원되는 모든 끝점에서 Visual Basic 스크립트를 실행할 수 있습니다.	선택하는 프로비저닝 방법에 따라 다릅니다.	모든 프로비저닝 방법에서 추가 단계로 지원되지만 Amazon AWS 시스템에서는 Visual Basic 스크립트를 사용할 수 없습니다.	프로비저닝 중 Visual Basic 스크립트 실행을 위한 검사 목록
Oracle, MySQL, WAR, 데이터베이스 스키마와 같은 미들웨어 및 애플리케이션 배포 구성 요소의 설치, 구성 및 수명 주기 관리를 자동화하는 애플리케이션 Blueprint를 프로비저닝합니다.	<ul style="list-style-type: none"> ■ vSphere ■ vCloud Air ■ vCloud Director ■ Amazon AWS 	<ul style="list-style-type: none"> ■ (필수) 게스트 에이전트 ■ (필수) 소프트웨어 부트스트랩 에이전트 및 게스트 에이전트 	<ul style="list-style-type: none"> ■ 복제 ■ 복제 (vCloud Air 또는 vCloud Director의 경우) ■ 연결된 복제 ■ Amazon 시스템 이미지 	Blueprint에서 Software 구성 요소를 사용하려는 경우에는 게스트 에이전트와 Software 부트스트랩 에이전트를 지원하는 프로비저닝 방법을 준비합니다. Software 준비에 대한 자세한 내용은 Software 프로비저닝 준비 항목을 참조하십시오.
게스트 에이전트를 사용하여 프로비저닝한 후에 추가로 시스템을 사용자 지정합니다.	모든 가상 시스템 끝점 및 Amazon AWS.	<ul style="list-style-type: none"> ■ (필수) 게스트 에이전트 ■ (선택 사항) 소프트웨어 부트스트랩 에이전트 및 게스트 에이전트 	가상 시스템 이미지를 제외한 모든 프로비저닝 방법이 지원됩니다.	프로비저닝 후 시스템을 사용자 지정하려는 경우 게스트 에이전트를 지원하는 프로비저닝 방법을 선택합니다. 게스트 에이전트에 대한 자세한 내용은 프로비저닝에서 vRealize Automation 게스트 에이전트 사용 항목을 참조하십시오.
게스트 운영 체제 없이 시스템을 프로비저닝합니다. 운영 체제는 프로비저닝 이후에 설치할 수 있습니다.	모든 가상 시스템 끝점.	지원되지 않음	기본	vRealize Automation 외부에서 사전 프로비저닝 준비가 필요하지 않습니다.
가상 시스템의 공간 효율적인 복사본(연결된 복제라고 함)을 프로비저닝합니다. 연결된 복제는 VM의 스냅샷에 기반하며, 델타 디스크 체인을 사용하여 상위 시스템과의 차이점을 추적합니다.	vSphere	<ul style="list-style-type: none"> ■ (선택 사항) 게스트 에이전트 ■ (선택 사항) 소프트웨어 부트스트랩 에이전트 및 게스트 에이전트 	연결된 복제	<p>기존 vSphere 가상 시스템이 있어야 합니다.</p> <p>Software를 지원하려는 경우 복제하려는 시스템에 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치해야 합니다.</p> <p>연결된 복제 VM을 프로비저닝하기 전에 Blueprint에서 식별되는 VM 스냅샷의 전원을 꺼야 합니다.</p>

표 1-5. 준비할 시스템 프로비저닝 방법 선택 (계속)

시나리오	지원되는 플랫폼	에이전트 지원	프로비저닝 방법	사전 프로비저닝 준비
Net App FlexClone 기술을 사용하여 가상 시스템의 공간 효율적인 복사본을 프로비저닝합니다.	vSphere	(선택 사항) 게스트 에이전트	NetApp FlexClone	복제를 통한 프로비저닝 준비를 위한 검사 목록
기존 Windows 또는 Linux 시스템에서 생성된 템플릿 개체(참조 시스템이라고 함)와 사용자 지정 개체에서 복제하는 방법으로 시스템을 프로비저닝합니다.	<ul style="list-style-type: none"> ■ vSphere ■ KVM (RHEV) ■ SCVMM 	<ul style="list-style-type: none"> ■ (선택 사항) 게스트 에이전트 ■ (vSphere에만 해당하는 선택 사항) 소프트웨어 부트스트랩 에이전트 및 게스트 에이전트 	복제	복제를 통한 프로비저닝 준비를 위한 검사 목록 항목을 참조하십시오. Software를 지원하려는 경우 복제하려는 vSphere 시스템에 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치해야 합니다.
템플릿 및 사용자 지정 개체에서 복제하여 vCloud Air 또는 vCloud Director 시스템을 프로비저닝합니다.	<ul style="list-style-type: none"> ■ vCloud Air ■ vCloud Director 	<ul style="list-style-type: none"> ■ (선택 사항) 게스트 에이전트 ■ (선택 사항) 소프트웨어 부트스트랩 에이전트 및 게스트 에이전트 	vCloud Air 또는 vCloud Director 복제	vCloud Air 및 vCloud Director 프로비저닝 준비 항목을 참조하십시오. Software를 지원하려는 경우 게스트 에이전트와 소프트웨어 부트스트랩 에이전트가 포함된 템플릿을 생성합니다. vCloud Air의 경우, vRealize Automation 환경과 vCloud Air 환경 간의 네트워크 연결을 구성합니다.
ISO 이미지에서 부팅하여 시스템을 프로비저닝하며, kickstart 또는 autoYaSt 구성 파일과 Linux 배포 이미지를 사용하여 시스템에 운영 체제를 설치합니다.	<ul style="list-style-type: none"> ■ 모든 가상 플랫폼 ■ Red Hat OpenStack 	게스트 에이전트가 준비 지침의 일부로 설치됩니다.	Linux Kickstart	Linux Kickstart 프로비저닝을 위한 준비
시스템을 프로비저닝하고 제어 기능을 SCCM 작업 시퀀스에 전달하여 ISO 이미지에서 부팅하고, Windows 운영 체제를 배포하고, vRealize Automation 게스트 에이전트를 설치합니다.	모든 가상 시스템 플랫폼.	게스트 에이전트가 준비 지침의 일부로 설치됩니다.	SCCM	SCCM 프로비저닝 준비
WinPE 환경으로 부팅하고, 기존 Windows 참조 시스템의 WIM(Windows Imaging File Format) 이미지를 사용하여 운영 체제를 설치하는 방법으로 시스템을 프로비저닝합니다.	<ul style="list-style-type: none"> ■ 모든 가상 플랫폼 ■ Red Hat OpenStack 	게스트 에이전트가 필요합니다. WinPE 이미지를 생성할 때에는 게스트 에이전트를 수동으로 삽입해야 합니다.	WIM	WIM 프로비저닝 준비

표 1-5. 준비할 시스템 프로비저닝 방법 선택 (계속)

시나리오	지원되는 플랫폼	에이전트 지원	프로비저닝 방법	사전 프로비저닝 준비
가상 시스템 이미지에서 인스턴스를 시작합니다.	Red Hat OpenStack	지원되지 않음	가상 시스템 이미지	가상 시스템 이미지 프로비저닝 준비 항목을 참조하십시오.
Amazon 시스템 이미지에서 인스턴스를 시작합니다.	Amazon AWS	<ul style="list-style-type: none"> ■ (선택 사항) 게스트 에이전트 ■ (선택 사항) 소프트웨어 부트스트랩 에이전트 및 게스트 에이전트 	Amazon 시스템 이미지	<p>Amazon 시스템 이미지와 인스턴스 유형을 Amazon AWS 계정과 연결합니다.</p> <p>Software를 지원하려면 게스트 에이전트와 소프트웨어 부트스트랩 에이전트가 포함된 Amazon 시스템 이미지를 생성하고 Amazon AWS 및 vRealize Automation 환경 간에 네트워크 및 VPC 간 연결을 구성합니다.</p>

프로비저닝 중 Visual Basic 스크립트 실행을 위한 검사 목록

시스템 프로비저닝 이전 또는 이후에 시스템 수명 주기에서 추가 단계로 사용자 지정 Visual Basic 스크립트를 실행하도록 vRealize Automation을 구성할 수 있습니다. 예를 들어 사전 프로비저닝 스크립트를 사용하여 프로비저닝 이전에 인증서 또는 보안 토큰을 생성한 다음 사후 프로비저닝 스크립트를 사용하여 시스템 프로비저닝 이후에 인증서 및 토큰을 사용할 수 있습니다. Visual Basic 스크립트를 프로비저닝 방법과 함께 실행할 수 있지만 Visual Basic 스크립트를 Amazon AWS 시스템과 함께 사용할 수는 없습니다.

표 1-6. 프로비저닝 중 Visual Basic 스크립트 실행 검사 목록

작업	위치	세부 정보
❑ Visual Basic 스크립트에 대한 EPI 에이전트를 설치 및 구성합니다.	일반적으로 Manager Service 호스트	vRealize Automation 7.3 설치의 내용을 참조하십시오.
❑ Visual Basic 스크립트를 생성합니다.	EPI 에이전트가 설치된 시스템	<p>vRealize Automation에는 EPI 에이전트 설치 디렉토리의 Scripts 하위 디렉토리의 샘플 Visual Basic 스크립트 PrePostProvisioningExample.vbs가 포함되어 있습니다. 이 스크립트에는 모든 인수를 사전에 로드하기 위한 머리글, 함수를 포함할 수 있는 본문, 업데이트된 사용자 지정 속성을 vRealize Automation로 반환하기 위한 바닥글이 포함되어 있습니다.</p> <p>Visual Basic 스크립트를 실행하면 EPI 에이전트가 모든 시스템 사용자 지정 속성을 인수로 스크립트에 전달합니다. 업데이트된 속성 값을 vRealize Automation로 반환하려면 이러한 속성을 사전에 배치하고 vRealize Automation에서 제공하는 함수를 호출합니다.</p>
❑ Blueprint의 스크립트에 포함하는데 필요한 정보를 수집합니다.	<p>정보를 캡처하고 인프라 설계자에게 전송</p> <p>참고 패브릭 관리자는 ExternalPreProvisioningVbScript 및 ExternalPostProvisioningVbScript 속성 집합을 사용하여 이 필수 정보를 제공하는 속성 그룹을 생성할 수 있습니다. 이렇게 하면 Blueprint 설계자가 이 정보를 자신의 Blueprint에 정확하게 포함하기가 더 쉽습니다.</p>	<ul style="list-style-type: none"> ■ 파일 이름과 확장명이 포함된 Visual Basic 스크립트의 완전한 경로입니다. 예: %System Drive\%Program Files (x86)\VMware\WvCAC\Agents\WEPI_Agents\WScripts\WSendEmail.vbs ■ 프로비저닝 전에 스크립트를 실행하려면 인프라 설계자가 스크립트에 대한 전체 경로를 사용자 지정 속성 ExternalPreProvisioningVbScript의 값으로 입력하도록 지시합니다. 프로비저닝 후에 스크립트를 실행하려면 사용자 지정 속성 ExternalPostProvisioningVbScript를 사용해야 합니다.

프로비저닝에서 vRealize Automation 게스트 에이전트 사용

배포 후 시스템을 추가로 사용자 지정하기 위해 참조 시스템에 게스트 에이전트를 설치할 수 있습니다. 예약된 게스트 에이전트 사용자 지정 속성을 사용하여 디스크 추가 및 포맷과 같은 기본 사용자 지정을 수행하거나 게스트 에이전트용 사용자 지정 스크립트를 직접 생성하여 프로비저닝된 시스템의 게스트 운영 체제 내에서 실행할 수 있습니다.

배포가 완료되고 사용자 지정 정의(제공한 경우)가 실행된 후 게스트 에이전트는 배포된 시스템의 사용자 지정 속성이 모두 포함된 XML 파일(c:\WVRMGuestAgent\site\workitem.xml)을 생성하고 게스트 에이전트 사용자 지정 속성을 사용하여 여기에 할당된 모든 작업을 완료한 다음 프로비저닝된 시스템에서 자체적으로 삭제됩니다.

배포된 시스템에서 실행될 게스트 에이전트용 사용자 지정 스크립트를 생성하고 시스템 Blueprint의 사용자 지정 속성을 사용하여 해당 스크립트의 위치와 실행 순서를 지정할 수 있습니다. 또한 시스템 Blueprint의 사용자 지정 속성을 사용하여 사용자 지정 속성 값을 스크립트에 매개 변수로 전달할 수도 있습니다.

예를 들어 게스트 에이전트를 사용하여 배포된 시스템을 다음과 같이 사용자 지정할 수 있습니다.

- IP 주소 변경
- 드라이브 추가 또는 포맷
- 보안 스크립트 실행
- Puppet 또는 Chef와 같은 다른 에이전트 초기화

명령줄 인수에서 암호화된 문자열을 사용자 지정 속성으로 제공할 수도 있습니다. 그러면 게스트 에이전트가 암호 해독하고 올바른 명령줄 인수로 인식할 수 있는 암호화된 정보를 저장할 수 있습니다.

참고 Linux 게스트 에이전트는 작업 항목의 vRealize Automation 사용자 지정 속성을 기준으로 Linux Kickstart 및 PXE 프로비저닝을 위한 생성 및 복제 작업 중에 정적 IP를 할당합니다. 게스트 에이전트는 정적 IP를 할당할 때 Ubuntu 16.x와 같은 새로운 일관된 네트워크 이름 지정 체계를 사용할 수 없습니다.

사용자 지정 스크립트를 시스템에 로컬로 설치할 필요는 없습니다. 프로비저닝된 시스템이 스크립트 위치에 네트워크 액세스할 수 있으면 게스트 에이전트가 스크립트를 액세스하고 실행할 수 있습니다. 모든 템플릿을 다시 구축하지 않고도 스크립트를 업데이트할 수 있기 때문에 이는 유지 보수 비용을 줄여줍니다.

예약, Blueprint 또는 게스트 에이전트 스크립트에 정보를 지정하여 가상 시스템에 대한 보안 설정이 프로비저닝되도록 구성할 수 있습니다. 프로비저닝된 시스템에 게스트 에이전트가 필요한 경우 예약 또는 Blueprint에 대한 요구 사항을 포함하는 보안 규칙을 추가해야 합니다. 예를 들어, 모든 시스템 간의 통신을 거부하는 기본 보안 정책을 사용하고 별도의 보안 정책에 의존하여 특정 시스템 간의 통신을 허용하는 경우 게스트 에이전트는 사용자 지정 단계 중 vRealize Automation과 통신하지 못할 수 있습니다. 시스템 프로비저닝 중에 이러한 문제를 피하려면 사용자 지정 단계 중 통신을 허용하는 기본 보안 정책을 사용합니다.

프로비저닝된 시스템에서 사용자 지정 스크립트를 실행할 게스트 에이전트를 설치하기로 선택한 경우에는 Blueprint에 적절한 게스트 에이전트 사용자 지정 속성이 포함되어야 합니다. 예를 들어 복제를 위해 템플릿에 게스트 에이전트를 설치하고, 프로비저닝된 시스템의 IP 주소를 변경하는 사용자 지정 스크립트를 생성하고, 스크립트를 공유 위치에 저장하는 경우에는 Blueprint에 여러 개의 사용자 지정 속성을 포함해야 합니다.

표 1-7. 게스트 에이전트로 프로비저닝된 시스템의 IP 주소를 변경하기 위한 사용자 지정 속성

사용자 지정 속성	설명
VirtualMachine.Admin.UseGuestAgent	프로비저닝된 시스템이 시작될 때 게스트 에이전트를 초기화하려면 true 로 설정합니다.
VirtualMachine.Customize.WaitComplete	모든 사용자 지정이 완료될 때까지 프로비저닝 워크플로가 게스트 에이전트에 작업 항목을 전송하지 못하도록 하려면 True 로 설정합니다.

표 1-7. 게스트 에이전트로 프로비저닝된 시스템의 IP 주소를 변경하기 위한 사용자 지정 속성 (계속)

사용자 지정 속성	설명
VirtualMachine.SoftwareN.ScriptPath	<p>애플리케이션 설치 스크립트에 대한 전체 경로를 지정합니다. 경로는 게스트 운영 체제에서 확인된 유효한 절대 경로여야 하며 스크립트 파일 이름을 포함해야 합니다.</p> <p>경로 문자열에 {CustomPropertyName}을 삽입하여 스크립트에 사용자 지정 속성 값을 매개 변수로 전달할 수 있습니다. 예를 들어, 값이 1234인 ActivationKey라는 이름의 사용자 지정 속성이 있는 경우 스크립트 경로는 D:\InstallApp.bat -key {ActivationKey}입니다. 게스트 에이전트가 명령 D:\InstallApp.bat -key 1234를 실행합니다. 그런 다음 이 값을 승인하고 사용하도록 스크립트 파일을 프로그래밍할 수 있습니다.</p> <p>시스템 소유자 이름을 스크립트에 전달하려면 {Owner}를 삽입합니다.</p> <p>경로 문자열에 {YourCustomProperty}를 삽입하여 사용자 지정 속성 값을 스크립트에 매개 변수로 전달할 수도 있습니다. 예를 들어</p> <p>값 <code>\\\\vra-scripts.mycompany.com\\scripts\\changeIP.bat</code>를 입력하면 공유 위치에서 changeIP.bat 스크립트가 실행되지만, 값 <code>\\\\vra-scripts.mycompany.com\\scripts\\changeIP.bat {VirtualMachine.Network0.Address}</code>를 입력하면 changeIP 스크립트가 실행되며 VirtualMachine.Network0.Address 속성의 값이 스크립트에 매개 변수로 전달됩니다.</p>
VirtualMachine.ScriptPath.Decrypt	<p>vRealize Automation에서 gagent 명령줄에 올바른 형식의 VirtualMachine.SoftwareN.ScriptPath 사용자 지정 속성 문자열로 전달되는 암호화된 문자열을 가져올 수 있도록 합니다.</p> <p>암호와 같은 암호화된 문자열을 명령줄 인수에서 사용자 지정 속성으로 제공할 수 있습니다. 이렇게 하면 게스트 에이전트가 암호 해독하고 올바른 명령줄 인수로 인식할 수 있는 암호화된 정보를 저장할 수 있습니다. 예를 들어</p> <p>VirtualMachine.Software0.ScriptPath = c:\Wdosomething.bat <i>password</i> 사용자 지정 속성 문자열은 실제 암호가 포함되어 있으므로 안전하지 않습니다.</p> <p>암호를 암호화하려면 vRealize Automation 사용자 지정 속성(예: MyPassword = password)을 생성하고 사용 가능한 확인란을 선택하여 암호화를 사용하도록 설정합니다. 게스트 에이전트는 [MyPassword] 항목을 사용자 지정 속성 MyPassword의 값으로 암호 해독하고 스크립트를 c:\Wdosomething.bat password로 실행합니다.</p> <ul style="list-style-type: none"> ■ 사용자 지정 속성 MyPassword = password를 생성합니다. 여기서 password는 실제 암호의 값입니다. 사용 가능한 확인란을 선택하여 암호화를 사용하도록 설정합니다. ■ 사용자 지정 속성 VirtualMachine.ScriptPath.Decrypt를 VirtualMachine.ScriptPath.Decrypt = true로 설정합니다.

표 1-7. 게스트 에이전트로 프로비저닝된 시스템의 IP 주소를 변경하기 위한 사용자 지정 속성 (계속)

사용자 지정 속성	설명
	<ul style="list-style-type: none"> ■ 사용자 지정 속성 <code>VirtualMachine.Software0.ScriptPath</code>를 <code>VirtualMachine.Software0.ScriptPath =</code> <code>c:\Wdosomething.bat [MyPassword]</code>로 설정합니다. <code>VirtualMachine.ScriptPath.Decrypt</code>를 <code>false</code>로 설정하거나 <code>VirtualMachine.ScriptPath.Decrypt</code> 사용자 지정 속성을 생 성하지 않으면 대괄호로 묶인 문자열([and])이 암호 해독 되지 않습니다.

게스트 에이전트와 함께 사용할 수 있는 사용자 지정 속성에 대한 자세한 내용은 사용자 지정 속성 참
조 자료 항목을 참조하십시오.

서버를 신뢰하도록 게스트 에이전트 구성

게스트 에이전트가 서버를 신뢰하도록 구성하는 가장 안전한 방법은 vRealize Automation
Manager Service 호스트에 대한 공용 키 PEM 파일을 올바른 게스트 에이전트 폴더에 설치하는 것
입니다.

Manager Service 호스트가 서버를 신뢰하도록 각 템플릿에서 `cert.pem` PEM 파일에 대한 게스트
에이전트 폴더를 찾으십시오.

- `gugent`를 사용하는 각 템플릿의 Windows 게스트 에이전트 폴더

```
C:\WVRMGuestAgent\cert.pem
```

- `gugent`를 사용하는 각 템플릿의 Linux 게스트 에이전트 폴더

```
/usr/share/gugent/cert.pem
```

`cert.pem` 파일을 이 위치에 두지 않을 경우 템플릿 참조 시스템이 게스트 에이전트를 사용할 수 없
습니다. 예를 들어 스크립트를 변경하여 VM이 시작된 후 공용 키 정보를 수집하려고 시도하는 경
우 보안 조건을 위반하게 됩니다.

구성된 환경에 따라 추가 고려 사항이 적용됩니다.

- WIM 설치의 경우 콘솔 실행 파일 및 사용자 인터페이스에 공용 키 PEM 파일 콘텐츠를 추가해야
합니다. 콘솔 플래그는 `/cert filename`입니다.
- RedHat kickstart 설치의 경우 공용 키를 샘플 파일에 잘라내 붙여넣지 않으면 게스트 에이전트
실행이 실패합니다.
- SCCM 설치의 경우 `cert.pem` 파일이 `VRMGuestAgent` 폴더에 상주해야 합니다.

- Linux vSphere 설치의 경우 cert.pem 파일이 /usr/share/gugent 폴더에 상주해야 합니다.

참고 필요한 경우 다음 스크립트를 <https://APPLIANCE/software/index.html>에서 다운로드하여 소프트웨어와 게스트 에이전트를 함께 설치할 수 있습니다. 해당 스크립트를 사용하면 템플릿 생성 시 SSL 인증서 지문 수락을 처리할 수 있습니다.

- Linux
prepare_vra_template.sh
- Windows
prepare_vra_template.ps1

소프트웨어와 게스트 에이전트를 함께 설치하는 경우 [Linux 참조 시스템에 게스트 에이전트 설치](#) 또는 [Windows 참조 시스템에 게스트 에이전트 설치](#)의 지침을 사용하지 않아도 됩니다.

Linux 참조 시스템에 게스트 에이전트 설치

Linux 게스트 에이전트를 참조 시스템에 설치하여 배포 이후에 시스템을 추가적으로 사용자 지정할 수 있습니다.

필수 조건

- 참조 시스템을 확인하거나 생성합니다.
- 다운로드한 게스트 에이전트 파일에는 tar.gz 및 RPM 패키지 형식이 둘 모두 들어 있습니다. 운영 체제에서 tar.gz 파일이나 RPM 파일을 설치할 수 없는 경우에는 변환 도구를 이용하여 설치 파일을 기본 패키지 형식으로 변환합니다.
- 게스트 에이전트와 Manager Service 시스템 간에 안전한 신뢰 관계를 구성합니다. [서버를 신뢰하도록 게스트 에이전트 구성](#) 항목을 참조하십시오.

프로시저

- 1 vRealize Automation 장치 관리 콘솔 페이지로 이동합니다.
예: <https://va-hostname.domain.com>.
- 2 페이지의 vRealize Automation 구성 요소 설치 섹션에서 **게스트 및 소프트웨어 에이전트 페이지**를 클릭합니다.
예: <https://va-hostname.domain.com/software/index.html>.
게스트 및 소프트웨어 에이전트 설치 관리자 페이지가 열리고 사용 가능한 다운로드에 대한 링크가 표시됩니다.
- 3 페이지의 게스트 에이전트 설치 관리자 섹션에서 **Linux 게스트 에이전트 패키지**를 클릭하고 LinuxGuestAgentPkgs.zip 파일을 다운로드하여 저장합니다.
- 4 다운로드한 LinuxGuestAgentPkgs.zip 파일의 압축을 풀어서 VraLinuxGuestAgent 폴더를 생성합니다.

- 5 프로비저닝하는 동안 배포하는 게스트 운영 체제에 해당하는 게스트 에이전트 패키지를 설치합니다.
 - a 프로비저닝 중에 배포할 게스트 운영 체제에 해당하는 VraLinuxGuestAgent 하위 디렉토리(예: rhel32)로 이동합니다.
 - b 기본 패키지 형식을 찾거나 패키지를 기본 패키지 형식으로 변환합니다.
 - c 게스트 에이전트 패키지를 참조 시스템에 설치합니다.

예를 들어 RPM 패키지의 파일을 설치하려면 `rpm -i gugent-gugent-7.1.0-4201531.i386.rpm`을 실행합니다.

- 6 `installgugent.sh Manager_Service_Hostname_fdqn:portnumber ssl platform`을 실행하여 게스트 에이전트가 Manager Service와 통신할 수 있도록 구성합니다.

Manager Service의 기본 포트 번호는 443입니다. 허용되는 플랫폼 값은 ec2, vcd, vca 및 vsphere입니다.

옵션	설명
로드 밸런서를 사용하고 있는 경우	<p>Manager Service 로드 밸런서의 정규화된 도메인 이름과 포트 번호를 입력합니다. 예:</p> <pre>cd /usr/share/gugent ./installgugent.sh load_balancer_manager_service.mycompany.com:443 ssl ec2</pre>
로드 밸런서를 사용하지 않는 경우	<p>Manager Service 시스템의 정규화된 도메인 이름과 포트 번호를 입력합니다. 예:</p> <pre>cd /usr/share/gugent ./installgugent.sh manager_service_machine.mycompany.com:443 ssl vsphere</pre>

- 7 배포된 시스템이 Manager Service SSL 인증서를 신뢰하도록 아직 구성되지 않은 경우에는 참조 시스템에 `cert.pem` 파일을 설치하여 신뢰 관계를 구성해야 합니다.
 - `cert.pem` 인증서를 가져와서 참조 시스템에 파일을 수동으로 설치하는 방법이 가장 안전합니다.
 - 더 편리한 방법을 사용하려면 Manager Service 로드 밸런서 또는 Manager Service 시스템에 연결하여 `cert.pem` 인증서를 다운로드하십시오.

옵션	설명
로드 밸런서를 사용하고 있는 경우	<p>참조 시스템의 루트 사용자 역할로 다음과 같은 명령을 실행합니다.</p> <pre>echo openssl s_client -connect manager_service_load_balancer.mycompany.com:443 sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>
로드 밸런서를 사용하지 않는 경우	<p>참조 시스템의 루트 사용자 역할로 다음과 같은 명령을 실행합니다.</p> <pre>echo openssl s_client -connect manager_service_machine.mycompany.com:443 sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>

- 8 게스트 에이전트를 Ubuntu 운영 체제에 설치하는 경우에는 다음 명령 집합 중 하나를 실행하여 공유 개체에 대한 심볼 링크를 생성합니다.

옵션	설명
64비트 시스템	<pre>cd /lib/x86_64-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>
32비트 시스템	<pre>cd /lib/i386-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>

후속 작업

참조 시스템을 복제를 위한 템플릿, Amazon 시스템 이미지 또는 IaaS 설계자가 Blueprint 생성 시 사용할 수 있는 스냅샷으로 변환합니다.

Windows 참조 시스템에 게스트 에이전트 설치

Windows 참조 시스템에 vRealize Automation Windows 게스트 에이전트를 설치하여 Windows 서비스로 실행하고 시스템의 추가 사용자 지정을 사용하도록 설정합니다.

필수 조건

- 참조 시스템을 확인하거나 생성합니다.
- 게스트 에이전트와 Manager Service 시스템 간에 안전한 신뢰 관계를 구성합니다. [서버를 신뢰하도록 게스트 에이전트 구성](#) 항목을 참조하십시오.

프로시저

- vRealize Automation 장치 **게스트 및 소프트웨어 에이전트 설치 관리자** 페이지로 이동합니다.
<https://vrealize-automation-appliance-FQDN/software>
- 게스트 에이전트 설치 관리자** 아래에서 32비트 또는 64비트 실행 파일을 다운로드하고 C: 드라이브의 루트에 저장합니다.

참고 게스트 에이전트 설치 절차에 대한 명령줄 대안이 있습니다. 실행 파일을 다운로드하는 대신 [게스트 및 소프트웨어 에이전트 설치 관리자] 페이지의 **Windows 소프트웨어 설치 관리자**로 이동할 수 있습니다. 여기서 prepare_vra_template.ps1 PowerShell 스크립트를 다운로드하여 실행할 수 있습니다.

```
PowerShell -NoProfile -ExecutionPolicy Bypass -Command prepare_vra_template.ps1
```

- 실행 파일을 실행하여 Windows 게스트 에이전트 파일을 추출합니다.
추출이 완료되면 C:\WVRMGuestAgent가 생성되고 파일이 추가됩니다.
C:\WVRMGuestAgent의 이름을 변경하지 마십시오.

4 게스트 에이전트가 Manager Service와 통신할 수 있도록 구성합니다.

- a 관리자 권한으로 명령 프롬프트를 엽니다.
- b C:\WVRMGuestAgent로 이동합니다.
- c C:\WVRMGuestAgent\ 디렉토리에 신뢰할 수 있는 Manager Service PEM 파일을 위치시켜 Manager Service 시스템을 신뢰하도록 게스트 에이전트를 구성합니다.
- d `win service -i -h Manager_Service_Hostname_fqdn:portnumber -p ssl`를 실행합니다.

Manager Service의 기본 포트 번호는 443입니다.

옵션	설명
로드 밸런서를 사용하고 있는 경우	Manager Service 로드 밸런서의 정규화된 도메인 이름과 포트 번호를 입력합니다. 예를 들어 <code>win service -i -h load_balancer_manager_service.mycompany.com:443 -p ssl</code> 을 입력합니다.
로드 밸런서를 사용하지 않는 경우	Manager Service 시스템의 정규화된 도메인 이름과 포트 번호를 입력합니다. 예를 들어 <code>win service -i -h manager_service_machine.mycompany.com:443 -p ssl</code> 을 입력합니다.
Amazon 시스템 이미지를 준비 중인 경우	Amazon 사용을 지정해야 합니다. 예를 들어 다음과 같이 지정합니다. <code>win service -i -h manager_service_machine.mycompany.com:443:443 -p ssl -c ec2</code>

Windows 서비스의 이름은 VCACGuestAgentService입니다. C:\WVRMGuestAgent에서 설치 로그 VCAC-GuestAgentService.log를 찾을 수 있습니다.

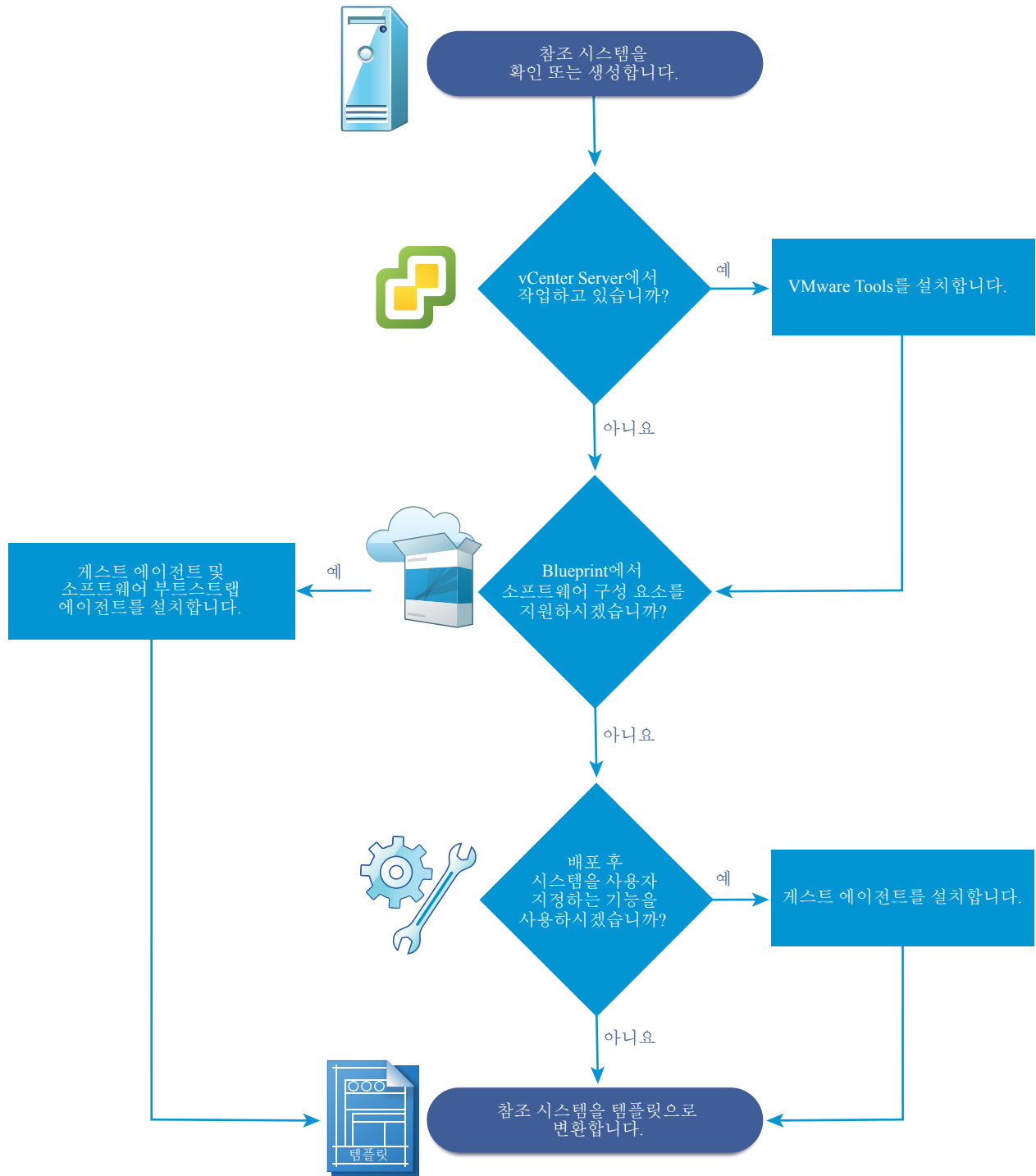
후속 작업

IaaS 설계자가 Blueprint 생성 시 템플릿을 사용할 수 있도록 참조 시스템을 복제를 위한 템플릿, Amazon 시스템 이미지 또는 스냅샷으로 변환합니다.

복제를 통한 프로비저닝 준비를 위한 검사 목록

Linux 및 Windows 가상 시스템을 복제하는 데 사용되는 템플릿과 사용자 지정 개체를 생성하려면 vRealize Automation 외부에서 몇 가지 준비 작업을 수행해야 합니다.

복제를 수행하려면 복제 원본으로 사용할 템플릿이 필요하며, 이 템플릿은 참조 시스템에서 생성됩니다.



복제를 통해 Windows 시스템을 프로비저닝하는 경우, 프로비저닝된 시스템을 Active Directory 도메인에 가입시키는 방법은 vCenter Server에서 사용자 지정 규격을 사용하거나 SCVMM 템플릿에 게스트 운영 체제 프로파일을 포함하는 방법뿐입니다. 복제를 통해 프로비저닝된 시스템은 프로비저닝을 수행하는 동안에는 Active Directory 컨테이너에 배치할 수 없습니다. 이 작업은 프로비저닝 후에 수동으로 수행해야 합니다.

표 1-8. 복제를 통한 프로비저닝 준비를 위한 검사 목록

작업	위치	세부 정보
<input type="checkbox"/> 참조 시스템을 식별하거나 생성합니다.	하이퍼바이저	하이퍼바이저가 제공한 설명서를 참조하십시오.
<input type="checkbox"/> (선택 사항) 복제 템플릿에서 Software 구성 요소를 지원하도록 구성하려면 참조 시스템에 vRealize Automation 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치합니다.	참조 시스템	Windows 참조 시스템의 경우 Software 지원을 위해 Windows 참조 시스템 준비 항목을 참조하십시오. Linux 참조 시스템의 경우 Software 지원을 위해 Linux 참조 시스템 준비 항목을 참조하십시오.
<input type="checkbox"/> (선택 사항) 복제 템플릿에서 Software 구성 요소를 지원할 필요가 없지만 배포된 시스템에 대한 사용자 지정 기능이 필요하면 참조 시스템에 vRealize Automation 게스트 에이전트를 설치합니다.	참조 시스템	프로비저닝에서 vRealize Automation 게스트 에이전트 사용 항목을 참조하십시오.
<input type="checkbox"/> vCenter Server 환경에서 작업 중인 경우 참조 시스템에 VMware Tools를 설치합니다.	vCenter Server	VMware Tools 설명서를 참조하십시오.
<input type="checkbox"/> 참조 시스템을 사용하여 복제용 템플릿을 생성합니다.	하이퍼바이저	참조 시스템은 전원이 켜져 있거나 꺼져 있을 수 있습니다. vCenter Server에서 복제하는 경우에는 템플릿을 생성하지 않고 참조 시스템을 직접 사용할 수 있습니다. 하이퍼바이저가 제공한 설명서를 참조하십시오.
<input type="checkbox"/> System Preparation Utility 정보 또는 Linux 사용자 지정을 적용하여, 복제된 시스템을 구성할 사용자 지정 개체를 생성합니다.	하이퍼바이저	Linux용으로 복제하는 경우에는 사용자 지정 개체를 생성하는 대신 Linux 게스트 에이전트를 설치하고 외부 사용자 지정 스크립트를 제공합니다. vCenter Server를 사용하여 복제하는 경우에는 사용자 지정 규격을 사용자 지정 개체로 제공해야 합니다. 하이퍼바이저가 제공한 설명서를 참조하십시오.
<input type="checkbox"/> 템플릿을 복제하는 Blueprint를 생성하는 데 필요한 정보를 수집합니다.	정보를 캡처하고 IaaS 설계자에게 전송합니다.	복제를 통한 가상 프로비저닝용 워크시트 항목을 참조하십시오.

복제를 통한 가상 프로비저닝용 워크시트

환경에서 준비한 템플릿을 위한 복제 Blueprint를 생성하는 데 필요한 템플릿, 사용자 지정 및 사용자 지정 속성에 대한 정보를 캡처하기 위해 지식 전달 워크시트를 작성합니다. 이 모든 정보가 모든 구형에 필요한 것은 아닙니다. 이 워크시트를 가이드로 사용하거나 워크시트 테이블을 편집을 위한 워드 프로세싱 도구에 복사하여 붙여넣습니다.

필수 템플릿 및 예약 정보

표 1-9. 템플릿 및 예약 정보 워크시트

필수 정보	내 값	세부 정보
템플릿 이름		
템플릿을 사용할 수 있는 예약 또는 적용할 예약 정책		프로비저닝 중 오류를 방지하려면 모든 예약에서 템플릿을 사용할 수 있는지 확인하거나 설계자가 템플릿을 사용할 수 있는 예약으로 Blueprint를 제한하는 데 사용할 수 있는 예약 정책을 생성합니다.
(vSphere에만 해당) 이 템플릿에 대해 요청된 복제 유형		<ul style="list-style-type: none"> ■ 복제 ■ 연결된 복제 ■ NetApp FlexClone
사용자 지정 구역 이름(정적 IP 주소를 사용한 복제에 필요)		사용자 지정 구역 개체 없이 Windows 시스템의 사용자 지정을 수행할 수 없습니다.
(SCVMM에만 해당) ISO 이름		
(SCVMM에만 해당) 가상 하드 디스크		
(SCVMM에만 해당) 프로비저닝된 시스템에 연결할 하드웨어 프로파일		

필수 속성 그룹

워크시트의 사용자 지정 속성 정보 섹션을 작성하거나 속성 그룹을 생성하고 수많은 개별 사용자 지정 속성 대신 속성 그룹을 Blueprint에 추가하도록 설계자에게 요청할 수 있습니다.

필수 vCenter Server 운영 체제

vCenter Server 프로비저닝을 위한 게스트 운영 체제 사용자 지정 속성을 제공해야 합니다.

표 1-10. vCenter Server 운영 체제

사용자 지정 속성	내 값	설명
VMware.VirtualCenter.OperatingSystem		vCenter Server에서 시스템을 생성할 때 사용하는 vCenter Server 게스트 운영 체제 버전 (VirtualMachineGuestOsIdentifier)을 지정합니다. 이 운영 체제 버전은 프로비저닝된 시스템에 설치될 운영 체제 버전과 일치해야 합니다. 관리자는 올바른 VMware.VirtualCenter.OperatingSystem 값을 포함하도록 미리 정의된 여러 개의 속성 집합 중 하나(예: VMware[OS_Version]Properties)를 사용하여 속성 그룹을 생성할 수 있습니다. 이 속성은 가상 프로비저닝을 위한 것입니다.

Visual Basic 스크립트 정보

시스템 수명 주기에서 추가 단계로 사용자 지정 Visual Basic 스크립트를 실행하도록 vRealize Automation을 구성한 경우 Blueprint에 스크립트에 대한 정보를 포함해야 합니다.

참고 패브릭 관리자는 ExternalPreProvisioningVbScript 및 ExternalPostProvisioningVbScript 속성 집합을 사용하여 이 필수 정보를 제공하는 속성 그룹을 생성할 수 있습니다. 이렇게 하면 Blueprint 설계자가 이 정보를 자신의 Blueprint에 정확하게 포함 하기가 더 쉽습니다.

표 1-11. Visual Basic 스크립트 정보

사용자 지정 속성	내 값	설명
ExternalPreProvisioningVbScript		프로비저닝 전에 스크립트를 실행합니다. 파일 이름 및 확장명을 포함하여 스크립트에 대한 완전한 경로를 입력합니다. <code>%System Drive%Program Files (x86)VMwareWvCAC AgentsWEPI_AgentsWScriptsWSendEmail.vbs.</code>
ExternalPostProvisioningVbScript		프로비저닝 후에 스크립트를 실행합니다. 파일 이름 및 확장명을 포함하여 스크립트에 대한 완전한 경로를 입력합니다. <code>%System Drive%Program Files (x86)VMwareWvCAC AgentsWEPI_AgentsWScriptsWSendEmail.vbs</code>

Linux 게스트 에이전트 사용자 지정 스크립트 정보

사용자 지정 스크립트 실행에 게스트 에이전트를 사용하도록 Linux 템플릿을 구성한 경우 Blueprint에 스크립트에 대한 정보를 포함해야 합니다.

표 1-12. Linux 게스트 에이전트 사용자 지정 스크립트 정보 워크시트

사용자 지정 속성	내 값	설명
Linux.ExternalScript.Name		운영 체제가 설치된 후 Linux 게스트 에이전트가 실행되는 선택적 사용자 지정 스크립트의 이름(예: config.sh)을 지정합니다. 이 속성은 Linux 에이전트가 설치된 템플릿에서 복제되는 Linux 시스템에 사용할 수 있습니다. 외부 스크립트를 지정하는 경우 Linux.ExternalScript.LocationType 및 Linux.ExternalScript.Path 속성을 사용하여 해당 위치도 정의해야 합니다.
Linux.ExternalScript.LocationType		Linux.ExternalScript.Name 속성에 명명된 사용자 지정 스크립트의 위치 유형을 지정합니다. 이 값은 로컬 또는 nfs일 수 있습니다. 또한 Linux.ExternalScript.Path 속성을 사용하여 스크립트 위치도 지정해야 합니다. 위치 유형이 nfs인 경우 Linux.ExternalScript.Server 속성도 사용합니다.
Linux.ExternalScript.Server		Linux.ExternalScript.Name에 명명된 Linux 외부 사용자 지정 스크립트가 위치한 NFS 서버의 이름(예: lab-ad.lab.local)을 지정합니다.
Linux.ExternalScript.Path		Linux 사용자 지정 스크립트에 대한 로컬 경로 또는 NFS 서버의 Linux 사용자 지정에 대한 내보내기 경로를 지정합니다. 이 값은 슬래시로 시작해야 하며 파일 이름을 포함하면 안 됩니다 (예: /scripts/linux/config.sh).

기타 게스트 에이전트 사용자 지정 속성

참조 시스템에 게스트 에이전트를 설치한 경우 사용자 지정 속성을 사용하여 배포 후 추가로 시스템을 사용자 지정할 수 있습니다.

표 1-13. 게스트 에이전트를 사용하여 복제된 시스템을 사용자 지정하기 위한 사용자 지정 속성 워크시트

사용자 지정 속성	내 값	설명
VirtualMachine.Admin.AddOwnerToAdmins		VirtualMachine.Admin.Owner 속성에 지정된 대로 시스템의 소유자를 시스템의 로컬 관리자 그룹에 추가하려면 True(기본값)로 설정합니다.
VirtualMachine.Admin.AllowLogin		VirtualMachine.Admin.Owner 속성에 지정된 대로 시스템 소유자를 로컬 원격 데스크톱 사용자 그룹에 추가하려면 True(기본값)로 설정합니다.

표 1-13. 게스트 에이전트를 사용하여 복제된 시스템을 사용자 지정하기 위한 사용자 지정 속성 워크시트 (계속)

사용자 지정 속성	내 값	설명
VirtualMachine.Admin.UseGuestAgent		게스트 에이전트가 복제를 위한 템플릿에서 서비스로 설치된 경우 해당 템플릿으로 복제된 시스템에서 게스트 에이전트 서비스를 사용하도록 설정하려면 시스템 Blueprint에서 True로 설정합니다. 시스템이 시작되면 게스트 에이전트 서비스가 시작됩니다. 게스트 에이전트를 사용하지 않으려면 False로 설정합니다. False로 설정하는 경우 향상된 복제 워크플로에서 게스트 운영 체제 작업에 게스트 에이전트를 사용하지 않아 VMwareCloneWorkflow에 대한 기능이 축소됩니다. 값을 지정하지 않거나 False 이외의 다른 값으로 설정하면 향상된 복제 워크플로가 작업 항목을 게스트 에이전트로 보냅니다.
VirtualMachine.DiskN.Active		시스템 디스크 N을 활성으로 지정하려면 True(기본값)로 설정합니다. 시스템 디스크 N을 비활성으로 지정하려면 False(기본값)로 설정합니다.
VirtualMachine.DiskN.Size		디스크 N의 크기를 GB 단위로 정의합니다. 예를 들어, 디스크 G의 크기를 150GB로 지정하려는 경우 사용자 지정 속성을 VirtualMachine.Disk0.Size로 정의하고 값 150을 입력합니다. 디스크 번호 지정은 순차적이어야 합니다. 기본적으로 시스템에는 VirtualMachine.Disk0.Size에서 참조하는 하나의 디스크가 있습니다. 여기서 크기는 시스템이 프로비저닝되는 Blueprint의 스토리지 값에 의해 지정됩니다. Blueprint 사용자 인터페이스의 스토리지 값은 VirtualMachine.Disk0.Size 속성의 값을 덮어씁니다. VirtualMachine.Disk0.Size 속성은 Blueprint의 스토리지 옵션과의 관계로 인해 사용자 지정 속성으로 사용할 수 없습니다. VirtualMachine.Disk1.Size, VirtualMachine.Disk2.Size 등을 지정하여 다른 디스크를 추가할 수 있습니다. VirtualMachine.Admin.TotalDiskUsage는 항상 .DiskN.Size 속성의 총계와 VMware.Memory.Reservation 크기 할당을 더한 값을 나타냅니다.
VirtualMachine.DiskN.Label		시스템 디스크 N에 대한 레이블을 지정합니다. 디스크 레이블은 최대 32자입니다. 디스크 번호 지정은 순차적이어야 합니다. 게스트 에이전트와 함께 사용될 때, 게스트 운영 체제 내 시스템 디스크 N의 레이블을 지정합니다.

표 1-13. 게스트 에이전트를 사용하여 복제된 시스템을 사용자 지정하기 위한 사용자 지정 속성 워크시트 (계속)

사용자 지정 속성	내 값	설명
VirtualMachine.DiskN.Letter		시스템 디스크 N의 드라이브 문자 또는 마운트 지점을 지정합니다. 기본값은 C입니다. 예를 들어 디스크 1에 문자 D를 지정하려면 사용자 지정 속성을 VirtualMachine.Disk1.Letter로 정의하고 값 D를 입력합니다. 디스크 번호 지정은 순차적이어야 합니다. 게스트 에이전트와 함께 사용될 때, 이 값은 게스트 운영 체제의 게스트 에이전트에 의해 추가 디스크 N이 마운트되는 마운트 지점 또는 드라이브 문자를 지정합니다.
VirtualMachine.Admin.CustomizeGuestOSDelay		사용자 지정이 완료된 후 게스트 운영 체제 사용자 지정이 시작되기 전까지 대기해야 할 시간을 지정합니다. 값은 HH:MM:SS 형식이어야 합니다. 값을 설정하지 않는 경우 기본값은 1분 (00:01:00)입니다. 이 사용자 지정 속성을 포함하지 않도록 선택한 경우 게스트 에이전트 작업 항목이 완료되기 전에 가상 시스템이 재부팅되면 프로비저닝이 실패할 수 있습니다.
VirtualMachine.Customize.WaitComplete		모든 사용자 지정이 완료될 때까지 프로비저닝 워크플로가 게스트 에이전트에 작업 항목을 전송하지 못하도록 하려면 True로 설정합니다.
VirtualMachine.SoftwareN.Name		프로비저닝 중에 설치 또는 실행할 소프트웨어 애플리케이션 N이나 스크립트에 대한 설명을 지정합니다. 이 속성은 선택적인 정보용 속성입니다. 이 속성이 향상된 복제 워크플로 또는 게스트 에이전트에 대해 실제적인 기능을 하지는 않지만 사용자 인터페이스에서 사용자 지정 소프트웨어를 선택하거나 소프트웨어 사용을 보고할 때 유용합니다.

표 1-13. 게스트 에이전트를 사용하여 복제된 시스템을 사용자 지정하기 위한 사용자 지정 속성 워크시트 (계속)

사용자 지정 속성	내 값	설명
VirtualMachine.SoftwareN.ScriptPath		<p>애플리케이션 설치 스크립트에 대한 전체 경로를 지정합니다. 경로는 게스트 운영 체제에서 확인된 유효한 절대 경로여야 하며 스크립트 파일 이름을 포함해야 합니다.</p> <p>경로 문자열에 {CustomPropertyName}을 삽입하여 스크립트에 사용자 지정 속성 값을 매개 변수로 전달할 수 있습니다. 예를 들어, 값이 1234인 ActivationKey라는 이름의 사용자 지정 속성이 있는 경우 스크립트 경로는 D:\InstallApp.bat -key {ActivationKey}입니다. 게스트 에이전트가 명령 D:\InstallApp.bat -key 1234를 실행합니다. 그런 다음 이 값을 승인하고 사용하도록 스크립트 파일을 프로그래밍할 수 있습니다.</p>
VirtualMachine.SoftwareN.ISOName		<p>데이터스토어 루트를 기준으로 ISO 파일의 경로와 파일 이름을 지정합니다. 형식은</p> <p><i>/folder_name/subfolder_name/file_name.iso</i>입니다. 값을 지정하지 않으면 ISO가 마운트되지 않습니다.</p>
VirtualMachine.SoftwareN.ISOLocation		<p>애플리케이션 또는 스크립트에서 사용될 ISO 이미지 파일이 들어 있는 스토리지 경로를 지정합니다. 경로의 형식을 호스트 예약에 표시된 것과 같이 지정합니다(예: netapp-1:it_nfs_1). 값을 지정하지 않으면 ISO가 마운트되지 않습니다.</p>

네트워킹 사용자 지정 속성

사용자 지정 속성을 사용하여 시스템에서 특정 네트워크 디바이스에 대한 구성을 지정할 수 있습니다.

다음 표에는 일반적인 네트워킹 관련 사용자 지정 속성이 나와 있습니다. 관련된 추가 사용자 지정 속성은 사용자 지정 속성 참조 자료에서 복제 Blueprints의 사용자 지정 속성 및 네트워킹을 위한 사용자 지정 속성을 참조하십시오.

표 1-14. 네트워킹 구성을 위한 사용자 지정 속성

사용자 지정 속성	내 값	설명
VirtualMachine.NetworkN.Address		정적 IP 주소로 프로비저닝된 시스템에서 네트워크 디바이스 N의 IP 주소를 지정합니다.
VirtualMachine.NetworkN.MacAddressType		<p>네트워크 디바이스 N의 MAC 주소가 생성된 것인지 아니면 사용자 정의(정적)인지 나타냅니다. 이 속성은 복제에 사용할 수 있습니다.</p> <p>기본값은 생성된입니다. 값이 정적인 경우 MAC 주소를 지정하려면 VirtualMachine.NetworkN.MacAddress도 사용해야 합니다.</p> <p>VirtualMachine.NetworkN 사용자 지정 속성은 개별 Blueprint 및 시스템에 특정됩니다. 시스템이 요청되면 시스템이 예약에 할당되기 전에 네트워크 및 IP 주소 할당이 수행됩니다. Blueprint는 특정 예약에 할당되지 않을 수 있으므로 예약에서 이 속성을 사용하지 마십시오. 이 속성은 요청 시 NAT 또는 요청 시 라우팅된 네트워크에 지원되지 않습니다.</p>
VirtualMachine.NetworkN.MacAddresss		<p>네트워크 디바이스 N의 MAC 주소를 지정합니다. 이 속성은 복제에 사용할 수 있습니다.</p> <p>VirtualMachine.NetworkN.MacAddressType의 값이 생성된인 경우 이 속성에는 생성된 주소가 포함됩니다.</p> <p>VirtualMachine.NetworkN.MacAddressType의 값이 정적인 경우 이 속성은 MAC 주소를 지정합니다. ESX Server 호스트에서 프로비저닝된 가상 시스템의 경우 주소는 VMware에서 지정한 범위에 있어야 합니다. 자세한 내용은 vSphere 설명서를 참조하십시오.</p> <p>VirtualMachine.NetworkN 사용자 지정 속성은 개별 Blueprint 및 시스템에 특정됩니다. 시스템이 요청되면 시스템이 예약에 할당되기 전에 네트워크 및 IP 주소 할당이 수행됩니다. Blueprint는 특정 예약에 할당되지 않을 수 있으므로 예약에서 이 속성을 사용하지 마십시오. 이 속성은 요청 시 NAT 또는 요청 시 라우팅된 네트워크에 지원되지 않습니다.</p>

표 1-14. 네트워킹 구성을 위한 사용자 지정 속성 (계속)

사용자 지정 속성	내 값	설명
VirtualMachine.NetworkN.Name		<p>연결할 네트워크의 이름을 지정합니다. 예를 들어 시스템을 연결할 네트워크 디바이스 N을 지정합니다. 이것은 NIC(네트워크 인터페이스 카드)와 동일합니다.</p> <p>기본적으로 시스템이 프로비저닝되는 예약에서 사용할 수 있는 네트워크 경로에서 네트워크가 할당됩니다.</p> <p>VirtualMachine.NetworkN.AddressType 및 VirtualMachine.NetworkN.ProfileName도 참조하십시오.</p> <p>이 속성의 값을 사용 가능한 예약의 네트워크 이름으로 설정하여 네트워크 디바이스를 특정 네트워크에 연결할 수 있습니다. 예를 들어 연결된 예약에서 네트워크를 선택한 경우 속성의 N에 대해 0과 1을 지정하면 두 개의 NIC와 여기에 할당된 값을 갖게 됩니다.</p> <p>VirtualMachine.NetworkN 사용자 지정 속성은 Blueprint 및 시스템에 특정됩니다. 시스템이 요청되면 시스템이 예약에 할당되기 전에 네트워크 및 IP 주소 할당이 수행됩니다. Blueprint는 특정 예약에 할당되지 않을 수 있으므로 예약에서 이 속성을 사용하지 마십시오. 이 속성은 요청 시 NAT 또는 요청 시 라우팅된 네트워크에 지원되지 않습니다.</p> <p>미리 정의된 사용 가능한 네트워크 목록에서 소비자의 선택을 기반으로 이 사용자 지정 속성을 사용하여 동적으로 VirtualMachine.Network0.Name을 설정하는 방법의 예는 vRA 7에서 네트워크 선택 드롭다운 추가 블로그 게시물을 참조하십시오.</p>
VirtualMachine.NetworkN.PortID		<p>vSphere Distributed Switch와 함께 dvPort 그룹을 사용할 때 네트워크 디바이스 N에 대해 사용할 포트 ID를 지정합니다.</p> <p>VirtualMachine.NetworkN 사용자 지정 속성은 개별 Blueprint 및 시스템에 특정됩니다. 시스템이 요청되면 시스템이 예약에 할당되기 전에 네트워크 및 IP 주소 할당이 수행됩니다. Blueprint는 특정 예약에 할당되지 않을 수 있으므로 예약에서 이 속성을 사용하지 마십시오. 이 속성은 요청 시 NAT 또는 요청 시 라우팅된 네트워크에 지원되지 않습니다.</p>

표 1-14. 네트워킹 구성을 위한 사용자 지정 속성 (계속)

사용자 지정 속성	내 값	설명
VirtualMachine.NetworkN.ProfileName 및 VirtualMachine.NetworkN.NetworkProfileName		<p>네트워크 디바이스 N에 정적 IP 주소를 할당하거나 복제된 시스템의 네트워크 디바이스 N에 할당할 수 있는 정적 IP 주소의 범위를 가져올 네트워크 프로파일의 이름을 지정합니다. 여기서 N=0은 첫 번째 디바이스, 1은 두 번째 디바이스 등의 순서입니다.</p> <ul style="list-style-type: none"> ■ 해당하는 네트워크 프로파일이 있는지 여부에 관계없이 VirtualMachine.NetworkN.ProfileName을 사용하여 예약에서 네트워크를 선택합니다. ■ 동일한 이름으로 해당하는 네트워크 프로파일이 있는 네트워크만 선택하려면 VirtualMachine.NetworkN.NetworkProfileName을 사용합니다. <p>속성이 가리키는 네트워크 프로파일은 IP 주소를 할당하는 데 사용됩니다. 하지만 프로비저닝된 시스템이 라운드 로빈 방식 모델을 사용하여 예약에서 선택되는 네트워크에 연결됩니다.</p>
<ul style="list-style-type: none"> ■ VirtualMachine.NetworkN.SubnetMask ■ VirtualMachine.NetworkN.Gateway ■ VirtualMachine.NetworkN.PrimaryDns ■ VirtualMachine.NetworkN.SecondaryDns ■ VirtualMachine.NetworkN.PrimaryWins ■ VirtualMachine.NetworkN.SecondaryWins ■ VirtualMachine.NetworkN.DnsSuffix ■ VirtualMachine.NetworkN.DnsSearchSuffixes 		<p>이름을 추가하면 여러 버전의 사용자 지정 속성을 생성할 수 있습니다. 예를 들어, 다음 속성은 높은, 보통 그리고 낮은 성능 요구 사항을 가진 시스템 및 일반적인 용도를 위해 설정된 로드 밸런싱 풀을 나열할 수 있습니다.</p> <ul style="list-style-type: none"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low <p>VirtualMachine.NetworkN.ProfileName에 지정된 네트워크 프로파일의 특성을 구성합니다.</p>

표 1-14. 네트워킹 구성을 위한 사용자 지정 속성 (계속)

사용자 지정 속성	내 값	설명
VCNS.LoadBalancerEdgePool.Names.name		<p>프로비저닝 중 가상 시스템이 할당되는 NSX 로드 밸런싱 풀을 지정합니다. 가상 시스템이 지정된 전체 풀의 모든 서비스 포트에 할당됩니다. 값은 Edge/풀 이름 또는 쉼표로 구분된 Edge/풀 이름의 목록입니다. 이름은 대/소문자를 구분합니다.</p> <p>이름을 추가하면 여러 버전의 사용자 지정 속성을 생성할 수 있습니다. 예를 들어, 다음 속성은 높은, 보통 그리고 낮은 성능 요구 사항을 가진 시스템 및 일반적인 용도를 위해 설정된 로드 밸런싱 풀을 나열할 수 있습니다.</p> <ul style="list-style-type: none"> VCNS.LoadBalancerEdgePool.Names VCNS.LoadBalancerEdgePool.Names.moderate VCNS.LoadBalancerEdgePool.Names.high VCNS.LoadBalancerEdgePool.Names.low
VCNS.SecurityGroup.Names.name		<p>프로비저닝 중 가상 시스템이 할당되는 NSX 보안 그룹을 지정합니다. 값은 보안 그룹 이름 또는 쉼표로 구분된 이름의 목록입니다. 이름은 대/소문자를 구분합니다.</p> <p>이름을 추가하면 여러 버전의 속성을 생성할 수 있습니다. 이러한 속성은 개별적으로 사용하거나 조합하여 사용할 수 있습니다. 예를 들어 다음 속성은 일반적인 용도, 영업 부서 및 지원을 위한 보안 그룹을 나열할 수 있습니다.</p> <ul style="list-style-type: none"> VCNS.SecurityGroup.Names VCNS.SecurityGroup.Names.sales VCNS.SecurityGroup.Names.support
VCNS.SecurityTag.Names.name		<p>프로비저닝 중 가상 시스템을 연결할 NSX 보안 태그를 지정합니다. 값은 보안 태그 이름 또는 쉼표로 구분된 이름의 목록입니다. 이름은 대/소문자를 구분합니다.</p> <p>이름을 추가하면 여러 버전의 속성을 생성할 수 있습니다. 이러한 속성은 개별적으로 사용하거나 조합하여 사용할 수 있습니다. 예를 들어 다음 속성은 일반적인 용도, 영업 부서 및 지원을 위한 보안 태그를 나열할 수 있습니다.</p> <ul style="list-style-type: none"> VCNS.SecurityTag.Names VCNS.SecurityTag.Names.sales VCNS.SecurityTag.Names.support

vCloud Air 및 vCloud Director 프로비저닝 준비

vRealize Automation을 사용하여 vCloud Air 및 vCloud Director 시스템의 프로비저닝을 준비하려면 템플릿과 사용자 지정 개체를 이용하여 조직 가상 데이터 센터를 구성해야 합니다.

vRealize Automation을 사용하여 vCloud Air 및 vCloud Director 리소스를 프로비저닝하려면 하나 이상의 시스템 리소스로 구성되고 복제 원본으로 사용할 수 있는 템플릿이 조직에 필요합니다.

조직 사이에 공유될 템플릿은 공용 템플릿이어야 합니다. 예약된 템플릿만 vRealize Automation에서 복제 원본으로 사용할 수 있습니다.

참고 템플릿에서 복제하는 방법으로 Blueprint를 생성하면 해당 템플릿의 고유한 식별자가 Blueprint에 연결됩니다. Blueprint를 vRealize Automation 카탈로그에 게시하여 프로비저닝 및 데이터 수집 프로세스에서 사용하면 연결된 템플릿이 인식됩니다. vCloud Air 또는 vCloud Director에서 템플릿을 삭제하면 연결된 템플릿이 더 이상 존재하지 않기 때문에 이후의 vRealize Automation 프로비저닝 및 데이터 수집이 실패합니다. 업데이트된 버전을 업로드해야 하는 경우를 예로 들자면, 템플릿을 삭제한 후 다시 생성하는 대신 vCloud Air vCloud Director 템플릿 교체 프로세스를 사용할 수 있습니다. 템플릿을 삭제한 후 다시 생성하는 대신 vCloud Air 또는 vCloud Director를 사용하여 템플릿을 교체하면 템플릿의 고유 ID가 그대로 유지되기 때문에 프로비저닝 및 데이터 수집을 계속해서 수행할 수 있습니다.

다음 개요에서는 vRealize Automation을 사용하여 끝점을 생성하고 예약 및 Blueprint를 정의하기 전에 수행해야 하는 단계를 보여 줍니다. 이러한 관리 작업에 대한 자세한 내용은 vCloud Air 및 vCloud Director 제품 설명서를 참조하십시오.

- 1 vCloud Air 또는 vCloud Director에서 복제용 템플릿을 생성한 후 조직 카탈로그에 추가합니다.
- 2 vCloud Air 또는 vCloud Director에서 템플릿을 사용하여 각 시스템의 게스트 운영 체제에 대해 암호, 도메인 및 스크립트 같은 사용자 지정 설정을 지정합니다.
이러한 설정 중 일부는 vRealize Automation을 사용하여 재정의할 수 있습니다.
사용자 지정은 리소스의 게스트 운영 체제에 따라 크게 달라질 수 있습니다.
- 3 vCloud Air 또는 vCloud Director에서 조직의 모든 사용자와 공유할 카탈로그를 구성합니다.
조직에 속한 모든 사용자와 그룹이 카탈로그에 액세스할 수 있도록 vCloud Air 또는 vCloud Director에서 적절한 조직에 대한 계정 관리자 액세스를 구성합니다. 이렇게 공유를 지정하지 않으면 vRealize Automation에서 끝점 또는 Blueprint 설계자에게 카탈로그 템플릿이 표시되지 않습니다.
- 4 Blueprint에 포함할 수 있도록 다음과 같은 정보를 수집합니다.
 - vCloud Air 또는 vCloud Director 템플릿의 이름
 - 템플릿에 지정된 총 스토리지 양

Linux Kickstart 프로비저닝을 위한 준비

Linux Kickstart 프로비저닝에는 새로 프로비저닝된 시스템에 대한 Linux 설치를 자동화하는 구성 파일이 사용됩니다. 프로비저닝을 준비하려면 부팅 가능한 ISO 이미지와 Kickstart 또는 autoYaST 구성 파일을 생성해야 합니다.

다음은 Linux Kickstart 프로비저닝을 준비하는 데 필요한 단계의 개괄적인 개요입니다.

- 1 네트워크에서 DHCP 서버를 사용할 수 있는지 확인합니다. vRealize Automation은 DHCP를 사용할 수 있는 경우에만 Linux Kickstart 프로비저닝을 사용하여 시스템을 프로비저닝할 수 있습니다.
- 2 구성 파일을 준비합니다. 구성 파일에는 vRealize Automation 서버 및 Linux 에이전트 설치 패키지의 위치를 지정해야 합니다. [Linux Kickstart 구성 샘플 파일 준비](#) 항목을 참조하십시오.
- 3 isolinux/isolinux.cfg 또는 loader/isolinux.cfg를 편집하여 구성 파일 및 적절한 Linux 배포 소스의 이름과 위치를 지정합니다.
- 4 부팅 ISO 이미지를 생성한 후 가상화 플랫폼의 필요한 위치에 저장합니다. 필수 위치에 대한 자세한 내용은 하이퍼바이저가 제공한 설명서를 참조하십시오.
- 5 (선택 사항) 사용자 지정 스크립트를 추가합니다.
 - a 설치 이후 사용자 지정 스크립트를 구성 파일에 지정하려면 [kickstart/autoYaST 구성 파일에 사용자 지정 스크립트 지정](#)을 참조하십시오.
 - b Blueprint에 포함된 Visual Basic 스크립트를 호출하려면 [프로비저닝 중 Visual Basic 스크립트 실행을 위한 검사 목록](#)을 참조하십시오.
- 6 Blueprint 설계자가 자신의 Blueprint에 포함할 수 있도록 다음과 같은 정보를 수집합니다.
 - a ISO 이미지의 이름과 위치
 - b vCenter Server 통합의 경우 vCenter Server가 시스템을 생성하는 데 사용할 vCenter Server 게스트 운영 체제 버전

참고 BootIsoProperties 속성 집합을 가진 속성 그룹을 생성하여 필수 ISO 정보를 수집할 수 있습니다. 이렇게 하면 이 정보를 Blueprint에 정확하고 보다 손쉽게 포함할 수 있습니다.

Linux Kickstart 구성 샘플 파일 준비

vRealize Automation은 필요에 맞게 수정하고 편집할 수 있는 샘플 구성 파일을 제공합니다. 이러한 파일을 사용할 수 있으려면 몇 가지 사항을 변경해야 합니다.

프로시저

- 1 vRealize Automation 장치 관리 콘솔 페이지로 이동합니다.
예: `https://va-hostname.domain.com`.

- 2 페이지의 vRealize Automation 구성 요소 설치 섹션에서 **게스트 및 소프트웨어 에이전트 페이지**를 클릭합니다.

예: `https://va-hostname.domain.com/software/index.html`.

게스트 및 소프트웨어 에이전트 설치 관리자 페이지가 열리고 사용 가능한 다운로드에 대한 링크가 표시됩니다.

- 3 페이지의 게스트 에이전트 설치 관리자 섹션에서 **Linux 게스트 에이전트 패키지**를 클릭하고 `LinuxGuestAgentPkgs.zip` 파일을 다운로드하여 저장합니다.
- 4 다운로드한 `LinuxGuestAgentPkgs.zip` 파일의 압축을 풀어서 `VraLinuxGuestAgent` 폴더를 생성합니다.
- 5 프로비저닝 중에 배포할 게스트 운영 체제에 해당하는 `VraLinuxGuestAgent` 하위 디렉토리로 이동합니다.

예: `rhel32`.

- 6 대상 시스템에 해당하는 샘플 하위 디렉토리에서 파일을 엽니다.

예: `samples/sample-https-rhel6-x86.cfg`.

- 7 모든 `host=dcac.example.net` 문자열 인스턴스를 Manager Service 또는 Manager Service의 로드 밸런서에 대한 IP 주소 또는 FQDN(정규화된 도메인 이름) 및 포트 번호로 바꿉니다.

플랫폼	필수 형식
vSphere ESXi	IP 주소(예: <code>--host=172.20.9.59</code>)
vSphere ESX	IP 주소(예: <code>--host=172.20.9.58</code>)
SUSE 10	IP 주소(예: <code>--host=172.20.9.57</code>)
그 외	FQDN(예: <code>--host=mycompany-host1.mycompany.local:443</code>)

- 8 `gugent.rpm` 또는 `gugent.tar.gz`의 각 인스턴스를 찾아 URL `rpm.example.net`을 게스트 에이전트 패키지의 위치로 바꿉니다.

예:

```
rpm -i nfs:172.20.9.59/suseagent/gugent.rpm
```

- 9 새로 프로비저닝한 시스템에서 액세스할 수 있는 위치에 파일을 저장합니다.

kickstart/autoYaST 구성 파일에 사용자 지정 스크립트 지정

구성 파일을 수정하면 새로 프로비저닝된 시스템에 사용자 지정 스크립트를 복사하거나 설치할 수 있습니다. Linux 에이전트는 워크플로의 지정된 지점에 스크립트를 실행합니다.

스크립트는 `./properties.xml` 파일(`/usr/share/gugent/site/workitem` 디렉토리) 중 아무 파일이나 참조할 수 있습니다.

필수 조건

- kickstart 또는 autoYaST 구성 파일을 준비합니다. [Linux Kickstart 구성 샘플 파일 준비](#) 항목을 참조하십시오.
- 스크립트는 시스템 프로비저닝 실패를 방지하기 위해 실패 시 0이 아닌 값을 반환해야 합니다.

프로시저

1 사용하고자 하는 스크립트를 생성하거나 식별합니다.

2 스크립트를 NN_scriptname으로 저장합니다.

여기서 NN은 두 자리 번호입니다. 스크립트를 낮은 번호부터 높은 번호 순서로 실행됩니다. 스크립트 두 개의 번호가 같으면 scriptname을 기준으로 알파벳 순서로 실행됩니다.

3 스크립트를 실행 가능한 상태로 만듭니다.

4 kickstart 또는 autoYaST 구성 파일의 사후 설치 섹션을 찾습니다.

kickstart에서는 이 섹션이 %post로 표시되고, autoYaST에서는 이 섹션이 post-scripts로 표시됩니다.

5 선택하는 /usr/share/gugent/site/workitem 디렉토리에 스크립트를 복사하거나 설치하도록 구성 파일의 사후 설치 섹션을 수정합니다.

사용자 지정 스크립트는 작업 항목 SetupOS(프로비저닝 생성) 및 CustomizeOS(프로비저닝 복제)와 함께 가상 kickstart/autoYaST에 대해 가장 일반적으로 실행되지만, 워크플로의 원하는 지점에서 스크립트를 실행할 수 있습니다.

예를 들어 다음과 같은 명령을 사용하면 새로 프로비저닝된 시스템의 /usr/share/gugent/site/SetupOS 디렉토리에 11_addusers.sh 스크립트를 복사하도록 구성 파일을 수정할 수 있습니다.

```
cp nfs:172.20.9.59/linuxscripts/11_addusers.sh /usr/share/gugent/site/SetupOS
```

Linux 에이전트는 작업 항목 디렉토리와 스크립트 파일 이름에 따라 지정된 순서대로 스크립트를 실행합니다.

SCCM 프로비저닝 준비

vRealize Automation은 새로 프로비저닝된 시스템을 ISO 이미지에서 부팅한 후, 제어 기능을 지정한 SCCM 작업 시퀀스에 전달합니다.

SCCM 프로비저닝은 Windows 운영 체제 배포에 대해 지원됩니다. Linux는 지원되지 않습니다. 소프트웨어 배포 및 업데이트는 지원되지 않습니다.

다음은 SCCM 프로비저닝을 준비하는 데 필요한 단계의 개괄적인 개요입니다.

1 네트워크 관리자에게 문의하여 다음과 같은 네트워크 요구 사항이 충족되는지 확인합니다.

- SCCM과 통신하려면 SCCM 서버의 NetBios 이름이 필요합니다. 하나 이상의 DEM(Distributed Execution Manager)이 SCCM 서버의 정규화된 이름을 해당하는 NetBios 이름에 대해 확인할 수 있어야 합니다.

- SCCM 서버와 vRealize Automation 서버가 같은 네트워크에 속해 있고, 서로 사용 가능한 상태여야 합니다.
- 2 vRealize Automation 게스트 에이전트가 포함된 소프트웨어 패키지를 생성합니다. [SCCM 프로비저닝을 위한 소프트웨어 패키지 생성](#) 항목을 참조하십시오.
- 3 SCCM에서 시스템을 프로비저닝하기 위한 원하는 작업 시퀀스를 생성합니다. 최종 단계에서는 생성한 소프트웨어 패키지(vRealize Automation 게스트 에이전트를 포함)를 설치해야 합니다. 작업 시퀀스 생성 및 소프트웨어 패키지 설치에 대한 자세한 내용은 SCCM 설명서를 참조하십시오.
- 4 작업 시퀀스를 위한 제로 터치 부팅 ISO 이미지를 생성합니다. 기본적으로 SCCM은 라이트 터치 부팅 ISO 이미지를 생성합니다. 제로 터치 ISO 이미지를 위해 SCCM을 구성하는 데 대한 자세한 내용은 SCCM 설명서를 참조하십시오.
- 5 가상화 플랫폼의 필요한 위치에 ISO 이미지를 복사합니다. 적절한 위치를 모르는 경우에는 하이퍼바이저가 제공한 설명서를 참조하십시오.
- 6 Blueprint 설계자가 Blueprint에 포함할 수 있도록 다음과 같은 정보를 수집합니다.
 - a 작업 시퀀스가 포함된 컬렉션의 이름
 - b 시퀀스가 포함된 컬렉션이 위치하고 있는 SCCM 서버의 정규화된 도메인 이름
 - c SCCM 서버의 사이트 코드
 - d SCCM 서버에 대한 관리자 수준의 자격 증명
 - e (선택 사항) SCVMM 통합의 경우 프로비저닝된 시스템에 연결할 ISO, 가상 하드 디스크 또는 하드웨어 프로파일

SCCM 프로비저닝을 위한 소프트웨어 패키지 생성

SCCM 작업 순서의 마지막 단계는 vRealize Automation 게스트 에이전트를 포함하는 소프트웨어 패키지를 설치하는 것입니다.

프로시저

- 1 vRealize Automation 장치 관리 콘솔 페이지로 이동합니다.
예: `https://va-hostname.domain.com`.
- 2 페이지의 vRealize Automation 구성 요소 설치 섹션에서 **게스트 및 소프트웨어 에이전트 페이지**를 클릭합니다.
예: `https://va-hostname.domain.com/software/index.html`.
게스트 및 소프트웨어 에이전트 설치 관리자 페이지가 열리고 사용 가능한 다운로드에 대한 링크가 표시됩니다.
- 3 페이지의 구성 요소 설치 섹션에서 Windows 게스트 에이전트 파일 (**32비트**) 또는 (**64비트**)를 클릭하고 GuestAgentInstaller.exe 또는 GuestAgentInstaller_x64.exe 파일을 다운로드하여 저장합니다.
- 4 SCCM에서 사용할 수 있는 위치에 Windows 게스트 에이전트를 추출합니다.
디렉토리 C:\WVRMGuestAgent가 생성됩니다. 이 디렉토리의 이름을 바꾸지 마십시오.

- 5 정의 파일 SCCMPackageDefinitionFile.sms에서 소프트웨어 패키지를 생성합니다.
- 6 분산 지점에서 소프트웨어 패키지를 사용할 수 있도록 설정합니다.
- 7 추출된 Windows 게스트 에이전트 파일의 콘텐츠를 소스 파일로 선택합니다.

WIM 프로비저닝 준비

WinPE 환경으로 부팅한 후 기존 Windows 참조 시스템의 WIM(Windows Imaging File Format) 이미지를 사용하여 운영 체제를 설치하는 방법으로 시스템을 프로비저닝합니다.

다음은 WIM 프로비저닝을 준비하는 데 필요한 단계의 개괄적인 개요입니다.

- 1 스테이징 영역을 확인하거나 생성합니다. 스테이징 영역은 다음에서 UNC 경로로 지정하거나 네트워크 드라이브로 매핑할 수 있는 네트워크 디렉토리여야 합니다.
 - 참조 시스템
 - WinPE 이미지가 구축된 시스템
 - 시스템을 프로비저닝하는 가상 호스트
- 2 네트워크에 DHCP 서버가 있는지 확인합니다. vRealize Automation은 DHCP를 사용할 수 있는 경우에만 WIM 이미지를 사용하여 시스템을 프로비저닝할 수 있습니다.
- 3 프로비저닝에 사용할 예정인 가상화 플랫폼에서 참조 시스템을 확인하거나 생성합니다. vRealize Automation 요구 사항은 [WIM 프로비저닝을 위한 참조 시스템 요구 사항](#) 항목을 참조하십시오. 참조 시스템을 생성하는 데 대한 자세한 내용은 하이퍼바이저에서 제공되는 설명서를 참조하십시오.
- 4 System Preparation Utility for Windows를 사용하여 배포를 위한 참조 시스템의 운영 체제를 준비합니다. [참조 시스템의 SysPrep 요구 사항](#) 항목을 참조하십시오.
- 5 참조 시스템의 WIM 이미지를 생성합니다. WIM 이미지 파일 이름에 공백이 포함되어 있으면 프로비저닝이 실패하므로 공백을 포함하지 마십시오.
- 6 vRealize Automation 게스트 에이전트가 포함된 WinPE 이미지를 생성합니다.
 - (선택 사항) 프로비저닝된 시스템을 사용자 지정하는 데 사용할 사용자 스크립트를 생성한 후 적절한 작업 항목 디렉토리에 배치합니다.
 - VirtIO를 네트워크 또는 스토리지 인터페이스에 사용하는 경우에는 필요한 드라이버가 WinPE 이미지 및 WIM 이미지에 포함되어 있는지 확인해야 합니다. [VirtIO 드라이버를 이용한 WIM 프로비저닝 준비](#) 항목을 참조하십시오.

WinPE 이미지를 생성할 때는 vRealize Automation 게스트 에이전트를 수동으로 삽입해야 합니다. [WinPE 이미지에 수동으로 게스트 에이전트 삽입](#) 항목을 참조하십시오.
- 7 가상화 플랫폼에서 필요로 하는 위치에 WinPE 이미지를 배치합니다. 위치를 모르는 경우에는 하이퍼바이저 설명서를 참조하십시오.
- 8 Blueprint에 포함할 다음의 정보를 수집합니다.
 - a WinPE ISO 이미지의 이름과 위치
 - b WIM 파일의 이름, WIM 파일의 UNC 경로 및 WIM 파일에서 원하는 이미지를 추출하는 데 사용되는 인덱스

- c 프로비저닝된 시스템의 네트워크 드라이브에 WIM 이미지 경로를 매핑하는 데 사용하는 사용자 이름과 암호
- d (선택 사항) 기본값인 K를 수락하지 않으려는 경우, 프로비저닝된 시스템에 WIM 이미지 경로가 매핑된 드라이브 문자
- e vCenter Server 통합의 경우 vCenter Server가 시스템을 생성하는 데 사용할 vCenter Server 게스트 운영 체제 버전
- f (선택 사항) SCVMM 통합의 경우 프로비저닝된 시스템에 연결할 ISO, 가상 하드 디스크 또는 하드웨어 프로파일

참고 속성 그룹을 생성하여 이러한 필수 정보를 모두 포함할 수 있습니다. 속성 그룹을 사용하면 모든 정보를 Blueprint에 올바르게 포함하기가 더 쉽습니다.

1 WIM 프로비저닝을 위한 참조 시스템 요구 사항

WIM 프로비저닝에는 참조 시스템에서 WIM 이미지를 생성하는 과정이 포함됩니다. vRealize Automation에서 WIM 이미지를 프로비저닝에 사용하려면 참조 시스템이 기본적인 요구 사항을 충족해야 합니다.

2 참조 시스템의 SysPrep 요구 사항

SysPrep 응답 파일에는 WIM 프로비저닝에 사용되는 몇 가지 필수 설정이 포함되어 있습니다.

3 VirtIO 드라이버를 이용한 WIM 프로비저닝 준비

VirtIO를 네트워크 또는 스토리지 인터페이스에 사용하는 경우에는 필요한 드라이버가 WinPE 이미지 및 WIM 이미지에 포함되어 있는지 확인해야 합니다. 일반적으로 VirtIO는 KVM (RHEV)을 사용하여 프로비저닝할 때 성능이 더 좋습니다.

4 WinPE 이미지에 수동으로 게스트 에이전트 삽입

WinPE 이미지에 수동으로 vRealize Automation 게스트 에이전트를 삽입해야 합니다.

WIM 프로비저닝을 위한 참조 시스템 요구 사항

WIM 프로비저닝에는 참조 시스템에서 WIM 이미지를 생성하는 과정이 포함됩니다. vRealize Automation에서 WIM 이미지를 프로비저닝에 사용하려면 참조 시스템이 기본적인 요구 사항을 충족해야 합니다.

다음은 참조 시스템을 준비하는 데 필요한 단계의 개괄적인 개요입니다.

- 1 참조 시스템의 운영 체제가 Windows Server 2008 R2, Windows Server 2012, Windows 7 또는 Windows 8이면 기본 설치 시 기본 파티션 이외에 시스템의 하드 디스크에 작은 파티션이 생성됩니다. 이와 같은 다중 파티션을 가진 참조 시스템에 생성된 WIM 이미지는 vRealize Automation에서 지원하지 않습니다. 이 파티션은 설치 프로세스 중에 삭제해야 합니다.
- 2 참조 시스템에 NET 4.5 및 Windows 7용 Windows AIK(자동 설치 키트)(WinPE 3.0 포함)를 설치합니다.
- 3 참조 시스템의 운영 체제가 Windows Server 2003 또는 Windows XP인 경우, 관리자 암호를 빈 상태로 재설정합니다. 즉, 암호를 사용하지 않도록 설정합니다.

- 4 (선택 사항) XenDesktop 통합을 사용하려면 Citrix Virtual Desktop Agent를 설치하고 구성합니다.
- 5 (선택 사항) vRealize Automation이 관리하는 Windows 시스템에서 특정 데이터(예: 시스템 소유자의 Active Directory 상태)를 수집하려면 WMI(Windows Management Instrumentation) 에이전트가 필요합니다. Windows 시스템을 성공적으로 관리하려면 WMI 에이전트를 설치하고(일반적으로 Manager Service 호스트에 설치), 이 에이전트가 Windows 시스템으로부터 데이터를 수집할 수 있도록 설정해야 합니다. vRealize Automation 7.3 설치 항목을 참조하십시오.

참조 시스템의 SysPrep 요구 사항

SysPrep 응답 파일에는 WIM 프로비저닝에 사용되는 몇 가지 필수 설정이 포함되어 있습니다.

표 1-15. Windows Server 또는 Windows XP 참조 시스템의 필수 SysPrep 설정

GuiUnattended 설정	값
AutoLogon	Yes
AutoLogonCount	1
AutoLogonUsername	username (username 및 password는 새로 프로비저닝된 시스템이 게스트 운영 체제로 부팅될 때 자동 로그인에 사용되는 자격 증명입니다. 일반적으로 관리자가 사용됩니다.)
AutoLogonPassword	AutoLogonUsername에 대응하는 password.

표 1-16. Windows Server 2003 또는 Windows XP를 사용하지 않는 참조 시스템의 필수 SysPrep 설정:

AutoLogon 설정	값
Enabled	Yes
LogonCount	1
Username	username (username 및 password는 새로 프로비저닝된 시스템이 게스트 운영 체제로 부팅될 때 자동 로그인에 사용되는 자격 증명입니다. 일반적으로 관리자가 사용됩니다.)
Password	password (username 및 password는 새로 프로비저닝된 시스템이 게스트 운영 체제로 부팅될 때 자동 로그인에 사용되는 자격 증명입니다. 일반적으로 관리자가 사용됩니다.)

참고 Windows Server 2003/Windows XP보다 최신 버전인 Windows 플랫폼을 사용하는 참조 시스템의 경우 사용자 지정 속성 Sysprep.GuiUnattended.AdminPassword를 사용하여 자동 로그인 암호를 설정해야 합니다. 이 작업을 수행하는 편리한 방법은 이 사용자 지정 속성을 포함하는 속성 그룹을 생성하여 테넌트 관리자와 비즈니스 그룹 관리자가 해당 Blueprint에 이 정보를 올바르게 포함할 수 있도록 하는 것입니다.

VirtIO 드라이버를 이용한 WIM 프로비저닝 준비

VirtIO를 네트워크 또는 스토리지 인터페이스에 사용하는 경우에는 필요한 드라이버가 WinPE 이미지 및 WIM 이미지에 포함되어 있는지 확인해야 합니다. 일반적으로 VirtIO는 KVM (RHEV)을 사용하여 프로비저닝할 때 성능이 더 좋습니다.

VirtIO용 Windows 드라이버는 Red Hat Enterprise Virtualization의 일부로 포함되며 Red Hat Enterprise Virtualization Manager 파일 시스템의 `/usr/share/virtio-win` 디렉토리에 있습니다. 이러한 드라이버는 Red Hat Enterprise Virtualization Guest Tools(`/usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso`)에도 포함되어 있습니다.

다음은 VirtIO 드라이버를 사용하여 WIM 기반 프로비저닝을 사용하도록 설정하는 개괄적인 프로세스입니다.

- 1 VirtIO 드라이버가 설치된 Windows 참조 시스템에서 WIM 이미지를 생성하거나, 드라이버를 기존 WIM 이미지에 삽입합니다.
- 2 VirtIO 드라이버 파일을 복사하고 드라이버를 WinPE 이미지에 삽입합니다.
- 3 `rhev-iso-uploader` 명령을 사용하여 WinPE 이미지 ISO를 Red Hat Enterprise Virtualization ISO 스토리지 도메인에 업로드합니다. RHEV에서 ISO 이미지를 관리하는 데 대한 자세한 내용은 Red Hat 설명서를 참조하십시오.
- 4 WIM 프로비저닝용 KVM (RHEV) Blueprint를 생성하고 WinPE ISO 옵션을 선택합니다. 사용자 지정 속성 `VirtualMachine.Admin.DiskInterfaceType`을 **VirtIO** 값과 함께 포함해야 합니다. 패브릭 관리자가 이 정보를 속성 그룹에 포함하여 Blueprint에 포함할 수 있습니다.

사용자 지정 속성 `Image.ISO.Location` 및 `Image.ISO.Name`은 KVM (RHEV) Blueprint에 사용되지 않습니다.

WinPE 이미지에 수동으로 게스트 에이전트 삽입

WinPE 이미지에 수동으로 vRealize Automation 게스트 에이전트를 삽입해야 합니다.

필수 조건

- .NET 4.5 및 Windows 7용 Windows AIK(자동 설치 키트)(WinPE 3.0 포함)가 설치되어 있고, 준비한 스테이징 영역에 액세스할 수 있는 Windows 시스템을 선택합니다.
- WinPE를 생성합니다.

프로시저

1 WinPE에 게스트 에이전트 설치

게스트 에이전트 파일을 수동으로 WinPE 이미지로 복사해야 합니다.

2 `doagent.bat` 파일 구성

`doagent.bat` 파일을 수동으로 구성해야 합니다.

3 `doagentc.bat` 파일 구성

`doagentc.bat` 파일을 수동으로 구성해야 합니다.

4 게스트 에이전트 속성 파일 구성

게스트 에이전트 속성 파일을 수동으로 구성해야 합니다.

프로시저

- 1 WinPE에 게스트 에이전트 설치.
- 2 doagent.bat 파일 구성.
- 3 doagentc.bat 파일 구성.
- 4 게스트 에이전트 속성 파일 구성.

WinPE에 게스트 에이전트 설치

게스트 에이전트 파일을 수동으로 WinPE 이미지로 복사해야 합니다.

필수 조건

- .NET 4.5 및 Windows 7용 Windows AIK(자동 설치 키트)(WinPE 3.0 포함)가 설치되어 있고, 준비한 스테이징 영역에 액세스할 수 있는 Windows 시스템을 선택합니다.
- WinPE를 생성합니다.

프로시저

- ◆ https://vRealize_VA_Hostname_fqdn/software/index.html에서 vRealize Automation 게스트 에이전트를 다운로드하고 설치합니다.
 - a GagentZip_version을 참조 시스템의 C 드라이브에 다운로드합니다.
운영 체제에 따라 GuestAgentInstaller.exe(32비트) 또는 GuestAgentInstaller_x64.exe(64비트)를 선택합니다.
 - b 파일을 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택합니다.
 - c **일반**을 클릭합니다.
 - d **차단 해제**를 클릭합니다.
 - e 파일을 C:\W에 추출합니다.

디렉토리 C:\WVRMGuestAgent가 생성됩니다. 이 디렉토리의 이름을 바꾸지 마십시오.

후속 작업

[doagent.bat 파일 구성](#).

doagent.bat 파일 구성

doagent.bat 파일을 수동으로 구성해야 합니다.

필수 조건

[WinPE에 게스트 에이전트 설치](#).

프로시저

- 1 WinPE 이미지 내의 VRMGuestAgent 디렉토리로 이동합니다.
예: C:\Program Files (x86)\VMware\Plugins\WVRM Agent\VRMGuestAgent.
- 2 doagent-template.bat 파일의 복사본을 생성하고 이름을 doagent.bat로 지정합니다.
- 3 doagent.bat를 텍스트 편집기에서 엽니다.
- 4 #Dcac Hostname# 문자열의 모든 인스턴스를 IaaS Manager Service 호스트의 정규화된 도메인 이름 및 포트 번호로 바꿉니다.

옵션	설명
로드 밸런서를 사용하고 있는 경우	IaaS Manager Service에 대한 로드 밸런서의 정규화된 도메인 이름 및 포트를 입력합니다. 예를 들면 다음과 같습니다. manager_service_LB.mycompany.com:443
로드 밸런서를 사용하지 않는 경우	IaaS Manager Service가 설치된 시스템의 정규화된 도메인 이름 및 포트를 입력합니다. 예를 들면 다음과 같습니다. manager_service.mycompany.com:443

- 5 #Protocol# 문자열의 모든 인스턴스를 /ssl 문자열로 바꿉니다.
- 6 #Comment# 문자열의 모든 인스턴스를 REM 으로 바꿉니다(REM 뒤에는 후행 공백이 있어야 함).
- 7 (선택 사항) 자체 서명된 인증서를 사용하는 경우 openssl 명령에 대한 주석을 제거합니다.

```
echo QUIT | c:\VRMGuestAgent\bin\openssl s_client -connect
```

- 8 파일을 저장한 후 닫습니다.
- 9 doagent.bat를 사용자 지정 스크립트로 포함하도록 WinPE에 대한 Startnet.cmd 스크립트를 편집합니다.

후속 작업

[doagentc.bat 파일 구성.](#)

doagentc.bat 파일 구성

doagentc.bat 파일을 수동으로 구성해야 합니다.

필수 조건

[doagent.bat 파일 구성.](#)

프로시저

- 1 WinPE 이미지 내의 VRMGuestAgent 디렉토리로 이동합니다.
예: C:\Program Files (x86)\VMware\Plugins\WVRM Agent\VRMGuestAgent.
- 2 doagentsvc-template.bat 파일의 복사본을 생성하고 이름을 doagentc.bat로 지정합니다.

- 3 doagentc.bat를 텍스트 편집기에서 엽니다.
- 4 #Comment# 문자열의 모든 인스턴스를 제거합니다.
- 5 #Dcac Hostname# 문자열의 모든 인스턴스를 Manager Service 호스트의 정규화된 도메인 이름 및 포트 번호로 바꿉니다.

Manager Service에 대한 기본 포트는 443입니다.

옵션	설명
로드 밸런서를 사용하고 있는 경우	Manager Service에 대한 로드 밸런서의 정규화된 도메인 이름 및 포트를 입력합니다. 예를 들면 다음과 같습니다. load_balancer_manager_service.mycompany.com:443
로드 밸런서를 사용하지 않는 경우	Manager Service의 정규화된 도메인 이름 및 포트를 입력합니다. 예를 들면 다음과 같습니다. manager_service.mycompany.com:443

- 6 #errorlevel# 문자열의 모든 인스턴스를 1 문자로 바꿉니다.
- 7 #Protocol# 문자열의 모든 인스턴스를 /ssl 문자열로 바꿉니다.
- 8 파일을 저장한 후 닫습니다.

후속 작업

게스트 에이전트 속성 파일 구성.

게스트 에이전트 속성 파일 구성

게스트 에이전트 속성 파일을 수동으로 구성해야 합니다.

필수 조건

doagentc.bat 파일 구성.

프로시저

- 1 WinPE 이미지 내의 VRMGuestAgent 디렉토리로 이동합니다.
예: C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent.
- 2 gugent.properties 파일의 복사본을 생성하고 이름을 gugent.properties.template으로 지정합니다.
- 3 gugent.properties.template 파일의 복사본을 생성하고 이름을 gugentc.properties로 지정합니다.
- 4 gugent.properties를 텍스트 편집기에서 엽니다.
- 5 GuestAgent.log 문자열의 모든 인스턴스를 X:/VRMGuestAgent/GuestAgent.log 문자열로 바꿉니다.
- 6 파일을 저장한 후 닫습니다.
- 7 gugentc.properties를 텍스트 편집기에서 엽니다.
- 8 GuestAgent.log 문자열의 모든 인스턴스를 C:/VRMGuestAgent/GuestAgent.log 문자열로 바꿉니다.

9 파일을 저장한 후 닫습니다.

가상 시스템 이미지 프로비저닝 준비

OpenStack을 사용하여 인스턴스를 프로비저닝하기 전에 OpenStack 제공자에서 가상 시스템 이미지와 플레이버를 구성해야 합니다.

가상 시스템 이미지

OpenStack 리소스에 대한 Blueprint를 생성할 때 사용 가능한 이미지 목록에서 가상 시스템 이미지를 선택할 수 있습니다.

가상 시스템 이미지는 운영 체제를 포함한 소프트웨어 구성이 포함된 템플릿입니다. 가상 시스템 이미지는 OpenStack 제공자에 의해 관리되며 데이터 수집 도중 가져옵니다.

Blueprint에서 사용되는 이미지가 나중에 OpenStack 제공자에서 삭제되면 Blueprint에서도 제거됩니다. 모든 이미지가 Blueprint에서 제거된 경우 Blueprint는 사용되지 않도록 설정되며 최소 하나의 이미지를 추가하기 전까지는 시스템 요청에 사용할 수 없습니다.

OpenStack 플레이버

OpenStack Blueprint를 생성할 때 플레이버를 하나 이상 선택할 수 있습니다.

OpenStack 플레이버는 OpenStack에 프로비저닝된 인스턴스를 위한 시스템 리소스 규격을 정의하는 가상 하드웨어 템플릿입니다. 플레이버는 OpenStack 제공자가 관리하며 데이터 수집 시 가져옵니다.

vRealize Automation에서는 몇 가지 OpenStack 플레이버를 지원합니다. OpenStack 플레이버 지원에 대한 최신 정보는 vRealize Automation 지원 매트릭스

(<https://www.vmware.com/support/pubs/vcac-pubs.html>) 항목을 참조하십시오.

Amazon 시스템 이미지 프로비저닝 준비

vRealize Automation에서의 프로비저닝을 위해 Amazon 시스템 이미지와 인스턴스 유형을 준비합니다.

Amazon 시스템 이미지 이해

Amazon 시스템 Blueprint를 생성할 때 사용 가능한 이미지 목록에서 Amazon 시스템 이미지를 선택할 수 있습니다.

Amazon 시스템 이미지는 운영 체제를 포함한 소프트웨어 구성이 포함되어 있는 템플릿입니다. 해당 이미지는 Amazon Web Services 계정을 통해 관리됩니다. vRealize Automation은 프로비저닝에 사용할 수 있는 인스턴스 유형을 관리합니다.

Amazon 시스템 이미지와 인스턴스 유형은 Amazon 영역에서 사용 가능해야 합니다. 모든 영역에서 모든 인스턴스 유형을 사용할 수 있는 것은 아닙니다.

Amazon Web Services, 사용자 커뮤니티 또는 AWS Marketplace 사이트에서 제공하는 Amazon 시스템 이미지를 선택할 수 있습니다. 또한 고유한 Amazon 시스템 이미지를 생성하고 필요한 경우 공유할 수도 있습니다. Amazon 시스템 이미지 하나를 사용하여 하나의 인스턴스 또는 여러 개의 인스턴스를 시작할 수 있습니다.

다음은 클라우드 시스템을 프로비저닝하는 데 사용하는 Amazon Web Services 계정의 Amazon 시스템 이미지에 적용되는 고려 사항입니다.

- Blueprint 각각에서 Amazon 시스템 이미지를 지정해야 합니다.

전용 Amazon 시스템 이미지는 특정 계정과 해당 계정의 모든 영역에서 사용할 수 있습니다. 공용 Amazon 시스템 이미지는 모든 계정에서 사용할 수 있지만 각 계정의 특정 영역에서만 사용할 수 있습니다.

- Blueprint 생성 시 데이터가 수집된 영역 중에서 지정된 Amazon 시스템 이미지가 선택됩니다. Amazon Web Services 계정이 여러 개 있는 경우 비즈니스 그룹 관리자는 모든 전용 Amazon 시스템 이미지에 대한 권한을 가지고 있어야 합니다. Amazon 시스템 이미지 영역과 지정된 사용자 위치는 해당하는 영역 및 위치가 일치하는 예약에 대해서만 프로비저닝 요청을 할 수 있도록 제한합니다.
- Amazon 시스템 이미지를 Amazon Web Services 계정에 분산시키는 데 예약 및 정책을 사용합니다. Blueprint에서 특정 예약 집합에 프로비저닝하는 것을 제한하려면 정책을 사용합니다.
- vRealize Automation에서는 클라우드 시스템에 사용자 계정을 생성할 수 없습니다. 시스템 소유자가 클라우드 시스템에 처음으로 연결할 때 소유자 직접 관리자로 로그인하여 자신의 vRealize Automation 사용자 자격 증명을 추가하거나, 관리자가 이 작업을 대신 수행해야 합니다. 이렇게 한 후에는 소유자가 자신의 vRealize Automation 사용자 자격 증명을 사용하여 로그인할 수 있습니다.

부팅할 때마다 Amazon 시스템 이미지가 관리자 암호를 생성할 경우, [시스템 레코드 편집] 페이지에 암호가 표시됩니다. 암호가 표시되지 않을 경우에는 Amazon Web Services 계정에서 암호를 찾을 수 있습니다. 부팅할 때마다 관리자 암호를 생성하도록 모든 Amazon 시스템 이미지를 구성할 수 있습니다. 뿐만 아니라 다른 사용자를 위해 시스템을 프로비저닝하는 사용자를 지원하기 위해 관리자 암호 정보를 제공할 수도 있습니다.

- Amazon Web Services 계정에 프로비저닝된 클라우드 시스템에서 원격 Microsoft WMI(Windows Management Instrumentation) 요청을 허용하려면 Microsoft WinRM(Windows Remote Management) 에이전트가 vRealize Automation에서 관리하는 Windows 시스템에서 데이터를 수집할 수 있도록 합니다. vRealize Automation 7.3 설치의 내용을 참조하십시오.
- 전용 Amazon 시스템 이미지는 테넌트 간에 표시될 수 있습니다.

자세한 내용은 Amazon 설명서에서 AMI(Amazon 시스템 이미지)를 참조하십시오.

Amazon 인스턴스 유형 이해

IaaS 설계자는 Amazon EC2 Blueprint 생성 시 하나 이상의 Amazon 인스턴스 유형을 선택합니다. IaaS 관리자는 인스턴스 유형을 추가 또는 제거하여 설계자가 사용할 수 있는 선택 항목을 제어할 수 있습니다.

Amazon EC2 인스턴스는 Amazon Web Services에서 애플리케이션을 실행할 수 있는 가상 서버입니다. 인스턴스는 Amazon 시스템 이미지에서 적절한 인스턴스 유형을 선택하여 생성됩니다.

Amazon Web Services 계정에 시스템을 프로비저닝하기 위해 인스턴스 유형이 지정된 Amazon 시스템 이미지에 적용됩니다. 사용 가능한 인스턴스 유형은 설계자가 Amazon EC2 Blueprint를 생성할 때 나열됩니다. 설계자는 하나 이상의 인스턴스 유형을 선택하고 선택된 인스턴스 유형은 시스템에 대한 프로비저닝을 요청할 때 사용자가 사용할 수 있는 선택 항목이 됩니다. 인스턴스 유형은 지정된 영역에서 지원되는 것이어야 합니다.

관련 정보는 Amazon 설명서에서 인스턴스 유형 선택 및 Amazon EC2 인스턴스 세부 정보 항목을 참조하십시오.

Amazon 인스턴스 유형 추가

Amazon Blueprint와 함께 사용하기 위해 일부 인스턴스 유형이 vRealize Automation과 함께 제공됩니다. 관리자가 인스턴스 유형을 추가 및 제거할 수 있습니다.

Blueprint 설계자가 Amazon Blueprint를 생성 또는 편집할 때 IaaS 관리자에 의해 관리되는 시스템 인스턴스 유형을 사용할 수 있습니다. Amazon 시스템 이미지 및 인스턴스 유형은 Amazon Web Services 제품을 통해 사용할 수 있습니다.

필수 조건

IaaS 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **인프라 > 관리 > 인스턴스 유형**을 클릭합니다.
- 2 **새로 만들기**를 클릭합니다.
- 3 다음 매개 변수를 지정하여 새 인스턴스 유형을 추가합니다.

사용 가능한 Amazon 인스턴스 유형 및 해당 매개 변수에 대해 지정할 수 있는 설정 값에 대한 자세한 내용은 EC2 인스턴스 유형 - AWS(Amazon Web Services) (aws.amazon.com/ec2) 및 인스턴스 유형(docs.aws.amazon.com)의 Amazon Web Services 설명서에서 확인할 수 있습니다.

- 이름
- API 이름
- 유형 이름
- IO 성능 이름
- CPU
- 메모리(GB)
- 스토리지(GB)
- 계산 단위

- 4 **저장** 아이콘()을 클릭합니다.

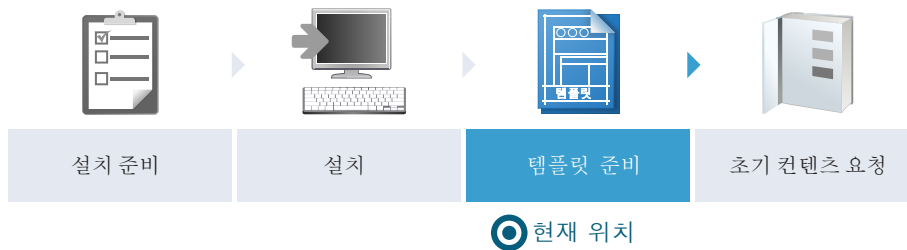
IaaS 설계자가 Amazon Web Services Blueprint를 생성할 때 사용자 지정 인스턴스 유형을 사용할 수 있습니다.

후속 작업

끝점에서 패브릭 그룹으로 계산 리소스를 추가합니다. [패브릭 그룹 생성](#) 항목을 참조하십시오.

시나리오: Rainpole에서의 시스템 프로비저닝을 위한 vSphere 리소스 준비

vRealize Automation 템플릿을 생성하는 vSphere 관리자로서 vSphere Web Client를 사용하여 vRealize Automation에서 CentOS 시스템 복제를 준비합니다.



기존 CentOS 참조 시스템을 vSphere 템플릿으로 변환하여 사용자와 사용자의 Rainpole 설계자가 vRealize Automation에서 CentOS 시스템을 복제하기 위한 Blueprint를 생성할 수 있습니다. 설정이 동일한 여러 가상 시스템을 배포함으로써 발생할 수 있는 충돌을 방지하기 위해 사용자와 사용자의 설계자가 Linux 템플릿용 복제 Blueprint를 생성하는 데 사용할 수 있는 일반 사용자 지정 규격을 생성합니다.

프로시저

1 시나리오: CentOS 참조 시스템을 Rainpole용 템플릿으로 변환

vSphere Client를 사용하여 vRealize Automation IaaS 설계자가 복제 Blueprint의 기초로 참조하도록 기존 CentOS 참조 시스템을 vSphere 템플릿으로 변환합니다.

2 시나리오: Rainpole에서 Linux 시스템 복제를 위해 사용자 지정 규격 생성

vSphere Client를 사용하여, Linux 시스템용 복제 Blueprint를 생성할 때 vRealize Automation IaaS 설계자가 사용할 표준 사용자 지정 규격을 생성합니다.

시나리오: CentOS 참조 시스템을 Rainpole용 템플릿으로 변환

vSphere Client를 사용하여 vRealize Automation IaaS 설계자가 복제 Blueprint의 기초로 참조하도록 기존 CentOS 참조 시스템을 vSphere 템플릿으로 변환합니다.

프로시저

- 1 참조 시스템에 루트 사용자로 로그인하고 변환을 위해 시스템을 준비합니다.

- a udev 지속성 규칙을 제거합니다.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b 이 템플릿에서 복제된 시스템이 고유한 식별자를 사용하도록 설정합니다.

```
/bin/sed -i '/^W(HWADDRW|UUIDW)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c 시스템 전원을 끕니다.

```
shutdown -h now
```

- 2 vSphere Web Client에 관리자로 로그인합니다.

- 3 **VM 옵션** 탭을 클릭합니다.

- 4 참조 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

- 5 **VM 이름** 텍스트 상자에 **Rainpole_centos_63_x86**을 입력합니다.

- 6 참조 시스템에 CentOS 게스트 운영 체제가 있더라도 **게스트 OS 버전** 드롭다운 메뉴에서 **Red Hat Enterprise Linux 6(64비트)**을 선택합니다.

CentOS를 선택하면 템플릿 및 사용자 지정 규격이 예상과 다르게 작동할 수 있습니다.

- 7 vSphere Web Client에서 **Rainpole_centos_63_x86** 참조 시스템을 마우스 오른쪽 버튼으로 클릭하고 **템플릿 > 템플릿으로 변환**을 선택합니다.

vCenter Server가 Rainpole_centos_63_x86 참조 시스템을 템플릿으로 표시하고 작업을 [최근 작업] 창에 표시합니다.

후속 작업

설정이 동일한 여러 가상 시스템을 배포함으로써 발생할 수 있는 충돌을 방지하기 위해 사용자와 사용자의 Rainpole 설계자가 Linux 템플릿용 복제 Blueprint를 생성하는 데 사용할 수 있는 일반 사용자 지정 규격을 생성합니다.

시나리오: Rainpole에서 Linux 시스템 복제를 위해 사용자 지정 규격 생성

vSphere Client를 사용하여, Linux 시스템용 복제 Blueprint를 생성할 때 vRealize Automation IaaS 설계자가 사용할 표준 사용자 지정 규격을 생성합니다.

프로시저

- 1 홈 페이지에서 **사용자 지정 규격 관리자**를 클릭하여 마법사를 엽니다.

- 2 **새로 만들기** 아이콘을 클릭합니다.

- 3 속성을 지정합니다.
 - a 대상 VM 운영 체제 드롭다운 메뉴에서 **Linux**를 선택합니다.
 - b 사용자 지정 규격 이름 텍스트 상자에 **Linux**를 입력합니다.
 - c 설명 텍스트 상자에 **Rainpole Linux cloning with vRealize Automation**을 입력합니다.
 - d 다음을 클릭합니다.
- 4 컴퓨터 이름을 설정합니다.
 - a 가상 시스템 이름 사용을 선택합니다.
 - b 도메인 이름 텍스트 상자에 복제된 시스템이 프로비저닝될 도메인을 입력합니다.
예를 들어 **rainpole.local**을 입력합니다.
 - c 다음을 클릭합니다.
- 5 영역 설정을 구성합니다.
- 6 다음을 클릭합니다.
- 7 모든 네트워크 인터페이스에서 DHCP 사용 등 게스트 운영 체제에 대해 표준 네트워크 설정 사용을 선택합니다.
- 8 표시되는 메시지에 따라 필요한 나머지 정보를 입력합니다.
- 9 완료할 준비가 됨 페이지에서 선택 항목을 검토하고 **마침**을 클릭합니다.

현재 Linux 시스템 복제를 위해 Blueprint를 생성하는 데 사용할 수 있는 일반 사용자 지정 규격이 있습니다.

후속 작업

설치 중에 생성한 구성 관리자로 vRealize Automation 콘솔에 로그인하고 개념 증명을 신속하게 설정하는 카탈로그 항목을 요청합니다.

Software 프로비저닝 준비

vSphere, vCloud Director, vCloud Air 및 Amazon AWS 시스템에 대한 vRealize Automation 프로비저닝 프로세스의 일부로 Software를 사용하여 애플리케이션 및 미들웨어를 배포합니다.

Blueprint에서 Software를 지원하고 참조 시스템을 템플릿, 스냅샷 또는 Amazon 시스템 이미지로 변환하기 전에 참조 시스템에 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치한 경우 시스템에 Software를 배포할 수 있습니다.

프로비저닝을 준비할 때 포트 지정에 대한 관련 정보는 [VMware vRealize Automation 정보](#)의 보안 구성 가이드 및 참조 아키텍처 항목을 참조하십시오.

표 1-17. Software 를 지원하는 프로비저닝 방법

시스템 유형	프로비저닝 방법	필요한 준비
vSphere	복제	복제 Blueprint는 vCenter Server 가상 시스템 템플릿을 기반으로 완전하고 독립적인 가상 시스템을 프로비저닝합니다. 복제용 템플릿에서 Software 구성 요소를 지원하도록 하려면 복제용 템플릿을 준비할 때 참조 시스템에 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치합니다. 복제를 통한 프로비저닝 준비를 위한 검사 목록 항목을 참조하십시오.
vSphere	연결된 복제	연결된 복제 Blueprint는 스냅샷을 기반으로 vSphere 시스템의 공간 효율적인 복사본을 프로비저닝하며, 델타 디스크 체인을 사용하여 상위 시스템과의 차이점을 추적합니다. 연결된 복제 Blueprint에서 Software 구성 요소를 지원하도록 하려면 스냅샷을 생성하기 전에 시스템에 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치합니다. 스냅샷 시스템이 Software를 지원하는 템플릿에서 복제된 경우 필요한 에이전트는 이미 설치되어 있습니다.
vCloud Director	복제	복제 Blueprint는 vCenter Server 가상 시스템 템플릿을 기반으로 완전하고 독립적인 가상 시스템을 프로비저닝합니다. 복제용 템플릿에서 Software 구성 요소를 지원하도록 하려면 복제용 템플릿을 준비할 때 참조 시스템에 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치합니다. 복제를 통한 프로비저닝 준비를 위한 검사 목록 항목을 참조하십시오.
vCloud Air	복제	복제 Blueprint는 vCenter Server 가상 시스템 템플릿을 기반으로 완전하고 독립적인 가상 시스템을 프로비저닝합니다. 복제용 템플릿에서 Software 구성 요소를 지원하도록 하려면 복제용 템플릿을 준비할 때 참조 시스템에 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치합니다. 복제를 통한 프로비저닝 준비를 위한 검사 목록 항목을 참조하십시오.
Amazon AWS	Amazon 시스템 이미지	Amazon 시스템 이미지는 운영 체제를 포함한 소프트웨어 구성이 포함되어 있는 템플릿입니다. Software를 지원하는 Amazon 시스템 이미지를 생성하려는 경우 루트 디바이스에 대해 EBS 볼륨을 사용하는 실행 중인 Amazon AWS 인스턴스에 연결합니다. 참조 시스템에 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치한 다음 인스턴스에서 Amazon 시스템 이미지를 생성합니다. Amazon EBS 지원형 AMI 생성에 대한 자세한 내용은 Amazon AWS 설명서를 참조하십시오. 게스트 에이전트와 Software 부트스트랩 에이전트가 프로비저닝된 시스템에서 작동하려면 네트워크 및 VPC 간 연결을 구성해야 합니다.

Software 를 사용하여 시스템 프로비저닝 준비

Software 구성 요소를 지원하려면 복제를 위한 템플릿으로 변환하기 전에 참조 시스템에 게스트 에이전트와 Software 부트스트랩 에이전트를 설치하고 Amazon 시스템 이미지를 생성하거나 스냅샷을 생성해야 합니다.

Software 지원을 위해 Windows 참조 시스템 준비

단일 스크립트를 사용하여 Windows 참조 시스템에서 Java Runtime Environment, 게스트 에이전트 및 Software 부트스트랩 에이전트를 설치합니다. 참조 시스템에서 복제를 위한 템플릿, 스냅샷 또는 Software 구성 요소를 지원하는 Amazon 시스템 이미지를 생성할 수 있습니다.

Software에서는 Windows CMD 또는 PowerShell 2.0을 사용한 스크립팅을 지원합니다.

중요 부팅 프로세스가 중단되어서는 안 됩니다. 로그인 메시지가 나타나기 전에 가상 시스템 부팅 프로세스가 일시 중지되지 않도록 가상 시스템을 구성합니다. 예를 들면 가상 시스템이 시작되는 동안 사용자 상호 작용을 요구하는 프로세스나 스크립트 메시지가 없는지 확인합니다.

필수 조건

- Windows 참조 시스템을 식별 또는 생성합니다.
- 참조 시스템과 IaaS Manager Service 호스트 간 보안 신뢰를 설정합니다. [서버를 신뢰하도록 게스트 에이전트 구성](#) 항목을 참조하십시오.
- 참조 시스템에서, Darwin 사용자에게 Log on as a service 액세스 권한이 있는지 확인합니다.
- 문제 해결 또는 다른 이유로 시스템에 원격으로 액세스하려는 경우 RDS(원격 데스크톱 서비스)를 설치합니다.
- 네트워크 구성 파일에서 네트워크 구성 아티팩트를 제거합니다.

프로시저

- 1 관리자로 Windows 참조 서버에 로그인합니다.
- 2 브라우저를 열고 vRealize Automation 장치의 소프트웨어 다운로드 페이지로 이동합니다.
`https://vrealize-automation-appliance-FQDN/software`
- 3 템플릿 ZIP을 Windows Server에 저장합니다.
`prepare_vra_template_windows.zip`
- 4 ZIP 콘텐츠를 폴더에 추출하고 다음 명령 중 하나를 사용하여 `prepare_vra_template.ps1` 스크립트를 실행합니다.
 - `Powershell -NoProfile -ExecutionPolicy Bypass -Command .\prepare_vra_template.ps1`
 - `.\prepare_vra_template.bat`
- 5 표시되는 메시지를 따릅니다.
- 6 완료되면 Windows 가상 시스템을 종료합니다.

스크립트가 이전의 게스트 또는 Software 부트스트랩 에이전트를 제거하고 지원되는 Java Runtime Environment 버전, 게스트 에이전트 및 Software 부트스트랩 에이전트를 설치합니다.

후속 작업

참조 시스템을 복제를 위한 템플릿, 스냅샷 또는 Amazon 시스템 이미지로 변환합니다. 각각 Software 구성 요소를 지원하며, 인프라 설계자는 Blueprint를 생성할 때 이를 사용할 수 있습니다.

Software 지원을 위해 Linux 참조 시스템 준비

단일 스크립트를 사용하여 Linux 참조 시스템에서 Java Runtime Environment, 게스트 에이전트 및 Software 부트스트랩 에이전트를 설치합니다. 참조 시스템에서 복제를 위한 템플릿, 스냅샷 또는 Software 구성 요소를 지원하는 Amazon 시스템 이미지를 생성할 수 있습니다.

Software에서는 Bash를 사용한 스크립팅을 지원합니다.

중요 부팅 프로세스가 중단되어서는 안 됩니다. 로그인 메시지가 나타나기 전에 가상 시스템 부팅 프로세스가 일시 중지되지 않도록 가상 시스템을 구성합니다. 예를 들면 가상 시스템이 시작되는 동안 사용자 상호 작용을 요구하는 프로세스나 스크립트 메시지가 없는지 확인합니다.

필수 조건

- Linux 참조 시스템을 식별 또는 생성합니다.
- 사용 중인 Linux 시스템에 따라 다음 명령을 사용할 수 있는지 확인합니다.
 - yum 또는 apt-get
 - wget 또는 curl
 - python
 - dmidecode(클라우드 제공자의 필요에 따름)
 - Linux 배포에 따른 sed, awk, perl, chkconfig, unzip 및 grep와 같은 일반 요구 사항

편집기로 다운로드한 prepare_vra_template.sh 스크립트를 검사하여 스크립트에서 사용하는 명령을 호출할 수도 있습니다.
- 문제 해결 또는 다른 이유로 시스템에 원격으로 액세스하려는 경우 OpenSSH를 설치합니다.
- 네트워크 구성 파일에서 네트워크 구성 아티팩트를 제거합니다.

프로시저

- 1 참조 시스템에 root로 로그인합니다.
- 2 vRealize Automation 장치에서 템플릿 tar.gz 패키지를 다운로드합니다.

```
wget https://vrealize-automation-appliance-  
FQDN/software/download/prepare_vra_template.tar.gz
```

환경에서 자체 서명된 인증서를 사용 중인 경우 --no-check-certificate 옵션이 필요할 수도 있습니다.

```
wget --no-check-certificate https://vrealize-automation-appliance-  
FQDN/software/download/prepare_vra_template.tar.gz
```

- 3 tar 패키지의 압축을 풉니다.
- 4 압축을 푼 tar 출력에서 설치 관리자 스크립트를 찾아 실행 파일로 만듭니다.

```
chmod +x prepare_vra_template.sh
```


5 다음 설치 관리자 스크립트를 실행합니다.

```
./prepare_vra_template.sh
```

비대화형 옵션 및 예상 값에 대한 정보가 필요한 경우 스크립트 도움말을 참조하십시오.

```
./prepare_vra_template.sh --help
```

6 표시되는 메시지를 따릅니다.

설치에 성공하면 확인 메시지가 나타납니다. 오류 및 로그가 나타나면 오류를 해결하고 스크립트를 다시 실행합니다.

7 완료되면 Linux 가상 시스템을 종료합니다.

스크립트가 이전의 게스트 또는 Software 부트스트랩 에이전트를 제거하고 지원되는 Java Runtime Environment 버전, 게스트 에이전트 및 Software 부트스트랩 에이전트를 설치합니다.

후속 작업

하이퍼바이저 또는 클라우드 제공자에서, 참조 시스템을 복제를 위한 템플릿, 스냅샷 또는 Amazon 시스템 이미지로 변환합니다. 각각 Software 구성 요소를 지원하며, 인프라 설계자는 Blueprint를 생성할 때 이를 사용할 수 있습니다.

vRealize Automation 에서 기존의 가상 시스템 템플릿 업데이트

템플릿, Amazon 시스템 이미지 또는 최신 버전의 Windows Software 부트스트랩 에이전트에 대한 스냅샷을 업데이트 중이거나 prepare_vra_template.sh 스크립트를 사용하는 대신 최신 Linux Software 부트스트랩 에이전트로 수동 업데이트하는 경우에는 기존 버전을 제거하고 모든 로그를 삭제해야 합니다.

Linux

Linux 참조 시스템의 경우 재설치하기 전에 prepare_vra_template.sh 스크립트를 실행하면 에이전트가 재설정되고 모든 로그가 제거됩니다. 하지만 수동으로 설치하려는 경우에는 참조 시스템에 루트 사용자로 로그인한 다음 아티팩트를 재설정하고 제거하는 명령을 실행해야 합니다.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

Windows

Windows 참조 시스템의 경우 기존 Software 에이전트 부트스트랩 및 vRealize Automation 6.0 이상의 게스트 에이전트를 제거하고 기존 런타임 로그 파일을 삭제합니다. PowerShell 명령 창에서 에이전트 및 아티팩트 제거 명령을 실행합니다.

```
c:\opt\vmware-appdirector\agent-bootstrap\agent_bootstrap_removal.bat
c:\opt\vmware-appdirector\agent-bootstrap\agent_reset.bat
```

시나리오: 시스템 복제 및 소프트웨어 구성 요소 Blueprint를 위해 vSphere CentOS 템플릿 준비

vCenter Server 관리자로서 vRealize Automation 설계자가 Linux CentOS 시스템을 복제하는 데 사용할 수 있는 vSphere 템플릿을 준비합니다. 템플릿이 소프트웨어 구성 요소를 포함하는 Blueprint를 지원하는지 확인하고 참조 시스템을 템플릿으로 전환하기 전에 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치합니다.

필수 조건

- VMware Tools가 설치되어 있는 Linux CentOS 참조 시스템을 식별하거나 생성합니다. Blueprint 설계자가 Blueprint 수준에서 인터넷 연결 기능을 추가하지 못하는 경우를 대비하여 인터넷 연결을 제공하기 위한 네트워크 어댑터를 최소 하나 포함합니다. 가상 시스템을 생성하는 데 대한 자세한 내용은 vSphere 설명서를 참조하십시오.
- 가상 시스템을 템플릿으로 변환하려면 vCenter Server에 연결되어 있어야 합니다. vSphere Client를 vSphere ESXi 호스트에 직접 연결하는 경우에는 템플릿을 생성할 수 없습니다.

프로시저

1 시나리오: 게스트 에이전트 사용자 지정 및 소프트웨어 구성 요소를 위해 참조 시스템 준비

템플릿에서 소프트웨어 구성 요소를 지원할 수 있도록 참조 시스템에 소프트웨어 부트스트랩 에이전트와 해당 필수 구성 요소, 게스트 에이전트를 설치합니다. 에이전트는 사용자의 템플릿을 사용하는 vRealize Automation 설계자가 소프트웨어 구성 요소를 해당 Blueprint에 포함할 수 있도록 합니다.

2 시나리오: CentOS 참조 시스템을 템플릿으로 변환

참조 시스템에 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치한 후에는 참조 시스템을 vRealize Automation 설계자가 복제 시스템 Blueprint를 생성하는 데 사용할 수 있는 템플릿으로 변환합니다.

3 시나리오: vSphere 복제를 위해 사용자 지정 규격 생성

Blueprint 설계자가 cpb_centos_63_x84 템플릿과 함께 사용하도록 사용자 지정 규격을 생성합니다.

Blueprint 설계자가 Linux CentOS 시스템을 복제하는 vRealize Automation Blueprint를 생성하는 데 사용할 수 있는 템플릿과 사용자 지정 규격을 참조 시스템에서 생성했습니다. 참조 시스템에 Software 부트스트랩 에이전트와 게스트 에이전트를 설치했기 때문에 설계자는 템플릿을 사용하여 Software 구성 요소 또는 기타 게스트 에이전트 사용자 지정(예: 스크립트 실행 또는 디스크 포맷)을 포함하는 정교한 카탈로그 항목 Blueprint를 생성할 수 있습니다. VMware Tools를 설치했기 때문에 설계자와 카탈로그 관리자는 사용자가 재구성, 스냅샷 생성, 재부팅과 같은 시스템에 대한 작업을 수행하도록 허용할 수 있습니다.

후속 작업

vRealize Automation 사용자, 그룹 및 리소스를 구성한 후에는 템플릿과 사용자 지정 규격을 사용하여 복제를 위한 시스템 Blueprint를 생성할 수 있습니다. Rainpole의 vRealize Automation 설치 및 구성 시나리오의 내용을 참조하십시오.

시나리오: 게스트 에이전트 사용자 지정 및 소프트웨어 구성 요소를 위해 참조 시스템 준비

템플릿에서 소프트웨어 구성 요소를 지원할 수 있도록 참조 시스템에 소프트웨어 부트스트랩 에이전트와 해당 필수 구성 요소, 게스트 에이전트를 설치합니다. 에이전트는 사용자의 템플릿을 사용하는 vRealize Automation 설계자가 소프트웨어 구성 요소를 해당 Blueprint에 포함할 수 있도록 합니다.

프로세스를 간소화하려면 별도의 패키지를 다운로드하여 설치하는 대신 두 에이전트를 모두 설치하는 vRealize Automation 스크립트를 다운로드하여 실행합니다.

또한 스크립트는 Manager Service 인스턴스에 연결하여 SSL 인증서를 다운로드합니다. 이는 Manager Service와 템플릿으로 배포된 시스템 간에 신뢰를 설정합니다. 스크립트를 사용하여 인증서를 다운로드하는 것은 수동으로 Manager Service SSL 인증서를 가져와서 /usr/share/gugent/cert.pem의 참조 시스템에 설치하는 것보다 보안성이 떨어집니다.

프로시저

- 1 웹 브라우저에서 다음 URL을 엽니다.

`https://vrealize-automation-appliance-FQDN/software/index.html`

- 2 `prepare_vra_template.sh` 스크립트를 참조 시스템에 저장합니다.
- 3 참조 시스템에서 `prepare_vra_template.sh` 실행 파일을 만듭니다.

```
chmod +x prepare_vra_template.sh
```

- 4 `prepare_vra_template.sh`를 실행합니다.

```
./prepare_vra_template.sh
```

- 5 표시되는 메시지를 따릅니다.

옵션 및 값에 대한 비대화형 정보를 원하는 경우 `./prepare_vra_template.sh --help`를 입력합니다.

설치가 완료되면 확인 메시지가 나타납니다. 오류 메시지와 로그가 나타나면 문제를 해결하고 스크립트를 다시 실행합니다.

시나리오: CentOS 참조 시스템을 템플릿으로 변환

참조 시스템에 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치한 후에는 참조 시스템을 vRealize Automation 설계자가 복제 시스템 Blueprint를 생성하는 데 사용할 수 있는 템플릿으로 변환합니다.

참조 시스템을 템플릿으로 변환한 후에는 템플릿을 가상 시스템으로 다시 변환하기 전에는 템플릿을 편집하거나 전원을 켤 수 없습니다.

프로시저

- 1 참조 시스템에 루트 사용자로 로그인하고 변환을 위해 시스템을 준비합니다.

- a udev 지속성 규칙을 제거합니다.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b 이 템플릿에서 복제된 시스템이 고유한 식별자를 사용하도록 설정합니다.

```
/bin/sed -i '/^W(HWADDRW|UUIDW)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c 소프트웨어 부트스트랩 에이전트를 설치한 이후에 참조 시스템을 재부팅하거나 재구성한 경우, 에이전트를 재설정합니다.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- d 시스템 전원을 끕니다.

```
shutdown -h now
```

- 2 vSphere Web Client에 관리자로 로그인합니다.
- 3 참조 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 4 **VM 이름** 텍스트 상자에 **cpb_centos_63_x84**를 입력합니다.
- 5 참조 시스템에 CentOS 게스트 운영 체제가 있더라도 **게스트 OS 버전** 드롭다운 메뉴에서 **Red Hat Enterprise Linux 6(64비트)**을 선택합니다.
CentOS를 선택하면 템플릿 및 사용자 지정 규격이 예상과 다르게 작동할 수 있습니다.
- 6 vSphere Web Client에서 참조 시스템을 마우스 오른쪽 버튼으로 클릭하고 **템플릿 > 템플릿으로 변환**을 선택합니다.

vCenter Server가 your cpb_centos_63_x84 참조 시스템을 템플릿으로 표시하고 작업을 [최근 작업] 창에 표시합니다. vRealize Automation에서 이미 vSphere 환경을 관리하고 있는 경우에는 다음 번에 자동화된 데이터 수집을 수행하는 동안 이 템플릿이 검색됩니다. vRealize Automation을 아직 구성하지 않은 경우에는 다음 번에 자동화된 데이터 수집을 수행하는 동안 해당 템플릿이 수집됩니다.

시나리오: vSphere 복제를 위해 사용자 지정 규격 생성

Blueprint 설계자가 cpb_centos_63_x84 템플릿과 함께 사용하도록 사용자 지정 규격을 생성합니다.

프로시저

- 1 vSphere Web Client에 관리자로 로그인합니다.
- 2 홈 페이지에서 **사용자 지정 규격 관리자**를 클릭하여 마법사를 엽니다.

- 3 새로 만들기 아이콘을 클릭합니다.
- 4 새로 만들기 아이콘을 클릭합니다.
- 5 속성을 지정합니다.
 - a 대상 VM 운영 체제 드롭다운 메뉴에서 **Linux**를 선택합니다.
 - b 사용자 지정 규격 이름 텍스트 상자에 **Customspecs**를 입력합니다.
 - c 설명 텍스트 상자에 **cpb_centos_63_x84 cloning with vRealize Automation**을 입력합니다.
 - d 다음을 클릭합니다.
- 6 컴퓨터 이름을 설정합니다.
 - a 가상 시스템 이름 사용을 선택합니다.
 - b 도메인 이름 텍스트 상자에 복제된 시스템이 프로비저닝될 도메인을 입력합니다.
 - c 다음을 클릭합니다.
- 7 영역 설정을 구성합니다.
- 8 다음을 클릭합니다.
- 9 모든 네트워크 인터페이스에서 DHCP 사용 등 게스트 운영 체제에 대해 표준 네트워크 설정 사용을 선택합니다.

패브릭 관리자와 인프라 설계자는 vRealize Automation에서 네트워크 프로파일을 생성하고 사용하는 방법으로 프로비저닝된 시스템에 대한 네트워크 설정을 처리합니다.
- 10 표시되는 메시지에 따라 필요한 나머지 정보를 입력합니다.
- 11 완료할 준비가 됨 페이지에서 선택 항목을 검토하고 마침을 클릭합니다.

시나리오: vSphere 샘플 애플리케이션 Blueprint용 Dukes Bank 가져오기 준비

vCenter Server 관리자로서 vRealize Automation Dukes Bank 샘플 애플리케이션을 프로비저닝하는 데 사용할 수 있는 vSphere CentOS 6.x Linux 템플릿과 사용자 지정 규격을 준비하려고 합니다.

템플릿이 샘플 애플리케이션 소프트웨어 구성 요소를 지원하도록 할 계획이므로 Linux 참조 시스템에 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 설치한 이후에 참조 시스템을 템플릿으로 변환하여 사용자 지정 규격을 생성합니다. 참조 시스템에서 SELinux를 사용하지 않도록 설정하여 해당 템플릿이 Dukes Bank 샘플 애플리케이션에 사용된 MySQL의 특정 구현을 지원하게 합니다.

필수 조건

- vRealize Automation을 설치하고 완전하게 구성합니다. Rainpole의 vRealize Automation 설치 및 구성 시나리오 항목을 참조하십시오.
- VMware Tools가 설치되어 있는 CentOS 6.x Linux 참조 시스템을 식별하거나 생성합니다. 가상 시스템을 생성하는 데 대한 자세한 내용은 vSphere 설명서를 참조하십시오.

- 가상 시스템을 템플릿으로 변환하려면 vCenter Server에 연결되어 있어야 합니다. vSphere Client를 vSphere ESXi 호스트에 직접 연결하는 경우에는 템플릿을 생성할 수 없습니다.

프로시저

1 시나리오: Dukes Bank vSphere 샘플 애플리케이션을 위해 참조 시스템 준비

템플릿으로 Dukes Bank 샘플 애플리케이션을 지원할 계획이기 때문에 vRealize Automation이 소프트웨어 구성 요소를 프로비저닝할 수 있도록 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 모두 참조 시스템에 설치해야 합니다. 프로세스를 간소화하기 위해, 패키지를 개별적으로 다운로드하고 설치하는 대신 게스트 에이전트와 소프트웨어 부트스트랩 에이전트 둘 모두를 설치하는 vRealize Automation 스크립트를 다운로드하여 실행합니다.

2 시나리오: 참조 시스템을 Dukes Bank vSphere 샘플 애플리케이션을 위한 템플릿으로 변환

참조 시스템에서 게스트 에이전트 및 소프트웨어 부트스트랩 에이전트를 설치한 후 SELinux를 사용하지 않게 설정하여 템플릿이 Dukes Bank 샘플 애플리케이션에 사용되는 MySQL의 특정 구현을 지원하게 합니다. Dukes Bank vSphere 샘플 애플리케이션을 프로비저닝하는 데 사용할 수 있는 템플릿으로 참조 시스템을 전환합니다.

3 시나리오: Dukes Bank vSphere 샘플 애플리케이션 시스템을 복제하는 사용자 지정 규격 생성

Dukes Bank 시스템 템플릿과 함께 사용할 사용자 지정 규격을 생성합니다.

vRealize Automation Dukes Bank 샘플 애플리케이션을 지원하는 참조 시스템으로부터 템플릿과 사용자 지정 규격을 생성했습니다.

시나리오: Dukes Bank vSphere 샘플 애플리케이션을 위해 참조 시스템 준비

템플릿으로 Dukes Bank 샘플 애플리케이션을 지원할 계획이기 때문에 vRealize Automation이 소프트웨어 구성 요소를 프로비저닝할 수 있도록 게스트 에이전트와 소프트웨어 부트스트랩 에이전트를 모두 참조 시스템에 설치해야 합니다. 프로세스를 간소화하기 위해, 패키지를 개별적으로 다운로드하고 설치하는 대신 게스트 에이전트와 소프트웨어 부트스트랩 에이전트 둘 모두를 설치하는 vRealize Automation 스크립트를 다운로드하여 실행합니다.

프로시저

- 1 참조 시스템에 루트 사용자로 로그인합니다.
- 2 vRealize Automation 장치에서 설치 스크립트를 다운로드합니다.

```
wget https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

환경에서 자체 서명된 인증서를 사용하는 경우에는 wget 옵션인 --no-check-certificate 옵션을 사용해야 할 수 있습니다. 예:

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

- 3 prepare_vra_template.sh 스크립트를 실행 가능한 상태로 만듭니다.

```
chmod +x prepare_vra_template.sh
```

4 prepare_vra_template.sh 설치 관리자 스크립트를 실행합니다.

```
./prepare_vra_template.sh
```

도움말 명령 ./prepare_vra_template.sh --help를 실행하여 비대화형 옵션 및 예상 값에 대한 정보를 확인할 수 있습니다.

5 프롬프트에 따라 설치를 완료합니다.

설치가 성공적으로 완료되면 확인 메시지가 표시됩니다. 콘솔에서 오류 메시지와 로그가 표시되면 오류를 해결한 후 설치 관리자 스크립트를 다시 실행합니다.

Dukes Bank 샘플 애플리케이션이 소프트웨어 구성 요소를 성공적으로 프로비저닝할 수 있도록 소프트웨어 부트스트랩 에이전트와 그 사전 요구 사항인 게스트 에이전트를 둘 모두 설치했습니다. 스크립트는 또한 Manager Service 인스턴스에 연결한 후 SSL 인증서를 다운로드하여 Manager Service와 템플릿에서 배포된 시스템 사이에 신뢰 관계를 구현했습니다. 이 방법은 Manager Service SSL 인증서를 가져와서 참조 시스템의 /usr/share/guagent/cert.pem에 수동으로 설치하는 방법보다는 안전하지 않습니다. 보안이 매우 중요한 경우에는 지금 이 인증서를 수동으로 바꿀 수 있습니다.

시나리오: 참조 시스템을 Dukes Bank vSphere 애플리케이션을 위한 템플릿으로 변환

참조 시스템에서 게스트 에이전트 및 소프트웨어 부트스트랩 에이전트를 설치한 후 SELinux를 사용하지 않게 설정하여 템플릿이 Dukes Bank 샘플 애플리케이션에 사용되는 MySQL의 특정 구현을 지원하게 합니다. Dukes Bank vSphere 샘플 애플리케이션을 프로비저닝하는 데 사용할 수 있는 템플릿으로 참조 시스템을 전환합니다.

참조 시스템을 템플릿으로 변환한 후에는 템플릿을 가상 시스템으로 다시 변환하기 전에는 템플릿을 편집하거나 전원을 켤 수 없습니다.

프로시저

1 참조 시스템에 루트 사용자로 로그인합니다.

- a /etc/selinux/config 파일을 편집하여 SELinux를 사용하지 않게 설정합니다.

```
SELINUX=disabled
```

SELinux를 사용하지 않게 설정해 두지 않으면, Dukes Bank 샘플 애플리케이션의 MySQL 소프트웨어 구성 요소가 예상대로 작동하지 않을 수 있습니다.

- b udev 지속성 규칙을 제거합니다.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- c 이 템플릿에서 복제된 시스템이 고유한 식별자를 사용하도록 설정합니다.

```
/bin/sed -i '/^W(HWADDRW|UUIDW)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```


- d 소프트웨어 부트스트랩 에이전트를 설치한 이후에 참조 시스템을 재부팅하거나 재구성한 경우, 에이전트를 재설정합니다.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- e 시스템 전원을 끕니다.

```
shutdown -h now
```

- 2 vSphere Web Client에 관리자로 로그인합니다.
- 3 참조 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 4 **VM 이름** 텍스트 상자에 **dukes_bank_template**을 입력합니다.
- 5 참조 시스템에 CentOS 게스트 운영 체제가 있는 경우에는 **게스트 OS 버전** 드롭다운 메뉴에서 **Red Hat Enterprise Linux 6(64비트)**을 선택합니다.
CentOS를 선택하면 템플릿 및 사용자 지정 규격이 예상과 다르게 작동할 수 있습니다.
- 6 **확인**을 클릭합니다.
- 7 vSphere Web Client에서 참조 시스템을 마우스 오른쪽 버튼으로 클릭하고 **템플릿 > 템플릿으로 변환**을 선택합니다.

vCenter Server가 dukes_bank_template 참조 시스템을 템플릿으로 표시하고 작업을 [최근 작업] 창에 표시합니다. vRealize Automation에서 이미 vSphere 환경을 관리하고 있는 경우에는 다음 번에 자동화된 데이터 수집을 수행하는 동안 이 템플릿이 검색됩니다. vRealize Automation을 아직 구성하지 않은 경우에는 다음 번에 자동화된 데이터 수집을 수행하는 동안 해당 템플릿이 수집됩니다.

시나리오: Dukes Bank vSphere 샘플 애플리케이션 시스템을 복제하는 사용자 지정 규격 생성

Dukes Bank 시스템 템플릿과 함께 사용할 사용자 지정 규격을 생성합니다.

프로시저

- 1 vSphere Web Client에 관리자로 로그인합니다.
- 2 홈 페이지에서 **사용자 지정 규격 관리자**를 클릭하여 마법사를 엽니다.
- 3 **새로 만들기** 아이콘을 클릭합니다.
- 4 속성을 지정합니다.
 - a **대상 VM 운영 체제** 드롭다운 메뉴에서 **Linux**를 선택합니다.
 - b **사용자 지정 규격 이름** 텍스트 상자에 **Customspecs_sample**을 입력합니다.
 - c **설명** 텍스트 상자에 **Dukes Bank customization spec**을 입력합니다.
 - d **다음**을 클릭합니다.

5 컴퓨터 이름을 설정합니다.

- a 가상 시스템 이름 사용을 선택합니다.
- b Dukes Bank 샘플 애플리케이션을 프로비저닝할 도메인을 **도메인 이름** 텍스트 상자에 입력합니다.
- c 다음을 클릭합니다.

6 영역 설정을 구성합니다.

7 다음을 클릭합니다.

8 모든 네트워크 인터페이스에서 DHCP 사용 등 게스트 운영 체제에 대해 표준 네트워크 설정 사용을 선택합니다.

패브릭 관리자와 인프라 설계자는 vRealize Automation에서 네트워크 프로파일을 생성하고 사용하는 방법으로 프로비저닝된 시스템에 대한 네트워크 설정을 처리합니다.

9 표시되는 메시지에 따라 필요한 나머지 정보를 입력합니다.

10 완료할 준비가 됨 페이지에서 선택 항목을 검토하고 **마침**을 클릭합니다.

Dukes Bank 샘플 애플리케이션을 프로비저닝하는 데 사용할 수 있는 템플릿과 사용자 지정 규격을 생성했습니다.

후속 작업

- 1 게이트웨이 및 IP 주소 범위를 제공하기 위해 외부 네트워크 프로파일을 생성합니다. [타사 IPAM 제공자를 사용하여 외부 네트워크 프로파일 생성](#) 항목을 참조하십시오.
- 2 외부 네트워크 프로파일을 vSphere 예약에 매핑합니다. [Hyper-V, KVM, SCVMM, vSphere 또는 XenServer에 대한 예약 생성](#) 항목을 참조하십시오. 샘플 애플리케이션은 외부 네트워크 프로파일 없이 프로비저닝할 수 없습니다.
- 3 Dukes Bank 샘플 애플리케이션을 해당 환경으로 가져옵니다. [시나리오: vSphere 샘플 애플리케이션용 Dukes Bank 가져오기 및 환경 구성](#) 항목을 참조하십시오.

Blueprint 프로비저닝을 위한 테넌트 및 리소스 준비

2

각각 고유한 사용자 그룹과 vRealize Automation 관리 대상으로 만든 리소스에 대한 고유한 액세스 권한을 가진 여러 개의 테넌트 환경을 구성할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [테넌트 설정 구성](#)
- [리소스 구성](#)

테넌트 설정 구성

테넌트 관리자는 사용자 인증과 같은 테넌트 설정을 구성하고 사용자 역할 및 비즈니스 그룹을 관리합니다. 시스템 관리자와 테넌트 관리자는 알림과 vRealize Automation 콘솔에 대한 브랜딩을 처리하기 위해 이메일 서버와 같은 옵션을 구성합니다.

테넌트 설정 구성 검사 목록을 사용하면 테넌트 설정을 구성하는 데 필요한 일련의 단계에 대한 개괄적인 개요를 볼 수 있습니다.

표 2-1. 테넌트 설정 구성 검사 목록

작업	vRealize Automation 역할	세부 정보
<input type="checkbox"/> 로컬 사용자 계정을 생성하고 테넌트 관리자를 할당합니다.	시스템 관리자	로컬 사용자 계정 생성에 대한 예는 Rainpole의 vRealize Automation 설치 및 구성 시나리오를 참조하십시오.
<input type="checkbox"/> 디렉토리 관리를 구성하여 테넌트 ID 관리와 액세스 제어 설정을 설정합니다.	테넌트 관리자	디렉토리 관리 구성 옵션 선택
<input type="checkbox"/> 비즈니스 그룹과 사용자 지정 그룹을 생성하고 vRealize Automation 콘솔에 대한 사용자 액세스 권한을 부여합니다.	테넌트 관리자	그룹 및 사용자 역할 구성
<input type="checkbox"/> (선택 사항) 사용자가 작업 할당을 완료하는 데 필요한 적절한 애플리케이션과 리소스에 액세스할 수 있도록 추가 테넌트를 생성합니다.	시스템 관리자	추가 테넌트 생성
<input type="checkbox"/> (선택 사항) vRealize Automation 콘솔의 테넌트 로그인 및 애플리케이션 페이지에서 사용자 지정 브랜딩을 구성합니다.	<ul style="list-style-type: none">■ 시스템 관리자■ 테넌트 관리자	사용자 지정 브랜딩 구성

표 2-1. 테넌트 설정 구성 검사 목록 (계속)

작업	vRealize Automation 역할	세부 정보
<input type="checkbox"/> (선택 사항) 특정 이벤트가 발생했을 때 사용자에게 알림을 보내도록 vRealize Automation을 구성합니다.	<ul style="list-style-type: none"> 시스템 관리자 테넌트 관리자 	알림 구성을 위한 검사 목록
<input type="checkbox"/> (선택 사항) XaaS 및 기타 확장성 지원을 위해 vRealize Orchestrator를 구성합니다.	<ul style="list-style-type: none"> 시스템 관리자 테넌트 관리자 	vRealize Orchestrator 구성
<input type="checkbox"/> (선택 사항) IaaS 설계자가 RDP 설정 구성을 위해 Blueprint에서 사용하는 사용자 지정 원격 데스크톱 프로토콜 파일을 생성합니다.	시스템 관리자	프로비저닝된 시스템에 대한 RDP 연결 지원을 위해 사용자 지정 RDP 파일 생성
<input type="checkbox"/> (선택 사항) 사용자가 시스템을 요청할 때 프로비저닝을 위한 적합한 위치를 선택하도록 허용하기 위해 패브릭 관리자와 IaaS 설계자가 활용할 수 있는 데이터 센터 위치를 정의합니다.	시스템 관리자	데이터 센터 위치 추가에 대한 예는 시나리오: 영역 간 배포를 위한 데이터 센터 위치 추가 항목을 참조하십시오.

디렉토리 관리 구성 옵션 선택

vRealize Automation 디렉토리 관리 기능을 사용하여 사용자 인증 요구 사항에 따라 Active Directory 링크를 구성할 수 있습니다.

디렉토리 관리는 사용자 지정 수준이 높은 사용자 인증을 지원하는 여러 옵션을 제공합니다.

표 2-2. 디렉토리 관리 구성 옵션 선택

구성 옵션	절차
Active Directory에 대한 링크를 구성합니다.	<ol style="list-style-type: none"> Active Directory에 대한 링크를 구성합니다. LDAP/IWA를 통한 Active Directory 링크 구성 항목을 참조하십시오. 고가용성을 위해 vRealize Automation을 구성한 경우, 고가용성을 위해 디렉토리 관리 구성을 참조하십시오.
(선택 사항) Active Directory 페더레이션된 서비스와의 양방향 통합을 구성하여 사용자 ID 및 암호 기반 디렉토리 링크의 보안을 향상합니다.	vRealize Automation과 Active Directory 간 양방향 신뢰 관계 구성
(선택 사항) 기존 Active Directory 링크에 사용자 및 그룹을 추가합니다.	Active Directory 연결에 사용자 또는 그룹 추가.
(선택 사항) 기본 정책을 편집하여 Active Directory 링크에 대해 사용자 지정 규칙을 적용합니다.	사용자 액세스 정책 관리.
(선택 사항) 네트워크 범위를 구성하여 사용자가 시스템에 로그인할 때 사용하는 IP 주소를 제한하고, 로그인 제한(시간 제한, 계정이 잠기기 전의 로그인 시도 횟수)을 관리합니다.	네트워크 범위 추가 또는 편집.

디렉토리 관리 개요

테넌트 관리자는 vRealize Automation 애플리케이션 콘솔에서 디렉토리 관리 옵션을 사용하여 테넌트 ID 관리 및 액세스 제어 설정을 구성할 수 있습니다.

관리 > 디렉토리 관리 탭에서 다음 설정을 관리할 수 있습니다.

표 2-3. 디렉토리 관리 설정

설정	설명
디렉토리	<p>[디렉토리] 페이지에서는 vRealize Automation 테넌트 사용자 인증 및 권한 부여를 지원하는 Active Directory 링크를 생성하고 관리할 수 있습니다. 하나 이상의 디렉토리를 생성하고 생성된 디렉토리를 Active Directory 배포와 동기화합니다. 이 페이지는 디렉토리에 동기화된 그룹 및 사용자의 수와 마지막 동기화 시간을 표시합니다. 지금 동기화를 클릭하여 디렉토리 동기화를 수동으로 시작할 수 있습니다.</p> <p>Active Directory 링크 생성을 위해 디렉토리 관리 사용 항목을 참조하십시오.</p> <p>디렉토리를 클릭하고 동기화 설정 버튼을 클릭하면 동기화 설정을 편집하고, ID 제공자 페이지로 이동하고, 동기화 로그를 볼 수 있습니다.</p> <p>[디렉토리 동기화 설정] 페이지에서는 동기화 빈도를 스케줄링하고, 이 디렉토리와 연결된 도메인 목록을 보고, 매핑된 특성 목록을 변경하고, 동기화되는 사용자 및 그룹 목록을 업데이트하고, 보호 대상을 설정할 수 있습니다.</p>
커넥터	<p>[커넥터] 페이지는 엔터프라이즈 네트워크용으로 배포된 커넥터를 나열합니다. 커넥터는 Active Directory와 디렉토리 관리 서비스 간 사용자 및 그룹 데이터를 동기화합니다. ID 제공자로 사용되는 경우에는 서비스에 대해 사용자를 인증합니다. 각 vRealize Automation 장치에는 기본적으로 하나의 커넥터가 포함되어 있습니다. 커넥터 및 커넥터 클러스터 관리 항목을 참조하십시오.</p>
사용자 특성	<p>[사용자 특성] 페이지는 디렉토리에서 동기화되는 기본 사용자 특성을 나열합니다. Active Directory 특성에 매핑할 수 있는 다른 특성을 추가할 수 있습니다. 디렉토리와의 동기화를 위해 특성 선택 항목을 참조하십시오.</p>
네트워크 범위	<p>이 페이지는 시스템에 대해 구성된 네트워크 범위를 나열합니다. 사용자가 그러한 IP 주소를 통해 액세스하도록 네트워크 범위를 구성합니다. 추가 네트워크 범위를 추가하고 기존 범위를 편집할 수 있습니다. 네트워크 범위 추가 또는 편집 항목을 참조하십시오.</p>
ID 제공자	<p>[ID 제공자] 페이지는 시스템에서 사용할 수 있는 ID 제공자를 나열합니다.</p> <p>vRealize Automation 시스템에는 기본 ID 제공자 역할을 하면서 많은 사용자의 요구를 충족하는 하나의 커넥터가 포함되어 있습니다. 타사 ID 제공자 인스턴스를 추가하거나 두 가지 모두의 조합을 가질 수 있습니다.</p> <p>타사 ID 제공자 연결 구성 항목을 참조하십시오.</p>
정책	<p>[정책] 페이지는 기본 액세스 정책 및 사용자가 생성한 기타 웹 애플리케이션 액세스 정책을 나열합니다. 정책은 사용자가 애플리케이션 포털에 액세스하거나 활성화된 웹 애플리케이션을 시작하기 위해 충족되어야 하는 기준을 지정하는 일련의 규칙입니다. 기본 정책은 대부분의 vRealize Automation 배포에 적합하지만 필요한 경우 편집할 수 있습니다. 사용자 액세스 정책 관리 항목을 참조하십시오.</p>

Active Directory 관련 중요 개념

Directories Management가 Active Directory 환경에 통합되는 방식을 이해하려면 몇 가지 Active Directory 관련 개념을 알고 있어야 합니다.

Connector

서비스 구성 요소인 connector는 다음 기능을 수행합니다.

- Active Directory 및 서비스 간에 사용자 및 그룹 데이터를 동기화합니다.
- ID 제공자로 사용될 경우 사용자를 서비스에 인증합니다.

connector가 기본 ID 제공자입니다. connector에서 지원하는 인증 방법은 VMware Identity Manager 관리를 참조하십시오. SAML 2.0 프로토콜을 지원하는 타사 ID 제공자를 사용할 수도 있습니다. 엔터프라이즈 보안 정책에 따라 타사 ID 제공자를 선호할 경우 connector가 지원하지 않는 인증 유형 또는 connector가 지원하는 인증 유형에 대해 타사 ID 제공자를 사용하십시오.

참고 타사 ID 제공자를 사용할 경우에도 사용자 및 그룹 데이터를 동기화하도록 connector를 구성해야 합니다.

디렉토리

Directories Management 서비스에는 Active Directory 특성 및 매개 변수를 사용하여 사용자 및 그룹을 정의하는 고유한 디렉토리 개념이 있습니다. 하나 이상의 디렉토리를 생성한 다음, 해당 디렉토리를 Active Directory 배포와 동기화합니다. 서비스에서 다음과 같은 디렉토리 유형을 생성할 수 있습니다.

- LDAP를 통한 Active Directory. 단일 Active Directory 도메인 환경에 연결할 계획인 경우 이 디렉토리 유형을 생성합니다. LDAP를 통한 Active Directory 디렉토리 유형의 경우 connector가 단순한 바인딩 인증을 사용하여 Active Directory에 바인딩합니다.
- Active Directory(통합된 Windows 인증). 다중 도메인 또는 다중 포리스트 Active Directory 환경에 연결할 계획인 경우 이 디렉토리 유형을 생성합니다. connector는 통합된 Windows 인증을 사용하여 Active Directory에 바인딩합니다.

사용 중인 Active Directory 환경(단일 도메인, 다중 도메인) 및 도메인 간에 사용된 신뢰 유형에 따라 생성하는 디렉토리 유형 및 개수가 달라집니다. 대부분의 환경에서는 하나의 디렉토리를 생성합니다.

Active Directory에 대한 직접적인 액세스 권한이 서비스에 없습니다. connector만 Active Directory에 대한 직접적인 액세스 권한을 갖고 있습니다. 따라서 서비스에서 생성한 각 디렉토리를 connector 인스턴스와 연결합니다.

작업자

디렉토리를 connector 인스턴스와 연결할 경우 connector가 작업자라고 하는 연결된 디렉토리에 대한 파티션을 생성합니다. connector 인스턴스에는 연결된 작업자가 여러 개 있을 수 있습니다. 각 작업자는 ID 제공자 역할을 합니다. 작업자별로 인증 방법을 정의 및 구성합니다.

connector는 하나 이상의 작업자를 통해 Active Directory 및 서비스 간에 사용자 및 그룹 데이터를 동기화합니다.

통합된 Windows 인증 유형의 작업자 두 개가 동일한 connector 인스턴스에 있으면 안 됩니다.

Active Directory 환경

단일 Active Directory 도메인, 단일 Active Directory 포리스트의 다중 도메인 또는 여러 Active Directory 포리스트의 다중 도메인으로 구성된 Active Directory 환경과 서비스를 통합할 수 있습니다.

단일 Active Directory 도메인 환경

단일 Active Directory 배포를 통해 단일 Active Directory 도메인의 사용자와 그룹을 동기화할 수 있습니다.

LDAP/IWA를 통한 Active Directory 링크 구성 항목을 참조하십시오. 이 환경의 경우 디렉토리를 서비스에 추가할 때 [LDAP를 통한 Active Directory] 옵션을 선택합니다.

다중 도메인, 단일 포리스트 Active Directory 환경

다중 도메인, 단일 포리스트 Active Directory 배포에서는 단일 포리스트 내에 있는 다중 Active Directory 도메인의 사용자와 그룹을 동기화할 수 있습니다.

이 Active Directory 환경에 대한 서비스를 단일 Active Directory, 통합 Windows 인증 디렉토리 유형 또는 글로벌 카탈로그 옵션으로 구성된 LDAP를 통한 Active Directory 디렉토리 유형으로 구성할 수 있습니다.

- 권장되는 옵션은 단일 Active Directory, 통합 Windows 인증 디렉토리 유형을 생성하는 것입니다.

LDAP/IWA를 통한 Active Directory 링크 구성 항목을 참조하십시오. 이 환경에 대해 디렉토리를 추가하는 경우 [Active Directory(통합 Windows 인증)] 옵션을 선택합니다.

신뢰 관계가 있는 다중 포리스트 Active Directory 환경

신뢰 관계가 있는 다중 포리스트 Active Directory 배포에서는 여러 포리스트에서 양방향 신뢰가 있는 다중 Active Directory 도메인의 사용자와 그룹을 동기화할 수 있습니다.

LDAP/IWA를 통한 Active Directory 링크 구성 항목을 참조하십시오. 이 환경에 대해 디렉토리를 추가하는 경우 [Active Directory(통합 Windows 인증)] 옵션을 선택합니다.

신뢰 관계가 없는 다중 포리스트 Active Directory 환경

신뢰 관계가 없는 다중 포리스트 Active Directory 배포에서는 여러 포리스트에서 신뢰 관계가 없는 다중 Active Directory 도메인의 사용자와 그룹을 동기화할 수 있습니다. 이 환경에서는 서비스에서 여러 디렉토리를 생성합니다(각 포리스트에 디렉토리 하나).

LDAP/IWA를 통한 Active Directory 링크 구성 항목을 참조하십시오. 이 서비스에서 생성하는 디렉토리의 유형은 포리스트에 따라 다릅니다. 다중 도메인이 있는 포리스트에서는 [Active Directory(통합 Windows 인증)] 옵션을 선택합니다. 단일 도메인이 있는 포리스트에서는 [LDAP를 통한 Active Directory] 옵션을 선택합니다.

Active Directory 링크 생성을 위해 디렉토리 관리 사용

vRealize Automation 테넌트를 생성한 후에는 테넌트 관리자로 시스템 콘솔에 로그인하고 사용자 인증을 지원하기 위한 Active Directory 링크를 생성해야 합니다.

디렉토리 관리를 사용하여 Active Directory 연결을 구성할 때 사용할 수 있는 Active Directory 통신 프로토콜 옵션에는 세 가지가 있습니다.

- LDAP를 통한 Active Directory - LDAP를 통한 Active Directory 프로토콜은 기본적으로 DNS 서비스 위치 조회를 지원합니다.

- Active Directory(Windows 통합 인증) - Active Directory(Windows 통합 인증)는 가입할 도메인을 구성하는 데 사용됩니다. 단일 도메인 배포에는 [LDAP를 통한 Active Directory]가 적합합니다. 모든 다중 도메인 및 다중 포리스트 배포에는 [Active Directory(Windows 통합 인증)]를 사용합니다.
- OpenLDAP - 오픈 소스 버전의 LDAP를 사용하여 디렉토리 관리 사용자 인증을 지원할 수 있습니다.

통신 프로토콜을 선택하고 Active Directory 링크를 구성한 후에는 Active Directory 구성과 함께 사용할 도메인을 지정한 다음 지정된 구성과 동기화할 사용자와 그룹을 선택할 수 있습니다.

LDAP/IWA를 통한 Active Directory 링크 구성

사용자 인증을 지원하기 위해 LDAP/IWA를 통한 Active Directory 링크를 구성할 수 있습니다. Directories Management 기능을 통해 Active Directory에 대한 링크를 구성하여 모든 테넌트에 대한 사용자 인증을 지원하고 Directories Management 디렉토리와 동기화할 사용자와 그룹을 선택할 수 있습니다.

디렉토리 관리와 함께 OpenLDAP를 사용하는 방법에 대한 정보와 지침은 [OpenLDAP Directory 연결 구성](#) 항목을 참조하십시오.

[Active Directory(통합 Windows 인증)]의 경우, 다중 포리스트 Active Directory를 구성했고 도메인 로컬 그룹에 서로 다른 포리스트의 도메인 구성원이 포함되었다면 도메인 로컬 그룹이 상주하는 도메인의 관리자 그룹에 Bind 사용자를 추가해야 합니다. 이렇게 하지 못하면 도메인 로컬 그룹에서 이러한 구성원이 누락됩니다.

필수 조건

- [사용자 특성] 페이지에서 필요한 기본 특성을 선택하고 추가 특성을 추가합니다. [디렉토리와의 동기화를 위해 특성 선택](#) 항목을 참조하십시오.
- Active Directory에서 동기화할 Active Directory 그룹 및 사용자의 목록.
- Active Directory가 SSL 또는 STARTTLS를 통한 액세스를 요구하는 경우 Active Directory 도메인 컨트롤러의 루트 CA 인증서가 필요합니다.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 디렉토리 관리 > 디렉토리**를 선택합니다.
- 2 **디렉토리 추가**를 클릭하고 **LDAP/IWA를 통한 Active Directory 추가**를 선택합니다.
- 3 [디렉토리 추가] 페이지의 **디렉토리 이름** 텍스트 상자에서 Active Directory 서버의 IP 주소를 지정합니다.

- 4 **디렉토리 이름** 텍스트 상자 아래의 라디오 버튼을 사용하여 적절한 Active Directory 통신 프로토콜을 선택합니다.

옵션	설명
Windows 인증	Active Directory(Windows 통합 인증) 를 선택합니다. [Active Directory(Windows 통합 인증)]의 경우 필요한 정보에는 도메인의 Bind 사용자 UPN 주소 및 암호가 포함됩니다.
LDAP	LDAP를 통한 Active Directory 를 선택합니다. [LDAP를 통한 Active Directory]의 경우 필요한 정보에는 기본 DN, Bind DN, Bind DN 암호가 포함됩니다.

- 5 디렉토리 동기화 및 인증 섹션에서 사용자를 Active Directory에서 VMware Directories Management 디렉토리로 동기화하는 커넥터를 구성합니다.

옵션	설명
동기화 커넥터	시스템에 사용할 적절한 커넥터를 선택합니다. 각 vRealize Automation 장치에는 기본 커넥터가 포함되어 있습니다. 커넥터를 선택할 때 도움이 필요한 경우 시스템 관리자에게 문의하십시오.
인증	적절한 라디오 버튼을 클릭하여 선택한 커넥터가 인증도 수행하는지 표시합니다. 타사 ID 제공자와 함께 Active Directory(통합 Windows 인증)를 사용하여 사용자를 인증하는 경우 아니요 를 클릭합니다. 사용자 및 그룹을 동기화하도록 Active Directory 연결을 구성한 후에 [ID 제공자] 페이지를 사용하여 인증을 위한 타사 ID 제공자를 추가합니다. PasswordIpdAdapter, SecurIDAdapter 및 RadiusAuthAdapter와 같은 인증 어댑터 사용에 대한 자세한 내용은 VMware Identity Manager 관리 가이드를 참조하십시오.
디렉토리 검색 특성	사용자 이름이 포함된 적절한 계정 특성을 선택합니다. userPrincipleName 대신 sAMAccount 특성을 사용하는 것이 좋습니다. 동기화 작업에 userPrincipleName을 사용하는 경우 사용자 이름이 필요한 제2 당사자 및 타사 소프트웨어와의 통합이 올바르게 작동하지 않을 수 있습니다. 참고 [서버 위치] 영역에서 이 디렉토리에 글로벌 카탈로그 있음 확인란을 선택하여 표시되는 글로벌 카탈로그를 사용할 때 sAMAccountName을 선택하면 사용자가 로그인할 수 없습니다.

- 6 [LDAP를 통한 Active Directory]를 선택한 경우에는 [서버 위치] 텍스트 상자에, [Active Directory(통합 Windows 인증)]를 선택한 경우에는 [도메인 가입 세부 정보] 텍스트 상자에 적절한 정보를 입력합니다.

옵션	설명
서버 위치 - LDAP를 통한 Active Directory가 선택된 경우 표시됨	<ul style="list-style-type: none"> ■ DNS 서비스 위치를 사용하여 Active Directory 도메인을 찾으려면, 이 디렉토리에서 DNS 서비스 위치 지원 확인란이 선택된 상태를 유지합니다. <p>참고 이 옵션을 선택하는 경우 636으로 할당된 포트를 변경할 수 없습니다.</p> <p>도메인 컨트롤러 목록이 자동으로 채워진 domain_krb.properties 파일이 디렉토리과 함께 생성됩니다. 도메인 컨트롤러 선택 정보 항목을 참조하십시오.</p> <p>Active Directory가 STARTTLS 암호화를 요구하는 경우 [인증서] 섹션에서 이 디렉토리에 대한 모든 연결은 STARTTLS를 사용해야 합니다. 확인란을 선택하고 Active Directory 루트 CA 인증서를 복사한 후 SSL 인증서 필드에 붙여넣습니다.</p> <ul style="list-style-type: none"> ■ 지정된 Active Directory에서 DNS 서비스 위치 조화를 사용하지 않는 경우 [서버 위치] 필드에서 이 디렉토리는 DNS 서비스 위치를 지원하지 않습니다. 옆의 확인란 선택을 해제하고 적절한 텍스트 상자에 Active Directory 서버 호스트 이름과 포트 번호를 입력합니다. <p>연결된 Active Directory가 글로벌 카탈로그를 사용하는 경우 이 디렉토리에 글로벌 카탈로그 있음 확인란을 선택합니다. 글로벌 카탈로그는 다중 도메인 Active Directory 포리스트의 모든 도메인에 있는 모든 개체에 대한 표현을 포함합니다.</p> <p>디렉토리를 글로벌 카탈로그로 구성하려면 Active Directory 환경에서 "다중 도메인, 단일 포리스트 Active Directory 환경" 섹션을 참조하십시오.</p> <p>Active Directory에 SSL을 통한 액세스가 필요한 경우, 인증서 제목 아래에서 SSL을 사용하기 위해 이 디렉토리에 모든 연결이 필요함 확인란을 선택하고 Active Directory SSL 인증서를 제공합니다.</p> <p>이 옵션을 선택하면 포트 636이 자동으로 사용되고 포트를 변경할 수 없습니다.</p> <p>인증서가 PEM 형식인지 확인하고 BEGIN CERTIFICATE 및 END CERTIFICATE 줄을 포함합니다.</p>
도메인 가입 세부 정보 - Active Directory(Windows 통합 인증)가 선택된 경우 표시됨	<p>도메인 이름, 도메인 관리자 이름 및 도메인 관리자 암호 텍스트 상자에 적절한 자격 증명을 입력합니다.</p> <p>Active Directory가 STARTTLS 암호화를 요구하는 경우 [인증서] 섹션에서 이 디렉토리에 대한 모든 연결은 STARTTLS를 사용해야 합니다. 확인란을 선택하고 Active Directory 루트 CA 인증서를 복사한 후 SSL 인증서 필드에 붙여넣습니다.</p> <p>인증서가 PEM 형식인지 확인하고 BEGIN CERTIFICATE 및 END CERTIFICATE 줄을 포함합니다.</p> <p>디렉토리가 여러 도메인을 사용하는 경우 모든 도메인에 대한 루트 CA 인증서를 한 번에 하나씩 추가합니다.</p> <p>참고 Active Directory가 STARTTLS를 요구하지만 사용자가 인증서를 제공하지 않으면 디렉토리를 생성할 수 없습니다.</p>

- 7 Bind 사용자 세부 정보 섹션에서 디렉토리 동기화를 원활히 수행할 수 있도록 적절한 자격 증명을 입력합니다.

[LDAP를 통한 Active Directory]의 경우:

옵션	설명
기본 DN	검색 기본 고유 이름을 입력합니다. 예를 들어 <code>cn=users,dc=corp,dc=local</code> 을 입력합니다.
Bind DN	바인딩 고유 이름을 입력합니다. 예를 들어, <code>cn=fritz infra,cn=users,dc=corp,dc=local</code>

[Active Directory(통합 Windows 인증)]의 경우:

옵션	설명
Bind 사용자 UPN	도메인을 인증할 수 있는 사용자의 사용자 계정 이름을 입력합니다. 예를 들어 <code>UserName@example.com</code> 을 입력합니다.
Bind DN 암호	[Bind 사용자] 암호를 입력합니다.

- 8 **연결 테스트**를 클릭하여 구성된 디렉토리에 대한 연결을 테스트합니다.

이 버튼은 [Active Directory(Windows 통합 인증)]를 선택한 경우 나타나지 않습니다.

- 9 **저장 및 다음**을 클릭합니다.

도메인 목록과 함께 [도메인 선택] 페이지가 나타납니다.

- 10 Active Directory 연결에 대해 나열된 도메인을 검토 및 업데이트합니다.

- [Active Directory(통합 Windows 인증)]의 경우 이 Active Directory 연결과 연결되어야 하는 도메인을 선택합니다.
- [LDAP를 통한 Active Directory]의 경우 확인 표시와 함께 사용 가능한 도메인이 나열됩니다.


참고 디렉토리가 생성된 후에 트러스팅 도메인을 추가하면 서비스에서 새 트러스팅 도메인을 자동으로 감지하지 못합니다. 서비스에서 도메인을 감지하도록 설정하려면 connector가 도메인을 탈퇴한 다음 다시 가입해야 합니다. connector가 도메인에 다시 가입하면 트러스팅 도메인이 목록에 나타납니다.

- 11 **다음**을 클릭합니다.

- 12 Directories Management 디렉토리 특성 이름이 올바른 Active Directory 특성에 매핑되어 있는지 확인합니다.

디렉토리 특성 이름이 올바르게 매핑되지 않은 경우, 드롭다운 메뉴에서 Active Directory 특성 수정을 선택합니다.

- 13 **다음**을 클릭합니다.


14 를 클릭하여 Active Directory에서 디렉토리로 동기화하려는 그룹을 선택합니다.

Active Directory에서 그룹을 추가할 때 해당 그룹의 구성원이 [사용자] 목록에 없는 경우 목록에 추가됩니다. 그룹을 동기화할 때 Active Directory에서 [도메인 사용자]가 기본 그룹으로 포함되어 있지 않은 사용자는 동기화되지 않습니다.

참고 Directories Management 사용자 인증 시스템은 그룹과 사용자를 추가할 때 Active Directory의 데이터를 가져오고 시스템의 속도는 Active Directory 기능에 의해 제한됩니다. 따라서 추가할 그룹과 사용자의 수에 따라 가져오기 작업에 상당한 시간이 걸릴 수 있습니다. 지연 또는 문제가 발생할 가능성을 최소화하려면 vRealize Automation 작업에 필요한 정도로만 그룹과 사용자의 수를 제한하십시오.


시스템 성능이 저하되거나 오류가 발생하면 불필요한 애플리케이션을 모두 닫고 Active Directory에 충분한 메모리가 할당되어 있는지 확인하십시오. 문제가 계속되면 필요한 만큼 Active Directory 메모리 할당을 늘리십시오. 많은 수의 사용자 및 그룹이 포함된 시스템의 경우 Active Directory 메모리 할당을 24GB까지 늘려야 할 수 있습니다.

15 다음을 클릭합니다.

16 추가 사용자를 추가하려면 를 클릭합니다.

적절한 값은 다음과 같습니다.

- 단일 사용자: `CN=username,CN=Users,OU=Users,DC=myCorp,DC=com`
- 여러 사용자: `OU=Users,OU=myUnit,DC=myCorp,DC=com`

사용자를 제외하려면 를 클릭하고 필터를 만들어 일부 사용자 유형을 제외합니다. 필터 기준으로 사용할 사용자 특성, 쿼리 규칙 및 값을 선택합니다.

17 다음을 클릭합니다.

18 디렉토리에 동기화되는 사용자 및 그룹의 수를 보려면 페이지를 검토합니다.

사용자 및 그룹을 변경하고 싶다면 [편집] 링크를 클릭합니다.

참고 이전에 지정된 기본 DN 아래에 있는 사용자 DN을 지정했는지 확인합니다. 사용자 DN이 기본 DN 외부에 있으면 해당 DN의 사용자가 동기화되지만 로그인할 수는 없습니다.

19 작업 공간으로 푸시를 클릭하여 디렉토리에 대한 동기화를 시작합니다.

Active Directory에 대한 연결이 완료되고 선택된 사용자와 그룹이 디렉토리에 추가됩니다. 이제는 **관리 > 사용자 및 그룹 > 디렉토리 사용자 및 그룹**을 선택하여 사용자와 그룹을 알맞은 vRealize Automation 역할에 할당할 수 있습니다. 자세한 내용은 [디렉토리 사용자 또는 그룹에 역할 할당](#)를 참조하십시오.

후속 작업

고가용성을 위해 vRealize Automation 환경이 구성된 경우, 고가용성을 위한 특정 디렉토리 관리를 구성해야 합니다. [고가용성을 위해 디렉토리 관리 구성](#) 항목을 참조하십시오.

- 인증 방법을 설정합니다. 사용자 및 그룹의 디렉토리 동기화 후에, 커넥터도 인증에 사용되는 경우 커넥터에서 추가 인증 방법을 설정할 수 있습니다. 타사가 인증 ID 제공자인 경우 커넥터에서 해당 ID 제공자를 구성합니다.
- 기본 액세스 정책을 검토합니다. 기본 액세스 정책은 전체 네트워크 범위의 모든 장치가 8시간의 세션 시간 초과 설정으로 웹 브라우저에 액세스하거나 2160시간(90일)의 세션 시간 초과 설정으로 클라이언트 애플리케이션에 액세스할 수 있도록 구성되어 있습니다. 기본 액세스 정책을 변경할 수 있으며 웹 애플리케이션을 카탈로그에 추가할 때 새 정책을 생성할 수 있습니다.
- 사용자 지정 브랜딩을 관리 콘솔, 사용자 포털 페이지 및 로그인 화면에 적용합니다.

OpenLDAP Directory 연결 구성

디렉토리 관리로 OpenLDAP Directory 연결을 구성할 수 있습니다.

여러 가지 다른 LDAP 프로토콜이 있지만, OpenLDAP가 vRealize Automation 디렉토리 관리와 함께 사용하도록 테스트와 승인 과정을 거친 유일한 프로토콜입니다.

LDAP 디렉토리를 통합하려면 해당 Directories Management 디렉토리를 만들고 LDAP 디렉토리에서 Directories Management 디렉토리로 사용자 및 그룹을 동기화합니다. 후속 업데이트에 대한 정기 동기화 스케줄을 설정할 수 있습니다.

또한 사용자에 대해 동기화할 LDAP 특성을 선택하여 Directories Management 특성에 매핑합니다.

LDAP 디렉토리 구성은 기본 스키마 또는 사용자 지정 스키마를 기반으로 할 수 있습니다. 또한 사용자 지정 특성을 정의할 수도 있습니다. Directories Management에서 사용자 또는 그룹 개체를 가져오기 위해 LDAP 디렉토리를 쿼리할 수 있도록 하려면 LDAP 디렉토리에 적용되는 LDAP 검색 필터 및 특성 이름을 제공해야 합니다.

특히 다음 정보를 제공해야 합니다.

- 그룹, 사용자 및 바인딩 사용자를 가져오기 위한 LDAP 검색 필터
- 그룹 멤버 자격, UUID 및 고유 이름에 대한 LDAP 특성 이름

필수 조건

- [사용자 특성] 페이지에서 구성을 검토하고 동기화할 다른 특성을 추가합니다. 디렉토리를 만들 때 Directories Management 특성을 LDAP 디렉토리 특성에 매핑합니다. 이러한 특성은 디렉토리의 사용자에 대해 동기화됩니다.

참고 사용자 특성을 변경할 경우 서비스의 다른 디렉토리에 대한 영향을 고려하십시오. Active Directory와 LDAP 디렉토리를 둘 다 추가하려면 **userName** 외에는 어떤 특성도 필수로 표시해서는 안 됩니다. [사용자 특성] 페이지의 설정은 서비스의 모든 디렉토리에 적용됩니다. 특성이 필수로 표시된 경우 해당 특성이 없는 사용자는 Directories Management 서비스에 동기화되지 않습니다.

- 바인딩 DN 사용자 계정. 만료되지 않는 암호를 사용하는 바인딩 DN 사용자 계정을 사용하는 것이 좋습니다.
- LDAP 디렉토리에서 사용자 및 그룹의 UUID는 일반 텍스트 형식이어야 합니다.
- LDAP 디렉토리에서 도메인 특성은 모든 사용자 및 그룹에 대해 존재해야 합니다.

Directories Management 디렉토리를 만들 때 이 특성을 Directories Management **도메인** 특성에 매핑합니다.

- 사용자 이름에 공백이 포함되어서는 안 됩니다. 사용자 이름에 공백이 포함된 경우 사용자는 동기화되지만 해당 사용자에게 사용 권한이 제공되지 않습니다.
- 인증서 인증을 사용하는 경우 사용자에게 userPrincipalName 및 이메일 주소 특성 값이 있어야 합니다.

프로시저

- 1 **관리 > 디렉토리 관리 > 디렉토리**를 선택합니다.
- 2 **디렉토리 추가**를 클릭하고 **LDAP 디렉토리 추가**를 선택합니다.
- 3 [LDAP 디렉토리 추가] 페이지에서 필요한 정보를 입력합니다.

옵션	설명
디렉토리 이름	Directories Management 디렉토리의 이름을 입력합니다.
디렉토리 동기화 및 인증	<p>a 동기화 커넥터 필드에서 LDAP 디렉토리의 사용자 및 그룹을 Directories Management 디렉토리에 동기화하는 데 사용할 커넥터를 선택합니다.</p> <p>커넥터 구성 요소는 기본적으로 Directories Management 서비스에서 항상 사용 가능합니다. 이 커넥터는 드롭다운 목록에 표시됩니다. 고가용성을 위해 여러 개의 Directories Management 장치를 설치하는 경우 각 장치의 커넥터 구성 요소가 목록에 나타납니다.</p> <p>LDAP 디렉토리용 커넥터가 별도로 필요하지 않습니다. Active Directory든 LDAP 디렉토리든 상관없이 하나의 커넥터가 여러 디렉토리를 지원할 수 있습니다.</p> <p>b 인증 필드에서 이 LDAP 디렉토리를 사용하여 사용자를 인증하려는 경우 예를 선택합니다.</p> <p>사용자를 인증하는 데 타사 ID 제공자를 사용하려면 아니요를 선택합니다. 사용자 및 그룹을 동기화하도록 디렉토리 연결을 추가한 후에는 관리 > 디렉토리 관리 > ID 제공자 페이지로 이동하여 인증을 위한 타사 ID 제공자를 추가합니다.</p> <p>c 대부분의 구성에서는 디렉토리 검색 특성 텍스트 상자에 선택되어 있는 사용자 지정 기본값을 그대로 둡니다. 사용자 지정 디렉토리 검색 특성 필드에서 사용자 및 그룹 이름에 사용할 LDAP 디렉토리 특성을 지정합니다. 이 특성은 LDAP 서버에서 사용자와 그룹 같은 엔티티를 고유하게 식별합니다. 예를 들어 cn를 입력합니다.</p>
서버 위치	<p>LDAP 디렉토리 서버 호스트 및 포트 번호를 입력합니다. 서버 호스트의 경우 정규화된 도메인 이름 또는 IP 주소를 지정할 수 있습니다. 예를 들어 myLDAPserver.example.com 또는 100.00.00.0을 지정할 수 있습니다.</p> <p>로드 밸런서 뒤에 서버 클러스터가 있는 경우 대신 로드 밸런서 정보를 입력합니다.</p>

옵션	설명
LDAP 구성	<p>Directories Management에서 LDAP 디렉토리를 쿼리하는 데 사용할 수 있는 LDAP 검색 필터 및 특성을 지정합니다. 기본값은 코어 LDAP 스키마에 따라 제공됩니다.</p> <p>쿼리 필터</p> <ul style="list-style-type: none"> ■ 그룹: 그룹 개체를 가져오기 위한 검색 필터입니다. 예: <code>(objectClass=group)</code> ■ 바인딩 사용자: 바인딩 사용자 개체, 즉 디렉토리에 바인딩할 수 있는 사용자를 가져오기 위한 검색 필터입니다. 예: <code>(objectClass=person)</code> ■ 사용자: 동기화할 사용자를 가져오기 위한 검색 필터입니다. 예: <code>(&(objectClass=user)(objectCategory=person))</code> <p>특성</p> <ul style="list-style-type: none"> ■ 멤버 자격: LDAP 디렉토리에서 그룹 멤버를 정의하는 데 사용되는 특성입니다. 예: <code>member</code> ■ 개체 UUID: LDAP 디렉토리에서 사용자 또는 그룹의 UUID를 정의하는 데 사용되는 특성입니다. 예: <code>entryUUID</code> ■ 고유 이름: LDAP 디렉토리에서 사용자 또는 그룹의 고유 이름에 사용되는 특성입니다. 예: <code>entryDN</code>
인증서	<p>LDAP 디렉토리에 SSL을 통한 액세스가 필요한 경우 이 디렉토리에 대한 모든 연결은 SSL을 사용해야 합니다. 확인란을 선택합니다. 그런 다음, LDAP 디렉토리 서버의 루트 CA SSL 인증서를 복사하여 SSL 인증서 텍스트 상자에 붙여 넣습니다. 인증서가 PEM 형식인지 확인하고 "BEGIN CERTIFICATE" 및 "END CERTIFICATE" 줄을 포함합니다.</p> <p>마지막으로, 이 페이지의 [서버 위치] 섹션에 있는 서버 포트 필드에 정확한 포트 번호가 지정되어 있는지 확인합니다.</p>
Bind 사용자 세부 정보	<p>기본 DN: 검색을 시작할 DN을 입력합니다. 예: <code>cn=users,dc=example,dc=com</code></p> <p>해당되는 모든 사용자는 [기본 DN] 아래 상주해야 합니다. [기본 DN] 아래에 특정 사용자가 없을 경우 그 사용자가 [기본 DN] 아래에 있는 그룹의 구성원일지라도 로그인할 수 없습니다.</p> <p>Bind DN: LDAP 디렉토리에 바인딩하는 데 사용할 DN을 입력합니다. 사용자 이름을 입력할 수도 있지만, 대부분의 배포에는 DN을 입력하는 것이 더 적절합니다.</p> <p>참고 만료되지 않는 암호를 가진 Bind DN 사용자 계정을 사용하는 것이 좋습니다.</p> <p>바인딩 DN 암호: 바인딩 DN 사용자의 암호를 입력합니다.</p>

- LDAP 디렉토리 서버에 대한 연결을 테스트하려면 **연결 테스트**를 클릭합니다.
연결에 실패한 경우 입력한 정보를 확인하고 적절히 변경합니다.
- 저장 및 다음**을 클릭합니다.
- [도메인 선택] 페이지에 올바른 도메인이 선택되어 있는지 확인한 후 **다음**을 클릭합니다.

- 7 [특성 매핑] 페이지에서 Directories Management 특성이 올바른 LDAP 특성에 매핑되어 있는지 확인합니다.

이러한 특성은 사용자에게 동기화됩니다.

중요 도메인 특성에 대한 매핑을 지정해야 합니다.

[사용자 특성] 페이지에서 목록에 특성을 추가할 수 있습니다.

- 8 다음을 클릭합니다.

- 9 [동기화할 그룹(사용자) 선택] 페이지에서 +를 클릭하여 LDAP 디렉토리에서 Directories Management 디렉토리로 동기화하려는 그룹을 선택합니다.

LDAP 디렉토리에 이름이 같은 그룹이 여러 개 있는 경우 그룹 페이지에서 해당 그룹에 대한 고유 이름을 지정해야 합니다.

Active Directory에서 그룹을 추가할 때 해당 그룹의 구성원이 [사용자] 목록에 없는 경우 목록에 추가됩니다. 그룹을 동기화할 때 Active Directory에서 [도메인 사용자]가 기본 그룹으로 포함되어 있지 않은 사용자는 동기화되지 않습니다.

중첩된 그룹 구성원 동기화 옵션이 기본적으로 사용되도록 설정되어 있습니다. 이 옵션이 사용되도록 설정되면 선택한 그룹에 직접 속하는 모든 사용자와 그 아래 중첩된 그룹에 속하는 모든 사용자가 동기화됩니다. 중첩된 그룹은 동기화되지 않고 중첩된 그룹에 속하는 사용자만 동기화됩니다. Directories Management 디렉토리에서 이러한 사용자는 동기화를 위해 선택한 최상위 그룹의 구성원으로 나타납니다. 실제로 선택한 그룹 아래의 계층은 평면화되며 모든 수준의 사용자가 선택한 그룹의 멤버로 Directories Management에 표시됩니다.

이 옵션을 사용하지 않도록 설정하면 동기화할 그룹을 지정할 때 해당 그룹에 직접 속하는 모든 사용자가 동기화됩니다. 그 아래 중첩된 그룹에 속하는 사용자는 동기화되지 않습니다. 그룹 트리를 탐색하는 데 리소스와 시간이 많이 소요되는 대규모 디렉토리 구성의 경우 이 옵션을 사용하지 않도록 설정하는 것이 좋습니다. 이 옵션을 사용하지 않도록 설정하는 경우 동기화할 사용자가 속하는 모든 그룹을 선택해야 합니다.

참고 Directories Management 사용자 인증 시스템은 그룹과 사용자를 추가할 때 Active Directory의 데이터를 가져오고 시스템의 속도는 Active Directory 기능에 의해 제한됩니다. 따라서 추가할 그룹과 사용자의 수에 따라 가져오기 작업에 상당한 시간이 걸릴 수 있습니다. 지연 또는 문제가 발생할 가능성을 최소화하려면 vRealize Automation 작업에 필요한 정도로만 그룹과 사용자의 수를 제한하십시오.

시스템 성능이 저하되거나 오류가 발생하면 불필요한 애플리케이션을 모두 닫고 디렉토리 관리에 충분한 메모리가 할당되어 있는지 확인하십시오. 문제가 계속되면 필요한 만큼 디렉토리 관리 메모리 할당을 늘리십시오. 많은 수의 사용자 및 그룹이 포함된 시스템의 경우 디렉토리 관리 메모리 할당을 24GB까지 늘려야 할 수 있습니다.

- 10 다음을 클릭합니다.

11 사용자를 더 추가하려면 + 를 클릭합니다. 예를 들어

CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com을 입력합니다.

여기에 개별 사용자는 물론이고, 조직 구성 단위도 추가할 수 있습니다.

일부 사용자 유형을 제외하도록 필터를 생성할 수 있습니다. 필터 기준으로 사용할 사용자 특성, 쿼리 규칙 및 값을 선택합니다.

12 다음을 클릭합니다.

13 페이지를 검토하여 디렉토리에 동기화되는 사용자 및 그룹의 수를 확인하고 기본 동기화 스케줄을 확인합니다.

사용자 및 그룹을 변경하거나 동기화 빈도를 변경하려면 **편집** 링크를 클릭합니다.

14 디렉토리 동기화를 클릭하여 디렉토리 동기화를 시작합니다.

LDAP 디렉토리 연결이 설정되고 사용자 및 그룹이 LDAP 디렉토리에서 Directories Management 디렉토리로 동기화됩니다.

이제는 **관리 > 사용자 및 그룹 > 디렉토리 사용자 및 그룹**을 선택하여 사용자와 그룹을 알맞은 vRealize Automation 역할에 할당할 수 있습니다. 자세한 내용은 [디렉토리 사용자 또는 그룹에 역할 할당](#)를 참조하십시오.

LDAP 디렉토리 통합의 제한 사항

디렉토리 관리에는 LDAP 디렉토리 통합과 관련된 몇 가지 중요한 제한 사항이 있습니다.

- 단일 도메인 LDAP 디렉토리 환경만 통합할 수 있습니다.
LDAP 디렉토리에서 여러 도메인을 통합하려면 각 도메인에 하나씩 추가 Directories Management 디렉토리를 만들어야 합니다.
- 다음 인증 방법은 LDAP 디렉토리 유형의 Directories Management 디렉토리에 지원되지 않습니다.
 - Kerberos 인증
 - RSA 적응 인증
 - 타사 ID 제공자로서의 ADFS
 - SecurlD
 - Vasco 및 SMS 암호 서버를 통한 Radius 인증
- LDAP 도메인을 가입시킬 수 없습니다.
- View 또는 Citrix 게시된 리소스와의 통합은 LDAP 디렉토리 유형의 Directories Management 디렉토리에 지원되지 않습니다.
- 사용자 이름에 공백이 포함되어서는 안 됩니다. 사용자 이름에 공백이 포함된 경우 사용자는 동기화되지만 해당 사용자에게 사용 권한이 제공되지 않습니다.

- Active Directory와 LDAP 디렉토리를 둘 다 추가하려면 필수로 표시될 수 있는 userName 외에는 [사용자 특성] 페이지에서 어떤 특성도 필수로 표시해서는 안 됩니다. [사용자 특성] 페이지의 설정은 서비스의 모든 디렉토리에 적용됩니다. 특성이 필수로 표시된 경우 해당 특성이 없는 사용자는 Directories Management 서비스에 동기화되지 않습니다.
- LDAP 디렉토리에 이름이 같은 여러 그룹이 있는 경우 Directories Management 서비스에서 해당 그룹에 대한 고유 이름을 지정해야 합니다. 동기화할 그룹을 선택할 때 이름을 지정할 수 있습니다.
- 사용자가 만료된 암호를 재설정하도록 허용하는 옵션은 사용할 수 없습니다.
- domain_krb.properties 파일은 지원되지 않습니다.

고가용성을 위해 디렉토리 관리 구성

디렉토리 관리를 사용하여 vRealize Automation에서 고가용성 Active Directory 연결을 구성할 수 있습니다.

각 vRealize Automation 장치에는 사용자 인증을 지원하는 커넥터가 포함되어 있지만 일반적으로 디렉토리 동기화를 수행하기 위한 단 하나의 커넥터만 구성되어 있습니다. 어떤 커넥터를 선택하여 동기화 커넥터로 사용하든 상관 없습니다. 디렉토리 관리 고가용성을 지원하려면 두 번째 vRealize Automation 장치에 해당하는 두 번째 커넥터를 구성해야 합니다. 이것은 ID 제공자에 연결하고 동일한 Active Directory를 가리킵니다. 이 구성을 사용하면 하나의 장치가 실패하는 경우 다른 장치가 사용자 인증 관리를 담당합니다.

고가용성 환경에서 모든 노드는 동일한 Active Directory 집합, 사용자, 인증 방법 등을 제공해야 합니다. 이러한 작업을 성공적으로 수행할 수 있는 가장 직접적인 방법은 로드 밸런서 호스트를 ID 제공자 호스트로 설정하여 ID 제공자를 클러스터로 승격시키는 것입니다. 이 구성을 사용하면 모든 인증 요청이 로드 밸런서로 전송되고 로드 밸런서는 요청을 두 커넥터 중 하나로 적절하게 전달합니다.

필수 조건

- 최소 2개의 vRealize Automation 장치 인스턴스로 vRealize Automation 배포를 구성합니다.
- 2개의 vRealize Automation 장치 인스턴스와 함께 단일 도메인에서 작동하는 [엔터프라이즈] 모드로 vRealize Automation을 설치합니다.
- vRealize Automation 배포와 함께 작업하도록 적절한 로드 밸런서를 설치하고 구성합니다.
- 설치된 vRealize Automation 장치 인스턴스와 함께 제공된 커넥터 중 하나를 사용하여 테넌트와 디렉토리 관리를 구성합니다. 테넌트 구성에 대한 자세한 내용은 [테넌트 설정 구성](#) 항목을 참조하십시오.

프로시저

- 1 vRealize Automation 배포의 로드 밸런서에 테넌트 관리자로 로그인합니다.
로드 밸런서 URL은 <로드 밸런서 주소>/vcac/org/tenant_name입니다.
- 2 **관리 > 디렉토리 관리 > ID 제공자**를 선택합니다.

3 현재 시스템에서 사용 중인 ID 제공자를 클릭합니다.

시스템을 위해 기본적인 ID 관리를 제공하는 기존의 디렉토리 및 커넥터가 나타납니다.

4 [ID 제공자 속성] 페이지에서 **커넥터 추가** 드롭다운 목록을 클릭하고 보조 vRealize Automation 장치에 해당하는 커넥터를 선택합니다.

5 커넥터를 선택할 때 나타나는 **Bind DN 암호** 텍스트 상자에 적절한 암호를 입력합니다.

6 커넥터 추가를 클릭합니다.

7 기본적으로 기본 커넥터가 **IdP 호스트 이름** 텍스트 상자에 나타납니다. 로드 밸런서를 가리키도록 호스트 이름을 변경합니다.

vRealize Automation 과 Active Directory 간 양방향 신뢰 관계 구성

ID 제공자와 Active Directory Federated Services 사이의 양방향 신뢰 관계를 구성하여 기본 vRealize Automation Active Directory 연결의 시스템 보안을 향상시킬 수 있습니다.

vRealize Automation과 Active Directory 간에 양방향 신뢰 관계를 구성하려면 사용자 지정 ID 제공자를 생성하고 Active Directory 메타데이터를 이 제공자에 추가해야 합니다. 또한 vRealize Automation 배포에서 사용하는 기본 정책을 수정해야 합니다. 마지막으로 ID 제공자를 인식하도록 Active Directory를 구성해야 합니다.

필수 조건

- vRealize Automation 배포를 위한 테넌트를 구성했고 기본 Active Directory 사용자 ID 및 암호 인증을 지원하도록 적절한 Active Directory 링크를 설정했는지 확인합니다.
- 네트워크에서 사용할 Active Directory를 설치하고 구성합니다.
- 적절한 ADFS(Active Directory Federated Services) 메타데이터를 가져옵니다.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 페더레이션 메타데이터 파일을 가져옵니다.

이 파일은

`https://servername.domain/FederationMetadata/2007-06/FederationMetadata.xml`에서 다운로드할 수 있습니다.

2 logout이라는 단어를 찾아 `https://servername.domain/adfs/ls/logout.aspx`를 가리키도록 각 인스턴스의 위치를 편집합니다.

예를 들어, 다음:

```
SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://servername.domain/adfs/ls/ "/>
```

위의 내용을 다음과 같이 변경해야 합니다.

```
SingleLogoutService
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://servername.domain/adfs/ls/logout.aspx"/>
```

3 배포를 위한 새 ID 제공자를 생성합니다.

- a **관리 > 디렉토리 관리 > ID 제공자**를 선택합니다.
- b **ID 제공자 추가**를 클릭하여 필드를 적절하게 완료합니다.

옵션	설명
ID 제공자 이름	새 ID 제공자 이름 입력
ID 제공자 메타데이터(URI 또는 XML)	Active Directory Federated Services 메타데이터 파일의 콘텐츠를 여기에 붙여넣습니다.
SAML 요청의 ID 정책 이름 지정(선택 사항)	적절한 경우 ID 정책 SAML 요청의 이름을 입력합니다.
사용자	사용자가 액세스 권한을 갖게 하려는 도메인을 선택합니다.
IDP 메타데이터 처리	추가한 메타데이터 파일을 클릭하여 처리합니다.
네트워크	사용자가 액세스 권한을 갖게 하려는 네트워크 범위를 선택합니다.
인증 방법	이 ID 제공자에 의해 사용된 인증 방법의 이름을 입력합니다.
SAML 컨텍스트	시스템에 적합한 컨텍스트를 선택합니다.
SAML 서명 인증서	디렉토리 관리 메타데이터를 다운로드하려면 SAML 메타데이터 머리글 옆의 링크를 클릭합니다.

- c 디렉토리 관리 메타데이터 파일을 sp.xml로 저장합니다.
- d **추가**를 클릭합니다.

4 기본 정책에 규칙을 추가합니다.

- a **관리 > 디렉토리 관리 > 정책**을 선택합니다.
- b 기본 정책 이름을 클릭합니다.
- c **정책 규칙** 머리글 아래에서 **+** 아이콘을 클릭하여 새 규칙을 추가합니다.

특정 네트워크 범위 및 디바이스에 사용할 적절한 기본 인증과 보조 인증을 지정하는 규칙을 생성하려면 [정책 규칙 추가] 페이지의 필드를 사용합니다.

예를 들어 네트워크 범위가 **내 시스템**이고 **모든 디바이스 유형**의 콘텐츠에 액세스해야 한다면 일반 배포의 경우 **ADFS 사용자 이름 및 암호** 방법을 사용하여 인증해야 합니다.

- d **저장**을 클릭하여 정책 업데이트를 저장합니다.
- e 기본 정책 페이지에서 새 규칙을 테이블 맨 위로 끌어 이 규칙이 기존 규칙에 우선하도록 지정합니다.

- 5 ADFS(Active Directory Federated Services) 관리 콘솔 또는 다른 적절한 도구를 사용하여 관련 당사자와 vRealize Automation ID 제공자 간 신뢰 관계를 설정합니다.

이러한 신뢰를 설정하려면 이전에 다운로드한 디렉토리 관리 메타데이터를 가져와야 합니다. 양방향 신뢰 관계를 위한 ADFS(Active Directory Federated Services) 구성에 관한 자세한 내용은 Microsoft Active Directory 설명서를 참조하십시오. 이러한 프로세스의 일부로 다음을 수행해야 합니다.

- 관련 당사자의 신뢰를 설정합니다. 이러한 신뢰를 설정하려면 복사 및 저장한 VMware ID 제공자 서비스 제공자 메타데이터 XML 파일을 가져와야 합니다.
- 특성 가져오기 규칙의 LDAP에서 검색된 특성을 원하는 SAML 형식으로 변환하는 할당 규칙을 생성합니다. 규칙을 생성한 후에는 다음 텍스트를 추가하여 규칙을 편집합니다.

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"vmwareidentity.domain.com");
```

Directories Management 및 SSO2 간 SAML 페더레이션 구성

vRealize Automation Directories Management와 SSO2를 사용하는 시스템 간에 SAML 페더레이션을 구성하여 Single Sign-On을 지원할 수 있습니다.

두 당사자 간에 SAML 연결을 생성하여 Directories Management 및 SSO2 간 페더레이션을 설정합니다. 현재 지원되는 유일한 종단 간 흐름은 SSO2가 ID 제공자(IdP) 역할을, Directories Management가 서비스 제공자(SP) 역할을 하는 것입니다.

SSO2 사용자 인증의 경우 Directories Management 및 SSO2에 동일한 계정이 존재해야 합니다. 최소한 사용자의 UPN(사용자 계정 이름)이 양쪽 끝에서 일치해야 합니다. 다른 특성은 SAML 제목을 식별하는 데 필요하기 때문에 다를 수 있습니다.

admin@vsphere.local과 같은 SSO2의 로컬 사용자인 경우, 해당하는 계정이 Directories Management에도 존재해야 합니다(여기서 최소한 사용자의 UPN이 일치해야 함). Directories Management 로컬 사용자 생성 API를 사용하여 수동으로 또는 스크립트로 이러한 계정을 생성합니다.

SSO2 및 Directories Management 간 SAML 설정에는 디렉토리 관리와 SSO 구성 요소에 대한 구성이 포함됩니다.

표 2-4. SAML 페더레이션 구성 요소 구성

구성 요소	구성
디렉토리 관리	SSO2를 Directories Management의 타사 ID 제공자로 구성하고 기본 인증 정책을 업데이트합니다. 자동화된 스크립트를 생성하여 Directories Management를 설정할 수 있습니다.
SSO2 구성 요소	Directories Management sp.xml 파일을 가져와서 Directories Management를 서비스 제공자로 구성합니다. 이 파일을 사용하면 Directories Management를 SP(서비스 제공자)로 사용하도록 SSO2를 구성할 수 있습니다.

필수 조건

- vRealize Automation 배포를 위한 테넌트를 구성합니다. [추가 테넌트 생성](#) 항목을 참조하십시오.
- 적절한 Active Directory 링크를 설정하여 기본 Active Directory 사용자 ID 및 암호 인증을 지원합니다.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 SSO2 사용자 인터페이스를 통해 SSO2 ID 제공자 메타데이터를 다운로드합니다.
 - a <https://<cloudvm-hostname>/>에서 관리자로 vCenter에 로그인합니다.
 - b **vSphere Web Client에 로그인** 링크를 클릭합니다.
 - c 왼쪽 탐색 창에서 **관리 > Single Sign-On > 구성**을 선택합니다.
 - d SAML 서비스 제공자 머리글 메타데이터에 인접한 위치에서 **다운로드**를 클릭합니다.
vsphere.local.xml 파일의 다운로드가 시작됩니다.
 - e vsphere.local.xml 파일의 콘텐츠를 복사합니다.
- 2 [vRealize Automation 디렉토리 관리 ID 제공자] 페이지에서 새 ID 제공자를 생성합니다.
 - a **테넌트 관리자**로 vRealize Automation에 로그인합니다.
 - b **관리 > 디렉토리 관리 > ID 제공자**를 선택합니다.
 - c **ID 제공자 추가**를 클릭하고 구성 정보를 제공합니다.

옵션	작업
ID 제공자 이름	새 ID 제공자의 이름을 입력합니다.
ID 제공자 메타데이터(URI 또는 XML) 텍스트 상자	SSO2 idp.xml 메타데이터 파일의 콘텐츠를 텍스트 상자에 붙여 넣고 IDP 메타데이터 처리 를 클릭합니다.
SAML 요청의 ID 정책 이름 지정(선택 사항)	http://schemas.xmlsoap.org/claims/UPN 을(를) 입력합니다.
사용자	사용자가 액세스 권한을 갖게 하려는 도메인을 선택합니다.
네트워크	액세스 권한을 갖게 하려는 사용자의 네트워크 범위를 선택합니다. 모든 IP 주소의 사용자를 인증하려면 모든 범위 를 선택합니다.
인증 방법	인증 방법의 이름을 입력합니다. 그런 다음 오른쪽의 SAML 컨텍스트 드롭 다운 메뉴를 사용하여 인증 방법을 <code>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</code> 에 매핑합니다.
SAML 서명 인증서	디렉토리 관리 메타데이터를 다운로드하려면 SAML 메타데이터 머리글 옆의 링크를 클릭합니다.

- d 디렉토리 관리 메타데이터 파일을 sp.xml로 저장합니다.
- e **추가**를 클릭합니다.

- 3 [디렉토리 관리 정책] 페이지를 사용하여 관련 인증 정책을 업데이트하고 타사 SSO2 ID 제공자로 인증을 리디렉션합니다.
 - a **관리 > 디렉토리 관리 > 정책**을 선택합니다.
 - b 기본 정책 이름을 클릭합니다.
 - c 기존 인증 규칙을 편집하려면 **정책 규칙** 머리글 아래에서 인증 방법을 클릭합니다.
 - d [정책 규칙 편집] 페이지에서 인증 방법을 암호에서 적절한 방법으로 변경합니다.
이 경우 인증 방법은 SSO2가 됩니다.
 - e **저장**을 클릭하여 정책 업데이트를 저장합니다.
- 4 왼쪽 탐색 창에서 **관리 > Single Sign-On > 구성**을 선택하고 **업데이트**를 클릭하여 sp.xml 파일을 vSphere에 업로드합니다.

Active Directory 연결에 사용자 또는 그룹 추가

기존 Active Directory 연결에 사용자 또는 그룹을 추가할 수 있습니다.

디렉토리 관리 사용자 인증 시스템은 그룹 및 사용자를 추가할 때 Active Directory에서 데이터를 가져옵니다. 데이터 전송 속도는 Active Directory 기능에 의해 제한됩니다. 따라서 추가되는 그룹 및 사용자 수에 따라 작업에 오랜 시간이 소요될 수 있습니다. 문제를 최소화하려면 그룹 및 사용자를 vRealize Automation 작업에 필요한 그룹 및 사용자로만 제한합니다. 문제가 발생하면 불필요한 애플리케이션을 닫고 배포에 Active Directory에 할당된 적절한 메모리가 있는지 확인합니다. 문제가 계속되면 Active Directory 메모리 할당을 늘립니다. 사용자 및 그룹 수가 많은 배포의 경우, Active Directory 메모리 할당을 24GB 정도까지 늘려야 할 수도 있습니다.

vRealize Automation 배포를 많은 사용자 및 그룹과 동기화할 때 로그 세부 정보를 사용할 수 있을 때까지 지연이 있을 수 있습니다. 로그 파일의 타임 스탬프는 콘솔에 표시된 완료된 시간과 다를 수 있습니다.

그룹 구성원이 [사용자] 목록에 없는 경우 Active Directory의 그룹을 추가하면 구성원이 목록에 추가됩니다. 그룹을 동기화할 때 Active Directory에서 [도메인 사용자]가 기본 그룹으로 포함되어 있지 않은 사용자는 동기화되지 않습니다.

참고 동기화 작업은 시작한 이후에 취소할 수 없습니다.

필수 조건

- Connector를 설치하고 활성화 코드를 활성화합니다. [사용자 특성] 페이지에서 필요한 기본 특성을 선택하고 추가 특성을 추가합니다.
vRealize Automation 구성에서 디렉토리와의 동기화를 위해 특성 선택 항목을 참조하십시오.
- Active Directory에서 동기화할 Active Directory 그룹 및 사용자의 목록.
- [LDAP를 통한 Active Directory]의 경우 필요한 정보에는 기본 DN, Bind DN, Bind DN 암호가 포함됩니다.
- [Active Directory(Windows 통합 인증)]의 경우 필요한 정보에는 도메인의 Bind 사용자 UPN 주소 및 암호가 포함됩니다.

- SSL을 통해 Active Directory에 액세스하는 경우에는 SSL 인증서의 사본이 필요합니다.
- Windows 인증과 통합된 다중 포리스트 Active Directory가 있으며 도메인 로컬 그룹에 다른 포리스트의 구성원이 포함되어 있는 경우 다음을 수행합니다. Bind 사용자를 도메인 로컬 그룹의 관리자 그룹에 추가합니다. Bind 사용자가 추가되지 않으면 이러한 구성원은 도메인 로컬 그룹에서 누락됩니다.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 디렉토리 관리 > 디렉토리**를 선택합니다.
- 2 원하는 디렉토리 이름을 클릭합니다.
- 3 **동기화 설정**을 클릭하여 동기화 옵션이 포함된 대화 상자를 엽니다.
- 4 사용자 또는 그룹 구성을 변경할지 여부에 따라 적합한 아이콘을 클릭합니다.

그룹 구성을 편집하려면:

- 그룹을 추가하려면 **+** 아이콘을 클릭하여 그룹 DN 정의에 대한 줄을 추가하고 적합한 그룹 DN을 입력합니다.
- 그룹 DN 정의를 삭제하려면 원하는 그룹 DN에 대한 **x** 아이콘을 클릭합니다.

사용자 구성을 편집하려면:

- ◆ 사용자를 추가하려면 **+** 아이콘을 클릭하여 사용자 DN 정의에 대한 줄을 추가하고 적합한 사용자 DN을 입력합니다.

사용자 DN 정의를 삭제하려면 원하는 사용자 DN에 대한 **x** 아이콘을 클릭합니다.

- 5 **저장**을 클릭하여 업데이트를 즉시 동기화하지 않고 변경 내용을 저장합니다. **저장 및 동기화**를 클릭하여 변경 내용을 저장하고 업데이트를 즉시 동기화합니다.

디렉토리와의 동기화를 위해 특성 선택

Active Directory와의 동기화를 위해 Directories Management 디렉토리를 설정하는 경우 디렉토리로 동기화되는 사용자 특성을 지정합니다. 디렉토리를 설정하기 전에 [사용자 특성] 페이지에서 필요한 기본 특성을 지정하고, 원하는 경우 Active Directory 특성으로 매핑하려는 추가 특성을 추가할 수 있습니다.

디렉토리가 생성되기 전에 [사용자 특성] 페이지를 구성한 경우 기본 특성을 필수에서 필수 아님으로 변경하거나, 특성을 필수로 표시하거나, 사용자 지정 특성을 추가할 수 있습니다.

매핑되는 기본 특성에 대한 목록은 [Active Directory에서 동기화하는 사용자 특성 관리](#) 항목을 참조하십시오.

디렉토리가 생성되면 필수 특성을 필수 아님으로 변경하고 사용자 지정 특성을 삭제할 수 있습니다. 특성을 필수 특성으로 변경할 수는 없습니다.

디렉토리에 동기화할 다른 특성을 추가한 경우 디렉토리가 생성된 후 디렉토리의 [매핑된 특성] 페이지로 이동하여 해당 특성을 Active Directory 특성에 매핑합니다.

프로시저

- 1 vRealize Automation에 시스템 또는 테넌트 관리자로 로그인합니다.
- 2 [관리] 탭을 클릭합니다.
- 3 **디렉토리 관리 > 사용자 특성**을 선택합니다.
- 4 [기본 특성] 섹션에서 필수 특성 목록을 검토하고 필수로 지정해야 하는 특성을 반영하도록 적절하게 변경합니다.
- 5 [특성] 섹션에서 Directories Management 디렉토리 특성 이름을 목록에 추가합니다.
- 6 **저장**을 클릭합니다.
기본 특성 상태가 업데이트되고 추가한 특성이 디렉토리의 [매핑된 특성] 목록에 추가됩니다.
- 7 디렉토리가 생성되었으면 [ID 저장소] 페이지로 이동하고 디렉토리를 선택합니다.
- 8 **동기화 설정 > 매핑된 특성**을 클릭합니다.
- 9 추가한 특성에 대한 드롭다운 메뉴에서 매핑할 Active Directory 특성을 선택합니다.
- 10 **저장**을 클릭합니다.

다음에 디렉토리가 Active Directory로 동기화될 때 디렉토리가 업데이트됩니다.

디렉토리 관리에 메모리 추가

많은 수의 사용자 또는 그룹을 포함하는 Active Directory 연결이 있는 경우 Directories Management에 추가 메모리를 할당해야 할 수 있습니다.

기본적으로 Directories Management 서비스에는 4GB의 메모리가 할당됩니다. 이것은 여러 개의 중소 규모 배포에 충분한 용량입니다. 많은 수의 사용자 또는 그룹을 사용하는 Active Directory 연결이 있는 경우 이 메모리 할당을 늘릴 필요가 있습니다. 시스템에 10만 명이 넘는 사용자가 포함되어 있는 경우(각각 30개 그룹, 총 750개 그룹) 메모리 할당을 늘리는 것이 적합합니다. 이러한 시스템의 경우 VMware에서는 Directories Management 메모리 할당을 6GB로 늘릴 것을 권장합니다.

디렉토리 관리 메모리는 vRealize Automation 장치에 할당된 총 메모리를 기반으로 계산됩니다. 다음 표에서는 관련 구성 요소에 대한 메모리 할당을 보여 줍니다.

표 2-5. vRealize Automation 장치 메모리 할당

가상 장치 메모리	vRA 서비스 메모리	vIDM 서비스 메모리
18GB	3.3GB	4GB
24GB	4.9GB	6GB
30GB	7.4GB	9.1GB

참고 이러한 할당은 가상 장치에서 모든 기본 서비스가 사용하도록 설정되어 있고 실행 중이라고 가정합니다. 일부 서비스가 중지되면 달라질 수 있습니다.

필수 조건

- vRealize Automation 배포에서 적절한 Active Directory 연결이 구성되어 있고 작동하고 있습니다.

프로시저

1 vRealize Automation 장치를 실행 중인 각 시스템을 중지합니다.

2 각 시스템에서 가상 장치 메모리 할당을 늘립니다.

18GB의 기본 메모리 할당을 사용 중인 경우, VMware에서는 메모리 할당을 24GB로 늘릴 것을 권장합니다.

3 vRealize Automation 장치 시스템을 다시 시작합니다.

DNS 서비스 위치(SRV) 조회 재정의의 위해 도메인 호스트 조회 파일 생성

통합 Windows 인증을 사용하도록 설정하면 DNS 서비스 위치 필드를 사용하도록 디렉토리 구성이 변경됩니다. connector 서비스 위치 조회는 사이트를 인식하지 못합니다. 임의의 DC 선택을 재정의 하려는 경우 domain_krb.properties라는 파일을 생성하고 SRV 조회보다 우선하는 호스트 값에 도메인을 추가합니다.

프로시저

1 appliance-va 명령줄에서 루트 권한을 가진 사용자로 로그인합니다.

2 디렉토리를 /usr/local/horizon/conf로 변경하고 domain_krb.properties라는 이름의 파일을 생성합니다.

3 domain_krb.properties 파일을 편집하여 도메인 목록을 호스트 값에 추가합니다. 정보를 <AD Domain>=<host:port>, <host2:port2>, <host2:port2>로 추가합니다.

예를 들어 목록을 example.com=examplehost.com:636, examplehost2.example.com:389로 입력합니다.

4 domain_krb.properties 파일의 소유자를 horizon으로, 그룹을 www로 변경합니다. `chown horizon:www /usr/local/horizon/conf/domain_krb.properties`를 입력합니다.

5 서비스를 다시 시작합니다. `service horizon-workspace restart`를 입력합니다.

Active Directory에서 동기화하는 사용자 특성 관리

[디렉토리 관리 사용자 특성] 페이지는 Active Directory 연결에 동기화하는 사용자 특성을 나열합니다.

[사용자 특성] 페이지에서 작성 및 저장하는 변경 내용은 Directories Management 디렉토리의 [매핑된 특성] 페이지에 추가됩니다. 특성 변경 내용은 다음에 Active Directory에 동기화될 때 디렉토리에 업데이트됩니다.

[사용자 특성] 페이지에는 Active Directory 특성에 매핑할 수 있는 기본 디렉토리 특성이 나열되어 있습니다. 필요한 특성을 선택하고 디렉토리에 동기화할 다른 Active Directory 특성을 추가할 수 있습니다.

표 2-6. 디렉토리에 동기화할 기본 Active Directory 특성

디렉토리 특성 이름	Active Directory 특성에 대한 기본 매핑
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName

표 2-6. 디렉토리에 동기화할 기본 Active Directory 특성 (계속)

디렉토리 특성 이름	Active Directory 특성에 대한 기본 매핑
employeeid	employeeID
domain	canonicalName. 개체의 정규화된 도메인 이름을 추가합니다.
disabled(외부 사용자 사용 안 함)	userAccountControl. UF_Account_Disable로 플래그 지정됩니다. 계정이 사용 안 함으로 설정되면 사용자는 애플리케이션과 리소스에 로그인 및 액세스할 수 없습니다. 사용자에게 사용 권한이 부여된 리소스는 계정에서 제거되지 않으므로 계정에서 플래그가 제거되면 사용자는 권한 있는 리소스에 로그인하고 액세스할 수 있습니다.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName

[사용자 특성] 페이지에는 Active Directory 특성에 매핑할 수 있는 기본 디렉토리 특성이 나열되어 있습니다. 필요한 특성을 선택하고 디렉토리에 동기화할 다른 Active Directory 특성을 추가할 수 있습니다.

표 2-7. 디렉토리에 동기화할 기본 Active Directory 특성

디렉토리 특성 이름	Active Directory 특성에 대한 기본 매핑
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeid	employeeID
domain	canonicalName. 개체의 정규화된 도메인 이름을 추가합니다.
disabled(외부 사용자 사용 안 함)	userAccountControl. UF_Account_Disable로 플래그 지정됩니다. 계정이 사용 안 함으로 설정되면 사용자는 애플리케이션과 리소스에 로그인 및 액세스할 수 없습니다. 사용자에게 사용 권한이 부여된 리소스는 계정에서 제거되지 않으므로 계정에서 플래그가 제거되면 사용자는 권한 있는 리소스에 로그인하고 액세스할 수 있습니다.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName

커넥터 및 커넥터 클러스터 관리

[커넥터] 페이지는 엔터프라이즈 네트워크용으로 배포된 커넥터를 나열합니다. 커넥터는 Active Directory와 디렉토리 관리 서비스 간 사용자 및 그룹 데이터를 동기화합니다. ID 제공자로 사용되는 경우에는 서비스에 대해 사용자를 인증합니다.

vRealize Automation에서 각 vRealize Automation 장치에는 고유한 커넥터가 포함되어 있으며 이러한 커넥터는 대부분의 배포에 적합합니다.

디렉토리를 커넥터 인스턴스와 연결하는 경우 커넥터가 작업자라고 하는 연결된 디렉토리에 대한 파티션을 생성합니다. 커넥터 인스턴스에 연결된 작업자가 여러 개 있을 수 있습니다. 각 작업자는 ID 제공자 역할을 합니다. 커넥터는 하나 이상의 작업자를 통해 Active Directory와 서비스 간의 사용자 및 그룹 데이터를 동기화합니다. 작업자별로 인증 방법을 정의 및 구성합니다.

[커넥터] 페이지에서 Active Directory 링크의 다양한 측면을 관리할 수 있습니다. 이 페이지에는 다양한 관리 작업을 완료할 수 있게 해 주는 테이블과 여러 버튼이 포함되어 있습니다.

- [작업자] 열에서 커넥터의 세부 정보를 볼 작업자를 선택하고 사용 가능한 인증 방법의 상태를 볼 [인증 어댑터] 페이지로 이동합니다. 인증에 대한 자세한 내용은 [대체 사용자 인증 제품을 디렉토리 관리와 통합](#) 항목을 참조하십시오.
- [ID 제공자] 열에서 보거나 편집하거나 사용하지 않도록 설정할 IdP를 선택합니다. [타사 ID 제공자 연결 구성](#) 항목을 참조하십시오.
- [연결된 디렉토리] 열에서 이 작업자와 연결된 디렉토리에 액세스합니다.
- **도메인 가입**을 클릭하여 커넥터를 특정 Active Directory 도메인에 가입시킵니다. 예를 들어 Kerberos 인증을 구성하는 경우 사용자를 포함하고 있거나 사용자를 포함하고 있는 도메인과 신뢰 관계를 형성하고 있는 Active Directory 도메인에 가입해야 합니다.
- 통합 Windows 인증 Active Directory로 디렉토리를 구성하는 경우 커넥터가 구성 세부 정보에 따라 도메인에 가입합니다.

클러스터된 환경의 커넥터

분산 vRealize Automation 배포 환경에서는 사용 가능한 모든 커넥터가 필요한 모든 사용자 권한 부여를 수행하지만, 모든 구성 동기화는 지정된 단일 커넥터에 의해 처리됩니다. 일반적으로 동기화에는 사용자 구성에 대한 추가, 삭제 또는 변경이 포함되며 모든 커넥터를 사용할 수 있는 한 동기화가 자동으로 수행됩니다. 하지만 일부 특정 상황에서는 자동 동기화가 실행되지 않을 수 있습니다.

기본 DN과 같은 디렉토리 구성과 관련된 변경 사항의 경우 vRealize Automation은 클러스터의 모든 커넥터에 업데이트를 자동으로 푸시하려고 시도합니다. 어떤 이유로 커넥터가 작동하지 않거나 연결할 수 없는 경우 해당 커넥터는 온라인 작업이 재개되어도 업데이트를 수신하지 않습니다. 업데이트를 자동으로 수신하지 못한 커넥터에 구성 변경 사항을 구현하려면 시스템 관리자가 적용 가능한 모든 커넥터에 변경 사항을 수동으로 저장해야 합니다.

디렉토리 동기화 프로파일 관련 변경 사항의 경우 vRealize Automation은 모든 커넥터에 업데이트를 자동으로 푸시하려고 시도합니다. 동기화 커넥터가 작동 중이면 업데이트가 저장되고 사용 가능한 모든 권한 부여 커넥터에 푸시됩니다. 하나 이상의 커넥터에 연결할 수 없는 경우 시스템 관리자가 일부 커넥터가 업데이트되지 않았음을 나타내는 경고를 받게 됩니다. 동기화 커넥터가 작동하지 않는 경우 업데이트가 실패하고 오류가 발생합니다. 시스템 관리자가 동기화 커넥터로 지정된 커넥터를 변경하면 사용 가능한 최신 프로파일 정보를 새 동기화 커넥터가 수신하며, 이 정보는 적용 가능하고 사용 가능한 모든 커넥터에 푸시됩니다.

도메인에 커넥터 시스템 가입

경우에 따라 디렉토리 관리 커넥터가 포함된 시스템을 도메인에 가입해야 할 수 있습니다.

LDAP를 통한 Active Directory 디렉토리의 경우, 디렉토리를 생성한 후 도메인에 가입할 수 있습니다. Active Directory(Windows 통합 인증) 디렉토리의 경우, 디렉토리를 생성할 때 커넥터가 도메인에 자동으로 가입됩니다. 두 경우 모두 사용자가 적절한 자격 증명을 제공해야 합니다.

도메인에 가입하려면 사용자에게 “컴퓨터를 AD 도메인에 가입”하는 권한을 갖는 Active Directory 자격 증명에 있어야 합니다. 이 자격 증명은 다음 권한을 사용하여 Active Directory에 구성됩니다.

- 컴퓨터 개체 작성
- 컴퓨터 개체 삭제

도메인에 가입할 때 Active Directory의 기본 위치에 컴퓨터 개체가 생성됩니다.

도메인에 가입할 권한이 없거나 회사 정책에 따라 컴퓨터 개체의 사용자 지정 위치가 필요한 경우, 관리자에게 해당 개체를 생성한 다음 커넥터 시스템을 도메인에 가입하도록 요청해야 합니다.

프로시저

- 1 Active Directory 관리자에게 회사 정책에 따라 결정된 위치에 Active Directory의 컴퓨터 개체를 생성해 달라고 요청합니다. 커넥터의 호스트 이름을 제공해야 합니다. `server.example.com`과 같은 FQDN(정규화된 도메인 이름)을 제공해야 합니다.

관리 콘솔의 [커넥터] 페이지에 있는 [호스트 이름] 열에서 호스트 이름을 확인할 수 있습니다. **관리 > 디렉토리 관리 > 커넥터**를 선택합니다.
- 2 컴퓨터 개체가 생성되면 [커넥터] 페이지에서 **도메인에 가입**을 클릭하고 디렉토리 관리에 제공되는 도메인 사용자 계정을 사용하여 도메인에 가입합니다.

도메인 컨트롤러 선택 정보

domain_krb.properties 파일은 DNS 서비스 위치(SRV 레코드) 조회가 사용하도록 설정된 디렉토리에 어떤 도메인 컨트롤러를 사용하는지 결정합니다. 여기에는 각 도메인의 도메인 컨트롤러 목록이 들어 있습니다. 이 파일은 처음에 커넥터가 생성하고, 이후에는 사용자가 유지 관리해야 합니다. 해당 파일에 따라 DNS 서비스 위치(SRV) 조회가 재정의됩니다.

다음 유형의 디렉토리는 DNS 서비스 위치 조회가 사용하도록 설정되어 있습니다.

- 이 디렉토리에서 DNS 서비스 위치 지원 옵션이 선택된 LDAP를 통한 Active Directory
- DNS 서비스 위치 조회가 항상 사용하도록 설정된 Active Directory(Windows 통합 인증)

DNS 서비스 위치 조회가 사용하도록 설정된 디렉토리를 처음 생성하는 경우, 가상 시스템의 /usr/local/horizon/conf 디렉토리에 domain_krb.properties 파일이 자동으로 생성되고 각 도메인의 도메인 컨트롤러가 이 파일에 자동으로 채워집니다. 이 파일을 채우기 위해 커넥터는 커넥터와 동일한 사이트에 있는 도메인 컨트롤러를 찾은 후 연결 가능하고 가장 빠르게 응답하는 두 개의 도메인 컨트롤러를 선택합니다.

DNS 서비스 위치가 사용하도록 설정된 디렉토리를 추가로 생성하거나 새 도메인을 Windows 통합 인증 디렉토리에 추가하는 경우, 새 도메인과 해당 도메인의 도메인 컨트롤러 목록이 파일에 추가됩니다.

언제든지 domain_krb.properties 파일을 편집하여 기본 선택을 재정의할 수 있습니다. 가장 좋은 방법은 디렉토리를 생성한 후 domain_krb.properties 파일을 보고 나열된 도메인 컨트롤러가 구성에 맞는 최적의 도메인 컨트롤러인지 확인하는 것입니다. 여러 개의 도메인 컨트롤러가 지역적으로 다른 위치에 있는 글로벌 Active Directory 배포에서 커넥터에 가까이 있는 도메인 컨트롤러를 사용하면 Active Directory와의 통신 속도가 향상됩니다.

그 외 다른 내용을 변경한 경우에도 파일을 수동으로 업데이트해야 합니다. 다음과 같은 규칙이 적용됩니다.

- domain_krb.properties 파일은 커넥터가 있는 가상 시스템에 생성됩니다. 일반 배포에서 배포된 추가 커넥터가 없으면 파일이 Directories Management 서비스 가상 시스템에 생성됩니다. 디렉토리에 추가 커넥터를 사용하고 있는 경우, 파일이 커넥터 가상 시스템에 작성됩니다. 하나의 가상 시스템에는 domain_krb.properties 파일이 한 개만 있을 수 있습니다.
- DNS 서비스 위치 조회가 사용하도록 설정된 디렉토리를 처음 생성하면 파일이 생성되고 이 파일에 각 도메인의 도메인 컨트롤러가 자동으로 채워집니다.
- 각 도메인의 도메인 컨트롤러는 우선 순위대로 나열됩니다. Active Directory에 연결하기 위해 커넥터는 목록에서 첫 번째 도메인 컨트롤러를 시도합니다. 해당 도메인 컨트롤러에 연결할 수 없으면 목록에서 두 번째 도메인 컨트롤러를 시도하는 식으로 계속 이어집니다.
- 이 파일은 DNS 서비스 위치 조회가 사용하도록 설정된 디렉토리를 새로 생성하거나 도메인을 Windows 통합 인증 디렉토리에 추가하는 경우에만 업데이트됩니다. 새 도메인과 해당 도메인의 도메인 컨트롤러 목록이 파일에 추가됩니다.

도메인 항목이 이미 파일에 있는 경우 업데이트되지 않는다는 점에 유의하십시오. 예를 들어, 디렉토리를 생성했다가 삭제하면 원래 도메인 항목이 파일에 남아 있고 업데이트되지 않습니다.

- 이 파일은 그 외 다른 시나리오에서도 자동으로 업데이트되지 않습니다. 예를 들어, 디렉토리를 삭제해도 도메인 항목이 파일에서 삭제되지 않습니다.
- 파일에 나열된 도메인 컨트롤러에 연결할 수 없는 경우, 파일을 편집하여 해당 도메인 컨트롤러를 제거합니다.
- 도메인 항목을 수동으로 추가하거나 편집하면 변경 내용을 덮어쓰지 않습니다.

도메인 컨트롤러를 선택하여 domain_krb.properties 파일을 자동으로 채우는 방법

domain_krb.properties 파일을 자동으로 채우기 위해 먼저 (IP 주소와 넷마스크를 기반으로) 커넥터가 상주하는 서브넷을 확인한 후 Active Directory 구성을 사용하여 해당 서브넷의 사이트를 식별하고, 사이트의 도메인 컨트롤러 목록을 가져오고, 목록에서 적절한 도메인으로 필터링하고, 가장 빠르게 응답하는 두 개의 도메인 컨트롤러를 선택하는 방법으로 도메인 컨트롤러를 선택하게 됩니다.

가장 가까이 있는 도메인 컨트롤러를 감지하기 위해서는 VMware Identity Manager에서 다음 요구 사항을 충족해야 합니다.

- 커넥터의 서브넷이 Active Directory 구성에 있거나 서브넷을 runtime-config.properties 파일에 지정해야 합니다.

서브넷은 사이트를 확인하는 데 사용됩니다.

- Active Directory 구성은 사이트를 인식해야 합니다.

서브넷을 확인할 수 없거나 Active Directory 구성에서 사이트가 인식되지 않는 경우, DNS 서비스 위치 조회를 사용하여 도메인 컨트롤러를 찾고, 연결 가능한 몇 개의 도메인 컨트롤러가 파일에 채워집니다. 이 도메인 컨트롤러가 커넥터와 지리적으로 동일한 위치에 있지 않을 수 있는데, 이때는 Active Directory와 통신할 때 시간이 지연되거나 제한 시간을 초과할 수 있음에 유의하십시오. 이 경우, domain_krb.properties 파일을 수동으로 편집하고 각 도메인에 사용할 올바른 도메인 컨트롤러를 지정합니다.

샘플 domain_krb.properties 파일

```
example.com=host1.example.com:389,host2.example.com:389
```

■ 기본 서브넷 선택 재정의

domain_krb.properties 파일을 자동으로 채우기 위해 커넥터는 커넥터와 Active Directory 간의 지연 시간이 최소화되도록 동일한 사이트에 있는 도메인 컨트롤러를 찾으려고 합니다.

■ domain_krb.properties 파일 편집

/usr/local/horizon/conf/domain_krb.properties 파일은 DNS 서비스 위치 조회가 사용하도록 설정된 디렉토리에 사용하는 도메인 컨트롤러를 결정합니다. 언제든지 이 파일을 편집하여 도메인의 도메인 컨트롤러 목록을 수정하거나 도메인 항목을 추가 또는 삭제할 수 있습니다. 변경한 내용은 재정의되지 않습니다.

■ domain_krb.properties 문제 해결

이 정보는 domain_krb.properties 파일의 문제를 해결하는 데 사용됩니다.

기본 서브넷 선택 재정의

domain_krb.properties 파일을 자동으로 채우기 위해 커넥터는 커넥터와 Active Directory 간의 지연 시간이 최소화되도록 동일한 사이트에 있는 도메인 컨트롤러를 찾으려고 합니다.

해당 사이트를 찾기 위해 커넥터는 IP 주소와 넷마스크를 기반으로 사이트가 상주하는 서브넷을 확인한 후 Active Directory 구성을 사용하여 해당 서브넷의 사이트를 식별합니다. 가상 시스템의 서브넷이 Active Directory에 있지 않거나 자동 서브넷 선택을 재정의하려는 경우, runtime-config.properties 파일에 서브넷을 지정할 수 있습니다.

프로시저

- 1 루트 사용자로 Directories Management 가상 시스템에 로그인합니다.

참고 디렉토리에 추가 커넥터를 사용하고 있는 경우, 커넥터 가상 시스템에 로그인합니다.

- 2 `/usr/local/horizon/conf/runtime-config.properties` 파일을 편집하고 다음 특성을 추가합니다.

`sitateware.subnet.override=subnet`

여기서 subnet은 사용할 도메인 컨트롤러가 있는 사이트의 서브넷입니다. 예:

`sitateware.subnet.override=10.100.0.0/20`

- 3 파일을 저장한 후 닫습니다.

- 4 서비스를 다시 시작합니다.

`service horizon-workspace restart`

domain_krb.properties 파일 편집

`/usr/local/horizon/conf/domain_krb.properties` 파일은 DNS 서비스 위치 조회가 사용하도록 설정된 디렉토리에 사용하는 도메인 컨트롤러를 결정합니다. 언제든지 이 파일을 편집하여 도메인의 도메인 컨트롤러 목록을 수정하거나 도메인 항목을 추가 또는 삭제할 수 있습니다. 변경한 내용은 재정의되지 않습니다.

이 파일은 커넥터에 의해 처음 생성되고 자동으로 채워집니다. 일부 시나리오에서는 이 파일을 사용자가 수동으로 업데이트해야 합니다.

- 기본적으로 선택된 도메인 컨트롤러가 구성에 맞는 최적의 도메인 컨트롤러가 아니면 이 파일을 편집하고 사용할 도메인 컨트롤러를 지정합니다.
- 디렉토리를 삭제하는 경우, 해당 도메인 항목도 파일에서 삭제합니다.
- 파일에 연결할 수 없는 도메인 컨트롤러가 있으면 해당 항목을 파일에서 제거합니다.

도메인 컨트롤러 선택 정보도 참조하십시오.

프로시저

- 1 루트 사용자로 Directories Management 가상 시스템에 로그인합니다.

참고 디렉토리에 추가 커넥터를 사용하고 있는 경우, 커넥터 가상 시스템에 로그인합니다.

- 2 디렉토리를 `/usr/local/horizon/conf`로 변경합니다.

- 3 `domain_krb.properties` 파일을 편집하여 도메인 목록을 호스트 값에 추가하거나 도메인 목록을 편집합니다.

다음 형식을 사용합니다.

`domain=host:port,host2:port,host3:port`

예:

`example.com=examplehost1.example.com:389,examplehost2.example.com:389`

도메인 컨트롤러를 우선 순위대로 나열합니다. Active Directory에 연결하기 위해 커넥터는 목록에서 첫 번째 도메인 컨트롤러를 시도합니다. 해당 도메인 컨트롤러에 연결할 수 없으면 목록에서 두 번째 도메인 컨트롤러를 시도하는 식으로 계속 이어집니다.

중요 도메인 이름은 소문자여야 합니다.

- 4 다음 명령을 사용하여 domain_krb.properties 파일의 소유자를 horizon으로, 그룹을 www로 변경합니다.

```
chown horizon:www /usr/local/horizon/conf/domain_krb.properties
```

- 5 서비스를 다시 시작합니다.

```
service horizon-workspace restart
```

domain_krb.properties 문제 해결

이 정보는 domain_krb.properties 파일의 문제를 해결하는 데 사용됩니다.

[도메인 확인 중 오류 발생] 오류

domain_krb.properties 파일에 도메인 항목이 이미 포함되어 있고 동일한 도메인에 대해 다른 유형의 디렉토리를 새로 생성하려고 하면 [도메인 생성 중 오류 발생] 오류가 발생합니다.

domain_krb.properties 파일을 편집하고 새 디렉토리를 생성하기 전에 도메인 항목을 수동으로 제거해야 합니다.

도메인 컨트롤러에 연결할 수 없음

domain_krb.properties 파일에 추가한 도메인 항목은 자동으로 업데이트되지 않습니다. 파일에 나열된 도메인 컨트롤러에 연결할 수 없게 되면 파일을 수동으로 편집하고 제거합니다.

액세스 정책 관리

Directories Management 정책은 사용자가 애플리케이션 포털에 액세스하거나 지정된 웹 애플리케이션을 시작하기 위해 충족되어야 하는 기준을 지정하는 일련의 규칙입니다.

규칙을 정책의 일부로 생성합니다. 정책의 각 규칙은 다음과 같은 정보를 지정할 수 있습니다.

- 엔터프라이즈 네트워크 내부 또는 외부와 같이 사용자가 로그인하도록 허용되는 네트워크 범위.
- 이 정책을 통해 액세스할 수 있는 디바이스 유형.
- 사용하도록 설정된 인증 방법이 적용되는 순서.
- 인증이 유효한 시간.
- 사용자 지정 액세스 거부 메시지

참고 이 정책은 웹 애플리케이션 세션이 지속되는 시간을 제어하지 않습니다. 사용자가 웹 애플리케이션을 시작해야 하는 시간을 제어합니다.

Directories Management 서비스에는 편집할 수 있는 기본 정책이 포함되어 있습니다. 이 정책은 전체 서비스에 대한 액세스를 제어합니다. [기본 액세스 정책 적용](#)의 내용을 참조하십시오. 특정 웹 애플리케이션에 대한 액세스를 제어하기 위해 추가 정책을 생성할 수 있습니다. 웹 애플리케이션에 정책을 적용하지 않는 경우 기본 정책이 적용됩니다.

액세스 정책 설정 구성

정책에는 하나 이상의 액세스 규칙이 포함되어 있습니다. 각 규칙은 전체 애플리케이션 포털 또는 지정된 웹 애플리케이션에 대한 사용자 액세스를 관리하기 위해 구성할 수 있는 설정으로 이루어져 있습니다.

네트워크 범위

각 규칙에 대해 네트워크 범위를 지정하여 사용자 기반을 결정합니다. 네트워크 범위는 하나 이상의 IP 범위로 구성됩니다. 액세스 정책 집합을 구성하기 전에 [ID 및 액세스 관리] 탭의 [설정] > [네트워크 범위] 페이지에서 네트워크 범위를 생성합니다.

디바이스 유형

규칙에서 관리하는 디바이스 유형을 선택합니다. 클라이언트 유형은 웹 브라우저, ID 관리자 클라이언트 앱, iOS, Android 및 모든 디바이스 유형입니다.

인증 방법

정책 규칙에 대한 인증 방법의 우선 순위를 설정합니다. 인증 방법은 나열된 순서대로 적용됩니다. 정책의 인증 방법 및 네트워크 범위 구성을 충족하는 첫 번째 ID 제공자 인스턴스가 선택되고, 사용자 인증 요청이 인증을 위해 ID 제공자 인스턴스로 전달됩니다. 인증이 실패하면 목록의 다음 인증 방법이 선택됩니다. 인증서 인증을 사용하는 경우 이 방법이 목록의 첫 번째 인증 방법이어야 합니다.

사용자가 로그인하기 위해서는 두 가지 인증 방법을 통해 자격 증명을 전달해야 하도록 액세스 정책 규칙을 구성할 수 있습니다. 하나 또는 두 개의 인증 방법이 실패하고 폴백 방법이 구성된 경우, 구성된 다음 인증 방법의 자격 증명을 입력하라는 메시지가 사용자에게 표시됩니다. 다음 두 시나리오에서는 인증 체인의 작동 방법을 설명합니다.

- 첫 번째 시나리오에서는 사용자가 자신의 암호 및 Kerberos 자격 증명을 사용하여 인증하도록 액세스 정책 규칙이 구성되어 있습니다. 인증을 위해 암호 및 RADIUS 자격 증명을 요구하는 폴백 인증이 설정되어 있습니다. 사용자가 암호는 올바르게 입력했지만, Kerberos 인증 자격 증명은 올바르게 입력하지 못했습니다. 사용자가 올바른 암호를 입력했기 때문에 폴백 인증 요청은 RADIUS 자격 증명에만 해당합니다. 사용자가 암호를 다시 입력할 필요가 없습니다.
- 두 번째 시나리오에서는 사용자가 자신의 암호 및 Kerberos 자격 증명을 사용하여 인증하도록 액세스 정책 규칙이 구성되어 있습니다. 인증을 위해 RSA SecurID 및 RADIUS를 요구하는 폴백 인증이 설정되어 있습니다. 사용자가 암호는 올바르게 입력했지만, Kerberos 인증 자격 증명은 올바르게 입력하지 못했습니다. 폴백 인증 요청은 인증을 위해 RSA SecurID 자격 증명과 RADIUS 자격 증명 모두에 해당합니다.

인증 세션 기간

각 규칙에 대해 이 인증이 유효한 기간을 설정합니다. 이 값은 마지막 인증 이벤트 후 사용자가 포털에 액세스하거나 특정 웹 애플리케이션을 시작할 수 있는 최대 시간을 결정합니다. 예를 들어, 웹 애플리케이션 규칙에서 값을 4로 지정하는 경우 사용자가 시간을 연장하는 다른 인증 이벤트를 시작하지 않는다면 4시간 동안 웹 애플리케이션을 시작할 수 있습니다.

사용자 지정 액세스 거부 오류 메시지

사용자가 잘못된 자격 증명, 잘못된 구성 또는 시스템 오류 때문에 로그인에 실패하면 액세스 거부 메시지가 표시됩니다. 기본 메시지는 다음과 같습니다.

유효한 인증 방법을 찾지 못했기 때문에 액세스가 거부되었습니다.

기본 메시지를 재정의하는 각 액세스 정책 규칙에 대해 사용자 지정 오류 메시지를 만들 수 있습니다. 사용자 지정 메시지에는 조치 메시지에 대한 텍스트 및 링크가 포함될 수 있습니다. 예를 들어 관리하려는 모바일 디바이스의 정책 규칙에서 사용자가 등록되지 않은 디바이스에서 로그인하려고 하면 다음의 사용자 지정 오류 메시지가 표시될 수 있습니다.

이 메시지 끝에 나오는 링크를 클릭하여 회사 리소스에 액세스할 수 있게 디바이스를 등록하십시오. 디바이스가 이미 등록된 경우 지원을 요청하십시오.

기본 정책 예

다음 정책은 애플리케이션 포털에 대한 액세스를 제어하기 위해 기본 정책을 구성할 수 있는 방법에 대한 예제 역할을 합니다. [사용자 액세스 정책 관리](#) 항목을 참조하십시오.

정책 규칙은 나열된 순서대로 평가됩니다. [정책 규칙] 섹션에서 규칙을 끌어서 놓으면 정책 순서를 변경할 수 있습니다.

다음 사용 사례에서 이 예제 정책은 모든 애플리케이션에 적용됩니다.

*** 정책 이름** default_access_policy_set 기본 정책

설명 Default access policy set

적용 대상 모든 애플리케이션

정책 규칙

이러한 웹 애플리케이션에 액세스할 규칙 목록을 생성할 수 있습니다. 각 규칙에 대해 IP 네트워크 범위, 애플리케이션에 액세스할 수 있는 디바이스 유형, 방법 및 인증 순서, 사용자가 재인증 전에 애플리케이션을 사용할 수 있는 최대 시간을 선택하십시오.

네트워크 범위	디바이스 유형	인증 방법	재인증	
모든 범위	웹 브라우저	Password	8 시간	✗ +
모든 범위	Identity Manager 클라이언트 애플리케이션	Password	2160 시간	✗ +

- 내부 네트워크(내부 네트워크 범위)의 경우 규칙에 대한 두 개의 인증 방법(Kerberos 및 암호 인증)이 폴백 방법으로 구성되어 있습니다. 내부 네트워크에서 앱 포털에 액세스하기 위해 서비스는 먼저 Kerberos 인증을 사용하여 사용자를 인증합니다. 이 방법이 규칙에 나열된 첫 번째 인증 방법이기 때문입니다. 이 방법이 실패할 경우 사용자에게 Active Directory 암호를 입력하라는 메시지가 표시됩니다. 사용자는 브라우저를 사용하여 로그인하고 이제 8시간 세션 동안 사용자 포털에 대한 액세스 권한을 갖습니다.

- 외부 네트워크(모든 범위)에서 액세스할 경우 하나의 인증 방법 RSA SecurID만 구성되어 있습니다. 외부 네트워크에서 앱 포털에 액세스하려면 사용자가 SecurID를 사용하여 로그인해야 합니다. 사용자는 브라우저를 사용하여 로그인하고 이제 4시간 세션 동안 사용자 앱 포털에 대한 액세스 권한을 갖습니다.
- 2 사용자가 리소스에 액세스할 경우 웹 애플리케이션 관련 정책이 적용되는 웹 애플리케이션을 제외하고 기본 포털 액세스 정책이 적용됩니다.

예를 들어, 해당 리소스의 재인증 시간은 기본 액세스 정책 규칙의 재인증 시간과 일치합니다. 앱 포털에 로그인한 사용자의 시간이 기본 액세스 정책 규칙에 따라 8시간일 경우 세션 중에 사용자가 리소스를 시작하면 사용자를 재인증하지 않고도 애플리케이션이 시작됩니다.

웹 애플리케이션 관련 정책 관리

카탈로그에 웹 애플리케이션을 추가할 때 웹 애플리케이션 관련 액세스 정책을 생성할 수 있습니다. 예를 들어 웹 애플리케이션에 대해 어느 IP 주소가 애플리케이션에 대한 액세스 권한을 갖는지, 어느 인증 방법을 사용하는지, 재인증이 필요할 때까지 얼마 동안 유효한지를 지정하는 규칙으로 정책을 생성할 수 있습니다.

다음 웹 애플리케이션 관련 정책은 지정된 웹 애플리케이션에 대한 액세스를 제어하기 위해 생성할 수 있는 정책의 예를 제공합니다.

예 1 엄격한 웹 애플리케이션 관련 정책

이 예에서는 새 정책이 생성되어 중요한 웹 애플리케이션에 적용됩니다.

The screenshot shows the configuration for a policy named "Sensitive Web Application". The policy is intended for web applications that should have limited access. The configuration includes a description, a list of applicable applications (AirWatch, Content Locker), and a table of rules.

정책 이름: Sensitive Web Application

설명: To be applied to Web application that should have limited access.

적용 대상: 카탈로그에서 이 정책을 적용할 애플리케이션을 선택하십시오. (AirWatch, Content Locker)

정책 규칙:

이러한 애플리케이션에 액세스하는 규칙 목록을 생성할 수 있습니다. 각 규칙에 대해 IP 네트워크 범위, 애플리케이션에 액세스할 수 있는 디바이스 유형, 방법 및 인증을 선택하고, 사용자가 재인증 전에 애플리케이션을 사용할 수 있는 최대 시간을 선택하십시오.

네트워크 범위	디바이스 유형	인증 방법	재인증	그룹	
Internal Network	웹 브라우저	먼저 다음을 시도하십시오. Kerberos 및 토큰 1개 이상	8 시간	모든 사용자	✗ +
모든 범위	웹 브라우저	Securid	4 시간	모든 사용자	✗ +

Buttons: 저장 (Save), 취소 (Cancel)

- 1 엔터프라이즈 네트워크 외부에서 서비스에 액세스하려면 사용자가 RSA SecurID로 로그인해야 합니다. 사용자가 브라우저를 사용하여 로그인하고 이제 기본 액세스 규칙에 제공된 대로 4시간 세션 동안 애플리케이션 포털에 액세스할 수 있습니다.
- 2 4시간 후 사용자가 중요한 웹 애플리케이션 정책 집합이 적용된 웹 애플리케이션을 시작하려고 합니다.

- 3 사용자 요청이 웹 브라우저 및 [모든 범위] 네트워크 범위에서 비롯되므로 서비스가 정책의 규칙을 확인하고 [모든 범위] 네트워크 범위의 정책을 적용합니다.

사용자가 RSA SecurID 인증 방법을 사용하여 로그인하지만 세션이 만료되었습니다. 사용자가 재인증을 위해 리디렉션됩니다. 재인증은 사용자에게 또 하나의 4시간 세션과 애플리케이션을 시작할 수 있는 능력을 제공합니다. 다음 4시간 동안 사용자는 재인증할 필요 없이 계속해서 애플리케이션을 시작할 수 있습니다.

예 2 더욱 엄격한 웹 애플리케이션 관련 정책

더욱 중요한 웹 애플리케이션에 적용할 더욱 엄격한 규칙의 경우 1시간 후 모든 디바이스에서 SecurID를 사용한 재 인증을 요청할 수 있습니다. 다음은 이러한 유형의 정책 액세스 규칙이 구현되는 방법에 대한 예입니다.

- 1 사용자가 암호 인증 방법을 사용하여 엔터프라이즈 네트워크 내부에서 로그인합니다.
이제 사용자는 예 1에서 설정한 대로 8시간 동안 애플리케이션 포털에 액세스할 수 있습니다.
- 2 사용자가 예 2 정책 규칙이 적용된 웹 애플리케이션을 즉시 시작하려고 하며 이를 위해서는 RSA SecurID 인증이 필요합니다.
- 3 사용자가 RSA SecurID 인증을 제공하는 ID 제공자로 리디렉션됩니다.
- 4 사용자가 로그인한 후 서비스가 애플리케이션을 시작하고 인증 이벤트를 저장합니다.
사용자는 계속해서 최대 1시간 동안 이 애플리케이션을 시작할 수 있지만 정책 규칙에 지정된 대로 1시간 후 재인증하도록 요청됩니다.

사용자 액세스 정책 관리

vRealize Automation에는 그대로 사용하거나 필요에 따라 편집하여 애플리케이션에 대한 테넌트 액세스를 관리할 수 있는 기본 사용자 액세스 정책이 제공됩니다.

vRealize Automation에는 기본 사용자 액세스 정책이 제공되며 새 정책을 추가할 수 없습니다. 규칙 추가를 위해 기존 정책을 편집할 수 있습니다.

필수 조건

- 배포에 적절한 ID 제공자를 선택하거나 구성합니다. [타사 ID 제공자 연결 구성](#) 항목을 참조하십시오.
- 배포에 적절한 네트워크 범위를 구성합니다. [네트워크 범위 추가 또는 편집](#) 항목을 참조하십시오.
- 배포에 적절한 인증 방법을 구성합니다. [대체 사용자 인증 제품을 디렉토리 관리와 통합](#) 항목을 참조하십시오.
- 전체 서비스에 대한 사용자 액세스를 제어하기 위해 기본 정책을 편집하려는 경우 웹 애플리케이션 관련 정책을 생성하기 전에 구성합니다.
- 카탈로그에 웹 애플리케이션을 추가합니다. 정책을 추가할 수 있으려면 [카탈로그] 페이지에 웹 애플리케이션이 나열되어야 합니다.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 디렉토리 관리 > 정책**을 선택합니다.
- 2 **정책 편집**을 클릭하고 새 정책을 추가합니다.
- 3 해당 텍스트 상자에 정책 이름과 설명을 추가합니다.
- 4 [적용 대상] 섹션에서 **선택**을 클릭하고 표시되는 페이지에서 이 정책과 연결된 웹 애플리케이션을 선택합니다.
- 5 [정책 규칙] 섹션에서 **+**를 클릭하여 규칙을 추가합니다.
[정책 규칙 추가] 페이지가 나타납니다.
 - a 이 규칙에 적용할 네트워크 범위를 선택합니다.
 - b 이 규칙에 대해 웹 애플리케이션에 액세스할 수 있는 디바이스의 유형을 선택합니다.
 - c 사용할 인증 방법을 적용되어야 할 순서대로 선택합니다.
 - d 웹 애플리케이션 세션이 열려 있는 시간을 지정합니다.
 - e **저장**을 클릭합니다.
- 6 필요한 경우 추가 규칙을 구성합니다.
- 7 **저장**을 클릭합니다.

추가적인 ID 제공자 연결 구성

필요에 따라 다양한 ID 관리 시나리오(추가적인 기본 제공 ID 제공자와 타사 ID 제공자 포함)를 지원하기 위해 추가적인 ID 제공자 연결을 구성할 수 있습니다.

디렉토리 관리를 통해 세 가지 유형의 ID 제공자 연결을 생성할 수 있습니다.

- 타사 IDP 생성 - 외부 타사 ID 제공자에 대한 연결을 생성할 때 이 항목을 사용합니다. 타사 ID 제공자 인스턴스를 추가하기 전에 다음 사항을 확인해야 합니다.
 - 타사 인스턴스가 SAML 2.0을 준수하는지, 서비스가 타사 인스턴스에 연결할 수 있는지 확인합니다.
 - 관리 콘솔에서 ID 제공자를 구성할 때 추가할 적절한 타사 메타데이터 정보를 가져옵니다. 타사 인스턴스에서 가져오는 메타데이터 정보는 메타데이터에 대한 URL이거나 실제 메타데이터입니다.
- 작업 공간 IDP 생성 - 디렉토리 관리를 구성하는 동안 사용자 인증을 위한 커넥터를 사용하도록 설정하면 작업 공간 IDP가 ID 제공자로 생성되고 암호 인증이 사용하도록 설정됩니다. 서로 다른 로드 밸런서 뒤에 작업 공간 ID 제공자를 추가로 구성할 수 있습니다.
- 기본 제공 IDP 생성 - 기본 제공 ID 제공자는 내부적인 디렉토리 관리 메커니즘을 사용하여 인증을 지원합니다. 온 프레미스 커넥터를 사용할 필요가 없는 인증 방법을 사용하도록 기본 제공 ID 제공자를 구성할 수 있습니다. 기본 제공 ID 제공자를 구성할 때 해당 제공자에 사용할 인증 방법을 연결합니다.

■ 타사 ID 제공자 연결 구성

vRealize Automation에는 기본 ID 제공자 연결 인스턴스가 제공됩니다. 사용자는 Just-in-Time 사용자 프로비저닝 또는 기타 사용자 지정 구성을 지원하도록 추가 ID 제공자 연결을 생성하고자 할 수 있습니다.

■ 추가 작업 공간 ID 제공자 구성

사용자를 인증할 디렉토리 관리 커넥터를 구성하면 작업 공간 IDP가 생성되고, 암호 인증이 사용하도록 설정됩니다.

■ 기본 제공 ID 제공자 연결 구성

기본 제공 ID 제공자를 여러 개 구성하고 이러한 ID 제공자에 인증 방법을 연결할 수 있습니다.

타사 ID 제공자 연결 구성

vRealize Automation에는 기본 ID 제공자 연결 인스턴스가 제공됩니다. 사용자는 Just-in-Time 사용자 프로비저닝 또는 기타 사용자 지정 구성을 지원하도록 추가 ID 제공자 연결을 생성하고자 할 수 있습니다.

vRealize Automation에는 기본 ID 제공자가 제공됩니다. 대부분의 경우 고객의 요구에 기본 제공자면 충분합니다. 기존 엔터프라이즈 ID 관리 솔루션을 사용하는 경우 사용자 지정 ID 제공자를 설정하여 사용자를 기존 ID 솔루션으로 리디렉션할 수 있습니다.

사용자 지정 ID 제공자를 사용하는 경우 디렉토리 관리는 해당 제공자의 SAML 메타데이터를 사용하여 제공자와의 신뢰 관계를 설정합니다. 이 관계가 설정된 후 디렉토리 관리는 주체 이름 ID에 기반하여 SAML 어설션의 사용자를 내부 vRealize Automation 사용자 목록에 매핑합니다.

필수 조건

- 인증을 위해 이 ID 제공자 인스턴스로 전송할 네트워크 범위를 구성합니다. [네트워크 범위 추가 또는 편집](#) 항목을 참조하십시오.
- 타사 메타데이터 문서에 액세스합니다. 메타데이터 URL 또는 실제 메타데이터일 수 있습니다.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 관리 > 디렉토리 관리 > ID 제공자를 선택합니다.

구성된 모든 ID 제공자가 이 페이지에 표시됩니다.

2 ID 제공자 추가를 클릭합니다.

ID 제공자 옵션이 있는 메뉴가 나타납니다.

3 타사 IDP 생성을 선택합니다.

4 ID 제공자를 구성하는 데 필요한 적절한 정보를 입력합니다.

옵션	설명
ID 제공자 이름	이 ID 제공자 인스턴스의 이름을 입력합니다.
SAML 메타데이터	<p>타사 IdP XML 기반 메타데이터 문서를 추가하여 ID 제공자와 신뢰를 설정합니다.</p> <ol style="list-style-type: none"> 1 SAML 메타데이터 URL 또는 xml 콘텐츠를 텍스트 상자에 입력합니다. 2 프로세스 IdP 메타데이터를 클릭합니다. IdP에서 지원하는 NameID 형식이 메타데이터에서 추출되어 이름 ID 형식 테이블에 추가됩니다. 3 이름 ID 값 열에서, 표시된 ID 형식에 매핑할 서비스의 사용자 특성을 선택합니다. 사용자 지정 타사 이름 ID 형식을 추가하고 이를 서비스의 사용자 특성 값에 매핑할 수 있습니다. 4 (선택사항) NameIDPolicy 응답 식별자 문자열 형식을 선택합니다.
사용자	이 ID 제공자를 사용하여 인증할 수 있는 사용자의 Directories Management 디렉토리를 선택합니다.
Just-in-Time 사용자 프로비저닝	<p>적절한 타사 ID 제공자를 사용하여 Just-in-Time 프로비저닝을 지원하는 적절한 옵션을 선택합니다.</p> <p>Just-in-Time 프로비저닝에 사용할 디렉토리 이름을 입력합니다.</p> <p>Just-in-Time 프로비저닝에 사용할 외부 ID 제공자 내에 있는 도메인을 하나 이상 입력합니다.</p>
네트워크	<p>서비스에 구성된 기존 네트워크 범위가 나열됩니다.</p> <p>사용자 IP 주소를 기반으로 사용자에게 대해 네트워크 범위(인증을 위해 이 ID 제공자 인스턴스로 전송할 네트워크 범위)를 선택합니다.</p>
인증 방법	타사 ID 제공자가 지원하는 인증 방법을 추가합니다. 인증 방법을 지원하는 SAML 인증 컨텍스트 클래스를 선택합니다.
SAML 서명 인증서	Directories Management SAML 서비스 제공자 메타데이터에 대한 URL을 보려면 SP(서비스 제공자) 메타데이터 를 클릭합니다. URL을 복사 및 저장합니다. 타사 ID 제공자의 SAML 어설션을 편집하여 Directories Management 사용자를 매핑할 경우 이 URL이 구성됩니다.
호스트 이름	호스트 이름 필드가 표시될 경우 인증을 위해 ID 제공자가 리디렉션되는 호스트 이름을 입력합니다. 443 이외의 비표준 포트를 사용할 경우 이를 호스트 이름:포트로 설정할 수 있습니다. 예를 들면 myco.example.com:8443입니다.

5 추가를 클릭합니다.

후속 작업

- 타사 ID 제공자 인스턴스를 구성하는 데 필요한 Directories Management 서비스 제공자 메타데이터를 복사 및 저장합니다. [ID 제공자 페이지]의 SAML 서명 인증서 섹션에서 이 메타데이터를 사용할 수 있습니다.
- ID 제공자의 인증 방법을 서비스 기본 정책에 추가합니다.

카탈로그에 추가할 리소스의 추가 및 사용자 지정에 대한 자세한 내용은 Directories Management에서 리소스 설정 가이드를 참조하십시오.

추가 작업 공간 ID 제공자 구성

사용자를 인증할 디렉토리 관리 커넥터를 구성하면 작업 공간 IDP가 생성되고, 암호 인증이 사용하도록 설정됩니다.

여러 로드 밸런서 뒤에서 작동하도록 추가 커넥터를 구성할 수 있습니다. 배포에 둘 이상의 로드 밸런서가 포함되어 있으면 각 로드 밸런서 구성에 인증을 위한 추가 작업 공간 ID 제공자를 구성할 수 있습니다.

프로시저

- 1 **관리 > 디렉토리 관리 > ID 제공자**를 선택합니다.
구성된 모든 ID 제공자가 이 페이지에 표시됩니다.
- 2 **ID 제공자 추가**를 클릭합니다.
ID 제공자 옵션이 있는 메뉴가 나타납니다.
- 3 **작업 공간 IDP 생성**을 선택합니다.
- 4 ID 제공자를 구성하는 데 필요한 적절한 정보를 입력합니다.

옵션	설명
ID 제공자 이름	이 기본 제공 ID 제공자 인스턴스의 이름을 입력합니다.
사용자	인증할 사용자를 선택합니다. 구성된 디렉토리가 나열됩니다.
사용자	이 작업 공간 ID 제공자를 사용하여 인증할 수 있는 사용자 그룹을 선택합니다.
네트워크	서비스에 구성된 기존 네트워크 범위가 나열됩니다. 인증을 위해 이 ID 제공자 인스턴스로 전송할 IP 주소를 기반으로 사용자에게 대한 네트워크 범위를 선택합니다.
인증 방법	서비스에 구성된 인증 방법이 표시됩니다. 이 ID 제공자에 연결할 인증 방법에 대한 확인란을 선택합니다. AirWatch 및 AirWatch Connector를 사용할 경우, 규정 준수 및 암호를 위해서는 AirWatch 구성 페이지에 해당 옵션이 사용하도록 설정되었는지 확인해야 합니다.

- 5 **추가**를 클릭합니다.

기본 제공 ID 제공자 연결 구성

기본 제공 ID 제공자를 여러 개 구성하고 이러한 ID 제공자에 인증 방법을 연결할 수 있습니다.

필수 조건

기본 제공 Kerberos 인증을 사용하는 경우 iOS 디바이스 관리 프로파일의 AirWatch 구성에서 사용할 KDC 발급자 인증서를 다운로드합니다.

프로시저

- 1 **관리 > 디렉토리 관리 > ID 제공자**를 선택합니다.
구성된 모든 ID 제공자가 이 페이지에 표시됩니다.
- 2 **ID 제공자 추가**를 클릭합니다.
ID 제공자 옵션이 있는 메뉴가 나타납니다.
- 3 **기본 제공 IDP 생성**을 선택합니다.

4 ID 제공자를 구성하는 데 필요한 적절한 정보를 입력합니다.

옵션	설명
ID 제공자 이름	이 기본 제공 ID 제공자 인스턴스의 이름을 입력합니다.
사용자	인증할 사용자를 선택합니다. 구성된 디렉토리가 나열됩니다.
네트워크	서비스에 구성된 기존 네트워크 범위가 나열됩니다. 인증을 위해 이 ID 제공자 인스턴스로 전송할 IP 주소를 기반으로 사용자에게 대한 네트워크 범위를 선택합니다.
인증 방법	서비스에 구성된 인증 방법이 표시됩니다. 이 ID 제공자에 연결할 인증 방법에 대한 확인란을 선택합니다. AirWatch 및 AirWatch Connector를 사용할 경우, 규정 준수 및 암호를 위해서는 AirWatch 구성 페이지에 적절한 옵션이 사용하도록 설정되었는지 확인해야 합니다.

5 추가를 클릭합니다.

대체 사용자 인증 제품을 디렉토리 관리와 통합

일반적으로 디렉토리 관리를 처음 구성할 경우 기존 vRealize Automation 인프라와 함께 제공되는 커넥터를 사용하여 사용자 ID 및 암호 기반의 인증 및 관리에 대한 Active Directory 연결을 생성합니다. 또는 디렉토리 관리를 Kerberos 또는 RSA SecurID와 같은 다른 인증 솔루션과 통합할 수 있습니다.

ID 제공자 인스턴스는 Directories Management connector 인스턴스, 타사 ID 제공자 인스턴스 또는 이 둘의 조합일 수 있습니다.

Directories Management 서비스에서 사용하는 ID 제공자 인스턴스는 SAML 2.0 어설션을 사용하여 서비스와 통신하는 네트워크 내부 페더레이션 기관을 만듭니다.

초기에 Directories Management 서비스를 배포할 때는 커넥터가 이 서비스의 초기 ID 제공자가 됩니다. 사용자 인증 및 관리에는 기존 Active Directory 인프라가 사용됩니다.

다음 인증 방법이 지원됩니다. 관리 콘솔에서 이러한 인증 방법을 구성할 수 있습니다.

표 2-8. 디렉토리 관리에서 지원하는 사용자 인증 유형

인증 유형	설명
암호(온-프레미스 배포)	Active Directory가 구성된 후 다른 구성 없이 Directories Management는 Active Directory 암호 인증을 지원합니다. 이 방법은 사용자를 직접 Active Directory에 대해 인증합니다.
데스크톱용 Kerberos	Kerberos 인증은 도메인 사용자에게 해당 애플리케이션 포털에 대한 단일 로그인 액세스를 제공합니다. 사용자는 네트워크에 로그인한 후 다시 로그인할 필요가 없습니다.
인증서(온-프레미스 배포)	클라이언트가 자신의 데스크톱 및 모바일 디바이스에서 인증서를 사용하여 인증하거나 스마트 카드 어댑터를 인증에 사용할 수 있도록 인증서 기반 인증을 구성할 수 있습니다. 인증서 기반 인증은 사용자가 소유한 항목과 사용자가 알고 있는 내용을 기반으로 합니다. X.509 인증서는 공용 키 인프라 표준을 사용하여 인증서 내에 포함된 공용 키가 사용자에게 속하는지 확인합니다.

표 2-8. 디렉토리 관리에서 지원하는 사용자 인증 유형 (계속)

인증 유형	설명
RSA SecurID(온-프레미스 배포)	RSA SecurID 인증이 구성된 경우 Directories Management는 RSA SecurID 서버에서 인증 에이전트로 구성됩니다. RSA SecurID 인증에서는 사용자가 토큰 기반 인증 시스템을 사용해야 합니다. RSA SecurID는 엔터프라이즈 네트워크 외부에서 Directories Management에 액세스하는 사용자를 위한 인증 방법입니다.
RADIUS(온-프레미스 배포)	RADIUS 인증은 2단계 인증 옵션을 제공합니다. Directories Management 서비스에 액세스할 수 있는 RADIUS 서버를 설정합니다. 사용자가 사용자 이름 및 암호를 사용하여 로그인할 경우 인증을 위해 액세스 요청이 RADIUS 서버에 제출됩니다.
RSA 어댑티브 인증(온-프레미스 배포)	RSA 인증은 사용자 이름 및 암호만으로 Active Directory에 대해 인증하는 것보다 더 강력한 다단계 인증을 제공합니다. RSA 어댑티브 인증이 사용하도록 설정된 경우 리스크 정책에 지정된 리스크 표시가 RSA 정책 관리 애플리케이션에 설정됩니다. 어댑티브 인증의 Directories Management 서비스 구성은 필요한 인증 프롬프트를 결정하는 데 사용됩니다.
모바일 SSO(iOS용)	iOS용 모바일 SSO 인증은 AirWatch 관리 iOS 디바이스의 Single Sign-On 인증에 사용됩니다. 모바일 SSO(iOS용) 인증에서는 Directories Management 서비스의 일부인 KDC(키 배포 센터)를 사용합니다. 이 인증 방법을 사용하도록 설정하려면 먼저 VMware Identity Manager 서비스에서 KDC 서비스를 초기화해야 합니다.
모바일 SSO(Android용)	Android용 모바일 SSO 인증은 AirWatch 관리 Android 디바이스의 Single Sign-On 인증에 사용됩니다. Directories Management 서비스와 AirWatch 간에 인증을 위해 AirWatch에서 인증서를 검색하는 프록시 서비스가 설정됩니다.
암호(AirWatch Connector)	사용자 암호 인증을 위해 AirWatch Cloud Connector를 Directories Management 서비스와 통합할 수 있습니다. AirWatch 디렉토리의 사용자를 동기화하도록 Directories Management 서비스를 구성합니다.

구성한 인증 방법, 기본 액세스 정책 규칙, 네트워크 범위 및 ID 제공자 인스턴스에 따라 사용자가 인증됩니다. 인증 방법을 구성한 후에는 디바이스 유형별로 사용할 인증 방법을 지정하는 액세스 정책 규칙을 만듭니다.

Directories Management 의 SecurID 구성

RSA SecurID 서버를 구성할 때 Directories Management 서비스 정보를 RSA SecurID 서버의 인증 에이전트로 추가하고 Directories Management 서비스에서 RSA SecurID 서버 정보를 구성해야 합니다.

추가적인 보안을 제공하기 위해 SecurID를 구성하는 경우 네트워크가 Directories Management 배포에 적절하게 구성되어 있는지 확인해야 합니다. 특히 SecurID의 경우, SecurID를 사용하여 네트워크 외부의 사용자를 인증하도록 적절한 포트가 열려 있는지 확인해야 합니다.

Directories Management 설치 마법사를 실행하고 Active Directory 연결을 구성했다면 RSA SecurID 서버 준비에 필요한 정보를 얻을 수 있습니다. Directories Management를 위한 RSA SecurID 서버를 준비한 후에는 관리 콘솔에서 SecurID를 사용하도록 설정합니다.

■ RSA SecurID 서버 준비

Directories Management 장치에 대한 정보를 인증 에이전트로 사용하여 RSA SecurID 서버를 구성해야 합니다. 필요한 정보는 네트워크 인터페이스의 호스트 이름 및 IP 주소입니다.

■ RSA SecurID 인증 구성

디렉토리 관리가 RSA SecurID 서버에서 인증 에이전트로 구성된 후 RSA SecurID 구성 정보를 커넥터에 추가해야 합니다.

RSA SecurID 서버 준비

Directories Management 장치에 대한 정보를 인증 에이전트로 사용하여 RSA SecurID 서버를 구성해야 합니다. 필요한 정보는 네트워크 인터페이스의 호스트 이름 및 IP 주소입니다.

필수 조건

- RSA Authentication Manager 버전 중 하나(RSA AM 6.1.2, 7.1 SP2 이상 또는 8.0 이상)가 엔터프라이즈 네트워크에 설치되어 작동하는지 확인합니다. Directories Management 서버는 AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51(Agent API 8.1 SP1)을 사용합니다. 이 항목은 이전 버전의 RSA Authentication Manager(RSA SecurID 서버)만 지원합니다. RSA Authentication Manager(RSA SecurID 서버)의 설치 및 구성에 대한 자세한 내용은 RSA 설명서를 참조하십시오.

프로시저

- 1 지원되는 버전의 RSA SecurID 서버에서 Directories Management 커넥터를 인증 에이전트로 추가합니다. 다음 정보를 입력합니다.

옵션	설명
호스트 이름	Directories Management의 호스트 이름입니다.
IP 주소	Directories Management의 IP 주소입니다.
대체 IP 주소	커넥터의 트래픽이 NAT(네트워크 주소 변환) 디바이스를 통해 RSA SecurID 서버에 도달하는 경우 장치의 개인 IP 주소를 입력합니다.

- 2 압축된 구성 파일을 다운로드하고 sdconf.rec 파일을 추출합니다.

Directories Management에서 RSA SecurID를 구성할 때 나중에 이 파일을 업로드하도록 준비하십시오.

후속 작업

관리 콘솔로 이동하고 [ID 및 액세스 관리] 탭([설정] 페이지)에서 커넥터를 선택하고, [AuthAdapters] 페이지에서 SecurID를 구성합니다.

RSA SecurID 인증 구성

디렉토리 관리가 RSA SecurID 서버에서 인증 에이전트로 구성된 후 RSA SecurID 구성 정보를 커넥터에 추가해야 합니다.

필수 조건

- RSA Authentication Manager(RSA SecurID 서버)가 설치되고 제대로 구성되어 있는지 확인합니다.
- RSA SecurID 서버에서 압축된 파일을 다운로드하고 서버 구성 파일을 추출합니다.

프로시저

- 1 테넌트 관리자로서 **관리 > 디렉토리 관리 > 커넥터**로 이동합니다.
- 2 [커넥터] 페이지에서 RSA SecurID로 구성 중인 커넥터의 작업자 링크를 선택합니다.
- 3 **인증 어댑터**를 클릭한 다음 **SecurIDIdpAdapter**를 클릭합니다.
ID 관리자 로그인 페이지로 리디렉션됩니다.
- 4 [인증 어댑터] 페이지의 SecurIDIdpAdapter 행에서 **편집**을 클릭합니다.
- 5 [SecurID 인증 어댑터] 페이지를 구성합니다.

RSA SecurID 서버에서 사용된 정보와 생성된 파일은 SecurID 페이지를 구성할 때 필요합니다.

옵션	작업
이름	이름은 필수입니다. 기본 이름은 SecurIDIdpAdapter입니다. 이 이름은 변경할 수 있습니다.
SecurID 사용	SecurID 인증을 사용하도록 설정하려면 이 확인란을 선택합니다.
허용된 인증 시도 수	RSA SecurID 토큰을 사용할 경우 최대 로그인 시도 실패 횟수를 입력합니다. 기본값은 5회입니다.
커넥터 주소	커넥터 인스턴스의 IP 주소를 입력합니다. 커넥터 장치를 인증 에이전트로 RSA SecurID 서버에 추가할 때 사용한 값과 입력한 값이 일치해야 합니다. RSA SecurID 서버에 대체 IP 주소 프롬프트에 할당된 값이 있는 경우 해당 값을 커넥터 IP 주소로 입력합니다. 대체 IP 주소가 할당되지 않은 경우 IP 주소 프롬프트에 할당된 값을 입력합니다.
에이전트 IP 주소	RSA SecurID 서버에서 IP 주소 프롬프트에 할당된 값을 입력합니다.
서버 구성	RSA SecurID 서버 구성 파일을 업로드합니다. 먼저 RSA SecurID 서버에서 압축된 파일을 다운로드하고 기본 이름이 sdconf.rec인 서버 구성 파일을 추출해야 합니다.
노드 암호	노드 암호 필드를 비워두면 노드 암호가 자동으로 생성됩니다. RSA SecurID 서버에서 노드 암호 파일을 지우고 노드 암호 파일을 의도적으로 업로드하지 않는 것이 좋습니다. RSA SecurID 서버의 노드 암호 파일과 서버 커넥터 인스턴스의 노드 암호 파일은 항상 일치해야 합니다. 한 위치에서 노드 암호를 변경한 경우 다른 위치에서도 변경해야 합니다.

- 6 **저장**을 클릭합니다.

후속 작업

인증 방법을 기본 액세스 정책에 추가합니다. **관리 > 디렉토리 관리 > 정책**으로 이동하고 **기본 정책 편집**을 클릭하여 SecurID 인증 방법이 올바른 인증 순서대로 규칙에 추가되도록 기본 정책 규칙을 편집합니다.

Directories Management 에 대한 RADIUS 구성

사용자가 RADIUS(Remote Authentication Dial-In User Service) 인증을 사용하도록 Directories Management를 구성할 수 있습니다. Directories Management 서비스에서 RADIUS 서버 정보를 구성합니다.

RADIUS 지원에서 다양한 대체 2단계 토큰 기반 인증 옵션을 제공합니다. RADIUS와 같은 2단계 인증 솔루션은 별도 서버에 설치된 인증 관리자와 작동하기 때문에 RADIUS 서버를 구성하고 ID 관리자 서비스에 액세스할 수 있도록 해야 합니다.

사용자가 [내 앱] 포털에 로그인하고 RADIUS 인증이 사용되도록 설정된 경우 브라우저에 특별한 로그인 대화상자가 표시됩니다. 사용자는 로그인 대화상자에 자신의 RADIUS 인증 사용자 이름 및 암호를 입력합니다. RADIUS 서버에서 액세스 암호를 요청할 경우 ID 관리자 서비스에서 두 번째 암호를 입력하라는 대화상자를 표시합니다. 현재 RADIUS 암호 요청에 대한 지원은 텍스트 입력을 요청하는 것으로 제한됩니다.

사용자가 대화상자에 자격 증명을 입력한 후 RADIUS 서버가 SMS 문자 메시지나 이메일 또는 일부 다른 대역 외 메커니즘을 사용한 텍스트를 코드와 함께 사용자 휴대폰으로 전송할 수 있습니다. 사용자는 이 텍스트 및 코드를 로그인 대화상자에 입력하여 인증을 완료할 수 있습니다.

RADIUS 서버가 Active Directory에서 사용자를 가져올 수 있는 기능을 제공할 경우 최종 사용자에게 RADIUS 인증 사용자 이름 및 암호를 입력하라는 메시지가 표시되기 전에 먼저 Active Directory 자격 증명을 제공하라는 메시지가 표시될 수 있습니다.

RADIUS 서버 준비

RADIUS 서버를 설정한 다음 Directories Management 서비스의 RADIUS 요청을 수락하도록 서버를 구성합니다.

RADIUS 서버 설정에 대한 자세한 내용은 RADIUS 벤더의 설정 가이드를 참조하십시오. RADIUS 구성 정보는 기록해 두십시오. 서비스에서 RADIUS를 구성할 때 이 정보를 사용하게 됩니다.

Directories Management를 구성하는 데 필요한 RADIUS 정보의 유형을 보려면 [디렉토리 관리에서 RADIUS 인증 구성](#) 항목을 참조하십시오.

고가용성에 사용될 보조 Radius 인증 서버를 설정할 수 있습니다. 기본 RADIUS 서버가 RADIUS 인증에 대해 구성된 서버 시간 제한 내에 응답하지 않으면 요청이 보조 서버로 라우팅됩니다. 기본 서버가 응답하지 않으면 보조 서버가 이후의 모든 인증 요청을 수신합니다.

디렉토리 관리에서 RADIUS 인증 구성

인증 관리자 서버에서 RADIUS 소프트웨어를 사용하도록 설정합니다. RADIUS 인증의 경우 벤더의 구성 설명서를 참조하십시오.

필수 조건

인증 관리자 서버에서 RADIUS 소프트웨어를 설치 및 구성합니다. RADIUS 인증의 경우 벤더의 구성 설명서를 참조하십시오.

서비스에서 RADIUS를 구성하려면 다음 RADIUS 서버 정보를 알고 있어야 합니다.

- RADIUS 서버의 IP 주소 또는 DNS 이름.
- 인증 포트 번호. 인증 포트는 일반적으로 1812입니다.
- 인증 유형. 인증 유형에는 PAP(암호 인증 프로토콜), CHAP(Challenge Handshake 인증 프로토콜), MSCHAP1, MSCHAP2(Microsoft Challenge Handshake 인증 프로토콜 버전 1 및 2)가 포함됩니다.
- RADIUS 프로토콜 메시지에서 암호화 및 암호 해독에 사용된 RADIUS 공유 암호.
- RADIUS 인증에 필요한 특정한 시간 초과 및 재시도 값.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 관리 > 디렉토리 관리 > 커넥터를 선택합니다.
- 2 [커넥터] 페이지에서 RADIUS 인증을 위해 구성 중인 커넥터의 작업자 링크를 선택합니다.
- 3 인증 어댑터를 클릭한 다음 **RadiusAuthAdapter**를 클릭합니다.
ID 관리자 로그인 페이지로 리디렉션됩니다.
- 4 편집을 클릭하여 [인증 어댑터] 페이지에서 이 필드를 구성합니다.

옵션	작업
이름	이름은 필수입니다. 기본 이름은 RadiusAuthAdapter입니다. 이 이름은 변경할 수 있습니다.
Radius 어댑터 사용	RADIUS 인증을 사용하도록 설정하려면 이 확인란을 선택합니다.
허용된 인증 시도 수	RADIUS를 사용하여 로그인할 경우 최대 로그인 시도 실패 횟수를 입력합니다. 기본값은 5회입니다.
Radius 서버에 대한 시도 횟수	총 재시도 횟수를 지정합니다. 기본 서버가 응답하지 않을 경우 서비스는 다시 재시도하기 전에 구성된 시간 동안 대기합니다.
Radius 서버 호스트 이름/주소	RADIUS 서버의 호스트 이름 또는 IP 주소를 입력합니다.
인증 포트	Radius 인증 포트 번호를 입력합니다. 일반적으로 1812입니다.
계정 포트	포트 번호에 0을 입력합니다. 지금은 계정 포트가 사용되지 않습니다.
인증 유형	RADIUS 서버에서 지원하는 인증 프로토콜을 입력합니다. PAP, CHAP, MSCHAP1 또는 MSCHAP2입니다.
공유 암호	RADIUS 서버와 VMware Identity Manager 서비스 간에 사용되는 공유 암호를 입력합니다.
서버 시간 초과(초)	RADIUS 서버 시간 초과(초)를 입력합니다. RADIUS 서버가 응답하지 않을 경우 해당 시간 초과 후 재시도를 전송합니다.
영역 접두사	(선택 사항) 사용자 계정 위치를 영역이라고 합니다. 영역 접두사 문자열을 지정할 경우 사용자 이름이 RADIUS 서버에 전송될 때 이름 시작 부분에 이 문자열이 배치됩니다. 예를 들어, 사용자 이름을 jdoe로 입력하고 영역 접두사 DOMAIN-A\를 지정한 경우 사용자 이름 DOMAIN-A\jdoe가 RADIUS 서버에 전송됩니다. 이 필드를 구성하지 않은 경우 입력한 사용자 이름만 전송됩니다.
영역 접미사	(선택 사항) 영역 접미사를 지정한 경우 사용자 이름 끝에 이 문자열이 배치됩니다. 예를 들어, 접미사가 @myco.com인 경우 사용자 이름 jdoe@myco.com이 RADIUS 서버에 전송됩니다.
로그인 페이지 암호 힌트	사용자가 올바른 Radius 암호를 입력하도록 안내하기 위해 사용자 로그인 페이지의 메시지에 표시할 텍스트 문자열을 입력합니다. 예를 들어, 처음에는 AD 암호, 그 다음에는 SMS 암호 를 사용하여 이 필드를 구성한 경우 로그인 페이지 메시지는 다음과 같습니다. AD 암호를 먼저 입력한 다음 SMS 암호를 입력하십시오. 기본 텍스트 문자열은 RADIUS 암호 입니다.

- 5 고가용성을 위해 보조 RADIUS 서버를 사용하도록 설정할 수 있습니다.
4단계에서 설명한 대로 보조 서버를 구성합니다.
- 6 저장을 클릭합니다.

후속 작업

RADIUS 인증 방법을 기본 액세스 정책에 추가합니다. **관리 > 디렉토리 관리 > 정책**을 선택하고 **기본 정책 편집**을 클릭하여 RADIUS 인증 방법이 올바른 인증 순서대로 규칙에 추가되도록 기본 정책 규칙을 편집합니다.

Directories Management 와 함께 사용할 인증서 또는 스마트 카드 어댑터 구성

클라이언트가 자신의 데스크톱 및 모바일 디바이스에서 인증서를 사용하여 인증하거나 스마트 카드 어댑터를 인증에 사용할 수 있도록 x509 인증서 인증을 구성할 수 있습니다. 인증서 기반 인증은 사용자가 갖고 있는 항목(개인 키 또는 스마트 카드) 및 사람들이 알고 있는 내용(개인 키에 대한 암호 또는 스마트 카드 PIN)을 기반으로 합니다. X.509 인증서는 PKI(공용 키 인프라) 표준을 사용하여 인증서 내에 포함된 공용 키가 사용자에게 속하는지 확인합니다. 스마트 카드 인증을 사용하여 사용자는 스마트 카드를 컴퓨터와 연결하고 PIN을 입력합니다.

스마트 카드 인증서는 사용자 컴퓨터의 로컬 인증서 저장소로 복사됩니다. 일부 예외가 있지만, 로컬 인증서 저장소의 인증서를 이 사용자의 컴퓨터에서 실행 중인 모든 브라우저에 사용할 수 있으며, 따라서 브라우저의 Directories Management 인스턴스에 사용할 수 있습니다.

■ 인증서 인증을 위한 사용자 계정 이름 사용

Active Directory에서 인증서 매핑을 사용할 수 있습니다. 인증서 및 스마트 카드 로그인에서는 Active Directory의 UPN(사용자 계정 이름)을 사용하여 사용자 계정의 유효성을 검사합니다. Directories Management 서비스에서 인증을 시도하는 사용자의 Active Directory 계정에는 인증서의 UPN에 해당하는 유효한 UPN이 있어야 합니다.

■ 인증에 필요한 인증 기관

인증서 인증을 사용한 로그인을 사용하도록 설정하려면 루트 인증서와 중간 인증서를 Directories Management에 업로드해야 합니다.

■ 인증서 해지 검사 사용

인증서가 해지된 사용자가 인증하지 못하도록 인증서 해지 검사를 구성할 수 있습니다. 사용자가 조직을 떠나거나, 스마트 카드를 분실하거나, 다른 부서로 이동한 경우 주로 인증서가 해지됩니다.

■ 디렉토리 관리를 위한 인증서 인증 구성

vRealize Automation 관리 콘솔 디렉토리 관리 기능에서 인증서 인증을 사용하도록 설정하고 구성합니다.

인증서 인증을 위한 사용자 계정 이름 사용

Active Directory에서 인증서 매핑을 사용할 수 있습니다. 인증서 및 스마트 카드 로그인에서는 Active Directory의 UPN(사용자 계정 이름)을 사용하여 사용자 계정의 유효성을 검사합니다. Directories Management 서비스에서 인증을 시도하는 사용자의 Active Directory 계정에는 인증서의 UPN에 해당하는 유효한 UPN이 있어야 합니다.

인증서에 UPN이 없을 경우 Directories Management 가 이메일 주소를 사용하여 사용자 계정을 검증하도록 구성할 수 있습니다.

또한 대체 UPN 유형을 사용하도록 설정할 수도 있습니다.

인증에 필요한 인증 기관

인증서 인증을 사용한 로그인을 사용하도록 설정하려면 루트 인증서와 중간 인증서를 Directories Management에 업로드해야 합니다.

인증서가 사용자 컴퓨터의 로컬 인증서 저장소에 복사됩니다. 일부 예외를 제외하고, 로컬 인증서 저장소의 인증서를 이 사용자 컴퓨터에서 실행되는 모든 브라우저에서 사용할 수 있으므로 이를 브라우저의 Directories Management 인스턴스에서 사용할 수 있습니다.

스마트 카드 인증의 경우 사용자가 Directories Management 인스턴스에 대한 연결을 시작할 때 Directories Management 서비스는 신뢰할 수 있는 CA(인증 기관)의 목록을 브라우저에 전송합니다. 브라우저가 사용 가능한 사용자 인증서에 대해 신뢰할 수 있는 CA의 목록을 검사하고 적합한 인증서를 선택한 다음 스마트 카드 PIN을 입력하라는 메시지를 사용자에게 표시합니다. 사용할 수 있는 유효한 사용자 인증서가 여러 개인 경우 브라우저에서 인증서를 선택하라는 메시지를 사용자에게 표시합니다.

사용자가 인증할 수 없다면 루트 CA와 중간 CA가 제대로 설정되지 않았거나 루트 CA와 중간 CA가 서버에 업로드된 후 서비스를 다시 시작하지 않은 경우입니다. 이러한 경우 브라우저는 설치된 인증서를 표시할 수 없고, 사용자는 올바른 인증서를 선택할 수 없으며, 인증서 인증은 실패합니다.

인증서 해지 검사 사용

인증서가 해지된 사용자가 인증하지 못하도록 인증서 해지 검사를 구성할 수 있습니다. 사용자가 조직을 떠나거나, 스마트 카드를 분실하거나, 다른 부서로 이동한 경우 주로 인증서가 해지됩니다.

CRL(인증서 해지 목록) 및 OCSP(온라인 인증서 상태 프로토콜)가 포함된 인증서 해지 검사는 지원됩니다. CRL은 인증서를 발행한 CA에서 게시한 해지된 인증서 목록입니다. OCSP는 인증서의 해지 상태를 가져오기 위해 사용하는 인증서 검증 프로토콜입니다.

인증서 인증을 구성할 때 관리 콘솔의 [커넥터] > [인증 어댑터] > [CertificateAuthAdapter] 페이지에서 인증서 해지 검사를 구성할 수 있습니다.

동일한 인증서 인증 어댑터 구성에서 CRL 및 OCSP를 둘 다 구성할 수 있습니다. 두 가지 유형의 인증서 해지 검사를 구성하고 [OCSP 실패 시 CRL 사용] 확인란을 선택한 경우, OCSP가 먼저 검사되고 OCSP가 실패한 경우 해지 검사가 CRL로 폴백됩니다. CRL이 실패한 경우 해지 검사가 OCSP로 폴백되지 않습니다.

CRL 검사를 사용하는 상태에서 로그인

인증서 해지를 사용하도록 설정한 경우 Directories Management 서버는 CRL을 읽어서 사용자 인증서의 해지 상태를 확인합니다.

인증서가 해지된 경우 인증서를 통한 인증이 실패합니다.

OCSP 인증서 검사를 사용하는 상태에서 로그인

OCSP(온라인 인증서 상태 프로토콜) 해지 검사를 구성한 경우 Directories Management 는 OCSP 응답자에게 요청을 전송하여 특정 사용자 인증서의 해지 상태를 확인합니다.

Directories Management 서버는 OCSP 서명 인증서를 사용하여 OCSP 응답자로부터 받은 응답이 올바른지 확인합니다.

인증서가 해지된 경우 인증이 실패합니다.

OSCP 응답자로부터 응답을 받지 못하거나 응답이 올바르지 않은 경우 CRL 검사로 폴백되도록 인증을 구성할 수 있습니다.

디렉토리 관리를 위한 인증서 인증 구성

vRealize Automation 관리 콘솔 디렉토리 관리 기능에서 인증서 인증을 사용하도록 설정하고 구성합니다.

필수 조건

- 사용자가 제공한 인증서를 서명한 CA에서 루트 인증서와 중간 인증서를 가져옵니다.
- (선택 사항) 인증서 인증을 위한 유효한 인증서 정책의 OID(개체 식별자) 목록.
- 해지 검사의 경우 CRL의 파일 위치, OCSP 서버의 URL.
- (선택 사항) OCSP 응답 서명 인증서 파일 위치.
- 인증 전에 동의 양식 표시를 사용하도록 설정한 경우, 동의 양식 콘텐츠.

프로시저

- 1 테넌트 관리자로서 **관리 > 디렉토리 관리 > 커넥터**로 이동합니다.
- 2 [커넥터] 페이지에서, 구성 중인 커넥터의 작업자 링크를 선택합니다.
- 3 **인증 어댑터**를 클릭한 다음 **CertificateAuthAdapter**를 클릭합니다.
ID 관리자 로그인 페이지로 리디렉션됩니다.
- 4 CertificateAuthAdapter 행에서 **편집**을 클릭합니다.
- 5 [인증서 인증 어댑터] 페이지를 구성합니다.

참고 별표(*)는 필수 필드를 나타냅니다. 다른 모든 필드는 선택 사항입니다.

옵션	설명
*이름	이름은 필수입니다. 기본 이름은 CertificateAuthAdapter입니다. 이 이름은 변경할 수 있습니다.
인증서 어댑터 사용	인증서 인증을 사용하도록 설정하려면 확인란을 선택합니다.
*루트 및 중간 CA 인증서	업로드할 인증서 파일을 선택합니다. DER 또는 PEM으로 인코딩된 여러 루트 CA 및 중간 CA 인증서를 선택할 수 있습니다.
업로드된 CA 인증서	업로드된 인증서 파일이 양식의 [업로드된 CA 인증서] 섹션에 나열됩니다. 새 인증서를 사용하려면 먼저 서비스를 다시 시작해야 합니다. 웹 서비스 다시 시작 을 클릭하여 서비스를 다시 시작하고 인증서를 신뢰할 수 있는 서비스에 추가합니다.
참고 서비스를 다시 시작해도 인증서 인증이 사용되도록 설정되지 않습니다. 서비스를 다시 시작한 후 이 페이지 구성을 계속하십시오. 페이지 끝에서 저장 을 클릭하면 서비스에서 인증서 인증이 사용되도록 설정됩니다.	
인증서에 UPN이 없는 경우 이메일 사용	UPN(사용자 계정 이름)이 인증서에 없는 경우 이 확인란을 선택하여 emailAddress 특성을 주체 대체 이름 확장으로 사용하여 사용자 계정을 검사합니다.

옵션	설명
수락된 인증서 정책	인증서 정책 확장에서 수락된 개체 ID 목록을 생성합니다. 인증서 발급 정책에 대한 OID(개체 ID 번호)를 입력합니다. 다른 값 추가 를 클릭하여 추가 OID를 추가합니다.
인증서 해지 사용	인증서 해지 검사를 사용하도록 설정하려면 이 확인란을 선택합니다. 이 경우 사용자 인증서를 해지한 사용자는 인증되지 않습니다.
인증서의 CRL 사용	인증서를 발급한 CA에서 게시한 CRL(인증서 해지 목록)을 사용하여 인증서 상태(해지됨 또는 해지 안됨)를 확인하려면 이 확인란을 선택합니다.
CRL 위치	CRL을 검색할 서버 파일 경로 또는 로컬 파일 경로를 입력합니다.
OCSP 해지 사용	OCSP(온라인 인증서 상태 프로토콜) 인증서 검증 프로토콜을 사용하여 인증서의 해지 상태를 가져오려면 이 확인란을 선택합니다.
OCSP 실패 시 CRL 사용	CRL 및 OCSP를 둘 다 구성한 경우, 이 확인란을 선택하여 OCSP 검사를 사용할 수 없는 경우 CRL 사용으로 폴백할 수 있습니다.
OCSP Nonce 전송	OCSP 요청의 고유한 식별자를 응답으로 전송하려면 이 확인란을 선택합니다.
OCSP URL	OCSP 해지를 사용하도록 설정한 경우 해지 검사를 위한 OCSP 서버 주소를 입력합니다.
OCSP 응답자의 서명 인증서	응답자에 대한 OCSP 인증서 경로(/path/to/file.cer)를 입력합니다.
인증 전에 동의 양식 사용	사용자가 인증서 인증을 사용하여 [내 앱] 포털에 로그인하기 전에 표시할 동의 양식 페이지를 포함하려면 이 확인란을 선택합니다.
동의 양식 콘텐츠	동의 양식에 표시되는 텍스트를 이 텍스트 상자에 입력합니다.

6 저장을 클릭합니다.

후속 작업

- 인증서 인증 방법을 기본 액세스 정책에 추가합니다. **관리 > 디렉토리 관리 > 정책**으로 이동하고 **기본 정책 편집**을 클릭하여 기본 정책 규칙을 편집하고 인증서를 추가한 다음, 해당 인증서를 기본 정책에 대한 첫 번째 인증 방법으로 설정합니다. 인증서가 정책 규칙에 나열된 첫 번째 인증 방법이어야 합니다. 그렇지 않으면 인증서 인증이 실패합니다.
- 인증서 인증이 구성되고 서비스 장치가 로드 밸런서 뒤에 설정된 경우 Directories Management connector가 로드 밸런서에서 SSL 패스스루를 사용하여 구성되고 로드 밸런서에서 SSL을 종료하도록 구성되지 않았는지 확인합니다. 이 구성을 통해 커넥터와 클라이언트 간에 SSL 핸드셰이크가 수행되어 인증서가 커넥터로 전달됩니다.

사용자를 인증하도록 타사 ID 제공자 인스턴스 구성

Directories Management 서비스에서 사용자를 인증하는 데 사용할 타사 ID 제공자를 구성할 수 있습니다.

관리 콘솔을 사용하여 타사 ID 제공자 인스턴스를 추가하기 전에 다음 작업을 완료합니다.

- 타사 인스턴스가 SAML 2.0을 준수하는지, 서비스가 타사 인스턴스에 연결할 수 있는지 확인합니다.
- 관리 콘솔에서 ID 제공자를 구성할 때 추가할 적절한 타사 메타데이터 정보를 가져옵니다. 타사 인스턴스에서 가져오는 메타데이터 정보는 메타데이터에 대한 URL이거나 실제 메타데이터입니다.

타사 ID 제공자 연결 구성

vRealize Automation에는 기본 ID 제공자 연결 인스턴스가 제공됩니다. 사용자는 Just-in-Time 사용자 프로비저닝 또는 기타 사용자 지정 구성을 지원하도록 추가 ID 제공자 연결을 생성하고자 할 수 있습니다.

vRealize Automation에는 기본 ID 제공자가 제공됩니다. 대부분의 경우 고객의 요구에 기본 제공자면 충분합니다. 기존 엔터프라이즈 ID 관리 솔루션을 사용하는 경우 사용자 지정 ID 제공자를 설정하여 사용자를 기존 ID 솔루션으로 리디렉션할 수 있습니다.

사용자 지정 ID 제공자를 사용하는 경우 디렉토리 관리는 해당 제공자의 SAML 메타데이터를 사용하여 제공자와의 신뢰 관계를 설정합니다. 이 관계가 설정된 후 디렉토리 관리는 주체 이름 ID에 기반하여 SAML 어설션의 사용자를 내부 vRealize Automation 사용자 목록에 매핑합니다.

필수 조건

- 인증을 위해 이 ID 제공자 인스턴스로 전송할 네트워크 범위를 구성합니다. [네트워크 범위 추가 또는 편집](#) 항목을 참조하십시오.
- 타사 메타데이터 문서에 액세스합니다. 메타데이터 URL 또는 실제 메타데이터일 수 있습니다.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 디렉토리 관리 > ID 제공자**를 선택합니다.
구성된 모든 ID 제공자가 이 페이지에 표시됩니다.
- 2 **ID 제공자 추가**를 클릭합니다.
ID 제공자 옵션이 있는 메뉴가 나타납니다.
- 3 **타사 IDP 생성**을 선택합니다.
- 4 ID 제공자를 구성하는 데 필요한 적절한 정보를 입력합니다.

옵션	설명
ID 제공자 이름	이 ID 제공자 인스턴스의 이름을 입력합니다.
SAML 메타데이터	<p>타사 IdP XML 기반 메타데이터 문서를 추가하여 ID 제공자와 신뢰를 설정합니다.</p> <ol style="list-style-type: none"> 1 SAML 메타데이터 URL 또는 xml 콘텐츠를 텍스트 상자에 입력합니다. 2 프로세스 IdP 메타데이터를 클릭합니다. IdP에서 지원하는 NameID 형식이 메타데이터에서 추출되어 이름 ID 형식 테이블에 추가됩니다. 3 이름 ID 값 열에서, 표시된 ID 형식에 매핑할 서비스의 사용자 특성을 선택합니다. 사용자 지정 타사 이름 ID 형식을 추가하고 이를 서비스의 사용자 특성 값에 매핑할 수 있습니다. 4 (선택사항) NameIDPolicy 응답 식별자 문자열 형식을 선택합니다.
사용자	이 ID 제공자를 사용하여 인증할 수 있는 사용자의 Directories Management 디렉토리를 선택합니다.
Just-in-Time 사용자 프로비저닝	<p>적절한 타사 ID 제공자를 사용하여 Just-in-Time 프로비저닝을 지원하는 적절한 옵션을 선택합니다.</p> <p>Just-in-Time 프로비저닝에 사용할 디렉토리 이름을 입력합니다.</p> <p>Just-in-Time 프로비저닝에 사용할 외부 ID 제공자 내에 있는 도메인을 하나 이상 입력합니다.</p>

옵션	설명
네트워크	서비스에 구성된 기존 네트워크 범위가 나열됩니다. 사용자 IP 주소를 기반으로 사용자에게 대해 네트워크 범위(인증을 위해 이 ID 제공자 인스턴스로 전송할 네트워크 범위)를 선택합니다.
인증 방법	타사 ID 제공자가 지원하는 인증 방법을 추가합니다. 인증 방법을 지원하는 SAML 인증 컨텍스트 클래스를 선택합니다.
SAML 서명 인증서	Directories Management SAML 서비스 제공자 메타데이터에 대한 URL을 보려면 SP(서비스 제공자) 메타데이터 를 클릭합니다. URL을 복사 및 저장합니다. 타사 ID 제공자의 SAML 어설션을 편집하여 Directories Management 사용자를 매핑할 경우 이 URL이 구성됩니다.
호스트 이름	호스트 이름 필드가 표시될 경우 인증을 위해 ID 제공자가 리디렉션되는 호스트 이름을 입력합니다. 443 이외의 비표준 포트를 사용할 경우 이를 호스트 이름:포트로 설정할 수 있습니다. 예를 들면 myco.example.com:8443입니다.

5 추가를 클릭합니다.

후속 작업

- 타사 ID 제공자 인스턴스를 구성하는 데 필요한 Directories Management 서비스 제공자 메타데이터를 복사 및 저장합니다. [ID 제공자 페이지]의 SAML 서명 인증서 섹션에서 이 메타데이터를 사용할 수 있습니다.
- ID 제공자의 인증 방법을 서비스 기본 정책에 추가합니다.

카탈로그에 추가할 리소스의 추가 및 사용자 지정에 대한 자세한 내용은 Directories Management에서 리소스 설정 가이드를 참조하십시오.

사용자에게 적용하기 위한 인증 방법 관리

Directories Management 서비스는 사용자가 구성하는 인증 방법, 기본 액세스 정책, 네트워크 범위 및 ID 제공자 인스턴스를 기반으로 사용자를 인증하려고 합니다.

사용자가 로그인하려고 하면 서비스가 기본 액세스 정책 규칙을 평가하여 적용할 정책의 규칙을 선택합니다. 인증 방법이 규칙에 나열된 순서대로 적용됩니다. 규칙의 인증 방법 및 네트워크 범위 요구 사항을 충족하는 첫 번째 ID 제공자 인스턴스가 선택되고 사용자 인증 요청이 인증을 위해 ID 제공자 인스턴스로 전달됩니다. 인증이 실패하는 경우 규칙에서 구성된 다음 인증 방법이 적용됩니다.

디바이스 유형별 또는 특정 네트워크 범위에서 디바이스 유형별로 인증 방법을 사용하도록 지정하는 규칙을 추가할 수 있습니다. 예를 들어 사용자가 특정 네트워크에서 iOS 디바이스를 사용하여 RSA SecurID로 인증해야 하는 규칙과 내부 네트워크 IP 주소에서 로그인하는 모든 디바이스 유형을 암호로 인증하도록 지정하는 규칙을 구성할 수 있습니다.

네트워크 범위 추가 또는 편집

네트워크 범위를 관리하여 사용자가 Active Directory 링크를 통해 로그인할 수 있는 IP 주소를 정의할 수 있습니다. 생성한 네트워크 범위를 특정 ID 제공자 인스턴스 및 액세스 정책 규칙에 추가합니다.

네트워크 토폴로지를 기반으로 Directories Management 배포의 네트워크 범위를 정의합니다.

ALL RANGES라고 하는 하나의 네트워크 범위가 기본값으로 생성됩니다. 이 네트워크 범위에는 인터넷에서 사용 가능한 모든 IP 주소(0.0.0.0 ~ 255.255.255.255)가 포함됩니다. 배포에 단일 ID 제공자 인스턴스가 있는 경우에도 IP 주소 범위를 변경하고 다른 범위를 추가하여 특정 IP 주소를 기본 네트워크 범위에 포함하거나 제외할 수 있습니다. 특정한 용도에 적용할 수 있는 특정 IP 주소를 사용하여 다른 네트워크 범위를 생성할 수 있습니다.

참고 기본 네트워크 범위인 ALL RANGES 및 해당 설명("모든 범위의 네트워크")은 편집할 수 있습니다. [네트워크 범위] 페이지에서 네트워크 범위 이름을 클릭하여 이름 및 설명을 편집할 뿐 아니라 텍스트를 다른 언어로 변경할 수도 있습니다.

필수 조건

- vRealize Automation 배포를 위한 테넌트를 구성했고 기본 Active Directory 사용자 ID 및 암호 인증을 지원하는 적절한 Active Directory 링크를 설정했습니다.
- 네트워크에서 사용할 Active Directory를 설치하고 구성합니다.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 디렉토리 관리 > 네트워크 범위**를 선택합니다.
- 2 기존 네트워크 범위를 편집하거나 새 네트워크 범위를 추가합니다.

옵션	설명
기존 범위 편집	편집할 네트워크 범위 이름을 클릭합니다.
범위 추가	네트워크 범위 추가 를 클릭하여 새 범위를 추가합니다.

- 3 양식을 작성합니다.

양식 항목	설명
이름	네트워크 범위의 이름을 입력합니다.
설명	네트워크 범위의 설명을 입력합니다.
View 포트	View 모듈을 사용하도록 설정한 경우에만 View 포트 옵션이 표시됩니다. 클라이언트 액세스 URL 호스트. 네트워크 범위에 대한 올바른 Horizon Client 액세스 URL을 입력합니다. 클라이언트 액세스 포트. 네트워크 범위에 대한 올바른 Horizon Client 액세스 포트 번호를 입력합니다.
IP 범위	원하는 모든 IP 주소가 포함되고 원하지 않는 모든 IP 주소가 제외될 때까지 IP 범위를 편집 또는 추가합니다.

후속 작업

- 각 네트워크 범위를 ID 제공자 인스턴스와 연결합니다.
- 네트워크 범위를 액세스 정책 규칙과 적절하게 연결합니다. [액세스 정책 설정 구성](#) 항목을 참조하십시오.

디렉토리와의 동기화를 위해 특성 선택

Active Directory와의 동기화를 위해 Directories Management 디렉토리를 설정하는 경우 디렉토리로 동기화되는 사용자 특성을 지정합니다. 디렉토리를 설정하기 전에 [사용자 특성] 페이지에서 필요한 기본 특성을 지정하고, 원하는 경우 Active Directory 특성으로 매핑하려는 추가 특성을 추가할 수 있습니다.

디렉토리가 생성되기 전에 [사용자 특성] 페이지를 구성한 경우 기본 특성을 필수에서 필수 아님으로 변경하거나, 특성을 필수로 표시하거나, 사용자 지정 특성을 추가할 수 있습니다.

매핑되는 기본 특성에 대한 목록은 [Active Directory에서 동기화하는 사용자 특성 관리](#) 항목을 참조하십시오.

디렉토리가 생성되면 필수 특성을 필수 아님으로 변경하고 사용자 지정 특성을 삭제할 수 있습니다. 특성을 필수 특성으로 변경할 수는 없습니다.

디렉토리에 동기화할 다른 특성을 추가한 경우 디렉토리가 생성된 후 디렉토리의 [매핑된 특성] 페이지로 이동하여 해당 특성을 Active Directory 특성에 매핑합니다.

프로시저

- 1 vRealize Automation에 시스템 또는 테넌트 관리자로 로그인합니다.
- 2 [관리] 탭을 클릭합니다.
- 3 **디렉토리 관리 > 사용자 특성**을 선택합니다.
- 4 [기본 특성] 섹션에서 필수 특성 목록을 검토하고 필수로 지정해야 하는 특성을 반영하도록 적절하게 변경합니다.
- 5 [특성] 섹션에서 Directories Management 디렉토리 특성 이름을 목록에 추가합니다.
- 6 **저장**을 클릭합니다.
기본 특성 상태가 업데이트되고 추가한 특성이 디렉토리의 [매핑된 특성] 목록에 추가됩니다.
- 7 디렉토리가 생성되었으면 [ID 저장소] 페이지로 이동하고 디렉토리를 선택합니다.
- 8 **동기화 설정 > 매핑된 특성**을 클릭합니다.
- 9 추가한 특성에 대한 드롭다운 메뉴에서 매핑할 Active Directory 특성을 선택합니다.
- 10 **저장**을 클릭합니다.

다음에 디렉토리가 Active Directory로 동기화될 때 디렉토리가 업데이트됩니다.

기본 액세스 정책 적용

Directories Management 서비스에는 애플리케이션 포털에 대한 사용자 액세스를 제어하는 기본 액세스 정책이 포함되어 있습니다. 정책을 편집하여 필요에 따라 정책 규칙을 변경할 수 있습니다.

암호 인증 외의 인증 방법을 사용하도록 설정한 경우에는 기본 정책을 편집하여 사용 설정된 인증 방법을 정책 규칙에 추가해야 합니다.

기본 액세스 정책의 각 규칙에서 애플리케이션 포털에 대한 사용자 액세스를 허용하려면 일련의 기준이 충족되어야 합니다. 네트워크 범위를 적용하고 콘텐츠에 액세스할 수 있는 사용자의 유형을 선택하고 사용할 인증 방법을 선택합니다. [액세스 정책 관리](#) 항목을 참조하십시오.

서비스가 수행하는 사용자 로그인 시도 횟수는 지정된 인증 방법에 따라 다릅니다. Kerberos 또는 인증서 인증의 경우에는 서비스가 단 1회의 인증만 시도합니다. 사용자 로그인에 성공하지 못한 경우 규칙의 다음 인증 방법이 시도됩니다. Active Directory 암호 및 RSA SecurID 인증의 경우 실패한 최대 로그인 시도 횟수는 기본적으로 5회로 설정됩니다. 사용자가 5회의 로그인 시도에 실패한 경우 서비스는 목록의 다음 인증 방법을 사용하여 사용자 로그인을 시도합니다. 인증 방법이 모두 사용된 경우 서비스는 오류 메시지를 표시합니다.

정책 규칙에 인증 방법 적용

기본 정책 규칙에는 암호 인증 방법만 구성되어 있습니다. 구성한 다른 인증 방법을 선택하고 인증 방법이 인증에 사용되는 순서를 설정하려면 정책 규칙을 편집해야 합니다.

필수 조건

조직에서 지원하는 인증 방법을 사용하도록 설정하고 구성합니다. [대체 사용자 인증 제품을 디렉토리 관리와 통합](#)의 내용을 참조하십시오.

프로시저

- 1 **관리 > 디렉토리 관리 > 정책**을 선택합니다.
- 2 편집할 기본 액세스 정책을 클릭합니다.
- 3 정책 규칙을 편집하려면 [정책 규칙], [인증 방법] 열에서 편집할 인증 방법을 클릭합니다.
새 정책 규칙을 추가하려면 + (추가) 아이콘을 클릭합니다.
- 4 [정책] 페이지에서 **저장**을 클릭한 다음, 다시 **저장**을 클릭합니다.

정책 규칙 편집

사용자의 네트워크 범위가

모든 범위

이고 사용자가 다음 위치에서 콘텐츠에 액세스하는 경우

웹 브라우저

사용해야 하는 인증 방법...

Password

▼

및

▼

▼

앞의 인증 방법이 실패할 경우

-인증 방법 선택-

▼

만

▼

+ 플백 방법

다음 시간 후에 재인증:

8

시간

- 5 **저장**을 클릭하고 정책 페이지에서 **저장**을 다시 클릭합니다.

Directories Management 에 대한 Kerberos 구성

Kerberos 인증은 Active Directory 도메인에 로그인한 사용자가 추가 인증 없이 해당 애플리케이션 포털에 액세스할 수 있도록 합니다. Windows 인증을 사용하도록 설정하여 Kerberos 프로토콜이 사용자 브라우저와 Directories Management 서비스 간 상호 작용을 보호하도록 허용합니다. Kerberos 기능이 배포에서 작동하도록 직접 Active Directory를 구성할 필요는 없습니다.

현재 사용자 브라우저와 서비스 간의 상호 작용은 Windows 운영 체제에서만 Kerberos에 의해 인증됩니다. 다른 운영 체제에서 서비스에 액세스하는 경우에는 Kerberos 인증을 사용하지 않습니다.

■ Kerberos 인증 구성

Kerberos 인증을 제공하도록 Directories Management 서비스를 구성하려면 도메인에 가입하여 Directories Management 커넥터에서 Kerberos 인증을 사용하도록 설정해야 합니다.

■ 웹 인터페이스에 액세스하도록 Internet Explorer 구성

배포에 대해 Kerberos가 구성된 경우, 그리고 Internet Explorer를 사용하여 웹 인터페이스에 액세스할 수 있는 권한을 사용자에게 부여할 경우 Internet Explorer 브라우저를 구성해야 합니다.

■ 웹 인터페이스에 액세스하도록 Firefox 구성

배포에 대해 Kerberos가 구성된 경우, 그리고 Firefox를 사용하여 웹 인터페이스에 액세스할 수 있는 권한을 사용자에게 부여할 경우 Firefox 브라우저를 구성해야 합니다.

■ 웹 인터페이스에 액세스하도록 Chrome 브라우저 구성

배포에 대해 Kerberos가 구성된 경우, 그리고 Chrome 브라우저를 사용하여 웹 인터페이스에 액세스할 수 있는 권한을 사용자에게 부여할 경우 Chrome 브라우저를 구성해야 합니다.

Kerberos 인증 구성

Kerberos 인증을 제공하도록 Directories Management 서비스를 구성하려면 도메인에 가입하여 Directories Management 커넥터에서 Kerberos 인증을 사용하도록 설정해야 합니다.

프로시저

- 1 테넌트 관리자로서 **관리 > 디렉토리 관리 > 커넥터**로 이동합니다.
- 2 [커넥터] 페이지에서, Kerberos 인증을 위해 구성 중인 커넥터의 경우 **도메인 가입**을 클릭합니다.

3 [도메인 가입] 페이지에서 Active Directory 도메인에 대한 정보를 입력합니다.

옵션	설명
도메인	Active Directory의 정규화된 도메인 이름을 입력합니다. 입력하는 도메인 이름은 커넥터 서버와 동일한 Windows 도메인이어야 합니다.
도메인 사용자	Active Directory의 계정(시스템을 해당 Active Directory 도메인에 가입시킬 수 있는 권한을 가진 계정)에 대한 사용자 이름을 입력합니다.
도메인 암호	AD 사용자 이름과 연결된 암호를 입력합니다. 이 암호는 Directories Management에서 저장하지 않습니다.

저장을 클릭합니다.

[도메인 가입] 페이지가 새로 고쳐지고 사용자가 현재 도메인에 가입되었음을 나타내는 메시지가 표시됩니다.

4 커넥터의 [작업자] 열에서 인증 어댑터를 클릭합니다.

5 KerberosLdpAdapter를 클릭합니다.

ID 관리자 로그인 페이지로 리디렉션됩니다.

6 KerberosLdpAdapter 행에서 편집을 클릭하고 Kerberos 인증 페이지를 구성합니다.

옵션	설명
이름	이름은 필수입니다. 기본 이름은 KerberosLdpAdapter입니다. 이 이름은 변경할 수 있습니다.
디렉토리 UID 특성	사용자 이름을 포함하는 계정 특성을 입력합니다.
Windows 인증 사용	사용자 브라우저와 Directories Management 간에서 인증 상호 작용을 확장하려면 이 옵션을 선택합니다.
NTLM 사용	사용 중인 Active Directory 인프라에서 NTLM 인증을 사용할 경우에만 이 옵션을 선택하여 NTLM(NT LAN Manager) 프로토콜 기반 인증을 사용하도록 설정합니다.
리디렉션 사용	라운드 로빈 DNS 및 로드 밸런서에 Kerberos 지원이 없는 경우 이 옵션을 선택합니다. 인증 요청이 리디렉션 호스트 이름으로 리디렉션됩니다. 이 옵션을 선택한 경우 리디렉션 호스트 이름 텍스트 상자에 리디렉션 호스트 이름을 입력합니다. 일반적으로 서비스의 호스트 이름입니다.

7 저장을 클릭합니다.

후속 작업

인증 방법을 기본 액세스 정책에 추가합니다. **관리 > 디렉토리 관리 > 정책**으로 이동하고 **기본 정책 편집**을 클릭하여 Kerberos 인증 방법이 올바른 인증 순서대로 규칙에 추가되도록 기본 정책 규칙을 편집합니다.

웹 인터페이스에 액세스하도록 Internet Explorer 구성

배포에 대해 Kerberos가 구성된 경우, 그리고 Internet Explorer를 사용하여 웹 인터페이스에 액세스할 수 있는 권한을 사용자에게 부여할 경우 Internet Explorer 브라우저를 구성해야 합니다.

Kerberos 인증은 Windows 운영 체제에서 Directories Management와 함께 작동합니다.

참고 다른 운영 체제에서는 이 Kerberos 관련 단계를 구현하지 마십시오.

필수 조건

각 사용자에게 대해 Internet Explorer 브라우저를 구성하거나 Kerberos를 구성한 후 사용자에게 지침을 제공하십시오.

프로시저

- 1 도메인의 사용자로 Windows에 로그인하는지 확인합니다.
- 2 Internet Explorer에서 자동 로그인을 사용하도록 설정합니다.
 - a **도구 > 인터넷 옵션 > 보안**을 선택합니다.
 - b **사용자 지정 수준**을 클릭합니다.
 - c **인트라넷 영역에서만 자동으로 그인**을 선택합니다.
 - d **확인**을 클릭합니다.
- 3 커넥터 가상 장치의 이 인스턴스가 로컬 인트라넷 영역에 속하는지 확인합니다.
 - a Internet Explorer를 사용하여 Directories Management 로그인 URL(<https://myconnectorhost.domain/authenticate/>)에 액세스합니다.
 - b 브라우저 창 상태 표시줄의 오른쪽 하단 모서리에서 영역을 찾습니다.
영역이 로컬 인트라넷인 경우 Internet Explorer구성이 완료되었습니다.
- 4 영역이 로컬 인트라넷이 아닌 경우 Directories Management 로그인 URL을 인트라넷 영역에 추가합니다.
 - a **도구 > 인터넷 옵션 > 보안 > 로컬 인트라넷 > 사이트**를 선택합니다.
 - b **인트라넷 네트워크를 자동으로 감지**를 선택합니다.
이 옵션을 선택하지 않은 경우 항목을 인트라넷 영역에 추가하는 이 옵션을 선택하는 것으로 충분합니다.
 - c (선택 사항) **인트라넷 네트워크를 자동으로 감지**를 선택한 경우 모든 대화상자가 닫힐 때까지 **확인**을 클릭합니다.
 - d [로컬 인트라넷] 대화상자에서 **고급**을 클릭합니다.
[로컬 인트라넷]이라는 두 번째 대화상자가 표시됩니다.
 - e **영역에 이 웹 사이트 추가** 텍스트 상자에 Directories Management URL을 입력합니다.
<https://myconnectorhost.domain/authenticate/>
 - f **추가 > 닫기 > 확인**을 클릭합니다.

- 5 Internet Explorer가 Windows 인증을 신뢰할 수 있는 사이트에 전달할 수 있는지 확인합니다.
 - a [인터넷 옵션] 대화상자에서 **고급** 탭을 클릭합니다.
 - b **통합된 Windows 인증 사용**을 선택합니다.
이 옵션은 Internet Explorer를 다시 시작한 경우에만 적용됩니다.
 - c **확인**을 클릭합니다.
- 6 웹 인터페이스에 로그인하여 액세스 권한을 확인합니다.
Kerberos 인증이 성공하면 테스트 URL이 웹 인터페이스로 이동합니다.

Kerberos 프로토콜은 이 Internet Explorer 브라우저 인스턴스와 Directories Management 간의 모든 상호 작용을 보안합니다. 이제 사용자는 Single Sign-On을 사용하여 [내 앱] 포털에 액세스할 수 있습니다.

웹 인터페이스에 액세스하도록 Firefox 구성

배포에 대해 Kerberos가 구성된 경우, 그리고 Firefox를 사용하여 웹 인터페이스에 액세스할 수 있는 권한을 사용자에게 부여할 경우 Firefox 브라우저를 구성해야 합니다.

Kerberos 인증은 Windows 운영 체제에서 Directories Management와 함께 작동합니다.

필수 조건

각 사용자에게 대해 Firefox 브라우저를 구성하거나 Kerberos를 구성한 후 사용자에게 지침을 제공하십시오.

프로시저

- 1 Firefox 브라우저의 URL 텍스트 상자에서 about:config를 입력하여 고급 설정을 액세스합니다.
- 2 **고급 기능 사용 동의**를 클릭합니다.
- 3 [기본 설정 이름] 열에서 **network.negotiate-auth.trusted-uris**를 두 번 클릭합니다.
- 4 텍스트 상자에 Directories Management URL을 입력합니다.
https://myconnectorhost.domain.com
- 5 **확인**을 클릭합니다.
- 6 [기본 설정 이름] 열에서 **network.negotiate-auth.delegation-uris**를 두 번 클릭합니다.
- 7 텍스트 상자에 Directories Management URL을 입력합니다.
https://myconnectorhost.domain.com/authenticate/
- 8 **확인**을 클릭합니다.
- 9 Firefox 브라우저를 사용하여 로그인 URL에 로그인하여 Kerberos 기능을 테스트합니다. 예를 들어, https://myconnectorhost.domain.com/authenticate/입니다.
Kerberos 인증이 성공하면 테스트 URL이 웹 인터페이스로 이동합니다.

Kerberos 프로토콜은 이 Firefox 브라우저 인스턴스와 Directories Management 간의 모든 상호 작용을 보안합니다. 이제 사용자는 Single Sign-On을 사용하여 [내 앱] 포털에 액세스할 수 있습니다.

웹 인터페이스에 액세스하도록 Chrome 브라우저 구성

배포에 대해 Kerberos가 구성된 경우, 그리고 Chrome 브라우저를 사용하여 웹 인터페이스에 액세스할 수 있는 권한을 사용자에게 부여할 경우 Chrome 브라우저를 구성해야 합니다.

Kerberos 인증은 Windows 운영 체제에서 Directories Management와 함께 작동합니다.

참고 다른 운영 체제에서는 이 Kerberos 관련 단계를 구현하지 마십시오.

필수 조건

- Kerberos를 구성합니다.
- Chrome에서는 Internet Explorer 구성을 사용하여 Kerberos 인증을 사용하도록 설정하기 때문에 Chrome에서 Internet Explorer 구성을 사용할 수 있도록 Internet Explorer를 구성해야 합니다. Kerberos 인증을 위해 Chrome을 구성하는 방법에 대한 자세한 내용은 Google 설명서를 참조하십시오.

프로시저

- 1 Chrome 브라우저를 사용하여 Kerberos 기능을 테스트합니다.
- 2 Directories Management(<https://myconnectorhost.domain.com/authenticate/>)에 로그인합니다.

Kerberos 인증이 성공하면 테스트 URL이 웹 인터페이스와 연결됩니다.

모든 관련된 Kerberos 구성이 올바르면 상대 프로토콜(Kerberos)이 이 Chrome 브라우저 인스턴스와 Directories Management 간의 모든 상호 작용을 보안합니다. 사용자는 Single Sign-On을 사용하여 [내 앱] 포털에 액세스할 수 있습니다.

디렉토리 관리용 외부 커넥터 업그레이드

vRealize Automation 디렉토리 관리 구성에서 외부 커넥터를 사용하는 경우 이 커넥터를 이따금 업그레이드해야 할 수 있습니다.

vRealize Automation 배포 버전을 업그레이드하거나 원하는 기능을 제공하는 새 커넥터 빌드를 사용하는 경우 외부 커넥터를 업그레이드해야 할 수 있습니다.

이 설명서의 내용은 독립형 외부 커넥터 장치를 추가로 배포한 사용자에게만 적용됩니다.

vRealize Automation에서는 외부 커넥터 장치가 스마트 카드 인증 등에 사용됩니다.

기본적으로 커넥터는 업그레이드 절차를 위해 VMware 웹 사이트를 사용하며 이를 위해 커넥터 장치가 인터넷에 연결되어 있어야 합니다. 해당되는 경우 커넥터 장치에 대해 프록시 서버 설정도 구성해야 합니다.

커넥터 인스턴스가 인터넷에 연결되어 있지 않으면 오프라인으로 업그레이드를 수행할 수 있습니다. 오프라인 업그레이드를 위해서는 업그레이드 패키지를 다운로드하고 업그레이드 파일을 호스팅하도록 로컬 웹 서버를 설정합니다.

대상 사용자

이 정보는 디렉토리 관리를 설치, 업그레이드 및 구성하는 모든 사용자를 대상으로 합니다. 이 정보는 가상 시스템 기술을 잘 아는 숙련된 Windows 또는 Linux 시스템 관리자를 위해 작성되었습니다.

외부 커넥터 업그레이드 준비

커넥터 업그레이드를 준비하려면 사용 가능한 업그레이드를 확인하고 해당되는 경우 장치에 대한 프록시 서버 설정 구성을 확인해야 합니다.

■ 온라인을 통한 외부 커넥터 업그레이드의 가용성 확인

커넥터 장치가 인터넷에 연결되어 있으면 장치에서 온라인으로 업그레이드할 수 있는지 확인할 수 있습니다.

■ 외부 커넥터 장치에 대한 프록시 서버 설정 구성

커넥터 가상 장치는 인터넷을 통해 VMware 업데이트 서버에 액세스합니다. 네트워크 구성이 HTTP 프록시를 사용하여 인터넷에 액세스할 수 있도록 하는 경우 장치에 맞게 프록시 설정을 조정해야 합니다.

온라인을 통한 외부 커넥터 업그레이드의 가용성 확인

커넥터 장치가 인터넷에 연결되어 있으면 장치에서 온라인으로 업그레이드할 수 있는지 확인할 수 있습니다.

프로시저

1 루트 사용자로 커넥터 장치에 로그인합니다.

2 다음 명령을 실행합니다.

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

3 다음 명령을 실행하여 온라인 업그레이드를 확인합니다.

```
/usr/local/horizon/update/updatemgr.hzn check
```

외부 커넥터 장치에 대한 프록시 서버 설정 구성

커넥터 가상 장치는 인터넷을 통해 VMware 업데이트 서버에 액세스합니다. 네트워크 구성이 HTTP 프록시를 사용하여 인터넷에 액세스할 수 있도록 하는 경우 장치에 맞게 프록시 설정을 조정해야 합니다.

프록시에서 인터넷 트래픽만 사용하도록 설정합니다. 프록시가 제대로 설정되어 있도록 하려면 내부 트래픽에 대한 매개 변수를 도메인 내에서 프록시 없음으로 설정하십시오.

참고 인증이 필요한 프록시 서버는 지원되지 않습니다.

필수 조건

- 커넥터 장치에 대해 루트 암호가 있는지 확인합니다.
- 프록시 서버 정보가 있는지 확인합니다.

프로시저

- 1 루트 사용자로 커넥터 장치에 로그인합니다.
- 2 명령줄에 YaST를 입력하여 YaST 유틸리티를 실행합니다.
- 3 왼쪽 창에서 **네트워크 서비스**를 선택한 후 **프록시**를 선택합니다.
- 4 **HTTP 프록시 URL** 및 **HTTPS 프록시 URL** 필드에 프록시 서버 URL을 입력합니다.
- 5 **완료**를 선택하고 YaST 유틸리티를 종료합니다.
- 6 새 프록시 설정을 사용하려면 커넥터 가상 장치에서 Tomcat 서버를 다시 시작합니다.

```
service horizon-workspace restart
```

이제 커넥터 장치에서 VMware 업데이트 서버를 사용할 수 있습니다.

외부 커넥터 온라인 업그레이드

연결이 적절하게 설정되어 있으면 디렉토리 외부 관리 커넥터를 온라인으로 업그레이드할 수 있습니다.

필수 조건

- 커넥터 장치에서 HTTP를 통해 포트 80으로 vapp-updates.vmware.com을 확인하고 연결할 수 있는지 확인합니다.
- 커넥터 업그레이드가 있는지 확인합니다. 적절한 명령을 실행하여 업그레이드를 확인합니다. 온라인 Directories Management 커넥터 업그레이드 가용성 확인을 참조하십시오.
- 장치의 기본 루트 파티션에서 2GB 이상의 디스크 공간을 사용할 수 있는지 확인합니다.
- 커넥터가 제대로 구성되어 있는지 확인합니다.
- 커넥터 장치의 스냅샷을 가져와 백업합니다. 스냅샷을 가져오는 방법에 대한 자세한 정보는 vSphere 설명서를 참조하십시오.
- 아웃바운드 HTTP 액세스에 HTTP 프록시 서버가 필요한 경우에는 커넥터 장치에 대해 프록시 서버 설정을 구성합니다. Directories Management 커넥터 장치에 대한 프록시 서버 설정 구성을 참조하십시오.

프로시저

- 1 루트 사용자로 커넥터 장치에 로그인합니다.
- 2 다음 명령을 실행합니다.

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

- 3 다음 명령을 실행하여 온라인 업그레이드가 있는지 확인합니다.

```
/usr/local/horizon/update/updatesmgr.hzn check
```

- 4 다음 명령을 실행하여 장치를 업데이트합니다.

```
/usr/local/horizon/update/updatesmgr.hzn update
```

업그레이드 중에 발생하는 메시지는 /opt/vmware/var/log/update.log의 update.log 파일에 저장됩니다.

- 5 updatesmgr.hzn check 명령을 다시 실행하여 최신 업데이트가 존재하지 않는지 확인합니다.

```
/usr/local/horizon/update/updatesmgr.hzn check
```

- 6 업그레이드된 장치 버전을 확인합니다.

```
vami-cli version --appliance
```

새 버전이 표시됩니다.

- 7 커넥터 장치를 다시 시작합니다.

```
reboot
```

외부 커넥터 오프라인 업그레이드

기존 vRealize Automation 디렉토리 관리 커넥터 장치를 인터넷에 연결하여 업그레이드할 수 없는 경우에는 오프라인 업그레이드를 수행할 수 있습니다. 로컬 웹 서버에 업그레이드 저장소를 설정하고 업그레이드에 로컬 웹 서버를 사용하도록 커넥터 장치를 구성해야 합니다.

필수 조건

- 커넥터 업그레이드가 있는지 확인합니다. My VMware 다운로드 사이트(my.vmware.com)에서 업그레이드가 있는지 확인합니다.
- 장치의 기본 루트 파티션에서 2GB 이상의 디스크 공간을 사용할 수 있는지 확인합니다.
- 커넥터가 제대로 구성되어 있는지 확인합니다.
- 커넥터 장치의 스냅샷을 가져와 백업합니다. 스냅샷을 가져오는 방법에 대한 자세한 정보는 vSphere 설명서를 참조하십시오.
- 로컬 웹 서버를 사용하여 업그레이드 파일을 호스팅하도록 커넥터 장치를 구성합니다. 오프라인 업그레이드를 위한 로컬 웹 서버 준비를 참조하십시오.

프로시저

1 오프라인 업그레이드를 위한 로컬 웹 서버 준비

오프라인 커넥터 업그레이드를 시작하기 전에 커넥터 장치의 하위 디렉토리를 포함하는 디렉토리 구조를 생성하여 로컬 웹 서버를 준비합니다.

2 커넥터 구성 및 오프라인 업그레이드 수행

오프라인 업그레이드를 수행할 로컬 웹 서버를 가리키도록 커넥터 장치를 구성합니다. 그런 다음 장치를 업그레이드합니다.

오프라인 업그레이드를 위한 로컬 웹 서버 준비

오프라인 커넥터 업그레이드를 시작하기 전에 커넥터 장치의 하위 디렉토리를 포함하는 디렉토리 구조를 생성하여 로컬 웹 서버를 준비합니다.

필수 조건

- My VMware에서 identity-manager-connector-버전 번호-빌드 번호-updaterepo.zip 파일을 다운로드합니다. my.vmware.com으로 가서 VMware Identity Manager 다운로드 페이지로 이동한 후 **VMware Identity Manager Connector 오프라인 업그레이드 패키지**에 나열된 파일을 다운로드합니다.
- IIS 웹 서버를 사용하는 경우에는 파일 이름에 특수 문자를 허용하도록 웹 서버를 구성합니다. 이는 **요청 필터링** 섹션에서 **더블 이스케이핑 허용** 옵션을 선택하여 구성할 수 있습니다.

프로시저

- 1 `http://YourWebServer/VM/`에서 웹 서버의 디렉토리를 생성하고 다운로드한 zip 파일을 이 위치에 복사합니다.
- 2 웹 서버에 `.sig(text/plain)` 및 `.sha256(text/plain)`에 대한 MIME 유형이 포함되어 있는지 확인합니다.
이러한 MIME 유형이 없으면 웹 서버의 업데이트 확인이 실패합니다.
- 3 파일을 압축 해제합니다.
추출한 ZIP 파일의 콘텐츠는 `http://YourWebServer/VM/`에서 제공됩니다.
파일에서 추출한 콘텐츠에는 `/manifest` 및 `/package-pool` 하위 디렉토리가 포함되어 있습니다.
- 4 다음 `updateLocal.hzn` 명령을 실행하여 URL에 유효한 업데이트 콘텐츠가 있는지 확인합니다.

```
/usr/local/horizon/update/updateLocal.hzn checkurl http://YourWebServer/VM
```

커넥터 구성 및 오프라인 업그레이드 수행

오프라인 업그레이드를 수행할 로컬 웹 서버를 가리키도록 커넥터 장치를 구성합니다. 그런 다음 장치를 업그레이드합니다.

필수 조건

오프라인 업그레이드를 위한 로컬 웹 서버를 준비합니다.

프로시저

- 1 루트 사용자로 커넥터 장치에 로그인합니다.

- 2 다음 명령을 실행하여 로컬 웹 서버를 사용하는 업그레이드 저장소를 구성합니다.

```
/usr/local/horizon/update/updateslocal.hzn seturl http://YourWebServer/VM/
```

참고 구성을 실행 취소하고 온라인 업그레이드를 수행하는 기능을 복원하려면 다음 명령을 실행할 수 있습니다.

```
/usr/local/horizon/update/updateslocal.hzn setdefault
```

- 3 업그레이드를 수행하십시오.

- a 다음 명령을 실행합니다.

```
/usr/local/horizon/update/updatesmgr.hzn updateinstaller
```

- b 다음 명령을 실행하여 사용 가능한 업그레이드 버전을 확인합니다.

```
/usr/local/horizon/update/updatesmgr.hzn check
```

- c 다음 명령을 실행하여 커넥터를 업데이트합니다.

```
/usr/local/horizon/update/updatesmgr.hzn update
```

업그레이드 중에 발생하는 메시지는 /opt/vmware/var/log/update.log의 update.log 파일에 저장됩니다.

- d updatesmgr.hzn check 명령을 다시 실행합니다.

```
/usr/local/horizon/update/updatesmgr.hzn check
```

- e 업그레이드된 장치 버전을 확인합니다.

```
vami-cli version --appliance
```

이 명령은 새 버전을 표시합니다.

- f 커넥터 장치를 다시 시작합니다.

예를 들어 명령줄에서 다음 명령을 실행합니다.

```
reboot
```

커넥터 업그레이드가 완료되었습니다.

외부 커넥터를 업그레이드한 후에 설정 구성

커넥터 2016.3.1.0 이상으로 업그레이드한 후 일부 설정을 구성해야 할 수도 있습니다.

Kerberos 인증으로 도메인 재가입

Kerberos 인증 또는 Active Directory(Windows 통합 인증) 디렉토리를 사용하는 경우 도메인을 탈퇴했다가 다시 가입해야 합니다. 배포 환경에 있는 모든 커넥터 가상 장치에 대해 이 작업이 필요합니다.

- 1 **관리 > 디렉토리 관리 > 커넥터**를 선택합니다.
- 2 [커넥터] 페이지에서 Kerberos 인증 또는 Active Directory(Windows 통합 인증) 디렉토리에 사용되고 있는 각 커넥터에 대해 **도메인 탈퇴**를 클릭합니다.
- 3 도메인에 가입하려면 도메인에 가입하기 위한 권한이 있는 Active Directory 자격 증명이 필요합니다. 자세한 내용은 [도메인에 커넥터 시스템 가입](#)를 참조하십시오.
- 4 Kerberos 인증을 사용하는 경우 Kerberos 인증 어댑터를 다시 사용하도록 설정합니다. [인증 어댑터] 페이지에 액세스하려면 [커넥터] 페이지의 **작업자** 열에서 해당 링크를 클릭하고 **인증 어댑터** 탭을 선택합니다.
- 5 사용 중인 다른 인증 어댑터가 사용되도록 설정되어 있는지 확인합니다.

도메인 페이지 업데이트

Active Directory(Windows 통합 인증) 또는 이 디렉토리는 **DNS 서비스 위치를 지원합니다**. 옵션이 설정된 상태로 [LDAP를 통한 Active Directory]를 사용하는 경우 디렉토리의 [도메인] 페이지를 저장하십시오.

- 1 **관리 > 디렉토리 관리 > 디렉토리**를 선택합니다.
- 2 해당 디렉토리를 선택하여 편집합니다.
- 3 바인딩 DN 사용자에게 대한 암호를 제공하고 **저장**을 클릭합니다.
- 4 페이지 왼쪽의 **동기화 설정**을 클릭하고 **도메인** 탭을 선택합니다.
- 5 **저장**을 클릭합니다.

DNS 서비스 위치와 도메인 컨트롤러

참고 커넥터 2016.3.1.0 이상에서 domain_krb.properties 파일이 자동으로 만들어지고 DNS 서비스 위치가 사용되도록 설정된 디렉토리가 만들어질 때 도메인 컨트롤러로 자동으로 채워집니다. 업그레이드 후에 [도메인] 페이지를 저장한 경우 원래 배포에 domain_krb.properties 파일이 있는 경우 사용자가 나중에 추가했을 수 있고 이전에는 파일에 없던 도메인으로 해당 파일이 업데이트됩니다. 원래 배포에 domain_krb.properties 파일이 없는 경우 해당 파일이 만들어지고 도메인 컨트롤러로 자동으로 채워집니다. domain_krb.properties 파일에 대한 자세한 내용은 [도메인 컨트롤러 선택 정보](#) 항목을 참조하십시오.

외부 커넥터 업그레이드 오류 문제 해결

오류 로그를 검토하여 vRA 디렉토리 관리 외부 커넥터 업그레이드 문제를 해결할 수 있습니다. 커넥터가 시작되지 않으면 스냅샷으로 롤백해서 이전 인스턴스로 되돌릴 수 있습니다.

■ 업그레이드 오류 로그 확인

오류 로그를 검토하여 업그레이드 중에 발생하는 오류를 해결합니다. 업그레이드 로그 파일은 /opt/vmware/var/log 디렉토리에 있습니다.

■ 커넥터의 스냅샷으로 롤백

업그레이드가 끝난 후 커넥터가 올바르게 시작되지 않는 상황에서 업그레이드 오류 로그를 검토한 후 업그레이드 명령을 다시 실행해도 문제를 해결할 수 없는 경우 이전 커넥터 인스턴스로 롤백할 수 있습니다.

■ 로그 파일 번들 수집

VMware 지원팀으로 보낼 로그 파일 번들을 수집할 수 있습니다. 커넥터 장치 구성 페이지에서 번들을 가져올 수 있습니다.

업그레이드 오류 로그 확인

오류 로그를 검토하여 업그레이드 중에 발생하는 오류를 해결합니다. 업그레이드 로그 파일은 /opt/vmware/var/log 디렉토리에 있습니다.

오류가 발생하면 업그레이드가 끝난 후 커넥터가 시작되지 않을 수 있습니다.

프로시저

- 1 커넥터 장치에 로그인합니다.
- 2 /opt/vmware/var/log 디렉토리로 이동합니다.
- 3 update.log 파일을 열고 오류 메시지를 검토합니다.
- 4 오류를 해결하고 업그레이드 명령을 다시 실행합니다. 업그레이드 명령은 중지된 지점부터 다시 시작됩니다.

참고 또는 스냅샷으로 되돌아가 업데이트를 다시 실행할 수 있습니다.

커넥터의 스냅샷으로 롤백

업그레이드가 끝난 후 커넥터가 올바르게 시작되지 않는 상황에서 업그레이드 오류 로그를 검토한 후 업그레이드 명령을 다시 실행해도 문제를 해결할 수 없는 경우 이전 커넥터 인스턴스로 롤백할 수 있습니다.

프로시저

- ◆ 원래 커넥터 인스턴스의 백업으로 가져온 스냅샷 중 하나로 되돌립니다. 자세한 정보는 vSphere 설명서를 참조하십시오.

로그 파일 번들 수집

VMware 지원팀으로 보낼 로그 파일 번들을 수집할 수 있습니다. 커넥터 장치 구성 페이지에서 번들을 가져올 수 있습니다.

다음 로그 파일이 번들로 수집됩니다.

표 2-9. 로그 파일

구성 요소	로그 파일 위치	설명
Apache Tomcat 로그 (catalina.log)	/opt/vmware/horizon/workspace/logs/catalina.log	Apache Tomcat은 다른 로그 파일에 기록되지 않은 메시지를 기록합니다.
구성기 로그 (configurator.log)	/opt/vmware/horizon/workspace/logs/configurator.log	구성기가 REST 클라이언트 및 웹 인터페이스에서 받는 요청입니다.
커넥터 로그 (connector.log)	/opt/vmware/horizon/workspace/logs/connector.log	웹 인터페이스에서 받은 각 요청의 기록입니다. 각 로그 항목에는 요청 URL, 타임 스탬프 및 예외도 포함됩니다. 동기화 작업은 기록되지 않습니다.

프로시저

- 1 커넥터 구성 페이지(<https://connectorURL:8443/cfg/logs>)에 로그인합니다.
- 2 로그 번들 준비를 클릭합니다.
- 3 번들을 다운로드하고 VMware 지원팀으로 보냅니다.

시나리오: 고가용성 vRealize Automation 에 대해 Active Directory 링크 구성

테넌트 관리자로서 고가용성 vRealize Automation 배포를 위한 사용자 인증을 지원하기 위해 LDAP 디렉토리 연결을 통한 Active Directory를 구성하려고 합니다.

각 vRealize Automation 장치에는 사용자 인증을 지원하는 커넥터가 포함되어 있지만 일반적으로 디렉토리 동기화를 수행하기 위한 단 하나의 커넥터만 구성되어 있습니다. 어떤 커넥터를 선택하여 동기화 커넥터로 사용하든 상관 없습니다. 디렉토리 관리 고가용성을 지원하려면 두 번째 vRealize Automation 장치에 해당하는 두 번째 커넥터를 구성해야 합니다. 이것은 ID 제공자에 연결하고 동일한 Active Directory를 가리킵니다. 이 구성을 사용하면 하나의 장치가 실패하는 경우 다른 장치가 사용자 인증 관리를 담당합니다.

고가용성 환경에서 모든 노드는 동일한 Active Directory 집합, 사용자, 인증 방법 등을 제공해야 합니다. 이러한 작업을 성공적으로 수행할 수 있는 가장 직접적인 방법은 로드 밸런서 호스트를 ID 제공자 호스트로 설정하여 ID 제공자를 클러스터로 승격시키는 것입니다. 이 구성을 사용하면 모든 인증 요청이 로드 밸런서로 전송되고 로드 밸런서는 요청을 두 커넥터 중 하나로 적절하게 전달합니다.

필수 조건

- 적절한 로드 밸런서와 함께 분산된 vRealize Automation 배포를 설치합니다. vRealize Automation 7.3 설치의 내용을 참조하십시오.
- 테넌트 관리자 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 관리 > 디렉토리 관리 > 디렉토리를 선택합니다.
- 2 디렉토리 추가를 클릭합니다.

3 특정 Active Directory 계정 설정을 입력하고 기본 옵션을 수락합니다.

옵션	샘플 입력
디렉토리 이름	Active Directory 도메인 이름의 IP 주소를 추가합니다.
동기화 커넥터	각 vRealize Automation 장치에는 커넥터가 포함되어 있습니다. 사용 가능한 커넥터 중 하나를 사용합니다.
기본 DN	서버가 검색하는 디렉토리에 대한 시작점의 DN(고유 이름)을 입력합니다. 예를 들어 cn=users,dc=corp,dc=local 을 입력합니다.
Bind DN	사용자를 검색할 권한이 있는 Active Directory 사용자 계정의 CN(일반 이름)을 포함하여 전체 DN(고유 이름)을 입력합니다. 예를 들어 cn=config_admin infra,cn=users,dc=corp,dc=local 을 입력합니다.
Bind DN 암호	사용자를 검색할 수 있는 계정에 대한 Active Directory 암호를 입력합니다.

4 연결 테스트를 클릭하여 구성된 디렉토리에 대한 연결을 테스트합니다.

연결이 실패하면 모든 필드의 항목을 확인하고 필요한 경우 시스템 관리자에게 문의합니다.

5 저장 및 다음을 클릭합니다.

도메인 목록과 함께 [도메인 선택] 페이지가 나타납니다.

6 기본 도메인이 선택된 상태로 두고 다음을 클릭합니다.

7 특성 이름이 올바른 Active Directory 특성에 매핑되어 있는지 확인합니다. 그렇지 않은 경우 드롭다운 메뉴에서 올바른 Active Directory 특성을 선택합니다. 다음을 클릭합니다.

8 동기화하려는 그룹과 사용자를 선택합니다.

a **추가** 아이콘(+)을 클릭합니다.

b 사용자 도메인을 입력하고 **그룹 찾기**를 클릭합니다.

예를 들어 **cn=users,dc=corp,dc=local**을 입력합니다.

c **모두 선택** 확인란을 선택합니다.

d **선택**을 클릭합니다.

e **다음**을 클릭합니다.

f 추가 사용자를 추가하려면 +를 클릭합니다. 예를 들어 **CN=username,CN=Users,OU-myUnit,DC=myCorp,DC=com**을 입력합니다.

사용자를 제외하려면 +를 클릭하고 필터를 만들어 일부 사용자 유형을 제외합니다. 필터 기준으로 사용할 사용자 특성, 쿼리 규칙 및 값을 선택합니다.

g **다음**을 클릭합니다.

9 페이지를 검토하여 디렉토리에 동기화되는 사용자 및 그룹의 수를 보고 디렉토리 동기화를 클릭합니다.

디렉토리 동기화 프로세스에는 약간의 시간이 걸리지만 백그라운드에서 수행되므로 작업을 계속할 수 있습니다.

10 고가용성 지원을 위한 두 번째 커넥터를 구성합니다.

- a vRealize Automation 배포의 로드 밸런서에 테넌트 관리자로 로그인합니다.
로드 밸런서 URL은 `load balancer address/vcac/org/tenant_name`입니다.
- b **관리 > 디렉토리 관리 > ID 제공자**를 선택합니다.
- c 현재 시스템에서 사용 중인 ID 제공자를 클릭합니다.
시스템을 위해 기본적인 ID 관리를 제공하는 기존의 디렉토리 및 커넥터가 나타납니다.
- d **커넥터 추가** 드롭다운 목록을 클릭하고 보조 vRealize Automation 장치에 해당하는 커넥터를 선택합니다.
- e 커넥터를 선택할 때 나타나는 **Bind DN 암호** 텍스트 상자에 적절한 암호를 입력합니다.
- f **커넥터 추가**를 클릭합니다.
- g 로드 밸런서를 가리키도록 호스트 이름을 편집합니다.

회사 Active Directory를 vRealize Automation에 연결했고 고가용성을 위해 디렉토리 관리를 구성했습니다.

후속 작업

향상된 보안을 제공하기 위해 ID 제공자와 Active Directory 간에 양방향 신뢰를 구성할 수 있습니다. [vRealize Automation과 Active Directory 간 양방향 신뢰 관계 구성](#) 항목을 참조하십시오.

vRealize Automation 에서 스마트 카드 및 타사 ID 제공자 인증을 위한 외부 커넥터 구성

사용자가 Keberos 같은 타사 ID 제공자 또는 스마트 카드 인증을 사용하는 경우, 시스템 관리자는 디렉토리 관리를 사용하여 사용자의 vRealize Automation 배포를 위한 외부 커넥터를 구성해야 합니다.

디렉토리 관리는 각 구성된 Active Directory에 대해 여러 개의 ID 제공자와 커넥터 클러스터를 지원합니다. 타사 ID 제공자 또는 스마트 카드 인증을 사용하려면 SSL 패스스루를 허용하는 로드 밸런서 뒤에 적절한 ID 제공자가 있는 단일 외부 커넥터 또는 커넥터 클러스터를 설정합니다. 자세한 내용은 [커넥터 및 커넥터 클러스터 관리](#)를 참조하십시오.

외부 커넥터 업데이트에 대한 자세한 내용은 [디렉토리 관리용 외부 커넥터 업그레이드](#) 항목을 참조하십시오.

스마트 카드 인증에 사용할 수 있는 인증서 구성 옵션은 여러 가지가 있습니다. [Directories Management](#)와 [함께 사용할 인증서 또는 스마트 카드 어댑터 구성](#) 항목을 참조하십시오.

필수 조건

- vRealize Automation 배포에 사용할 적절한 Active Directory 연결을 구성합니다.
- [VMware vRealize Automation 도구 및 SDK](#)에서 커넥터를 구성하는 데 필요한 OVA 파일을 다운로드합니다.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 커넥터 활성화 토큰 생성

스마트 카드 인증에 사용할 커넥터 가상 장치를 배포하기 전에 vRealize Automation 콘솔에서 새 커넥터의 활성화 코드를 생성합니다. 이 활성화 코드는 디렉토리 관리와 커넥터 간의 통신을 설정하는 데 사용됩니다.

2 커넥터 OVA 파일 배포

커넥터 OVA 파일을 다운로드한 후 VMware vSphere Client 또는 vSphere Web Client를 사용하여 이 파일을 배포할 수 있습니다.

3 커넥터 설정 구성

커넥터 OVA를 배포한 후 설정 마법사를 실행하여 장치를 활성화하고 관리자 암호를 구성해야 합니다.

4 공용 CA(인증 기관) 적용

디렉토리 관리가 설치된 경우, 기본 SSL 인증서가 생성됩니다. 이 기본 인증서는 테스트 목적으로 사용할 수 있고, 운영 환경에서는 상업용 SSL 인증서를 생성하고 설치해야 합니다.

5 작업 공간 ID 제공자 생성

외부 커넥터와 함께 사용하기 위해 작업 공간 ID 제공자를 생성해야 합니다.

6 인증서 인증 구성 및 기본 액세스 정책 규칙 구성

vRealize Automation Active Directory 및 도메인에 사용할 외부 커넥터를 구성해야 합니다.

커넥터 활성화 토큰 생성

스마트 카드 인증에 사용할 커넥터 가상 장치를 배포하기 전에 vRealize Automation 콘솔에서 새 커넥터의 활성화 코드를 생성합니다. 이 활성화 코드는 디렉토리 관리와 커넥터 간의 통신을 설정하는 데 사용됩니다.

단일 커넥터 또는 커넥터 클러스터를 구성할 수 있습니다. 커넥터 클러스터를 사용하려는 경우, 필요한 커넥터마다 이 절차를 반복합니다.

필수 조건

- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 **관리 > 디렉토리 관리 > 커넥터**를 선택합니다.

2 **커넥터 ID 이름** 텍스트 상자에 새 커넥터의 이름을 입력합니다.

3 **Enter**를 누릅니다.

커넥터의 활성화 코드가 **커넥터 활성화 코드** 상자에 표시됩니다.

4 OVA 파일을 사용하여 커넥터를 구성할 때 사용하기 위해 활성화 코드를 복사해 둡니다.

커넥터 OVA 파일 배포

커넥터 OVA 파일을 다운로드한 후 VMware vSphere Client 또는 vSphere Web Client를 사용하여 이 파일을 배포할 수 있습니다.

vSphere Client 또는 vSphere Web Client를 사용하여 OVA 파일을 배포합니다.

필수 조건

- connector OVA 배포에 사용할 DNS 레코드와 호스트 이름을 확인합니다.
- vSphere Web Client를 사용하는 경우, Firefox 또는 Chrome 브라우저를 사용합니다. OVA 파일을 배포할 때 Internet Explorer를 사용하지 마십시오.
- [VMware vRealize Automation 도구 및 SDK](#)에서 커넥터를 구성하는 데 필요한 OVA 파일을 다운로드합니다.

프로시저

- 1 vSphere Client 또는 vSphere Web Client에서 **파일 > OVF 템플릿 배포**를 선택합니다.
- 2 [OVF 템플릿 배포] 페이지에서 사용자 connector 배포의 정보를 입력합니다.

페이지	설명
소스	OVA 패키지 위치로 이동하거나, 특정 URL을 입력합니다.
OVA 템플릿 세부 정보	올바른 버전을 선택했는지 확인합니다.
라이선스	최종 사용자 라이선스 계약을 읽고 동의 를 클릭합니다.
이름 및 위치	가상 장치의 이름을 입력합니다. 이 이름은 인벤토리 폴더 내에서 고유해야 하고 최대 80자를 포함할 수 있습니다. 이름은 대/소문자를 구분합니다. 가상 장치의 위치를 선택합니다.
호스트/클러스터	배포된 템플릿을 실행할 호스트 또는 클러스터를 선택합니다.
리소스 풀	리소스 풀을 선택합니다.
스토리지	가상 시스템 파일을 저장할 위치를 선택합니다.
디스크 포맷	파일의 디스크 포맷을 선택합니다. 운영 환경의 경우, 썸 프로비저닝 포맷을 선택합니다. 평가 및 테스트 목적인 경우, 썸 프로비저닝 포맷을 사용합니다.
네트워크 매핑	사용자 환경의 네트워크를 OVF 템플릿의 네트워크에 매핑합니다.

페이지	설명
속성	<p>a 시간대 설정 필드에서 올바른 시간대를 선택합니다.</p> <p>b [고객 환경 항상 프로그램] 확인란은 기본적으로 선택되어 있습니다. VMware는 사용자 요구 사항을 제품에 반영하기 위해 귀하의 배포에 대한 데이터를 익명으로 수집하고 있습니다. 데이터 수집을 원하지 않는 경우, 확인란을 선택 취소하십시오.</p> <p>c [호스트 이름] 확인란에 사용할 호스트 이름을 입력합니다. 이 상자를 비워 두면 리버스 DNS를 사용하여 호스트 이름을 조회합니다.</p> <p>d connector에 대한 정적 IP 주소를 구성하려면 기본 게이트웨이, DNS, IP 주소 및 넷마스크별로 주소를 입력합니다.</p> <hr/> <p>중요 호스트 이름을 포함하여 4개 주소 필드 중 하나라도 비어 있으면 DHCP가 사용됩니다.</p> <hr/> <p>DHCP를 구성하려면 주소 필드를 비워 둡니다.</p>
완료 준비	선택 사항을 검토하고 마침 을 클릭합니다.

네트워크 속도에 따라 배포하는 데 몇 분이 소요될 수 있습니다. 진행 상황 대화 상자에서 진행률을 확인할 수 있습니다.

- 3 배포가 완료되면 장치를 선택하고 마우스 오른쪽 단추를 클릭한 후 **전원 > 전원 켜기**를 선택합니다.

장치가 초기화되었습니다. **콘솔** 탭으로 이동하면 세부 정보를 확인할 수 있습니다. 가상 장치 초기화가 완료되면 콘솔 화면에 버전과 설정 완료를 위해 설정 마법사에 로그인할 수 있는 URL이 표시됩니다.

후속 작업

설정 마법사를 사용하여 활성화 코드와 관리 암호를 추가합니다.

커넥터 설정 구성

커넥터 OVA를 배포한 후 설정 마법사를 실행하여 장치를 활성화하고 관리자 암호를 구성해야 합니다.

필수 조건

- 커넥터의 활성화 코드를 생성한 상태입니다.
- 커넥터 장치의 전원이 켜져 있고 커넥터 URL을 알고 있는지 확인합니다.
- 커넥터 관리자, 루트 계정 및 sshuser 계정에 사용할 암호 목록을 수집합니다.

프로시저

- 1 설정 마법사를 실행하려면 OVA를 배포한 후 콘솔 탭에 표시된 connector URL을 입력합니다.
- 2 시작 페이지에서 **계속**을 클릭합니다.

3 다음 connector 가상 장치 관리자 계정에 대해 강력한 암호를 생성합니다.

강력한 암호는 8자 이상이며 대문자, 소문자 그리고 하나 이상의 숫자 또는 특수 문자를 포함해야 합니다.

옵션	설명
장치 관리자	장치 관리자 암호를 생성합니다. 사용자 이름은 admin 이며 변경할 수 없습니다. 이 계정 및 암호를 사용하여 connector 서비스에 로그인한 후 인증서, 장치 암호 및 syslog 구성을 관리합니다. 중요 admin 사용자 암호는 6자 이상이어야 합니다.
루트 계정	connector 장치를 설치하는 데 기본 VMware 루트 암호가 사용되었습니다. 새 루트 암호를 생성합니다.
sshsuser 계정	커넥터 장치에 원격 액세스하는 데 사용할 암호를 생성합니다.

4 계속을 클릭합니다.

5 커넥터 활성화 페이지에서 활성화 코드를 붙여 넣고 계속을 클릭합니다.

6 vRealize Automation 내부 커넥터에서 자체 서명된 인증서를 사용 중인 경우 vRealize Automation 장치에서 cat /etc/apache2/server-cert.pem 명령을 실행하여 적절한 인증서를 가져올 수 있습니다.

로드 밸런서에서 **SSL 종료** 탭을 선택하고 /horizon_workspace_rootca.pem에 대한 링크를 클릭합니다.

활성화 코드를 확인한 후 서비스와 커넥터 인스턴스 간의 통신이 설정되면 커넥터 구성을 완료할 수 있습니다.

후속 작업

서비스에서 요구 사항에 따라 환경을 설정합니다. 예를 들어, 두 개의 Windows 통합 인증 디렉토리를 동기화하기 위해 커넥터를 추가한 경우 디렉토리를 생성하고 이 디렉토리를 새 커넥터와 연결합니다.

공용 CA(인증 기관) 적용

디렉토리 관리가 설치된 경우, 기본 SSL 인증서가 생성됩니다. 이 기본 인증서는 테스트 목적으로 사용할 수 있고, 운영 환경에서는 상업용 SSL 인증서를 생성하고 설치해야 합니다.

참고 Directories Management가 로드 밸런서를 나타내는 경우, SSL 인증서가 로드 밸런서에 적용됩니다.

인증서를 가져올 때는 **이 키를 내보내기 가능으로 표시**를 선택해야 합니다.

사용자 지정 인증서에 대한 CSR을 생성하는 경우 CN 또는 인증 기관의 사이트 도메인 이름을 지정하 기만 하면 됩니다.

필수 조건

CSR(인증서 서명 요청)을 생성하고 CA에서 유효한 서명된 인증서를 구합니다. 사용자 조직에서 CA 서명이 있는 SSL 인증서를 제공하는 경우, 이 인증서를 사용해도 됩니다. 인증서는 PEM 형식이어야 합니다.

프로시저

- 1 다음 위치에서 관리자로 커넥터 장치 관리 페이지에 로그인합니다.

`https://myconnector.mycompany:8443/cfg`

- 2 관리자 콘솔에서 **장치 설정**을 클릭합니다.

VA 구성이 기본적으로 선택되어 있습니다.

- 3 **구성 관리**를 클릭합니다.

- 4 VMware Identify Manager 서버 관리자 암호를 입력합니다.

- 5 **인증서 설치**를 선택합니다.

- 6 [Identity Manager 장치에서 SSL 종료] 탭에서 **사용자 지정 인증서**를 선택합니다.

- 7 **SSL 인증서 체인** 텍스트 상자에 호스트, 중간 및 루트 인증서를 순서대로 붙여 넣습니다.

SSL 인증서는 전체 인증서 체인을 올바른 순서대로 포함한 경우에만 작동합니다. 각 인증서에 대해 -----BEGIN CERTIFICATE----- 줄과 -----END CERTIFICATE----- 줄 사이의 모든 내용을 복사합니다(해당 줄 포함).

인증서에 FQDN 호스트 이름이 포함되어 있는지 확인합니다.

- 8 [개인 키] 텍스트 상자에 개인 키를 붙여 넣습니다. -----BEGIN RSA PRIVATE KEY 줄과 -----END RSA PRIVATE KEY 줄 사이의 모든 내용을 복사합니다.

- 9 **저장**을 클릭합니다.

예: 인증서 예

인증서 체인 예

-----BEGIN CERTIFICATE-----

jIQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+

...

...

...

W53+O05j5xsxzDJfWr1lqBIFF/OkIYCPcyK1

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

WdR9Vpg3WQT5+C3HU17bUOwvhp/rjIQvt90+

...

...

...

O05j5xsxzDJfWr1lqBIFF/OkIYCPW53+cyK1

인증서 체인 예

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

dR9Vpg3WQTjIQvt9W5+C3HU17bUOwvhp/r0+

...

...

...

5j5xsxzDJfWr1lqW53+O0BIFF/OkIYCPcyK1

-----END CERTIFICATE-----

개인 키 예

-----BEGIN RSA PRIVATE KEY-----

jIQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+

...

...

...

1lqBIFFW53+O05j5xsxzDJfWr/OkIYCPcyK1

-----END RSA PRIVATE KEY-----

작업 공간 ID 제공자 생성

외부 커넥터와 함께 사용하기 위해 작업 공간 ID 제공자를 생성해야 합니다.

필수 조건

- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 디렉토리 관리 > ID 제공자**를 선택합니다.
- 2 **ID 제공자 추가**를 선택합니다.
- 3 표시되는 메뉴에서 **작업 공간 IDP 생성**을 선택합니다.
- 4 **ID 제공자 이름** 필드에 ID 제공자의 이름을 입력합니다.
- 5 이 ID 제공자를 사용할 사용자에게 해당하는 디렉토리를 선택합니다.
선택한 디렉토리에 따라 이 ID 제공자의 선택 항목으로 표시되는 커넥터가 결정됩니다.
- 6 스마트 카드 인증에 구성된 외부 커넥터를 하나 이상 선택합니다.

참고 배포 위치가 로드 밸런서 뒤이면 로드 밸런서 URL을 입력합니다.

- 7 이 ID 제공자에 액세스하는 네트워크를 선택합니다.
- 8 **추가**를 클릭합니다.

인증서 인증 구성 및 기본 액세스 정책 규칙 구성

vRealize Automation Active Directory 및 도메인에 사용할 외부 커넥터를 구성해야 합니다.

필수 조건

테넌트 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 **관리 > 디렉토리 관리 > 커넥터**를 선택합니다.

2 **작업자** 열에서 원하는 커넥터를 선택합니다.

선택한 작업자가 커넥터 **세부 정보** 탭의 **작업자 이름** 텍스트 상자에 표시되고 커넥터 유형 정보가 **커넥터 유형** 텍스트 상자에 표시됩니다.

3 **연결된 디렉토리** 텍스트 상자에 원하는 Active Directory를 지정하여 커넥터가 해당 Active Directory에 연결되도록 합니다.

4 **연결된 도메인** 텍스트 상자에 적절한 도메인 이름을 입력합니다.

5 **AuthAdapters** 탭을 선택하고 CertificateAuthAdapter를 사용하도록 설정합니다.

6 배포 환경에 맞게 인증서 인증을 구성합니다.

[디렉토리 관리를 위한 인증서 인증 구성](#) 항목을 참조하십시오.

7 **관리 > 디렉토리 관리 > 정책**을 선택합니다.

8 **기본 정책 편집**을 클릭합니다.

9 인증서를 정책 규칙에 추가하고 인증서를 첫 번째 인증 방법으로 설정합니다.

인증서가 정책 규칙에 나열된 첫 번째 인증 방법이어야 합니다. 그렇지 않으면 인증서 인증이 실패합니다.

다중 도메인 또는 다중 포리스트 Active Directory 링크 생성

시스템 관리자로서 다중 도메인 또는 다중 포리스트 Active Directory 링크를 구성해야 합니다.

다중 도메인 또는 다중 포리스트 Active Directory 링크 구성을 위한 절차는 본질적으로 동일합니다.

다중 포리스트 링크의 경우, 모든 적용 가능한 도메인 간에 양방향 신뢰가 필요합니다.

필수 조건

- 적절한 로드 밸런서와 함께 분산된 vRealize Automation 배포를 설치합니다. vRealize Automation 7.3 설치의 내용을 참조하십시오.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 배포에 적합한 도메인 및 Active Directory 포리스트를 구성합니다.

프로시저

1 **관리 > 디렉토리 관리 > 디렉토리**를 선택합니다.

- 2 **디렉토리 추가**를 클릭합니다.
- 3 [디렉토리 추가] 페이지의 **디렉토리 이름** 텍스트 상자에서 Active Directory 서버의 이름을 지정합니다.
- 4 **디렉토리 이름** 머리글 아래에서 **Active Directory(Windows 통합 인증)**를 선택합니다.
- 5 디렉토리 동기화 및 인증 섹션에서 사용자를 Active Directory에서 VMware Directories Management 디렉토리로 동기화하는 커넥터를 구성합니다.

옵션	설명
동기화 커넥터	시스템에 사용할 적절한 커넥터를 선택합니다. 각 vRealize Automation 장치에는 기본 커넥터가 포함되어 있습니다. 커넥터를 선택할 때 도움이 필요한 경우 시스템 관리자에게 문의하십시오.
인증	적절한 라디오 버튼을 클릭하여 선택한 커넥터가 인증도 수행하는지 표시합니다.
디렉토리 검색 특성	사용자 이름이 포함된 적절한 계정 특성을 선택합니다.

배포 구성에 따라 하나 이상의 커넥터를 사용할 수 있습니다.

- 6 **도메인 이름**, **도메인 관리자 이름** 및 **도메인 관리자 암호** 텍스트 상자에 적절한 도메인 가입 자격 증명을 입력합니다.

하나의 예로 다음과 같이 입력할 수 있습니다. **도메인 이름**: hs.trcint.com, **도메인 관리자 이름**: devadmin, **도메인 관리자 암호**: xxxx.

- 7 **Bind 사용자 세부 정보** 섹션에서 디렉토리 동기화를 원활히 수행할 수 있도록 적절한 Active Directory(Windows 통합 인증) 자격 증명을 입력합니다.

옵션	설명
Bind 사용자 UPN	도메인을 인증할 수 있는 사용자의 사용자 계정 이름을 입력합니다. 예를 들어 UserName@example.com을 입력합니다.
Bind DN 암호	[Bind 사용자] 암호를 입력합니다.

- 8 **저장 및 다음**을 클릭합니다.

도메인 목록과 함께 [도메인 선택] 페이지가 나타납니다.


- 9 해당 확인란을 클릭하여 시스템 배포를 위한 원하는 도메인을 선택합니다.

- 10 **다음**을 클릭합니다.

- 11 Directories Management 디렉토리 특성 이름이 올바른 Active Directory 특성에 매핑되어 있는지 확인합니다.

디렉토리 특성 이름이 잘못 매핑되어 있는 경우 드롭다운 메뉴에서 올바른 Active Directory 특성을 선택합니다.


- 12 **다음**을 클릭합니다.

13 를 클릭하여 Active Directory에서 디렉토리로 동기화하려는 그룹을 선택합니다.


Active Directory 그룹을 추가할 때 해당 그룹의 구성원이 [사용자] 목록에 없는 경우 목록에 추가됩니다.

참고 Directories Management 사용자 인증 시스템은 그룹과 사용자를 추가할 때 Active Directory의 데이터를 가져오고 시스템의 속도는 Active Directory 기능에 의해 제한됩니다. 따라서 추가할 그룹과 사용자의 수에 따라 가져오기 작업에 상당한 시간이 걸릴 수 있습니다. 지연 또는 문제가 발생할 가능성을 최소화하려면 vRealize Automation 작업에 필요한 정도로만 그룹과 사용자의 수를 제한하십시오. 시스템 성능이 저하되거나 오류가 발생하면 불필요한 애플리케이션을 모두 닫고 Active Directory에 충분한 메모리가 할당되어 있는지 확인하십시오. 문제가 계속되면 필요한 만큼 Active Directory 메모리 할당을 늘리십시오. 많은 수의 사용자 및 그룹이 포함된 시스템의 경우 Active Directory 메모리 할당을 24GB까지 늘려야 할 수 있습니다.

14 다음을 클릭합니다.

15 추가 사용자를 추가하려면 를 클릭합니다. 예를 들어

CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com을 입력합니다.

사용자를 제외하려면 를 클릭하고 필터를 만들어 일부 사용자 유형을 제외합니다. 필터 기준으로 사용할 사용자 특성, 쿼리 규칙 및 값을 선택합니다.

16 다음을 클릭합니다.

17 디렉토리에 동기화되는 사용자 및 그룹의 수를 보려면 페이지를 검토합니다.

사용자 및 그룹을 변경하고 싶다면 [편집] 링크를 클릭합니다.

18 작업 공간으로 푸시를 클릭하여 디렉토리에 대한 동기화를 시작합니다.

후속 작업

그룹 및 사용자 역할 구성

테넌트 관리자는 비즈니스 그룹과 사용자 지정 그룹을 생성하고, vRealize Automation 콘솔에 대한 사용자 액세스 권한을 부여합니다.

디렉토리 사용자 또는 그룹에 역할 할당

테넌트 관리자는 사용자나 그룹에 역할을 할당하여 사용자에게 액세스 권한을 부여합니다.

사용자나 그룹이 파이프라인을 수정하고 트리거할 수 있게 허용하려면 해당 사용자와 그룹에 사용 권한을 할당해야 합니다. 사용자와 그룹에 릴리스 관리자 역할을 할당하면 사용자와 그룹이 파이프라인을 수정하고 트리거할 수 있습니다. 사용자와 그룹에 릴리스 엔지니어 역할을 할당하면 사용자와 그룹이 파이프라인을 트리거할 수 있습니다. 자세한 내용은 vRealize Code Stream 사용 가이드를 참조하십시오.

필수 조건

테넌트 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 사용자 및 그룹 > 디렉토리 사용자 및 그룹**을 선택합니다.
- 2 **검색** 상자에 사용자 또는 그룹 이름을 입력하고 Enter 키를 누릅니다.
이름에 콜뱅이(@), 백슬래시(\) 또는 슬래시(/)를 사용하지 마십시오. user@domain 양식으로 전체 사용자 또는 그룹 이름을 입력하여 검색을 최적화할 수 있습니다.
- 3 역할을 할당하려는 사용자 또는 그룹의 이름을 클릭합니다.
- 4 [이 사용자에게 역할 추가] 목록에서 역할을 하나 이상 선택합니다.
[선택한 역할에서 부여한 권한] 목록에는 부여하는 특정 권한이 표시됩니다.
- 5 (선택 사항) **다음**을 클릭하여 사용자 또는 그룹에 대한 추가 정보를 봅니다.
- 6 **사용자 세부 정보** 페이지의 **일반** 탭에서 사용자를 추가할 역할 목록을 스크롤합니다.
 - a 파이프라인을 수정하고 트리거할 수 있는 사용 권한을 사용자에게 부여하려면 **릴리스 관리자** 확인란을 선택합니다.
 - b 파이프라인을 트리거할 수 있는 사용 권한을 사용자에게 부여하려면 **릴리스 엔지니어** 확인란을 선택합니다.
- 7 **업데이트**를 클릭합니다.

현재 vRealize Automation 콘솔에 로그인한 사용자는 로그아웃했다가 vRealize Automation 콘솔에 다시 로그인해야 자신에게 액세스 권한이 부여된 페이지로 이동할 수 있습니다.

후속 작업

선택적으로 Active Directory 연결의 사용자 및 그룹에서 고유한 사용자 지정 그룹을 생성할 수 있습니다. [사용자 지정 그룹 생성](#) 항목을 참조하십시오.

사용자 지정 그룹 생성

테넌트 관리자는 다른 사용자 지정 그룹, ID 저장소 그룹 및 개별 ID 저장소 사용자를 결합하여 사용자 지정 그룹을 생성할 수 있습니다. 사용자 지정 그룹을 사용하면 사업 부문, 부서 또는 기타 조직 구성 단위에 해당하는 비즈니스 그룹에 비해 vRealize Automation 내에서 액세스를 보다 세부적으로 제어할 수 있습니다.

사용자 지정 그룹을 사용하면 작업에 대한 액세스 권한을 표준 vRealize Automation 그룹 할당보다 더 세부적으로 부여할 수 있습니다. 예를 들어 테넌트 내에서 테넌트 관리자가 특정 사용 권한을 가진 사용자를 제어할 수 있도록 하는 사용자 지정 그룹을 생성할 수 있습니다.

사용자 지정 그룹에 역할을 할당할 수 있지만 모든 경우에 필요한 것은 아닙니다. 예를 들어, 모든 시스템의 사전 승인에 사용하도록 시스템 사양 승인자라는 사용자 지정 그룹을 만들 수 있습니다. 또한 모든 그룹을 한 장소에서 관리할 수 있도록 사용자 지정 그룹을 만들어 비즈니스 그룹에 매핑할 수도 있습니다. 이러한 경우 역할을 할당할 필요가 없습니다.

필수 조건

테넌트 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 **관리 > 사용자 및 그룹 > 사용자 지정 그룹**을 선택합니다.

2 **추가** 아이콘(+)을 클릭합니다.

3 **새 그룹 이름** 텍스트 상자에 그룹 이름을 입력합니다.

사용자 지정 그룹 이름에는 세미콜론(;)과 등호(=)의 조합을 사용할 수 없습니다.

4 (선택 사항) **새 그룹 설명** 텍스트 상자에 설명을 입력합니다.

5 [이 그룹에 역할 추가] 목록에서 역할을 하나 이상 선택합니다.

[선택한 역할에서 부여한 권한] 목록에는 부여하는 특정 권한이 표시됩니다.

6 **다음**을 클릭합니다.

7 사용자와 그룹을 추가하여 사용자 지정 그룹을 생성합니다.

a **검색** 상자에 사용자 또는 그룹 이름을 입력하고 Enter 키를 누릅니다.

이름에 콜뱅이(@), 백슬래시(\) 또는 슬래시(/)를 사용하지 마십시오. user@domain 양식으로 전체 사용자 또는 그룹 이름을 입력하여 검색을 최적화할 수 있습니다.

b 사용자 지정 그룹에 추가할 사용자 또는 그룹을 선택합니다.

8 **추가**를 클릭합니다.

현재 vRealize Automation 콘솔에 로그인한 사용자는 로그아웃했다가 vRealize Automation 콘솔에 다시 로그인해야 자신에게 액세스 권한이 부여된 페이지로 이동할 수 있습니다.

비즈니스 그룹 생성

비즈니스 그룹은 서비스와 리소스 집합을 사용자 집합에 연결하는 데 사용됩니다. 이러한 그룹은 종종 LOB(사업 부문), 부서 또는 기타 조직 구성 단위에 해당합니다. 예약을 구성하고 비즈니스 그룹 구성원에 대한 서비스 카탈로그 항목을 프로비저닝하는 권한을 사용자에게 부여할 수 있도록 비즈니스 그룹을 생성합니다.

비즈니스 그룹 역할에 여러 사용자를 추가하려면, 여러 개별 사용자를 추가하거나, ID 저장소 그룹이나 사용자 지정 그룹을 역할에 추가하여 동시에 여러 사용자를 추가할 수 있습니다. 예를 들어 사용자 지정 그룹 판매 지원 팀을 생성하고 해당 그룹을 지원 역할에 추가할 수 있습니다. 또한 기존 ID 저장소 사용자 그룹을 사용할 수 있습니다. 선택하는 사용자 및 그룹은 ID 저장소에서 유효해야 합니다.

vCloud Director 통합을 지원하려면 vRealize Automation 비즈니스 그룹의 동일한 비즈니스 그룹 구성원이 vCloud Director 조직의 구성원이기도 해야 합니다.

테넌트 관리자가 비즈니스 그룹을 생성한 후에는 비즈니스 관리자가 관리자 이메일 주소와 구성원을 수정할 수 있는 권한을 갖습니다. 테넌트 관리자는 모든 옵션을 수정할 수 있습니다.

이 절차는 IaaS가 설치 및 구성되었다고 가정합니다.

필수 조건

- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

- 비즈니스 그룹의 구성원이 생성한 시스템을 특정 Active Directory 조직 구성 단위에 추가하려는 경우 Active Directory 정책을 구성합니다. [Active Directory 정책 생성](#) 항목을 참조하십시오. 비즈니스 그룹을 생성할 때 정책을 적용하거나 나중에 추가할 수 있습니다.
- 프로비저닝된 시스템 이름 앞에 붙는 기본 시스템 접두사를 그룹에 제공하려면 패브릭 관리자에게 접두사를 요청합니다. [시스템 접두사 구성](#) 항목을 참조하십시오. 시스템 접두사는 XaaS 요청에 적용할 수 없습니다.

프로시저

- 1 **관리 > 사용자 및 그룹 > 비즈니스 그룹**을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 비즈니스 그룹 세부 정보를 구성합니다.

옵션	설명
이름	비즈니스 그룹의 이름을 입력합니다.
설명	설명을 입력합니다.
관리자 이메일 수신인	용량 경고 알림을 받아야 하는 사용자의 이메일 주소를 하나 이상 입력합니다. 이메일 별칭 주소는 지원되지 않으며 각 이메일 주소는 특정 사용자에게 해당되는 것이어야 합니다. 여러 항목은 쉼표로 구분합니다. 예를 들면 다음과 같습니다. <code>JoeAdmin@mycompany.com,WeiMgr@mycompany.com</code> .
Active Directory 정책	비즈니스 그룹에 대한 기본 Active Directory 정책을 선택합니다.

- 4 사용자 지정 속성을 추가합니다.
- 5 사용자 이름 또는 사용자 지정 사용자 그룹 이름을 입력하고 Enter 키를 누릅니다.

하나 이상의 개인 또는 사용자 지정 사용자 그룹을 비즈니스 그룹에 추가할 수 있습니다. 사용자를 지금 지정하거나 빈 비즈니스 그룹을 생성하고 나중에 채울 수 있습니다.

옵션	설명
그룹 관리자 역할	사용 권한을 생성하고 그룹에 대한 승인 정책을 할당할 수 있습니다.
지원 역할	비즈니스 그룹의 다른 구성원을 대신하여 서비스 카탈로그 항목을 요청하고 관리할 수 있습니다.
공유 액세스 역할	다른 비즈니스 그룹 구성원이 배포하는 리소스에서 사용하고 작업을 실행할 수 있습니다.
사용자 역할	권한이 부여된 서비스 카탈로그 항목을 요청할 수 있습니다.

- 6 **다음**을 클릭합니다.

7 기본 인프라 옵션을 구성합니다.

옵션	설명
기본 시스템 접두사	<p>비즈니스 그룹에 대해 미리 구성된 시스템 접두사를 선택합니다.</p> <p>이 접두사는 시스템 Blueprint에 의해 사용됩니다. Blueprint가 기본 접두사를 사용하는데 기본 접두사를 제공하지 않으면 비즈니스 그룹 이름을 기반으로 시스템 접두사가 생성됩니다. 가장 좋은 방법은 기본 접두사를 제공하는 것입니다. 특정 접두사로 Blueprint를 구성하거나 서비스 카탈로그 사용자가 Blueprint를 요청할 때 그것을 재정의하도록 허용할 수도 있습니다.</p> <p>XaaS Blueprint는 기본 시스템 접두사를 사용하지 않습니다. 여기에서 접두사를 구성하고 이 비즈니스 그룹에 XaaS Blueprint에 대한 사용 권한을 부여한 경우 이것은 XaaS 시스템의 프로비저닝에 영향을 주지 않습니다.</p>
Active Directory 컨테이너	<p>Active Directory 컨테이너를 입력합니다. 이 옵션은 WIM 프로비저닝에만 적용됩니다.</p> <p>기타 프로비저닝 방법을 사용하려면 프로비저닝된 시스템을 AD 컨테이너에 가입시키기 위한 추가 구성이 필요합니다.</p>

8 추가를 클릭합니다.

패브릭 관리자는 예약을 생성하여 비즈니스 그룹에 리소스를 할당할 수 있습니다. 비즈니스 그룹 관리자는 비즈니스 그룹의 구성원을 위한 사용 권한을 생성할 수 있습니다.

후속 작업

- 비즈니스 그룹에서 시스템을 프로비저닝하는 위치를 기반으로 비즈니스 그룹에 대한 예약을 생성합니다. [예약 선택 시나리오](#) 항목을 참조하십시오.
- 카탈로그 항목이 게시되고 서비스가 존재하는 경우 비즈니스 그룹 구성원에 대한 사용 권한을 생성할 수 있습니다. [사용자에게 서비스, 카탈로그 항목 및 작업에 대한 사용 권한 부여](#) 항목을 참조하십시오.

그룹 구성원을 표시할 때 성능 저하 문제 해결

그룹의 세부 정보를 볼 때 비즈니스 그룹 또는 사용자 지정 그룹 구성원이 느리게 표시됩니다.

문제점

많은 수의 사용자가 있는 환경에서 사용자 정보를 볼 때 사용자 인터페이스에 사용자 이름이 느리게 로드됩니다.

원인

대규모 Active Directory 환경이 포함된 환경에서는 이름을 로드하는 데 더 많은 시간이 걸립니다.

해결 방법

- ◆ 검색 워크로드를 줄이려면 가능한 경우 이름별로 수백 명의 개별 구성원을 추가하는 대신 Active Directory 그룹 또는 사용자 지정 그룹을 사용합니다.

추가 테넌트 생성

시스템 관리자는 사용자가 적절한 애플리케이션 및 리소스에 액세스하여 작업 할당을 완료할 수 있도록 추가적인 vRealize Automation 테넌트를 생성할 수 있습니다.

테넌트는 소프트웨어 인스턴스 내에서 작업하는, 특정 권한을 가진 사용자의 그룹입니다. 일반적으로 기본 vRealize Automation 테넌트는 시스템 설치 및 초기 구성 중에 생성됩니다. 그 이후 관리자는 사용자가 로그인하여 작업 할당을 완료할 수 있도록 추가적인 테넌트를 생성할 수 있습니다. 관리자는 시스템 작업에 필요한 만큼 테넌트를 생성할 수 있습니다. 테넌트를 생성할 때 관리자는 이름, 로그인 URL, 로컬 사용자, 관리자와 같은 기본적인 구성을 지정해야 합니다. 기본적인 테넌트 정보를 구성했다면 테넌트 관리자는 vRealize Automation 콘솔의 [관리] 탭에서 디렉토리 관리 기능을 사용하여 로그인하고 적절한 Active Directory 연결을 설정해야 합니다. 또한 테넌트 관리자는 사용자 지정 브랜딩을 테넌트에 적용할 수 있습니다.

필수 조건

시스템 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 테넌트 정보 지정

테넌트 구성의 첫 번째 단계는 새 테넌트를 명명하고 vRealize Automation에 추가한 후 테넌트별 액세스 URL을 생성하는 것입니다.

2 로컬 사용자 구성

vRealize Automation 시스템 관리자는 해당하는 각 테넌트의 로컬 사용자를 구성해야 합니다.

3 관리자 지정

테넌트에 대해 구성된 ID 저장소에서 하나 이상의 테넌트 관리자와 IaaS 관리자를 지정할 수 있습니다.

테넌트 정보 지정

테넌트 구성의 첫 번째 단계는 새 테넌트를 명명하고 vRealize Automation에 추가한 후 테넌트별 액세스 URL을 생성하는 것입니다.

필수 조건

시스템 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 테넌트**를 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 **이름** 텍스트 상자에 이름을 입력합니다.
- 4 (선택 사항) **설명** 텍스트 상자에 설명을 입력합니다.

5 URL 이름 텍스트 상자에 테넌트의 고유한 식별자를 입력합니다.

이 URL 토큰은 vRealize Automation 콘솔 URL에 테넌트 관련 식별자를 추가하는 데 사용됩니다.

예를 들어 **mytenant**를 입력하여 URL `https://vrealize-appliance-hostname.domain.name/vcac/org/mytenant`를 생성합니다.

참고 vRealize Automation 7.0 및 7.1에서는 테넌트 URL에 소문자만 사용해야 합니다.

6 (선택 사항) 연락처 이메일 텍스트 상자에 이메일 주소를 입력합니다.

7 제출하고 다음 단계로 진행을 클릭합니다.

로컬 사용자 구성

vRealize Automation 시스템 관리자는 해당하는 각 테넌트의 로컬 사용자를 구성해야 합니다.

관리자가 테넌트에 대한 일반 정보를 생성하면 [로컬 사용자] 탭이 활성화되고 관리자는 테넌트에 액세스할 수 있는 사용자를 지정할 수 있습니다. 테넌트 구성이 완료되면 로컬 테넌트 사용자가 해당 테넌트에 로그인하여 작업 할당을 완료할 수 있습니다.

참고 사용자를 추가한 후에는 해당 구성을 변경할 수 없습니다. 사용자 구성에 관한 내용을 변경하려면 사용자를 삭제하고 다시 생성해야 합니다.

프로시저

- 1 [로컬 사용자] 탭에서 **추가** 버튼을 클릭합니다.
- 2 [사용자 세부 정보] 대화 상자의 **이름** 및 **성** 필드에 사용자의 이름과 성을 입력합니다.
- 3 **이메일** 필드에 사용자 이메일 주소를 입력합니다.
- 4 **사용자 이름** 및 **암호** 필드에 사용자의 사용자 ID와 암호를 입력합니다.
- 5 **추가** 버튼을 클릭합니다.
- 6 해당하는 경우 테넌트의 모든 로컬 사용자에 대해 이러한 단계를 반복합니다.

테넌트에 대해 지정된 로컬 사용자가 생성됩니다.

관리자 지정

테넌트에 대해 구성된 ID 저장소에서 하나 이상의 테넌트 관리자와 IaaS 관리자를 지정할 수 있습니다.

테넌트 관리자는 테넌트 관련 브랜딩을 구성하고 ID 저장소, 그룹, 사용 권한 및 해당 테넌트의 컨텍스트 내에 있는 공유 Blueprint를 관리합니다. IaaS 관리자는 IaaS의 인프라 소스 끝점을 구성하고 패브릭 관리자를 지정하고 IaaS 로그를 모니터링합니다.

필수 조건

- IaaS 관리자를 지정하기 전에 IaaS를 설치해야 합니다. IaaS 설치에 대한 자세한 내용은 vRealize Automation 7.3 설치 항목을 참조하십시오.

프로시저

- 1 **테넌트 관리자** 검색 상자에 사용자 또는 그룹의 이름을 입력하고 Enter 키를 누릅니다.
보다 빠른 결과를 얻으려면 전체 사용자 또는 그룹 이름(예: myAdmins@mycompany.domain)을 입력합니다. 이 단계를 반복하여 추가적인 테넌트 관리자를 지정합니다.
- 2 IaaS를 설치한 경우 **IaaS 관리자** 검색 상자에 사용자 또는 그룹의 이름을 입력하고 Enter 키를 누릅니다.
보다 빠른 결과를 얻으려면 전체 사용자 또는 그룹 이름(예: IaaSAdmins@mycompany.domain)을 입력합니다. 이 단계를 반복하여 추가적인 인프라 관리자를 지정합니다.
- 3 **추가**를 클릭합니다.

테넌트 삭제

시스템 관리자는 vRealize Automation에서 원하지 않는 테넌트를 삭제할 수 있습니다.

테넌트를 삭제하는 경우 해당 테넌트가 vRealize Automation 인터페이스에서는 즉시 제거되지만 배포에서 완전하게 제거되려면 몇 시간이 걸릴 수 있습니다. 테넌트를 삭제하고 동일한 URL을 가진 다른 테넌트를 생성하려는 경우 새 테넌트를 생성하기 전에 기존 테넌트가 완전하게 삭제되도록 몇 시간의 여유를 두십시오.

필수 조건

시스템 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 테넌트**를 선택합니다.
- 2 삭제할 테넌트를 선택합니다.
테넌트를 선택할 때 실제 이름을 클릭하지 마십시오. 그러면 테넌트가 편집을 위해 열립니다.
- 3 **삭제**를 클릭합니다.

테넌트가 vRealize Automation 배포에서 삭제됩니다.

(선택 사항) 사용자 지정 브랜딩 구성

vRealize Automation을 사용하면 테넌트 로그인 및 애플리케이션 페이지에 사용자 지정 브랜딩을 적용할 수 있습니다.

사용자 지정 브랜딩에는 텍스트 및 배경색, 비즈니스 로고, 회사 이름, 개인 정보 보호 정책, 저작권 문구 및 테넌트 로그인 페이지나 애플리케이션 페이지에 표시하고자 하는 기타 관련 정보가 포함될 수 있습니다.

테넌트 로그인 페이지를 위한 사용자 지정 브랜딩

[로그인 화면 브랜딩] 페이지에서는 vRealize Automation 테넌트 로그인 페이지에 사용자 지정 브랜딩을 적용할 수 있습니다.

테넌트 로그인 페이지에 기본 vRealize Automation 브랜딩을 사용하거나, [로그인 화면 브랜딩] 페이지를 사용하여 사용자 지정 브랜딩을 구성할 수 있습니다. 참고로 사용자 지정 브랜딩은 모든 테넌트 애플리케이션에 동일한 방식으로 적용됩니다.

이 페이지에서는 모든 테넌트 로그인 페이지의 브랜딩을 구성할 수 있습니다.

[로그인 화면 브랜딩] 페이지의 [미리 보기] 창에 현재 구현되어 있는 테넌트 로그인 브랜딩이 표시됩니다.

참고 새 테넌트 로그인 페이지 브랜딩을 저장한 후 브랜딩이 모든 로그인 페이지에 표시될 때까지 최대 5분의 지연이 있을 수 있습니다.

필수 조건

브랜딩에 사용자 지정 로고나 기타 이미지를 사용하려면 적절한 파일이 준비되어 있어야 합니다.

프로시저

- 1 vRealize Automation에 시스템 또는 테넌트 관리자로 로그인합니다.
- 2 **관리** 탭을 클릭합니다.
- 3 [효과] 머리글 아래의 확인란을 사용하여 원하는 시각적 효과를 선택합니다.
모든 효과는 선택 사항입니다.
- 4 **브랜딩 > 로그인 화면 브랜딩**을 선택합니다.
- 5 [로고] 필드 아래쪽의 **업로드**를 클릭한 다음 적절한 폴더로 이동하여 로고 이미지 파일을 선택합니다.
- 6 원하는 경우 [이미지](선택 사항) 필드 아래쪽의 **업로드**를 클릭한 다음 적절한 폴더로 이동하여 추가적인 이미지 파일을 선택합니다.
- 7 원하는 경우 **배경색**, **마스트 헤드 색상**, **로그인 버튼 배경색** 및 **로그인 버튼 전경색** 필드에 적절한 16진수 코드를 입력합니다.
필요한 경우 인터넷에서 16진수 색상 코드 목록을 검색해 보십시오.
- 8 **저장**을 클릭하여 설정을 적용합니다.

이제 테넌트 사용자가 해당 로그인 페이지에서 사용자 지정 브랜딩을 볼 수 있습니다.

테넌트 애플리케이션을 위한 사용자 지정 브랜딩

[애플리케이션 브랜딩] 페이지에서는 vRealize Automation 테넌트 애플리케이션에 사용자 지정 브랜딩을 적용할 수 있습니다.

사용자 애플리케이션에 기본 vRealize Automation 브랜딩을 사용하거나, [애플리케이션 브랜딩] 페이지를 사용하여 사용자 지정 브랜딩을 구성할 수 있습니다. 이 페이지에서는 애플리케이션 페이지의 머리글과 바닥글에 브랜딩을 구성할 수 있습니다. 참고로 사용자 지정 브랜딩은 모든 사용자 애플리케이션에 동일한 방식으로 적용됩니다.

[애플리케이션 브랜딩] 페이지의 맨 아래쪽에는 현재 구현된 머리글 또는 바닥글 브랜딩이 표시됩니다.

필수 조건

브랜딩에 사용자 지정 로고를 사용하려면 로고 이미지 파일이 준비되어 있어야 합니다.

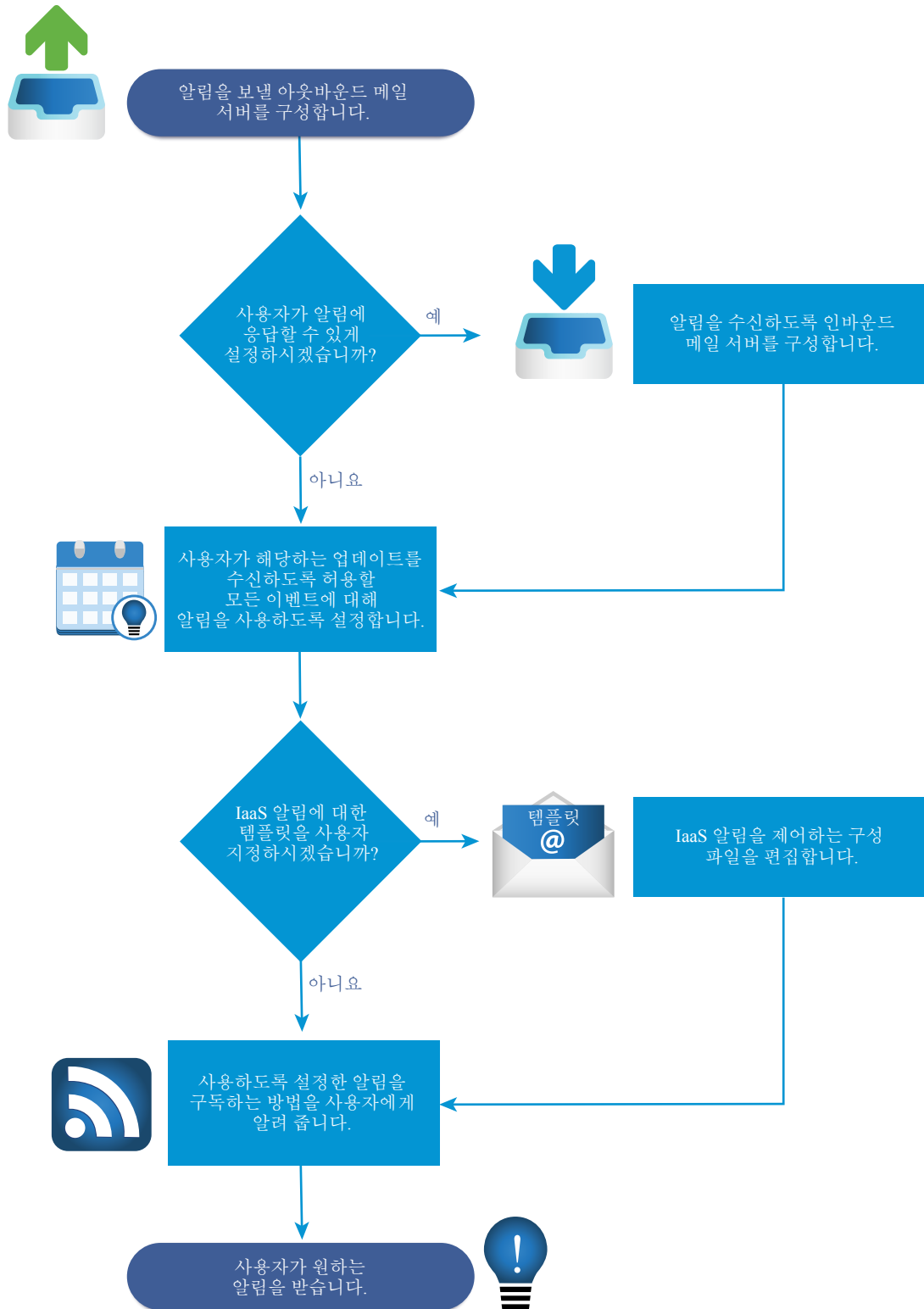
프로시저

- 1 vRealize Automation에 시스템 또는 테넌트 관리자로 로그인합니다.
- 2 **관리** 탭을 클릭합니다.
- 3 **브랜딩 > 애플리케이션 브랜딩**을 선택합니다.
- 4 **머리글** 탭을 클릭합니다(아직 활성화되지 않은 경우).
- 5 기본 vRealize Automation 브랜딩을 사용하려면 **기본값 사용** 확인란을 클릭합니다.
- 6 사용자 지정 브랜딩을 구현하려면 **머리글** 및 **바닥글** 탭의 필드에서 적절한 옵션을 선택합니다.
 - a **머리글 로고** 필드 아래쪽에 있는 **찾아보기** 버튼을 클릭한 다음 적절한 폴더로 이동하여 로고 이미지 파일을 선택합니다.
 - b **회사 이름** 필드에 적절한 회사 이름을 입력합니다.
지정한 이름은 사용자가 로고 위로 마우스를 가져가면 나타납니다.
 - c **제품 이름** 필드에 적절한 이름을 입력합니다.
여기에 입력하는 이름은 애플리케이션 머리글에서 로고 옆에 나타납니다.
 - d **16진수 배경색** 필드에 애플리케이션 주변 배경색에 해당하는 적절한 16진수 색상 코드를 입력합니다.
필요한 경우 인터넷에서 16진수 색상 코드 목록을 검색해 보십시오.
 - e **16진수 텍스트 색** 필드에 텍스트 색상에 해당하는 적절한 16진수 코드를 입력합니다.
필요한 경우 인터넷에서 16진수 텍스트 색상 코드 목록을 검색해 보십시오.
 - f **다음**을 클릭하여 [바닥글] 탭을 활성화합니다.
 - g **저작권 알림** 필드에 원하는 문구를 입력합니다.
 - h **개인 정보 보호 정책 링크** 필드에 회사의 개인 정보 정책에 대한 링크를 입력합니다.
 - i **연락처 링크** 필드에 원하는 회사 연락처 정보를 입력합니다.
- 7 **업데이트**를 클릭하여 브랜딩 구성을 구현합니다.

이제 테넌트 사용자가 해당 애플리케이션 페이지에서 사용자 지정 브랜딩을 볼 수 있습니다.

(선택 사항) 알림 구성을 위한 검사 목록

특정 이벤트가 발생했을 때 사용자에게 알림을 보내도록 vRealize Automation을 구성할 수 있습니다. 사용자는 구독할 알림을 선택할 수 있지만 알림 트리거로 사용하도록 설정된 이벤트 중에서만 선택할 수 있습니다.



알림 구성 검사 목록은 알림을 구성하는 데 필요한 단계의 순서에 대한 개괄적인 개요를 제공하며, 각 단계에 대한 세부 지침 또는 의사 결정 요점에 대한 링크를 제공합니다.

표 2-10. 알림 구성을 위한 검사 목록

작업	필요한 역할	세부 정보
<input type="checkbox"/> 알림을 보낼 아웃바운드 이메일 서버를 구성합니다.	<ul style="list-style-type: none"> ■ 시스템 관리자는 기본 글로벌 서버를 구성합니다. ■ 테넌트 관리자는 해당 테넌트를 위해 서버를 구성합니다. 	테넌트가 사용할 서버를 처음 구성하는 경우에는 테넌트 관련 아웃바운드 이메일 서버 추가 항목을 참조하십시오. 기본 글로벌 서버를 재정의해야 할 경우에는 시스템 기본 아웃바운드 이메일 서버 재정의 항목을 참조하십시오. 모든 테넌트가 사용할 기본 글로벌 서버를 구성하려면 글로벌 아웃바운드 이메일 서버 생성 항목을 참조하십시오.
<input type="checkbox"/> (선택 사항) 사용자가 알림에 응답하여 작업을 완료할 수 있도록 인바운드 이메일 서버를 구성합니다.	<ul style="list-style-type: none"> ■ 시스템 관리자는 기본 글로벌 서버를 구성합니다. ■ 테넌트 관리자는 해당 테넌트를 위해 서버를 구성합니다. 	테넌트가 사용할 서버를 처음 구성하는 경우에는 테넌트 관련 인바운드 이메일 서버 추가 항목을 참조하십시오. 기본 글로벌 서버를 재정의해야 할 경우에는 시스템 기본 인바운드 이메일 서버 재정의 항목을 참조하십시오. 모든 테넌트가 사용할 기본 글로벌 서버를 구성하려면 글로벌 인바운드 이메일 서버 생성 항목을 참조하십시오.
<input type="checkbox"/> (선택 사항) 시스템 만료 날짜 전에 이메일 알림을 보낼 시기를 지정합니다.	시스템 관리자	시스템 만료에 대한 이메일 알림 날짜 사용자 지정 항목을 참조하십시오.
<input type="checkbox"/> 사용자 알림을 트리거할 vRealize Automation 이벤트를 선택합니다. 사용자는 관리자가 알림 트리거로 설정한 이벤트에 대해서만 알림을 구독할 수 있습니다.	테넌트 관리자	알림 구성 항목을 참조하십시오.
<input type="checkbox"/> (선택 사항) 해당 시스템과 관련된 이벤트(예: 리스 만료)에 대해 시스템 소유자에게 알림을 보내는 데 사용할 템플릿을 구성합니다.	vRealize Automation 서버 설치 디렉토리(보통 %SystemDrive%\Program Files\X86\VMware\VMware Workstation\WTemplate\ 아래)의 WTemplates 디렉토리에 액세스할 수 있는 사람이라면 누구나 이러한 이메일 알림에 대한 템플릿을 구성할 수 있습니다.	자동 IaaS 이메일 템플릿 구성 항목을 참조하십시오.
<input type="checkbox"/> 사용하도록 설정한 알림을 구독하는 방법에 대한 지침을 사용자에게 제공합니다. 사용자는 자신의 역할과 관련된 알림만 구독하도록 선택할 수 있습니다.	모든 사용자	알림 구독 항목을 참조하십시오.

알림을 위한 글로벌 이메일 서버 구성

테넌트 관리자는 자신의 테넌트를 위한 알림 구성의 일부로 이메일 서버를 추가할 수 있습니다. 시스템 관리자는 시스템 기본값으로 모든 테넌트에 나타나는 글로벌 인바운드 및 아웃바운드 이메일 서버를 설정할 수 있습니다. 테넌트 관리자가 알림 사용을 설정하기 전에 이러한 설정을 재정의하지 않으면 vRealize Automation은 글로벌 구성된 이메일 서버를 사용합니다.

글로벌 인바운드 이메일 서버 생성

시스템 관리자는 승인 응답과 같은 인바운드 이메일 알림을 처리하기 위해 글로벌 인바운드 이메일 서버를 생성할 수 있습니다. 인바운드 서버는 하나만 생성할 수 있습니다. 이 서버는 모든 테넌트에 대해 기본값으로 표시됩니다. 테넌트 관리자가 알림 사용을 설정하기 전에 이러한 설정을 재정의하지 않으면 vRealize Automation은 글로벌 구성된 이메일 서버를 사용합니다.

필수 조건

시스템 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 이메일 서버**를 선택합니다.
- 2 **추가** 아이콘(+)을 클릭합니다.
- 3 **이메일 - 인바운드**를 선택합니다.
- 4 **확인**을 클릭합니다.
- 5 **이름** 텍스트 상자에 이름을 입력합니다.
- 6 (선택 사항) **설명** 텍스트 상자에 설명을 입력합니다.
- 7 (선택 사항) 보안을 위해 SSL을 사용하도록 **SSL** 확인란을 선택합니다.
- 8 서버 프로토콜을 선택합니다.
- 9 **서버 이름** 텍스트 상자에 서버의 이름을 입력합니다.
- 10 **서버 포트** 텍스트 상자에 서버 포트 번호를 입력합니다.
- 11 **폴더 이름** 텍스트 상자에 이메일의 폴더 이름을 입력합니다.
이 옵션은 IMAP 서버 프로토콜을 선택한 경우에만 필요합니다.
- 12 **사용자 이름** 텍스트 상자에 사용자 이름을 입력합니다.
- 13 **암호** 텍스트 상자에 암호를 입력합니다.
- 14 vRealize Automation 사용자가 회신할 수 있는 이메일 주소를 **이메일 주소** 텍스트 상자에 입력합니다.
- 15 (선택 사항) 알림 서비스가 검색한 모든 처리된 이메일을 서버에서 삭제하려면 **서버에서 삭제**를 선택합니다.
- 16 vRealize Automation이 자체 서명된 인증서를 이메일 서버에서 수락하는지 여부를 선택합니다.
- 17 **연결 테스트**를 클릭합니다.
- 18 **추가**를 클릭합니다.

글로벌 아웃바운드 이메일 서버 생성

시스템 관리자는 아웃바운드 이메일 알림을 처리하기 위해 글로벌 아웃바운드 이메일 서버를 생성할 수 있습니다. 아웃바운드 서버는 하나만 생성할 수 있습니다. 이 서버는 모든 테넌트에 대해 기본값으로 표시됩니다. 테넌트 관리자가 알림 사용을 설정하기 전에 이러한 설정을 재정의하지 않으면 vRealize Automation은 글로벌 구성된 이메일 서버를 사용합니다.

필수 조건

시스템 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 이메일 서버**를 선택합니다.
- 2 **추가** 아이콘(+)을 클릭합니다.
- 3 **이메일 - 아웃바운드**를 선택합니다.
- 4 **확인**을 클릭합니다.
- 5 **이름** 텍스트 상자에 이름을 입력합니다.
- 6 (선택 사항) **설명** 텍스트 상자에 설명을 입력합니다.
- 7 **서버 이름** 텍스트 상자에 서버의 이름을 입력합니다.
- 8 암호화 방법을 선택합니다.
 - **SSL 사용**을 클릭합니다.
 - **TLS 사용**을 클릭합니다.
 - 통신을 암호화하지 않으려면 **없음**을 클릭합니다.
- 9 **서버 포트** 텍스트 상자에 서버 포트 번호를 입력합니다.
- 10 (선택 사항) 서버에서 인증이 필요한 경우 **필요** 확인란을 선택합니다.
 - a **사용자 이름** 텍스트 상자에 사용자 이름을 입력합니다.
 - b **암호** 텍스트 상자에 암호를 입력합니다.
- 11 vRealize Automation 이메일의 출처로 표시할 이메일 주소를 **보낸 사람 주소** 텍스트 상자에 입력합니다.
이 이메일 주소는 제공한 사용자 이름과 암호에 해당합니다.
- 12 vRealize Automation이 자체 서명된 인증서를 이메일 서버에서 수락하는지 여부를 선택합니다.
- 13 **연결 테스트**를 클릭합니다.
- 14 **추가**를 클릭합니다.

테넌트 관련 아웃바운드 이메일 서버 추가

테넌트 관리자는 아웃바운드 이메일 서버를 추가하여 승인 등 작업 항목 완료에 대한 알림을 보낼 수 있습니다.

각 테넌트는 하나의 아웃바운드 이메일 서버만 가질 수 있습니다. 시스템 관리자가 이미 글로벌 아웃바운드 이메일 서버를 구성한 경우 [시스템 기본 아웃바운드 이메일 서버 재정의](#)를 참조하십시오.

필수 조건

- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 이메일 서버에서 인증을 요구하는 경우 지정된 사용자가 ID 저장소 및 비즈니스 그룹에 있어야 합니다.

프로시저

- 1 **관리 > 알림 > 이메일 서버**를 선택합니다.
- 2 **추가** 아이콘(+)을 클릭합니다.
- 3 **이메일 - 아웃바운드**를 선택합니다.
- 4 **확인**을 클릭합니다.
- 5 **이름** 텍스트 상자에 이름을 입력합니다.
- 6 (선택 사항) **설명** 텍스트 상자에 설명을 입력합니다.
- 7 **서버 이름** 텍스트 상자에 서버의 이름을 입력합니다.
- 8 암호화 방법을 선택합니다.
 - **SSL 사용**을 클릭합니다.
 - **TLS 사용**을 클릭합니다.
 - 통신을 암호화하지 않으려면 **없음**을 클릭합니다.
- 9 **서버 포트** 텍스트 상자에 서버 포트 번호를 입력합니다.
- 10 (선택 사항) 서버에서 인증이 필요한 경우 **필요** 확인란을 선택합니다.
 - a **사용자 이름** 텍스트 상자에 사용자 이름을 입력합니다.
 - b **암호** 텍스트 상자에 암호를 입력합니다.
- 11 vRealize Automation 이메일의 출처로 표시할 이메일 주소를 **보낸 사람 주소** 텍스트 상자에 입력합니다.
이 이메일 주소는 제공한 사용자 이름과 암호에 해당합니다.
- 12 vRealize Automation이 자체 서명된 인증서를 이메일 서버에서 수락하는지 여부를 선택합니다.
이 옵션은 암호화를 사용하도록 설정한 경우에만 사용할 수 있습니다.
 - 자체 서명된 인증서를 수락하려면 **예**를 클릭합니다.
 - 자체 서명된 인증서를 거부하려면 **아니요**를 클릭합니다.
- 13 **연결 테스트**를 클릭합니다.
- 14 **추가**를 클릭합니다.

테넌트 관련 인바운드 이메일 서버 추가

사용자가 승인 등 작업 항목 완료에 대한 알림에 응답할 수 있도록 테넌트 관리자는 인바운드 이메일 서버를 추가할 수 있습니다.

각 테넌트는 하나의 인바운드 이메일 서버만 가질 수 있습니다. 시스템 관리자가 이미 글로벌 인바운드 이메일 서버를 구성한 경우 [시스템 기본 인바운드 이메일 서버 재정의](#)를 참조하십시오.

필수 조건

- 테넌트 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 지정된 사용자가 ID 저장소 및 비즈니스 그룹에 있는지 확인합니다.

프로시저

- 1 **관리 > 알림 > 이메일 서버**를 선택합니다.
- 2 **추가** 아이콘(+)을 클릭합니다.
- 3 **이메일 - 인바운드**를 선택하고 **확인**을 클릭합니다.
- 4 다음과 같은 인바운드 이메일 서버 옵션을 구성합니다.

옵션	작업
이름	인바운드 이메일 서버의 이름을 입력합니다.
설명	인바운드 이메일 서버의 설명을 입력합니다.
보안	SSL 사용 확인란을 선택합니다.
프로토콜	서버 프로토콜을 선택합니다.
서버 이름	서버 이름을 입력합니다.
서버 포트	서버 포트 번호를 입력합니다.

- 5 **폴더 이름** 텍스트 상자에 이메일의 폴더 이름을 입력합니다.
이 옵션은 IMAP 서버 프로토콜을 선택한 경우에만 필요합니다.
- 6 **사용자 이름** 텍스트 상자에 사용자 이름을 입력합니다.
- 7 **암호** 텍스트 상자에 암호를 입력합니다.
- 8 vRealize Automation 사용자가 회신할 수 있는 이메일 주소를 **이메일 주소** 텍스트 상자에 입력합니다.
- 9 (선택 사항) 알림 서비스가 검색한 모든 처리된 이메일을 서버에서 삭제하려면 **서버에서 삭제**를 선택합니다.
- 10 vRealize Automation이 자체 서명된 인증서를 이메일 서버에서 수락하는지 여부를 선택합니다.
이 옵션은 암호화를 사용하도록 설정한 경우에만 사용할 수 있습니다.
 - 자체 서명된 인증서를 수락하려면 **예**를 클릭합니다.
 - 자체 서명된 인증서를 거부하려면 **아니요**를 클릭합니다.

11 **연결 테스트**를 클릭합니다.

12 **추가**를 클릭합니다.

시스템 기본 아웃바운드 이메일 서버 재정의

시스템 관리자가 시스템의 기본 아웃바운드 이메일 서버를 구성한 경우, 테넌트 관리자는 이 글로벌 설정을 재정의할 수 있습니다.

필수 조건

테넌트 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 알림 > 이메일 서버**를 선택합니다.
- 2 아웃바운드 이메일 서버를 선택합니다.
- 3 **글로벌 재정의**를 클릭합니다.
- 4 **이름** 텍스트 상자에 이름을 입력합니다.
- 5 (선택 사항) **설명** 텍스트 상자에 설명을 입력합니다.
- 6 **서버 이름** 텍스트 상자에 서버의 이름을 입력합니다.
- 7 암호화 방법을 선택합니다.
 - **SSL 사용**을 클릭합니다.
 - **TLS 사용**을 클릭합니다.
 - 통신을 암호화하지 않으려면 **없음**을 클릭합니다.
- 8 **서버 포트** 텍스트 상자에 서버 포트 번호를 입력합니다.
- 9 (선택 사항) 서버에서 인증이 필요한 경우 **필요** 확인란을 선택합니다.
 - a **사용자 이름** 텍스트 상자에 사용자 이름을 입력합니다.
 - b **암호** 텍스트 상자에 암호를 입력합니다.
- 10 vRealize Automation 이메일의 출처로 표시할 이메일 주소를 **보낸 사람 주소** 텍스트 상자에 입력합니다.

이 이메일 주소는 제공한 사용자 이름과 암호에 해당합니다.
- 11 vRealize Automation이 자체 서명된 인증서를 이메일 서버에서 수락하는지 여부를 선택합니다.

이 옵션은 암호화를 사용하도록 설정한 경우에만 사용할 수 있습니다.

 - 자체 서명된 인증서를 수락하려면 **예**를 클릭합니다.
 - 자체 서명된 인증서를 거부하려면 **아니요**를 클릭합니다.
- 12 **연결 테스트**를 클릭합니다.
- 13 **추가**를 클릭합니다.

시스템 기본 인바운드 이메일 서버 재정의

시스템 관리자가 시스템의 기본 인바운드 이메일 서버를 구성한 경우, 테넌트 관리자는 이 글로벌 설정을 재정의할 수 있습니다.

필수 조건

테넌트 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 알림 > 이메일 서버**를 선택합니다.
- 2 [이메일 서버] 테이블에서 인바운드 이메일 서버를 선택합니다.
- 3 **글로벌 재정의**를 클릭합니다.
- 4 다음과 같은 인바운드 이메일 서버 옵션을 입력합니다.

옵션	작업
이름	인바운드 이메일 서버의 이름을 입력합니다.
설명	인바운드 이메일 서버의 설명을 입력합니다.
보안	보안을 위해 SSL을 사용하도록 SSL 확인란을 선택합니다.
프로토콜	서버 프로토콜을 선택합니다.
서버 이름	서버 이름을 입력합니다.
서버 포트	서버 포트 번호를 입력합니다.

- 5 **폴더 이름** 텍스트 상자에 이메일의 폴더 이름을 입력합니다.
이 옵션은 IMAP 서버 프로토콜을 선택한 경우에만 필요합니다.
- 6 **사용자 이름** 텍스트 상자에 사용자 이름을 입력합니다.
- 7 **암호** 텍스트 상자에 암호를 입력합니다.
- 8 vRealize Automation 사용자가 회신할 수 있는 이메일 주소를 **이메일 주소** 텍스트 상자에 입력합니다.
- 9 (선택 사항) 알림 서비스가 검색한 모든 처리된 이메일을 서버에서 삭제하려면 **서버에서 삭제**를 선택합니다.
- 10 vRealize Automation이 자체 서명된 인증서를 이메일 서버에서 수락하는지 여부를 선택합니다.
이 옵션은 암호화를 사용하도록 설정한 경우에만 사용할 수 있습니다.
 - 자체 서명된 인증서를 수락하려면 **예**를 클릭합니다.
 - 자체 서명된 인증서를 거부하려면 **아니요**를 클릭합니다.
- 11 **연결 테스트**를 클릭합니다.
- 12 **추가**를 클릭합니다.

시스템 기본 이메일 서버로 되돌리기

시스템 기본 서버를 재정의하는 테넌트 관리자는 설정을 원래의 글로벌 설정으로 되돌릴 수 있습니다.

필수 조건

테넌트 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 알림 > 이메일 서버**를 선택합니다.
- 2 되돌릴 이메일 서버를 선택합니다.
- 3 **글로벌로 되돌리기**를 클릭합니다.
- 4 **예**를 클릭합니다.

알림 구성

각 사용자는 알림을 수신할지 여부를 결정하지만 테넌트 관리자는 알림을 트리거하는 이벤트를 결정합니다.

필수 조건

- 테넌트 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 테넌트 관리자 또는 시스템 관리자가 아웃바운드 이메일 서버를 구성했는지 확인합니다. [테넌트 관련 아웃바운드 이메일 서버 추가](#) 항목을 참조하십시오.

프로시저

- 1 **관리 > 알림 > 시나리오**를 선택합니다.
- 2 하나 이상의 알림을 선택합니다.
- 3 **활성화**를 클릭합니다.

기본 설정에서 알림을 구독한 사용자는 이제 알림을 수신합니다.

시스템 만료에 대한 이메일 알림 날짜 사용자 지정

시스템 만료 날짜 전에 이메일 알림을 보낼 시기를 지정할 수 있습니다.

vRealize Automation에서 만료 알림 이메일을 보내는 시스템의 만료 날짜 전 일 수를 지정하는 설정을 변경할 수 있습니다. 이 이메일은 사용자에게 시스템의 만료 날짜를 알려줍니다. 기본 설정은 시스템이 만료되기 7일 전입니다.

프로시저

- 1 관리자 액세스 권한이 있는 자격 증명을 사용하여 vRealize Automation Server에 로그인합니다.
- 2 `/etc/vcac/setenv-user`로 이동하여 파일을 엽니다.

- 3 다음 줄을 파일에 추가하여 시스템이 만료되기 전 일 수를 지정합니다. 이 예에서 3은 시스템이 만료되기 3일 전을 지정합니다.

```
VCAC_OPTS="$VCAC_OPTS -Dlease.enforcement.prearchive.notification.days=3"
```

- 4 다음 명령을 실행하여 가상 장치에서 vCAC 서비스를 다시 시작합니다.

```
service vcac-server restart
```

후속 작업

고가용성 로드 밸런서 환경에서 작업 중인 경우 HA 환경 내 모든 가상 장치에 대해 이 절차를 반복합니다.

자동 IaaS 이메일 템플릿 구성

해당 시스템이 관련된 다양한 vRealize Automation 이벤트에 대해 시스템 소유자에게 알림 이메일이 전송되도록 구성할 수 있습니다.

알림을 트리거하는 이벤트에는 아카이브 기간 및 가상 시스템 리스의 만료 또는 만료 임박이 포함됩니다.

vRealize Automation 이메일 알림 구성, 사용 또는 사용 안 함에 대한 자세한 내용은 다음 블로그 기사와 기술 자료 문서를 참조하십시오.

- [vRealize Automation에서 이메일 사용자 지정](#)
- [Customizing email templates in vRealize Automation \(2088805\)\(vRealize Automation에서 이메일 템플릿 사용자 지정 \(2088805\)\)](#)
- [Examples for customizing email templates in vRealize Automation \(2102019\)\(vRealize Automation에서 이메일 템플릿 사용자 지정 예 \(2102019\)\)](#)

알림 구독

관리자가 알림을 구성한 경우에는 vRealize Automation에서 알림을 받도록 구독할 수 있습니다. 알림 이벤트에는 카탈로그 요청 또는 필요한 승인의 성공적 완료가 포함될 수 있습니다.

필수 조건

vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 기본 설정을 클릭합니다.
- 2 알림 테이블에서 이메일 프로토콜의 **사용** 확인란을 선택합니다.
- 3 적용을 클릭합니다.
- 4 닫기를 클릭합니다.

(선택 사항) 프로비저닝된 시스템에 대한 RDP 연결 지원을 위해 사용자 지정 RDP 파일 생성

시스템 관리자는 IaaS 설계자가 RDP 설정 구성을 위해 Blueprint에서 사용하는 사용자 지정 원격 데스크톱 프로토콜 파일을 생성합니다. RDP 파일을 생성한 다음 파일에 대한 전체 경로 이름을 설계자에게 제공하면 설계자가 이 파일을 Blueprint에 포함할 수 있고 이후 카탈로그 관리자가 RDP 작업에 대한 사용 권한을 사용자에게 부여할 수 있습니다.

참고 Internet Explorer를 사용 중이고 보안 강화 구성을 사용하도록 설정했다면 .rdp 파일을 다운로드할 수 없습니다.

필수 조건

관리자로 IaaS Manager Service에 로그인합니다.

프로시저

- 1 현재 디렉토리를 <vRA_installation_dir>WRdp로 설정합니다.
- 2 동일한 디렉토리에서 Default.rdp 파일을 복사하고 파일 이름을 Console.rdp로 변경합니다.
- 3 편집기에서 Console.rdp 파일을 엽니다.
- 4 RDP 설정을 파일에 추가합니다.
예를 들어 **connect to console:i:1**을 추가합니다.
- 5 분산 환경에서 작업 중인 경우 Model Manager Website 구성 요소가 설치되어 있는 IaaS 호스트 시스템에 관리 권한이 있는 사용자로 로그인합니다.
- 6 Console.rdp 파일을 vRA_installation_dir\Website\WRdp 디렉토리에 복사합니다.

IaaS 설계자는 RDP 사용자 지정 속성을 Windows 시스템 Blueprint에 추가할 수 있고 이후 카탈로그 관리자는 RDP를 사용하여 연결 작업에 대한 사용 권한을 사용자에게 부여할 수 있습니다.

[Windows 시스템 Blueprint에 RDP 연결 지원 추가](#) 항목을 참조하십시오.

(선택 사항) 시나리오: 영역 간 배포를 위한 데이터 센터 위치 추가

시스템 관리자는 패브릭 관리자가 각 데이터 센터의 계산 리소스에 적합한 위치를 적용할 수 있도록 보스턴 및 런던 데이터 센터에 대한 위치를 정의하고자 합니다. Blueprint 설계자는 Blueprint를 생성할 때 사용자가 카탈로그 항목 요청 양식을 작성하면서 보스턴 또는 런던의 시스템을 프로비저닝하도록 선택할 수 있도록 위치 기능을 사용하도록 설정할 수 있습니다.

런던과 보스턴에 데이터 센터가 각각 하나씩 있는 경우, 보스턴 사용자가 런던 인프라에서 시스템을 프로비저닝하지 않게 하거나, 런던 사용자가 보스턴 인프라에서 시스템을 프로비저닝하지 않게 하려고 합니다. 보스턴 사용자가 보스턴 인프라에서 프로비저닝하고 런던 사용자가 런던 인프라에서 프로비저닝하도록 사용자가 시스템을 요청할 때 프로비저닝을 위한 적합한 위치를 선택하도록 허용하고자 합니다.



테넌트 또는 비즈니스 그룹을 기반으로 xml 파일에서 데이터 센터 위치를 필터링할 수 없습니다. 다중 테넌트 환경에서 작업할 때에는 속성 정의를 사용하여 테넌트 또는 비즈니스 그룹을 기반으로 필터링할 수 있습니다. 속성 정의 사용에 대한 자세한 내용은 블로그 게시물 [동적 속성 정의를 사용하는 방법](#)을 참조하십시오.

프로시저

- 1 관리자 자격 증명을 사용하여 IaaS 웹 서버 호스트에 로그인합니다.
이는 IaaS 웹 사이트 구성 요소를 설치한 시스템입니다.
- 2 Windows 서버 설치 디렉토리(일반적으로 %SystemDrive%\Program Files x86\VMware\VCACWServer)의 파일 Website\XmlData\DataCenterLocations.xml을 편집합니다.
- 3 파일의 CustomDataType 섹션을 편집하여 각 위치에 대한 데이터 이름 항목을 생성합니다.

```
<CustomDataType>
  <Data Name="London" Description="London datacenter" />
  <Data Name="Boston" Description="Boston datacenter" />
</CustomDataType>
```

- 4 파일을 저장한 후 닫습니다.
- 5 Manager Service를 다시 시작합니다.
- 6 2개 이상의 IaaS 웹 서버 호스트가 있는 경우 각 중복 인스턴스에서 이 절차를 반복합니다.

패브릭 관리자는 각 데이터 센터에 있는 계산 리소스에 적합한 위치를 적용할 수 있습니다. [시나리오: 영역 간 배포를 위한 계산 리소스에 위치 적용](#) 항목을 참조하십시오.

후속 작업

Blueprint에 Vrm.DataCenter.Location 속성을 추가하거나 Blueprint에서 **요청에 위치 표시** 옵션을 사용하여 사용자가 시스템 프로비저닝을 요청할 때 데이터 센터 위치를 필수적으로 입력하도록 할 수 있습니다.

vRealize Orchestrator 구성

vRealize Orchestrator은 XaaS 및 기타 확장성을 지원하도록 vRealize Automation을 확장하는 자동 및 관리 엔진입니다. vRealize Automation 장치에 미리 구성된 vRealize Orchestrator 서버를 구성 및 사용하거나 vRealize Orchestrator를 외부 서버 인스턴스로 배포하고 외부 인스턴스를 vRealize Automation과 연결할 수 있습니다.

vRealize Orchestrator를 사용하면 관리자와 설계자가 워크플로 디자이너를 사용하여 복잡한 자동화 작업을 개발하고 vRealize Automation에서 워크플로를 액세스 및 실행할 수 있습니다.

vRealize Orchestrator는 vRealize Orchestrator 플러그인을 사용하여 외부 기술과 애플리케이션을 액세스하고 제어할 수 있습니다.

vRealize Orchestrator를 사용하도록 vRealize Automation을 구성하면 XaaS Blueprint 관리의 일환으로 vRealize Orchestrator 서비스 카탈로그에 Orchestrator 워크플로를 게시할 수 있습니다.

IaaS 시스템의 관리를 확장하기 위해 Orchestrator 워크플로를 실행하려면 vRealize Orchestrator를 끝점으로 구성해야 합니다.

구성 권한

시스템 관리자와 테넌트 관리자는 외부 또는 포함된 vRealize Orchestrator 서버를 사용하도록 vRealize Automation을 구성할 수 있습니다.

또한 시스템 관리자는 각 테넌트에서 사용할 수 있는 워크플로 폴더를 결정할 수도 있습니다.

테넌트 관리자는 vRealize Orchestrator 플러그인을 끝점으로 구성할 수 있습니다.

역할	vRealize Orchestrator 관련 구성 권한
시스템 관리자	<ul style="list-style-type: none"> 모든 테넌트에 대해 vRealize Orchestrator 서버를 구성합니다. 테넌트별 기본 vRealize Orchestrator 워크플로 폴더를 정의합니다.
테넌트 관리자	<ul style="list-style-type: none"> 고유한 테넌트에 대해 vRealize Orchestrator 서버를 구성합니다. vRealize Orchestrator 플러그인을 끝점으로 추가합니다.

내장된 vRealize Orchestrator 서버 구성

vRealize Automation 장치에는 vRealize Orchestrator의 미리 구성된 인스턴스가 포함되어 있습니다. vRealize Orchestrator 서버 서비스가 기본적으로 실행 중이지만 제어 센터에 액세스하려면 구성 서비스를 수동으로 시작해야 합니다.

필수 조건

vRealize Automation 장치를 배포합니다. 자세한 내용은 vRealize Automation 7.3 설치에서 vRealize Automation 장치 배포 항목을 참조하십시오.

프로시저

- 1 시스템 관리자 또는 테넌트 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 2 관리 > VRO 구성 > 서버 구성을 선택합니다.
- 3 기본 Orchestrator 서버 사용을 클릭합니다.

포함된 vRealize Orchestrator 서버에 대한 연결이 이제 구성되었습니다. **VCAC** 워크플로 폴더와 관련 유틸리티 작업의 가져오기가 자동으로 수행됩니다. **VCAC > ASD** 워크플로 폴더에는 끝점을 구성하고 리소스 매핑을 생성하기 위한 워크플로가 포함되어 있습니다.

테넌트에 대한 기본 워크플로 폴더 구성

시스템 관리자는 각기 다른 폴더로 워크플로를 그룹화한 다음 테넌트별 워크플로 범주를 정의할 수 있습니다. 이렇게 함으로써 시스템 관리자는 다른 테넌트의 사용자에게 동일한 vRealize Orchestrator 서버의 다른 워크플로 폴더에 대한 액세스 권한을 부여할 수 있습니다.

필수 조건

시스템 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 고급 서비스 > 기본 vRO 폴더**를 선택합니다.
- 2 편집할 테넌트의 이름을 클릭합니다.
- 3 vRealize Orchestrator 워크플로 라이브러리를 찾아본 다음 폴더를 선택합니다.
- 4 **추가**를 클릭합니다.

테넌트에 대한 기본 vRealize Orchestrator 워크플로 폴더를 정의했습니다.

후속 작업

기본 워크플로 폴더를 정의할 모든 테넌트에 대해 해당 절차를 반복합니다.

vRealize Orchestrator 구성 인터페이스에 로그인

vRealize Automation에 포함된 기본 vRealize Orchestrator 인스턴스의 구성을 편집하려면 vRealize Orchestrator 구성 서비스를 시작하고 vRealize Orchestrator 구성 인터페이스에 로그인해야 합니다.

vRealize Orchestrator 구성 서비스는 vRealize Automation 장치에서 기본적으로 시작되지 않습니다. vRealize Orchestrator 구성 서비스를 시작하여 vRealize Orchestrator 구성 인터페이스에 액세스해야 합니다.

프로시저

- 1 vRealize Orchestrator 구성 서비스를 시작합니다.
 - a vRealize Automation 장치 Linux 콘솔에 루트로 로그인합니다.
 - b `service vco-configurator start`를 입력하고 Enter 키를 누릅니다.
- 2 웹 브라우저에서 vRealize Automation URL에 연결합니다.
- 3 **vRealize Orchestrator 제어 센터**를 클릭합니다.

`https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter`로 리디렉션됩니다.
- 4 vRealize Orchestrator 제어 센터에 로그인합니다.

사용자 이름은 vRealize Automation 장치 관리자가 구성합니다.

vRealize Orchestrator 클라이언트에 로그인합니다.

일반적인 관리 작업을 수행하거나 기본 vRealize Orchestrator 인스턴스에서 워크플로를 편집하고 생성하려면 vRealize Orchestrator 클라이언트에 로그인해야 합니다.

vRealize Orchestrator 클라이언트 인터페이스는 관리 권한을 가지고 있으며 워크플로, 작업 및 기타 사용자 지정 요소를 개발하고자 하는 개발자를 위해 설계되었습니다.

프로시저

- 1 웹 브라우저에서 vRealize Automation URL에 연결합니다.
- 2 **vRealize Orchestrator 클라이언트**를 클릭합니다.
클라이언트 파일이 다운로드됩니다.
- 3 다운로드를 클릭하고 프롬프트에 따릅니다.
- 4 vRealize Orchestrator 로그인 페이지에서 **호스트 이름** 텍스트 상자에 vRealize Automation 장치의 도메인 이름 또는 IP를 입력하고 **443**을 기본 포트 번호로 입력합니다.
예를 들어 `vrealize_automation_appliance_ip:443`을 입력합니다.
- 5 vRealize Orchestrator 클라이언트 사용자 이름과 암호를 사용하여 로그인합니다.
자격 증명은 기본 테넌트 관리자의 사용자 이름과 암호입니다.
- 6 **인증서 경고** 창에서 인증서 경고를 처리할 옵션을 선택합니다.

vRealize Orchestrator 클라이언트는 SSL 인증서를 사용하여 vRealize Orchestrator 서버와 통신합니다. 신뢰할 수 있는 CA는 설치하는 동안에는 인증서에 서명하지 않습니다. vRealize Orchestrator 서버에 연결할 때마다 인증서 경고가 수신됩니다.

옵션	설명
무시	현재 SSL 인증서를 계속 사용합니다. 같은 vRealize Orchestrator 서버에 다시 연결하거나, 원격 vRealize Orchestrator 서버와 워크플로를 동기화하려고 시도하면 경고 메시지가 다시 나타납니다.
취소	창을 닫고 로그인 프로세스를 중지합니다.
이 인증서를 설치하고 이와 관련된 보안 경고를 더 이상 표시 안 함	인증서를 설치하고 보안 경고를 더 이상 표시하지 않으려면 이 확인란을 선택하고 무시 를 클릭합니다.

기본 SSL 인증서를 CA가 서명한 인증서로 변경할 수 있습니다. SSL 인증서를 변경하는 데 대한 자세한 내용은 VMware vRealize Orchestrator 설치 및 구성을 참조하십시오.

후속 작업

시스템에서 루트 액세스 권한을 설정하거나, 워크플로를 개발하거나, 패키지를 가져올 수 있습니다. 자세한 내용은 VMware vRealize Orchestrator 클라이언트 사용 및 VMware vRealize Orchestrator를 사용한 개발을 참조하십시오.

외부 vRealize Orchestrator 서버 구성

외부 vRealize Orchestrator 서버를 사용하도록 vRealize Automation을 설정할 수 있습니다.

시스템 관리자는 모든 테넌트에 대해 전체적으로 기본 vRealize Orchestrator 서버를 구성할 수 있습니다. 테넌트 관리자는 해당 테넌트에 대해서만 vRealize Orchestrator 서버를 구성할 수 있습니다.

외부 vRealize Orchestrator 서버 인스턴스에 연결하려면 vRealize Orchestrator에서 보기 및 실행 권한을 가진 사용자 계정이 필요합니다.

- Single Sign-On 인증. 사용자 정보가 XaaS 요청과 함께 vRealize Orchestrator로 전달되고 사용자에게 요청된 워크플로에 대한 보기 및 실행 권한이 부여됩니다.
- 기본 인증. 제공된 사용자 계정이 보기 및 실행 권한을 가진 vRealize Orchestrator 그룹의 구성원이거나 vcoadmins 그룹의 구성원이어야 합니다.

필수 조건

- 외부 vRealize Orchestrator 장치를 설치 및 구성합니다. vRealize Orchestrator 정보 센터 (https://www.vmware.com/support/pubs/orchestrator_pubs.html)에서 vRealize Orchestrator 설치 및 구성 항목을 참조하십시오.
- 시스템 관리자 또는 테넌트 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 기본 워크플로 폴더를 구성합니다. [테넌트에 대한 기본 워크플로 폴더 구성](#) 항목을 참조하십시오.

프로시저

- 1 **관리 > vRO 구성 > 서버 구성**을 선택합니다.
- 2 **외부 Orchestrator 서버 사용**을 클릭합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 4 **호스트** 텍스트 상자에 vRealize Orchestrator 서버가 실행되는 시스템의 IP 또는 DNS 이름을 입력합니다.

참고 외부 Orchestrator가 클러스터 모드에서 작동하도록 구성되어 있는 경우 클러스터의 Orchestrator 서버에 걸쳐 클라이언트 요청을 분산하는 로드 밸런서 가상 서버의 IP 주소 또는 호스트 이름을 입력합니다.

- 5 **포트** 텍스트 상자에 외부 vRealize Orchestrator 서버와 통신하기 위한 포트 번호를 입력합니다.

8281은 vRealize Orchestrator의 기본 포트입니다.

6 인증 유형을 선택합니다.

옵션	설명
Single Sign-On	vCenter Single Sign-On을 사용하여 vRealize Orchestrator 서버에 연결합니다. 이 옵션은 하나의 공통 vCenter Single Sign-On 인스턴스를 사용하도록 vRealize Orchestrator 및 vRealize Automation을 구성한 경우에만 적용할 수 있습니다.
기본	사용자 이름 및 암호 텍스트 상자에 입력하는 사용자 이름과 암호를 사용하여 vRealize Orchestrator 서버에 연결합니다. 제공하는 계정은 vRealize Orchestrator vcoadmins 그룹의 구성원이거나 보기 및 실행 권한을 가진 그룹의 구성원이어야 합니다.

7 연결 테스트를 클릭합니다.

8 확인을 클릭합니다.

외부 vRealize Orchestrator 서버에 대한 연결을 구성했고 **VCAC** 워크플로 폴더 및 관련 유틸리티를 자동으로 가져왔습니다. **VCAC > ASD** 워크플로 폴더에는 끝점을 구성하고 리소스 매핑을 생성하기 위한 워크플로가 포함되어 있습니다.

후속 작업

[vRealize Orchestrator 클라이언트에 로그인합니다.](#)

리소스 구성

vRealize Automation Blueprint 정의 및 시스템 프로비저닝을 지원하도록 끝점, 예약 및 네트워크 프로파일 같은 리소스를 구성할 수 있습니다.

IaaS 리소스 구성을 위한 검사 목록

IaaS 관리자와 패브릭 관리자는 IaaS 리소스를 구성하여 기존 인프라를 vRealize Automation과 통합하고 인프라 리소스를 vRealize Automation 비즈니스 그룹에 할당합니다.

IaaS 리소스 구성을 위한 검사 목록을 사용하면 IaaS 리소스를 구성하는 데 필요한 일련의 단계에 대한 개괄적인 개요를 볼 수 있습니다.

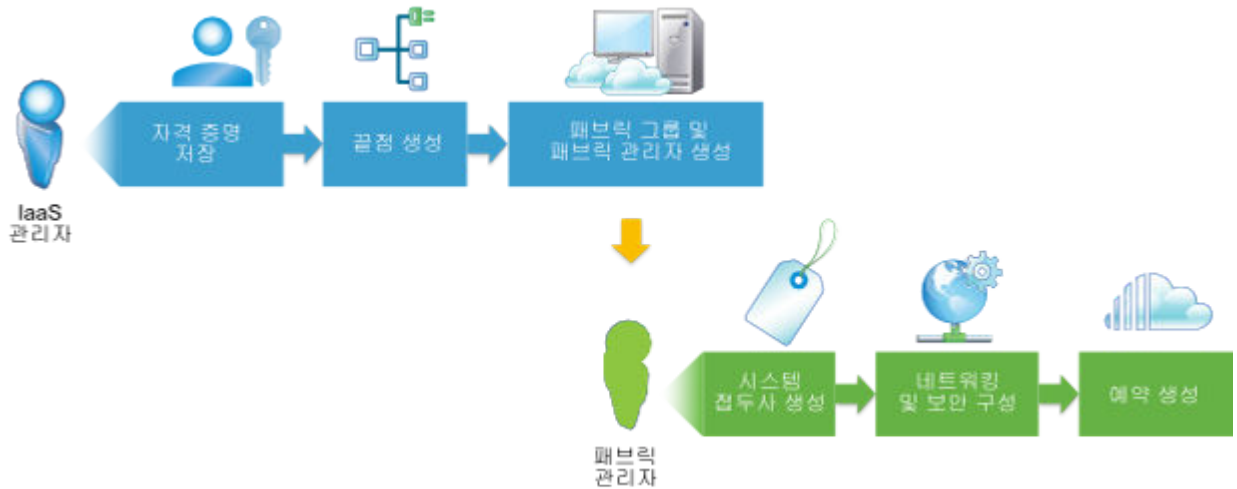


표 2-11. IaaS 리소스 구성을 위한 검사 목록

작업	vRealize Automation 역할	세부 정보
□ 인프라에 대한 끝점을 생성하여 리소스를 vRealize Automation 관리 대상으로 만듭니다.	IaaS 관리자	끝점 선택 시나리오.
□ 패브릭 그룹을 생성하여 인프라 리소스를 그룹으로 구성하고, 해당 리소스를 관리할 관리자 한 명 이상을 vRealize Automation 패브릭 관리자로 할당합니다.	IaaS 관리자	패브릭 그룹 생성.
□ vRealize Automation를 통해 프로비저닝되는 시스템의 이름을 생성하는 데 사용되는 시스템 접두사를 구성합니다.	패브릭 관리자	시스템 접두사 구성.
□ (선택 사항) 프로비저닝된 시스템의 네트워크 설정을 구성할 네트워크 프로파일을 생성합니다.	패브릭 관리자	네트워크 프로파일 생성.
□ 예약, 그리고 필요한 경우 예약과 스토리지 예약 프로파일을 생성하여 인프라 리소스를 비즈니스 그룹에 할당합니다.	<ul style="list-style-type: none"> IaaS 관리자 (패브릭 관리자로도 구성된 경우) 패브릭 관리자 	예약 및 예약 정책 구성.

끝점 구성

vRealize Automation에서 현재 인프라와 통신할 수 있게 하는 끝점을 생성하고 구성합니다.

끝점 정의는 유형에 따라 분류됩니다.

클라우드

클라우드 범주에는 vCloud Air, vCloud Director, Amazon EC2 및 OpenStack 끝점 유형이 포함됩니다.

IPAM

이 범주는 Infoblox IPAM 같은 타사 IPAM 끝점 유형을 vRealize Orchestrator 워크플로에 등록한 경우에만 표시됩니다.

■ 관리

이 범주에는 vRealize Operations Manager 끝점만 포함됩니다.

■ 네트워크 및 보안

이 범주에는 프록시 및 NSX 끝점 유형이 포함됩니다.

프록시 끝점은 Amazon, vCloud Air 또는 vCloud Director 끝점에 연결할 수 있습니다.

NSX 끝점은 vSphere 끝점에 연결할 수 있습니다.

■ 오케스트레이션

이 범주에는 vRealize Orchestrator 끝점만 포함됩니다.

■ 스토리지

이 범주에는 NetApp ONTAP 끝점이 포함됩니다.

■ 가상

가상 범주에는 vSphere, Hyper-V(SCVMM) 및 KVM(RHEV) 끝점 유형이 포함됩니다.

vRealize Orchestrator에서 추가적인 끝점 유형을 구성한 후 vRealize Automation에서 지원되는 끝점 유형과 함께 사용할 수 있습니다. 프로그래밍 방식으로 끝점을 가져오고 내보낼 수도 있습니다.

업그레이드 또는 마이그레이션 후 끝점 사용에 대한 자세한 내용은 [업그레이드 또는 마이그레이션된 끝점 사용 시 고려 사항](#)을 참조하십시오.

끝점 선택 시나리오

대상 끝점 유형에 따라 끝점 시나리오를 선택합니다.

사용할 수 있는 끝점 설정에 대한 자세한 내용은 [끝점 설정 참조](#)를 참조하십시오.

표 2-12. 끝점 선택 시나리오

끝점	추가 정보
vSphere	vSphere 끝점 생성
NSX	NSX 끝점을 생성하고 vSphere 끝점에 연결
vCloud Air(구독 또는 OnDemand)	vCloud Air 끝점 생성
vCloud Director	vCloud Director 끝점 생성
vRealize Orchestrator	vRealize Orchestrator 끝점 생성
vRealize Operations	vRealize Operations Manager 끝점 생성
타사 IPAM 제공자	타사 IPAM 제공자 끝점 생성
Microsoft Azure	Microsoft Azure 끝점 생성
Puppet	Puppet 끝점 생성
Amazon	<ul style="list-style-type: none"> ■ Amazon 끝점 생성 ■ (선택 사항) Amazon 인스턴스 유형 추가
OpenStack	OpenStack 끝점 생성

표 2-12. 끝점 선택 시나리오 (계속)

끝점	추가 정보
프록시	프록시 끝점을 생성하고 클라우드 끝점에 연결
Hyper-V(SCVMM)	Hyper-V(SCVMM) 끝점 생성
KVM(RHEV)	끝점 설정 참조
NetApp ONTAP	<ul style="list-style-type: none"> 가상 프로비저닝을 위한 공간 효율적인 스토리지 끝점 설정 참조
Hyper-V(독립형), XenServer 또는 Xen 풀 마스터	Hyper-V, XenServer 또는 Xen 풀 끝점 생성
끝점 가져오기	프로그래밍 방식으로 끝점 가져오기 또는 내보내기

끝점 설정 참조

끝점 설정은 데이터 수집 및 서비스 카탈로그 배포를 위한 위치 및 액세스 자격 증명을 정의하는 데 사용됩니다.

일반 탭

대부분의 vRealize Automation 끝점에는 다음 옵션이 포함됩니다. 특정 끝점 유형에만 해당하는 설정은 별도로 명시되어 있습니다.

표 2-13. 일반 탭 설정

설정	설명
이름	끝점 이름을 입력합니다.
설명	끝점 설명을 입력합니다.
주소	<p>끝점별 주소 형식을 사용하여 끝점 주소를 입력합니다.</p> <ul style="list-style-type: none"> KVM(RHEV) 또는 NetApp ONTAP 끝점의 주소는 다음 형식 중 하나여야 합니다. <ul style="list-style-type: none"> <code>https://FQDN</code> <code>https://IP_address</code> <p>예: <code>https://mycompany-kvmrhev1.mycompany.local</code> 또는 <code>netapp-1.mycompany.local</code></p> OpenStack 끝점의 주소는 <code>https://FQDN/powervc/openstack/ service</code> 형식이어야 합니다. 예: <code>https://openstack.mycompany.com/powervc/openstack/admin.</code> OpenStack 끝점의 주소는 다음 형식 중 하나여야 합니다. <ul style="list-style-type: none"> <code>https://FQDN:500</code> <code>https://IP_address:500</code> vSphere 끝점의 주소는 <code>https://host/sdk</code> 형식이어야 합니다. NSX 끝점의 주소는 <code>https://host</code> 형식이어야 합니다. vRealize Orchestrator 끝점의 주소는 <code>https</code> 프로토콜 주소여야 하며 vRealize Orchestrator 서버의 정규화된 도메인 이름이나 IP 주소 및 vRealize Orchestrator 포트 번호를 포함해야 합니다(예: <code>https://vrealize-automation-appliance-hostname:443/vco.</code>) vRealize Operations 끝점의 주소는 <code>https://host/suite-api</code> 형식이어야 합니다.

표 2-13. 일반 탭 설정 (계속)

설정	설명
통합 자격 증명	vSphere 통합 자격 증명을 사용하도록 선택한 경우에는 사용자 이름과 암호를 입력할 필요가 없습니다. 이 설정은 vSphere 끝점에만 적용됩니다.
사용자 이름	사용자 인터페이스에 제안된 대로 끝점별 형식으로 끝점에 대해 저장한 관리자 수준 사용자 이름을 입력합니다.
암호	끝점에 대해 저장한 관리자 수준의 암호를 입력합니다.
OpenStack 프로젝트	OpenStack 테넌트 이름을 입력합니다. 이 설정은 OpenStack 끝점에만 적용됩니다.
조직	조직 관리자인 경우에는 vCloud Director 조직 이름을 입력할 수 있습니다. 이 설정은 vCloud Director에만 적용됩니다.
액세스 키 ID	Amazon AWS 키 ID를 입력합니다. 이 설정은 Amazon 끝점에만 적용됩니다.
비밀 액세스 키	Amazon AWS 비밀 액세스 키를 입력합니다. 이 설정은 Amazon 끝점에만 적용됩니다.
포트	연결할 포트 값을 프록시 끝점 주소에 입력합니다. 이 설정은 프록시 끝점에만 적용됩니다.
우선 순위	1보다 크거나 같은 정수를 우선 순위 값으로 입력합니다. 값이 작을수록 우선 순위가 높습니다. 우선 순위 값은 포함된 <code>VMware.VCenterOrchestrator.Priority</code> 사용자 지정 속성에 연결됩니다. 이 설정은 vRealize Orchestrator 끝점에만 적용됩니다.

속성 탭

모든 끝점 유형은 속성 탭을 사용하여 사용자 지정 속성 또는 속성 그룹과 설정을 캡처합니다. 특정 끝점 유형의 사용자 지정 속성 예를 보려면 사용자 지정 속성 참조 자료 항목을 참조하십시오.

연결 탭

어느 끝점에서 연결하는지에 따라 NSX 끝점 또는 프록시 끝점에 대한 연결을 생성할 수 있습니다. vSphere 끝점을 NSX 끝점과 연결하여 vSphere 끝점에 NSX 설정을 할당할 수 있습니다. vCloud Air, vCloud Director 또는 Amazon 끝점을 프록시 끝점과 연결하여 vCloud Air, vCloud Director 또는 Amazon 끝점에 프록시 설정을 할당할 수도 있습니다.

연결 테스트

연결 테스트 작업을 사용하여 vSphere, NSX 또는 vRealize Operations Manager 끝점의 자격 증명, 호스트 끝점 주소 및 인증서를 검증할 수 있습니다. [연결 테스트를 사용할 때의 고려 사항](#) 항목을 참조하십시오.

vSphere 끝점 생성

vRealize Automation에서 vSphere 환경과 통신하고, 계산 리소스를 검색하고, 데이터를 수집하고, 시스템을 프로비저닝하도록 허용하는 끝점을 생성할 수 있습니다. 필요한 경우 NSX 끝점에 연결하여 NSX 설정을 vSphere 끝점에 연결할 수 있습니다.

NSX Manager를 사용 중이던 vSphere 끝점을 업그레이드 또는 마이그레이션한 경우 소스 vSphere 끝점과 새로운 NSX 끝점 간 연결이 포함된 새로운 NSX 끝점이 생성됩니다.

vSphere 환경이 NSX와 통합되어 있는 경우 [NSX 끝점을 생성하고 vSphere 끝점에 연결](#) 항목을 참조하십시오.

연결 및 인증서 신뢰 검증에 대한 자세한 내용은 [연결 테스트를 사용할 때의 고려 사항](#) 항목을 참조하십시오.

필수 조건

- **laaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- vSphere 프록시 에이전트를 설치하여 vSphere 끝점을 관리하고 끝점 및 에이전트에 대해 동일한 정확한 이름을 사용해야 합니다. 에이전트 설치에 대한 자세한 내용은 vRealize Automation 7.3 설치 항목을 참조하십시오.
- vSphere 끝점에 대해 추가적인 NSX 네트워크 및 보안 설정을 구성하려면 NSX 끝점을 생성하십시오. vSphere 끝점을 생성할 때 NSX 끝점에 연결할 수 있습니다. [NSX 끝점을 생성하고 vSphere 끝점에 연결](#) 항목을 참조하십시오.

프로시저

1 **인프라 > 끝점 > 끝점**을 선택합니다.

2 **새로 만들기 > 가상 > vSphere**를 선택합니다.

3 **이름** 텍스트 상자에 이름을 입력합니다.

이름은 설치 중 vSphere 프록시 에이전트에 제공한 끝점 이름과 일치해야 하며, 그렇지 않으면 데이터 수집이 실패합니다.

4 (선택 사항) **설명** 텍스트 상자에 설명을 입력합니다.

5 **주소** 텍스트 상자에 vCenter Server 인스턴스의 URL을 입력합니다.

URL은 `https://hostname/sdk` 또는 `https://IP_address/sdk` 형식이어야 합니다.

예를 들어 `https://vsphereA/sdk`를 입력합니다.

6 vSphere 관리자 수준 사용자 이름과 암호를 입력하거나 vSphere 통합 자격 증명을 대신 사용합니다.

사용자 지정 특성을 수정할 수 있는 권한을 가진 자격 증명을 제공합니다.

사용자 이름 형식은 `domain\username`입니다.

vSphere 프록시 에이전트의 서비스 계정을 사용하여 vCenter Server에 연결하려면 **통합 자격 증명 사용**을 선택합니다.

vSphere 통합 자격 증명을 사용하도록 선택한 경우에는 사용자 이름과 암호를 입력할 필요가 없습니다.

- 7 (선택 사항) **속성**을 클릭하고 제공된 사용자 지정 속성, 속성 그룹 또는 끝점에 대한 사용자 고유의 속성 정의를 추가합니다.
- 8 (선택 사항) 끝점에 대한 NSX 네트워크 및 보안 설정을 구성하려면 **연결**을 클릭하고 기존 NSX 끝점에 연결합니다.

연결을 생성하려면 최소 하나의 NSX 끝점이 있어야 합니다.

- 9 (선택 사항) 자격 증명, 호스트 끝점 주소 및 인증서 신뢰를 검증하려면 **연결 테스트**를 클릭합니다. 이 작업은 끝점에서 데이터가 수집될 수 있도록 Manager Service와 에이전트가 실행 중인지도 확인합니다. **확인** 작업은 이와 동일한 조건을 테스트합니다.

연결 테스트 작업은 다음 조건에 대한 정보를 반환합니다.

- 인증서 오류

인증서가 없거나, 인증서를 신뢰할 수 없거나, 인증서가 만료된 경우 인증서 지문을 수락하라는 메시지가 표시됩니다. 지문을 수락하지 않아도 끝점을 저장할 수 있지만 시스템 프로비저닝이 실패할 수 있습니다.

- 에이전트 오류

연결된 vSphere 에이전트를 찾을 수 없습니다. 테스트가 성공하려면 에이전트가 실행 중이어야 합니다.

- 호스트 오류

지정된 끝점 주소에 연결할 수 없거나 연결된 Manager Service가 실행 중이 아닙니다. 테스트가 성공하려면 Manager Service가 실행 중이어야 합니다.

- 자격 증명 오류

지정된 사용자 이름 및 암호 조합이 지정된 주소의 끝점에 대해 올바르지 않습니다.

- Timeout

허용된 2분이라는 시간 내에 테스트 작업을 완료하지 못했습니다.

연결 테스트 작업이 실패해도 끝점을 저장할 수 있지만 시스템 프로비저닝이 실패할 수 있습니다.

신뢰할 수 있는 인증서 문제(예: 인증서가 만료됨)가 있는 경우 인증서 지문을 수락하라는 메시지가 표시됩니다.

- 10 **확인**을 클릭하여 끝점을 저장합니다.

확인 작업은 **연결 테스트** 작업과 동일한 조건을 테스트합니다. 이전 조건을 찾은 경우 메시지가 반환됩니다. 저장이 가능한 경우 검토할 수 있도록 화면에 오류가 표시됩니다.

vRealize Automation이 끝점에서 데이터를 수집하고 계산 리소스를 검색합니다.

참고 초기 데이터 수집 후에 vSphere 데이터 센터의 이름을 바꾸지 마십시오. 바꾸는 경우 프로비저닝이 실패할 수 있습니다.

후속 작업

끝점에서 패브릭 그룹으로 계산 리소스를 추가합니다. [패브릭 그룹 생성](#) 항목을 참조하십시오.

NSX 끝점을 생성하고 vSphere 끝점에 연결

NSX 끝점을 생성하고 해당 NSX 설정을 기존 vSphere 끝점에 연결할 수 있습니다.

NSX Manager를 사용 중이던 vSphere 끝점을 업그레이드 또는 마이그레이션한 경우 소스 vSphere 끝점과 새로운 NSX 끝점 간 연결이 포함된 새로운 NSX 끝점이 생성됩니다.

NSX 연결 및 인증서 신뢰 검증에 대한 자세한 내용은 [연결 테스트를 사용할 때의 고려 사항](#)을 참조하십시오.

NSX 끝점 생성과 관련된 정보는 이 [vmwarelab 블로그 게시물](#)과 같은 공개 문서를 참조하십시오.

필수 조건

- **laaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- vSphere 프록시 에이전트를 설치하여 vSphere 끝점을 관리하고 끝점 및 에이전트에 대해 동일한 정확한 이름을 사용해야 합니다. 에이전트 설치에 대한 자세한 내용은 vRealize Automation 7.3 설치 항목을 참조하십시오.
- NSX 네트워크 설정을 구성합니다. [네트워크 및 보안 구성 요소 설정 구성](#) 항목을 참조하십시오.
- [vSphere 끝점 생성](#).

vRealize Automation에서 NSX 네트워크, 보안 및 로드 밸런싱 기능 사용을 준비하는 과정에서, NSX Manager 자격 증명을 사용할 때에는 NSX Manager 관리자 계정을 사용해야 합니다.

프로시저

- 1 **인프라 > 끝점 > 끝점**을 선택합니다.
- 2 **새로 만들기 > 네트워크 및 보안 > NSX**를 선택합니다.
- 3 **이름** 텍스트 상자에 이름을 입력합니다.
- 4 (선택 사항) **설명** 텍스트 상자에 설명을 입력합니다.
- 5 **주소** 텍스트 상자에 NSX 인스턴스의 URL을 입력합니다.
URL은 `https://hostname` 또는 `https://IP_address` 형식이어야 합니다.
예: `https://nsx-manager.local`.
- 6 NSX 끝점에 대해 저장된 NSX 관리자 수준의 사용자 이름과 암호를 입력합니다.
- 7 (선택 사항) **속성**을 클릭하고 제공된 사용자 지정 속성, 속성 그룹 또는 끝점에 대한 사용자 고유의 속성 정의를 추가합니다.

- 8 NSX 네트워크 및 보안 설정을 기존 vSphere 끝점에 연결하려면 **연결**을 클릭하고 기존 vSphere 끝점을 선택합니다.

연결을 생성하려면 우선 vSphere 끝점을 생성해야 합니다.

NSX 끝점은 하나의 vSphere 끝점에만 연결할 수 있습니다. 이러한 연결 제약 조건은 범용 요청 시 네트워크를 프로비저닝하여 다른 vCenter에서 프로비저닝된 vSphere 시스템에 이 네트워크를 연결할 수 없다는 것을 의미합니다.

- 9 (선택 사항) 자격 증명, 호스트 끝점 주소 및 인증서 신뢰를 검증하려면 **연결 테스트**를 클릭합니다. 이 작업은 끝점에서 데이터가 수집될 수 있도록 Manager Service와 에이전트가 실행 중인지도 확인합니다. **확인** 작업은 이와 동일한 조건을 테스트합니다.

연결 테스트 작업은 다음 조건에 대한 정보를 반환합니다.

- 인증서 오류

인증서가 없거나, 인증서를 신뢰할 수 없거나, 인증서가 만료된 경우 인증서 지문을 수락하라는 메시지가 표시됩니다. 지문을 수락하지 않아도 끝점을 저장할 수 있지만 시스템 프로비저닝이 실패할 수 있습니다.

- 에이전트 오류

연결된 vSphere 에이전트를 찾을 수 없습니다. 테스트가 성공하려면 에이전트가 실행 중이어야 합니다.

- 호스트 오류

지정된 끝점 주소에 연결할 수 없거나 연결된 Manager Service가 실행 중이 아닙니다. 테스트가 성공하려면 Manager Service가 실행 중이어야 합니다.

- 자격 증명 오류

지정된 사용자 이름 및 암호 조합이 지정된 주소의 끝점에 대해 올바르지 않습니다.

- Timeout

허용된 2분이라는 시간 내에 테스트 작업을 완료하지 못했습니다.

연결 테스트 작업이 실패해도 끝점을 저장할 수 있지만 시스템 프로비저닝이 실패할 수 있습니다.

신뢰할 수 있는 인증서 문제(예: 인증서가 만료됨)가 있는 경우 인증서 지문을 수락하라는 메시지가 표시됩니다.

- 10 **확인**을 클릭하여 끝점을 저장합니다.

확인 작업은 **연결 테스트** 작업과 동일한 조건을 테스트합니다. 이전 조건을 찾은 경우 메시지가 반환됩니다. 저장이 가능한 경우 검토할 수 있도록 화면에 오류가 표시됩니다.

vRealize Automation이 끝점에서 데이터를 수집하고 계산 리소스를 검색합니다.

후속 작업

끝점에서 패브릭 그룹으로 계산 리소스를 추가합니다. [패브릭 그룹 생성](#) 항목을 참조하십시오.

vCloud Air 끝점 생성

OnDemand 또는 구독 서비스에 대해 vCloud Air 끝점을 생성할 수 있습니다. 선택적으로 프록시 끝점에 연결하여 프록시 설정을 vCloud Director 끝점에 연결할 수 있습니다.

vCloud Air 관리 콘솔에 대한 자세한 내용은 vCloud Air 설명서를 참조하십시오.

참고 vCloud Air 끝점 및 vCloud Director 끝점에 정의된 예약은 시스템 프로비저닝에 대해 네트 워크 프로파일의 사용을 지원하지 않습니다.

vCloud Air 끝점의 경우 조직 이름 및 vDC 이름이 vCloud Air 구독 인스턴스에 대해 동일해야 합니다.

끝점에 프록시 설정 연결에 대한 자세한 내용은 [프록시 끝점을 생성하고 클라우드 끝점에 연결](#)을 참조하십시오.

필수 조건

- **laaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- vCloud Air 구독 서비스 또는 OnDemand 계정에 대해 **가상 인프라 관리자** 권한이 있는지 확인합니다.
- 추가적인 보안을 구성하고 프록시 서버를 통과하도록 연결을 강제하려는 경우 프록시 끝점을 생성합니다. vCloud Director 끝점을 생성하면서 프록시 끝점에 연결할 수 있습니다. [프록시 끝점을 생성하고 클라우드 끝점에 연결](#) 항목을 참조하십시오.

프로시저

- 1 **인프라 > 끝점 > 끝점**을 선택합니다.
- 2 **새로 만들기 > 클라우드 > vCloud Air**를 선택합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 4 **주소** 텍스트 상자의 기본 vCloud Air 끝점 주소를 수락하거나 새로 입력합니다.

기본 vCloud Air 끝점 주소는 Default URL for vCloud Air endpoint 글로벌 속성에 지정된 것처럼 <https://vca.vmware.com>입니다.

- 5 관리자 수준 사용자 이름과 암호를 입력합니다.

자격 증명은 vCloud Air 구독 서비스 또는 OnDemand 계정 관리자의 것이어야 합니다.

사용자 이름 형식은 domain\username입니다.

VMware Remote Console을 사용하여 연결할 수 있는 권한을 가진 조직 관리자의 자격 증명을 제공합니다.

- 6 (선택 사항) **속성**을 클릭하고 제공된 사용자 지정 속성, 속성 그룹 또는 끝점에 대한 사용자 고유의 속성 정의를 추가합니다.
- 7 (선택 사항) 추가적인 보안을 구성하고 프록시 서버를 통과하도록 연결을 강제하려면 **연결**을 클릭하고 기존 프록시 끝점에 연결합니다.

연결을 생성하려면 최소 하나의 프록시 끝점이 있어야 합니다.

8 확인을 클릭합니다.

후속 작업

패브릭 그룹 생성.

vCloud Director 끝점 생성

vCloud Director 끝점을 생성하여 환경 내의 모든 vCloud Director 가상 데이터 센터(vDC)를 관리하거나 별도의 끝점을 생성하여 각 vCloud Director 조직을 관리할 수 있습니다. 선택적으로 프록시 끝점에 연결하여 프록시 설정을 vCloud Director 끝점에 연결할 수 있습니다.

조직 vDC에 대한 자세한 내용은 vCloud Director 설명서를 참조하십시오.

동일한 vCloud Director 인스턴스에 대해 단일 끝점 및 개별 조직 끝점을 생성하지 마십시오.

vRealize Automation은 프록시 에이전트를 사용하여 vSphere 리소스를 관리합니다.

참고 vCloud Air 끝점 및 vCloud Director 끝점에 정의된 예약은 시스템 프로비저닝에 대해 네트워크 프로파일의 사용을 지원하지 않습니다.

끝점에 프록시 설정 연결에 대한 자세한 내용은 [프록시 끝점을 생성하고 클라우드 끝점에 연결](#)을 참조하십시오.

필수 조건

- **IaaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 추가적인 보안을 구성하고 프록시 서버를 통과하도록 연결을 강제하려는 경우 프록시 끝점을 생성합니다. vCloud Director 끝점을 생성하면서 프록시 끝점에 연결할 수 있습니다. [프록시 끝점을 생성하고 클라우드 끝점에 연결](#)의 내용을 참조하십시오.

프로시저

- 1 **인프라 > 끝점 > 끝점**을 선택합니다.
- 2 **새로 만들기 > 클라우드 > vCloud Director**를 선택합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 4 **주소** 텍스트 상자에 vCloud Director 서버의 URL을 입력합니다.
URL은 FQDN 또는 IP_address 유형이어야 합니다.
예를 들어 https://mycompany.com을 입력합니다.
- 5 관리자 수준 사용자 이름과 암호를 입력합니다.
 - vCloud Director 서버에 연결하고 사용자가 관리 역할을 가진 조직을 지정하려면 조직 관리자 자격 증명을 사용합니다. 이러한 자격 증명을 사용하면 끝점이 연결된 조직 vDC에만 액세스할 수 있습니다. vCloud Director 인스턴스의 각 추가 조직에 대해 끝점을 추가하여 vRealize Automation과 통합할 수 있습니다.
 - vCloud Director 인스턴스의 모든 조직 vDC에 대한 액세스를 허용하려면 vCloud Director에 대한 시스템 관리자 자격 증명을 사용하고 **조직** 텍스트 상자를 비워 둡니다.

6 조직 관리자인 경우 **조직** 텍스트 상자에 vCloud Director 조직 이름을 입력할 수 있습니다.

옵션	설명
모든 조직 vCD 검색	사설 클라우드에 vCloud Director를 구현한 경우 애플리케이션이 사용할 수 있는 모든 조직 vDC를 검색하도록 조직 텍스트 상자를 비워 둘 수 있습니다.
각 조직 vCD에 대해 끝점 구분	조직 텍스트 상자에 vCloud Director 조직 이름을 입력합니다.

조직 이름이 vCloud Director 조직 이름과 일치하고, 이 이름이 가상 데이터 센터(vDC) 이름으로 나타날 수도 있습니다. Virtual Private Cloud를 사용 중인 경우 이 이름은 M123456789-12345 형식의 고유 식별자가 됩니다. 전용 클라우드에서 이것은 대상 vDC의 지정된 이름입니다.

예를 들어 [조직] 필드를 비워 둔 상태로 시스템 수준에서 vCloud Director에 직접 연결하는 경우 시스템 관리자 자격 증명이 필요합니다. 끝점에 조직을 입력하는 경우 해당 조직에서 조직 관리자 자격 증명을 가진 사용자가 필요합니다.

VMware Remote Console을 사용하여 연결할 수 있는 권한을 가진 자격 증명을 제공합니다.

- 단일 끝점을 사용하여 모든 조직을 관리하려면 시스템 관리자의 자격 증명을 제공합니다.
- 각 조직 vDC(가상 데이터 센터)를 개별 끝점을 사용하여 관리하려면 각 vDC에 대해 별도의 조직 관리자 자격 증명을 생성합니다.

동일한 vCloud Director 인스턴스에 대해 단일 시스템 수준 끝점 및 개별 조직 끝점을 생성하지 마십시오.

- 7 (선택 사항) **속성**을 클릭하고 제공된 사용자 지정 속성, 속성 그룹 또는 끝점에 대한 사용자 고유의 속성 정의를 추가합니다.
- 8 (선택 사항) 추가적인 보안을 구성하고 프록시 서버를 통과하도록 연결을 강제하려면 **연결**을 클릭하고 기존 프록시 끝점에 연결합니다.

연결을 생성하려면 최소 하나의 프록시 끝점이 있어야 합니다.

9 **확인**을 클릭합니다.

후속 작업

[패브릭 그룹 생성](#).

Amazon 끝점 생성

Amazon 인스턴스에 연결할 끝점을 생성할 수 있습니다. 필요한 경우 프록시 끝점에 연결하여 프록시 설정을 Amazon 끝점에 연결할 수 있습니다.

vRealize Automation에는 Blueprint를 생성할 때 사용할 수 있는 몇 가지 Amazon 인스턴스 유형이 제공되지만 고유한 인스턴스 유형을 가져오려는 경우에는 [Amazon 인스턴스 유형 추가](#) 항목을 참조하십시오.

끝점에 프록시 설정 연결에 대한 자세한 내용은 [프록시 끝점을 생성하고 클라우드 끝점에 연결](#)을 참조하십시오.

필수 조건

- **IaaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 추가적인 보안을 구성하고 프록시 서버를 통과하도록 연결을 강제하려는 경우 프록시 끝점을 생성합니다. Amazon 끝점을 생성할 때 프록시 끝점에 연결할 수 있습니다. [프록시 끝점을 생성하고 클라우드 끝점에 연결](#) 항목을 참조하십시오.

프로시저

- 1 **인프라 > 끝점 > 끝점**을 선택합니다.
- 2 **새로 만들기 > 클라우드 > Amazon EC2**를 선택합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
일반적으로 이 이름은 이 끝점에 해당하는 Amazon 계정을 나타냅니다.
- 4 Amazon 끝점의 관리자 수준 액세스 키 ID를 입력합니다.
하나의 끝점만 Amazon 액세스 키 ID와 연결될 수 있습니다.
Amazon 끝점을 생성하는 데 필요한 액세스 키를 얻으려면 AWS 전체 액세스 권한 관리자 정책으로 추가 구성되거나 AWS 전체 액세스 권한 관리자 자격 증명을 가진 사용자로부터 키를 요청해야 합니다. 자세한 내용은 Amazon 설명서를 참조하십시오.
- 5 Amazon 끝점의 비밀 액세스 키를 입력합니다.
- 6 (선택 사항) **속성**을 클릭하고 제공된 사용자 지정 속성, 속성 그룹 또는 끝점에 대한 사용자 고유의 속성 정의를 추가합니다.
- 7 (선택 사항) 추가적인 보안을 구성하고 프록시 서버를 통과하도록 연결을 강제하려면 **연결**을 클릭하고 기존 프록시 끝점에 연결합니다.
연결을 생성하려면 최소 하나의 프록시 끝점이 있어야 합니다.
- 8 **확인**을 클릭합니다.

끝점을 생성하면 vRealize Automation이 Amazon Web Services 영역에서 데이터를 수집하기 시작합니다.

후속 작업

끝점에서 패브릭 그룹으로 계산 리소스를 추가합니다. [패브릭 그룹 생성](#) 항목을 참조하십시오.

Amazon 인스턴스 유형 추가

Amazon Blueprint와 함께 사용하기 위해 일부 인스턴스 유형이 vRealize Automation과 함께 제공됩니다. 관리자가 인스턴스 유형을 추가 및 제거할 수 있습니다.

Blueprint 설계자가 Amazon Blueprint를 생성 또는 편집할 때 IaaS 관리자에 의해 관리되는 시스템 인스턴스 유형을 사용할 수 있습니다. Amazon 시스템 이미지 및 인스턴스 유형은 Amazon Web Services 제품을 통해 사용할 수 있습니다.

필수 조건

IaaS 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 **인프라 > 관리 > 인스턴스 유형**을 클릭합니다.

2 **새로 만들기**를 클릭합니다.

3 다음 매개 변수를 지정하여 새 인스턴스 유형을 추가합니다.

사용 가능한 Amazon 인스턴스 유형 및 해당 매개 변수에 대해 지정할 수 있는 설정 값에 대한 자세한 내용은 EC2 인스턴스 유형 - AWS(Amazon Web Services) (aws.amazon.com/ec2) 및 인스턴스 유형(docs.aws.amazon.com)의 Amazon Web Services 설명서에서 확인할 수 있습니다.

- 이름
- API 이름
- 유형 이름
- IO 성능 이름
- CPU
- 메모리(GB)
- 스토리지(GB)
- 계산 단위

4 **저장** 아이콘()을 클릭합니다.

IaaS 설계자가 Amazon Web Services Blueprint를 생성할 때 사용자 지정 인스턴스 유형을 사용할 수 있습니다.

후속 작업

끝점에서 패브릭 그룹으로 계산 리소스를 추가합니다. [패브릭 그룹 생성](#) 항목을 참조하십시오.

프록시 끝점을 생성하고 클라우드 끝점에 연결

프록시 끝점을 생성하고 해당 프록시 설정을 vCloud Air, vCloud Director 또는 Amazon 끝점에 연결할 수 있습니다.

프록시 관리자를 사용 중이던 vCloud Air, vCloud Director 또는 Amazon 끝점을 업그레이드 또는 마이그레이션한 경우 vCloud Air, vCloud Director 또는 Amazon 끝점과 새로운 프록시 끝점 간 연결이 포함된 새로운 vCloud Air, vCloud Director 또는 Amazon 끝점이 생성됩니다.

필수 조건

- **IaaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 다음의 끝점 유형 중 하나를 만듭니다.
 - [vCloud Air 끝점 생성](#)
 - [Amazon 끝점 생성](#)

■ vCloud Director 끝점 생성

프록시 끝점에서 연결을 생성하려면 vCloud Air, vCloud Director 또는 Amazon 끝점이 하나 이상 있어야 합니다.

프로시저

- 1 **인프라 > 끝점 > 끝점**을 선택합니다.
- 2 **새로 만들기 > 네트워크 및 보안 > 프록시**를 선택합니다.
- 3 **이름** 텍스트 상자에 이름을 입력합니다.
- 4 (선택 사항) **설명** 텍스트 상자에 설명을 입력합니다.
- 5 설치된 프록시 에이전트의 URL을 **주소** 텍스트 상자에 입력합니다.
- 6 **포트** 텍스트 상자에 프록시 서버 연결을 위해 사용할 포트 번호를 입력합니다.
- 7 관리자 수준 사용자 이름과 암호를 입력합니다.
- 8 (선택 사항) **속성**을 클릭하고 제공된 사용자 지정 속성, 속성 그룹 또는 끝점에 대한 사용자 고유의 속성 정의를 추가합니다.
- 9 프록시 설정을 vCloud Air, vCloud Director 또는 Amazon 끝점에 연결하려면 **연결**을 클릭하고 끝점을 하나 이상 선택합니다.

연결을 생성하려면 최소 하나의 vCloud Air, vCloud Director 또는 Amazon 끝점이 있어야 합니다.

프록시 끝점을 둘 이상의 끝점에 연결할 수 있습니다.
- 10 **확인**을 클릭합니다.

vRealize Automation이 끝점에서 데이터를 수집하고 계산 리소스를 검색합니다.

후속 작업

끝점에서 패브릭 그룹으로 계산 리소스를 추가합니다. [패브릭 그룹 생성](#) 항목을 참조하십시오.

vRealize Orchestrator 끝점 생성

vRealize Orchestrator 끝점을 생성하여 vRealize Orchestrator 서버에 연결할 수 있습니다.

서로 다른 vRealize Orchestrator 서버에 연결하도록 여러 끝점을 구성할 수 있지만 각 끝점에 대해 우선 순위를 구성해야 합니다.

vRealize Orchestrator 워크플로를 실행할 때 vRealize Automation은 우선 순위가 가장 높은 vRealize Orchestrator 끝점을 먼저 시도합니다. 이 끝점에 연결할 수 없으면 vRealize Orchestrator 서버가 워크플로를 실행할 수 있을 때까지 우선 순위가 다음으로 높은 끝점을 계속 시도합니다.

필수 조건

- **laaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **인프라 > 끝점 > 끝점**을 선택합니다.
- 2 **새로 만들기 > 오케스트레이션 > vRealize Orchestrator**를 선택합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 4 vRealize Orchestrator 서버의 정규화된 이름 또는 IP 주소와 vRealize Orchestrator 포트 번호가 포함된 URL을 입력합니다.

전송 프로토콜은 HTTPS여야 합니다. 지정된 포트가 없으면 기본 포트 443이 사용됩니다.

vRealize Automation 장치에 포함된 기본 vRealize Orchestrator 인스턴스를 사용하려면 `https://vrealize-automation-appliance-hostname:443/vco`를 입력합니다.

- 5 **사용자 이름 및 암호** 텍스트 상자에 vRealize Orchestrator 자격 증명을 입력하여 vRealize Orchestrator 끝점에 연결합니다.

사용하는 자격 증명에는 IaaS에서 호출할 모든 vRealize Orchestrator 워크플로에 대한 실행 권한이 있어야 합니다.

vRealize Automation 장치에 포함된 기본 vRealize Orchestrator 인스턴스를 사용하려는 경우 사용자 이름은 `administrator@vsphere.local`이고 암호는 SSO 구성 시 지정한 관리자 암호입니다.

- 6 **우선 순위** 텍스트 상자에 1보다 크거나 같은 정수를 입력합니다.

값이 낮을수록 우선 순위가 높습니다.

- 7 (선택 사항) **속성**을 클릭하고 제공된 사용자 지정 속성, 속성 그룹 또는 끝점에 대한 사용자 고유의 속성 정의를 추가합니다.

- 8 **확인**을 클릭합니다.

네트워킹을 위한 vRealize Orchestrator 끝점 구성

vRealize Orchestrator 워크플로를 호출하기 위해 vRealize Automation 워크플로를 사용 중인 경우 vRealize Orchestrator 인스턴스 또는 서버를 끝점으로 구성해야 합니다.

vRealize Orchestrator 끝점 추가에 대한 자세한 내용은 [vRealize Orchestrator 끝점 생성](#)을 참조하십시오.

vRealize Orchestrator 끝점을 시스템 Blueprint와 연결하여 해당 Blueprint에서 프로비저닝된 시스템에 대한 모든 vRealize Orchestrator 워크플로가 해당 끝점을 사용하여 실행되도록 할 수 있습니다.

vRealize Automation에는 포함된 vRealize Orchestrator 인스턴스가 기본적으로 포함되어 있습니다. 테스트 환경에서 vRealize Automation 워크플로를 실행하거나 개념 검증을 생성하기 위한 vRealize Orchestrator 끝점으로 이 인스턴스를 사용하는 것이 좋습니다.

운영 환경에서 vRealize Automation 워크플로를 실행할 때도 이 vRealize Orchestrator 끝점을 사용하는 것이 좋습니다.

vRealize Orchestrator 플러그인은 vRealize Orchestrator 7.1 이상에서 자동으로 설치됩니다. vRealize Orchestrator 플러그인을 별도로 설치하지 않아도 됩니다.

vRealize Operations Manager 끝점 생성

vRealize Operations Manager 끝점을 생성하여 vRealize Operations Manager 호스트 제품군 API에 연결할 수 있습니다.

vRealize Operations Manager 연결 및 인증서 신뢰 검증에 대한 자세한 내용은 [연결 테스트를 사용할 때의 고려 사항](#)을 참조하십시오.

필수 조건

- **laaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **인프라 > 끝점 > 끝점**을 선택합니다.
- 2 **새로 만들기 > 관리 > vRealize Operations Manager**를 선택합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 4 **주소** 텍스트 상자에 vRealize Operations Manager 서버의 URL을 입력합니다.
URL은 `https://hostname/suite-api` 형식이어야 합니다.
- 5 vRealize Operations Manager 사용자 이름 및 암호 자격 증명을 입력합니다.
- 6 (선택 사항) **속성**을 클릭하고 제공된 사용자 지정 속성, 속성 그룹 또는 끝점에 대한 사용자 고유의 속성 정의를 추가합니다.
- 7 (선택 사항) 자격 증명, 호스트 끝점 주소 및 인증서 신뢰를 검증하려면 **연결 테스트**를 클릭합니다. 이 작업은 끝점에서 데이터가 수집될 수 있도록 Manager Service와 에이전트가 실행 중인지도 확인합니다. **확인** 작업은 이와 동일한 조건을 테스트합니다.

연결 테스트 작업은 다음 조건에 대한 정보를 반환합니다.

■ 인증서 오류

인증서가 없거나, 인증서를 신뢰할 수 없거나, 인증서가 만료된 경우 인증서 지문을 수락하라는 메시지가 표시됩니다. 지문을 수락하지 않아도 끝점을 저장할 수 있지만 시스템 프로비저닝이 실패할 수 있습니다.

■ 에이전트 오류

연결된 vSphere 에이전트를 찾을 수 없습니다. 테스트가 성공하려면 에이전트가 실행 중이어야 합니다.

■ 호스트 오류

지정된 끝점 주소에 연결할 수 없거나 연결된 Manager Service가 실행 중이 아닙니다. 테스트가 성공하려면 Manager Service가 실행 중이어야 합니다.

■ 자격 증명 오류

지정된 사용자 이름 및 암호 조합이 지정된 주소의 끝점에 대해 올바르지 않습니다.

■ Timeout

허용된 2분이라는 시간 내에 테스트 작업을 완료하지 못했습니다.

연결 테스트 작업이 실패해도 끝점을 저장할 수 있지만 시스템 프로비저닝이 실패할 수 있습니다.

신뢰할 수 있는 인증서 문제(예: 인증서가 만료됨)가 있는 경우 인증서 지문을 수락하라는 메시지가 표시됩니다.

8 확인을 클릭합니다.

타사 IPAM 제공자 끝점 생성

vRealize Orchestrator에서 타사 IPAM 끝점 유형을 등록 및 구성한 경우 vRealize Automation에서 해당 IPAM 솔루션 제공자에 대한 끝점을 생성할 수 있습니다.

외부 IPAM 솔루션을 제공하기 위해 vRealize Orchestrator 패키지를 가져오고

vRealize Orchestrator에서 IPAM 끝점 유형을 등록한 경우, vRealize Automation 끝점을 생성할 때 해당 IPAM 끝점 유형을 선택할 수 있습니다.

참고 이 예는 VMware Solution Exchange에서 다운로드할 수 있는 Infoblox IPAM 플러그인 사용을 기준으로 합니다. VMware에서 제공하는 IPAM 솔루션 SDK를 사용하여 사용자 고유의 IPAM 제공자 패키지를 생성한 경우에도 이 절차를 사용할 수 있습니다. 사용자 고유의 타사 IPAM 솔루션 패키지를 가져오고 구성하는 절차는 사전 요구 사항에 설명된 내용과 같습니다.

vRealize Orchestrator에서 IPAM 솔루션 제공자 플러그인에 대한 끝점 유형을 등록할 때 vRealize Automation의 첫 번째 IPAM 끝점이 생성됩니다.

필수 조건

- vRealize Orchestrator에서 타사 IPAM 제공자 패키지 얻기 및 가져오기.
- vRealize Orchestrator에서 타사 IPAM 끝점 유형을 등록하도록 워크플로 실행.
- IaaS 관리자로 vRealize Automation 콘솔에 로그인합니다.

이 예에서는 타사 IPAM 제공자 플러그인 또는 패키지에 대해 vRealize Orchestrator에 등록된 끝점 유형을 사용하여 Infoblox IPAM 끝점을 생성합니다.

프로시저

1 인프라 > 끝점 > 끝점을 선택합니다.

2 새로 만들기 > IPAM > IPAM 끝점 유형을 선택합니다.

등록된 외부 IPAM 제공자 끝점 유형(예: Infoblox)을 선택합니다. 외부 IPAM 제공자 끝점은 타사 vRealize Orchestrator 패키지를 가져오고 패키지 워크플로를 실행하여 끝점 유형을 등록한 경우에만 사용할 수 있습니다.

Infoblox IPAM의 경우, 기본 IPAM 끝점 유형만 나열됩니다. 사용자 지정 속성을 사용하여 보조 IPAM 끝점 유형을 지정할 수 있습니다.

이 예에서는 등록된 외부 IPAM 끝점 유형(예: **Infoblox NIOS**)을 선택합니다.

3 이름을 입력하고 원하는 경우 설명을 입력합니다.

- 4 제공자별 URL 형식(예: https://host_name/name)을 사용하여 주소 텍스트 상자에 등록된 IPAM 끝점의 위치를 입력합니다.

예를 들어 vRealize Orchestrator에서 IPAM 끝점 유형을 등록한 경우 https://nsx62-scale-infoblox 및 https://nsx62-scale-infoblox2와 같은 몇 가지 IPAM 끝점을 생성할 수 있습니다. 기본 등록된 끝점 유형을 입력합니다. 또한 보조 IPAM 끝점을 하나 이상 지정하기 위해 사용자 지정 속성을 사용하여 IPAM 솔루션 제공자와 관련된 확장 가능한 속성을 예물레이트할 수 있습니다.

- 5 IPAM 솔루션 제공자 계정에 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

vRealize Automation에서 작업할 때 끝점을 생성, 구성 및 편집하려면 IPAM 솔루션 제공자 계정 자격 증명이 필요합니다. vRealize Automation은 IPAM 끝점 자격 증명을 사용하여 IP 주소를 할당하고 다른 작업을 수행하기 위해 지정된 끝점 유형(예: Infoblox)과 통신합니다. 이 동작은 vRealize Automation에서 vSphere 끝점 자격 증명을 사용하는 방식과 비슷합니다.

- 6 (선택 사항) 속성을 클릭하고 특정 IPAM 솔루션 제공자에 의미 있는 끝점 속성을 추가합니다.

Infoblox 및 Bluecat과 같은 각 IPAM 솔루션 제공자는 vRealize Automation 사용자 지정 속성을 사용하여 예물레이트할 수 있는 고유 확장 가능한 특성을 사용합니다. 예를 들어 Infoblox는 확장 가능한 특성을 사용하여 기본 끝점과 보조 끝점을 구별합니다.

- 7 확인을 클릭합니다.

후속 작업

끝점에서 패브릭 그룹으로 계산 리소스를 추가합니다. [패브릭 그룹 생성](#) 항목을 참조하십시오.

Microsoft Azure 끝점 생성

vRealize Automation과 Azure 배포 간에 자격 증명을 통한 연결을 원활하게 하기 위해 Microsoft Azure 끝점을 생성할 수 있습니다.

끝점은 가상 시스템 Blueprint를 생성하는 데 사용할 수 있는 리소스(이 경우 Azure 인스턴스)에 대한 연결을 설정합니다. Azure 가상 시스템 프로비저닝을 위한 Blueprint의 기준으로 사용할 Azure 끝점이 있어야 합니다. 여러 Azure 구독을 사용하는 경우 각 구독 ID에 대한 끝점이 필요합니다.

대안으로 vRealize Orchestrator 워크플로 트리의 라이브러리 > Azure > 구성 아래 있는 [Azure 연결 추가] 명령을 사용하여 vRealize Orchestrator에서 Azure 연결을 직접 생성할 수 있습니다. 대부분의 시나리오에서 여기의 설명대로 끝점 구성을 통해 연결을 생성하는 것이 기본 옵션입니다.

Azure 끝점은 vRealize Orchestrator 및 XaaS 기능에서 지원됩니다. Azure 끝점을 생성, 삭제 또는 편집할 수 있습니다. 기존 끝점을 변경하고 몇 시간 동안 업데이트된 연결을 통해 Azure 포털에서 업데이트를 실행하지 않으면 service vco-service restart 명령을 사용하여 vRealize Orchestrator 서비스를 다시 시작해야 합니다. 서비스를 다시 시작하는 데 실패하면 오류가 발생할 수 있습니다.

필수 조건

- Microsoft Azure 인스턴스를 구성하고 사용할 수 있는 구독 ID를 제공하는 유효한 Microsoft Azure 구독을 얻습니다. Azure 구성 및 구독 ID 얻기에 대한 자세한 내용은 <http://www.vaficionado.com/2016/11/using-new-microsoft-azure-endpoint-vrealize-automation-7-2/>를 참조하십시오.
- vRealize Automation 배포에는 최소한 하나의 테넌트와 하나의 비즈니스 그룹이 있어야 합니다.
- <https://azure.microsoft.com/ko-kr/documentation/articles/resource-group-create-service-principal-portal>에 설명된 대로 Active Directory 애플리케이션을 생성합니다.
- 끝점 및 Blueprint 구성 중에 필요하므로 다음과 같은 Azure 관련 정보를 기록해 둡니다.
 - 구독 ID
 - 테넌트 ID
 - 스토리지 계정 이름
 - 리소스 그룹 이름
 - 위치
 - 가상 네트워크 이름
 - 클라이언트 애플리케이션 ID
 - 클라이언트 애플리케이션 비밀 키
 - 가상 시스템 이미지 URN
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 끝점 > Orchestrator 끝점**을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 [플러그인] 탭에서 **플러그인** 드롭다운 메뉴를 클릭하고 [Azure 플러그인]을 선택합니다.
- 4 **다음**을 클릭합니다.
- 5 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 6 **다음**을 클릭합니다.
- 7 **세부 정보** 탭에 있는 텍스트 상자에 끝점에 맞는 적절한 값을 입력합니다.

매개 변수	설명
연결 설정	
Azure 연결	

매개 변수	설명
연결 이름	새 끝점 연결의 고유한 이름입니다. 이 이름은 특정 연결을 식별하는 데 도움이 되도록 vRealize Orchestrator 인터페이스에 나타납니다.
Azure 구독 ID	Azure 구독 식별자입니다. ID는 스토리지 계정, 가상 시스템 및 기타 사용자에게 액세스 권한이 있는 Azure 리소스를 정의합니다.
리소스 관리자 설정	
Azure 서비스 URI	Azure 인스턴스에 액세스할 수 있는 URI입니다. https://management.azure.com/ 의 기본값은 여러 일반 구현에 적절합니다.
테넌트 ID	끝점에서 사용할 Azure 테넌트 ID입니다.
클라이언트 ID	끝점에서 사용할 Azure 클라이언트 식별자입니다. Active Directory 애플리케이션 생성 시 할당됩니다.
클라이언트 암호	Azure 클라이언트 ID와 함께 사용되는 키입니다. Active Directory 애플리케이션 생성 시 이 키가 할당됩니다.
로그인 URL	Azure 인스턴스에 액세스하는 데 사용하는 URL입니다. https://login.windows.net/ 의 기본값은 여러 일반 구현에 적절합니다.
프록시 설정	
프록시 호스트	회사가 프록시 웹 서버를 사용하는 경우 해당 서버의 호스트 이름을 입력합니다.
프록시 포트	회사가 프록시 웹 서버를 사용하는 경우 해당 서버의 포트 번호를 입력합니다.

8 완료를 클릭합니다.

후속 작업

Azure의 적절한 리소스 그룹, 스토리지 계정 및 네트워크 보안 그룹을 생성합니다. 구현에 적절한 경우 로드 밸런서도 생성해야 합니다.

작업	옵션
Azure 리소스 그룹 생성	<ul style="list-style-type: none"> Azure 포털을 사용하여 리소스 그룹을 생성합니다. 구체적인 지침은 Azure 설명서를 참조하십시오. Library/Azure/Resource/Create 리소스 그룹에 있는 적절한 vRealize Orchestrator 워크플로를 사용합니다. vRealize Automation에서 vRealize Orchestrator 워크플로가 포함된 XaaS Blueprint를 생성하고 게시합니다. 리소스 그룹을 서비스 및 사용 권한에 연결한 후 이 리소스 그룹을 요청할 수 있습니다. 리소스 그룹 리소스 유형은 vRealize Automation에서 지원 또는 관리되지 않습니다.
Azure 스토리지 계정 생성	<ul style="list-style-type: none"> Azure를 사용하여 스토리지 계정을 생성합니다. 구체적인 지침은 Azure 설명서를 참조하십시오. Library/Azure/Storage/Create 스토리지 계정에 있는 적절한 vRealize Orchestrator 워크플로를 사용합니다. vRealize Automation에서 vRealize Orchestrator 워크플로가 포함된 XaaS Blueprint를 생성하고 게시합니다. 스토리지 계정을 서비스 및 사용 권한에 연결한 후 이 스토리지 계정을 요청할 수 있습니다.
Azure 네트워크 보안 그룹 생성	<ul style="list-style-type: none"> Azure를 사용하여 보안 그룹을 생성합니다. 구체적인 지침은 Azure 설명서를 참조하십시오. Library/Azure/Network/Create 네트워크 보안 그룹에 있는 적절한 vRealize Orchestrator 워크플로를 사용합니다. vRealize Automation에서 vRealize Orchestrator 워크플로가 포함된 XaaS Blueprint를 생성하고 게시합니다. 보안 그룹을 서비스 및 사용 권한에 연결한 후 이 보안 그룹을 요청할 수 있습니다.

Puppet 끝점 생성

Puppet 끝점을 생성하여 vSphere 가상 시스템에 Puppet 구성 관리 구성 요소를 추가할 수 있습니다. 이러한 구성 요소를 사용하면 Puppet Master를 사용하여 가상 시스템에 구성 관리를 적용할 수 있습니다.

끝점은 외부 리소스(이 경우 Puppet Master 인스턴스)에 대한 연결을 설정합니다. 끝점을 통해 vSphere 가상 시스템 Blueprint에 Puppet 구성 관리 구성 요소를 배치할 수 있습니다. 이러한 Blueprint에 기반한 프로비저닝된 가상 시스템은 연결된 Puppet Master에 의한 제어를 용이하게 하는 Puppet 에이전트를 포함합니다.

필수 조건

- 환경에 적합하게 Puppet Enterprise를 설치 및 구성합니다.
- vRealize Orchestrator 배포에 Puppet 플러그인 버전 3.0을 다운로드하고 설치합니다. 플러그인은 <https://solutionexchange.vmware.com/store/products/puppet-plugin-for-vrealize-automation>에서 다운로드할 수 있습니다. 플러그인 설치 및 사용에 대한 내용은 https://docs.puppet.com/pe/latest/vro_intro.html 항목을 참조하십시오.

프로시저

- 1 **관리 > 끝점 > Orchestrator** 끝점을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 [플러그인] 탭에서 **플러그인** 드롭다운 메뉴를 클릭하고 **Puppet 플러그인**을 선택합니다.
- 4 **다음**을 클릭합니다.
- 5 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 6 **다음**을 클릭합니다.
- 7 **세부 정보** 탭에 있는 텍스트 상자에 끝점에 맞는 적절한 값을 입력합니다.

매개 변수	설명
이 Puppet Master의 표시 이름	끝점 연결과 연결된 Puppet Master의 이름입니다. 이 이름은 특정 연결을 식별하는 데 도움이 되도록 vRealize Orchestrator 인터페이스에 나타납니다.
호스트 이름 또는 IP 주소	이 끝점에 사용되는 Puppet Master의 FQDN 또는 IP 주소입니다.
SSH 포트	이 Puppet Master의 보안 통신에 사용하도록 정의된 포트입니다.
SSH RBAC 및 사용자 이름	Puppet Master와의 연결에 필요한 역할 기반 액세스 제어 사용자 이름입니다.
SSH 및 RBAC 암호	Puppet Master와의 보안 구성에 필요한 역할 기반 액세스 제어 사용자 이름입니다.
이 마스터의 셸 명령에 sudo를 사용하시겠습니까?	관리자가 이 끝점을 기반으로 하는 가상 시스템의 보안 옵션에 대해 Linux 서버에서 Sudo 명령을 사용할 수 있도록 하려면 이 옵션을 선택합니다.

- 8 **확인**을 클릭합니다.

이제 Puppet 에이전트가 포함된 vSphere 가상 시스템을 배포할 수 있도록 vSphere Blueprint에 Puppet 구성 관리 구성 요소를 추가할 수 있습니다.

Hyper-V(SCVMM) 끝점 생성

끝점을 생성하여 vRealize Automation이 SCVMM 환경과 통신하고, 계산 리소스를 검색하고, 데이터를 수집하고, 시스템을 프로비저닝하도록 허용할 수 있습니다.

필수 조건

- **IaaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- Hyper-V(SCVMM) 끝점을 관리하려면 DEM 에이전트를 설치하고 구성해야 합니다. 자세한 정보는 vRealize Automation 7.3 설치에서 SCVMM 요구 사항 정보를 참조하십시오.

관련 정보는 [SCVMM 환경 준비](#) 항목을 참조하십시오.

프로시저

- 1 **인프라 > 끝점 > 끝점**을 선택합니다.

2 새로 만들기 > 가상 > Hyper-V(SCVMM)를 선택합니다.

3 이름 텍스트 상자에 이름을 입력합니다.

4 (선택 사항) 설명 텍스트 상자에 설명을 입력합니다.

5 주소 텍스트 상자에 끝점의 URL을 입력합니다.

URL은 *FQDN* 또는 *IP_address* 유형이어야 합니다.

예를 들어 `mycompany-scvmm1.mycompany.local`을 입력합니다.

6 이 끝점에 대해 저장한 관리자 수준 사용자 이름과 암호를 입력합니다.

자격 증명을 이미 저장하지 않은 경우 지금 저장할 수 있습니다.

7 (선택 사항) 속성을 클릭하고 제공된 사용자 지정 속성, 속성 그룹 또는 끝점에 대한 사용자 고유의 속성 정의를 추가합니다.

8 확인을 클릭합니다.

vRealize Automation이 끝점에서 데이터를 수집하고 계산 리소스를 검색합니다.

후속 작업

끝점에서 패브릭 그룹으로 계산 리소스를 추가합니다. [패브릭 그룹 생성](#) 항목을 참조하십시오.

OpenStack 끝점 생성

vRealize Automation에서 OpenStack 인스턴스와 통신할 수 있도록 끝점을 생성합니다.

필수 조건

- **IaaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- vRealize Automation DEM이 OpenStack 또는 PowerVC 요구 사항을 충족하는 시스템에 설치되어 있는지 확인합니다. vRealize Automation 7.3 설치의 내용을 참조하십시오.
- 원하는 OpenStack이 현재 지원되는지 확인합니다. vRealize Automation 지원 매트릭스의 내용을 참조하십시오.

이전 버전의 vRealize Automation 설치에서 업그레이드 또는 마이그레이션한 후 OpenStack 끝점에 대한 데이터 수집이 실패하면 각 Keystone V3 OpenStack 끝점에

`VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` 사용자 지정 속성을 추가하여 유효한 도메인 이름을 지정하고 데이터 수집을 사용하도록 설정할 수 있습니다.

프로시저

1 인프라 > 끝점 > 끝점을 선택합니다.

2 새로 만들기 > 클라우드 > OpenStack을 선택합니다.

3 이름을 입력하고 원하는 경우 설명을 입력합니다.

4 주소 텍스트 상자에 끝점의 URL을 입력합니다.

옵션	설명
PowerVC	URL은 <code>http://myPowerVC.com:5000</code> 또는 <code>http://FQDN:5000</code> 형식이어야 합니다.
Openstack	URL은 <code>FQDN:5000</code> 또는 <code>IP_address:5000</code> 형식이어야 합니다. 끝점 주소에 <code>/v2.0</code> 접미사를 포함하지 마십시오.

5 관리자 수준 사용자 이름과 암호를 입력합니다.

제공하는 자격 증명에는 끝점과 연결된 OpenStack 테넌트의 관리자 역할이 있어야 합니다.

6 OpenStack 프로젝트 텍스트 상자에 OpenStack 테넌트 이름을 입력합니다.

서로 다른 OpenStack 테넌트를 가진 여러 끝점을 설정한 경우 각 테넌트에 대한 예약 정책을 생성합니다. 이렇게 하면 시스템이 적절한 테넌트 리소스에 프로비저닝됩니다.

7 속성을 클릭하고 제공된 사용자 지정 속성, 속성 그룹 또는 끝점에 대한 사용자 고유의 속성 정의를 추가합니다.

Keystone V3이 적용되는 경우 특정 도메인을 지정하려면

`VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` 사용자 지정 속성을 추가합니다.

8 확인을 클릭합니다.

vRealize Automation이 끝점에서 데이터를 수집하고 계산 리소스를 검색합니다.

후속 작업

끝점에서 패브릭 그룹으로 계산 리소스를 추가합니다. [패브릭 그룹 생성](#) 항목을 참조하십시오.

Hyper-V, XenServer 또는 Xen 풀 끝점 생성

vRealize Automation에서 Hyper-V, XenServer 또는 Xen 풀 마스터 환경과 통신하고, 계산 리소스 검색, 데이터 수집 및 시스템 프로비저닝 작업을 수행할 수 있도록 끝점을 생성할 수 있습니다.

필수 조건

- **IaaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 시스템 관리자가 끝점과 일치하는 저장된 자격 증명으로 프록시 에이전트를 설치해야 합니다. vRealize Automation 7.3 설치의 내용을 참조하십시오.

프로시저

1 인프라 > 끝점 > 에이전트를 선택합니다.

- 계산 리소스** 텍스트 상자에 Hyper-V 서버, Xen 서버 또는 Xen 풀 마스터의 정규화된 DNS 이름을 입력합니다.

참고 Xen 풀 끝점의 경우에는 풀 마스터의 이름을 입력해야 합니다.

vRealize Automation 계산 리소스 테이블에서 중복 항목을 피하려면 구성된 Xen 풀 마스터 주소와 일치하는 주소를 지정합니다. 예를 들어 Xen 풀 마스터 주소에서 호스트 이름을 사용하는 경우 FQDN이 아닌 호스트 이름을 입력합니다. Xen 풀 마스터 주소에서 FQDN을 사용한다면 FQDN을 입력합니다.

- 프록시 에이전트 이름** 드롭다운 메뉴에서 시스템 관리자가 이 끝점에 대해 설치한 프록시 에이전트를 선택합니다.
- (선택 사항) **설명** 텍스트 상자에 설명을 입력합니다.
- 확인**을 클릭합니다.

vRealize Automation이 끝점에서 데이터를 수집하고 계산 리소스를 검색합니다.

후속 작업

끝점에서 패브릭 그룹으로 계산 리소스를 추가합니다. [패브릭 그룹 생성](#) 항목을 참조하십시오.

연결 테스트를 사용할 때의 고려 사항

연결 테스트 작업을 사용하여 vSphere, NSX 또는 vRealize Operations Manager 끝점의 자격 증명, 호스트 끝점 주소 및 인증서를 검증할 수 있습니다.

이 작업은 끝점에서 데이터가 수집될 수 있도록 Manager Service와 에이전트가 실행 중인지도 확인합니다.

연결 테스트 작업은 다음 조건에 대한 정보를 반환합니다.

- **인증서 오류**

인증서가 없거나, 인증서를 신뢰할 수 없거나, 인증서가 만료된 경우 인증서 지문을 수락하라는 메시지가 표시됩니다. 지문을 수락하지 않아도 끝점을 저장할 수 있지만 시스템 프로비저닝이 실패할 수 있습니다.

- **에이전트 오류**

연결된 vSphere 에이전트를 찾을 수 없습니다. 테스트가 성공하려면 에이전트가 실행 중이어야 합니다.

- **호스트 오류**

지정된 끝점 주소에 연결할 수 없거나 연결된 Manager Service가 실행 중이 아닙니다. 테스트가 성공하려면 Manager Service가 실행 중이어야 합니다.

- **자격 증명 오류**

지정된 사용자 이름 및 암호 조합이 지정된 주소의 끝점에 대해 올바르지 않습니다.

- **Timeout**

허용된 2분이라는 시간 내에 테스트 작업을 완료하지 못했습니다.

업그레이드 또는 마이그레이션된 끝점에서 **연결 테스트**를 실행할 때 오류가 수신되면 **업그레이드 또는 마이그레이션된 끝점 사용 시 고려 사항**에서 인증서 신뢰를 설정하는 데 필요한 단계를 참조하십시오.

프로그래밍 방식으로 끝점 가져오기 또는 내보내기

vRealize Automation 7.3 이상에서 끝점을 프로그래밍 방식으로 가져오고 내보내려면 새로운 vRealize Automation 끝점-구성-서비스 REST API를 사용하거나 vRealize CloudClient를 사용해야 합니다.

vRealize CloudClient 설명서에는 해당하는 모든 명령줄 형식, 샘플 및 사용 정보가 포함되어 있습니다.

<https://developercenter.vmware.com/tool/cloudclient>의 vRealize CloudClient 제품 페이지에서 vRealize CloudClient 애플리케이션 및 설명서를 다운로드할 수 있습니다.

끝점 소스 보기 및 데이터 수집 실행

특정 끝점에 연결된 계산 리소스와 시스템을 볼 수 있습니다. 데이터 수집을 수동으로 시작할 수도 있습니다.

필수 조건

- **IaaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 끝점이 하나 이상 있는지 확인합니다.

프로시저

1 **인프라 > 끝점 > 끝점**을 선택합니다.

2 기존 끝점 행을 선택하고 **작업**을 클릭합니다.

다음의 사용 가능한 작업 중 하나를 선택합니다.

- **계산 리소스 보기**를 클릭하여 **인프라 > 계산 리소스** 페이지를 엽니다. 이 페이지에서는 계산 리소스 설정을 보고 편집할 수 있습니다.
- **시스템 보기**를 클릭하여 **인프라 > 관리되는 시스템** 페이지를 엽니다.
- **데이터 수집**을 클릭하여 [데이터 수집] 페이지를 열고 끝점에 대한 데이터 수집을 시작합니다. 페이지를 새로 고치면 요청의 현재 상태를 표시할 수 있습니다.

업그레이드 또는 마이그레이션된 끝점 사용 시 고려 사항

업그레이드하거나 vRealize Automation 7.3 이전 릴리스에서 마이그레이션한 후 다음과 같은 고려 사항을 이해하고 이에 대한 작업을 수행하는 것이 중요합니다.

이 정보는 이 vRealize Automation 릴리스로 업그레이드 또는 마이그레이션된 끝점에 적용됩니다.

- vRealize Automation 7.3 이전 릴리스에서 업그레이드 또는 마이그레이션하는 경우, 프록시 설정이 포함된 각 vCloud Air, vCloud Director 및 Amazon 끝점은 해당 프록시 설정이 포함된 새로운 프록시 끝점에 연결됩니다.

업그레이드 또는 마이그레이션 후 새로운 프록시 끝점 이름은 Proxy_YYYYYY이며, 여기서 YYYYYY는 프록시 URL, 포트 및 자격 증명의 해시입니다. 서로 다른 끝점(예: vCloud Air 또는 Amazon 끝점)에 동일한 프록시 설정(예: 동일한 URL, 포트 및 자격 증명)을 사용한 경우 업그레이드 또는 마이그레이션 이후에 프록시 끝점이 하나만 있고 vCloud Air 및 Amazon 끝점과 새로운 프록시 끝점 간 연결이 있습니다. 프록시 끝점은 둘 이상의 Amazon, vCloud Air 또는 vCloud Director 끝점에 연결할 수 있습니다.

- NSX 관리자 설정이 포함된 vSphere 끝점을 업그레이드 또는 마이그레이션하면 업그레이드된 각 vSphere 끝점은 해당 NSX 관리자 설정이 포함된 새로운 NSX 끝점에 연결됩니다.

업그레이드 또는 마이그레이션 후 NSX 끝점 이름은 NSX_XXXXXX이며, 여기서 XXXXXX는 vRealize Automation 7.3 이전 릴리스에서의 상위 vSphere 끝점 이름입니다.

- vRealize Automation 업그레이드 또는 마이그레이션이 완료되면 인프라 관리자가 새로운 NSX 및 프록시 끝점 이름을 변경할 수 있습니다.
- 업그레이드 또는 마이그레이션된 끝점의 기본 보안 설정은 신뢰할 수 없는 인증서를 허용하지 않는 것입니다.
- 신뢰할 수 없는 인증서를 사용하고 있는 경우에는 이전 버전의 vRealize Automation 설치에서 업그레이드 또는 마이그레이션한 후 인증서 검증을 사용하도록 모든 vSphere 및 NSX 끝점에 대해 다음 단계를 수행해야 합니다. 그렇지 않으면 인증서 오류가 발생하고 끝점 작업이 실패합니다. 자세한 내용은 <http://kb.vmware.com/kb/2150230>의 VMware 기술 자료 문서 vRA 7.3으로 업그레이드 후 끝점 통신이 끊김(2150230) 및 <http://kb.vmware.com/kb/2108294>의 웹 브라우저 인증서 주의를 방지하도록 vCenter Server 루트 인증서를 다운로드 및 설치하는 방법(2108294)을 참조하십시오.
 - a 업그레이드 또는 마이그레이션 후에 vRealize Automation vSphere 에이전트 시스템에 로그인하고 **서비스** 탭을 사용하여 vSphere 에이전트를 다시 시작합니다.
마이그레이션이 모든 에이전트를 다시 시작하지 못할 수 있으므로 필요한 경우 에이전트를 수동으로 다시 시작합니다.
 - b 적어도 하나 이상의 ping 보고가 완료될 때까지 기다립니다. ping 보고가 완료되려면 1~2분 정도가 소요됩니다.
 - c vSphere 에이전트가 데이터 수집을 시작하면 vRealize Automation에 IaaS 관리자로 로그인합니다.
 - d **인프라 > 끝점 > 끝점**을 클릭합니다.
 - e vSphere 끝점을 편집하고 **연결 테스트**를 클릭합니다.
 - f 인증서 프롬프트가 표시되면 **확인**을 클릭하여 인증서를 수락합니다.
인증서 프롬프트가 표시되지 않으면 현재 끝점에 대한 Windows 시스템 호스팅 서비스의 신뢰할 수 있는 루트 인증 기관(예: 프록시 에이전트 시스템 또는 DEM 시스템)에 인증서가 올바르게 저장되어 있을 수 있습니다.
 - g **확인**을 클릭하여 인증서 수락을 적용하고 끝점을 저장합니다.
 - h 각 vSphere 끝점에 대해 이 절차를 반복합니다.

i 각 NSX 끝점에 대해 이 절차를 반복합니다.

연결 테스트 작업이 성공해도 일부 데이터 수집 또는 프로비저닝 작업이 실패하면 끝점 역할을 하는 모든 에이전트 시스템과 모든 DEM 시스템에 동일한 인증서를 설치할 수 있습니다. 또는 기존 시스템에서 인증서를 제거하고 실패한 끝점에 대해 이전 절차를 반복할 수 있습니다.

- vRealize Automation 7.2 및 이전 버전에서 프로그래밍 방식으로 끝점을 생성, 편집 및 삭제하는 데 사용했던 vRealize Automation REST API가 vRealize Automation 7.3 이상에서는 더 이상 지원되지 않습니다. vRealize Automation 7.3 이상에서 프로그래밍 방식으로 끝점을 생성, 편집 및 삭제하려면 새로운 vRealize Automation 끝점-구성-서비스 REST API 또는 vRealize CloudClient를 사용해야 합니다.
- 이전 버전의 vRealize Automation 설치에서 업그레이드 또는 마이그레이션한 후 OpenStack 끝점에 대한 데이터 수집이 실패하면 각 Keystone V3 OpenStack 끝점에 `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` 사용자 지정 속성을 추가하여 유효한 도메인 이름을 지정하고 데이터 수집을 사용하도록 설정할 수 있습니다.
- 타사 IPAM 끝점(예: Infoblox IPAM)을 업그레이드하면 RegisterIPAMEndpoint 워크플로가 포함된 vRealize Orchestrator 패키지가 업그레이드됩니다. vRealize Automation 업그레이드가 완료되면 vRealize Orchestrator에서 워크플로를 다시 실행해야 할 수 있습니다.
- 여러 끝점의 자격 증명을 변경하려는 경우, 끝점을 개별적으로 편집하거나 vRealize CloudClient를 사용하여 대량 업데이트를 수행할 수 있습니다.
- vCloud Air 및 vCloud Director와 같은 일부 끝점 유형은 vRealize Automation 6.2.x에서 vRealize Automation 7.3 이상으로 직접 업그레이드 또는 마이그레이션할 수 없습니다.
- vRealize Automation 7.3으로 성공적으로 업그레이드 또는 마이그레이션한 후 **인프라 > 끝점** 페이지가 끝점을 표시하지 않거나 일부 끝점 유형 및 끝점만 표시하는 경우 [기술 자료 문서 2150252](#)에서 제안되는 해결 방법을 참조하십시오.

끝점 삭제 시 고려 사항

특정 조건에서 특정 끝점 유형을 삭제할 수 있습니다.

- 데이터가 수집되지 않은 끝점은 삭제할 수 있습니다.
- OpenStack, Amazon 및 VRO 끝점은 데이터는 수집되었지만 예약이 없는 경우 삭제할 수 있습니다. 기타 끝점 유형은 데이터가 수집된 경우 삭제할 수 없습니다.
- 타사 IPAM 끝점은 네트워크 프로파일에 대한 연결이 없는 경우 삭제할 수 있습니다.
- vSphere 끝점을 삭제할 때 확인 프롬프트에 다음과 같은 종속성이 나열됩니다.
 - 끝점에서 데이터가 수집되었습니다.
 - 끝점이 계산 리소스에 매핑되는 예약에서 참조되었습니다. 예약에서 참조되는 끝점은 삭제할 수 없습니다. 예약에 계산 리소스가 필요합니다.
 - 끝점에 기존 Blueprint에서 참조되는 템플릿이 포함되어 있습니다.
끝점을 삭제할 때 Blueprint는 삭제되지 않습니다.
- 사용 중인 가상 시스템에서 끝점을 사용합니다.

- vRealize Automation 7.3에서 소개된 새로운 CREATE, EDIT 및 DELETE vRealize Automation 끝점-구성-서비스 REST API를 사용하거나 vRealize CloudClient를 사용하여 끝점을 프로그래밍 방식으로 삭제할 수 있습니다. vRealize Automation 7.3 이전의 끝점-구성-서비스 REST API를 사용하여 끝점을 삭제할 수 없습니다.

연결된 vSphere 끝점 찾을 수 없음 문제 해결

vSphere 끝점에 대한 데이터 수집이 실패하는 경우는 프록시 이름과 끝점 이름이 일치하지 않기 때문일 수 있습니다.

문제점

vSphere 끝점에 대해 데이터 수집이 실패합니다. 로그 메시지에 다음과 비슷한 오류가 반환됩니다.

```
This exception was caught: The attached endpoint 'vCenter' cannot be found.
```

원인

vRealize Automation에서 구성하는 끝점 이름은 설치 중 vSphere 프록시 에이전트에 제공된 끝점 이름과 반드시 일치해야 합니다. 끝점 이름과 프록시 에이전트 이름이 일치하지 않으면 vSphere 끝점에 대한 데이터 수집이 실패합니다. 이름이 일치하는 끝점이 구성되기 전까지는 로그 메시지에 다음과 비슷한 오류가 반환됩니다.

```
This exception was caught: The attached endpoint 'expected endpoint name' cannot be found.
```

해결 방법

- 1 인프라 > 모니터링 > 로그를 선택합니다.
- 2 연결된 끝점을 찾을 수 없음 오류 메시지를 찾습니다.

예를 들면 다음과 같습니다.

```
This exception was caught: The attached endpoint 'expected endpoint name' cannot be found.
```

- 3 로그 메시지에 표시된 끝점 이름과 일치하도록 vSphere 끝점을 편집합니다.
 - a 인프라 > 끝점 > 끝점을 선택합니다.
 - b 편집할 끝점의 이름을 클릭합니다.
 - c 이름 텍스트 상자에 필요한 끝점 이름을 입력합니다.
 - d 확인을 클릭합니다.

이제 프록시 에이전트가 끝점과 통신할 수 있으며 데이터 수집이 성공적으로 이뤄집니다.

패브릭 그룹 생성

인프라 리소스를 패브릭 그룹으로 구성하고, 패브릭 그룹의 리소스를 관리할 패브릭 관리자를 한 명 이상 할당합니다.

패브릭 그룹은 가상 끝점과 클라우드 끝점에 필요합니다. 여러 사용자를 한 번에 한 명씩 추가하거나 ID 저장소 그룹 또는 사용자 지정 그룹을 패브릭 관리자로 선택하는 방법으로 패브릭 관리자 역할을 여러 사용자에게 부여할 수 있습니다.

필수 조건

- **IaaS 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 끝점을 하나 이상 생성합니다. [끝점 선택 시나리오](#) 항목을 참조하십시오.

프로시저

- 1 **인프라 > 패브릭 그룹**을 선택합니다.
- 2 **새 패브릭 그룹**을 클릭합니다.
- 3 **이름** 텍스트 상자에 이름을 입력합니다.
- 4 (선택 사항) **설명** 텍스트 상자에 설명을 입력합니다.
- 5 **패브릭 관리자** 텍스트 상자에 사용자 이름 또는 그룹 이름을 입력하고 Enter 키를 누릅니다.
이 단계를 반복하여 여러 명의 사용자 또는 그룹을 역할에 추가합니다.
- 6 패브릭 그룹에 추가할 **계산 리소스**를 하나 이상 클릭합니다.

패브릭 그룹을 위해 선택한 클러스터에 있는 리소스만 데이터 수집 시 검색됩니다. 예를 들어 선택한 클러스터에 있는 템플릿만 검색되고 비즈니스 그룹에 대해 생성하는 예약에 복제하는 데 사용될 수 있습니다.

- 7 **확인**을 클릭합니다.

이제 패브릭 관리자가 시스템 접두사를 구성할 수 있습니다. [시스템 접두사 구성](#) 항목을 참조하십시오.

현재 vRealize Automation 콘솔에 로그인한 사용자는 로그아웃했다가 vRealize Automation 콘솔에 다시 로그인해야 자신에게 액세스 권한이 부여된 페이지로 이동할 수 있습니다.

시스템 접두사 구성

vRealize Automation을 통해 프로비저닝된 시스템의 이름을 생성할 때 사용되는 시스템 접두사를 생성할 수 있습니다. 시스템 접두사는 Blueprint 설계 캔버스에 시스템 구성 요소를 정의할 때 필요합니다.

접두사는 기본 이름이고, 이름 뒤에는 지정한 자릿수의 카운터가 붙습니다. 모든 자릿수가 사용되면 vRealize Automation은 첫 번째 숫자로 롤백합니다.

시스템 접두사는 다음과 같은 제한을 따라야 합니다.


- 대/소문자를 구분하지 않는 ASCII 문자(a-z), 0-9 사이의 숫자 및 하이픈(-)만 포함합니다.
- 하이픈으로 시작하지 않습니다.
- 다른 기호, 문장 부호 또는 공백을 사용할 수 없습니다.

- 호스트 이름이 15자로 제한되는 Windows 기준을 따르도록 15자 이하(숫자 포함)여야 합니다. 이보다 긴 호스트 이름은 시스템이 프로비저닝될 때 잘리며, 다음에 데이터 수집을 실행할 때 업데이트됩니다. 그러나 WIM 프로비저닝의 경우 이름이 잘리지 않고, 지정한 이름이 15자보다 길면 프로비저닝이 실패합니다.
- vRealize Automation에서는 단일 인스턴스에서 같은 이름을 가진 여러 개의 가상 시스템을 지원하지 않습니다. 선택한 명명 규칙으로 인해 시스템 이름이 중복될 경우 vRealize Automation은 중복되는 이름을 가진 시스템을 프로비저닝하지 않습니다. 가능한 경우 vRealize Automation은 이미 사용 중인 이름을 건너뛰고, 지정된 시스템 접두사를 사용하여 새 시스템 이름을 생성합니다. 고유한 이름을 생성할 수 없으면 프로비저닝이 실패합니다.

필수 조건

패브릭 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 인프라 > 관리 > 시스템 접두사를 클릭합니다.
- 2 새로 만들기를 클릭합니다.
- 3 이름 텍스트 상자에 시스템 접두사를 입력합니다.
- 4 자릿수 텍스트 상자에 카운터 자릿수를 입력합니다.
- 5 다음 번호 텍스트 상자에 카운터 시작 번호를 입력합니다.
- 6 저장 아이콘()을 클릭합니다.

테넌트 관리자는 사용자가 vRealize Automation에 액세스하여 시스템을 요청할 수 있도록 비즈니스 그룹을 생성할 수 있습니다.

네트워크 프로파일 생성

네트워크 프로파일에는 게이트웨이, 서브넷 및 주소 범위와 같은 IP 정보가 들어 있습니다.

vRealize Automation은 vSphere DHCP 또는 지정된 IPAM 제공자를 사용하여 프로비저닝하는 시스템에 IP 주소를 할당합니다.

사용 가능한 네트워크 유형을 정의하는 네트워크 프로파일을 생성할 수 있습니다. 여기에는 요청 시 NAT(네트워크 주소 변환)를 위한 외부 네트워크 프로파일 및 템플릿, 새로운 네트워크 경로에 대한 적절한 라우팅 설정과 NSX 논리적 스위치를 빌드하는 라우팅된 네트워크 프로파일이 포함됩니다. 네트워크 구성 요소를 Blueprint에 추가하는 경우 네트워크 프로파일이 필요합니다.

네트워크 프로파일은 시스템이 프로비저닝될 때 네트워크 설정을 구성하는 데 사용됩니다. 또한 네트워크 프로파일은 시스템을 프로비저닝할 때 생성된 NSX Edge 디바이스의 구성도 지정합니다. 예약 및 Blueprint를 생성할 때 네트워크 프로파일을 식별합니다. 예약에서 네트워크 프로파일을 네트워크 경로에 할당하고 그러한 경로 중 하나를 Blueprint의 시스템 구성 요소에 대해 지정할 수 있습니다.

Blueprint에서 네트워크 구성 요소를 정의할 때 Blueprint 생성자가 적절한 네트워크 프로파일을 지정합니다. 시스템을 프로비저닝하기 위해 네트워크 어댑터와 로드 밸런서를 정의하는 경우 기존 네트워크 프로파일 및 요청 시 NAT 또는 라우팅된 네트워크 프로파일을 사용할 수 있습니다.

네트워크 프로파일은 Infoblox와 같은 타사 IPAM(IP 주소 관리) 제공자도 지원합니다. IPAM에 대한 네트워크 프로파일을 구성하면 프로비저닝된 시스템에서 IP 주소 데이터 및 DNS, 게이트웨이와 같은 관련 정보를 구성된 IPAM 솔루션에서 가져올 수 있습니다. Infoblox와 같은 타사 제공자에 대해 외부 IPAM 패키지를 사용하여 네트워크 프로파일에 사용할 IPAM 끝점을 정의할 수 있습니다.

참고 타사 IPAM 제공자를 사용 중이며 시스템을 배포할 네트워크를 지정하려는 경우 각 VLAN에 대해 별도의 네트워크 프로파일을 사용하여 [기술 자료 문서 2148656](#)에 설명된 알려진 문제를 방지합니다.

타사 IPAM 제공자를 사용하는 대신 vRealize Automation 제공된 IPAM 끝점을 사용하는 경우 네트워크 프로파일에서 사용할 수 있는 IP 주소 범위를 지정할 수 있습니다. 시스템에 할당되는 지정된 범위의 각 IP 주소는 시스템이 제거되면 재할당을 위해 회수됩니다. 네트워크 프로파일을 생성하여 시스템에 할당할 수 있는 정적 IP 주소의 범위를 정의할 수 있습니다. 복제를 통해 또는 kickstart/autoYaST 프로비저닝을 사용하여 가상 시스템을 프로비저닝하는 경우, 요청하는 시스템 소유자는 미리 결정된 범위의 정적 IP 주소를 할당할 수 있습니다.

예약의 특정 네트워크 경로에 네트워크 프로파일을 할당할 수 있습니다. vSphere와 같은 일부 시스템 구성 요소 유형의 경우, Blueprint를 생성하거나 편집할 때 네트워크 프로파일을 할당할 수 있습니다.

참고 배포된 가상 시스템의 네트워크 프로파일은 변경할 수 없지만 해당 VM이 연결되어 있는 네트워크는 변경할 수 있습니다. 네트워크가 다른 네트워크 프로파일에 연결되어 있으면 vRealize Automation은 해당 네트워크 프로파일의 IP 주소를 VM에 할당합니다. 하지만 게스트 운영 체제에서 IP 주소를 업데이트하기 전까지 VM은 이전 IP 주소를 계속 사용합니다. 배포된 VM에서 [재구성] 작업을 사용할 수도 있지만, 이 경우에도 게스트 운영 체제에서 IP 주소를 업데이트해야 합니다.

예약과 Blueprint에 네트워크 프로파일을 지정하는 경우, Blueprint 값이 우선합니다. 예를 들어, VirtualMachine.NetworkN.ProfileName 사용자 지정 속성을 사용하여 Blueprint에 또는 Blueprint에 사용되는 예약에 네트워크 프로파일을 지정하면 Blueprint에 지정된 네트워크 프로파일이 우선합니다. 하지만 Blueprint에서 사용자 지정 속성이 사용되지 않고 사용자가 시스템 NIC를 위한 네트워크 프로파일을 선택하는 경우, vRealize Automation에서는 네트워크 프로파일이 지정되는 시스템 NIC에 대한 예약 네트워크 경로를 사용합니다.

이러한 네트워크 유형에 대한 자세한 내용은 NSX 정보 센터 (https://www.vmware.com/support/pubs/nsx_pubs.html)에서 NSX 관리 가이드를 참조하십시오.

표 2-14. vRealize Automation 네트워크 프로파일에 사용 가능한 네트워크 유형

네트워크 유형	설명
외부	<p>vSphere 서버에 구성된 기존 네트워크입니다. NAT 및 라우팅된 네트워크 유형의 외부적인 부분입니다. 외부 네트워크 프로파일은 외부 네트워크에서 사용할 수 있는 정적 IP 주소의 범위를 정의할 수 있습니다. 제공된 VMware IPAM 끝점 또는 Infoblox IPAM과 같은 vRealize Orchestrator에서 등록하고 구성한 타사 IPAM 서비스 제공자 끝점에서 가져온 IP 범위를 사용할 수 있습니다. IP 범위는 할당 중에 IP 블록에서 생성됩니다.</p> <p>정적 IP 범위를 갖는 외부 네트워크 프로파일은 NAT 및 라우팅된 네트워크를 위한 사전 요구 사항입니다. 기존 네트워크를 위한 외부 네트워크 프로파일 생성 항목을 참조하십시오.</p>
NAT	<p>프로비저닝 중 생성된 요청 시 네트워크입니다. 외부 통신에 한 IP 주소 집합을 사용하고 내부 통신에 다른 IP 주소 집합을 사용하는 NAT 네트워크입니다.</p> <p>일대일 NAT 네트워크에서, 모든 가상 시스템에는 외부 네트워크 프로파일의 외부 IP 주소와 NAT 네트워크 프로파일의 내부 IP 주소가 할당됩니다. 일대다 NAT 네트워크에서, 모든 시스템은 외부 통신을 위해 외부 네트워크 프로파일의 단일 IP 주소를 공유합니다.</p> <p>제공된 VMware IPAM 끝점 또는 Infoblox IPAM과 같은 vRealize Orchestrator에서 등록하고 구성한 타사 IPAM 서비스 제공자 끝점에서 가져온 IP 범위를 사용할 수 있습니다. IP 범위는 할당 중에 IP 블록에서 생성됩니다.</p> <p>NAT 네트워크 프로파일은 상호 통신을 위해 변환 테이블을 사용하는 로컬 및 외부 네트워크를 정의합니다.</p> <p>요청 시 네트워크를 위한 NAT 네트워크 프로파일 생성 항목을 참조하십시오.</p>
라우팅됨	<p>프로비저닝 중 생성된 요청 시 네트워크입니다. 라우팅된 네트워크에는 DLR(논리적 분산 라우터)을 사용하여 서로 연결된 서브넷에 걸쳐 나누어진 라우팅 가능 IP 공간이 포함됩니다.</p> <p>새로운 모든 라우팅된 네트워크에는 사용 가능한 다음 서브넷이 할당되어 있으며 동일한 네트워크 프로파일을 사용하는 다른 라우팅된 네트워크와 연결되어 있습니다. 동일한 라우팅된 네트워크 프로파일을 가진 라우팅된 네트워크로 프로비저닝된 가상 시스템은 서로 통신할 수 있으며 외부 네트워크와도 통신할 수 있습니다.</p> <p>제공된 VMware IPAM 끝점 또는 Infoblox IPAM과 같은 vRealize Orchestrator에서 등록하고 구성한 타사 IPAM 서비스 제공자 끝점에서 가져온 IP 범위를 사용할 수 있습니다. IP 범위는 할당 중에 IP 블록에서 생성됩니다.</p> <p>라우팅된 네트워크 프로파일은 라우팅 가능 공간과 사용 가능한 서브넷을 정의합니다.</p> <p>요청 시 네트워크를 위한 라우팅된 네트워크 프로파일 생성 항목을 참조하십시오.</p>

네트워크 프로파일을 사용하여 IP 주소 범위 제어

네트워크 프로파일을 사용해 Linux kickstart 또는 autoYaST를 사용하여 복제를 통해 프로비저닝된 가상 시스템이나, kickstart를 사용하여 OpenStack에서 프로비저닝된 클라우드 시스템에 사전 정의된 범위의 정적 IP 주소를 할당할 수 있습니다.

기본적으로 vRealize Automation은 프로비저닝된 시스템에 DHCP(Dynamic Host Configuration Protocol)를 사용하여 IP 주소를 할당합니다.

네트워크 프로파일을 생성하여 시스템에 할당 가능한 정적 IP 주소의 범위를 정의할 수 있습니다. 예약의 특정 네트워크 경로에 네트워크 프로파일을 할당할 수 있습니다. 복제를 통하거나 kickstart 또는 autoYaST를 통해 프로비저닝되고 연결된 네트워크 프로파일을 사용하여 네트워크 경로에 연결된 시스템은 할당된 정적 IP 주소를 사용하여 프로비저닝됩니다. 정적 IP 주소 할당을 사용하는 프로비저닝의 경우 사용자 지정 규칙을 사용해야 합니다.

기존의 요청 시 NAT 또는 요청 시 라우팅된 네트워크 구성 요소를 설계 캔버스에 추가하고 vSphere 시스템 구성 요소를 연결할 네트워크 프로파일을 선택하는 방법으로 네트워크 프로파일을 Blueprint의 vSphere 시스템 구성 요소에 할당할 수 있습니다. 또한 사용자 지정 속성 `VirtualMachine.NetworkN.ProfileName`(여기서 N은 네트워크 식별자)을 사용하여 Blueprint에 네트워크 프로파일을 할당할 수도 있습니다.

필요한 경우 제공된 vRealize Automation IPAM이나 네트워크 프로파일에 등록 및 구성된 타사 IPAM 서비스 제공자 끝점을 사용하여 IP 주소를 가져와 구성할 수 있습니다. 외부 IPAM 요구 사항에 대한 자세한 내용은 [타사 IPAM 제공자 지원을 제공하기 위한 검사 목록](#) 항목을 참조하십시오.

네트워크 프로파일에서 타사 IPAM 서비스 제공자 끝점을 선택하면 vRealize Automation은 Infoblox와 같은 등록된 외부 IPAM 제공자 끝점에서 IP 범위를 검색합니다. 그런 다음 해당 끝점의 IP 값을 할당합니다. 지정된 서브넷 마스크 범위는 IP 블록에서 서브넷을 할당하는 데 사용됩니다.

예약과 Blueprint에 네트워크 프로파일을 지정하는 경우, Blueprint 값이 우선합니다. 예를 들어, `VirtualMachine.NetworkN.ProfileName` 사용자 지정 속성을 사용하여 Blueprint에 또는 Blueprint에 사용되는 예약에 네트워크 프로파일을 지정하면 Blueprint에 지정된 네트워크 프로파일이 우선합니다. 하지만 Blueprint에서 사용자 지정 속성이 사용되지 않고 사용자가 시스템 NIC를 위한 네트워크 프로파일을 선택하는 경우, vRealize Automation에서는 네트워크 프로파일이 지정되는 시스템 NIC에 대한 예약 네트워크 경로를 사용합니다.

네트워크 프로파일 IP 주소를 가져오기 위한 CSV 파일 형식 이해

올바른 형식의 CSV 파일을 사용하여 IP 주소 네트워크 범위를 vRealize Automation 네트워크 프로파일로 가져올 수 있습니다.

CSV 파일 항목은 다음 형식을 준수해야 합니다.

CSV 필드	설명
<code>ip_address</code>	IPv4 형식의 IP 주소입니다.
<code>machine_name</code>	vRealize Automation의 관리되는 시스템 이름입니다. 이 필드가 비어 있으면 기본적으로 이름이 없습니다. 이 필드가 비어 있으면 <code>status</code> 필드 값이 <code>Allocated</code> 일 수 없습니다.
<code>status</code>	<code>Allocated</code> 또는 <code>Unallocated</code> 이며, 대/소문자를 구분합니다. 필드가 비어 있으면 기본값은 <code>Unallocated</code> 입니다. <code>status</code> 가 <code>Allocated</code> 이면 <code>machine_name</code> 필드를 비워둘 수 없습니다.
<code>NIC_offset</code>	음수가 아닌 정수입니다. 선택 사항입니다.

다음 예제 항목은 NIC 오프셋을 지정하지 않습니다.

```
100.10.100.1,mymachine01,Allocated
```

CSV 파일에서 네트워크 프로파일로 IP 주소 가져오기

올바른 형식의 CSV 파일을 가져와서 IP 주소를 네트워크 프로파일 범위에 추가할 수 있습니다. vRealize Automation에서 범위를 편집하거나, 변경되거나 다른 CSV 파일을 가져와서 네트워크 프로파일 범위의 주소를 변경할 수도 있습니다.

CSV 파일에서 가져오거나 값을 수동으로 입력하여 네트워크 프로파일 범위에서 IP 주소를 추가하거나 변경할 수 있습니다. 또는 타사 IPAM 제공자가 IP 주소를 제공하게 할 수 있습니다.

- 초기 IP 주소 범위를 vRealize Automation 네트워크 프로파일에 가져옵니다.

- 가져온 값을 적용하여 네트워크 프로파일에 처음으로 이름이 지정된 네트워크 범위를 만듭니다.
- 네트워크 범위 vRealize Automation에서 하나 이상의 IP 주소를 삭제합니다.
- 변경된 CSV 또는 다른 CSV 파일을 가져와서 네트워크 범위 값이 어떻게 변경되었는지 검토합니다.

타사 IPAM 끝점을 사용하는 네트워크 프로파일의 경우 vRealize Automation이 아니라 타사 IPAM 제공자가 IP 주소를 관리하기 때문에 **CSV에서 가져오기** 옵션을 사용할 수 없습니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 네트워크 범위로 가져오려는 IP 주소가 포함된 CSV 파일을 생성합니다. [타사 IPAM 제공자를 사용하여 외부 네트워크 프로파일 생성](#) 및 [네트워크 프로파일 IP 주소를 가져오기 위한 CSV 파일 형식 이해](#) 항목을 참조하십시오.

프로시저

- 1 **인프라 > 예약 > 네트워크 프로파일**을 선택합니다.
- 2 **새로 만들기**를 클릭하고 드롭다운 메뉴에서 **네트워크 프로파일 유형**을 선택합니다.
이 예에서는 **외부**를 선택합니다.
- 3 **이름** 텍스트 상자에 **CSV를 사용한 내 네트워크 프로파일**을 입력합니다.
- 4 **설명** 텍스트 상자에 **CSV를 사용하여 네트워크 IP 주소 범위 테스트**를 입력합니다.
CSV 파일 가져오기 옵션은 **네트워크 범위** 및 **IP 주소** 탭 페이지에 있는 설정에 적용됩니다. 따라서 처음 두 개 탭을 빠르게 이동하여 기본 네트워크 프로파일 정보를 입력합니다.
- 5 원하면 구성된 IPAM 끝점을 선택합니다(사용 가능한 항목이 있는 경우). 그렇지 않으면, 이 단계를 건너뛰니다.
- 6 **서브넷 마스크** 및 **게이트웨이** 텍스트 상자에 적절한 IP 주소 값을 입력합니다.
- 7 **DNS** 탭을 클릭합니다.
- 8 DNS 접미사와 같은 관련 정보를 입력하고 **네트워크 범위** 탭을 클릭합니다.
네트워크 범위 탭을 클릭하면 **CSV에서 가져오기** 옵션을 사용할 수 있습니다.
- 9 **새로 만들기**를 클릭하여 새 네트워크 범위 이름과 IP 주소 범위를 수동으로 입력하거나 **CSV에서 가져오기**를 클릭하여 올바른 형식의 CSV 파일에서 IP 주소 정보를 가져옵니다.
 - **새로 만들기**를 클릭합니다.
 - a 네트워크 범위 이름을 입력합니다.
 - b 네트워크 범위에 대한 설명을 입력합니다.
 - c 범위의 시작 IP 주소를 입력합니다.

d 범위의 끝 IP 주소를 입력합니다.

■ **CSV에서 가져오기**를 클릭합니다.

a CSV 파일을 찾아 선택하거나 **CSV에서 가져오기** 대화상자에서 CSV 파일을 끌어옵니다.

CSV 파일의 행은 ip_address, machine_name, status, NIC_offset 형식입니다.

예:

```
100.10.100.1,mymachine01,Allocated
```

CSV 필드	설명
ip_address	IPv4 형식의 IP 주소입니다.
machine_name	vRealize Automation의 관리되는 시스템 이름입니다. 이 필드가 비어 있으면 기본적으로 이름이 없습니다. 이 필드가 비어 있으면 status 필드 값이 Allocated일 수 없습니다.
status	Allocated 또는 Unallocated이며, 대/소문자를 구분합니다. 필드가 비어 있으면 기본값은 Unallocated입니다. status가 Allocated이면 machine_name 필드를 비워둘 수 없습니다.
NIC_offset	음수가 아닌 정수입니다. 선택 사항입니다.

b **적용**을 클릭합니다.

10 확인을 클릭합니다.

IP 범위 이름이 정의된 범위 목록에 나타납니다. 범위 내의 IP 주소가 정의된 IP 주소 목록에 나타납니다.

적용을 클릭하거나 저장하고 네트워크 프로파일을 편집하고 나면 업로드된 IP 주소가 **IP 주소** 페이지에 나타납니다.

11 IP 주소 탭을 클릭하여 지정된 주소 공간 범위의 IP 주소 데이터를 표시합니다.

CSV 파일에서 IP 주소 정보를 가져온 경우, 범위 이름이 CSV에서 가져옴으로 생성됩니다.

12 (선택 사항) 네트워크 범위 드롭다운 메뉴에서 IP 주소 정보를 선택하여 IP 주소 항목을 필터링합니다.

모든 정의된 네트워크 범위, CSV 파일에서 가져온 네트워크 범위 또는 명명된 네트워크 범위에 대한 정보를 표시할 수 있습니다. 세부 정보에는 시작 IP 주소, 시스템 이름, 마지막 수정 날짜 및 타임 스탬프, IP 상태가 있습니다.

후속 작업

CSV 파일에서 IP 주소를 다시 가져오는 경우, 이전 IP 주소가 가져온 CSV 파일에 있는 정보로 대체됩니다.

기존 네트워크를 위한 외부 네트워크 프로파일 생성

외부 네트워크 프로파일을 생성하여 프로비저닝 중 NSX Edge 장치가 사용되도록 구성하는 것을 포함하여 시스템 프로비저닝을 위해 기존 네트워크를 구성하도록 네트워크 설정을 지정할 수 있습니다.

제공된 vRealize Automation IPAM 제공자 끝점 또는 vRealize Orchestrator에 등록된 Infoblox와 같은 타사 IPAM 제공자 끝점을 사용할 수 있습니다.

제공된 IPAM 끝점을 사용하여 외부 네트워크 프로파일 생성

외부 네트워크 프로파일을 생성하여 기존 네트워크에서 시스템을 프로비저닝할 때 사용할 네트워크 속성과 정적 IP 주소 범위를 정의할 수 있습니다.

네트워크 프로파일에서 시스템 프로비저닝에 사용하기 위한 하나 이상의 네트워크 정적 IP 주소 범위를 정의할 수 있습니다. 범위를 지정하지 않는 경우 네트워크 프로파일을 네트워크 예약 정책으로 사용하여 가상 시스템 네트워크 카드(vNIC)에 대한 예약 네트워크 경로를 선택할 수 있습니다.

외부 네트워크 프로파일 생성 및 외부 IPAM 제공자 끝점 사용에 대한 자세한 내용은 [타사 IPAM 제공자를 사용하여 외부 네트워크 프로파일 생성](#)을 참조하십시오.

프로시저

1 제공되는 IPAM 끝점을 사용하여 외부 네트워크 프로파일 정보 지정

외부 네트워크 프로파일은 기존 네트워크의 네트워크 속성과 설정을 식별합니다. 외부 네트워크 프로파일은 NAT 및 라우팅된 네트워크 프로파일의 요구 사항입니다.

2 Object Missing

후속 작업

네트워크 프로파일을 예약의 네트워크 경로에 할당하거나 Blueprint 설계자가 Blueprint에서 네트워크 프로파일을 지정할 수 있습니다. 요청 시 NAT 또는 라우팅된 네트워크 프로파일 생성 시 외부 네트워크 프로파일을 사용할 수 있습니다.

제공되는 IPAM 끝점을 사용하여 외부 네트워크 프로파일 정보 지정

외부 네트워크 프로파일은 기존 네트워크의 네트워크 속성과 설정을 식별합니다. 외부 네트워크 프로파일은 NAT 및 라우팅된 네트워크 프로파일의 요구 사항입니다.

Infoblox와 같은 등록된 타사 IPAM 끝점에서 IPAM 주소 정보를 가져와 외부 네트워크 프로파일을 생성하는 방법에 대한 자세한 내용은 [타사 IPAM 제공자 지원을 제공하기 위한 검사 목록](#) 및 [타사 IPAM 제공자를 사용하여 외부 네트워크 프로파일 생성](#) 항목을 참조하십시오. VMware 내부 IPAM 끝점을 사용하여 네트워크 프로파일을 생성하려면 다음 절차를 따릅니다.

필수 조건

- 패브릭 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **인프라 > 예약 > 네트워크 프로파일**을 선택합니다.
- 2 **새로 만들기**를 클릭하고 드롭다운 메뉴에서 **기존** 또는 **외부**를 선택합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 4 제공된 **vRealize Automation IPAM** 끝점에 대한 기본 **IPAM 끝점** 값을 그대로 사용합니다.
- 5 **서브넷 마스크** 텍스트 상자에 IP 서브넷 마스크를 입력합니다.

서브넷 마스크는 네트워크 프로파일에 대해 정의할 라우팅 가능한 전체 주소 공간의 크기를 지정합니다.

예를 들어 255.255.0.0을 입력합니다.

6 게이트웨이 텍스트 상자에 Edge 또는 라우팅된 게이트웨이 주소를 입력합니다.

표준 IPv4 주소 형식을 사용하십시오. 예를 들어 10.10.110.1을 입력합니다.

네트워크 프로파일에 정의된 게이트웨이 IP 주소는 할당 중에 NIC에 할당됩니다. 네트워크 프로파일의 **게이트웨이** 텍스트 상자에 아무 값도 할당되지 않은 경우 Edge 시스템을 프로비저닝 할 때 VirtualMachine.Network0.Gateway 사용자 지정 속성을 사용해야 합니다.

7 DNS 탭을 클릭합니다.

8 필요한 경우 DNS 및 WINS 값을 입력합니다.

DNS 값은 DNS 이름 등록 및 확인을 위해 사용됩니다. 내부 IPAM 끝점을 사용하고 있으면 DNS 및 WINS 필드는 선택 사항입니다. 외부 IPAM 끝점을 사용하고 있으면 DNS 및 WINS 값은 타사 IPAM 제공자에 의해 제공됩니다.

- a (선택 사항) **기본 DNS** 서버 값을 입력합니다.
- b (선택 사항) **보조 DNS** 서버 값을 입력합니다.
- c (선택 사항) **DNS 접미사** 값을 입력합니다.
- d (선택 사항) **DNS 검색 접미사** 값을 입력합니다.
- e (선택 사항) **기본 설정 WINS** 서버 값을 입력합니다.
- f (선택 사항) **대체 WINS** 서버 값을 입력합니다.

후속 작업

정적 IP 주소에 대한 IP 범위를 구성할 수 있습니다. [Object Missing](#) 항목을 참조하십시오.

Object Missing

This object is not available in the repository.

타사 IPAM 제공자를 사용하여 외부 네트워크 프로파일 생성

vRealize Orchestrator에서 타사 제공자로부터 IP 주소를 얻기 위해 가져오고 구성하고 등록한 해당 타사 IPAM 제공자 솔루션을 사용할 수 있습니다.

등록된 타사 IPAM 솔루션 제공자 끝점을 사용하여 게이트웨이, 서브넷 마스크 및 DHCP/WINS 설정을 가져오는 외부 네트워크 프로파일을 생성할 수 있습니다.

네트워크 프로파일에서 시스템 프로비저닝에 사용하기 위한 하나 이상의 네트워크 정적 IP 주소 범위를 정의할 수 있습니다. 범위를 지정하지 않는 경우 네트워크 프로파일을 네트워크 예약 정책으로 사용하여 가상 시스템 네트워크 카드(vNIC)에 대한 예약 네트워크 경로를 선택할 수 있습니다.

IPAM 제공자를 사용하지 않거나 제공된 내부 IPAM 제공자 끝점을 사용하여 외부 네트워크 프로파일을 생성하는 방법에 대한 자세한 내용은 [제공된 IPAM 끝점을 사용하여 외부 네트워크 프로파일 생성](#) 항목을 참조하십시오.

프로시저

1 타사 IPAM 끝점을 사용하여 외부 네트워크 프로파일 정보 지정

외부 네트워크 프로파일은 기존 네트워크의 네트워크 속성과 설정을 식별합니다. 외부 네트워크 프로파일은 NAT 및 라우팅된 네트워크 프로파일의 요구 사항입니다. vRealize Orchestrator에서 IPAM 끝점을 등록하고 구성한 경우, IPAM 제공자에서 IP 주소 정보를 제공해야 한다고 지정할 수 있습니다.

2 타사 IPAM 끝점을 사용하여 외부 네트워크 프로파일 IP 범위 구성

네트워크 프로파일에서 시스템 프로비저닝에 사용하기 위한 하나 이상의 네트워크 정적 IP 주소 범위를 정의할 수 있습니다. 범위를 지정하지 않는 경우 네트워크 프로파일을 네트워크 예약 정책으로 사용하여 가상 시스템 네트워크 카드(vNIC)에 대한 예약 네트워크 경로를 선택할 수 있습니다.

후속 작업

네트워크 프로파일을 예약의 네트워크 경로에 할당하거나 Blueprint 설계자가 Blueprint에서 네트워크 프로파일을 지정할 수 있습니다. 요청 시 NAT 또는 라우팅된 네트워크 프로파일 생성 시 외부 네트워크 프로파일을 사용할 수 있습니다.

타사 IPAM 끝점을 사용하여 외부 네트워크 프로파일 정보 지정

외부 네트워크 프로파일은 기존 네트워크의 네트워크 속성과 설정을 식별합니다. 외부 네트워크 프로파일은 NAT 및 라우팅된 네트워크 프로파일의 요구 사항입니다. vRealize Orchestrator에서 IPAM 끝점을 등록하고 구성한 경우, IPAM 제공자에서 IP 주소 정보를 제공해야 한다고 지정할 수 있습니다.

필수 조건

- vRealize Orchestrator에서 외부 IPAM 제공자 플러그인을 가져오고 구성한 후 IPAM 제공자 끝점 유형을 vRealize Orchestrator에 등록했는지 확인합니다. 이 예에서 지원되는 외부 IPAM 솔루션 제공자는 Infoblox입니다. [타사 IPAM 제공자 지원을 제공하기 위한 검사 목록](#) 항목을 참조하십시오.
- [타사 IPAM 제공자 끝점 생성](#).
- 등록된 IPAM 끝점 워크플로를 사용하여 vRealize Orchestrator Appliance를 글로벌 테넌트의 독립형 Orchestrator로 구성합니다(administrator @ vsphere.local).
- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **인프라 > 예약 > 네트워크 프로파일**을 선택합니다.
- 2 **새로 만들기**를 클릭하고 드롭다운 메뉴에서 **기존** 또는 **외부**를 선택합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.

- 4 하나 이상의 타사 IPAM 제공자 끝점을 구성한 경우 **IPAM 끝점** 드롭다운 메뉴에서 타사 IPAM 끝점을 선택합니다.

vRealize Orchestrator에서 등록한 타사 IPAM 제공자 끝점을 선택하면 지정된 IPAM 서비스 제공자로부터 IP 주소를 가져옵니다. 서브넷 마스크와 같은 IP 규격 및 DNS/WINS 옵션은 해당 기능이 선택된 타사 IPAM 끝점에 의해 제어되기 때문에 사용할 수 없습니다.

후속 작업

이제 IP 주소의 네트워크 범위를 정의하면 네트워크 프로파일 정의가 완료됩니다.

타사 IPAM 끝점을 사용하여 외부 네트워크 프로파일 IP 범위 구성

네트워크 프로파일에서 시스템 프로비저닝에 사용하기 위한 하나 이상의 네트워크 정적 IP 주소 범위를 정의할 수 있습니다. 범위를 지정하지 않는 경우 네트워크 프로파일을 네트워크 예약 정책으로 사용하여 가상 시스템 네트워크 카드(vNIC)에 대한 예약 네트워크 경로를 선택할 수 있습니다.

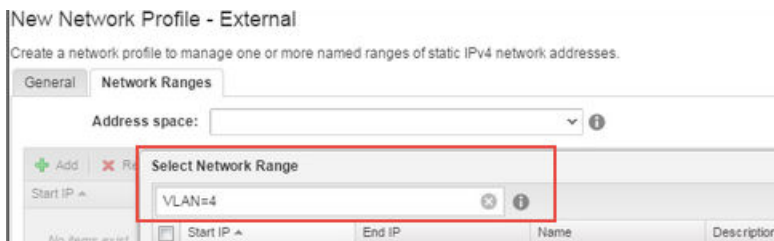
타사 IPAM 제공자가 제공한 IP 주소를 사용하여 IP 범위를 정의할 수 있습니다.

vRealize Automation은 범위 세부 정보가 아닌 외부 IPAM 범위 ID만 데이터베이스에 저장합니다. 이 페이지 또는 Blueprint에서 네트워크 프로파일을 편집하는 경우 vRealize Automation은 IPAM 서비스를 호출하여 선택된 범위 ID를 기반으로 범위 세부 정보를 가져옵니다.

참고 일부 타사 IPAM 제공자의 경우 네트워크 범위를 반환할 때 쿼리에 시간 초과가 발생하여 빈 목록이 반환되는 알려진 문제가 있습니다. 이에 대한 해결 방법으로 시간 초과를 피하도록 검색 기준을 제공하면 네트워크 범위 정보를 얻을 수 있습니다.

예를 들어 IPAM 제공자에 따라서 IPAM 제공자 애플리케이션의 각 네트워크에 VLAN이라는 속성을 추가하고 이 속성에 4와 같은 값을 할당할 수 있습니다. 그런 다음 vRealize Automation 네트워크 프로파일 페이지의 **네트워크 범위 선택** 텍스트 상자에서 속성 및 값(예: VLAN=4)을 기준으로 필터링할 수

있습니다.



대안으로 다음 절차를 사용하여 시간 초과 설정을 늘릴 수 있습니다.

- 1 각각의 vRealize Automation 장치 노드에서 `/etc/vcac/webapps/o11n-gateway-service/WEB-INF/classes/META-INF/spring/root/o11n-gateway-service-context.xml` 파일을 엽니다.
- 2 시간 초과 값을 30초에서 더 큰 수로 변경합니다.
- 3 `service vcac-server restart`를 입력하여 vcac-server를 다시 시작합니다.

필수 조건

타사 IPAM 끝점을 사용하여 외부 네트워크 프로파일 정보 지정.

프로시저

- 1 **네트워크 범위** 탭을 클릭하여 새 네트워크 범위를 생성하거나 기존 네트워크 범위를 선택합니다.

각 이름, 설명, 시작 IP 주소 및 끝 IP 주소와 같은 선택한 범위에 대한 세부 정보가 나타납니다. 상태 관련 정보도 제공됩니다.

- 2 **주소 공간** 드롭다운 메뉴에서 끝점에 대해 사용할 수 있는 모든 주소 공간 목록에서 주소 공간을 선택합니다.

- 3 **추가**를 클릭하고 지정된 주소 공간에 대해 사용할 수 있는 네트워크 범위를 하나 이상 선택합니다.

타사 IPAM 제공자를 사용할 때 네트워크 범위를 선택하면 목록이 비어 있을 수 있습니다. 자세한 내용은 기술 자료 문서 2148656(<http://kb.vmware.com/kb/2148656>)을 참조하십시오.

- 4 **확인**을 클릭합니다.

IP 범위 이름이 정의된 범위 목록에 나타납니다. 범위 내의 IP 주소가 정의된 IP 주소 목록에 나타납니다.

적용을 클릭하거나 저장하고 네트워크 프로파일을 편집하고 나면 업로드된 IP 주소가 **IP 주소** 페이지에 나타납니다.

- 5 **확인**을 클릭하여 네트워크 프로파일을 완료합니다.

후속 작업

네트워크 프로파일을 예약의 네트워크 경로에 할당하거나 Blueprint 설계자가 Blueprint에서 네트워크 프로파일을 지정할 수 있습니다.

요청 시 네트워크를 위한 라우팅된 네트워크 프로파일 생성

제공된 vRealize Automation IPAM 끝점 또는 제대로 구성되고 등록된 타사 IPAM 끝점을 사용하는 요청 시 라우팅된 네트워크 프로파일을 생성할 수 있습니다.

라우팅된 네트워크 프로파일은 여러 네트워크로 나누어지는 라우팅 가능한 IP 공간을 나타냅니다. 새 라우팅된 네트워크는 각각 라우팅 가능한 IP 공간에서 사용 가능한 다음 서브넷을 할당합니다. 라우팅된 네트워크에서 같은 네트워크 프로파일을 사용하는 다른 모든 라우팅된 네트워크에 액세스할 수 있습니다. 각 라우팅된 서브넷은 동일한 네트워크 프로파일에서 생성된 다른 모든 서브넷에 액세스할 수 있습니다.

타사 IPAM 제공자의 경우, 타사 IPAM 제공자가 라우팅 가능한 IP 공간을 생성하고 관리합니다. 네트워크 관리자는 타사 IPAM 제공자를 사용하여 라우팅 가능한 IP 공간을 정의하고 그에 대한 IP 블록을 생성합니다. 라우팅된 네트워크 프로파일을 생성하거나 편집할 때 타사 IPAM 제공자에서 검색된 IP 블록을 하나 이상 선택할 수 있습니다.

타사 IPAM 제공자에서 라우팅된 네트워크 프로파일의 새 인스턴스가 할당되는 경우

vRealize Automation이 라우팅된 프로파일 및 서브넷 크기에 의해 결정되는 IP 블록을 사용하여 다음 사용할 수 있는 서브넷을 예약하고 범위를 생성하도록 제공자를 호출합니다. 결과 범위가 동일한 배포에서 라우팅된 네트워크에 할당된 시스템에 IP 주소를 할당하는 데 사용됩니다.

제공된 IPAM 끝점을 사용하여 라우팅된 네트워크 프로파일 생성

제공된 IPAM 끝점으로 라우팅된 네트워크 프로파일을 사용 중인 경우 요청 시 라우팅된 네트워크에 대해 라우팅 가능 IP 공간 및 사용할 수 있는 서브넷을 정의할 수 있습니다.

제공된 vRealize Automation IPAM 끝점을 사용하여 라우팅된 네트워크 프로파일에 정적 IP 주소 범위 및 기본 IP 주소를 할당할 수 있습니다.

제공된 VMware IPAM 끝점 또는 Infoblox IPAM과 같은 vRealize Orchestrator에서 등록하고 구성한 타사 IPAM 서비스 제공자 끝점에서 가져온 IP 범위를 사용할 수 있습니다. IP 범위는 할당 중에 IP 블록에서 생성됩니다.

프로시저

1 vRealize Automation IPAM 끝점으로 라우팅된 네트워크 프로파일 정보 지정

네트워크 프로파일 정보는 라우팅된 네트워크 속성, 해당하는 기본 외부 네트워크 프로파일 및 제공된 IPAM 끝점 사용 시 네트워크 프로비저닝에 사용되는 기타 값을 식별합니다.

2 vRealize Automation IPAM 끝점으로 라우팅된 네트워크 프로파일 IP 범위 구성

네트워크 프로비저닝에 사용할 수 있도록 정적 IP 주소 범위를 하나 이상 정의할 수 있습니다.

vRealize Automation IPAM 끝점으로 라우팅된 네트워크 프로파일 정보 지정

네트워크 프로파일 정보는 라우팅된 네트워크 속성, 해당하는 기본 외부 네트워크 프로파일 및 제공된 IPAM 끝점 사용 시 네트워크 프로비저닝에 사용되는 기타 값을 식별합니다.

타사 IPAM 끝점을 사용하여 라우팅된 네트워크 프로파일을 생성하려는 경우 [타사 IPAM 끝점으로 라우팅된 네트워크 프로파일 정보 지정](#)을 참조하십시오.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 외부 네트워크 프로파일을 생성합니다. [제공된 IPAM 끝점을 사용하여 외부 네트워크 프로파일 생성](#) 항목을 참조하십시오.

프로시저

- 1 **인프라 > 예약 > 네트워크 프로파일**을 선택합니다.
- 2 **새로 만들기**를 클릭하고 드롭다운 메뉴에서 **라우팅됨**을 선택합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 4 제공된 **vRealize Automation IPAM** 끝점에 대한 기본 **IPAM 끝점** 값을 그대로 사용합니다.
- 5 **외부 네트워크 프로파일** 드롭다운 메뉴에서 기존 외부 네트워크 프로파일을 선택합니다.
- 6 **서브넷 마스크** 텍스트 상자에 외부 네트워크 프로파일에 연결된 서브넷 마스크를 입력합니다.

서브넷 마스크는 네트워크 프로파일에 대해 정의할 라우팅 가능한 전체 주소 공간의 크기를 지정합니다.

예를 들어 255.255.0.0을 입력합니다.

- 7 서브넷 마스크 범위** 텍스트 상자 드롭다운 메뉴에서 값을 선택하여 **IP 범위** 페이지의 **범위 생성** 옵션에 따라 범위가 생성되는 방식을 결정합니다.

예를 들어 255.255.255.0을 입력합니다.

서브넷 마스크 범위는 이 공간을 네트워크 프로파일의 모든 배포 인스턴스에 할당되는 개별 주소 블록으로 파티션하는 방법을 정의합니다. 서브넷 마스크 범위에 대한 값을 선택하는 경우 라우팅된 네트워크에 사용할 것으로 예상하는 배포 수를 고려합니다.

범위는 라우팅된 네트워크 프로파일을 사용하는 각 배포에 사용됩니다. 사용 가능한 라우팅된 범위 수는 서브넷 마스크를 서브넷 마스크 범위로 나눈 값(예: 255.255.0.0/255.255.255.0 = 256)과 같습니다.

- 8 기본 IP** 텍스트 상자에 사용 가능한 첫 번째 IP 주소를 입력합니다.

타사 끝점을 선택하면 이 옵션을 사용할 수 없습니다.

예를 들어 120.120.0.1을 입력합니다.

- 9 DNS** 탭을 클릭합니다.

- 10** 필요한 경우 DNS 및 WINS 값을 입력합니다.

DNS 값은 DNS 이름 등록 및 확인을 위해 사용됩니다. 내부 IPAM 끝점을 사용하고 있으면 DNS 및 WINS 필드는 선택 사항입니다. 외부 IPAM 끝점을 사용하고 있으면 DNS 및 WINS 값은 타사 IPAM 제공자에 의해 제공됩니다.

- a (선택 사항) **기본 DNS** 서버 값을 입력합니다.
- b (선택 사항) **보조 DNS** 서버 값을 입력합니다.
- c (선택 사항) **DNS 접미사** 값을 입력합니다.
- d (선택 사항) **DNS 검색 접미사** 값을 입력합니다.
- e (선택 사항) **기본 설정 WINS** 서버 값을 입력합니다.
- f (선택 사항) **대체 WINS** 서버 값을 입력합니다.

후속 작업

[vRealize Automation IPAM 끝점으로 라우팅된 네트워크 프로파일 IP 범위 구성](#).

vRealize Automation IPAM 끝점으로 라우팅된 네트워크 프로파일 IP 범위 구성

네트워크 프로비저닝에 사용할 수 있도록 정적 IP 주소 범위를 하나 이상 정의할 수 있습니다.

프로비저닝 중 새로운 모든 라우팅된 네트워크는 사용 가능한 다음 범위를 할당하고 이것을 해당 IP 공간으로 사용합니다.

필수 조건

[vRealize Automation IPAM 끝점으로 라우팅된 네트워크 프로파일 정보 지정](#).

프로시저

1 네트워크 범위 탭을 클릭하여 새 네트워크 범위를 생성하거나 기존 네트워크 범위를 선택합니다.

각 이름, 설명, 시작 IP 주소 및 끝 IP 주소와 같은 선택한 범위에 대한 세부 정보가 나타납니다. 상태 관련 정보도 제공됩니다.

2 범위 생성을 클릭하여 [일반] 탭에 입력한 서브넷 마스크, 서브넷 마스크 범위 및 기본 IP 주소 정보 정보를 기반으로 네트워크 범위를 생성합니다.

기본 IP 주소를 시작으로, vRealize Automation은 서브넷 마스크 범위를 기반으로 범위를 생성합니다.

예를 들어 vRealize Automation은 범위1 ~ 범위n의 이름을 사용하여 서브넷 마스크가 255.255.0.0이고 서브넷 마스크 범위가 255.255.255.0인 경우 255개 IP 범위를 생성합니다.

3 확인을 클릭합니다.

타사 IPAM 끝점을 사용하여 라우팅된 네트워크 프로파일 생성

타사 IPAM 끝점이 포함된 라우팅된 네트워크 프로파일을 사용하면 타사 IPAM 제공자가 라우팅 가능 IP 공간을 생성하고 관리합니다.

라우팅된 네트워크 프로파일에서 타사 IPAM 끝점을 사용하는 경우 제공자가 요청 시 네트워크의 각 인스턴스에 대해 새 IP 범위를 생성합니다.

제공된 VMware IPAM 끝점 또는 Infoblox IPAM과 같은 vRealize Orchestrator에서 등록하고 구성한 타사 IPAM 서비스 제공자 끝점에서 가져온 IP 범위를 사용할 수 있습니다. IP 범위는 할당 중에 IP 블록에서 생성됩니다.

프로시저

1 타사 IPAM 끝점으로 라우팅된 네트워크 프로파일 정보 지정

네트워크 프로파일 정보는 라우팅된 네트워크 속성, 해당하는 기본 외부 네트워크 프로파일 및 타사 IPAM 끝점 사용 시 네트워크 프로비저닝에 사용되는 기타 값을 식별합니다.

2 타사 IPAM 끝점으로 라우팅된 네트워크 프로파일 IP 범위 구성

네트워크 프로비저닝에 사용할 수 있도록 정적 IPv4 네트워크 주소의 명명된 범위를 하나 이상 관리할 수 있습니다.

타사 IPAM 끝점으로 라우팅된 네트워크 프로파일 정보 지정

네트워크 프로파일 정보는 라우팅된 네트워크 속성, 해당하는 기본 외부 네트워크 프로파일 및 타사 IPAM 끝점 사용 시 네트워크 프로비저닝에 사용되는 기타 값을 식별합니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 외부 네트워크 프로파일을 생성합니다. **제공된 IPAM 끝점을 사용하여 외부 네트워크 프로파일 생성** 또는 **타사 IPAM 제공자를 사용하여 외부 네트워크 프로파일 생성** 항목을 참조하십시오.
- 타사 IPAM 끝점을 생성하고 구성합니다. **타사 IPAM 제공자 끝점 생성** 항목을 참조하십시오.

프로시저

- 1 **인프라 > 예약 > 네트워크 프로파일**을 선택합니다.
- 2 **새로 만들기**를 클릭하고 드롭다운 메뉴에서 **라우팅됨**을 선택합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 4 하나 이상의 타사 IPAM 제공자 끝점을 구성한 경우 **IPAM 끝점** 드롭다운 메뉴에서 타사 IPAM 끝점을 선택합니다.

vRealize Orchestrator에서 등록한 타사 IPAM 제공자 끝점을 선택하면 지정된 IPAM 서비스 제공자로부터 IP 주소를 가져옵니다. 서브넷 마스크와 같은 IP 규격 및 DNS/WINS 옵션은 해당 기능이 선택된 타사 IPAM 끝점에 의해 제어되기 때문에 사용할 수 없습니다.

- 5 **외부 네트워크 프로파일** 드롭다운 메뉴에서 기존 외부 네트워크 프로파일을 선택합니다.

지정된 IPAM 끝점을 사용하도록 구성된 외부 네트워크 프로파일만 나열되고 선택할 수 있습니다.

- 6 **서브넷 마스크 범위** 텍스트 상자 드롭다운 메뉴에서 값을 선택하여 프로비저닝을 위해 생성할 네트워크 서브넷 수를 결정합니다.

예를 들어 255.255.255.0을 입력합니다.

서브넷 마스크 범위는 이 공간을 네트워크 프로파일의 모든 배포 인스턴스에 할당되는 개별 주소 블록으로 파티션하는 방법을 정의합니다. 서브넷 마스크 범위에 대한 값을 선택하는 경우 라우팅된 네트워크에 사용할 것으로 예상하는 배포 수를 고려합니다.

범위는 라우팅된 네트워크 프로파일을 사용하는 각 배포에 사용됩니다. 사용 가능한 라우팅된 범위 수는 서브넷 마스크를 서브넷 마스크 범위로 나눈 값(예: 255.255.0.0/255.255.255.0 = 256)과 같습니다.

- 7 **IP 블록** 탭을 클릭하여 주소 공간을 정의하고 정적 IPv4 네트워크 주소의 이름이 있는 범위 하나 이상을 관리합니다.

사용 가능한 IP 블록은 요청 시 라우팅을 위해 생성되거나 할당되는 IP 범위에 대한 소스입니다.

후속 작업

[타사 IPAM 끝점으로 라우팅된 네트워크 프로파일 IP 범위 구성](#).

타사 IPAM 끝점으로 라우팅된 네트워크 프로파일 IP 범위 구성

네트워크 프로비저닝에 사용할 수 있도록 정적 IPv4 네트워크 주소의 명명된 범위를 하나 이상 관리할 수 있습니다.

프로비저닝 중 각각의 새로운 라우팅된 네트워크는 사용 가능한 다음 범위를 할당하고 할당된 범위를 해당 IP 공간으로 사용합니다. IP 블록은 타사 IPAM 제공자로부터 얻습니다. 프로비저닝 중 제공된 서브넷 마스크 범위와 일치하는 서브넷 마스크가 있는 블록에서 라우팅된 네트워크가 할당됩니다.

필수 조건

[타사 IPAM 끝점으로 라우팅된 네트워크 프로파일 정보 지정](#).

프로시저

- 1 **주소 공간** 드롭다운 메뉴에서 주소 공간을 선택하여 프로비저닝에 사용할 수 있는 IP 블록을 제한합니다.

주소 공간 텍스트 상자 아래 섹션에서 하나 이상의 IP 블록을 추가한 후에는 **주소 공간** 값을 더 이상 선택할 수 없습니다. 라우팅된 네트워크 프로파일은 두 개 이상의 주소 공간에 걸쳐 있을 수 없습니다.

- 2 제공자의 검색 구문을 사용하거나 [검색] 드롭다운 메뉴에서 선택하여 하나 이상의 IP 블록 또는 IPAM 제공자 범위를 추가합니다.

IP 블록은 타사 IPAM 제공자에서 검색됩니다.

타사 IPAM 제공자를 사용할 때 네트워크 범위를 선택하면 목록이 비어 있을 수 있습니다. 자세한 내용은 기술 자료 문서 2148656(<http://kb.vmware.com/kb/2148656>)을 참조하십시오.

- a **추가**를 클릭합니다.
- b **검색**을 클릭합니다.
- c 검색 구문을 입력하거나 드롭다운 메뉴에서 하나 이상의 IP 블록을 선택합니다.
- d **확인**을 클릭합니다.

- 3 **적용**을 클릭합니다.

- 4 **확인**을 클릭합니다.

요청 시 네트워크를 위한 NAT 네트워크 프로파일 생성

제공된 vRealize Automation IPAM 끝점 또는 제대로 구성되고 등록된 타사 IPAM 끝점을 사용하는 요청 시 NAT 네트워크 프로파일을 생성할 수 있습니다.

제공된 IPAM 끝점을 사용하여 NAT 네트워크 프로파일 생성

외부 네트워크 프로파일과 관련하여 요청 시 NSX NAT 네트워크 프로파일을 생성할 수 있습니다. 제공된 vRealize Automation IPAM 끝점을 사용하는 경우 NAT 네트워크 프로파일에 정적 IP 및 DHCP 주소 범위를 할당할 수 있습니다.

NAT 네트워크는 외부 통신에 한 IP 주소 집합을 사용하고 내부 통신에 다른 IP 주소 집합을 사용합니다. 외부 IP 주소는 외부 네트워크 프로파일에서 할당되고 내부 NAT IP 주소는 NAT 네트워크 프로파일에 의해 정의됩니다. 새 NAT 네트워크를 프로비저닝하는 경우 NAT 네트워크 프로파일의 새 인스턴스가 생성되어 시스템 IP 주소를 할당하는 데 사용됩니다.

제공된 VMware IPAM 끝점 또는 Infoblox IPAM과 같은 vRealize Orchestrator에서 등록하고 구성한 타사 IPAM 서비스 제공자 끝점에서 가져온 IP 범위를 사용할 수 있습니다. IP 범위는 할당 중에 IP 블록에서 생성됩니다.

NAT 일대다 네트워크의 경우 Blueprint에 NAT 네트워크 구성 요소를 추가할 때 구성할 수 있고 배포에서 NAT 네트워크를 편집할 때 변경할 수 있는 NAT 규칙을 정의할 수 있습니다.

프로시저

1 vRealize Automation IPAM 끝점을 사용하는 NAT 네트워크 프로파일 정보 지정

네트워크 프로파일은 포함된 vRealize Automation IPAM을 사용하여 NAT 네트워크 속성, 기본 외부 네트워크 프로파일, NAT 유형 및 네트워크 프로비저닝에 사용되는 기타 값을 식별합니다.

2 vRealize Automation IPAM 끝점을 사용하여 NAT 네트워크 프로파일 IP 범위 구성

네트워크 프로비저닝에 사용할 수 있도록 정적 IP 주소 범위를 하나 이상 정의할 수 있습니다.

vRealize Automation IPAM 끝점을 사용하는 NAT 네트워크 프로파일 정보 지정

네트워크 프로파일은 포함된 vRealize Automation IPAM을 사용하여 NAT 네트워크 속성, 기본 외부 네트워크 프로파일, NAT 유형 및 네트워크 프로비저닝에 사용되는 기타 값을 식별합니다.

타사 IPAM 끝점을 사용하는 NAT 네트워크 프로파일을 생성하려면 [타사 IPAM 끝점을 사용하는 NAT 네트워크 프로파일 정보 지정](#) 항목을 참조하십시오.

필수 조건

- 패브릭 관리자 vRealize Automation 콘솔에 로그인합니다.
- 외부 네트워크 프로파일을 생성합니다. [제공된 IPAM 끝점을 사용하여 외부 네트워크 프로파일 생성](#) 항목을 참조하십시오.

프로시저

- 1 **인프라 > 예약 > 네트워크 프로파일**을 선택합니다.
- 2 **새로 만들기**를 클릭하고 드롭다운 메뉴에서 **NAT**를 선택합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 4 제공된 **vRealize Automation IPAM** 끝점에 대한 기본 **IPAM 끝점** 값을 그대로 사용합니다.
- 5 **외부 네트워크 프로파일** 드롭다운 메뉴에서 기존 외부 네트워크 프로파일을 선택합니다.
- 6 **NAT 유형** 드롭다운 메뉴에서 일대일 또는 일대다 네트워크 주소 변환 유형을 선택합니다.

옵션	설명
일대일	<p>각 네트워크 어댑터에 외부 정적 IP 주소를 할당합니다. 각 시스템이 외부 네트워크에 액세스할 수 있으며, 외부 네트워크에서도 각 시스템에 액세스할 수 있습니다.</p> <p>NSX Edge 업링크에 할당된 모든 외부 IP 주소는 동일한 서브넷의 일부여야 합니다. vRealize Automation에서 NAT 1:1을 사용할 때, 해당하는 외부 네트워크 프로파일에는 단일 서브넷 내에 존재하는 IP 범위만 포함되어야 합니다.</p>
일대다	<p>네트워크의 모든 시스템이 외부 IP 주소 하나를 공유합니다. 내부 시스템은 DHCP 또는 정적 IP 주소를 사용할 수 있습니다. 모든 시스템에서 외부 네트워크에 액세스할 수 있지만 외부 네트워크에서는 그 어떤 시스템에도 액세스할 수 없습니다. 이 옵션을 선택하면 DHCP 그룹의 사용 확인란이 활성화됩니다.</p> <p>NAT 일대다 변환 유형을 사용하면 NAT 네트워크 구성 요소를 Blueprint에 추가할 때 NAT 규칙을 정의할 수 있습니다.</p>

7 서브넷 마스크 텍스트 상자에 IP 서브넷 마스크를 입력합니다.

서브넷 마스크는 네트워크 프로파일에 대해 정의할 라우팅 가능한 전체 주소 공간의 크기를 지정합니다.

예를 들어 255.255.0.0을 입력합니다.

8 게이트웨이 텍스트 상자에 Edge 또는 라우팅된 게이트웨이 주소를 입력합니다.

표준 IPv4 주소 형식을 사용하십시오. 예를 들어 10.10.110.1을 입력합니다.

네트워크 프로파일에 정의된 게이트웨이 IP 주소는 할당 중에 NIC에 할당됩니다. 네트워크 프로파일의 **게이트웨이** 텍스트 상자에 아무 값도 할당되지 않은 경우 Edge 시스템을 프로비저닝 할 때 VirtualMachine.Network0.Gateway 사용자 지정 속성을 사용해야 합니다.

9 (선택 사항) DHCP 그룹에서 사용 확인란을 선택하고 **IP 범위 시작** 및 **IP 범위 끝** 값을 입력합니다.

이 확인란은 NAT 유형을 [일대다]로 설정한 경우에만 선택할 수 있습니다.

10 (선택 사항) 시스템에서 IP 주소를 사용할 수 있는 시간을 정의하려면 DHCP 리스 시간을 설정합니다.**11 DNS** 탭을 클릭합니다.**12 필요한 경우 DNS 및 WINS 값을 입력합니다.**

DNS 값은 DNS 이름 등록 및 확인을 위해 사용됩니다. 내부 IPAM 끝점을 사용하고 있으면 DNS 및 WINS 필드는 선택 사항입니다. 외부 IPAM 끝점을 사용하고 있으면 DNS 및 WINS 값은 타사 IPAM 제공자에 의해 제공됩니다.

- a (선택 사항) **기본 DNS** 서버 값을 입력합니다.
- b (선택 사항) **보조 DNS** 서버 값을 입력합니다.
- c (선택 사항) **DNS 접미사** 값을 입력합니다.
- d (선택 사항) **DNS 검색 접미사** 값을 입력합니다.
- e (선택 사항) **기본 설정 WINS** 서버 값을 입력합니다.
- f (선택 사항) **대체 WINS** 서버 값을 입력합니다.

후속 작업

[vRealize Automation IPAM 끝점을 사용하여 NAT 네트워크 프로파일 IP 범위 구성.](#)

vRealize Automation IPAM 끝점을 사용하여 NAT 네트워크 프로파일 IP 범위 구성

네트워크 프로비저닝에 사용할 수 있도록 정적 IP 주소 범위를 하나 이상 정의할 수 있습니다.

네트워크 IP 주소 범위의 시작 및 끝을 DHCP 주소와 겹치게 할 수 없습니다. 겹치는 주소 범위가 있는 프로파일을 저장하려고 하면 vRealize Automation에 검증 오류가 표시됩니다.

필수 조건

[vRealize Automation IPAM 끝점을 사용하는 NAT 네트워크 프로파일 정보 지정.](#)

프로시저

- 1 **네트워크 범위** 탭을 클릭하여 새 네트워크 범위를 생성하거나 기존 네트워크 범위를 선택합니다.

각 이름, 설명, 시작 IP 주소 및 끝 IP 주소와 같은 선택한 범위에 대한 세부 정보가 나타납니다. 상태 관련 정보도 제공됩니다.

- 2 **새로 만들기**를 클릭하여 새 네트워크 범위 이름과 IP 주소 범위를 수동으로 입력하거나 **CSV에서 가져오기**를 클릭하여 올바른 형식의 CSV 파일에서 IP 주소 정보를 가져옵니다.

- **새로 만들기**를 클릭합니다.

- a 네트워크 범위 이름을 입력합니다.
- b 네트워크 범위에 대한 설명을 입력합니다.
- c 범위의 시작 IP 주소를 입력합니다.
- d 범위의 끝 IP 주소를 입력합니다.

- **CSV에서 가져오기**를 클릭합니다.

- a CSV 파일을 찾아 선택하거나 **CSV에서 가져오기** 대화상자에서 CSV 파일을 끌어옵니다. CSV 파일의 행은 ip_address, machine_name, status, NIC_offset 형식입니다. 예:

```
100.10.100.1,mymachine01,Allocated
```

CSV 필드	설명
ip_address	IPv4 형식의 IP 주소입니다.
machine_name	vRealize Automation의 관리되는 시스템 이름입니다. 이 필드가 비어 있으면 기본적으로 이름이 없습니다. 이 필드가 비어 있으면 status 필드 값이 Allocated일 수 없습니다.
status	Allocated 또는 Unallocated이며, 대/소문자를 구분합니다. 필드가 비어 있으면 기본값은 Unallocated입니다. status가 Allocated이면 machine_name 필드를 비워둘 수 없습니다.
NIC_offset	음수가 아닌 정수입니다. 선택 사항입니다.

- b **적용**을 클릭합니다.

- 3 **확인**을 클릭합니다.

IP 범위 이름이 정의된 범위 목록에 나타납니다. 범위 내의 IP 주소가 정의된 IP 주소 목록에 나타납니다.

적용을 클릭하거나 저장하고 네트워크 프로파일을 편집하고 나면 업로드된 IP 주소가 **IP 주소** 페이지에 나타납니다.

- 4 **IP 주소** 탭을 클릭하여 명명된 네트워크 범위의 IP 주소를 표시합니다.

- 5 (선택 사항) **네트워크 범위** 드롭다운 메뉴에서 IP 주소 정보를 선택하여 IP 주소 항목을 필터링합니다.

모든 정의된 네트워크 범위, CSV 파일에서 가져온 네트워크 범위 또는 명명된 네트워크 범위에 대한 정보를 표시할 수 있습니다. 세부 정보에는 시작 IP 주소, 시스템 이름, 마지막 수정 날짜 및 타임 스탬프, IP 상태가 있습니다.

- 6 (선택 사항) **IP 상태** 드롭다운 메뉴에서 상태 유형을 선택하여 IP 주소 항목을 선택한 IP 상태와 일치하는 항목으로만 필터링합니다. 상태 설정은 [할당됨], [할당 취소됨], [제거됨] 및 [만료됨]입니다.

IP 주소가 만료되거나 삭제된 상태인 경우, **회수**를 클릭하면 해당 IP 주소 범위를 할당할 수 있게 됩니다. 회수를 적용하려면 프로파일을 저장해야 합니다. 주소는 즉시 회수되지 않으므로 상태 열이 [만료됨] 또는 [제거됨]에서 [할당됨]로 바로 변경되지 않습니다.

7 확인을 클릭합니다.

타사 IPAM 끝점을 사용하여 NAT 네트워크 프로파일 생성

외부 네트워크 프로파일과 관련하여 요청 시 NSX NAT 네트워크 프로파일을 생성할 수 있습니다. 타사 IPAM 끝점이 포함된 NSX NAT 네트워크 프로파일을 사용 중인 경우 타사 IPAM 제공자가 IP 공간을 생성하고 관리합니다.

NAT 네트워크 프로파일에 타사 IPAM 끝점을 사용하면 해당 제공자가 요청 시 네트워크의 각 인스턴스에 대해 새 IP 범위를 만듭니다. 하나 이상의 범위로 정의된 내부 IP 주소 집합은 NAT 네트워크의 모든 인스턴스에 대해 타사 IPAM 제공자 끝점에 생성됩니다. 이러한 IP 범위는 동일한 배포에서 NAT 네트워크에 할당된 시스템에 IP 주소를 할당하는 데 사용됩니다. 단일 주소 공간 내에 중복된 IP 주소가 정의될 수 없으므로 NAT 네트워크의 각 인스턴스에 대해 제공자가 새 주소 공간을 생성합니다. NAT 네트워크가 삭제된 경우 IPAM 제공자 끝점 및 새 주소 공간에서 해당 네트워크의 범위가 삭제됩니다.

제공된 VMware IPAM 끝점 또는 Infoblox IPAM과 같은 vRealize Orchestrator에서 등록하고 구성한 타사 IPAM 서비스 제공자 끝점에서 가져온 IP 범위를 사용할 수 있습니다. IP 범위는 할당 중에 IP 블록에서 생성됩니다.

NAT 일대다 네트워크의 경우 Blueprint에 NAT 네트워크 구성 요소를 추가할 때 구성할 수 있고 배포에서 NAT 네트워크를 편집할 때 변경할 수 있는 NAT 규칙을 정의할 수 있습니다.

프로시저

1 타사 IPAM 끝점을 사용하는 NAT 네트워크 프로파일 정보 지정

네트워크 프로파일 정보는 NAT 네트워크 속성, 해당하는 기본 외부 네트워크 프로파일 및 타사 IPAM 끝점 사용 시 네트워크 프로비저닝에 사용되는 기타 값을 식별합니다.

2 타사 IPAM 끝점으로 NAT 네트워크 프로파일 IP 범위 구성

NAT를 사용하여 네트워크를 프로비저닝하는 데 사용하기 위한 하나 이상의 IP 주소 범위를 정의할 수 있습니다.

타사 IPAM 끝점을 사용하는 NAT 네트워크 프로파일 정보 지정

네트워크 프로파일 정보는 NAT 네트워크 속성, 해당하는 기본 외부 네트워크 프로파일 및 타사 IPAM 끝점 사용 시 네트워크 프로비저닝에 사용되는 기타 값을 식별합니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 외부 네트워크 프로파일을 생성합니다. **제공된 IPAM 끝점을 사용하여 외부 네트워크 프로파일 생성** 또는 **타사 IPAM 제공자를 사용하여 외부 네트워크 프로파일 생성** 항목을 참조하십시오.

- 타사 IPAM 끝점을 생성하고 구성합니다. [타사 IPAM 제공자 끝점 생성](#) 항목을 참조하십시오.

프로시저

- 1 **인프라 > 예약 > 네트워크 프로파일**을 선택합니다.
- 2 **새로 만들기**를 클릭하고 드롭다운 메뉴에서 **NAT**를 선택합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 4 하나 이상의 타사 IPAM 제공자 끝점을 구성한 경우 **IPAM 끝점** 드롭다운 메뉴에서 타사 IPAM 끝점을 선택합니다.

vRealize Orchestrator에서 등록한 타사 IPAM 제공자 끝점을 선택하면 지정된 IPAM 서비스 제공자로부터 IP 주소를 가져옵니다. 서브넷 마스크와 같은 IP 규격 및 DNS/WINS 옵션은 해당 기능이 선택된 타사 IPAM 끝점에 의해 제어되기 때문에 사용할 수 없습니다.

- 5 **외부 네트워크 프로파일** 드롭다운 메뉴에서 기존 외부 네트워크 프로파일을 선택합니다.

지정된 IPAM 끝점을 사용하도록 구성된 외부 네트워크 프로파일만 나열되고 선택할 수 있습니다.

- 6 **NAT 유형** 드롭다운 메뉴에서 일대일 또는 일대다 네트워크 주소 변환 유형을 선택합니다.

옵션	설명
일대일	<p>각 네트워크 어댑터에 외부 정적 IP 주소를 할당합니다. 각 시스템이 외부 네트워크에 액세스할 수 있으며, 외부 네트워크에서도 각 시스템에 액세스할 수 있습니다.</p> <p>NSX Edge 업링크에 할당된 모든 외부 IP 주소는 동일한 서브넷의 일부여야 합니다. vRealize Automation에서 NAT 1:1을 사용할 때, 해당하는 외부 네트워크 프로파일에는 단일 서브넷 내에 존재하는 IP 범위만 포함되어야 합니다.</p>
일대다	<p>네트워크의 모든 시스템이 외부 IP 주소 하나를 공유합니다. 내부 시스템에서는 정적 IP 주소만 사용할 수 있습니다. 모든 시스템에서 외부 네트워크에 액세스할 수 있지만 외부 네트워크에서는 그 어떤 시스템에도 액세스할 수 없습니다.</p> <p>타사 IPAM 제공자와 함께 NAT를 사용할 때 DHCP는 지원되지 않습니다.</p> <p>NAT 일대다 변환 유형을 사용하면 NAT 네트워크 구성 요소를 Blueprint에 추가할 때 NAT 규칙을 정의할 수 있습니다.</p>

- 7 **서브넷 마스크** 텍스트 상자에 IP 서브넷 마스크를 입력합니다.

서브넷 마스크는 네트워크 프로파일에 대해 정의할 라우팅 가능한 전체 주소 공간의 크기를 지정합니다.

예를 들어 255.255.0.0을 입력합니다.

- 8 **게이트웨이** 텍스트 상자에 Edge 또는 라우팅된 게이트웨이 주소를 입력합니다.

표준 IPv4 주소 형식을 사용하십시오. 예를 들어 10.10.110.1을 입력합니다.

네트워크 프로파일에 정의된 게이트웨이 IP 주소는 할당 중에 NIC에 할당됩니다. 네트워크 프로파일의 **게이트웨이** 텍스트 상자에 아무 값도 할당되지 않은 경우 Edge 시스템을 프로비저닝 할 때 VirtualMachine.Network0.Gateway 사용자 지정 속성을 사용해야 합니다.

- 9 **DNS** 탭을 클릭합니다.

10 필요한 경우 DNS 및 WINS 값을 입력합니다.

DNS 값은 DNS 이름 등록 및 확인을 위해 사용됩니다. 내부 IPAM 끝점을 사용하고 있으면 DNS 및 WINS 필드는 선택 사항입니다. 외부 IPAM 끝점을 사용하고 있으면 DNS 및 WINS 값은 타사 IPAM 제공자에 의해 제공됩니다.

- a (선택 사항) **기본 DNS** 서버 값을 입력합니다.
- b (선택 사항) **보조 DNS** 서버 값을 입력합니다.
- c (선택 사항) **DNS 접미사** 값을 입력합니다.
- d (선택 사항) **DNS 검색 접미사** 값을 입력합니다.
- e (선택 사항) **기본 설정 WINS** 서버 값을 입력합니다.
- f (선택 사항) **대체 WINS** 서버 값을 입력합니다.

후속 작업

타사 IPAM 끝점으로 NAT 네트워크 프로파일 IP 범위 구성.

타사 IPAM 끝점으로 NAT 네트워크 프로파일 IP 범위 구성

NAT를 사용하여 네트워크를 프로비저닝하는 데 사용하기 위한 하나 이상의 IP 주소 범위를 정의할 수 있습니다.

필수 조건

타사 IPAM 끝점을 사용하는 NAT 네트워크 프로파일 정보 지정.

프로시저**1 네트워크 범위** 탭을 클릭하여 새 네트워크 범위를 생성하거나 기존 네트워크 범위를 선택합니다.

각 이름, 설명, 시작 IP 주소 및 끝 IP 주소와 같은 선택한 범위에 대한 세부 정보가 나타납니다. 상태 관련 정보도 제공됩니다.

2 새로 만들기를 클릭하여 새 네트워크 범위 이름과 IP 주소 범위를 수동으로 입력하거나 **CSV에서 가져오기**를 클릭하여 올바른 형식의 CSV 파일에서 IP 주소 정보를 가져옵니다.■ **새로 만들기**를 클릭합니다.

- a 네트워크 범위 이름을 입력합니다.
- b 네트워크 범위에 대한 설명을 입력합니다.
- c 범위의 시작 IP 주소를 입력합니다.
- d 범위의 끝 IP 주소를 입력합니다.

■ **CSV에서 가져오기**를 클릭합니다.

- a CSV 파일을 찾아 선택하거나 **CSV에서 가져오기** 대화상자에서 CSV 파일을 끌어옵니다.

CSV 파일의 행은 ip_address, machine_name, status, NIC_offset 형식입니다.

예:

```
100.10.100.1,mymachine01,Allocated
```

CSV 필드	설명
ip_address	IPv4 형식의 IP 주소입니다.
machine_name	vRealize Automation의 관리되는 시스템 이름입니다. 이 필드가 비어 있으면 기본적으로 이름이 없습니다. 이 필드가 비어 있으면 status 필드 값이 Allocated일 수 없습니다.
status	Allocated 또는 Unallocated이며, 대/소문자를 구분합니다. 필드가 비어 있으면 기본값은 Unallocated입니다. status가 Allocated이면 machine_name 필드를 비워둘 수 없습니다.
NIC_offset	음수가 아닌 정수입니다. 선택 사항입니다.

b 적용을 클릭합니다.

3 확인을 클릭합니다.

IP 범위 이름이 정의된 범위 목록에 나타납니다. 범위 내의 IP 주소가 정의된 IP 주소 목록에 나타납니다.

적용을 클릭하거나 저장하고 네트워크 프로파일을 편집하고 나면 업로드된 IP 주소가 **IP 주소** 페이지에 나타납니다.

4 IP 주소 탭을 클릭하여 명명된 네트워크 범위의 IP 주소를 표시합니다.

5 (선택 사항) 네트워크 범위 드롭다운 메뉴에서 IP 주소 정보를 선택하여 IP 주소 항목을 필터링합니다.

모든 정의된 네트워크 범위, CSV 파일에서 가져온 네트워크 범위 또는 명명된 네트워크 범위에 대한 정보를 표시할 수 있습니다. 세부 정보에는 시작 IP 주소, 시스템 이름, 마지막 수정 날짜 및 타임 스탬프, IP 상태가 있습니다.

6 (선택 사항) IP 상태 드롭다운 메뉴에서 상태 유형을 선택하여 IP 주소 항목을 선택한 IP 상태와 일치하는 항목으로만 필터링합니다. 상태 설정은 [할당됨], [할당 취소됨], [제거됨] 및 [만료됨]입니다.

IP 주소가 만료되거나 삭제된 상태인 경우, 회수를 클릭하면 해당 IP 주소 범위를 할당할 수 있게 됩니다. 회수를 적용하려면 프로파일을 저장해야 합니다. 주소는 즉시 회수되지 않으므로 상태 열이 [만료됨] 또는 [제거됨]에서 [할당됨]로 바로 변경되지 않습니다.

7 확인을 클릭합니다.

프로비저닝된 시스템을 제거하여 IP 주소 해제

배포를 제거하면 해당 IP 주소가 삭제됩니다. 네트워크 프로파일 범위의 IPS 같이, 할당된 IP는 이후 프로비저닝에 사용할 수 있도록 해제됩니다.

정적 IP 주소를 사용하는 시스템을 제거하면 다른 시스템이 해당 IP 주소를 사용할 수 있게 됩니다. 정적 IP 주소를 회수하는 프로세스가 30분마다 실행되기 때문에 사용되지 않는 주소를 즉시 사용하지 못할 수 있습니다.

타사 IPAM 제공자를 사용하는 경우 vRealize Automation이 타사 IPAM 제공자 플러그인 또는 패키지에서 vRealize Orchestrator 워크플로를 사용하여 연결된 IP 주소를 삭제합니다.

예약 및 예약 정책 구성

vRealize Automation 예약은 프로비저닝 요청에 대한 시스템 배치를 결정하는 정책, 우선 순위 및 할당량을 정의할 수 있습니다.

예약 정책은 시스템 프로비저닝을 사용 가능한 일부 예약으로 제한합니다. Blueprint 설계자는 스토리지 예약 정책을 사용하여 시스템 볼륨을 여러 데이터 스토어에 할당할 수 있습니다.

성공적인 프로비저닝을 위해서는 예약에 사용 가능한 스토리지가 충분해야 합니다. 예약의 스토리지 가용성은 다음에 따라 달라집니다.

- 데이터스토어/클러스터에서 사용할 수 있는 스토리지의 양
- 해당 데이터스토어/클러스터에 예약된 해당 스토리지의 양
- vRealize Automation에 이미 할당되어 있는 해당 스토리지의 양

예를 들어 vCenter Server에 데이터스토어/클러스터에 사용할 수 있는 스토리지가 있는 경우에도 예약에 충분한 스토리지가 예약되지 않으면 프로비저닝이 실패하면서 "할당에 사용할 예약이 없음..." 오류가 표시됩니다. 예약에 할당된 스토리지는 해당 예약에 대한 VM(상태에 관계없음)의 수에 따라 다릅니다. 자세한 내용은 VMware 기술 자료 문서 시스템 XXX: 그룹 XXX 내에 할당에 사용할 예약이 없음. 총 XXGB의 스토리지가 요청됨(2151030)(<http://kb.vmware.com/kb/2151030>)을 참조하십시오.

예약

vRealize Automation 예약을 생성하여 패브릭 그룹의 프로비저닝 리소스를 특정 비즈니스 그룹에 할당할 수 있습니다.

예를 들어 예약을 사용하여 메모리 공유, CPU, 네트워킹 및 단일 계산 리소스의 스토리지 리소스가 특정 비즈니스 그룹에 속하도록 지정하거나 특정 시스템이 특정 비즈니스 그룹에 할당되도록 지정할 수 있습니다.

참고 예약에 의해 프로비저닝된 시스템에 할당된 스토리지와 메모리는 해당 시스템이 vRealize Automation에서 [제거] 작업에 의해 삭제될 때 해제됩니다. 시스템이 vCenter Server에서 삭제되는 경우에는 스토리지와 메모리가 해제되지 않습니다.

다음 시스템 유형에 대한 예약을 생성할 수 있습니다.

- vSphere
- vCloud Air
- vCloud Director
- Amazon EC2
- Azure
- Hyper V(SCVMM)
- Hyper-V 독립형
- KVM(RHEV)

- OpenStack
- XenServer

예약, Blueprint 또는 게스트 에이전트 스크립트에 정보를 지정하여 가상 시스템에 대한 보안 설정이 프로비저닝되도록 구성할 수 있습니다. 프로비저닝될 시스템에 게스트 에이전트가 필요한 경우 예약 또는 Blueprint에 대한 요구 사항을 포함하는 보안 규칙을 추가해야 합니다. 예를 들어, 모든 시스템 간의 통신을 거부하는 기본 보안 정책을 사용하고 별도의 보안 정책에 의존하여 특정 시스템 간의 통신을 허용하는 경우 게스트 에이전트는 사용자 지정 단계 중 vRealize Automation과 통신하지 못할 수 있습니다. 시스템 프로비저닝 중에 이러한 문제를 피하려면 사용자 지정 단계 중 통신을 허용하는 기본 보안 정책을 사용합니다.

예약 선택 시나리오

비즈니스 그룹에 리소스를 할당하기 위한 예약을 생성할 수 있습니다. 시나리오에 따라 예약을 생성하는 절차가 다릅니다.

대상 끝점 유형에 따라 예약 시나리오를 선택합니다.

각 비즈니스 그룹에는 해당 유형의 시스템을 프로비저닝하기 위해 해당 구성원에 대한 예약이 하나 이상 있어야 합니다. 예를 들어 OpenStack 예약은 있지만 Amazon 예약이 없는 비즈니스 그룹은 Amazon에서 시스템을 요청할 수 없습니다. 이 예에서는 비즈니스 그룹에 Amazon 리소스에 대한 예약을 명시적으로 할당해야 합니다.

표 2-15. 예약 선택 시나리오

시나리오	절차
vSphere 예약을 생성합니다.	Hyper-V, KVM, SCVMM, vSphere 또는 XenServer에 대한 예약 생성
vCloud Air 끝점에 대한 리소스를 할당하기 위한 예약을 생성합니다.	vCloud Air 예약 생성
vCloud Director 끝점에 대한 리소스를 할당하기 위한 예약을 생성합니다.	vCloud Director 예약 생성
Amazon 리소스에서 리소스를 할당하기 위한 예약을 생성합니다(Amazon Virtual Private Cloud 사용 또는 사용 안 함).	Amazon EC2 예약 생성
OpenStack 리소스에서 리소스를 할당하기 위한 예약을 생성합니다.	OpenStack 예약 생성
Hyper-V에 대한 리소스를 할당하기 위한 예약을 생성합니다.	Hyper-V, KVM, SCVMM, vSphere 또는 XenServer에 대한 예약 생성
KVM에 대한 리소스를 할당하기 위한 예약을 생성합니다.	Hyper-V, KVM, SCVMM, vSphere 또는 XenServer에 대한 예약 생성
OpenStack에서 리소스를 할당하기 위한 예약을 생성합니다. 리소스.	OpenStack 예약 생성
SCVMM에 대한 리소스를 할당하기 위한 예약을 생성합니다.	Hyper-V, KVM, SCVMM, vSphere 또는 XenServer에 대한 예약 생성

표 2-15. 예약 선택 시나리오 (계속)

시나리오	절차
XenServer에 대한 리소스를 할당하기 위한 예약을 생성합니다.	Hyper-V, KVM, SCVMM, vSphere 또는 XenServer에 대한 예약 생성
Microsoft Azure에 대한 리소스를 할당하기 위한 예약을 생성합니다.	Microsoft Azure를 위한 예약 생성

클라우드 범주 예약 생성

클라우드 범주 유형 예약은 특정 vRealize Automation 비즈니스 그룹에 대해 클라우드 서비스 계정의 프로비저닝 서비스에 대한 액세스를 제공합니다. 사용 가능한 클라우드 예약 유형에는 Amazon, OpenStack, vCloud Air 및 vCloud Director가 있습니다.

예약은 특정 vRealize Automation 비즈니스 그룹에 할당된 계산 리소스 하나의 메모리, CPU, 네트워크 및 스토리지 리소스를 공유하는 것입니다.

비즈니스 그룹은 하나의 끝점 또는 여러 끝점에서 여러 개의 예약을 사용할 수 있습니다.

예약의 할당 모델은 연결된 데이터 센터의 할당 모델에 따라 달라집니다. 사용 가능한 할당 모델에는 할당 풀, 용량제 및 예약 풀이 있습니다. 할당 모델에 대한 자세한 내용은 vCloud Director 또는 vCloud Air 설명서를 참조하십시오.

비즈니스 그룹에 할당된 패브릭 리소스의 공유를 정의하는 것 외에, 예약은 정책, 우선 순위 그리고 시스템 배치를 결정하는 할당량을 정의할 수 있습니다.

성공적인 프로비저닝을 위해서는 예약에 사용 가능한 스토리지가 충분해야 합니다. 예약의 스토리지 가용성은 다음에 따라 달라집니다.

- 데이터스토어/클러스터에서 사용할 수 있는 스토리지의 양
- 해당 데이터스토어/클러스터에 예약된 해당 스토리지의 양
- vRealize Automation에 이미 할당되어 있는 해당 스토리지의 양

예를 들어 vCenter Server에 데이터스토어/클러스터에 사용할 수 있는 스토리지가 있는 경우에도 예약에 충분한 스토리지가 예약되지 않으면 프로비저닝이 실패하면서 "할당에 사용할 예약이 없음..." 오류가 표시됩니다. 예약에 할당된 스토리지는 해당 예약에 대한 VM(상태에 관계없음)의 수에 따라 다릅니다. 자세한 내용은 VMware 기술 자료 문서 시스템 XXX: 그룹 XXX 내에 할당에 사용할 예약이 없음. 총 XXGB의 스토리지가 요청됨(2151030)(<http://kb.vmware.com/kb/2151030>)을 참조하십시오.

클라우드 예약의 선택 논리 이해

비즈니스 그룹의 구성원이 클라우드 시스템에 대한 프로비저닝 요청을 생성하면

vRealize Automation은 해당 비즈니스 그룹이 사용할 수 있는 예약 중 하나에서 시스템을 선택합니다. 클라우드 예약에는 Amazon, OpenStack, vCloud Air 및 vCloud Director가 포함됩니다.

시스템이 프로비저닝되는 예약은 다음과 같은 기준을 충족해야 합니다.

- 예약은 시스템이 요청된 Blueprint와 플랫폼 유형이 동일해야 합니다.
- 예약은 사용할 수 있게 설정되어 있어야 합니다.

- 예약은 해당 시스템 할당량에 용량이 남아 있거나, 할당량에 제한이 없어야 합니다.

할당된 시스템 할당량에는 전원이 켜진 시스템만 포함됩니다. 예를 들어 예약의 할당량이 50인 경우, 40대의 시스템이 프로비저닝되었지만 그 중 20대만 전원이 켜져 있으면 예약의 할당량은 80%가 아니라 40%만 할당된 것입니다.

- 예약에는 시스템 요청에 지정된 보안 그룹이 있어야 합니다.
- 예약은 Blueprint에 지정된 시스템 이미지를 가진 영역과 연결되어 있어야 합니다.
- 예약에는 시스템을 프로비저닝하는 데 충분한 할당되지 않은 메모리와 스토리지 리소스가 있어야 합니다.

용량제 예약의 경우에는 리소스에 제한이 없을 수 있습니다.

- Amazon 시스템의 경우, 요청은 사용 가능한 영역을 지정하고, 시스템에 VPC(Virtual Private Cloud)의 서브넷을 프로비저닝할지 아니면 VPC가 아닌 위치의 서브넷을 프로비저닝할지 지정합니다. 예약은 네트워크 유형(VPC 또는 VPC 이외)과 일치해야 합니다.
- vCloud Air 또는 vCloud Director의 경우, 요청에 할당 모델이 지정된 경우 예약에 연결된 가상 데이터 센터도 동일한 할당 모델을 사용해야 합니다.
- vCloud Director 또는 vCloud Air의 경우 지정된 조직이 사용할 수 있게 설정되어 있어야 합니다.
- 모든 Blueprint 템플릿을 예약에서 사용할 수 있어야 합니다. 예약 정책이 두 개 이상의 리소스에 매핑되는 경우 템플릿이 공용 템플릿이어야 합니다.
- 클라우드 제공자가 네트워크 선택 기능을 지원하고 Blueprint에 특정 네트워크 설정이 지정되어 있는 경우 예약은 동일한 네트워크를 가지고 있어야 합니다.

Blueprint 또는 예약에 정적 IP 주소 할당을 위한 네트워크 프로파일 지정된 경우, 새 시스템을 할당할 IP 주소를 사용할 수 있어야 합니다.

- 요청에 할당 모델이 지정된 경우, 예약에 지정된 할당 모델은 요청에 지정된 할당 모델과 일치해야 합니다.
- Blueprint에 예약 정책이 지정된 경우, 예약은 해당 예약 정책에 속해 있어야 합니다.

예약 정책은 선택한 예약이 특정 Blueprint에서 시스템을 프로비저닝하기 위한 모든 추가적인 요구 사항을 충족하는지 보장하는 방식입니다. 예를 들어 Blueprint에서 특정 시스템 이미지를 사용하는 경우, 예약 정책을 사용하면 필요한 이미지를 가진 영역과 연결된 예약만 사용하도록 프로비저닝을 제한할 수 있습니다.

선택한 모든 기준을 모두 충족하는 예약이 없으면 프로비저닝이 실패합니다.

모든 기준을 충족하는 예약이 여러 개 있는 경우에는 요청된 시스템을 프로비저닝하는 데 사용할 예약이 다음과 같은 논리에 따라 결정됩니다.

- 우선 순위 값이 낮은 예약이 우선 순위 값이 높은 예약보다 먼저 선택됩니다.
- 여러 예약의 우선 순위가 동일한 경우, 할당된 시스템 할당량의 비율이 가장 낮은 예약이 선택됩니다.

- 여러 예약의 우선 순위 및 할당량 사용량이 동일한 경우, 라운드 로빈 방식으로 예약 간에 시스템이 분산됩니다.

참고 네트워크 프로파일의 라운드 로빈 선택은 지원되지 않지만 네트워크(있는 경우)의 라운드 로빈 선택은 지원되므로 이를 서로 다른 네트워크 프로파일과 연결할 수 있습니다.

시스템 볼륨을 프로비저닝하는 데 충분한 용량을 가진 스토리지 경로 여러 개를 예약에서 사용할 수 있는 경우에는 다음과 같은 논리에 따라 스토리지 경로가 선택됩니다.

- 우선 순위 값이 낮은 스토리지 경로가 우선 순위 값이 높은 스토리지 경로보다 먼저 선택됩니다.
- Blueprint 또는 요청에 스토리지 예약 정책이 지정된 경우, 스토리지 경로는 해당 스토리지 예약 정책에 속해 있어야 합니다.

사용자 지정 속성 `VirtualMachine.DiskN.StorageReservationPolicyMode`이 Not Exact로 설정되어 있고, 스토리지 용량이 충분하고 사용 가능한 스토리지 경로가 스토리지 예약 정책에 없는 경우에는 지정된 스토리지 예약 정책 외부에 있는 스토리지 경로를 사용하여 프로비저닝이 진행됩니다. `VirtualMachine.DiskN.StorageReservationPolicyMode`의 기본값은 Exact입니다.

- 여러 스토리지 경로의 우선 순위가 동일한 경우, 라운드 로빈 예약을 사용하여 스토리지 경로 간에 시스템이 분산됩니다.

Amazon EC2 예약 생성

비즈니스 그룹의 구성원이 시스템 프로비저닝을 요청할 수 있으려면 우선 예약을 생성하여 시스템에 리소스를 할당해야 합니다.

Amazon Virtual Private Cloud 또는 Amazon 비VPC의 Amazon 예약에 대해 작업을 수행할 수 있습니다. Amazon Web Services 사용자는 Amazon Virtual Private Cloud를 생성하여 해당 규격에 따라 가상 네트워크 토폴로지를 설계할 수 있습니다. Amazon VPC를 사용할 계획인 경우 Amazon VPC를 vRealize Automation 예약에 할당해야 합니다. 항목을 참조하십시오.

Amazon 예약을 생성하거나 Blueprint에 시스템 구성 요소를 구성할 경우, 지정된 Amazon 영역에 사용 가능한 보안 그룹 목록 중에서 선택할 수 있습니다. 보안 그룹 가져오기는 데이터를 수집하는 동안 수행됩니다.

참고 예약을 생성한 이후에는 비즈니스 그룹 또는 계산 리소스 연결을 변경할 수 없습니다.

AWS Management Console을 사용한 Amazon VPC 생성에 대한 자세한 내용은 Amazon Web Services 설명서를 참조하십시오.

프로시저

1 Amazon 예약 정보 지정

각 예약은 지정된 계산 리소스의 시스템 요청을 위한 액세스 권한을 부여하도록 특정 비즈니스 그룹에 대해 구성되어 있습니다.

2 Amazon 예약을 위한 리소스 및 네트워크 설정 지정

이 vRealize Automation 예약으로부터 시스템을 프로비저닝하기 위한 리소스 및 네트워크 설정을 지정합니다.

3 Amazon 예약을 위한 사용자 지정 속성 및 경고 지정

사용자 지정 속성을 vRealize Automation 예약에 연결할 수 있습니다. 또한 예약 리소스가 부족한 경우 이메일 알림을 보내도록 경고를 구성할 수도 있습니다.

Amazon 예약 정보 지정

각 예약은 지정된 계산 리소스의 시스템 요청을 위한 액세스 권한을 부여하도록 특정 비즈니스 그룹에 대해 구성되어 있습니다.


참고 예약을 생성한 이후에는 비즈니스 그룹 또는 계산 리소스 연결을 변경할 수 없습니다.

[예약] 페이지에서 **범주별 필터링** 옵션을 사용하면 추가, 편집 또는 삭제 시 예약의 표시 여부를 제어할 수 있습니다. 테스트 에이전트 예약은 범주별로 필터링할 때 예약 목록에 나타나지 않습니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 테넌트 관리자가 비즈니스 그룹을 하나 이상 생성했는지 확인합니다.
- 계산 리소스가 있는지 확인합니다.
- 네트워크 설정을 구성합니다.
- (선택 사항) 네트워크 프로필 정보를 구성합니다.
- 원하는 Amazon 네트워크에 대한 액세스 권한이 있는지 확인합니다. 예를 들어 VPC를 사용하려는 경우 Amazon VPC(Virtual Private Cloud) 네트워크에 대한 액세스 권한이 있는지 확인합니다.
- 필수 키 쌍이 있는지 확인합니다. [키 쌍 관리](#) 항목을 참조하십시오.

프로시저

- 1 **인프라 > 예약 > 예약**을 선택합니다.
- 2 **새로 만들기** 아이콘()을 클릭하고, 생성할 예약 유형을 선택합니다.
Amazon EC2를 선택합니다.
- 3 (선택 사항) **기존 예약에서 복사** 드롭다운 메뉴에서 기존 예약을 선택합니다.
선택한 예약의 데이터가 표시됩니다. 필요에 따라 새 예약을 변경할 수 있습니다.
- 4 **이름** 텍스트 상자에 이름을 입력합니다.
- 5 **테넌트** 드롭다운 메뉴에서 테넌트를 선택합니다.
- 6 **비즈니스 그룹** 드롭다운 메뉴에서 비즈니스 그룹을 선택합니다.
이 비즈니스 그룹에 속해 있는 사용자만 이 예약을 사용하여 시스템을 프로비저닝할 수 있습니다.
- 7 (선택 사항) **예약 정책** 드롭다운 메뉴에서 예약 정책을 선택합니다.
이 옵션은 예약 정책이 하나 이상 있어야 사용할 수 있습니다 나중에 예약을 편집하여 예약 정책을 지정할 수 있습니다.
예약 정책은 특정 예약을 대상으로만 프로비저닝을 제한하는 데 사용됩니다.

8 우선 순위 텍스트 상자에 숫자를 입력하여 예약의 우선 순위를 설정합니다.

우선 순위는 비즈니스 그룹에 예약이 두 개 이상 있는 경우에 사용됩니다. 우선 순위가 1인 예약은 우선 순위가 2인 예약보다 우선적으로 프로비저닝에 사용됩니다.

9 (선택 사항) 예약을 활성 상태로 유지하지 않으려면 **이 예약 사용** 확인란의 선택을 취소합니다.

이 페이지 밖으로 이동하지 마십시오. 예약이 아직 완료되지 않았습니다.

Amazon 예약을 위한 리소스 및 네트워크 설정 지정

이 vRealize Automation 예약으로부터 시스템을 프로비저닝하기 위한 리소스 및 네트워크 설정을 지정합니다.

Amazon 예약을 생성하거나 Blueprint에서 시스템 구성 요소를 구성할 때는 지정된 Amazon 계정 영역에 사용 가능한 보안 그룹 목록 중에서 선택할 수 있습니다. 보안 그룹 가져오기는 데이터를 수집하는 동안 수행됩니다. 보안 그룹은 방화벽처럼 작동하여 시스템에 대한 액세스를 제어합니다. 각 영역에는 기본 보안 그룹이 하나 이상 있습니다. 관리자는

Amazon Web Services Management Console을 사용하여 추가적인 보안 그룹을 생성하고, Microsoft Remote Desktop Protocol 또는 SSH에 대한 포트를 구성하고, Amazon VPN에 대한 가상 전용 네트워크를 설정합니다. Amazon Web Services에서 보안 그룹을 생성하고 사용하는 방법에 대한 자세한 내용은 Amazon 설명서를 참조하십시오.

로드 밸런서 관련 정보는 vRealize Automation 구성 항목을 참조하십시오.

필수 조건

[Amazon 예약 정보 지정.](#)

프로시저

1 리소스 탭을 클릭합니다.

2 시스템을 프로비저닝할 계산 리소스를 **계산 리소스** 드롭다운 메뉴에서 선택합니다.

사용 가능한 Amazon 영역이 나열되어 있습니다.

3 (선택 사항) **시스템 할당량** 텍스트 상자에 숫자를 입력하여 이 예약에 프로비저닝할 수 있는 시스템의 최대 개수를 설정합니다.

전원이 켜진 시스템만 이 할당량의 개수에 포함됩니다. 예약을 제한하지 않으려면 이 텍스트 상자를 비워 둡니다.

4 **키 쌍** 드롭다운 메뉴에서 계산 인스턴스에 키 쌍을 할당할 방법을 선택합니다.

옵션	설명
지정되지 않음	예약 수준이 아니라 Blueprint 수준에서 키 쌍의 동작을 제어합니다.
비즈니스 그룹별로 자동 생성됨	동일한 비즈니스 그룹에 프로비저닝된 모든 시스템이 동일한 키 쌍을 사용합니다. 시스템에서 동일한 계산 리소스와 비즈니스 그룹을 사용하는 경우, 다른 예약에 프로비저닝된 시스템도 여기에 포함됩니다. 이 방법으로 생성된 키 쌍은 비즈니스 그룹에 연결되기 때문에 비즈니스 그룹이 삭제되면 키 쌍도 함께 삭제됩니다.

옵션	설명
시스템별로 자동 생성됨	각 시스템에는 고유한 키 쌍이 있습니다. 시스템 사이에 키 쌍이 공유되지 않기 때문에 이 방법이 가장 안전합니다.
특정 키 쌍	이 예약에 프로비저닝된 모든 시스템이 동일한 키 쌍을 사용합니다. 이 예약에 사용할 키 쌍을 찾습니다.

- 키 쌍 드롭다운 메뉴에서 **특정 키 쌍**을 선택한 경우, **특정 키 쌍** 드롭다운 메뉴에서 키 쌍 값을 선택합니다.
- Amazon Virtual Private Cloud에 대해 구성된 경우 **VPC의 서브넷에 할당** 확인란을 선택합니다. 그렇지 않으면 확인란을 선택하지 않은 상태로 둡니다.

VPC의 서브넷에 할당을 선택한 경우, 다음 위치 또는 서브넷, 보안 그룹 및 로드 밸런서 옵션이 이 페이지가 아닌 팝업 메뉴에 나타납니다.

VPC 예약의 경우 예약에서 허용된 각 VPC에 대해 보안 그룹 및 서브넷을 지정합니다.

- 위치 또는 서브넷** 목록에서 사용 가능한 하나 이상의 위치(VPC 이외) 또는 서브넷(VPC)을 선택합니다.

프로비저닝에 사용하려는 사용 가능한 각 위치 또는 서브넷을 선택합니다.

- 프로비저닝하는 동안 시스템에 할당할 수 있는 보안 그룹을 **보안 그룹** 목록에서 하나 이상 선택합니다.

프로비저닝 중 시스템에 할당할 수 있는 각 보안 그룹을 선택합니다. 사용 가능한 각 영역에는 보안 그룹을 하나 이상 지정해야 합니다.

- 로드 밸런서** 목록에서 사용 가능한 로드 밸런서를 하나 이상 선택합니다.

Elastic Load Balancer 기능을 사용 중인 경우 선택한 위치 또는 서브넷에 적용되는 사용 가능한 하나 이상의 로드 밸런서를 선택합니다.

이제 **저장**을 클릭하여 예약을 저장할 수 있습니다. 또는 사용자 지정 속성을 추가하여 예약 규격을 더 세부적으로 제어할 수 있습니다. 이 예약에 할당된 리소스가 줄어들 경우 알림을 보내도록 이메일 경고를 구성할 수도 있습니다.

Amazon 예약을 위한 사용자 지정 속성 및 경고 지정

사용자 지정 속성을 vRealize Automation 예약에 연결할 수 있습니다. 또한 예약 리소스가 부족한 경우 이메일 알림을 보내도록 경고를 구성할 수도 있습니다.

사용자 지정 속성 및 이메일 경고는 예약에 사용할 수 있는 선택적인 구성입니다. 사용자 지정 속성을 연결하거나 경고를 설정하지 않으려면 **저장**을 클릭하여 예약 생성을 완료하십시오.

사용자 지정 속성은 필요한 만큼 추가할 수 있습니다.

경고를 구성한 경우, 경고는 지정한 임계값에 도달했을 때가 아니라 매일 생성됩니다.

중요 알림은 이메일 경고가 구성되고 알림을 사용하도록 설정한 경우에만 전송됩니다.

필수 조건

Amazon 예약을 위한 리소스 및 네트워크 설정 지정.

프로시저

- 1 속성 탭을 클릭합니다.
- 2 새로 만들기를 클릭합니다.
- 3 올바른 사용자 지정 속성 이름을 입력합니다.
- 4 해당하는 경우, 속성 값을 입력합니다.
- 5 저장을 클릭합니다.
- 6 (선택 사항) 추가적인 사용자 지정 속성을 모두 추가합니다.
- 7 경고 탭을 클릭합니다.
- 8 용량 경고 확인란을 사용하도록 설정하여, 전송할 경고를 구성합니다.
- 9 슬라이더를 이용하여 사용 가능한 리소스 할당의 임계값을 설정합니다.
- 10 경고 알림을 수신할 AD 사용자 또는 그룹 이름(이메일 주소 아님)을 받는 사람 텍스트 상자에 입력합니다.

각 줄에 하나씩 이름을 입력합니다. Enter 키를 눌러 여러 항목을 구분합니다.

- 11 이메일 경고에 그룹 관리자를 포함하려면 그룹 관리자에게 경고 보내기를 선택합니다.
이메일 경고가 비즈니스 그룹 관리자 이메일 수신인 목록에 포함된 사용자에게 전송됩니다.
- 12 미리 알림 빈도(일)를 지정합니다.
- 13 저장을 클릭합니다.

예약이 저장되고 [예약] 목록에 표시됩니다.

후속 작업

선택적인 예약 정책을 구성하거나 프로비저닝 준비를 시작할 수 있습니다.

Blueprint를 생성할 수 있는 권한을 가진 사용자는 이제 Blueprint를 생성할 수 있습니다.

OpenStack 예약 생성

비즈니스 그룹의 구성원이 시스템 프로비저닝을 요청할 수 있으려면 우선 예약을 생성하여 시스템에 리소스를 할당해야 합니다.

OpenStack 예약을 생성합니다.

프로시저

- 1 **OpenStack 예약 정보 지정**
각 예약은 지정된 계산 리소스의 시스템 요청을 위한 액세스 권한을 부여하도록 특정 비즈니스 그룹에 대해 구성되어 있습니다.
- 2 **OpenStack 예약을 위한 리소스 및 네트워크 설정 지정**
이 vRealize Automation 예약을 통해 프로비저닝되는 시스템에서 사용할 수 있는 리소스와 네트워크 설정을 지정합니다.

3 OpenStack 예약을 위한 사용자 지정 속성 및 경고 지정

사용자 지정 속성을 vRealize Automation 예약에 연결할 수 있습니다. 또한 예약 리소스가 부족한 경우 이메일 알림을 보내도록 경고를 구성할 수도 있습니다.

OpenStack 예약 정보 지정

각 예약은 지정된 계산 리소스의 시스템 요청을 위한 액세스 권한을 부여하도록 특정 비즈니스 그룹에 대해 구성되어 있습니다.


참고 예약을 생성한 이후에는 비즈니스 그룹 또는 계산 리소스 연결을 변경할 수 없습니다.

[예약] 페이지에서 **범주별 필터링** 옵션을 사용하면 추가, 편집 또는 삭제 시 예약의 표시 여부를 제어할 수 있습니다. 테스트 에이전트 예약은 범주별로 필터링할 때 예약 목록에 나타나지 않습니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 테넌트 관리자가 비즈니스 그룹을 하나 이상 생성했는지 확인합니다.
- 계산 리소스가 있는지 확인합니다.
- 선택적 보안 그룹 또는 부동 소수점 IP 주소가 구성되었는지 확인합니다.
- 필수 키 쌍이 있는지 확인합니다. [키 쌍 관리](#) 항목을 참조하십시오.
- 계산 리소스가 있는지 확인합니다.
- 네트워크 설정을 구성합니다.

프로시저

- 1 **인프라 > 예약 > 예약**을 선택합니다.
- 2 **새로 만들기** 아이콘()을 클릭하고, 생성할 예약 유형을 선택합니다.
OpenStack을 선택합니다.
- 3 (선택 사항) **기존 예약에서 복사** 드롭다운 메뉴에서 기존 예약을 선택합니다.
선택한 예약의 데이터가 표시됩니다. 필요에 따라 새 예약을 변경할 수 있습니다.
- 4 **이름** 텍스트 상자에 이름을 입력합니다.
- 5 **테넌트** 드롭다운 메뉴에서 테넌트를 선택합니다.
- 6 **비즈니스 그룹** 드롭다운 메뉴에서 비즈니스 그룹을 선택합니다.
이 비즈니스 그룹에 속해 있는 사용자만 이 예약을 사용하여 시스템을 프로비저닝할 수 있습니다.
- 7 (선택 사항) **예약 정책** 드롭다운 메뉴에서 예약 정책을 선택합니다.
이 옵션은 예약 정책이 하나 이상 있어야 사용할 수 있습니다 나중에 예약을 편집하여 예약 정책을 지정할 수 있습니다.
예약 정책은 특정 예약을 대상으로만 프로비저닝을 제한하는 데 사용됩니다.

8 우선 순위 텍스트 상자에 숫자를 입력하여 예약의 우선 순위를 설정합니다.

우선 순위는 비즈니스 그룹에 예약이 두 개 이상 있는 경우에 사용됩니다. 우선 순위가 1인 예약은 우선 순위가 2인 예약보다 우선적으로 프로비저닝에 사용됩니다.

9 (선택 사항) 예약을 활성 상태로 유지하지 않으려면 **이 예약 사용** 확인란의 선택을 취소합니다.

이 페이지 밖으로 이동하지 마십시오. 예약이 아직 완료되지 않았습니다.

OpenStack 예약을 위한 리소스 및 네트워크 설정 지정

이 vRealize Automation 예약을 통해 프로비저닝되는 시스템에서 사용할 수 있는 리소스와 네트워크 설정을 지정합니다.

필수 조건

[OpenStack 예약 정보 지정](#).

프로시저

1 리소스 탭을 클릭합니다.

2 시스템을 프로비저닝할 계산 리소스를 **계산 리소스** 드롭다운 메뉴에서 선택합니다.

선택한 클러스터에 위치해 있는 템플릿만 이 예약을 사용하는 복제 작업에 사용할 수 있습니다.

프로비저닝하는 동안 로컬 스토리지에 연결된 호스트에 시스템이 배치됩니다. 예약에서 로컬 스토리지를 사용하는 경우 예약에 의해 프로비저닝되는 모든 시스템은 해당 로컬 스토리지가 들어 있는 호스트에서 생성됩니다. 하지만 VirtualMachine.Admin.ForceHost 사용자 지정 속성을 사용하는 경우 시스템이 다른 호스트로 프로비저닝되도록 강제되고 프로비저닝이 실패합니다. 또한 시스템 복제에 사용된 템플릿이 로컬 스토리지에 있지만 다른 클러스터의 시스템에 연결되어 있는 경우에도 프로비저닝이 실패합니다. 이 경우 템플릿에 액세스할 수 없기 때문에 프로비저닝이 실패합니다.

3 (선택 사항) **시스템 할당량** 텍스트 상자에 숫자를 입력하여 이 예약에 프로비저닝할 수 있는 시스템의 최대 개수를 설정합니다.

전원이 켜진 시스템만 이 할당량의 개수에 포함됩니다. 예약을 제한하지 않으려면 이 텍스트 상자를 비워 둡니다.

4 키 쌍 드롭다운 메뉴에서 계산 인스턴스에 키 쌍을 할당할 방법을 선택합니다.

옵션	설명
지정되지 않음	예약 수준이 아니라 Blueprint 수준에서 키 쌍의 동작을 제어합니다.
비즈니스 그룹별로 자동 생성됨	동일한 비즈니스 그룹에 프로비저닝된 모든 시스템이 동일한 키 쌍을 사용합니다. 시스템에서 동일한 계산 리소스와 비즈니스 그룹을 사용하는 경우, 다른 예약에 프로비저닝된 시스템도 여기에 포함됩니다. 이 방법으로 생성된 키 쌍은 비즈니스 그룹에 연결되기 때문에 비즈니스 그룹이 삭제되면 키 쌍도 함께 삭제됩니다.
시스템별로 자동 생성됨	각 시스템에는 고유한 키 쌍이 있습니다. 시스템 사이에 키 쌍이 공유되지 않기 때문에 이 방법이 가장 안전합니다.
특정 키 쌍	이 예약에 프로비저닝된 모든 시스템이 동일한 키 쌍을 사용합니다. 이 예약에 사용할 키 쌍을 찾습니다.

- 5 **키 쌍** 드롭다운 메뉴에서 **특정 키 쌍**을 선택한 경우, **특정 키 쌍** 드롭다운 메뉴에서 키 쌍 값을 선택합니다.
- 6 프로비저닝하는 동안 시스템에 할당할 수 있는 보안 그룹을 **보안 그룹** 목록에서 하나 이상 선택합니다.
- 7 **네트워크** 탭을 클릭합니다.
- 8 이 예약을 사용하여 프로비저닝된 시스템의 네트워크 경로를 구성합니다.

- a (선택 사항) 해당 옵션을 사용할 수 있는 경우, **끝점** 드롭다운 메뉴에서 스토리지 끝점을 선택합니다.

NetApp ONTAP 끝점이 있고 호스트가 가상 호스트이면 끝점 옆에 FlexClone 옵션이 표시됩니다. NetApp ONTAP 끝점이 있으면 스토리지 경로에 할당된 끝점이 예약 페이지에 표시됩니다. 스토리지 경로의 끝점을 추가, 업데이트 또는 삭제하면 적용되는 모든 예약에 변경 내용이 표시됩니다.

스토리지 경로의 끝점을 추가, 업데이트 또는 삭제하면 예약 페이지에 변경 내용이 표시됩니다.

- b **네트워크 경로** 목록에서 이 예약을 사용하여 프로비저닝된 시스템의 네트워크 경로를 선택합니다.
- c (선택 사항) 나열된 네트워크 프로파일을 **네트워크 프로파일** 드롭다운 메뉴에서 선택합니다.

이 옵션은 네트워크 프로파일이 하나 이상 있어야 사용할 수 있습니다.

예약에 네트워크 경로를 두 개 이상 선택할 수 있지만 시스템을 프로비저닝할 때는 네트워크 한 개만 사용됩니다.

이제 **저장**을 클릭하여 예약을 저장할 수 있습니다. 또는 사용자 지정 속성을 추가하여 예약 규격을 더 세부적으로 제어할 수 있습니다. 이 예약에 할당된 리소스가 줄어들 경우 알림을 보내도록 이메일 경고를 구성할 수도 있습니다.

OpenStack 예약을 위한 사용자 지정 속성 및 경고 지정

사용자 지정 속성을 vRealize Automation 예약에 연결할 수 있습니다. 또한 예약 리소스가 부족한 경우 이메일 알림을 보내도록 경고를 구성할 수도 있습니다.

사용자 지정 속성 및 이메일 경고는 예약에 사용할 수 있는 선택적인 구성입니다. 사용자 지정 속성을 연결하거나 경고를 설정하지 않으려면 **저장**을 클릭하여 예약 생성을 완료하십시오.

사용자 지정 속성은 필요한 만큼 추가할 수 있습니다.

중요 알림은 이메일 경고가 구성되고 알림을 사용하도록 설정한 경우에만 전송됩니다.

경고를 구성한 경우, 경고는 지정한 임계값에 도달했을 때가 아니라 매일 생성됩니다.

필수 조건

OpenStack 예약을 위한 리소스 및 네트워크 설정 지정.

프로시저

- 1 **속성** 탭을 클릭합니다.

- 2 **새로 만들기**를 클릭합니다.
- 3 올바른 사용자 지정 속성 이름을 입력합니다.
- 4 해당하는 경우, 속성 값을 입력합니다.
- 5 **저장**을 클릭합니다.
- 6 (선택 사항) 추가적인 사용자 지정 속성을 모두 추가합니다.
- 7 **경고** 탭을 클릭합니다.
- 8 **용량 경고** 확인란을 사용하도록 설정하여, 전송할 경고를 구성합니다.
- 9 슬라이더를 이용하여 사용 가능한 리소스 할당의 임계값을 설정합니다.
- 10 경고 알림을 수신할 AD 사용자 또는 그룹 이름(이메일 주소 아님)을 **받는 사람** 텍스트 상자에 입력합니다.
 각 줄에 하나씩 이름을 입력합니다. Enter 키를 눌러 여러 항목을 구분합니다.
- 11 이메일 경고에 그룹 관리자를 포함하려면 **그룹 관리자에게 경고 보내기**를 선택합니다.
 이메일 경고가 비즈니스 그룹 **관리자 이메일 수신인** 목록에 포함된 사용자에게 전송됩니다.
- 12 미리 알림 빈도(일)를 지정합니다.
- 13 **저장**을 클릭합니다.

예약이 저장되고 [예약] 목록에 표시됩니다.

후속 작업

선택적인 예약 정책을 구성하거나 프로비저닝 준비를 시작할 수 있습니다.

Blueprint를 생성할 수 있는 권한을 가진 사용자는 이제 Blueprint를 생성할 수 있습니다.

vCloud Air 예약 생성

비즈니스 그룹의 구성원이 시스템 프로비저닝을 요청할 수 있으려면 우선 vRealize Automation 예약을 생성하여 시스템에 리소스를 할당해야 합니다.

각 비즈니스 그룹에는 해당 유형의 시스템을 프로비저닝하기 위해 해당 구성원에 대한 예약이 하나 이상 있어야 합니다.

프로시저

1 vCloud Air 예약 정보 지정

각 vCloud Air 시스템 구독 또는 OnDemand 리소스에 대해 예약을 생성할 수 있습니다. 각 예약은 시스템 요청을 위한 액세스 권한 부여를 위해 특정 비즈니스 그룹에 대해 구성되어 있습니다.

2 vCloud Air 예약을 위한 리소스 및 네트워크 설정 지정

이 vRealize Automation 예약을 통해 프로비저닝되는 vCloud Air 시스템에서 사용할 수 있는 리소스와 네트워크 설정을 지정합니다.

3 vCloud Air 예약을 위한 사용자 지정 속성 및 경고 지정

사용자 지정 속성을 vRealize Automation 예약에 연결할 수 있습니다. 또한 예약 리소스가 부족한 경우 이메일 알림을 보내도록 경고를 구성할 수도 있습니다.

후속 작업

선택적인 예약 정책을 구성하거나 프로비저닝 준비를 시작할 수 있습니다.

Blueprint를 생성할 수 있는 권한을 가진 사용자는 이제 Blueprint를 생성할 수 있습니다.

vCloud Air 예약 정보 지정

각 vCloud Air 시스템 구독 또는 OnDemand 리소스에 대해 예약을 생성할 수 있습니다. 각 예약은 시스템 요청을 위한 액세스 권한 부여를 위해 특정 비즈니스 그룹에 대해 구성되어 있습니다.

[예약] 페이지에서 **범주별 필터링** 옵션을 사용하면 추가, 편집 또는 삭제 시 예약의 표시 여부를 제어할 수 있습니다. 테스트 에이전트 예약은 범주별로 필터링할 때 예약 목록에 나타나지 않습니다.

참고 예약을 생성한 이후에는 비즈니스 그룹 또는 계산 리소스 연결을 변경할 수 없습니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 테넌트 관리자가 비즈니스 그룹을 하나 이상 생성했는지 확인합니다.
- 계산 리소스가 있는지 확인합니다.
- 네트워크 설정을 구성합니다.
- (선택 사항) 네트워크 프로파일 정보를 구성합니다.

프로시저

1 **인프라 > 예약 > 예약**을 선택합니다.

2 **새로 만들기** 아이콘(+)을 클릭하고, 생성할 예약 유형을 선택합니다.

사용할 수 있는 클라우드 예약 유형은 Amazon, OpenStack, vCloud Air 및 vCloud Director입니다.

vCloud Air를 선택합니다.

3 (선택 사항) **기존 예약에서 복사** 드롭다운 메뉴에서 기존 예약을 선택합니다.

선택한 예약의 데이터가 표시됩니다. 필요에 따라 새 예약을 변경할 수 있습니다.

4 **이름** 텍스트 상자에 이름을 입력합니다.

5 **테넌트** 드롭다운 메뉴에서 테넌트를 선택합니다.

6 **비즈니스 그룹** 드롭다운 메뉴에서 비즈니스 그룹을 선택합니다.

이 비즈니스 그룹에 속해 있는 사용자만 이 예약을 사용하여 시스템을 프로비저닝할 수 있습니다.

7 (선택 사항) **예약 정책** 드롭다운 메뉴에서 예약 정책을 선택합니다.

이 옵션은 예약 정책이 하나 이상 있어야 사용할 수 있습니다 나중에 예약을 편집하여 예약 정책을 지정할 수 있습니다.

예약 정책은 특정 예약을 대상으로만 프로비저닝을 제한하는 데 사용됩니다.

8 **우선 순위** 텍스트 상자에 숫자를 입력하여 예약의 우선 순위를 설정합니다.

우선 순위는 비즈니스 그룹에 예약이 두 개 이상 있는 경우에 사용됩니다. 우선 순위가 1인 예약은 우선 순위가 2인 예약보다 우선적으로 프로비저닝에 사용됩니다.

9 (선택 사항) 예약을 활성 상태로 유지하지 않으려면 **이 예약 사용** 확인란의 선택을 취소합니다.

이 페이지 밖으로 이동하지 마십시오. 예약이 아직 완료되지 않았습니다.

vCloud Air 예약을 위한 리소스 및 네트워크 설정 지정

이 vRealize Automation 예약을 통해 프로비저닝되는 vCloud Air 시스템에서 사용할 수 있는 리소스와 네트워크 설정을 지정합니다.

vCloud Director 예약을 통해 프로비저닝되는 시스템에 사용할 수 있는 리소스 할당 모델에는 할당 풀, 용량제 및 예약 풀이 있습니다. 용량제의 경우, 스토리지 또는 메모리 양을 지정할 필요는 없지만 스토리지 경로에 대한 우선 순위를 지정해야 합니다. 이러한 할당 모델에 대한 자세한 내용은 vCloud Air 설명서를 참조하십시오.

표준 또는 디스크 수준 스토리지 프로파일을 지정할 수 있습니다. 여러 수준의 디스크 스토리지는 vCloud Air 끝점에서 사용할 수 있습니다.

SDRS(Storage Distributed Resource Scheduler) 스토리지를 사용하는 통합의 경우, SDRS가 이 예약에서 프로비저닝된 시스템에 대해 로드 밸런싱 및 스토리지 배치를 자동으로 처리할 수 있도록 스토리지 클러스터를 선택할 수 있습니다. [SDRS 자동화 모드]를 [자동]으로 설정해야 합니다. 그렇지 않은 경우에는 클러스터 내의 데이터스토어를 선택하여 독립형 데이터스토어 동작을 사용할 수 있습니다. FlexClone 스토리지 디바이스에 대해서는 SDRS가 지원되지 않습니다.

참고 vCloud Air 끝점 및 vCloud Director 끝점에 정의된 예약은 시스템 프로비저닝에 대해 네트워크 프로파일의 사용을 지원하지 않습니다.

필수 조건

[vCloud Director 예약 정보 지정](#).

프로시저

1 **리소스** 탭을 클릭합니다.

2 시스템을 프로비저닝할 계산 리소스를 **계산 리소스** 드롭다운 메뉴에서 선택합니다.

선택한 클러스터에 위치해 있는 템플릿만 이 예약을 사용하는 복제 작업에 사용할 수 있습니다.

3 할당 모델을 선택합니다.

- 4 (선택 사항) **시스템 할당량** 텍스트 상자에 숫자를 입력하여 이 예약에 프로비저닝할 수 있는 시스템의 최대 개수를 설정합니다.

전원이 켜진 시스템만 이 할당량의 개수에 포함됩니다. 예약을 제한하지 않으려면 이 텍스트 상자를 비워 둡니다.

- 5 [메모리] 테이블에서 이 예약에 할당할 메모리 양(GB)을 지정합니다.

예약의 전반적인 메모리 값은 선택한 계산 리소스에서 파생됩니다.

- 6 나열된 스토리지 경로를 하나 이상 선택합니다.

사용할 수 있는 스토리지 경로 옵션은 선택한 계산 리소스에서 파생됩니다.

- a **이 예약은 예약됨** 텍스트 상자에 값을 입력하여 이 예약에 할당할 스토리지 양을 지정합니다.

- b **우선 순위** 텍스트 상자에 값을 입력하여 이 예약과 관련된 다른 스토리지 경로에 대한 이 스토리지 경로의 상대적 우선 순위 값을 지정합니다.

우선 순위는 여러 스토리지 경로에 사용됩니다. 우선 순위가 0인 스토리지 경로가 우선 순위 1을 가진 경로보다 먼저 사용됩니다.

- c 이 스토리지 경로를 이 예약에 사용하지 않으려면 **사용 안 함** 옵션을 클릭합니다.

- d 이 단계를 반복하여 클러스터 및 데이터스토어를 필요에 맞게 구성합니다.

- 7 **네트워크** 탭을 클릭합니다.

- 8 이 예약을 사용하여 프로비저닝된 시스템의 네트워크 경로를 구성합니다.

- a (선택 사항) 해당 옵션을 사용할 수 있는 경우, **끝점** 드롭다운 메뉴에서 스토리지 끝점을 선택합니다.

NetApp ONTAP 끝점이 있고 호스트가 가상 호스트이면 끝점 옆에 FlexClone 옵션이 표시됩니다 NetApp ONTAP 끝점이 있으면 스토리지 경로에 할당된 끝점이 예약 페이지에 표시됩니다. 스토리지 경로의 끝점을 추가, 업데이트 또는 삭제하면 적용되는 모든 예약에 변경 내용이 표시됩니다.

스토리지 경로의 끝점을 추가, 업데이트 또는 삭제하면 예약 페이지에 변경 내용이 표시됩니다.

- b **네트워크 경로** 목록에서 이 예약을 사용하여 프로비저닝된 시스템의 네트워크 경로를 선택합니다.

- c (선택 사항) 나열된 네트워크 프로파일을 **네트워크 프로파일** 드롭다운 메뉴에서 선택합니다.

이 옵션은 네트워크 프로파일이 하나 이상 있어야 사용할 수 있습니다.

예약에 네트워크 경로를 두 개 이상 선택할 수 있지만 시스템을 프로비저닝할 때는 네트워크 한 개만 사용됩니다.

이제 **저장**을 클릭하여 예약을 저장할 수 있습니다. 또는 사용자 지정 속성을 추가하여 예약 규격을 더 세부적으로 제어할 수 있습니다. 이 예약에 할당된 리소스가 줄어들 경우 알림을 보내도록 이메일 경고를 구성할 수도 있습니다.

vCloud Air 예약을 위한 사용자 지정 속성 및 경고 지정

사용자 지정 속성을 vRealize Automation 예약에 연결할 수 있습니다. 또한 예약 리소스가 부족한 경우 이메일 알림을 보내도록 경고를 구성할 수도 있습니다.

사용자 지정 속성 및 이메일 경고는 예약에 사용할 수 있는 선택적인 구성입니다. 사용자 지정 속성을 연결하거나 경고를 설정하지 않으려면 **저장**을 클릭하여 예약 생성을 완료하십시오.

사용자 지정 속성은 필요한 만큼 추가할 수 있습니다.

경고를 구성한 경우, 경고는 지정한 임계값에 도달했을 때가 아니라 매일 생성됩니다.

중요 알림은 이메일 경고가 구성되고 알림을 사용하도록 설정한 경우에만 전송됩니다.

제한을 지정하지 않고 생성한 용량제 예약에 대해서는 경고를 사용할 수 없습니다.

필수 조건

vCloud Air 예약을 위한 리소스 및 네트워크 설정 지정

프로시저

- 1 속성 탭을 클릭합니다.
- 2 새로 만들기를 클릭합니다.
- 3 올바른 사용자 지정 속성 이름을 입력합니다.
- 4 해당하는 경우, 속성 값을 입력합니다.
- 5 (선택 사항) 속성 값을 암호화하려면 **암호화됨** 확인란을 선택합니다.
- 6 (선택 사항) 값을 입력하도록 사용자에게 요청하려면 **사용자에게 확인** 확인란을 선택합니다.
이 옵션은 프로비저닝 시에 재정의할 수 없습니다.
- 7 **저장**을 클릭합니다.
- 8 (선택 사항) 추가적인 사용자 지정 속성을 모두 추가합니다.
- 9 **경고** 탭을 클릭합니다.
- 10 **용량 경고** 확인란을 사용하도록 설정하여, 전송할 경고를 구성합니다.
- 11 슬라이더를 이용하여 사용 가능한 리소스 할당의 임계값을 설정합니다.
- 12 경고 알림을 수신할 AD 사용자 또는 그룹 이름(이메일 주소 아님)을 **받는 사람** 텍스트 상자에 입력합니다.
각 줄에 하나씩 이름을 입력합니다. Enter 키를 눌러 여러 항목을 구분합니다.
- 13 이메일 경고에 그룹 관리자를 포함하려면 **그룹 관리자에게 경고 보내기**를 선택합니다.
이메일 경고가 비즈니스 그룹 **관리자 이메일 수신인** 목록에 포함된 사용자에게 전송됩니다.
- 14 미리 알림 빈도(일)를 지정합니다.
- 15 **저장**을 클릭합니다.

예약이 저장되고 [예약] 목록에 표시됩니다.

vCloud Director 예약 생성

비즈니스 그룹의 구성원이 시스템 프로비저닝을 요청할 수 있으려면 우선 vRealize Automation 예약을 생성하여 시스템에 리소스를 할당해야 합니다.

각 비즈니스 그룹에는 해당 유형의 시스템을 프로비저닝하기 위해 해당 구성원에 대한 예약이 하나 이상 있어야 합니다.

프로시저

1 vCloud Director 예약 정보 지정

각 vCloud Director 조직 가상 데이터 센터(VDC)에 대해 예약을 생성할 수 있습니다. 각 예약은 지정된 계산 리소스의 시스템 요청을 위한 액세스 권한을 부여하도록 특정 비즈니스 그룹에 대해 구성되어 있습니다.

2 vCloud Director 예약을 위한 리소스 및 네트워크 설정 지정

이 vRealize Automation 예약을 통해 프로비저닝되는 vCloud Director 시스템에서 사용할 수 있는 리소스와 네트워크 설정을 지정합니다.

3 vCloud Director 예약을 위한 사용자 지정 속성 및 경고 지정

사용자 지정 속성을 vRealize Automation 예약에 연결할 수 있습니다. 또한 예약 리소스가 부족한 경우 이메일 알림을 보내도록 경고를 구성할 수도 있습니다.

후속 작업

선택적인 예약 정책을 구성하거나 프로비저닝 준비를 시작할 수 있습니다.

Blueprint를 생성할 수 있는 권한을 가진 사용자는 이제 Blueprint를 생성할 수 있습니다.

vCloud Director 예약 정보 지정

각 vCloud Director 조직 가상 데이터 센터(VDC)에 대해 예약을 생성할 수 있습니다. 각 예약은 지정된 계산 리소스의 시스템 요청을 위한 액세스 권한을 부여하도록 특정 비즈니스 그룹에 대해 구성되어 있습니다.

[예약] 페이지에서 **범주별 필터링** 옵션을 사용하면 추가, 편집 또는 삭제 시 예약의 표시 여부를 제어할 수 있습니다. 테스트 에이전트 예약은 범주별로 필터링할 때 예약 목록에 나타나지 않습니다.

참고 예약을 생성한 이후에는 비즈니스 그룹 또는 계산 리소스 연결을 변경할 수 없습니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 테넌트 관리자가 비즈니스 그룹을 하나 이상 생성했는지 확인합니다.
- 계산 리소스가 있는지 확인합니다.
- 네트워크 설정을 구성합니다.
- (선택 사항) 네트워크 프로파일 정보를 구성합니다.

프로시저

- 1 **인프라 > 예약 > 예약**을 선택합니다.

2 새로 만들기 아이콘(+)을 클릭하고, 생성할 예약 유형을 선택합니다.

사용할 수 있는 클라우드 예약 유형은 Amazon, OpenStack, vCloud Air 및 vCloud Director입니다.

vCloud Director를 선택합니다.

3 (선택 사항) 기존 예약에서 복사 드롭다운 메뉴에서 기존 예약을 선택합니다.

선택한 예약의 데이터가 표시됩니다. 필요에 따라 새 예약을 변경할 수 있습니다.

4 이름 텍스트 상자에 이름을 입력합니다.

5 테넌트 드롭다운 메뉴에서 테넌트를 선택합니다.

6 비즈니스 그룹 드롭다운 메뉴에서 비즈니스 그룹을 선택합니다.

이 비즈니스 그룹에 속해 있는 사용자만 이 예약을 사용하여 시스템을 프로비저닝할 수 있습니다.

7 (선택 사항) 예약 정책 드롭다운 메뉴에서 예약 정책을 선택합니다.

이 옵션은 예약 정책이 하나 이상 있어야 사용할 수 있습니다 나중에 예약을 편집하여 예약 정책을 지정할 수 있습니다.

예약 정책은 특정 예약을 대상으로만 프로비저닝을 제한하는 데 사용됩니다.

8 우선 순위 텍스트 상자에 숫자를 입력하여 예약의 우선 순위를 설정합니다.

우선 순위는 비즈니스 그룹에 예약이 두 개 이상 있는 경우에 사용됩니다. 우선 순위가 1인 예약은 우선 순위가 2인 예약보다 우선적으로 프로비저닝에 사용됩니다.

9 (선택 사항) 예약을 활성 상태로 유지하지 않으려면 이 예약 사용 확인란의 선택을 취소합니다.

이 페이지 밖으로 이동하지 마십시오. 예약이 아직 완료되지 않았습니다.

vCloud Director 예약을 위한 리소스 및 네트워크 설정 지정

이 vRealize Automation 예약을 통해 프로비저닝되는 vCloud Director 시스템에서 사용할 수 있는 리소스와 네트워크 설정을 지정합니다.

vCloud Director 예약을 통해 프로비저닝되는 시스템에 사용할 수 있는 리소스 할당 모델에는 할당 풀, 용량제 및 예약 풀이 있습니다. 용량제의 경우, 스토리지 또는 메모리 양을 지정할 필요는 없지만 스토리지 경로에 대한 우선 순위를 지정해야 합니다. 이러한 할당 모델에 대한 자세한 내용은 vCloud Director 설명서를 참조하십시오.

표준 또는 디스크 수준 스토리지 프로파일을 지정할 수 있습니다. 여러 수준의 디스크 스토리지는 vCloud Director 5.6 이상의 끝점에서 사용할 수 있습니다. 여러 수준의 디스크 스토리지는 vCloud Director 5.5 끝점에서 지원되지 않습니다.

SDRS(Storage Distributed Resource Scheduler) 스토리지를 사용하는 통합의 경우, SDRS가 이 예약에서 프로비저닝된 시스템에 대해 로드 밸런싱 및 스토리지 배치를 자동으로 처리할 수 있도록 스토리지 클러스터를 선택할 수 있습니다. [SDRS 자동화 모드]를 [자동]으로 설정해야 합니다. 그렇지 않은 경우에는 클러스터 내의 데이터스토어를 선택하여 독립형 데이터스토어 동작을 사용할 수 있습니다. FlexClone 스토리지 디바이스에 대해서는 SDRS가 지원되지 않습니다.

참고 vCloud Air 끝점 및 vCloud Director 끝점에 정의된 예약은 시스템 프로비저닝에 대해 네트워크 프로파일의 사용을 지원하지 않습니다.

필수 조건

vCloud Director 예약 정보 지정.

프로시저

- 1 리소스 탭을 클릭합니다.
- 2 시스템을 프로비저닝할 계산 리소스를 **계산 리소스** 드롭다운 메뉴에서 선택합니다.
선택한 클러스터에 위치해 있는 템플릿만 이 예약을 사용하는 복제 작업에 사용할 수 있습니다.
- 3 할당 모델을 선택합니다.
- 4 (선택 사항) **시스템 할당량** 텍스트 상자에 숫자를 입력하여 이 예약에 프로비저닝할 수 있는 시스템의 최대 개수를 설정합니다.
전원이 켜진 시스템만 이 할당량의 개수에 포함됩니다. 예약을 제한하지 않으려면 이 텍스트 상자를 비워 둡니다.
- 5 [메모리] 테이블에서 이 예약에 할당할 메모리 양(GB)을 지정합니다.
예약의 전반적인 메모리 값은 선택한 계산 리소스에서 파생됩니다.
- 6 나열된 스토리지 경로를 하나 이상 선택합니다.
사용할 수 있는 스토리지 경로 옵션은 선택한 계산 리소스에서 파생됩니다.
 - a **이 예약은 예약됨** 텍스트 상자에 값을 입력하여 이 예약에 할당할 스토리지 양을 지정합니다.
 - b **우선 순위** 텍스트 상자에 값을 입력하여 이 예약과 관련된 다른 스토리지 경로에 대한 이 스토리지 경로의 상대적 우선 순위 값을 지정합니다.
우선 순위는 여러 스토리지 경로에 사용됩니다. 우선 순위가 0인 스토리지 경로가 우선 순위 1을 가진 경로보다 먼저 사용됩니다.
 - c 이 스토리지 경로를 이 예약에 사용하지 않으려면 **사용 안 함** 옵션을 클릭합니다.
 - d 이 단계를 반복하여 클러스터 및 데이터스토어를 필요에 맞게 구성합니다.
- 7 **네트워크** 탭을 클릭합니다.

8 이 예약을 사용하여 프로비저닝된 시스템의 네트워크 경로를 구성합니다.

- a (선택 사항) 해당 옵션을 사용할 수 있는 경우, **끝점** 드롭다운 메뉴에서 스토리지 끝점을 선택합니다.

NetApp ONTAP 끝점이 있고 호스트가 가상 호스트이면 끝점 옆에 FlexClone 옵션이 표시됩니다 NetApp ONTAP 끝점이 있으면 스토리지 경로에 할당된 끝점이 예약 페이지에 표시됩니다. 스토리지 경로의 끝점을 추가, 업데이트 또는 삭제하면 적용되는 모든 예약에 변경 내용이 표시됩니다.

스토리지 경로의 끝점을 추가, 업데이트 또는 삭제하면 예약 페이지에 변경 내용이 표시됩니다.

- b **네트워크 경로** 목록에서 이 예약을 사용하여 프로비저닝된 시스템의 네트워크 경로를 선택합니다.

- c (선택 사항) 나열된 네트워크 프로파일을 **네트워크 프로파일** 드롭다운 메뉴에서 선택합니다.

이 옵션은 네트워크 프로파일이 하나 이상 있어야 사용할 수 있습니다.

예약에 네트워크 경로를 두 개 이상 선택할 수 있지만 시스템을 프로비저닝할 때는 네트워크 한 개만 사용됩니다.

이제 **저장**을 클릭하여 예약을 저장할 수 있습니다. 또는 사용자 지정 속성을 추가하여 예약 규격을 더 세부적으로 제어할 수 있습니다. 이 예약에 할당된 리소스가 줄어들 경우 알림을 보내도록 이메일 경고를 구성할 수도 있습니다.

vCloud Director 예약을 위한 사용자 지정 속성 및 경고 지정

사용자 지정 속성을 vRealize Automation 예약에 연결할 수 있습니다. 또한 예약 리소스가 부족한 경우 이메일 알림을 보내도록 경고를 구성할 수도 있습니다.

사용자 지정 속성 및 이메일 경고는 예약에 사용할 수 있는 선택적인 구성입니다. 사용자 지정 속성을 연결하거나 경고를 설정하지 않으려면 **저장**을 클릭하여 예약 생성을 완료하십시오.

사용자 지정 속성은 필요한 만큼 추가할 수 있습니다.

경고를 구성한 경우, 경고는 지정한 임계값에 도달했을 때가 아니라 매일 생성됩니다.

중요 알림은 이메일 경고가 구성되고 알림을 사용하도록 설정한 경우에만 전송됩니다.

제한을 지정하지 않고 생성한 용량제 예약에 대해서는 경고를 사용할 수 없습니다.

필수 조건

vCloud Director 예약을 위한 리소스 및 네트워크 설정 지정.

프로시저

- 1 **속성** 탭을 클릭합니다.
- 2 **새로 만들기**를 클릭합니다.
- 3 올바른 사용자 지정 속성 이름을 입력합니다.
- 4 해당하는 경우, 속성 값을 입력합니다.

- 5 (선택 사항) 속성 값을 암호화하려면 **암호화됨** 확인란을 선택합니다.
- 6 (선택 사항) 값을 입력하도록 사용자에게 요청하려면 **사용자에게 확인** 확인란을 선택합니다.
이 옵션은 프로비저닝 시에 재정의할 수 없습니다.
- 7 **저장**을 클릭합니다.
- 8 (선택 사항) 추가적인 사용자 지정 속성을 모두 추가합니다.
- 9 **경고** 탭을 클릭합니다.
- 10 **용량 경고** 확인란을 사용하도록 설정하여, 전송할 경고를 구성합니다.
- 11 슬라이더를 이용하여 사용 가능한 리소스 할당의 임계값을 설정합니다.
- 12 경고 알림을 수신할 AD 사용자 또는 그룹 이름(이메일 주소 아님)을 **받는 사람** 텍스트 상자에 입력합니다.
각 줄에 하나씩 이름을 입력합니다. Enter 키를 눌러 여러 항목을 구분합니다.
- 13 이메일 경고에 그룹 관리자를 포함하려면 **그룹 관리자에게 경고 보내기**를 선택합니다.
이메일 경고가 비즈니스 그룹 **관리자 이메일 수신인** 목록에 포함된 사용자에게 전송됩니다.
- 14 미리 알림 빈도(일)를 지정합니다.
- 15 **저장**을 클릭합니다.

예약이 저장되고 [예약] 목록에 표시됩니다.

Microsoft Azure를 위한 예약 생성

특정 비즈니스 그룹에 대한 Azure 예약을 생성하여 해당 그룹의 사용자에게 지정된 계산 리소스에 대해 Azure 가상 시스템을 요청할 수 있는 권한을 부여합니다.

패포가 VPN 터널을 통해 Single Sign-On을 지원하는 경우 [속성] 탭의 설정을 사용하여 Azure 가상 시스템으로 이 기능에 대한 지원을 구성할 수 있습니다.

참고 Azure 예약 생성 시 경고가 적용되지 않으므로 경고를 무시합니다. 예약을 생성한 이후에는 비즈니스 그룹 연결을 변경할 수 없습니다. 또한 다른 시스템 유형과 달리 Azure 예약과 Blueprint 간에 직접 링크가 없습니다.

[예약] 페이지에서 **범주별 필터링** 옵션을 사용하면 추가, 편집 또는 삭제 시 예약의 표시 여부를 제어할 수 있습니다. 테스트 에이전트 예약은 범주별로 필터링할 때 예약 목록에 나타나지 않습니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 테넌트 관리자가 비즈니스 그룹을 하나 이상 생성했는지 확인합니다.
- (선택 사항) 네트워크 프로파일 정보를 구성합니다.
- 필요한 Azure 리소스에 액세스할 수 있는지 확인합니다.


- 필수 키 쌍이 있는지 확인합니다. 키 쌍에 대한 자세한 내용은 vRealize Automation 구성 항목을 참조하십시오.
- 유효한 Azure 구독 ID를 얻고 이 ID가 해당하는 Azure 끝점에 사용된 항목과 일치해야 합니다. 여러 Azure 구독을 사용하는 경우 각 구독에 대해 예약을 생성해야 합니다.
- 배포가 VPN 터널을 통해 Single Sign-On을 지원하는 경우 예약을 생성하기 전에 적절한 VPC 연결을 구성해야 합니다. [네트워크에서 Azure로 VPC 연결 구성](#) 항목을 참조하십시오.

Microsoft Azure 기본 예약 정보 구성

Microsoft Azure 예약을 위한 기본 정보를 지정합니다.

[예약 정책]을 제외한 [예약 정보] 페이지의 모든 정보는 필수 항목입니다. 이후의 Azure 예약 페이지에 표시되는 모든 정보는 선택 사항입니다.

프로시저

- 인프라 > 관리 > 예약**을 선택합니다.
- 새로 만들기** 아이콘()을 클릭하고, 생성할 예약 유형을 선택합니다.
Azure를 선택합니다.
- (선택 사항) **기존 예약에서 복사** 드롭다운 메뉴에서 기존 예약을 선택합니다.
선택한 예약의 데이터가 표시됩니다. 필요에 따라 새 예약을 변경할 수 있습니다.
- 이름** 텍스트 상자에 이름을 입력합니다.
- 비즈니스 그룹** 드롭다운 메뉴에서 비즈니스 그룹을 선택합니다.
이 비즈니스 그룹에 속해 있는 사용자만 이 예약을 사용하여 시스템을 프로비저닝할 수 있습니다.
- 예약 정책은 Azure 예약에 적용되지 않으므로 **예약 정책** 텍스트 상자는 무시합니다.
- 우선 순위** 텍스트 상자에 숫자를 입력하여 예약의 우선 순위를 설정합니다.
우선 순위는 비즈니스 그룹에 예약이 두 개 이상 있는 경우에 사용됩니다. 우선 순위가 1인 예약은 우선 순위가 2인 예약보다 우선적으로 프로비저닝에 사용됩니다.
- (선택 사항) 예약을 활성 상태로 유지하지 않으려면 **이 예약 사용** 확인란의 선택을 취소합니다.
- 확인**을 클릭합니다.

Azure 예약 리소스 정보 구성

Azure 예약을 설정할 때, 사용 중인 Azure 인스턴스를 바탕으로 리소스 그룹과 스토리지 계정 정보를 할당할 수 있습니다. 예약을 설정하면, 가상 시스템을 프로비저닝할 때 vRealize Automation 프로비저닝 논리는 예약에 의해 지정된 리소스 정보에 따라 리소스 그룹과 스토리지 계정 같은 리소스의 할당을 시도합니다.

예약에서 Azure 가상 시스템에 대한 [리소스 그룹]과 [스토리지 계정] 정보를 구성할 수 있지만, 예약에서 이런 필드를 공백으로 둘 수도 있습니다. 이런 필드를 공백으로 두면, 지정된 Azure 구독 ID와 관련된 기본 리소스 그룹과 스토리지 계정 정보가 관련된 모든 Blueprint에 사용됩니다. Blueprint를 생성하거나 가상 시스템을 프로비저닝할 때 이 정보를 업데이트할 수도 있습니다.

필수 조건

Azure 인스턴스의 구독 ID를 가져옵니다.

프로시저

1 구독 ID 텍스트 상자에 자신의 Azure 구독 ID를 입력하거나 붙여 넣습니다.

2 위치 드롭다운을 클릭하여 예약 위치를 선택합니다.

이 필드를 공백으로 두어 위치를 알 수 없는 예약을 생성할 수 있지만, 그렇게 하더라도 Blueprint를 생성할 때나 Azure 가상 시스템을 프로비저닝할 때 위치 정보를 지정해야 합니다.

3 [리소스 그룹] 테이블에서 새로 만들기를 클릭합니다.

a Azure 인스턴스에서 알맞은 리소스 그룹 이름 정보를 **이름** 텍스트 상자에 붙여 넣습니다.

참고 이름 상자를 비워 둘 수 없습니다.

b **우선 순위** 텍스트 상자에 숫자로 표시되는 우선 순위 값을 할당합니다.

이 할당에 따라 [리소스 그룹]에 두 개 이상의 리소스 그룹이 있을 때의 우선 순위가 결정되며, 숫자가 낮을수록 우선 순위가 높습니다.

c **저장**을 클릭하여 리소스 그룹을 예약에 추가합니다.

4 [스토리지 계정] 테이블에서 새로 만들기를 클릭합니다.

a Azure 인스턴스에서 알맞은 스토리지 계정 이름 정보를 **이름** 텍스트 상자에 붙여 넣습니다.

참고 이름 상자를 비워 둘 수 없습니다.

b **우선 순위** 텍스트 상자에 숫자로 표시되는 우선 순위 값을 할당합니다.

c **저장**을 클릭하여 스토리지 계정을 예약에 추가합니다.

이 할당에 따라 예약에 두 개 이상의 스토리지 계정이 있을 때의 우선 순위가 결정되며, 숫자가 낮을수록 우선 순위가 높습니다.

5 확인을 클릭하여 다음 탭으로 진행합니다.

Azure 속성 구성

여러 네트워크 간의 통신을 지원하기 위해 VPN 터널링과 같은 옵션을 지원하도록 Azure 예약에 사용자 지정 속성을 추가할 수 있습니다. 이 기능을 통해 Blueprint에 소프트웨어 구성 요소를 쉽게 추가할 수도 있습니다.

네트워크에서 VPN 터널링을 지원하기 위해 적절한 URL을 정의하는 사용자 지정 속성을 생성해야 합니다. 또한 이전에 다운로드한 Azure 터널링 구성 스크립트에 대한 경로를 정의하는 속성을 생성해야 합니다.

Azure 터널 물리적 시스템의 개인 IP 주소와 포트 1443을 사용합니다. 이것은 SSH 터널을 호출할 때 vRealize_automation_appliance_fqdn에 대해 할당한 것입니다.

다음 테이블은 VPN 터널링을 지원하는 데 필요한 속성의 이름 및 값을 보여줍니다.

이름	값
Azure.Windows.ScriptPath	Windows 기반 시스템의 터널링을 구성하는 다운로드된 스크립트에 대한 경로를 지정합니다. 배포에 맞게 경로를 업데이트합니다.
Azure.Linux.ScriptPath	Linux 기반 시스템의 터널링을 구성하는 다운로드된 스크립트에 대한 경로를 지정합니다. 배포에 맞게 경로를 업데이트합니다.
agent.download.url	배포에서 VPN 에이전트의 URL을 지정합니다. URL 형식은 <code>https:// Private_IP:1443/software-service/resources/noble-agent.jar</code> 입니다.
software.agent.service.url	배포에 대한 VPN 소프트웨어 에이전트 서비스 URL을 입력합니다. URL 형식은 <code>https:// Private_IP:1443/software-service/api</code> 입니다.
software.ebs.url	배포에 대한 이벤트 브로커 서비스 URL을 입력합니다. URL 형식은 <code>https:// Private_IP:1443/event-broker-service/api</code> 입니다.

필수 조건

- vRealize Automation 장치의 **게스트 및 소프트웨어 에이전트 설치 관리자** 페이지에서 VMware 제공 Azure 스크립트를 다운로드합니다.

이 스크립트는 VPN 터널링을 지원하는 데 필요한 Azure 확장을 설치합니다. 스크립트에는 두 가지가 있습니다. `script.ps1` 및 `script.sh`. `.ps1` 파일은 Windows 시스템용이며 `.sh` 파일은 Linux 시스템용입니다.

- `https://vrealize-automation-appliance-fqdn/software`를 실행하여 [VMware vRealize Automation 장치] 페이지를 엽니다.
- [vRealize Automation 구성 요소(IaaS, 게스트 및 소프트웨어 에이전트, 도구)를 설치하려면] 머리글 아래에서 **게스트 및 소프트웨어 에이전트** 링크를 클릭합니다.
- [Azure 시스템] 머리글 아래에서 Azure 스크립트 파일을 다운로드합니다. 스크립트 파일을 적절한 위치에 저장합니다. Azure 예약 사용자 지정 속성을 구성할 때 이 위치를 가리켜야 합니다.

프로시저

- 1 속성 탭을 클릭합니다.
- 2 새로 만들기를 클릭합니다.
- 3 [속성] 대화상자에 사용자 지정 속성의 적절한 이름 및 값을 입력합니다.
- 4 각 속성을 생성할 때 대화상자에서 **확인**을 클릭하여 해당 속성을 추가합니다.
- 5 모든 필수 속성을 추가했으면 **확인**을 클릭하여 설정을 저장합니다.

후속 작업

VPN 터널링을 지원하도록 사용자 지정 속성을 생성한 후에는 Azure Blueprint에 대한 소프트웨어 구성 요소를 생성할 수 있습니다. 자세한 내용은 vRealize Automation 구성을 참조하십시오.

Azure에 대한 소프트웨어 구성 요소를 설정할 때는 [새 소프트웨어] 페이지의 [컨테이너] 드롭다운에서 **Azure 가상 시스템**을 선택합니다.

Azure 예약 네트워크 정보 구성

예약에서 Azure 가상 시스템에 대한 가상 네트워크 및 로드 밸런서 정보를 구성할 수 있습니다.

이 페이지의 일부나 전부를 공백으로 두고 가상 시스템을 프로비저닝할 때 가상 네트워크 및 로드 밸런서 정보를 구성하도록 선택할 수도 있습니다.

네트워크 프로파일을 지정하고 서브넷을 지정하지 않으면 지정된 네트워크 프로파일의 첫 번째 기존 네트워크 범위의 이름이 서브넷 이름으로 사용됩니다. 네트워크 프로파일을 지정한 경우에는 vNet 텍스트 상자를 공백으로 둘 수 있습니다. 이 경우에는 지정된 네트워크 프로파일의 이 첫 번째 네트워크 범위의 이름이 서브넷 이름으로 사용되고, vNet 이름은 관련된 서브넷을 포함하는 첫 번째 Azure vNet으로 확인됩니다.

필수 조건

해당되는 경우 Azure 인스턴스에서 적절한 가상 네트워크 및 로드 밸런서 정보를 가져옵니다.

프로시저

- 1 [네트워크] 테이블에서 **새로 만들기**를 클릭하여 가상 시스템과 함께 사용하기에 알맞은 Azure 가상 네트워크를 구성합니다.
 - a Azure 인스턴스에서 알맞은 vNet 이름 정보를 **vNet** 텍스트 상자에 붙여 넣습니다.
 - b Azure 인스턴스에서 알맞은 서브넷 이름 정보를 **서브넷** 텍스트 상자에 붙여 넣습니다.
서브넷 규격은 선택 사항입니다. 이 상자를 비워 두면 기본적으로 지정된 vNet의 서브넷이 사용됩니다.
 - c **네트워크 프로파일** 텍스트 상자에 알맞은 이름을 입력하거나 붙여 넣습니다. Blueprint에서 네트워크 프로파일을 사용하여 네트워크 인터페이스 카드를 네트워크와 연결할 수 있습니다.
네트워크 프로파일 규격은 선택 사항입니다. 네트워크 프로파일 규격이 Azure 네트워크 구성체와 결합되도록 하는 게 아니라, 네트워크 프로파일을 기반으로 Blueprint를 생성하려는 경우에 사용하며, 이는 vRealize Automation에 정의되어 있습니다.
 - d 해당되는 경우 **우선 순위** 텍스트 상자에 숫자로 표시되는 우선 순위 값을 할당합니다.
이 할당에 따라 가상 네트워크에 두 개 이상의 예약이 있을 때의 우선 순위가 결정되며, 숫자가 낮을수록 우선 순위가 높습니다.
 - e **저장**을 클릭하여 리소스 그룹을 예약에 추가합니다.

- 2 여러 시스템을 배포하는 중에 로드 밸런서를 사용하는 경우 [로드 밸런서] 테이블에서 **새로 만들기**를 클릭합니다.

- a Azure 인스턴스에서 알맞은 로드 밸런서 이름을 **이름** 텍스트 상자에 붙여 넣습니다.
- b Azure 인스턴스에서 알맞은 이름을 **백 엔드 주소 풀** 텍스트 상자에 붙여 넣습니다.
- c 해당되는 경우 **우선 순위** 텍스트 상자에 숫자로 표시되는 우선 순위 값을 할당합니다.

이 할당에 따라 가상 네트워크에 두 개 이상의 로드 밸런서가 있을 때의 우선 순위가 결정되며, 숫자가 낮을수록 우선 순위가 높습니다.

- d **저장**을 클릭하여 로드 밸런서를 예약에 추가합니다.

- 3 방화벽을 통해 통신해야 하는 여러 시스템을 배포하려는 경우 [보안 그룹] 테이블에서 **새로 만들기**를 클릭합니다.

- a Azure 인스턴스에서 보안 그룹 이름을 **이름** 텍스트 상자에 붙여 넣습니다.
- b 해당되는 경우 **우선 순위** 텍스트 상자에 숫자로 표시되는 우선 순위 값을 할당합니다.

이 할당에 따라 가상 네트워크에 두 개 이상의 보안 그룹이 있을 때의 우선 순위가 결정되며, 숫자가 낮을수록 우선 순위가 높습니다.

- c **저장**을 클릭하여 보안 그룹을 예약에 추가합니다.

4 확인을 클릭합니다.

시나리오: 개념 증명 환경을 위해 Amazon 예약 생성

개념 증명 환경을 위해 SSH 터널을 사용하여 일시적으로 네트워크 및 Amazon VPC 간 연결을 설정했기 때문에 Software 부트스트랩과 게스트 에이전트가 터널을 통해 통신을 실행하도록 하려면 Amazon 예약에 사용자 지정 속성을 추가해야 합니다.

네트워크 및 Amazon VPC 간 연결은 게스트 에이전트를 사용하여 프로비저닝된 시스템을 사용자 지정하거나 Blueprint에 Software 구성 요소를 포함하려는 경우에만 필요합니다. 운영 환경이라면 Amazon Web Services를 통해 공식적으로 이 연결을 구성하겠지만 개념 증명 환경에서 작업 중이므로 임시 SSH 터널을 구성했습니다.

패브릭 관리자 권한을 사용하여, Amazon Web Services 리소스를 할당하고 SSH 터널링을 지원하는 몇 개의 사용자 지정 속성을 포함하기 위한 예약을 생성합니다. 또한 터널 시스템과 동일한 영역 및 VPC에서 예약을 구성합니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 네트워크 및 Amazon VPC 간 연결이 설정되도록 SSH 터널을 구성합니다. Amazon AWS 터널 시스템의 개인 IP 주소, 서브넷 및 보안 그룹을 기록해 둡니다. [시나리오: 개념 증명 환경을 위해 네트워크 및 Amazon VPC 간 연결 구성](#) 항목을 참조하십시오.
- 개념 증명 환경에서 Blueprint를 설계해야 하는 IT 조직 구성원을 위한 비즈니스 그룹을 생성합니다. [비즈니스 그룹 생성](#) 항목을 참조하십시오.
- 테넌트 관리자가 비즈니스 그룹을 하나 이상 생성했는지 확인합니다.

프로시저

1 시나리오: 개념 증명 환경을 위해 Amazon AWS 예약 정보 지정

Blueprint 설계자 팀이 개념 증명 환경에서 기능을 테스트할 수 있도록 팀을 위해 리소스를 예약하려고 합니다. 따라서 설계자 비즈니스 그룹에 리소스를 할당하도록 이 예약을 구성합니다.

2 시나리오: 개념 증명 환경을 위해 Amazon AWS 네트워크 설정 지정

터널 시스템에서 사용 중인 것과 동일한 영역 및 네트워킹 설정을 사용하도록 예약을 구성하고 이 예약에 대해 전원을 켤 수 있는 시스템의 수를 제한하여 리소스 사용량을 관리합니다.

3 시나리오: 터널을 통해 에이전트 통신을 실행하도록 사용자 지정 속성 지정

네트워크 및 Amazon VPC 간 연결을 구성할 때 Amazon AWS 터널 시스템이 vRealize Automation 리소스에 액세스할 수 있도록 포트 전달을 구성했습니다.

시나리오: 개념 증명 환경을 위해 Amazon AWS 예약 정보 지정

Blueprint 설계자 팀이 개념 증명 환경에서 기능을 테스트할 수 있도록 팀을 위해 리소스를 예약하려고 합니다. 따라서 설계자 비즈니스 그룹에 리소스를 할당하도록 이 예약을 구성합니다.

참고 예약을 생성한 이후에는 비즈니스 그룹 또는 계산 리소스 연결을 변경할 수 없습니다.

프로시저

1 인프라 > 예약 > 예약을 선택합니다.

2 새로 만들기 아이콘(+)을 클릭하고, 생성할 예약 유형을 선택합니다.

Amazon을 선택합니다.

3 이름 텍스트 상자에 Amazon Tunnel POC를 입력합니다.

4 비즈니스 그룹 드롭다운 메뉴에서 Blueprint 설계자를 위해 생성한 비즈니스 그룹을 선택합니다.

5 우선 순위 텍스트 상자에 1을 입력하여 이 예약을 가장 높은 우선 순위로 설정합니다.

예약에 대해 비즈니스 그룹과 우선 순위를 구성했지만 아직 리소스를 할당하고 SSH 터널에 대한 사용자 지정 속성을 구성해야 합니다.

시나리오: 개념 증명 환경을 위해 Amazon AWS 네트워크 설정 지정

터널 시스템에서 사용 중인 것과 동일한 영역 및 네트워킹 설정을 사용하도록 예약을 구성하고 이 예약에 대해 전원을 켤 수 있는 시스템의 수를 제한하여 리소스 사용량을 관리합니다.

프로시저

1 리소스 탭을 클릭합니다.

2 시스템을 프로비저닝할 계산 리소스를 계산 리소스 드롭다운 메뉴에서 선택합니다.

터널 시스템이 위치한 Amazon AWS 영역을 선택합니다.

3 (선택 사항) 시스템 할당량 텍스트 상자에 숫자를 입력하여 이 예약에 프로비저닝할 수 있는 시스템의 최대 개수를 설정합니다.

전원이 켜진 시스템만 이 할당량의 개수에 포함됩니다. 예약을 제한하지 않으려면 이 텍스트 상자를 비워 둡니다.

4 키 쌍 드롭다운 메뉴에서 **키 쌍 지정**을 선택합니다.

이것은 개념 증명 환경이므로 이 예약을 사용하여 프로비저닝되는 모든 시스템에 대해 단일 키 쌍을 공유하도록 선택합니다.

5 키 쌍 드롭다운 메뉴에서 설계자와 공유하려는 키 쌍을 선택합니다.**6 VPC의 서브넷에 할당** 확인란을 선택합니다.**7** 터널 시스템에서 사용 중인 것과 동일한 서브넷과 보안 그룹을 선택합니다.

터널 시스템과 동일한 영역 및 네트워킹 설정을 사용하도록 예약을 구성했지만 Software 부트스트랩 에이전트와 게스트 에이전트가 터널을 통해 통신을 실행하도록 사용자 지정 속성을 추가해야 합니다.

시나리오: 터널을 통해 에이전트 통신을 실행하도록 사용자 지정 속성 지정

네트워크 및 Amazon VPC 간 연결을 구성할 때 Amazon AWS 터널 시스템이 vRealize Automation 리소스에 액세스할 수 있도록 포트 전달을 구성했습니다.

그러한 포트에 액세스하도록 에이전트를 구성하려면 예약에 터널 사용자 지정 속성을 추가해야 합니다.

참고 조직의 네트워크와 vRealize Automation 네트워크 사이에 PAT 또는 NAT 시스템 네트워크를 사용하는 경우 이러한 속성을 사용하여 개인 IP 주소 및 포트에 액세스할 수 있습니다.

프로시저**1 속성** 탭을 클릭합니다.**2 새로 만들기**를 클릭합니다.**3** 터널 사용자 지정 속성을 구성합니다.

Amazon AWS 터널 시스템의 개인 IP 주소와 포트 1443을 사용합니다. 이것은 SSH 터널을 호출할 때 vRealize_automation_appliance_fqdn에 대해 할당한 것입니다.

옵션	값
software.ebs.url	https://Private_IP:1443/event-broker-service/api
software.agent.service.url	https://Private_IP:1443/software-service/api
agent.download.url	https://Private_IP:1443/software-service/resources/nobel-agent.jar

4 저장을 클릭합니다.

Amazon AWS 리소스를 설계자 비즈니스 그룹에 할당하기 위해 예약을 생성했습니다. 게스트 에이전트와 Software 부트스트랩 에이전트를 지원하도록 예약을 구성했습니다. 설계자는 게스트 에이전트를 활용하여 배포된 시스템을 사용자 지정하거나 Software 구성 요소를 포함하는 Blueprint를 생성할 수 있습니다.

가상 범주 예약 생성

가상 범주 유형 예약을 사용하면 특정 vRealize Automation 비즈니스 그룹에 대한 가상 시스템 배포의 프로비저닝 서비스에 액세스할 수 있습니다. 사용할 수 있는 가상 예약 유형으로는 vSphere, Hyper-V, KVM, SCVMM 및 XenServer가 있습니다.

예약은 특정 vRealize Automation 비즈니스 그룹에 할당된 계산 리소스 하나의 메모리, CPU, 네트워크 및 스토리지 리소스를 공유하는 것입니다.

비즈니스 그룹은 하나의 끝점 또는 여러 끝점에서 여러 개의 예약을 사용할 수 있습니다.

가상 시스템을 프로비저닝하려면 가상 계산 리소스에 대한 예약 하나 이상이 비즈니스 그룹에 있어야 합니다. 각 예약은 비즈니스 그룹 하나에만 사용할 수 있지만 비즈니스 그룹은 단일 계산 리소스에 대한 여러 개의 예약 및 서로 다른 유형의 계산 리소스에 대한 여러 개의 예약을 사용할 수 있습니다.

비즈니스 그룹에 할당된 패브릭 리소스의 공유를 정의하는 것 외에, 예약은 정책, 우선 순위 그리고 시스템 배치를 결정하는 할당량을 정의할 수 있습니다.

성공적인 프로비저닝을 위해서는 예약에 사용 가능한 스토리지가 충분해야 합니다. 예약의 스토리지 가용성은 다음에 따라 달라집니다.

- 데이터스토어/클러스터에서 사용할 수 있는 스토리지의 양
- 해당 데이터스토어/클러스터에 예약된 해당 스토리지의 양
- vRealize Automation에 이미 할당되어 있는 해당 스토리지의 양

예를 들어 vCenter Server에 데이터스토어/클러스터에 사용할 수 있는 스토리지가 있는 경우에도 예약에 충분한 스토리지가 예약되지 않으면 프로비저닝이 실패하면서 "할당에 사용할 예약이 없음..." 오류가 표시됩니다. 예약에 할당된 스토리지는 해당 예약에 대한 VM(상태에 관계없음)의 수에 따라 다릅니다. 자세한 내용은 VMware 기술 자료 문서 시스템 XXX: 그룹 XXX 내에 할당에 사용할 예약이 없음. 총 XXGB의 스토리지가 요청됨(2151030)(<http://kb.vmware.com/kb/2151030>)을 참조하십시오.

예약의 선택 논리 이해

비즈니스 그룹의 구성원이 가상 시스템에 대한 프로비저닝 요청을 생성하면 vRealize Automation은 해당 비즈니스 그룹이 사용할 수 있는 예약 중 하나에서 시스템을 선택합니다.

시스템이 프로비저닝되는 예약은 다음과 같은 기준을 충족해야 합니다.

- 예약은 시스템이 요청된 Blueprint와 플랫폼 유형이 동일해야 합니다.
일반 가상 Blueprint는 모든 유형의 가상 예약에 프로비저닝할 수 있습니다.
- 예약은 사용할 수 있게 설정되어 있어야 합니다.
- 계산 리소스가 액세스 가능한 상태여야 하며 유지 보수 모드이면 안 됩니다.
- 예약은 해당 시스템 할당량에 용량이 남아 있거나, 할당량에 제한이 없어야 합니다.

할당된 시스템 할당량에는 전원이 켜진 시스템만 포함됩니다. 예를 들어 예약의 할당량이 50인 경우, 40대의 시스템이 프로비저닝되었지만 그 중 20대만 전원이 켜져 있으면 예약의 할당량은 80%가 아니라 40%만 할당된 것입니다.

- 예약에는 시스템을 프로비저닝하는 데 충분한 할당되지 않은 메모리와 스토리지 리소스가 있어야 합니다.

가상 예약의 시스템 할당량, 메모리 또는 스토리지가 모두 할당된 상태이면 해당 예약에서는 가상 시스템을 더 이상 프로비저닝할 수 없습니다. 가상화 계산 리소스의 물리적 용량 이상으로 리소스를 예약할 수 있지만(오버 커밋), 계산 리소스의 물리적 용량이 100% 할당된 경우에는 리소스가 회수되기 전까지 해당 계산 리소스를 사용하는 그 어떤 예약에도 시스템을 추가적으로 프로비저닝할 수 없습니다.

- Blueprint에 특정 네트워크 설정이 지정되어 있으면 예약에도 동일한 네트워크가 있어야 합니다. Blueprint 또는 예약에 정적 IP 주소 할당을 위한 네트워크 프로파일이 지정된 경우, 새 시스템을 할당할 IP 주소를 사용할 수 있어야 합니다.

- Blueprint 또는 예약에 위치가 지정되어 있으면 계산 리소스가 해당 위치에 연결되어 있어야 합니다.

사용자 지정 속성 VRM.Datacenter.Policy의 값이 **Exact**인 경우, 해당 위치에 연결된 계산 리소스에 대해 다른 모든 기준을 충족하는 예약이 없으면 프로비저닝이 실패합니다.

VRM.Datacenter.Policy의 값이 **NotExact**인 경우, 해당 위치에 연결된 계산 리소스에 대해 다른 모든 기준을 충족하는 예약이 없으면 위치에 관계없이 다른 예약에서 프로비저닝을 진행할 수 있습니다. 이 옵션은 기본값입니다.

- Blueprint 또는 요청에 사용자 지정 속성 VirtualMachine.Host.TpmEnabled가 지정된 경우에는 예약에 대한 계산 리소스에 신뢰할 수 있는 하드웨어가 설치되어 있어야 합니다.
- Blueprint에 예약 정책이 지정된 경우, 예약은 해당 예약 정책에 속해 있어야 합니다.

예약 정책은 선택한 예약이 특정 Blueprint에서 시스템을 프로비저닝하기 위한 모든 추가적인 요구 사항을 충족하는지 보장하는 방식입니다. 예를 들어 예약 정책을 사용하면 복제를 위한 특정 템플릿을 사용하는 계산 리소스만 프로비저닝하도록 제한할 수 있습니다.

선택한 모든 기준을 모두 충족하는 예약이 없으면 프로비저닝이 실패합니다.

모든 기준을 충족하는 예약이 여러 개 있는 경우에는 요청된 시스템을 프로비저닝하는 데 사용할 예약이 다음과 같은 논리에 따라 결정됩니다.

- 우선 순위 값이 낮은 예약이 우선 순위 값이 높은 예약보다 먼저 선택됩니다.
- 여러 예약의 우선 순위가 동일한 경우, 할당된 시스템 할당량의 비율이 가장 낮은 예약이 선택됩니다.
- 여러 예약의 우선 순위 및 할당량 사용량이 동일한 경우, 라운드 로빈 방식으로 예약 간에 시스템이 분산됩니다.

참고 네트워크 프로파일의 라운드 로빈 선택은 지원되지 않지만 네트워크(있는 경우)의 라운드 로빈 선택은 지원되므로 이를 서로 다른 네트워크 프로파일과 연결할 수 있습니다.

시스템 볼륨을 프로비저닝하는 데 충분한 용량을 가진 스토리지 경로 여러 개를 예약에서 사용할 수 있는 경우에는 다음과 같은 논리에 따라 스토리지 경로가 선택됩니다.

- Blueprint 또는 요청에 스토리지 예약 정책이 지정된 경우, 스토리지 경로는 해당 스토리지 예약 정책에 속해 있어야 합니다.

사용자 지정 속성 VirtualMachine.DiskN.StorageReservationPolicyMode의 값이 **NotExact**이고 스토리지 예약 정책 내에 용량이 충분한 스토리지 경로가 없는 경우, 지정된 스토리지 예약 정책 외부의 스토리지 경로를 사용하여 프로비저닝을 진행할 수 있습니다.

VirtualMachine.DiskN.StorageReservationPolicyMode의 기본값은 **Exact**입니다.

- 우선 순위 값이 낮은 스토리지 경로가 우선 순위 값이 높은 스토리지 경로보다 먼저 선택됩니다.
- 여러 스토리지 경로의 우선 순위가 동일한 경우, 라운드 로빈 방식으로 스토리지 경로 간에 시스템이 분산됩니다.

NSX 네트워크 및 보안 가상화를 위해 vSphere 예약 생성

vSphere 예약을 생성하여 외부 네트워크와 라우팅된 게이트웨이를 네트워크용 네트워크 프로파일에 할당하고, 전송 영역을 지정하고, 보안 그룹을 시스템 구성 요소에 할당할 수 있습니다.

NSX를 구성한 경우 Blueprint를 생성하거나 편집할 때 NSX 전송 영역, Edge 및 라우팅된 게이트웨이 예약 정책 그리고 App 분리 설정을 지정할 수 있습니다. 이러한 설정은 **Blueprint** 및 **Blueprint 속성** 페이지의 **NSX 설정** 탭에서 사용할 수 있습니다.

설계 캔버스에 추가하는 네트워크 및 보안 구성 요소 설정은 NSX 구성에서 파생됩니다. 이러한 설정을 사용하려면 vSphere 클러스터의 NSX 인벤토리에 대해 데이터 수집을 실행해야 합니다. 네트워크 및 보안 구성 요소는 NSX에만 해당하며 vSphere 시스템 구성 요소와만 사용할 수 있습니다. NSX 구성에 대한 자세한 내용은 NSX 관리 가이드를 참조하십시오.

vRealize Automation은 NAT 또는 라우팅된 네트워크를 사용하는 시스템을 프로비저닝할 때 라우팅된 게이트웨이를 네트워크 라우터로 프로비저닝합니다. Edge 또는 라우팅된 게이트웨이는 계산 리소스를 사용하는 관리 시스템입니다. 또한 라우팅된 게이트웨이는 프로비저닝된 시스템 구성 요소의 네트워크 통신을 관리합니다. Edge 또는 라우팅된 게이트웨이를 프로비저닝하는 데 사용되는 예약은 NAT 및 라우팅된 네트워크 프로파일에 사용되는 외부 네트워크를 결정합니다. 뿐만 아니라 Edge 또는 라우팅된 게이트웨이가 라우팅된 네트워크를 구성하는 데 사용한 예약도 결정합니다. 예약이 라우팅된 게이트웨이는 라우팅된 네트워크를 라우팅 테이블의 항목과 연결합니다.

Edge 또는 라우팅된 게이트웨이 예약 정책을 지정하여 Edge 또는 라우팅된 게이트웨이를 사용하는 시스템을 프로비저닝할 때 어떤 예약을 사용할지 확인할 수 있습니다. 기본적으로 vRealize Automation에서는 라우팅된 게이트웨이와 시스템 구성 요소에 대해 동일한 예약을 사용합니다.

vRealize Automation에서 그러한 예약으로 프로비저닝되는 모든 구성 요소 시스템에 대해 기본 보안 정책을 적용할 하나 이상의 보안 그룹을 예약에서 선택합니다. 프로비저닝되는 모든 시스템은 이와 같이 지정된 보안 그룹에 추가됩니다.

프로비저닝을 성공적으로 수행하려면 Blueprint에서 시스템 네트워크를 정의할 때 예약의 전송 영역이 시스템 Blueprint의 전송 영역과 일치해야 합니다. 마찬가지로 시스템의 라우팅된 게이트웨이를 프로비저닝하려면 예약에 정의된 전송 영역이 Blueprint에 대해 정의된 전송 영역과 일치해야 합니다.

라우팅된 네트워크를 구성할 때 Edge 또는 라우팅된 게이트웨이와 네트워크 프로파일을 예약에서 선택할 경우, 라우팅된 네트워크를 서로 연결하는 데 사용할 네트워크 경로를 선택하고, 라우팅된 네트워크 프로파일을 구성하는 데 사용되는 외부 네트워크 프로파일을 여기에 할당합니다. 네트워크 경로에 할당하는 데 사용할 수 있는 네트워크 프로파일 목록은 네트워크 인터페이스에 대해 선택한 서브넷 마스크와 기본 IP 주소에 기반하여, 네트워크 경로의 서브넷과 일치하도록 필터링됩니다.

Edge 또는 라우팅된 게이트웨이를 vRealize Automation 예약에 사용하려면 NSX 환경에서 라우팅된 게이트웨이를 외부적으로 구성한 다음 인벤토리 데이터 수집을 실행합니다. NSX의 경우에는 작동 중인 NSX Edge 인스턴스가 있어야만 정적 경로의 기본 게이트웨이 또는 Edge 서비스 게이트웨이 또는 분산 라우터에 대한 동적 라우팅 세부 정보를 구성할 수 있습니다. 자세한 내용은 NSX 관리 가이드를 참조하십시오.

Hyper-V, KVM, SCVMM, vSphere 또는 XenServer에 대한 예약 생성

비즈니스 그룹의 구성원이 시스템 프로비저닝을 요청할 수 있으려면 우선 예약을 생성하여 시스템에 리소스를 할당해야 합니다.

각 비즈니스 그룹에는 해당 유형의 시스템을 프로비저닝하기 위해 해당 구성원에 대한 예약이 하나 이상 있어야 합니다. 예를 들어 vSphere 예약은 있지만 KVM (RHEV) 예약이 없는 비즈니스 그룹은 KVM (RHEV) 가상 시스템을 요청할 수 없습니다. 이 예에서, 비즈니스 그룹에는 특별히 KVM (RHEV) 리소스에 대한 예약이 할당되어야 합니다.

프로시저

1 가상 예약 정보 지정

각 예약은 지정된 계산 리소스의 시스템 요청을 위한 액세스 권한을 사용자에게 부여하도록 특정 비즈니스 그룹에 대해 구성되어 있습니다.

2 가상 예약을 위한 리소스 및 네트워킹 설정 지정

이 vRealize Automation 예약으로부터 시스템을 프로비저닝하기 위한 리소스 및 네트워크 설정을 지정합니다.

3 가상 예약을 위한 사용자 지정 속성 및 경고 지정

사용자 지정 속성을 vRealize Automation 예약에 연결할 수 있습니다. 또한 예약 리소스가 부족한 경우 이메일 알림을 보내도록 경고를 구성할 수도 있습니다.

가상 예약 정보 지정

각 예약은 지정된 계산 리소스의 시스템 요청을 위한 액세스 권한을 사용자에게 부여하도록 특정 비즈니스 그룹에 대해 구성되어 있습니다.

[예약] 페이지에서 **범주별 필터링** 옵션을 사용하면 추가, 편집 또는 삭제 시 예약의 표시 여부를 제어할 수 있습니다. 테스트 에이전트 예약은 범주별로 필터링할 때 예약 목록에 나타나지 않습니다.


참고 예약을 생성한 이후에는 비즈니스 그룹 또는 계산 리소스 연결을 변경할 수 없습니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 테넌트 관리자가 비즈니스 그룹을 하나 이상 생성했는지 확인합니다.
- 계산 리소스가 있는지 확인합니다.
- 네트워크 설정을 구성합니다.
- (선택 사항) 네트워크 프로파일 정보를 구성합니다.

프로시저

1 **인프라 > 예약 > 예약**을 선택합니다.

2 **새로 만들기** 아이콘()을 클릭하고, 생성할 예약 유형을 선택합니다.

사용할 수 있는 가상 예약 유형은 Hyper-V, KVM, SCVMM, vSphere 및 XenServer입니다.

예를 들어 **vSphere**를 선택합니다.

3 (선택 사항) **기존 예약에서 복사** 드롭다운 메뉴에서 기존 예약을 선택합니다.

선택한 예약의 데이터가 표시됩니다. 필요에 따라 새 예약을 변경할 수 있습니다.

4 **이름** 텍스트 상자에 이름을 입력합니다.

5 **테넌트** 드롭다운 메뉴에서 테넌트를 선택합니다.

6 **비즈니스 그룹** 드롭다운 메뉴에서 비즈니스 그룹을 선택합니다.

이 비즈니스 그룹에 속해 있는 사용자만 이 예약을 사용하여 시스템을 프로비저닝할 수 있습니다.

7 (선택 사항) **예약 정책** 드롭다운 메뉴에서 예약 정책을 선택합니다.

이 옵션은 예약 정책이 하나 이상 있어야 사용할 수 있습니다 나중에 예약을 편집하여 예약 정책을 지정할 수 있습니다.

예약 정책은 특정 예약을 대상으로만 프로비저닝을 제한하는 데 사용됩니다.

8 **우선 순위** 텍스트 상자에 숫자를 입력하여 예약의 우선 순위를 설정합니다.

우선 순위는 비즈니스 그룹에 예약이 두 개 이상 있는 경우에 사용됩니다. 우선 순위가 1인 예약은 우선 순위가 2인 예약보다 우선적으로 프로비저닝에 사용됩니다.

9 (선택 사항) 예약을 활성 상태로 유지하지 않으려면 **이 예약 사용** 확인란의 선택을 취소합니다.

이 페이지 밖으로 이동하지 마십시오. 예약이 아직 완료되지 않았습니다.

가상 예약을 위한 리소스 및 네트워킹 설정 지정

이 vRealize Automation 예약으로부터 시스템을 프로비저닝하기 위한 리소스 및 네트워크 설정을 지정합니다.

vSphere 환경을 사용하고 Net App FlexClone 기술을 사용하는 스토리지 디바이스가 있는 경우에는 예약에서 FlexClone 데이터스토어를 선택할 수 있습니다. FlexClone 스토리지 디바이스에 대해서는 SDRS가 지원되지 않습니다.

성공적인 프로비저닝을 위해서는 예약에 사용 가능한 스토리지가 충분해야 합니다. 예약의 스토리지 가용성은 다음에 따라 달라집니다.

- 데이터스토어/클러스터에서 사용할 수 있는 스토리지의 양
- 해당 데이터스토어/클러스터에 예약된 해당 스토리지의 양
- vRealize Automation에 이미 할당되어 있는 해당 스토리지의 양

예를 들어 vCenter Server에 데이터스토어/클러스터에 사용할 수 있는 스토리지가 있는 경우에도 예약에 충분한 스토리지가 예약되지 않으면 프로비저닝이 실패하면서 "할당에 사용할 예약이 없음..." 오류가 표시됩니다. 예약에 할당된 스토리지는 해당 예약에 대한 VM(상태에 관계없음)의 수에 따라 다릅니다. 자세한 내용은 VMware 기술 자료 문서 시스템 XXX: 그룹 XXX 내에 할당에 사용할 예약이 없음. 총 XXGB의 스토리지가 요청됨(2151030)(<http://kb.vmware.com/kb/2151030>)을 참조하십시오.

필수 조건

가상 예약 정보 지정.

프로시저

1 리소스 탭을 클릭합니다.

2 시스템을 프로비저닝할 계산 리소스를 **계산 리소스** 드롭다운 메뉴에서 선택합니다.

선택한 클러스터에 위치해 있는 템플릿만 이 예약을 사용하는 복제 작업에 사용할 수 있습니다.

프로비저닝하는 동안 로컬 스토리지에 연결된 호스트에 시스템이 배치됩니다. 예약에서 로컬 스토리지를 사용하는 경우 예약에 의해 프로비저닝되는 모든 시스템은 해당 로컬 스토리지가 들어 있는 호스트에서 생성됩니다. 하지만 VirtualMachine.Admin.ForceHost 사용자 지정 속성을 사용하는 경우 시스템이 다른 호스트로 프로비저닝되도록 강제되고 프로비저닝이 실패합니다. 또한 시스템 복제에 사용된 템플릿이 로컬 스토리지에 있지만 다른 클러스터의 시스템에 연결되어 있는 경우에도 프로비저닝이 실패합니다. 이 경우 템플릿에 액세스할 수 없기 때문에 프로비저닝이 실패합니다.

3 (선택 사항) **시스템 할당량** 텍스트 상자에 숫자를 입력하여 이 예약에 프로비저닝할 수 있는 시스템의 최대 개수를 설정합니다.

전원이 켜진 시스템만 이 할당량의 개수에 포함됩니다. 예약을 제한하지 않으려면 이 텍스트 상자를 비워 둡니다.

4 [메모리] 테이블에서 이 예약에 할당할 메모리 양(GB)을 지정합니다.

예약의 전반적인 메모리 값은 선택한 계산 리소스에서 파생됩니다.

5 나열된 스토리지 경로를 하나 이상 선택합니다.

사용할 수 있는 스토리지 경로 옵션은 선택한 계산 리소스에서 파생됩니다.

SDRS(Storage Distributed Resource Scheduler) 스토리지를 사용하는 통합의 경우, SDRS가 이 예약에서 프로비저닝된 시스템에 대해 로드 밸런싱 및 스토리지 배치를 자동으로 처리할 수 있도록 스토리지 클러스터를 선택할 수 있습니다. [SDRS 자동화 모드]를 [자동]으로 설정해야 합니다. 그렇지 않은 경우에는 클러스터 내의 데이터스토어를 선택하여 독립형 데이터스토어 동작을 사용할 수 있습니다. FlexClone 스토리지 디바이스에 대해서는 SDRS가 지원되지 않습니다.

클러스터 또는 스토리지 클러스터의 개별 디스크를 선택할 수 있지만 함께 선택할 수는 없습니다. 스토리지 클러스터를 선택하는 경우 SDRS가 이 예약에서 프로비저닝된 시스템에 대한 스토리지 배치 및 로드 밸런싱을 제어합니다.

6 계산 리소스에 대해 사용 가능한 경우 **리소스 풀** 드롭다운 메뉴에서 리소스 풀을 선택합니다.

7 네트워크 탭을 클릭합니다.

8 이 예약을 사용하여 프로비저닝된 시스템의 네트워크 경로를 구성합니다.

- a (선택 사항) 해당 옵션을 사용할 수 있는 경우, **끝점** 드롭다운 메뉴에서 스토리지 끝점을 선택합니다.

NetApp ONTAP 끝점이 있고 호스트가 가상 호스트이면 끝점 옆에 FlexClone 옵션이 표시됩니다 NetApp ONTAP 끝점이 있으면 스토리지 경로에 할당된 끝점이 예약 페이지에 표시됩니다. 스토리지 경로의 끝점을 추가, 업데이트 또는 삭제하면 적용되는 모든 예약에 변경 내용이 표시됩니다.

스토리지 경로의 끝점을 추가, 업데이트 또는 삭제하면 예약 페이지에 변경 내용이 표시됩니다.

- b **네트워크 경로** 목록에서 이 예약을 사용하여 프로비저닝된 시스템의 네트워크 경로를 선택합니다.

- c (선택 사항) 나열된 네트워크 프로파일을 **네트워크 프로파일** 드롭다운 메뉴에서 선택합니다.

이 옵션은 네트워크 프로파일이 하나 이상 있어야 사용할 수 있습니다.

예약에 네트워크 경로를 두 개 이상 선택할 수 있지만 시스템을 프로비저닝할 때는 네트워크 한 개만 사용됩니다.

이제 **저장**을 클릭하여 예약을 저장할 수 있습니다. 또는 사용자 지정 속성을 추가하여 예약 규격을 더 세부적으로 제어할 수 있습니다. 이 예약에 할당된 리소스가 줄어들 경우 알림을 보내도록 이메일 경고를 구성할 수도 있습니다.

가상 예약을 위한 사용자 지정 속성 및 경고 지정

사용자 지정 속성을 vRealize Automation 예약에 연결할 수 있습니다. 또한 예약 리소스가 부족한 경우 이메일 알림을 보내도록 경고를 구성할 수도 있습니다.

사용자 지정 속성 및 이메일 경고는 예약에 사용할 수 있는 선택적인 구성입니다. 사용자 지정 속성을 연결하거나 경고를 설정하지 않으려면 **저장**을 클릭하여 예약 생성을 완료하십시오.

사용자 지정 속성은 필요한 만큼 추가할 수 있습니다.

중요 알림은 이메일 경고가 구성되고 알림을 사용하도록 설정한 경우에만 전송됩니다.

경고를 구성한 경우, 경고는 지정한 임계값에 도달했을 때가 아니라 매일 생성됩니다.

필수 조건

가상 예약을 위한 리소스 및 네트워킹 설정 지정.

프로시저

- 1 속성 탭을 클릭합니다.
- 2 새로 만들기를 클릭합니다.
- 3 올바른 사용자 지정 속성 이름을 입력합니다.
- 4 해당하는 경우, 속성 값을 입력합니다.
- 5 (선택 사항) 속성 값을 암호화하려면 **암호화됨** 확인란을 선택합니다.

- 6 (선택 사항) 값을 입력하도록 사용자에게 요청하려면 **사용자에게 확인** 확인란을 선택합니다.
이 옵션은 프로비저닝 시에 재정의할 수 없습니다.
- 7 (선택 사항) 추가적인 사용자 지정 속성을 모두 추가합니다.
- 8 **경고** 탭을 클릭합니다.
- 9 **용량 경고** 확인란을 사용하도록 설정하여, 전송할 경고를 구성합니다.
- 10 슬라이더를 이용하여 사용 가능한 리소스 할당의 임계값을 설정합니다.
- 11 경고 알림을 수신할 AD 사용자 또는 그룹 이름(이메일 주소 아님)을 **받는 사람** 텍스트 상자에 입력합니다.
각 줄에 하나씩 이름을 입력합니다. Enter 키를 눌러 여러 항목을 구분합니다.
- 12 이메일 경고에 그룹 관리자를 포함하려면 **그룹 관리자에게 경고 보내기**를 선택합니다.
이메일 경고가 비즈니스 그룹 **관리자 이메일 수신인** 목록에 포함된 사용자에게 전송됩니다.
- 13 미리 알림 빈도(일)를 지정합니다.
- 14 **저장**을 클릭합니다.

예약이 저장되고 [예약] 목록에 표시됩니다.

후속 작업

선택적인 예약 정책을 구성하거나 프로비저닝 준비를 시작할 수 있습니다.

Blueprint를 생성할 수 있는 권한을 가진 사용자는 이제 Blueprint를 생성할 수 있습니다.

예약을 편집하여 네트워크 프로파일 할당

예를 들어 예약에서 프로비저닝된 시스템에 대한 정적 IP 할당을 사용하도록 설정하기 위해 해당 예약에 네트워크 프로파일을 할당할 수 있습니다.

새 **Blueprint** 또는 **Blueprint 속성** 페이지의 **속성** 탭에서 `VirtualMachine.NetworkN.ProfileName` 사용자 지정 속성을 사용하여 Blueprint에 네트워크 프로파일을 할당할 수도 있습니다.

예약과 Blueprint에 네트워크 프로파일을 지정하는 경우, Blueprint 값이 우선합니다. 예를 들어, `VirtualMachine.NetworkN.ProfileName` 사용자 지정 속성을 사용하여 Blueprint에 또는 Blueprint에 사용되는 예약에 네트워크 프로파일을 지정하면 Blueprint에 지정된 네트워크 프로파일이 우선합니다. 하지만 Blueprint에서 사용자 지정 속성이 사용되지 않고 사용자가 시스템 NIC를 위한 네트워크 프로파일을 선택하는 경우, vRealize Automation에서는 네트워크 프로파일이 지정되는 시스템 NIC에 대한 예약 네트워크 경로를 사용합니다.

참고 이 정보는 Amazon Web Services에는 적용되지 않습니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 네트워크 프로파일을 생성합니다. [네트워크 프로파일 생성](#)를 참조하십시오.

프로시저

- 1 **인프라 > 예약 > 예약**을 선택합니다.
- 2 예약을 가리키고 **편집**을 클릭합니다.
- 3 **네트워크** 탭을 클릭합니다.
- 4 네트워크 경로에 네트워크 프로파일을 할당합니다.
 - a 정적 IP 주소를 사용하도록 설정하려는 네트워크 경로를 선택합니다.
네트워크 경로 옵션은 **리소스** 탭의 설정에서 파생됩니다.
 - b **네트워크 프로파일** 드롭다운 메뉴에서 프로파일을 선택하여, 사용 가능한 네트워크 프로파일을 경로에 매핑합니다.
 - c (선택 사항) 이 단계를 반복하여 이 예약에서 추가적인 네트워크 경로에 네트워크 프로파일을 할당합니다.
- 5 **확인**을 클릭합니다.

예약 정책

예약 정책을 사용하면 예약 요청이 처리되는 방법을 제어할 수 있습니다. Blueprint에서 시스템을 프로비저닝하는 경우에는 예약 정책에 지정된 리소스만 프로비저닝할 수 있게 제한됩니다.

예약 정책은 예약 요청이 처리되는 방법을 제어하는 선택적인 수단을 제공합니다. Blueprint에 예약 정책을 적용하여 해당 Blueprint에서 프로비저닝된 시스템이 사용 가능한 일부 예약으로 제한되도록 할 수 있습니다.

예약 정책을 사용하면 리소스를 서비스 수준별로 여러 그룹에 수집하거나 특정 유형의 리소스를 특정 용도에 맞게 간편하게 제공할 수 있습니다. 사용자가 시스템을 요청하면 이 시스템은 필요한 용량이 충분히 있는 적절한 유형의 예약에 프로비저닝될 수 있습니다. 다음 시나리오에서는 예약 정책에 사용할 수 있는 몇 가지 예를 보여 줍니다.

- 프로비저닝된 시스템이 NetApp FlexClone을 지원하는 특정 디바이스와 함께 예약에 배치되도록 보장
- 특정 Blueprint에 필요한 시스템 이미지가 포함된 특정 영역에 클라우드 시스템이 프로비저닝되도록 제한
- 용량제 할당 모델 기능을 해당 기능을 지원하는 시스템 유형에 사용하기 위한 추가적인 수단

예약 정책에 예약을 여러 개 추가할 수 있지만 예약은 하나의 정책에만 속할 수 있습니다. 예약 정책 하나를 둘 이상의 Blueprint에 할당할 수 있습니다. Blueprint는 예약 정책을 하나만 사용할 수 있습니다.

참고 vCloud Air 끝점 및 vCloud Director 끝점에 정의된 예약은 시스템 프로비저닝에 대해 네트워크 프로파일의 사용을 지원하지 않습니다.

참고 플랫폼에서 SDRS를 사용하도록 설정한 경우에는 SDRS를 사용하여 개별 가상 시스템 디스크의 스토리지 또는 가상 시스템의 모든 스토리지를 로드 밸런싱할 수 있습니다. SDRS 데이터스토어 클러스터로 작업하는 경우 예약 정책과 스토리지 예약 정책을 사용할 때 충돌이 발생할 수 있습니다. 예를 들어 정책이나 스토리지 정책의 예약 중 하나에서 독립형 데이터스토어나 SDRS 클러스터 내의 데이터스토어를 선택하면 가상 시스템 스토리지가 SDRS를 기반으로 하지 않고 고정될 수 있습니다. SDRS 클러스터에 대한 스토리지 배치로 시스템에 대한 재프로비저닝을 요청하는 경우 SDRS 자동화 수준이 사용되지 않도록 설정되면 시스템이 삭제됩니다.

예약 정책 구성

예약 정책을 생성하여 리소스를 서비스 수준별로 여러 그룹에 수집하거나 특정 유형의 리소스를 특정 용도에 맞게 간편하게 제공할 수 있습니다. 예약 정책을 생성한 후 예약으로 채워야 테넌트 관리자와 비즈니스 그룹 관리자가 Blueprint에서 해당 정책을 효과적으로 사용할 수 있습니다.

예약 정책에는 서로 다른 유형의 예약이 포함될 수 있지만 특정 요청에 사용할 예약을 선택할 때는 Blueprint 유형에 맞는 예약만 고려됩니다.

프로시저

1 예약 정책 생성

예약 정책을 사용하여 유사한 예약을 함께 그룹화할 수 있습니다.

2 예약에 예약 정책 할당

예약을 생성할 때 예약에 예약 정책을 할당할 수 있습니다. 기존 예약을 편집하여 예약 정책을 할당하거나 예약 정책 할당을 변경할 수도 있습니다.

예약 정책 생성

예약 정책을 사용하여 유사한 예약을 함께 그룹화할 수 있습니다.

우선 예약 정책을 생성한 다음 예약에 정책을 추가하여 Blueprint 작성자가 Blueprint에서 예약 정책을 사용하도록 허용하십시오.

정책은 빈 컨테이너로 생성됩니다.

[예약 정책] 페이지에서 **유형별 필터링** 옵션을 사용하면 추가, 편집 또는 삭제 시 예약 정책의 표시 여부를 제어할 수 있습니다.

필수 조건

패브릭 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **인프라 > 예약 > 예약 정책**을 선택합니다.
- 2 **추가**를 클릭합니다.
- 3 **이름** 텍스트 상자에 이름을 입력합니다.
- 4 **유형** 드롭다운 메뉴에서 **예약 정책**을 선택합니다.
- 5 **설명** 텍스트 상자에 설명을 입력합니다.
- 6 **업데이트**를 클릭하여 정책을 저장합니다.

예약에 예약 정책 할당

예약을 생성할 때 예약에 예약 정책을 할당할 수 있습니다. 기존 예약을 편집하여 예약 정책을 할당하거나 예약 정책 할당을 변경할 수도 있습니다.

필수 조건

예약 정책 생성.

프로시저

- 1 **인프라 > 예약 > 예약**을 선택합니다.
- 2 예약을 가리키고 **편집**을 클릭합니다.
- 3 **예약 정책** 드롭다운 메뉴에서 예약 정책을 선택합니다.
- 4 **저장**을 클릭합니다.

스토리지 예약 정책

Blueprint 설계자가 vSphere, KVM (RHEV) 및 SCVMM 플랫폼 유형의 서로 다른 데이터스토어 또는 vCloud Air나 vCloud Director 리소스 같이 기타 리소스의 서로 다른 스토리지 프로파일에 가상 시스템의 볼륨을 할당할 수 있도록 스토리지 예약 정책을 생성할 수 있습니다.

가상 시스템의 볼륨을 서로 다른 데이터스토어 또는 서로 다른 스토리지 프로파일에 할당하면

Blueprint 설계자가 스토리지 공간을 보다 효과적으로 활용할 수 있습니다. 예를 들어 더 느리고 보다 저렴한 데이터스토어나 스토리지 프로파일에 운영 체제 볼륨을 배포하고, 더 빠른 데이터스토어나 스토리지 프로파일에 데이터베이스 볼륨을 배포할 수 있습니다.

일부 시스템 끝점은 단일 스토리지 프로파일만 지원하지만 여러 수준의 디스크 스토리지를 지원하는 시스템 끝점도 있습니다. 여러 수준의 디스크 스토리지는 vCloud Director 5.6 이상의 끝점과 vCloud Air 끝점에서 사용할 수 있습니다. 여러 수준의 디스크 스토리지는 vCloud Director 5.5 끝점에서 지원되지 않습니다.

Blueprint를 생성할 때 볼륨에 단일 데이터스토어를 할당하거나 여러 데이터스토어를 나타내는 스토리지 예약 정책을 할당할 수 있습니다. Blueprint 설계자가 볼륨에 단일 데이터스토어 또는 스토리지 프로파일을 할당하면 vRealize Automation에서는 가능한 경우 해당 데이터스토어 또는 스토리지 프로파일을 프로비저닝 시간에 사용합니다. 설계자가 볼륨에 스토리지 예약 정책을 할당하면 vRealize Automation에서는 vCloud Air 또는 vCloud Director 같은 다른 리소스로 작업할 경우, 해당 정책의 데이터스토어 또는 스토리지 프로파일을 프로비저닝 시간에 사용합니다.

스토리지 예약 정책은 기본적으로 유사한 특성(예: 속도 또는 가격)을 가진 데이터스토어나 스토리지 프로파일을 그룹화하기 위해 패브릭 관리자가 하나 이상의 데이터스토어 또는 스토리지 프로파일에 적용하는 태그입니다. 데이터스토어 또는 스토리지 프로파일은 한 번에 하나의 스토리지 예약 정책에만 할당할 수 있지만 스토리지 예약 정책은 여러 가지 다른 데이터스토어를 가질 수 있습니다.

스토리지 예약 정책을 생성한 후 하나 이상의 데이터스토어 또는 스토리지 프로파일에 할당할 수 있습니다. 그러면 Blueprint 생성자가 가상 Blueprint의 볼륨에 스토리지 예약 정책을 할당합니다. 사용자가 Blueprint를 사용하는 시스템을 요청하는 경우 vRealize Automation는 Blueprint에 지정된 스토리지 예약 정책을 사용하여 시스템의 볼륨에 사용할 데이터스토어나 스토리지 프로파일을 선택합니다.

참고 플랫폼에서 SDRS를 사용하도록 설정한 경우에는 SDRS를 사용하여 개별 가상 시스템 디스크의 스토리지 또는 가상 시스템의 모든 스토리지를 로드 밸런싱할 수 있습니다. SDRS 데이터스토어 클러스터로 작업하는 경우 예약 정책과 스토리지 예약 정책을 사용할 때 충돌이 발생할 수 있습니다. 예를 들어 정책이나 스토리지 정책의 예약 중 하나에서 독립형 데이터스토어나 SDRS 클러스터 내의 데이터스토어를 선택하면 가상 시스템 스토리지가 SDRS를 기반으로 하지 않고 고정될 수 있습니다. SDRS 클러스터에 대한 스토리지 배치로 시스템에 대한 재프로비저닝을 요청하는 경우 SDRS 자동화 수준이 사용되지 않도록 설정되면 시스템이 삭제됩니다.

예약에 의해 프로비저닝된 시스템에 할당된 스토리지와 메모리는 해당 시스템이 vRealize Automation에서 [제거] 작업에 의해 삭제될 때 해제됩니다. 시스템이 vCenter Server에서 삭제되는 경우에는 스토리지와 메모리가 해제되지 않습니다.

예를 들어 기존 배포에 포함된 시스템과 연결되어 있는 예약은 삭제할 수 없습니다. vCenter Server에서 배포된 시스템을 수동으로 이동하거나 삭제할 경우, vRealize Automation에서는 배포된 시스템을 라이브 상태로 계속 인식하기 때문에 연결된 예약을 삭제하지 못합니다.

스토리지 예약 정책 구성

스토리지 예약 정책을 생성하여 속도나 가격과 같은 유사한 특성을 가진 데이터스토어를 그룹화할 수 있습니다. 스토리지 예약 정책을 생성한 후 데이터스토어로 채운 다음 Blueprint에서 해당 정책을 사용해야 합니다.

프로시저

1 스토리지 예약 정책 생성

스토리지 예약 정책을 사용하여 속도나 가격과 같은 유사한 특성을 가진 데이터스토어를 그룹화할 수 있습니다.

2 데이터스토어에 스토리지 예약 정책 할당

스토리지 예약 정책을 계산 리소스에 연결할 수 있습니다. 스토리지 예약 정책이 생성되면 데이터스토어로 채웁니다. 하나의 데이터스토어는 단 하나의 스토리지 예약 정책에만 포함될 수 있습니다. Blueprint에서 사용할 데이터스토어 그룹을 생성하려면 여러 데이터스토어를 추가합니다.

스토리지 예약 정책 생성

스토리지 예약 정책을 사용하여 속도나 가격과 같은 유사한 특성을 가진 데이터스토어를 그룹화할 수 있습니다.

정책은 빈 컨테이너로 생성됩니다.

[예약 정책] 페이지에서 **유형별 필터링** 옵션을 사용하면 추가, 편집 또는 삭제 시 예약 정책의 표시 여부를 제어할 수 있습니다.

필수 조건

패브릭 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **인프라 > 예약 > 예약 정책**을 선택합니다.
- 2 **추가**를 클릭합니다.
- 3 **이름** 텍스트 상자에 이름을 입력합니다.
- 4 **유형** 드롭다운 메뉴에서 **스토리지 예약 정책**을 선택합니다.
- 5 **설명** 텍스트 상자에 설명을 입력합니다.
- 6 **업데이트**를 클릭하여 정책을 저장합니다.


데이터스토어에 스토리지 예약 정책 할당

스토리지 예약 정책을 계산 리소스에 연결할 수 있습니다. 스토리지 예약 정책이 생성되면 데이터스토어로 채웁니다. 하나의 데이터스토어는 단 하나의 스토리지 예약 정책에만 포함될 수 있습니다. Blueprint에서 사용할 데이터스토어 그룹을 생성하려면 여러 데이터스토어를 추가합니다.


필수 조건

[스토리지 예약 정책 생성](#).

프로시저

- 1 **인프라 > 계산 리소스 > 계산 리소스**를 선택합니다.
- 2 계산 리소스를 가리키고 **편집**을 클릭합니다.
- 3 **구성** 탭을 클릭합니다.
- 4 스토리지 테이블의 스토리지 예약 정책에 추가할 데이터스토어를 찾습니다.
- 5 원하는 **Storage Path** 개체 옆에 있는 **편집** 아이콘()을 클릭합니다.
- 6 **스토리지 예약 정책** 열 드롭다운 메뉴에서 스토리지 예약 정책을 선택합니다.

시스템을 프로비저닝한 후에는 스토리지 예약 정책을 변경할 수 없습니다. 변경하는 경우 디스크의 스토리지 프로파일이 변경됩니다.

- 7 **저장** 아이콘()을 클릭합니다.
- 8 **확인**을 클릭합니다.
- 9 (선택 사항) 스토리지 예약 정책에 추가 데이터스토어를 할당합니다.

워크로드 배치

Blueprint를 배포할 때 워크로드 배치는 수집된 데이터를 사용하여, 사용 가능한 리소스를 기반으로 Blueprint 배치 위치를 권장합니다. vRealize Automation 및 vRealize Operations Manager는 함께 작동하여 새로운 Blueprint를 배포할 때 워크로드의 배치 권장 사항을 제공합니다.

vRealize Automation은 비즈니스 그룹, 예약 및 할당량 같은 조직 정책을 관리하면서 vRealize Operations Manager의 용량 분석과 통합하여 시스템을 배치합니다. 워크로드 배치는 vSphere 끝점에 대해서만 사용할 수 있습니다.

사용된 워크로드 배치 용어

워크로드 배치에 몇 가지 용어가 사용됩니다.

- vSphere의 클러스터는 vRealize Automation의 계산 리소스에 매핑됩니다.
- 예약에는 계산과 스토리지가 포함되며, 스토리지는 개별 데이터스토어 또는 데이터스토어 클러스터로 구성될 수 있습니다. 예약에는 여러 데이터스토어, 데이터스토어 클러스터 또는 둘 모두 포함될 수 있습니다.
- 여러 예약이 동일한 클러스터를 참조할 수 있습니다.
- 가상 시스템을 여러 클러스터로 이동할 수 있습니다.
- 워크로드 배치를 사용하도록 설정하면 프로비저닝 워크플로는 배치 정책을 사용하여 Blueprint를 배치할 위치를 권장합니다.

워크로드 배치를 사용하여 Blueprint 프로비저닝

워크로드 배치를 사용하여 Blueprint를 배치하면 프로비저닝 워크플로는 vRealize Automation의 예약과 vRealize Operations Manager의 배치 최적화를 사용합니다.

- 1 vRealize Automation은 배치 대상을 허용하는 거버넌스 규칙을 제공합니다.
- 2 vRealize Operations Manager는 분석 데이터를 기준으로 배치 최적화 권장 사항을 제공합니다.
- 3 vRealize Automation은 vRealize Operations Manager의 배치 권장 사항에 따라 프로비저닝 프로세스를 계속합니다.

vRealize Operations Manager가 권장 사항을 제공할 수 없거나, 권장 사항을 사용할 수 없으면 vRealize Automation은 기본 배치 논리로 돌아갑니다.

개발자가 카탈로그 항목을 선택하고 양식을 완성하여 카탈로그 항목을 요청하면 vRealize Automation이 다음 고려 사항에 따라 가상 시스템을 프로비저닝합니다.

표 2-16. 가상 시스템 프로비저닝 고려 사항

고려 사항	효과
정책	vRealize Automation 예약 정책이 둘 이상의 예약을 나타낼 수 있습니다.
예약	<p>vRealize Automation은 요청을 평가하고, 요청에 포함된 제약 조건을 충족할 수 있는 예약을 결정합니다.</p> <ul style="list-style-type: none"> 배치가 사용되고 vRealize Operations Manager 분석에 기반하는 경우 vRealize Automation은 vRealize Operations Manager로 예약 목록을 전달하여 운영 메트릭을 기반으로 배치에 가장 적합한 예약을 결정합니다. 배치가 vRealize Operations Manager에 기반하지 않는 경우 vRealize Automation은 우선 순위 및 가용성을 기준으로 배치를 결정합니다. <p>리소스가 사용되었는지 추적하기 위해 예약이 업데이트됩니다.</p> <p>vRealize Operations Manager가 권장하는 클러스터 또는 데이터스토어를 vRealize Automation에서 용량이 부족하거나 더 이상 적용할 수 없다고 판단하는 경우 vRealize Automation에서 예외를 기록합니다. vRealize Automation은 기본 배치 메커니즘에 따라 프로비저닝을 계속할 수 있습니다.</p>

가상 시스템의 리소스를 식별하기 위해 vRealize Automation은 후보 예약 목록을 제공합니다. 목록 내의 각 후보는 클러스터 및 하나 이상의 데이터스토어 또는 데이터스토어 클러스터를 포함할 수 있습니다. vRealize Operations Manager는 후보 예약을 사용하여 대상 후보 목록을 생성하고 최적의 대상을 찾습니다.

vRealize Operations Manager의 정책은 클러스터에 대한 밸런스 수준, 활용률 및 버퍼 공간을 설정합니다. 단일 예약, 즉 클러스터 또는 데이터스토어 클러스터의 경우 vRealize Automation은 권장 사항이 실행 가능한 배치 대상인지 여부를 검증합니다.

- 대상이 실행 가능하면 vRealize Automation은 권장 사항에 따라 Blueprint를 배포합니다.
- 대상이 실행 가능하지 않으면 vRealize Automation은 기본 배치 동작을 사용하여 가상 시스템을 배치합니다.

배치 고려 사항에서는 상태 및 활용률 문제도 고려해야 합니다. 클라우드 관리자와 가상 인프라 관리자는 인프라를 관리하지만, 개발자는 애플리케이션의 상태를 중요하게 생각합니다. 이러한 개발자를 지원하려면 워크로드 배치 전략에서 상태 및 활용률 문제도 고려해야 합니다.

표 2-17. 상태 및 활용도 문제에 대한 고려 사항

워크로드 문제	배치 솔루션
개발자가 환경에서 상태 문제를 발견했습니다.	vRealize Automation이 문제가 발생하거나 대규모 워크로드에 의해 초과 활용된 클러스터에 Blueprint를 프로비저닝합니다. vRealize Automation은 vRealize Operations Manager의 용량 분석을 통합하여 충분한 용량을 갖춘 클러스터에서 Blueprint를 프로비저닝해야 합니다.
개발자가 활용률 문제를 발견했습니다.	환경의 클러스터가 충분히 활용되지 않습니다. vRealize Automation은 vRealize Operations Manager가 제공하는 용량 분석을 통합하여 활용도가 최대화되는 클러스터에 Blueprint를 프로비저닝해야 합니다.

Blueprint를 프로비저닝하는 사용자

다음과 같은 사용자가 Blueprint를 프로비저닝하는 작업을 수행합니다.

표 2-18. Blueprint를 프로비저닝하기 위한 사용자 및 역할

단계	사용자	작업	필요한 역할
1	클라우드 관리자 또는 VI(가상 인프라) 관리자	가상 시스템의 초기 배치가 조직 정책을 준수하는지, 운영 분석 데이터에 따라 최적화되었는지 확인합니다.	IaaS 관리자 역할
1	패브릭 관리자	vRealize Automation에서 예약, 예약 정책 및 배치 정책을 정의합니다.	패브릭 관리자 역할, 인프라 설계자
1	IaaS 관리자	워크로드 배치에 필요한 vSphere 및 vRealize Operations Manager 끝점을 정의합니다.	IaaS 관리자 역할
2	인프라 설계자	가상 시스템 구성 요소 유형에 대해 직접 작업하는 Blueprint 설계자로서, Blueprint 작성 시 가상 시스템에 예약 정책을 할당합니다. 예약 정책을 Blueprint에 가상 시스템의 속성으로 지정합니다.	인프라 설계자
3	인프라 설계자, 애플리케이션 설계자, 소프트웨어 설계자 및 XaaS 설계자	<p>가상 시스템을 프로비저닝하는 Blueprint를 생성하고 게시합니다. 인프라 설계자만 시스템 구성 요소에 대해 직접 작업합니다. 다른 설계자 역할에서는 중첩 시 인프라 Blueprint를 다시 사용할 수 있지만 시스템 구성 요소 설정을 편집할 수 없습니다.</p> <p>Blueprint에는 단일 구성 요소가 포함되거나, 중첩된 Blueprint, XaaS 구성 요소, 다중 계층 애플리케이션의 여러 가상 시스템 등이 포함될 수 있습니다.</p> <p>vRealize Automation은 예약 구성에 따라 가상 시스템을 배치하고 필요한 경우 Blueprint의 시스템 구성 요소 수준에서 예약 정책을 포함합니다. 예를 들어 Blueprint에는 시스템별로 서로 다른 정책이 적용되는 두 개의 시스템이 포함될 수 있습니다.</p> <p>또한 vRealize Automation은 vRealize Operations Manager가 제공하는 운영 분석 데이터에 따라 가상 시스템을 최적화합니다.</p>	인프라 설계자
4	클라우드 관리자 또는 VI 관리자	<p>vRealize Automation이 프로비저닝하는 가상 시스템의 초기 배치를 제어하는 정책을 선택합니다.</p> <p>관리자는 다음을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> ■ API를 사용하여 정책을 선택합니다. ■ 워크로드의 밸런싱을 위해 vRealize Automation에서 각 서버를 차례로 사용하는 라운드 기본 배치 정책을 사용합니다. 이 접근 방식을 사용할 경우 vRealize Operations Manager의 입력이 필요하지 않습니다. 	IaaS 관리자 역할, 인프라 설계자
5	VI 관리자	vRealize Operations Manager에서 사용자 지정 데이터 센터 및 사용자 지정 그룹을 구축합니다. 그런 다음 VI 관리자는 해당 사용자 지정 데이터 센터에 대한 워크로드를 통합하고 밸런싱하는 데 사용되는 정책을 적용합니다.	IaaS 관리자 역할, 인프라 설계자
6	패브릭 관리자	<p>vRealize Automation에서 배치 정책을 선택합니다.</p> <p>워크로드 배치 정책을 사용하여 새 Blueprint를 배포할 때 vRealize Automation이 시스템을 배치하는 위치를 결정할 수 있게 합니다. 배치 정책에는 vRealize Operations Manager의 입력이 필요합니다.</p>	패브릭 관리자 역할

표 2-18. Blueprint를 프로비저닝하기 위한 사용자 및 역할 (계속)

단계	사용자	작업	필요한 역할
7	개발자	가상 시스템을 프로비저닝하기 위한 Blueprint를 요청합니다. Blueprint는 3계층 애플리케이션을 실행하는 여러 시스템으로 구성될 수 있습니다.	
8	개발자	개발자가 Blueprint를 배포할 경우 vRealize Operations Manager는 요청에 대한 관련 클러스터에 맞는 배치 정책을 검색합니다.	

배치 정책에 대한 자세한 내용은 [배치 정책](#) 항목을 참조하십시오.

워크로드 배치를 구성하려면 [워크로드 배치 구성](#) 항목을 참조하십시오.

가상 시스템을 배치하는 데 DRS(Distributed Resource Scheduler)가 필요함

vSphere DRS는 vRealize Automation 및 vRealize Operations Manager에서 가상 시스템을 프로비저닝하고 배치하는 데 사용하는 배치 엔진입니다.

vRealize Automation이 가상 시스템에 대한 최상의 배치를 제안하려면 클러스터에서 DRS를 사용하도록 설정하고 완전히 자동화하도록 설정해야 합니다. 그러면 vRealize Automation은 vSphere DRS API를 사용하여 가상 시스템의 올바른 배치를 결정합니다.

vRealize Automation은 vRealize Operations Manager 배치 서비스와 통합됩니다.

vRealize Operations Manager는 DRS를 사용하도록 설정되고 완전히 자동화되어 있는 클러스터에 대해서만 배치 권장 정보를 제공합니다.

워크로드 배치에 대한 제한 사항

새 Blueprint를 배포할 때 워크로드 배치를 위한 배치 정책을 사용하여 시스템을 배치할 경우, 다음의 제한 사항에 유의하십시오.

- vRealize Operations Manager에서 vRealize Automation 솔루션은 vRealize Automation이 관리하는 클러스터 및 가상 시스템을 식별합니다.
- vRealize Automation이 vRealize Operations Manager에서 데이터 센터 또는 사용자 지정 데이터 센터 컨테이너의 하위 개체를 관리할 경우에는 해당 개체를 재조정 또는 이동하는 기능을 사용할 수 없습니다. vRealize Automation의 관리 개체에 대해 작업 제외를 설정하거나 해제할 수 없습니다.
- vRealize Automation이 관리하는 개체의 경우 워크로드 배치 동작은 다음과 같습니다.
 - 사용자 지정 데이터 센터 또는 데이터 센터에 vRealize Automation이 관리하는 클러스터가 포함된 경우 워크로드 배치에서 클러스터 재조정을 허용하지 않습니다.
 - 클러스터에 vRealize Automation이 관리하는 가상 시스템이 포함된 경우 워크로드 배치 시 해당 가상 시스템을 이동할 수 없습니다.
- vRealize Operations Manager는 vCenter Server에서 리소스 풀에 대한 워크로드 배치를 지원하지 않습니다.
- vRealize Operations Manager는 현재 릴리스에서 vSAN을 지원하지 않습니다.

워크로드 배치 구성 권한

워크로드 배치 및 배치 정책을 사용하려면 vRealize Automation 및 vRealize Operations Manager에서 구성 권한이 있어야 합니다.

vRealize Automation에서 워크로드 배치를 구성하려면 패브릭 관리자 역할이 있어야 합니다. vRealize Automation 정보 센터에서 사용자 역할 개요를 참조하십시오.

vRealize Operations Manager에서, 워크로드 배치를 위한 사용자 역할을 생성하고 해당 역할에 사용 권한을 할당해야 합니다.

- 사용자 계정에서 vSphere 호스트 및 클러스터에 대한 읽기 전용 사용 권한을 할당하고 개체 계층에서 vSphere 스토리지에 대한 읽기 전용 사용 권한을 할당합니다.
- 워크로드 배치 시 사용자 역할이 API 호출을 사용할 수 있으려면 API에 읽기 및 쓰기 사용 권한을 할당합니다. **관리 > 액세스 제어 > 사용 권한**을 선택하고 **REST API > 다른 모든 읽기, 쓰기 API**를 선택합니다.

vRealize Automation은 사용자가 끝점을 등록할 때 그리고 카탈로그 항목을 요청하는 사용자를 대신해 프로비저닝하는 동안 배치 권장 사항을 요청하기 위해 vRealize Operations Manager 역할을 사용합니다.

자세한 내용은 vRealize Operations Manager 정보 센터에서 액세스 제어를 참조하십시오.

배치 정책

배치 정책을 사용하여 새 Blueprint를 배포할 때 vRealize Automation이 시스템을 배치하는 위치를 결정할 수 있게 합니다. 배치 정책에서는 vRealize Operations Manager의 분석을 사용하여 클러스터의 워크로드를 식별하는 방식으로 배치 대상을 제안할 수 있습니다.

배치 정책을 사용하려면 먼저 여러 단계를 수행해야 합니다. vRealize Automation에서 vRealize Operations Manager 및 vCenter Server 인스턴스에 대한 끝점을 생성합니다. 그런 다음 패브릭 그룹을 생성하고 vCenter Server 끝점에 예약을 추가합니다.

vRealize Operations Manager에서 vRealize Automation에 워크로드 배치 분석을 제공할 수 있도록 다음을 수행해야 합니다.

- 워크로드 배치에 사용되는 vRealize Operations Manager 인스턴스에 vRealize Automation 솔루션을 설치합니다.
- vCenter Server를 모니터링하도록 vRealize Operations Manager를 구성합니다.

워크로드 배치를 위해 vRealize Automation 및 vRealize Operations Manager를 구성하려면 [워크로드 배치 구성](#) 항목을 참조하십시오.

배치 정책 찾기

vRealize Automation 인스턴스에서 **인프라 > 예약 > 배치 정책**을 선택합니다.

vRealize Operations Manager가 제공하는 워크로드 배치 분석을 사용하려면 **배치 권장 사항에 대해 vRealize Operations Manager 사용**을 선택합니다.

워크로드 배치 정책을 사용하지 않으면 vRealize Automation은 기본 배치 방법을 사용합니다.

워크로드 배치 구성

새 Blueprint를 배포할 때 배치 정책을 사용하여 시스템을 배치하려면

vRealize Operations Manager가 제공하는 분석을 사용하도록 vRealize Automation을 구성합니다. 클러스터 계산 리소스에 대한 워크로드를 통합하고 균형을 조정하는 정책을 적용하도록 vRealize Operations Manager를 구성할 수도 있습니다.

vRealize Automation에서 끝점을 구성하고, 패브릭 그룹을 생성하고, 예약을 추가합니다.

vRealize Operations Manager에서 워크로드 균형 조정을 지원하도록 정책을 구성하고 해당 정책을 사용자 지정 계산 리소스가 포함된 사용자 지정 그룹에 적용합니다.

필수 조건

배치 정책이 Blueprint에 대한 배치 대상을 제안할 수 있으려면 먼저 몇 가지 단계를 수행해야 합니다.

- 배치 정책을 이해합니다. [배치 정책](#) 항목을 참조하십시오.
- 워크로드 배치에 사용 중인 vRealize Operations Manager 인스턴스에 대해 vRealize Automation에 끝점이 있는지 확인합니다. [vRealize Operations Manager 끝점 생성](#) 항목을 참조하십시오.
- vCenter Server 인스턴스에 대해 vRealize Automation에 끝점이 있는지 확인합니다. [vSphere 끝점 생성](#) 항목을 참조하십시오.
- vCenter Server 끝점에 예약을 추가합니다. [예약](#) 항목을 참조하십시오.
- 패브릭 그룹을 추가하고 사용자가 패브릭 그룹 관리자인지 확인합니다. [패브릭 그룹 생성](#) 항목을 참조하십시오.
- 동일한 vCenter Server 인스턴스를 포함하는지 확인하기 위해 vRealize Operations Manager가 vRealize Automation이 모니터링하는 인프라와 동일한 인프라를 모니터링하는지 확인합니다. vRealize Operations Manager 정보 센터에서 [vRealize Operations Manager의 VMware vSphere 솔루션](#)을 참조하십시오.
- 예약, 스토리지 예약, Blueprint 및 위임 제공자를 이해합니다. vRealize Automation 정보 센터를 참조하십시오.
- 워크로드 배치에 사용된 vRealize Operations Manager 정책의 채우기 및 균형 조정 설정을 이해하고 정의합니다. vRealize Operations Manager 정보 센터에서 [워크로드 자동화 세부 정보](#)를 참조하십시오.

프로시저

1 워크로드 배치를 위한 vRealize Automation 구성

새 Blueprint를 배포할 때 워크로드 배치 분석을 사용하여 시스템을 배치하려면 vRealize Automation 인스턴스를 준비해야 합니다.

2 vRealize Automation에서 워크로드 배치를 위해 vRealize Operations Manager 구성

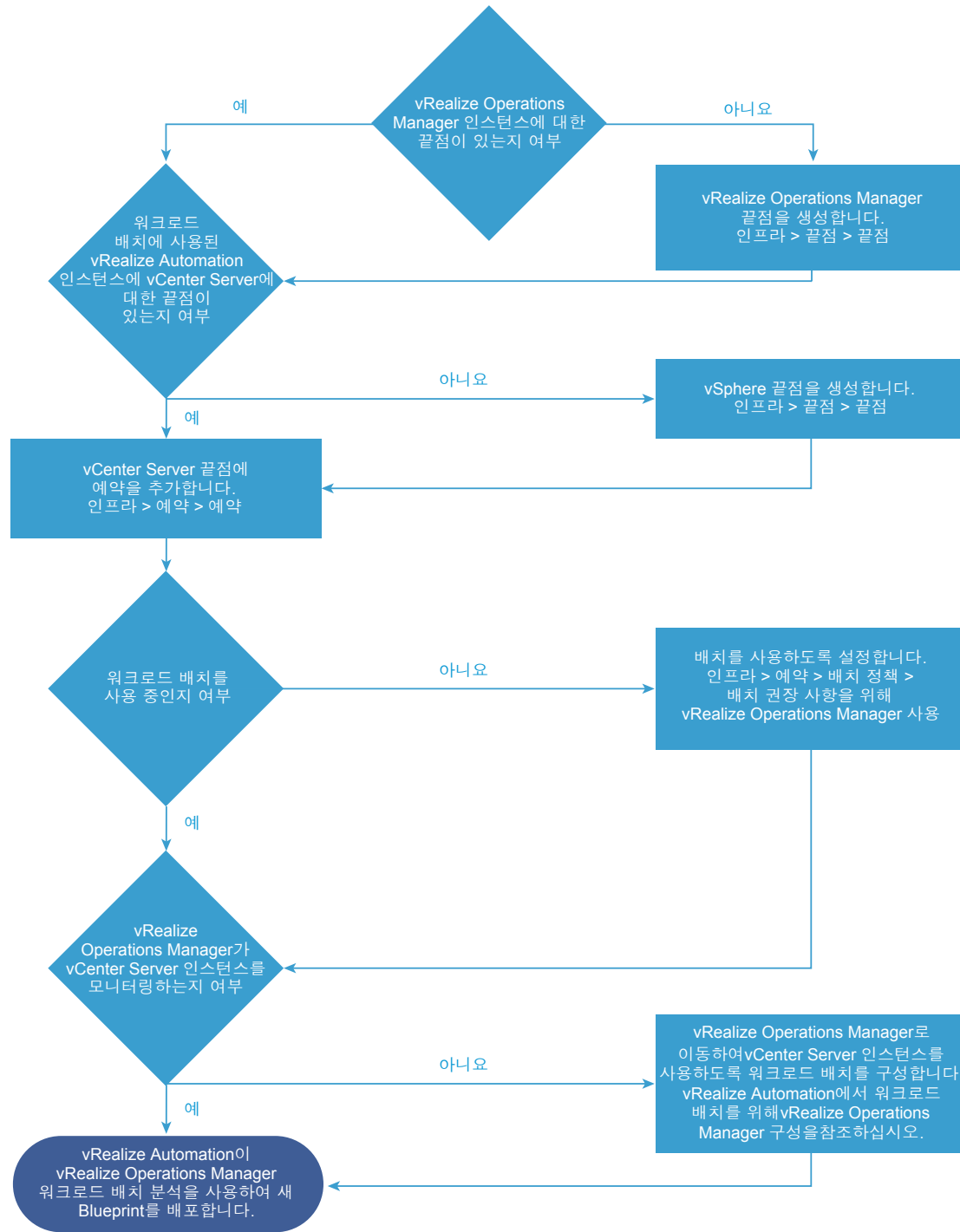
새 Blueprint를 배포할 때 시스템을 배치하기 위해 vRealize Automation에 워크로드 배치 분석을 제공하려면 vRealize Operations Manager 인스턴스를 준비해야 합니다.

워크로드 배치 분석을 사용하여 새 Blueprint에 대한 배치 대상을 제안하도록 vRealize Automation 및 vRealize Operations Manager를 구성했습니다.

워크로드 배치를 위한 vRealize Automation 구성

새 Blueprint를 배포할 때 워크로드 배치 분석을 사용하여 시스템을 배치하려면 vRealize Automation 인스턴스를 준비해야 합니다.

배치 정책을 사용하도록 vRealize Automation 인스턴스를 준비하려면 끝점을 구성하고, 패브릭 그룹을 생성하고, 예약을 추가합니다.



필수 조건

- 워크로드 배치를 사용하려면 요구 사항을 이해해야 합니다. [워크로드 배치 구성](#) 항목을 참조하십시오.
- vRealize Automation에서, 자격 증명을 검증하도록 vRealize Operations Manager에 대한 특정 사용자 역할 및 사용 권한을 추가합니다. vRealize Automation 정보 센터에서 사용자 역할 개요를 참조하십시오.

프로시저

- 1 vRealize Automation 인스턴스에서 vRealize Operations Manager 인스턴스에 대한 끝점을 추가하고 **확인**을 클릭합니다.
 - a **인프라 > 끝점 > 끝점**을 선택합니다.
 - b **새로 만들기 > 관리 > vRealize Operations Manager**를 선택합니다.
 - c **vRealize Operations Manager** 끝점에 대한 일반 정보를 입력합니다.
 끝점에 대한 속성은 지정할 필요가 없습니다.
- 2 vRealize Automation 인스턴스에서 vCenter Server 인스턴스에 대한 끝점을 추가하고 **확인**을 클릭합니다.
 - a **인프라 > 끝점 > 끝점**을 선택합니다.
 - b **새로 만들기 > 가상 > vSphere(vCenter)**를 선택합니다.
 - c vCenter Server 끝점에 대한 일반 정보, 속성 및 연결을 입력합니다.
 끝점을 추가한 후 vRealize Automation이 끝점에서 데이터를 수집하면 해당 끝점에 대한 계산 리소스를 사용할 수 있습니다. 그런 다음 생성하는 패브릭 그룹에 해당 계산 리소스를 추가할 수 있습니다.
- 3 다른 사용자가 예약을 생성하고 배치 정책을 사용하도록 설정할 수 있게 패브릭 그룹을 생성합니다.
 - a **인프라 > 끝점 > 패브릭 그룹**을 선택합니다.
 - b **새로 만들기**를 클릭하고 패브릭 그룹에 대한 정보를 입력합니다.

옵션	설명
이름	패브릭 그룹의 의미 있는 이름을 입력합니다.
설명	유용한 설명을 입력합니다.
패브릭 관리자	패브릭 관리자로 지정할 각 사용자의 이메일 주소를 입력합니다.
계산 리소스	관리자가 관리할 수 있는 계산 리소스 클러스터를 선택합니다.

패브릭 그룹에 계산 리소스를 추가한 후 vRealize Automation이 끝점에서 데이터를 수집하면 패브릭 관리자가 계산 리소스에 대한 예약을 생성할 수 있습니다.

4 vCenter Server 인스턴스에서 계산 리소스에 대한 예약을 생성합니다.

- a 인프라 > 예약 > 예약을 선택합니다.
- b 새로 만들기 > vSphere(vCenter)를 선택합니다.
- c 각 탭에서 예약에 대한 정보를 입력합니다.

옵션	작업
일반	예약 정책, 정책에 대한 우선 순위를 선택하고 이 예약 사용 을 클릭합니다.
리소스	시스템 할당량, 메모리 및 스토리지를 선택합니다. 리소스 풀은 선택할 필요가 없습니다.
네트워크	네트워크 어댑터를 선택합니다. 네트워크 프로파일은 선택할 필요가 없습니다.
속성	필요한 경우 사용자 지정 속성을 예약에 추가합니다.
경고	필요한 경우 용량이 예약에 대한 임계값을 초과하면 받는 사람에게 알리도록 용량 경고 를 선택합니다.

5 배치 정책을 사용하도록 설정합니다.

- a 인프라 > 예약 > 배치 정책을 선택합니다.
- b 배치 권장 사항을 위해 **vRealize Operations Manager 사용** 확인란을 선택합니다.

사용자가 Blueprint를 배포할 때 vRealize Automation이 vRealize Operations Manager 분석을 사용하여 시스템을 배치하도록 구성했습니다.

후속 작업

vCenter Server 인스턴스를 모니터링하도록 vRealize Operations Manager를 구성하고 클러스터 계산 리소스에 워크로드 배치 정책을 적용합니다. [vRealize Automation에서 워크로드 배치를 위해 vRealize Operations Manager 구성](#) 항목을 참조하십시오.

vRealize Automation에서 워크로드 배치를 위해 vRealize Operations Manager 구성

새 Blueprint를 배포할 때 시스템을 배치하기 위해 vRealize Automation에 워크로드 배치 분석을 제공하려면 vRealize Operations Manager 인스턴스를 준비해야 합니다.

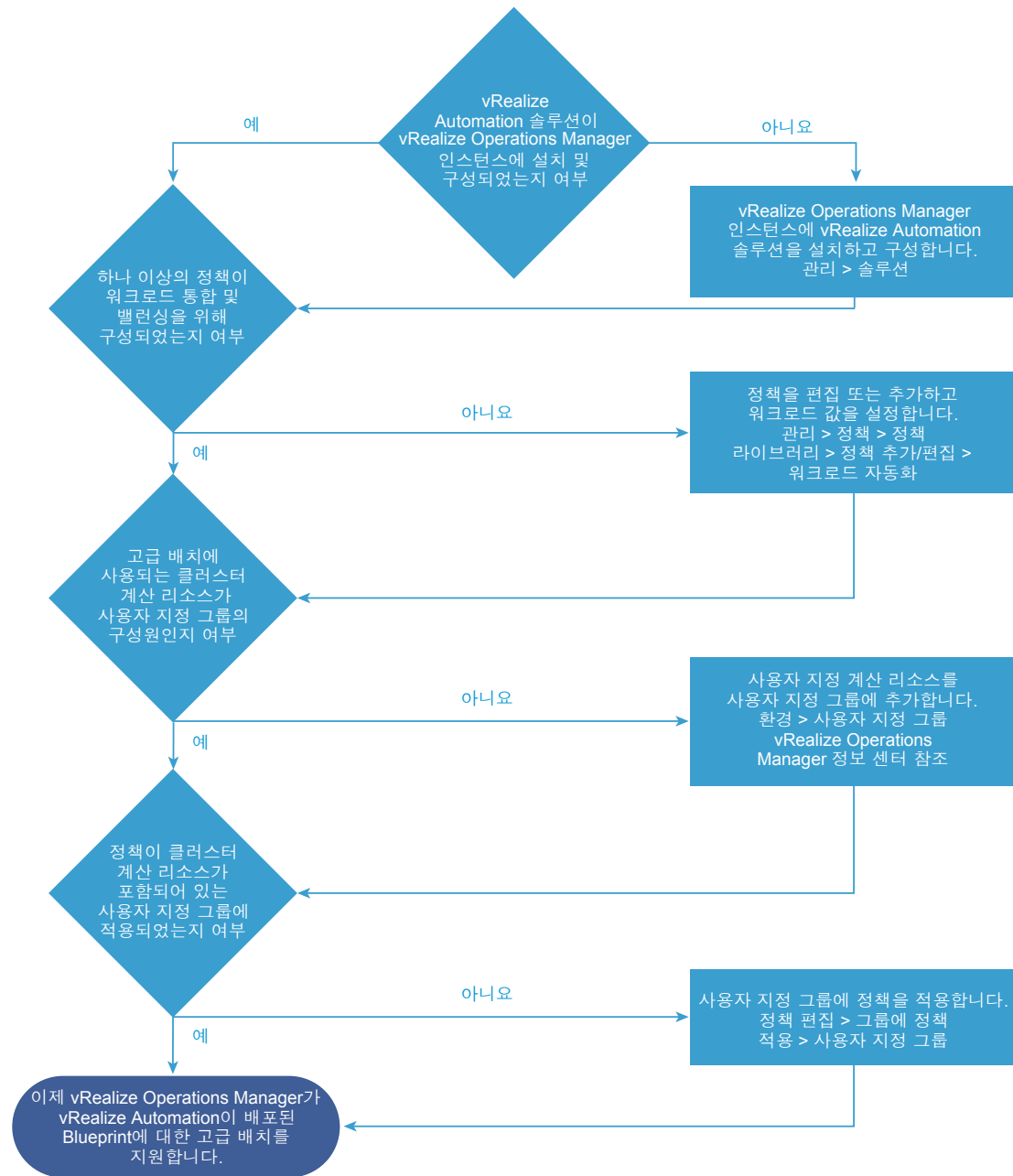
주의 관리 팩이 포함된 vRealize Automation 솔루션은 단일 vRealize Operations Manager 인스턴스에만 설치해야 합니다.

vRealize Automation에 분석을 제공하도록 vRealize Operations Manager 인스턴스를 준비하려면 vRealize Automation 솔루션을 설치 및 구성합니다. 또한 정책을 구성하고 이 정책을 클러스터 계산 리소스에 적용해야 합니다.

vRealize Automation 솔루션을 구성한 후에는 vRealize Automation이 관리하는 가상 시스템을 이동하거나 재조정할 수 없습니다.

vRealize Automation 솔루션이 vRealize Operations Manager 인스턴스에 설치되어 있지 않은 경우에도 vRealize Automation이 관리하는 가상 시스템을 워크로드 배치가 이동하거나 재조정할 수 있습니다.

워크로드 배치가 가상 시스템을 이동할 수 있으려면 해당 가상 시스템이 데이터 센터 또는 사용자 지정 데이터 센터에 있어야 합니다.



필수 조건

- 워크로드 배치 분석을 사용하도록 vRealize Automation을 구성합니다. 워크로드 배치를 위한 [vRealize Automation 구성](#) 항목을 참조하십시오.

- 워크로드 배치에 사용 중인 vRealize Operations Manager 인스턴스에 vRealize Automation 솔루션이 설치 및 구성되어 있는지 확인합니다. 이 솔루션에 대한 자세한 내용은 [Solution Exchange의 vRealize Automation에 대한 관리 팩](#)을 참조하십시오.
vRealize Operations Manager에서 워크로드 배치가 작동하는 방식에 대한 자세한 내용은 vRealize Operations Manager 설명서에서 [워크로드 자동화 세부 정보](#) 및 관련 항목을 참조하십시오.

프로시저

- 1 워크로드 배치를 관리하는 vRealize Operations Manager 인스턴스에서 vRealize Automation 솔루션을 설치 및 구성합니다.
 솔루션이 이미 설치되었을 수 있습니다.
 - a vRealize Operations Manager에 설치된 솔루션을 보려면 **관리 > 솔루션**을 클릭합니다.
 - b vRealize Automation 솔루션이 이미 설치되어 있는지 확인합니다.
 vRealize Automation 솔루션이 목록에 표시되지 않으면 솔루션을 다운로드하여 설치합니다. [Solution Exchange의 vRealize Automation에 대한 관리 팩](#)을 참조하십시오.
 - c 솔루션이 목록에 표시되면 **VMware vRealize Automation 솔루션**을 선택하고 **구성**을 클릭합니다.
 - d vRealize Automation 솔루션을 구성하고 설정을 저장합니다.
 솔루션 구성에 대한 자세한 내용은 vRealize Operations Manager 정보 센터에서 [vRealize Operations Manager의 솔루션](#)을 참조하십시오.
- 2 vRealize Operations Manager 기본 정책을 사용하지 않을 경우 사용자 지정 그룹을 생성해야 합니다. 그런 후 사용자 지정 그룹에 클러스터 계산 리소스를 추가합니다.
 클러스터에 기본 정책이 아닌 정책을 적용하려면 사용자 지정 그룹을 추가합니다. 그런 다음 사용자 지정 그룹에 해당 정책을 적용합니다. 기본 정책을 사용하는 경우 기본 정책이 모든 개체에 적용되기 때문에 사용자 지정 그룹을 생성할 필요가 없습니다.
 - a **환경 > 사용자 지정 그룹**을 클릭합니다.
 - b 클러스터에 대한 사용자 지정 그룹이 없으면 사용자 지정 그룹을 생성합니다.
 자세한 내용은 vRealize Operations Manager 정보 센터에서 [사용자 시나리오: 사용자 지정 개체 그룹 생성](#) 항목을 참조하십시오.
 - c 사용자 지정 그룹에 클러스터를 추가하고 사용자 지정 그룹을 저장합니다.

- 3** 클러스터에서 워크로드를 통합하고 균형을 조정하도록 정책을 구성하고 해당 정책을 사용자 지정 그룹에 적용합니다.

통합, 균형 조정, 채우기, CPU, 메모리 및 디스크 공간에 대한 설정을 구축하도록 vRealize Operations Manager에서 정책을 구성합니다. 예를 들어 클러스터 상태 및 용량을 기반으로 새로 관리되는 워크로드에 대한 최상의 배치를 결정하기 위해 워크로드 통합이라는 설정을 수정합니다. 워크로드 균형 조정에 대한 임계값 설정도 워크로드를 배치하는 데 필요한 강도의 수준까지 수정합니다. 하나 이상의 정책을 구성하여 클러스터 계산 리소스에 적용할 수 있습니다.

- a 정책을 찾으려면 **관리 > 정책 > 정책 라이브러리**를 클릭합니다.
- b 워크로드 값을 설정하려면 **정책 추가/편집**을 클릭하고 **워크로드 자동화**를 클릭합니다.

[워크로드 통합] 및 [클러스터 헤드룸]이라는 설정은 가상 시스템의 초기 배치에 적용됩니다.

- [워크로드 통합]을 **없음**으로 설정하면 워크로드 배치는 정책이 적용되는 모든 클러스터 사이에 워크로드 밸런싱을 수행합니다. [워크로드 통합]을 그 이외의 값으로 설정하면 워크로드 배치는 가장 바쁜 클러스터부터 채웁니다.
- [클러스터 헤드룸]은 클러스터 내의 예약된 버퍼 공간이며 총 용량의 백분율로 표시됩니다. 예를 들어 클러스터 헤드룸을 20%로 설정하면 이 버퍼 때문에 워크로드 배치가 해당 클러스터에 가상 시스템을 배치하지 못할 수 있습니다. 배치하지 못하는 이유는 CPU, 메모리 또는 디스크 공간을 위한 클러스터의 여유 용량이 20% 더 적기 때문입니다.

- c 정책 작업 공간에서 **그룹에 정책 적용**을 클릭합니다.
- d 사용자 지정 그룹을 선택합니다.
- e 정책을 저장합니다.

사용자가 Blueprint를 배포할 때 vRealize Automation이 워크로드 배치 분석을 사용하여 시스템의 배치 대상을 제안하도록 vRealize Operations Manager를 구성했습니다.

후속 작업

vRealize Automation 및 vRealize Operations Manager가 환경의 끝점 및 개체에서 데이터를 수집할 때까지 기다립니다. 그러면 새 Blueprint를 배포할 때 확인을 위해 vRealize Automation에 워크로드 배치 권장 사항, 대상 후보 및 선택한 배치가 표시됩니다.

워크로드 배치 문제 해결

워크로드 배치에서 문제가 발생한 경우 문제 해결 정보를 사용하여 문제를 해결하십시오.

워크로드 배치가 제대로 작동하려면 vRealize Automation 솔루션이 필요함

워크로드 배치는 개별 시스템을 기반으로 하며 배치는 시스템 수준에서 수행됩니다. vRealize Automation 및 vRealize Operations Manager를 함께 설치하는 경우 vRealize Automation 솔루션도 설치해야 합니다.

관리 팩과 어댑터가 포함되어 있는 이 솔루션은 컨테이너 재조정 또는 VM 이동 작업이 사용되지 않도록 설정된 클러스터를 식별합니다. 재조정 작업은 클러스터가 속하는 사용자 지정 데이터 센터에서 사용되지 않도록 설정됩니다.

- 관리되는 vRealize Automation 클러스터가 없는 사용자 지정 데이터 센터에 속하는 관리되지 않는 vRealize Automation 클러스터의 경우 VM 이동 및 컨테이너 재조정 작업이 사용되도록 설정됩니다. 관리되는 vRealize Automation 클러스터의 경우에는 이러한 작업이 사용되지 않도록 설정됩니다.
- vRealize Operations Manager에서 vRealize Automation 어댑터는 예약을 매핑하는 클러스터에 있는 VM을 이동 또는 재조정하지 못하도록 차단합니다.

주의 vRealize Automation 솔루션은 단일 vRealize Operations Manager 인스턴스에만 설치해야 합니다.

고가용성이 사용되도록 설정되었지만 사용되지 않도록 설정해야 함

HA가 사용되도록 설정되어 있으면 vRealize Operations Manager가 다운된 경우 워크로드 배치 시간이 초과되어 vRealize Operations Manager 호출이 실패할 수 있음

vRealize Automation은 catalina.out 로그 파일에 워크로드 배치 오류를 로깅합니다.

vRealize Automation의 vSphere 끝점이 모니터링되지 않음

vRealize Operations Manager는 예약 클러스터를 포함하는 vSphere vCenter Server 인스턴스를 모니터링하지 않습니다.

vRealize Operations Manager가 클러스터, 데이터스토어 또는 데이터스토어 클러스터에 대한 vRealize Automation 후보 예약 배치를 시도할 때 해당 예약을 인식하지 못하면 예약을 무시합니다. 배치 응답에서, vRealize Operations Manager는 예약을 인식할 수 없음을 vRealize Automation에 전달합니다.

그러면 vRealize Automation이 요청 실행의 배치 세부 정보에서 후보 예약에 대해 경고 아이콘을 표시하여 예약이 인식되지 않았음을 나타냅니다.

불일치가 발생한 경우 vRealize Automation 이 목록 맨 위에 나타남

vRealize Automation 및 vRealize Operations Manager는 인프라의 서로 다른 보기를 관리합니다. 하지만 둘 모두 동일한 인프라에서 동일한 vCenter Server 인스턴스를 관리해야 합니다.

연결 해제 및 불일치를 식별하고 세부 정보를 표시해야 합니다.

vRealize Automation 어댑터가 다운된 경우 수행할 조치

초기 배치에서는 사용자가 설치 직후에 클러스터를 추가하는 경우와 같이, vRealize Operations Manager에서 받는 대상 후보 목록을 항상 준수합니다.

관리 팩과 어댑터가 포함되어 있는 vRealize Automation 솔루션을 vRealize Operations Manager에서 사용할 수 없는 경우에는 VM 이동 및 컨테이너 재조정 작업을 사용할 수 있습니다.

키 쌍 관리

키 쌍은 클라우드 인스턴스를 프로비저닝하고 클라우드 인스턴스에 연결하는 데 사용됩니다. 키 쌍은 Windows 암호를 해독하거나 Linux 시스템에 로그인하는 데 사용됩니다.

키 쌍은 Amazon AWS를 사용하여 프로비저닝을 할 때 필요합니다. Red Hat OpenStack의 경우 키 쌍은 선택 사항입니다.

기존 키 쌍은 클라우드 끝점을 추가할 때 데이터 수집의 일부로 가져옵니다. 패브릭 관리자는 vRealize Automation 콘솔을 사용하여 키 쌍을 생성하고 관리할 수도 있습니다.

vRealize Automation 콘솔에서 키 쌍을 삭제하면 클라우드 서비스 계정에서도 해당 키 쌍이 삭제됩니다.

키 쌍을 수동으로 관리하는 방법 이외에 시스템 또는 비즈니스 그룹 단위로 키 쌍을 자동으로 생성하도록 vRealize Automation을 구성할 수 있습니다.

- 패브릭 관리자는 예약 수준에서 키 쌍의 자동 생성을 구성할 수 있습니다.
- 키 쌍을 Blueprint 수준에서 제어하려면 패브릭 관리자가 예약에서 **지정되지 않음**을 선택해야 합니다.
- 테넌트 관리자 또는 비즈니스 그룹 관리자는 Blueprint 수준에서 키 쌍의 자동 생성을 구성할 수 있습니다.
- 키 쌍 생성이 예약 수준과 Blueprint 수준 모두에 구성되어 있는 경우에는 예약 설정이 Blueprint 설정을 재정의합니다.


키 쌍 생성

vRealize Automation을 사용하면 끝점에 사용할 키 쌍을 생성할 수 있습니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 클라우드 끝점을 생성하고 클라우드 계산 리소스를 패브릭 그룹에 추가합니다. **끝점 선택 시나리오** 및 **패브릭 그룹 생성** 항목을 참조하십시오.

프로시저

- 1 **인프라 > 예약 > 키 쌍**을 선택합니다.
- 2 **새로 만들기**를 클릭합니다.
- 3 **이름** 텍스트 상자에 이름을 입력합니다.
- 4 **계산 리소스** 드롭다운 메뉴에서 클라우드 영역을 선택합니다.
- 5 **저장** 아이콘()을 클릭합니다.

[비밀 키] 열의 값이 *****가 되면 키 쌍을 사용할 준비가 된 것입니다.



키 쌍용 개인 키 업로드

PEM 형식의 키 쌍용 개인 키를 업로드할 수 있습니다.

필수 조건

- 패브릭 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 키 쌍이 이미 있어야 합니다. [키 쌍 생성](#) 항목을 참조하십시오.

프로시저

- 1 **인프라 > 예약 > 키 쌍**을 선택합니다.
- 2 개인 키를 업로드할 키 쌍을 찾습니다.
- 3 **편집** 아이콘()을 클릭합니다.
- 4 다음 방법 중 하나를 사용하여 키를 업로드합니다.
 - PEM 인코딩된 파일을 찾아서 **업로드**를 클릭합니다.
 - -----BEGIN RSA PRIVATE KEY-----부터 -----END RSA PRIVATE KEY-----까지의 개인 키 텍스트를 붙여넣습니다.
- 5 **저장** 아이콘()을 클릭합니다.


키 쌍에서 개인 키 내보내기

키 쌍에서 PEM으로 인코딩된 파일로 개인 키를 내보낼 수 있습니다.

필수 조건

- 패브릭 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 개인 키가 있는 키 쌍이 있어야 합니다. [키 쌍용 개인 키 업로드](#) 항목을 참조하십시오.

프로시저

- 1 **인프라 > 예약 > 키 쌍**을 선택합니다.
- 2 개인 키를 내보낼 키 쌍을 찾습니다.
- 3 **내보내기** 아이콘()을 클릭합니다.
- 4 파일을 저장할 위치로 이동한 다음 **저장**을 클릭합니다.

시나리오: 영역 간 배포를 위한 계산 리소스에 위치 적용

패브릭 관리자는 영역 간 배포를 지원하기 위해 계산 리소스를 보스턴 또는 런던 데이터 센터에 속해 있는 것으로 레이블을 지정하고자 합니다. Blueprint 설계자가 해당 Blueprint에 대한 위치 기능을 사용하도록 설정하는 경우 사용자가 보스턴 또는 런던 데이터 센터에서 시스템을 프로비저닝할지 선택할 수 있습니다.



런던과 보스턴에 데이터 센터가 있으며 보스턴의 사용자가 런던 인프라에서 시스템을 프로비저닝하거나 런던의 사용자가 보스턴 인프라에서 시스템을 프로비저닝하지 않길 바랍니다. 보스턴 사용자가 보스턴 인프라에서 프로비저닝하고 런던 사용자가 런던 인프라에서 프로비저닝하도록 사용자가 시스템을 요청할 때 프로비저닝을 위한 적합한 위치를 선택하도록 허용하고자 합니다.

필수 조건

- **패브릭 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 시스템 관리자는 데이터 센터 위치를 정의합니다. **시나리오: 영역 간 배포를 위한 데이터 센터 위치 추가** 항목을 참조하십시오.

프로시저

- 1 **인프라 > 계산 리소스 > 계산 리소스**를 선택합니다.
- 2 보스턴 데이터 센터에 위치한 계산 리소스를 가리키고 **편집**을 클릭합니다.
- 3 **위치** 드롭다운 메뉴에서 보스턴을 선택합니다.
- 4 **확인**을 클릭합니다.
- 5 계산 리소스를 보스턴 및 런던 위치에 연결하려면 필요에 따라 이 절차를 반복합니다.

IaaS 설계자는 사용자가 카탈로그 항목 요청 양식을 작성하면서 보스턴 또는 런던의 시스템을 프로비저닝하도록 선택할 수 있도록 위치 기능을 사용하도록 설정할 수 있습니다. **시나리오: 영역 간 배포에 사용할 데이터 센터 위치를 사용자가 선택할 수 있도록 허용** 항목을 참조하십시오.

타사 IPAM 제공자를 사용하여 vRealize Automation 배포 프로비저닝

Infoblox 같이 지원되는 타사 IPAM 솔루션 제공자로부터 vRealize Automation 네트워크 프로파일의 사용에 사용할 IP 주소와 범위를 가져올 수 있습니다.

네트워크 프로파일의 IP 주소 범위는 Blueprint에서 지정하는 연결된 예약에 사용됩니다. 권한 있는 사용자가 Blueprint 카탈로그 항목을 사용하여 시스템 프로비저닝을 요청하면 타사 IPAM의 지정된 IP 주소 범위에서 IP 주소를 가져옵니다. 시스템 배포 후 vRealize Automation 항목 세부 정보 페이지를 조회하여 사용된 IP 주소를 확인할 수 있습니다.

표 2-19. Infoblox IPAM을 사용하여 vRealize Automation 배포를 프로비저닝하기 위한 준비 검사 목록

작업	설명	세부 정보
타사 IPAM 솔루션 제공자 플러그인 또는 패키지를 받고, 가져오고, 구성합니다.	vRealize Orchestrator 플러그인을 받아 가져오고, vRealize Orchestrator 구성 워크플로를 실행하고, vRealize Orchestrator에서 IPAM 제공자 끝점 유형을 등록합니다. VMware Solution Exchange(https://marketplace.vmware.com/vsx)에 필요한 IPAM 제공자 패키지가 없으면 IPAM 솔루션 제공자 SDK 및 지원 설명서를 사용하여 고유의 패키지를 생성할 수 있습니다. code.vmware.com 에서 vRealize Automation Third-Party IPAM Integration SDK 7.3 페이지를 참조하십시오.	타사 IPAM 제공자 지원을 제공하기 위한 검사 목록 항목을 참조하십시오.
타사 IPAM 솔루션 제공자 끝점을 생성합니다.	vRealize Automation에서 새 IPAM 끝점을 생성합니다.	타사 IPAM 제공자 끝점 생성 항목을 참조하십시오.
외부 네트워크 프로파일에 타사 IPAM 솔루션 제공자 끝점 설정을 지정합니다.	vRealize Automation에서 외부 네트워크 프로파일을 생성하고 정의된 IPAM 끝점을 지정합니다.	타사 IPAM 제공자를 사용하여 외부 네트워크 프로파일 생성 항목을 참조하십시오.
필요한 경우 라우팅된 네트워크 프로파일에 타사 IPAM 솔루션 제공자 끝점 설정을 지정합니다.	vRealize Automation에서 요청 시 네트워크 프로파일을 생성하고 정의된 IPAM 끝점을 지정합니다.	타사 IPAM 끝점을 사용하여 라우팅된 네트워크 프로파일 생성 또는 타사 IPAM 끝점을 사용하여 NAT 네트워크 프로파일 생성 항목을 참조하십시오.
네트워크 프로파일을 사용할 예약을 정의합니다.	vRealize Automation에서 네트워크 프로파일을 호출하는 예약을 생성합니다.	Hyper-V, KVM, SCVMM, vSphere 또는 XenServer에 대한 예약 생성 항목을 참조하십시오.
네트워크 프로파일을 사용하는 Blueprint를 정의합니다.	vRealize Automation에서 예약을 사용하는 Blueprint를 생성합니다.	3장사용자에게 서비스 Blueprint 제공 항목을 참조하십시오.
사용 가능하도록 Blueprint를 카탈로그에 게시합니다.	vRealize Automation에서 Blueprint를 카탈로그에 게시합니다. 필요한 사용 권한을 추가합니다.	Blueprint 게시 항목을 참조하십시오.
Blueprint 카탈로그 항목을 사용하여 시스템 프로비저닝을 요청합니다.	Blueprint 카탈로그 항목을 사용하여 vRealize Automation에서 시스템 프로비저닝을 요청합니다.	서비스 카탈로그 관리 항목을 참조하십시오.

XaaS 리소스 구성

XaaS 끝점을 구성하여 vRealize Automation을 환경에 연결할 수 있습니다.

vRealize Orchestrator 플러그인을 끝점으로 구성할 때 vRealize Orchestrator 구성 인터페이스를 사용하는 대신 vRealize Automation 사용자 인터페이스를 사용하여 플러그인을 구성합니다.

VMware 및 타사 기술을 vRealize Automation에 노출하기 위해 vRealize Orchestrator 기능 및 vRealize Orchestrator 플러그인을 사용하려는 경우 플러그인을 끝점으로 추가하여 vRealize Orchestrator 플러그인을 구성할 수 있습니다. 이러한 방식으로 vCenter Server 인스턴스, Microsoft Active Directory 호스트 등과 같은 서로 다른 호스트 및 서버에 대한 연결을 생성합니다.

vRealize Automation UI를 사용하여 vRealize Orchestrator 플러그인을 끝점으로 추가할 때 기본 vRealize Orchestrator 서버에서 구성 워크플로를 실행합니다. 구성 워크플로는 **vRealize Automation > XaaS > 끝점 구성** 워크플로 폴더에 위치해 있습니다.

중요 vRealize Orchestrator 및 vRealize Automation 콘솔에서 단일 플러그인을 구성하는 것은 지원되지 않으며 오류가 발생합니다.

Active Directory 플러그인을 끝점으로 구성

끝점을 추가하고 Active Directory 플러그인을 구성하여 실행 중인 Active Directory 인스턴스에 연결하고 사용자와 사용자 그룹, Active Directory 컴퓨터, 조직 구성 단위 등을 관리합니다.

Active Directory 끝점을 추가한 후에는 언제든지 업데이트할 수 있습니다.

필수 조건

- Microsoft Active Directory 인스턴스에 액세스할 수 있는지 확인합니다. Microsoft Active Directory 설명서를 참조합니다.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 끝점 > Orchestrator 끝점**을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 **플러그인** 드롭다운 메뉴에서 **Active Directory**를 선택합니다.
- 4 **다음**을 클릭합니다.
- 5 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 6 **다음**을 클릭합니다.
- 7 Active Directory 서버 세부 정보를 구성합니다.
 - a **Active Directory 호스트 IP/URL** 텍스트 상자에 Active Directory가 실행되는 호스트의 IP 주소 또는 DNS 이름을 입력합니다.
 - b **포트** 텍스트 상자에 Active Directory 서버의 조회 포트를 입력합니다.

vRealize Orchestrator는 Active Directory 계층 도메인 구조를 지원합니다. 도메인 컨트롤러가 글로벌 카탈로그를 사용하도록 구성되어 있는 경우 포트 3268을 사용해야 합니다. 기본 포트 389는 글로벌 카탈로그 서버에 연결하는 데 사용할 수 없습니다. 포트 389 및 3268 뿐만 아니라 636을 LDAPS에 사용할 수 있습니다.

- c **루트** 텍스트 상자에 Active Directory 서버의 루트 요소를 입력합니다.

예를 들어 도메인 이름이 mycompany.com이라면 루트 Active Directory는 **dc=mycompany,dc=com**입니다.

이 노드는 적절한 자격 증명을 입력한 후 서비스 디렉토리를 찾는 데 사용됩니다. 대규모 서비스 디렉토리의 경우 트리에서 노드를 지정하면 검색 범위를 좁혀 성능을 높일 수 있습니다. 예를 들어 전체 디렉토리에서 검색하는 대신 **ou=employees,dc=mycompany,dc=com**을 지정할 수 있습니다. 이 루트 요소는 직원 그룹의 모든 사용자를 표시합니다.

- d (선택 사항) vRealize Orchestrator 및 Active Directory 간 연결을 위한 암호화된 인증을 활성화하려면 **SSL 사용** 드롭다운 메뉴에서 **예**를 선택합니다.

자체 서명된 인증서인 경우라도 확인을 위한 메시지를 표시하지 않고 SSL 인증서를 자동으로 가져옵니다.

- e (선택 사항) **기본 도메인** 텍스트 상자에 도메인을 입력합니다.

예를 들어 도메인 이름이 mycompany.com인 경우 **@mycompany.com**을 입력합니다.

8 공유 세션 설정을 구성합니다.

vRealize Orchestrator에서 자격 증명을 사용하여 모든 Active Directory 워크플로 및 작업을 실행합니다.

- a **공유 세션의 사용자 이름** 텍스트 상자에 공유 세션의 사용자 이름을 입력합니다.

- a **공유 세션의 암호** 텍스트 상자에 공유 세션의 암호를 입력합니다.

9 완료

Active Directory 인스턴스를 끝점으로 추가했습니다. XaaS 설계자는 XaaS를 사용하여 Active Directory 플러그인 워크플로를 카탈로그 항목 및 리소스 작업으로 게시할 수 있습니다.

후속 작업

- vRealize Automation Blueprint를 사용하여 환경에서 Active Directory 사용자를 관리하려면 Active Directory를 기반으로 XaaS Blueprint를 생성합니다. 하나의 예로 [사용자 생성 및 수정을 위해 XaaS Blueprint 및 작업 생성](#) 항목을 참조하십시오.
- 시스템이 배포될 때 vRealize Automation을 사용하여 Active Directory 기록을 생성하려는 경우 서로 다른 Active Directory 정책을 생성한 다음 각각의 비즈니스 그룹과 Blueprint에 적용할 수 있습니다. [Active Directory 정책 생성 및 적용](#) 항목을 참조하십시오.


HTTP-REST 플러그인을 끝점으로 구성

끝점을 추가하고 REST 호스트에 연결하도록 HTTP-REST 플러그인을 구성할 수 있습니다.

필수 조건

- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- REST 호스트에 대한 액세스 권한이 있는지 확인합니다.

프로시저

- 1 **관리 > 끝점 > Orchestrator 끝점**을 선택합니다.
- 2 **새로 만들기** 아이콘()을 클릭합니다.
- 3 **플러그인** 드롭다운 메뉴에서 **HTTP-REST**를 선택합니다.
- 4 **다음**을 클릭합니다.
- 5 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 6 **다음**을 클릭합니다.
- 7 REST 호스트에 대한 정보를 제공합니다.
 - a **이름** 텍스트 상자에 호스트의 이름을 입력합니다.
 - b **URL** 텍스트 상자에 호스트의 주소를 입력합니다.

참고 Kerberos 액세스 인증을 사용하는 경우 FDQN 형식으로 호스트 주소를 제공해야 합니다.

- c (선택 사항) **연결 시간 제한(초)** 텍스트 상자에 연결 시간 제한이 발생하기 전의 시간(초)을 입력합니다.
기본값은 30초입니다.
- d (선택 사항) **작업 시간 제한(초)** 텍스트 상자에 작업 시간 제한이 발생하기 전의 시간(초)을 입력합니다.
기본값은 60초입니다.
- 8 (선택 사항) 프록시 설정을 구성합니다.
 - a **프록시 사용** 드롭다운 메뉴에서 프록시를 사용하려면 **예**를 선택합니다.
 - b **프록시 주소** 텍스트 상자에 프록시 서버의 IP를 입력합니다.
 - c **프록시 포트** 텍스트 상자에 프록시 서버와 통신하기 위한 포트 번호를 입력합니다.
- 9 **다음**을 클릭합니다.

10 인증 유형을 선택합니다.

옵션	작업
없음	인증이 필요하지 않습니다.
OAuth 1.0	<p>OAuth 1.0 프로토콜을 사용합니다. OAuth 1.0 하의 필수 인증 매개 변수를 제공해야 합니다.</p> <ul style="list-style-type: none"> a 소비자 키 텍스트 상자에 소비자를 서비스 제공자로 식별하는 데 사용되는 키를 입력합니다. b 소비자 비밀번호 텍스트 상자에 소비자 키의 소유권을 설정하기 위한 비밀을 입력합니다. c (선택 사항) 액세스 토큰 텍스트 상자에 보호된 리소스에 대한 액세스 권한을 얻기 위해 소비자가 사용하는 액세스 토큰을 입력합니다. d (선택 사항) 액세스 토큰 비밀번호 텍스트 상자에 토큰의 소유권을 설정하기 위해 소비자가 사용하는 비밀을 입력합니다.
OAuth 2.0	<p>OAuth 2.0 프로토콜을 사용합니다.</p> <p>토큰 텍스트 상자에 인증 토큰을 입력합니다.</p>
기본	<p>기본 액세스 인증을 제공합니다. 호스트와의 통신이 공유 세션 모드에 있습니다.</p> <ul style="list-style-type: none"> a 인증 사용자 이름 텍스트 상자에 공유 세션의 사용자 이름을 입력합니다. b 인증 암호 텍스트 상자에 공유 세션의 암호를 입력합니다.
다이제스트	<p>암호화를 사용하는 다이제스트 액세스 인증을 제공합니다. 호스트와의 통신이 공유 세션 모드에 있습니다.</p> <ul style="list-style-type: none"> a 인증 사용자 이름 텍스트 상자에 공유 세션의 사용자 이름을 입력합니다. b 인증 암호 텍스트 상자에 공유 세션의 암호를 입력합니다.
NTLM	<p>Windows SSP(보안 지원 공급자) 프레임워크 내에 NTLM(NT LAN Manager) 액세스 인증을 제공합니다. 호스트와의 통신이 공유 세션 모드에 있습니다.</p> <ul style="list-style-type: none"> a 공유 세션에 대한 사용자 자격 증명을 제공합니다. <ul style="list-style-type: none"> ■ 인증 사용자 이름 텍스트 상자에 공유 세션의 사용자 이름을 입력합니다. ■ 인증 암호 텍스트 상자에 공유 세션의 암호를 입력합니다. b NTLM 세부 정보 구성 <ul style="list-style-type: none"> ■ (선택 사항) NTLM 인증용 워크스테이션 텍스트 상자에 워크스테이션 이름을 입력합니다. ■ NTLM 인증용 도메인 텍스트 상자에 도메인 이름을 입력합니다.
Kerberos	<p>Kerberos 액세스 인증을 제공합니다. 호스트와의 통신이 공유 세션 모드에 있습니다.</p> <ul style="list-style-type: none"> a 인증 사용자 이름 텍스트 상자에 공유 세션의 사용자 이름을 입력합니다. b 인증 암호 텍스트 상자에 공유 세션의 암호를 입력합니다.

11 완료를 클릭합니다.

끝점을 구성하고 REST 호스트를 추가했습니다. XaaS 설계자는 XaaS를 사용하여 HTTP-REST 플러그인 워크플로를 카탈로그 항목 및 리소스 작업으로 게시할 수 있습니다.

PowerShell 플러그인을 끝점으로 구성

vRealize Orchestrator 작업 및 워크플로에서 PowerShell 스크립트와 cmdlet을 호출하고 그 결과에 대해 작업할 수 있도록 끝점을 추가하고 PowerShell 플러그인을 구성하여 실행 중인 PowerShell 호스트에 연결할 수 있습니다.

필수 조건

- Windows PowerShell 호스트에 대한 액세스 권한이 있는지 확인합니다. Microsoft Windows PowerShell에 대한 자세한 내용은 Windows PowerShell 설명서를 참조하십시오.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 끝점 > Orchestrator 끝점**을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 **플러그인** 드롭다운 메뉴에서 **PowerShell**을 선택합니다.
- 4 **다음**을 클릭합니다.
- 5 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 6 **다음**을 클릭합니다.
- 7 PowerShell 호스트 세부 정보를 지정합니다.
 - a **이름** 텍스트 상자에 호스트의 이름을 입력합니다.
 - b **호스트/IP** 텍스트 상자에 호스트의 IP 주소 또는 FQDN을 입력합니다.
- 8 플러그인이 연결될 PowerShell 호스트 유형을 선택합니다.

옵션	작업
WinRM	<ol style="list-style-type: none"> a [PowerShell 호스트 세부 정보] 아래의 포트 텍스트 상자에 호스트와 통신하는 데 사용할 포트 번호를 입력합니다. b 전송 프로토콜 드롭다운 메뉴에서 전송 프로토콜을 선택합니다. <p>참고 HTTPS 전송 프로토콜을 사용하는 경우 원격 PowerShell 호스트의 인증서를 vRealize Orchestrator Keystore로 가져옵니다.</p> <ol style="list-style-type: none"> c 인증 드롭다운 메뉴에서 인증 유형을 선택합니다. <p>참고 Kerberos 인증을 사용하려면 WinRM 서비스에서 해당 인증을 사용하도록 설정합니다. Kerberos 인증 구성에 대한 자세한 내용은 PowerShell 플러그인 사용을 참조하십시오.</p>
SSH	없음.

- 9 **사용자 이름 및 암호** 텍스트 상자에 PowerShell 호스트와의 공유 세션 통신을 위한 자격 증명을 입력합니다.
- 10 **완료**를 클릭합니다.

Windows PowerShell 호스트를 끝점으로 추가했습니다. XaaS 설계자는 XaaS를 사용하여 PowerShell 플러그인 워크플로를 카탈로그 항목 및 리소스 작업으로 게시할 수 있습니다.

SOAP 플러그인을 끝점으로 구성

끝점을 추가하고 SOAP 플러그인을 구성하여 SOAP 서비스를 인벤토리 개체로 정의하고 정의된 개체에서 SOAP 작업을 수행할 수 있습니다.

필수 조건

- SOAP 호스트에 대한 액세스 권한이 있는지 확인합니다. 이 플러그인은 SOAP 버전 1.1과 1.2, WSDL 1.1과 2.0을 지원합니다.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 끝점 > Orchestrator** 끝점을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 **플러그인** 드롭다운 메뉴에서 **SOAP**를 선택합니다.
- 4 **다음**을 클릭합니다.
- 5 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 6 **다음**을 클릭합니다.
- 7 SOAP 호스트에 대한 세부 정보를 제공합니다.
 - a **이름** 텍스트 상자에 호스트의 이름을 입력합니다.
 - b **WSDL 콘텐츠 제공** 드롭다운 메뉴에서 WSDL 콘텐츠를 텍스트로 제공할지 여부를 선택합니다.

옵션	작업
예	WSDL 콘텐츠 텍스트 상자에 WSDL 텍스트를 입력합니다.
아니요	WSDL URL 텍스트 상자에 올바른 경로를 입력합니다.

 - c (선택 사항) **연결 시간 제한(초)** 텍스트 상자에 연결 시간 제한이 발생하기 전의 시간(초)을 입력합니다.
기본값은 30초입니다.
 - d (선택 사항) **요청 시간 제한(초)** 텍스트 상자에 작업 시간 제한이 발생하기 전의 시간(초)을 입력합니다.
기본값은 60초입니다.

8 (선택 사항) 프록시 설정을 지정합니다.

- a 프록시를 사용하려면 **프록시** 드롭다운 메뉴에서 **예**를 선택합니다.
- b **주소** 텍스트 상자에 프록시 서버의 IP를 입력합니다.
- c **포트** 텍스트 상자에 프록시 서버와 통신하기 위한 포트 번호를 입력합니다.

9 다음을 클릭합니다.**10 인증 유형을 선택합니다.**

옵션	작업
없음	인증이 필요하지 않습니다.
기본	기본 액세스 인증을 제공합니다. 호스트와의 통신이 공유 세션 모드에 있습니다. a 사용자 이름 텍스트 상자에 공유 세션의 사용자 이름을 입력합니다. b 암호 텍스트 상자에 공유 세션의 암호를 입력합니다.
다이제스트	암호화를 사용하는 다이제스트 액세스 인증을 제공합니다. 호스트와의 통신이 공유 세션 모드에 있습니다. a 사용자 이름 텍스트 상자에 공유 세션의 사용자 이름을 입력합니다. b 암호 텍스트 상자에 공유 세션의 암호를 입력합니다.
NTLM	Windows SSP(보안 지원 공급자) 프레임워크에서 NTLM(NT LAN Manager) 액세스 인증을 제공합니다. 호스트와의 통신이 공유 세션 모드에 있습니다. a 사용자 자격 증명을 제공합니다. ▪ 사용자 이름 텍스트 상자에 공유 세션의 사용자 이름을 입력합니다. ▪ 암호 텍스트 상자에 공유 세션의 암호를 입력합니다. b NTLM 설정을 제공합니다. ▪ NTLM 도메인 텍스트 상자에 도메인 이름을 입력합니다. ▪ (선택 사항) NTLM 워크스테이션 텍스트 상자에 워크스테이션 이름을 입력합니다.
협상	Kerberos 액세스 인증을 제공합니다. 호스트와의 통신이 공유 세션 모드에 있습니다. a 사용자 자격 증명을 제공합니다. 1 사용자 이름 텍스트 상자에 공유 세션의 사용자 이름을 입력합니다. 2 암호 텍스트 상자에 공유 세션의 암호를 입력합니다. b Kerberos 서비스 SPN 텍스트 상자에 Kerberos 서비스 SPN을 입력합니다.

11 완료를 클릭합니다.

SOAP 서비스를 추가했습니다. XaaS 설계자는 XaaS를 사용하여 SOAP 플러그인 워크플로를 카탈로그 항목 및 리소스 작업으로 게시할 수 있습니다.

vCenter Server 플러그인을 끝점으로 구성

끝점을 추가하고 vCenter Server 플러그인을 구성하여 실행 중인 vCenter Server 인스턴스에 연결하고 XaaS Blueprint를 생성하여 vSphere 인벤토리 개체를 관리할 수 있습니다.

필수 조건

- vCenter Server를 설치하고 구성합니다. vSphere 설치 및 설정을 참조하십시오.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 끝점 > Orchestrator 끝점**을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 **플러그인** 드롭다운 메뉴에서 **vCenter Server**를 선택합니다.
- 4 **다음**을 클릭합니다.
- 5 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 6 **다음**을 클릭합니다.
- 7 vCenter Server 인스턴스에 대한 정보를 제공합니다.
 - a **추가할 vCenter Server 인스턴스의 IP 또는 호스트 이름** 텍스트 상자에 시스템의 IP 주소 또는 DNS 이름을 입력합니다.
 이것은 추가하려는 vCenter Server 인스턴스가 설치되는 시스템의 IP 주소 또는 DNS 이름입니다.
 - b vCenter Server 인스턴스와 통신하기 위한 포트를 **vCenter Server 인스턴스의 포트** 텍스트 상자에 입력합니다.
 기본 포트는 443입니다.
 - c vCenter Server 인스턴스에 연결하기 위해 사용할 SDK의 위치를 **vCenter Server 인스턴스에 연결하기 위해 사용할 SDK의 위치** 텍스트 상자에 입력합니다.
 예를 들어 `/sdk`를 입력합니다.
- 8 **다음**을 클릭합니다.
- 9 연결 매개 변수를 정의합니다.
 - a vCenter Server 인스턴스의 HTTP 포트를 **vCenter Server 인스턴스의 HTTP 포트 - VC 플러그인 버전 5.5.2 이전에 적용 가능** 텍스트 상자에 입력합니다.
 - b vCenter Server 인스턴스에 대한 연결을 설정하기 위해 사용할 vRealize Orchestrator에 대한 자격 증명을 **vCenter Server 인스턴스에 연결하기 위해 Orchestrator에서 사용할 사용자의 사용자 이름** 및 **vCenter Server 인스턴스에 연결하기 위해 Orchestrator에서 사용할 사용자의 암호** 텍스트 상자에 입력합니다.
 선택하는 사용자는 vCenter Server 확장을 관리할 수 있는 권한과 일련의 사용자 지정된 권한을 가진 유효한 사용자여야 합니다.
- 10 **완료**를 클릭합니다.

vCenter Server 인스턴스를 끝점으로 추가했습니다. XaaS 설계자는 XaaS를 사용하여 vCenter Server 플러그인 워크플로를 카탈로그 항목 및 리소스 작업으로 게시할 수 있습니다.

Microsoft Azure 끝점 생성

vRealize Automation과 Azure 배포 간에 자격 증명을 통한 연결을 원활하게 하기 위해 Microsoft Azure 끝점을 생성할 수 있습니다.

끝점은 가상 시스템 Blueprint를 생성하는 데 사용할 수 있는 리소스(이 경우 Azure 인스턴스)에 대한 연결을 설정합니다. Azure 가상 시스템 프로비저닝을 위한 Blueprint의 기준으로 사용할 Azure 끝점이 있어야 합니다. 여러 Azure 구독을 사용하는 경우 각 구독 ID에 대한 끝점이 필요합니다.

대안으로 vRealize Orchestrator 워크플로 트리의 **라이브러리 > Azure > 구성** 아래 있는 [Azure 연결 추가] 명령을 사용하여 vRealize Orchestrator에서 Azure 연결을 직접 생성할 수 있습니다. 대부분의 시나리오에서 여기의 설명대로 끝점 구성을 통해 연결을 생성하는 것이 기본 옵션입니다.

Azure 끝점은 vRealize Orchestrator 및 XaaS 기능에서 지원됩니다. Azure 끝점을 생성, 삭제 또는 편집할 수 있습니다. 기존 끝점을 변경하고 몇 시간 동안 업데이트된 연결을 통해 Azure 포털에서 업데이트를 실행하지 않으면 `service vco-service restart` 명령을 사용하여 vRealize Orchestrator 서비스를 다시 시작해야 합니다. 서비스를 다시 시작하는 데 실패하면 오류가 발생할 수 있습니다.

필수 조건

- Microsoft Azure 인스턴스를 구성하고 사용할 수 있는 구독 ID를 제공하는 유효한 Microsoft Azure 구독을 얻습니다. Azure 구성 및 구독 ID 연기에 대한 자세한 내용은 <http://www.vaficionado.com/2016/11/using-new-microsoft-azure-endpoint-vrealize-automation-7-2/>를 참조하십시오.
- vRealize Automation 배포에는 최소한 하나의 테넌트와 하나의 비즈니스 그룹이 있어야 합니다.
- <https://azure.microsoft.com/ko-kr/documentation/articles/resource-group-create-service-principal-portal>에 설명된 대로 Active Directory 애플리케이션을 생성합니다.
- 끝점 및 Blueprint 구성 중에 필요하므로 다음과 같은 Azure 관련 정보를 기록해 둡니다.
 - 구독 ID
 - 테넌트 ID
 - 스토리지 계정 이름
 - 리소스 그룹 이름
 - 위치
 - 가상 네트워크 이름
 - 클라이언트 애플리케이션 ID
 - 클라이언트 애플리케이션 비밀 키
 - 가상 시스템 이미지 URN
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 끝점 > Orchestrator 끝점**을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 [플러그인] 탭에서 **플러그인** 드롭다운 메뉴를 클릭하고 [Azure 플러그인]을 선택합니다.
- 4 **다음**을 클릭합니다.
- 5 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 6 **다음**을 클릭합니다.
- 7 **세부 정보** 탭에 있는 텍스트 상자에 끝점에 맞는 적절한 값을 입력합니다.

매개 변수	설명
연결 설정	
Azure 연결	
연결 이름	새 끝점 연결의 고유한 이름입니다. 이 이름은 특정 연결을 식별하는 데 도움이 되도록 vRealize Orchestrator 인터페이스에 나타납니다.
Azure 구독 ID	Azure 구독 식별자입니다. ID는 스토리지 계정, 가상 시스템 및 기타 사용자에게 액세스 권한이 있는 Azure 리소스를 정의합니다.
리소스 관리자 설정	
Azure 서비스 URI	Azure 인스턴스에 액세스할 수 있는 URI입니다. https://management.azure.com/의 기본값은 여러 일반 구현에 적절합니다.
테넌트 ID	끝점에서 사용할 Azure 테넌트 ID입니다.
클라이언트 ID	끝점에서 사용할 Azure 클라이언트 식별자입니다. Active Directory 애플리케이션 생성 시 할당됩니다.
클라이언트 암호	Azure 클라이언트 ID와 함께 사용되는 키입니다. Active Directory 애플리케이션 생성 시 이 키가 할당됩니다.
로그인 URL	Azure 인스턴스에 액세스하는 데 사용하는 URL입니다. https://login.windows.net/의 기본값은 여러 일반 구현에 적절합니다.
프록시 설정	
프록시 호스트	회사가 프록시 웹 서버를 사용하는 경우 해당 서버의 호스트 이름을 입력합니다.
프록시 포트	회사가 프록시 웹 서버를 사용하는 경우 해당 서버의 포트 번호를 입력합니다.

- 8 **완료**를 클릭합니다.

후속 작업

Azure의 적절한 리소스 그룹, 스토리지 계정 및 네트워크 보안 그룹을 생성합니다. 구현에 적절한 경우 로드 밸런서도 생성해야 합니다.

작업	옵션
Azure 리소스 그룹 생성	<ul style="list-style-type: none"> Azure 포털을 사용하여 리소스 그룹을 생성합니다. 구체적인 지침은 Azure 설명서를 참조하십시오. Library/Azure/Resource/Create 리소스 그룹에 있는 적절한 vRealize Orchestrator 워크플로를 사용합니다. vRealize Automation에서 vRealize Orchestrator 워크플로가 포함된 XaaS Blueprint를 생성하고 게시합니다. 리소스 그룹을 서비스 및 사용 권한에 연결한 후 이 리소스 그룹을 요청할 수 있습니다. 리소스 그룹 리소스 유형은 vRealize Automation에서 지원 또는 관리되지 않습니다.
Azure 스토리지 계정 생성	<ul style="list-style-type: none"> Azure를 사용하여 스토리지 계정을 생성합니다. 구체적인 지침은 Azure 설명서를 참조하십시오. Library/Azure/Storage/Create 스토리지 계정에 있는 적절한 vRealize Orchestrator 워크플로를 사용합니다. vRealize Automation에서 vRealize Orchestrator 워크플로가 포함된 XaaS Blueprint를 생성하고 게시합니다. 스토리지 계정을 서비스 및 사용 권한에 연결한 후 이 스토리지 계정을 요청할 수 있습니다.
Azure 네트워크 보안 그룹 생성	<ul style="list-style-type: none"> Azure를 사용하여 보안 그룹을 생성합니다. 구체적인 지침은 Azure 설명서를 참조하십시오. Library/Azure/Network/Create 네트워크 보안 그룹에 있는 적절한 vRealize Orchestrator 워크플로를 사용합니다. vRealize Automation에서 vRealize Orchestrator 워크플로가 포함된 XaaS Blueprint를 생성하고 게시합니다. 보안 그룹을 서비스 및 사용 권한에 연결한 후 이 보안 그룹을 요청할 수 있습니다.

컨테이너 생성 및 구성

vRealize Automation에서 컨테이너 탭을 사용하여 vRealize Automation의 컨테이너 통합 애플리케이션을 열고 vRealize Automation Blueprint 설계자가 사용할 수 있도록 컨테이너 및 컨테이너 네트워크 설정을 생성 및 구성할 수 있습니다.

통합 컨테이너 애플리케이션에서 새 템플릿 및 이미지와 기존 템플릿 및 이미지를 사용하여 컨테이너를 정의할 수 있습니다. 그런 다음 vRealize Automation Blueprint에 컨테이너 구성 요소 및 해당 구성 요소에 연결된 네트워크 설정을 추가할 수 있습니다.

컨테이너 호스트 관리

[호스트]에서 추가하는 호스트를 보고 관리할 수 있습니다. 컨테이너의 컨텍스트에서, 호스트는 컨테이너를 실행할 수 있게 해주는 가상 시스템 또는 인프라입니다.

[호스트] 탭에는 새 호스트를 추가하고, 기존 호스트의 프로비저닝 요청 상태를 모니터링하고, 컨테이너에 대한 이벤트 로그를 보고, 호스트에서 데이터를 수집을 수행하기 위한 컨트롤이 포함되어 있습니다.

[요청] 및 [이벤트 로그] 패널은 페이지의 오른쪽에 있습니다.

컨테이너 호스트 추가

컨테이너를 배포할 호스트를 추가해야 합니다.

컨테이너에서 호스트를 추가하거나 생성할 때 오른쪽에 있는 네 개의 패널 중 하나를 클릭하여 추가 옵션이 있는 도구 모음을 확장할 수 있습니다. 배치 영역, 자격 증명, 인증서 및 배포 정책을 추가하거나 관리할 수 있습니다.

프로시저

- 1 컨테이너 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 2 컨테이너 탭을 클릭합니다.
- 3 호스트 추가를 클릭합니다.
- 4 `http(s)://<호스트 이름>:<포트>` 형식으로 호스트 IP 주소나 호스트 이름을 입력합니다.
- 5 호스트 유형에서 Docker 호스트의 주소를 입력했는지 또는 VCH(가상 컨테이너 호스트)의 주소를 입력했는지 선택합니다.
- 6 목록에서 로그인 자격 증명을 선택합니다.
컨테이너는 자격 증명 인증과 공용-개인 키 인증을 지원합니다.
- 7 확인을 클릭하여 구성된 매개 변수가 유효함을 확인합니다.
확인이 완료되면 추가 정보를 추가할 수 있는 새 텍스트 상자가 표시됩니다.
- 8 (선택 사항) 목록에서 배치 영역을 선택합니다.

참고 VCH를 구성하고 있는 경우 배치 영역 및 배치가 자동으로 생성되고 호스트에 연결됩니다.

- 9 (선택 사항) 목록에서 배포 정책을 선택합니다.
- 10 (선택 사항) 호스트에 대한 사용자 지정 속성을 정의합니다.
- 11 추가를 클릭합니다.

컨테이너에 호스트를 성공적으로 추가했습니다.

후속 작업

컨테이너 배치 및 배치 영역 생성 및 관리

컨테이너 배포 정책 사용

배포 정책을 호스트 및 컨테이너 정의에 연결할 수 있습니다. vRealize Automation의 컨테이너에서 배포 정책을 사용하여 컨테이너를 배포할 때 적용되는 특정 호스트 및 할당량에 대한 기본 설정을 지정합니다.

컨테이너에 적용되는 배포 정책은 컨테이너 호스트에 적용되는 배치보다 우선 순위가 높습니다.

컨테이너 배치 및 배치 영역 생성 및 관리

배치 및 배치 영역을 사용하여 비즈니스 그룹에서 사용되는 리소스를 제한하고 예약할 수 있습니다. 예약된 메모리 양에 대한 우선 순위를 설정할 수도 있습니다.

생성한 배치를 가리키고 해당하는 버튼을 클릭하여 배치를 편집 또는 삭제할 수 있습니다.

배치를 생성하거나 관리할 때 오른쪽의 **배치 영역** 버튼을 클릭하여 배치 영역을 추가하거나 관리할 수 있습니다.

참고 VCH를 구성한 경우에는 배치 및 배치 영역이 자동으로 구성되고 해당 설정은 변경할 수 없습니다. **편집** 아이콘을 클릭하여 배치에 비즈니스 그룹을 할당해야 합니다.

필수 조건

- **컨테이너 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 지정한 메모리 리소스를 사용할 수 있는지 확인합니다.
- 하나 이상의 호스트가 구성되었고 컨테이너 네트워크 구성에 대해 사용할 수 있는지 확인하십시오.

프로시저

1 **컨테이너** 탭을 클릭합니다.

2 **배치**를 클릭합니다.

3 **추가**를 클릭합니다.

4 배치의 이름을 입력합니다.

5 비즈니스 그룹에 배치를 할당합니다.

6 목록에서 배치 영역을 선택합니다.

7 목록에서 배포 정책을 선택합니다.

8 (선택 사항) 배치에 대한 우선 순위 값을 입력합니다.

양수를 입력합니다. 1은 가장 높은 우선 순위를 나타냅니다. 가장 낮은 우선 순위를 지정하려면 필드를 비워 둡니다.

9 인스턴스 수를 지정합니다.

10 사용할 수 있는 최대 메모리 양을 선택합니다.

0과 배치 영역에서 사용할 수 있는 메모리 양 간 숫자를 선택합니다. 이 배치의 리소스에 대해 사용할 수 있는 전체 메모리입니다. 0을 입력하여 제한이 없도록 지정합니다.

11 **저장**을 클릭합니다.

호스트에 대한 배포 정책 설정

컨테이너를 배포할 때 적용되는 특정 호스트 및 할당량에 대한 기본 설정을 지정합니다.

프로시저

1 컨테이너 호스트를 생성하거나 편집합니다.

2 오른쪽의 **배포 정책**을 클릭하여 추가 옵션이 포함된 도구 모음을 확장합니다.

3 **추가**를 클릭한 후 배포 정책 이름과 설명을 설정합니다.

4 **호스트 추가** 또는 **호스트 편집** 보기의 **배포 정책** 드롭다운 메뉴에서 정책을 선택합니다.

배치에 대한 배포 정책 설정

배치 구성에 대한 배포 정책을 설정합니다.

필수 조건

프로시저

- 1 컨테이너 탭을 클릭합니다.
- 2 배치를 클릭합니다.
- 3 배치 위로 마우스 커서를 이동하고 **편집** 아이콘을 클릭합니다.
- 4 **배포 정책** 드롭다운 목록에서 기존 정책을 선택합니다.

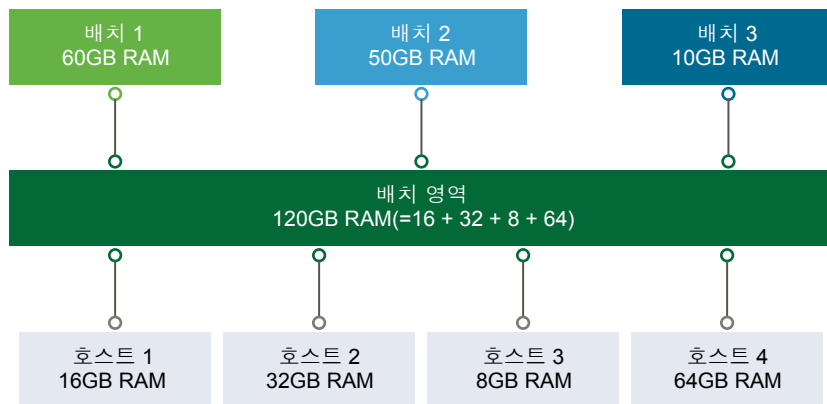
이 드롭다운 목록에는 정책을 검색하고, 새 정책을 생성하고, 정책을 관리하는 데 필요한 컨트롤도 포함되어 있습니다. [배치] 페이지의 오른쪽에 있는 **배포 정책** 아이콘을 클릭하여 정책 구성을 위한 컨트롤에 액세스할 수도 있습니다.

- 5 **저장**을 클릭합니다.

컨테이너 배치 영역 사용

배치 영역은 일련의 호스트로, 배치 영역에서 사용할 수 있는 리소스는 해당 영역 내에 있는 호스트의 모든 리소스 합을 나타냅니다. 각각의 배치는 vRealize Automation의 컨테이너에서 배치 영역에 할당됩니다. 배치 두 개 이상에서 배치 영역 하나를 관리할 수 있습니다.

배치 영역을 관리하는 배치는 풀에서 사용할 수 있는 것보다 많은 리소스를 일괄적으로 예약할 수 없습니다.



컨테이너를 프로비저닝하면 비즈니스 그룹, 사용 가능한 리소스 및 우선 순위를 기준으로 배치가 필터링됩니다.

컨테이너 설정 구성

신규 및 기존의 컨테이너 구성 속성과 설정을 사용하여 단일 컨테이너 또는 다중 컨테이너 애플리케이션을 정의할 수 있습니다.

핵심적인 vRealize Automation의 컨테이너 설정 외에, 컨테이너 구성 요소를 사용하는 배포에 다음과 같은 vRealize Automation 설정도 사용할 수 있습니다.

- 상태 구성
- 링크
- 노출된 서비스
- 클러스터 크기 및 축소/확장 매개 변수

컨테이너 에 상태 점검 구성

사용자 지정 기준을 바탕으로 컨테이너의 상태를 업데이트하도록 상태 점검 방법을 구성할 수 있습니다.

컨테이너에서 명령을 실행할 때 HTTP 또는 TCP 프로토콜을 사용할 수 있습니다. 상태 점검 방법을 지정할 수도 있습니다.

필수 조건

- 지원되는 vRealize Automation 배포에서 vRealize Automation의 컨테이너이 사용하도록 설정되었는지 확인하십시오.
- **컨테이너 관리자** 또는 **컨테이너 설계자** 역할 권한이 있는지 확인하십시오.

프로시저

- 1 vRealize Automation에 로그인합니다.
- 2 **컨테이너** 탭을 클릭합니다.
- 3 왼쪽 창에서 **템플릿**을 클릭합니다.
- 4 템플릿 또는 이미지를 편집합니다.

옵션	설명
템플릿을 편집하려면 다음과 같이 하십시오.	<ul style="list-style-type: none"> ■ 열리는 템플릿의 오른쪽 위 섹션에서 편집을 클릭합니다. ■ 템플릿에 여러 템플릿이 포함되어 있는 경우 편집하려는 템플릿을 가리키고 열리는 템플릿의 오른쪽 위 섹션에서 편집을 클릭합니다.
이미지를 편집하려면 다음과 같이 하십시오.	이미지의 프로비저닝 버튼 옆의 화살표를 클릭하고 추가 정보 입력 을 클릭합니다.

- 5 **상태 구성** 탭을 클릭합니다.

6 상태 모드를 선택합니다.

표 2-20. 상태 구성 모드

모드	설명
없음	기본값. 상태 점검이 구성되지 않습니다.
HTTP	HTTP를 선택하는 경우 액세스할 API, 사용할 HTTP 방법 및 버전을 입력해야 합니다. API는 상대적이며 컨테이너의 주소를 입력할 필요가 없습니다. 작업에 대한 시간 초과 기간을 지정하고 상태 임계값을 설정할 수도 있습니다. 예를 들어 정상 상태 임계값 2는 컨테이너가 정상이고 실행 중 상태로 간주하려면 연속 호출 성공이 2회 발생해야 한다는 것을 의미합니다. 비정상 상태 임계값 2는 컨테이너가 비정상이고 오류 상태로 간주하려면 호출 실패가 2회 발생해야 한다는 것을 의미합니다. 정상 상태 및 비정상 상태 임계값 사이의 모든 상태의 경우 컨테이너 상태는 저하됩니다.
TCP 연결	TCP 연결을 선택하는 경우 컨테이너에 대한 포트만 입력해야 합니다. 상태 점검이 제공된 포트에서 컨테이너와의 TCP 연결 설정을 시도합니다. 작업에 대한 시간 초과 값을 지정하고 HTTP로 정상 또는 비정상 상태 임계값을 설정할 수도 있습니다.
명령	명령을 선택하는 경우 컨테이너에서 실행될 명령을 입력해야 합니다. 상태 점검 성공 여부는 명령 종료 상태로 결정됩니다.
프로비저닝 시 상태 점검 무시	프로비저닝 시 상태 점검을 강제하려면 이 옵션을 선택 취소합니다. 강제하면 하나의 성공적인 상태 점검이 통과될 때까지 컨테이너가 프로비저닝된 것으로 고려되지 않습니다.
자동 배포	컨테이너가 오류 상태일 때 컨테이너를 자동으로 다시 배포합니다.

7 템플릿으로 저장을 클릭하여 설정을 저장하거나 비즈니스 그룹을 선택하고 프로비저닝을 클릭하여 컨테이너를 배포합니다.

컨테이너 에 링크 구성

링크와 노출된 서비스는 컨테이너 서비스 사이의 통신과 호스트 사이의 로드 밸런싱을 처리합니다. 컨테이너에서 컨테이너에 대한 링크 설정을 구성할 수 있습니다.

애플리케이션에서 여러 서비스 간에 통신할 수 있도록 지원하는 링크를 사용할 수 있습니다. 컨테이너의 링크는 Docker 링크와 유사하지만, 호스트 사이에서 컨테이너들을 연결합니다. 링크는 서비스 이름과 별칭의 두 부분으로 구성됩니다. 서비스 이름은 호출되는 서비스나 템플릿의 이름입니다. 별칭은 서비스와의 통신에 사용하는 호스트 이름입니다.

예를 들어, 웹 및 데이터베이스 서비스를 포함하는 애플리케이션이 있고 **my-db** 별칭을 사용하여 웹 서비스에서 데이터베이스 서비스에 대한 링크를 정의하는 경우, 웹 서비스 애플리케이션은 my-db: {PORT_OF_DB}에 대한 TCP 연결을 개시합니다. PORT_OF_DB는 컨테이너 설정에 의해 호스트에 할당되는 공용 포트와는 상관없이, 데이터베이스가 수신 대기하는 포트입니다. MySQL이 기본 포트인 3306 포트에서 업데이트 여부를 확인 중이고 컨테이너 호스트에 대해 게시된 포트가 32799인 경우, 웹 애플리케이션은 my-db:3306로 데이터베이스에 액세스합니다.

참고 링크 대신 네트워크를 사용하는 것이 좋습니다. 링크는 이제 컨테이너 클러스터를 연결할 때 다음 사항을 포함해 상당한 제한이 있는 구식 Docker 기능입니다.

- Docker는 같은 별칭을 가진 여러 개의 링크를 지원하지 않습니다. vRealize Automation의 컨테이너에서 자동으로 링크 별칭을 생성하도록 허용하는 것이 좋습니다.
- 런타임에서 컨테이너의 링크를 업데이트할 수 없습니다. 연결된 클러스터를 확장하거나 축소할 때 종속된 컨테이너의 링크는 업데이트되지 않습니다.

필수 조건

- 지원되는 vRealize Automation 배포에서 vRealize Automation의 컨테이너이 사용하도록 설정되었는지 확인하십시오.
- **컨테이너 관리자** 또는 **컨테이너 설계자** 역할 권한이 있는지 확인하십시오.
- 브리지 네트워크를 서비스 연결에 사용할 수 있는지 확인합니다.
- 대상 서비스의 내부 포트가 게시되어 있는지 확인합니다. 교차 통신을 위해, 서비스를 다른 포트로 매핑할 수 있지만 호스트 외부에서 서비스에 액세스할 수 있어야 합니다.
- 서비스 호스트가 서로 액세스할 수 있는지 확인합니다.

프로시저

- 1 vRealize Automation에 로그인합니다.
- 2 **컨테이너** 탭을 클릭합니다.
- 3 왼쪽 창에서 **템플릿**을 클릭합니다.
- 4 템플릿 또는 이미지를 편집합니다.

옵션	설명
템플릿을 편집하려면 다음과 같이 하십시오.	<ul style="list-style-type: none"> ■ 열려는 템플릿의 오른쪽 위 섹션에서 편집을 클릭합니다. ■ 템플릿에 여러 템플릿이 포함되어 있는 경우 편집하려는 템플릿을 가리키고 열려는 템플릿의 오른쪽 위 섹션에서 편집을 클릭합니다.
이미지를 편집하려면 다음과 같이 하십시오.	이미지의 프로비저닝 버튼 옆의 화살표를 클릭하고 추가 정보 입력 을 클릭합니다.

- 5 템플릿을 편집하려면 다음과 같이 하십시오.
 - a 열려는 템플릿의 오른쪽 위 섹션에서 **편집**을 클릭합니다.
 - b 템플릿에 여러 템플릿이 포함되어 있는 경우 편집하려는 템플릿을 가리키고 열려는 템플릿의 오른쪽 위 섹션에서 **편집**을 클릭합니다.

6 이미지를 편집하려면 다음과 같이 하십시오.

- a 이미지의 **프로비저닝** 버튼 옆의 화살표를 클릭하고 **추가 정보 입력**을 클릭합니다.

컨테이너 프로비저닝 또는 **컨테이너 정의 편집** 페이지가 나타나 편집 가능한 속성 및 설정 범주 집합에 대한 액세스를 제공합니다.

7 기본 탭을 클릭합니다.

8 **서비스** 텍스트 상자에 컨테이너가 종속되어 있는 서비스로 구성된 쉽표로 구분된 목록을 입력합니다.

9 **별칭** 텍스트 상자에 서비스 또는 서비스로 구성된 쉽표로 구분된 목록을 설명하는 이름을 입력합니다.

10 **저장**을 클릭합니다.

컨테이너 에 노출된 서비스 구성

컨테이너 설정에 주소와 자리 표시자를 입력하여 로드 밸런서에 대해 고유한 호스트 이름을 사용할 수 있습니다.

자리 표시자에 따라 URL 중 자동으로 생성되는 부분의 위치가 결정됩니다. 이 값은 각 호스트 이름에 대해 고유합니다. 이 주소는 자리 표시자의 위치를 지정하는 %s 형식의 문자를 지원합니다.

참고 자리 표시자가 사용되지 않는 경우에는 시스템 구성에 따라 호스트 이름의 접두사나 접미사로 배치됩니다.

공개적으로 노출해야 하는 서비스를 포함하고 축소 및 확장도 해야 하는 애플리케이션을 만드는 경우 요청을 각 노드로 대상 지정할 수 있는 로드 밸런서를 사용하는 것이 좋습니다. 애플리케이션을 프로비저닝한 후, 서비스가 vRealize Automation에 의해 축소되거나 확장될 때마다 로드 밸런서 구성이 업데이트됩니다.

필수 조건

- 지원되는 vRealize Automation 배포에서 vRealize Automation의 컨테이너이 사용하도록 설정되었는지 확인하십시오.
- **컨테이너 관리자** 또는 **컨테이너 설계자** 역할 권한이 있는지 확인하십시오.

프로시저

1 vRealize Automation에 로그인합니다.

2 **컨테이너** 탭을 클릭합니다.

3 왼쪽 창에서 **템플릿**을 클릭합니다.

4 템플릿 또는 이미지를 편집합니다.

옵션	설명
템플릿을 편집하려면 다음과 같이 하십시오.	<ul style="list-style-type: none"> 열려는 템플릿의 오른쪽 위 섹션에서 편집을 클릭합니다. 템플릿에 여러 템플릿이 포함되어 있는 경우 편집하려는 템플릿을 가리키고 열려는 템플릿의 오른쪽 위 섹션에서 편집을 클릭합니다.
이미지를 편집하려면 다음과 같이 하십시오.	이미지의 프로비저닝 버튼 옆의 화살표를 클릭하고 추가 정보 입력 을 클릭합니다.

5 네트워크 탭을 클릭합니다.

6 주소 텍스트 상자에 자리 표시자의 위치를 입력합니다.

주소 호스트가 가상 호스트로 작동합니다. 주소 호스트에 액세스하려면 etc/hosts 파일에 매핑 정보를 추가하거나 컨테이너 주소를 호스트 이름에 매핑하는 DNS를 사용할 수 있습니다.

7 컨테이너 포트 텍스트 상자에 서비스 노출에 사용되는 포트 번호를 입력합니다.

양식에 제공되는 샘플 형식을 사용하십시오. 컨테이너 애플리케이션이 두 개 이상의 포트를 노출하는 경우, 어떤 내부 포트가 서비스를 노출할 수 있는지 지정합니다.

8 저장을 클릭합니다.

컨테이너 에서 클러스터 크기 및 스케일 구성

클러스터 크기를 지정하는 컨테이너 배치 설정을 사용하여 컨테이너 클러스터를 생성할 수 있습니다.

클러스터를 구성하면 컨테이너는 지정된 개수의 컨테이너를 프로비저닝합니다. 요청은 클러스터에 있는 모든 컨테이너 사이에서 로드 밸런싱됩니다.

프로비저닝된 컨테이너 또는 애플리케이션에서 클러스터 크기를 수정하여 클러스터의 크기를 하나 단위로 늘리거나 줄일 수 있습니다. 런타임에 클러스터 크기를 수정할 때는 모든 선호도 필터와 배치 규칙이 고려됩니다.

필수 조건

- 지원되는 vRealize Automation 배포에서 vRealize Automation의 컨테이너이 사용하도록 설정되었는지 확인하십시오.
- 컨테이너 관리자 또는 컨테이너 설계자 역할 권한이 있는지 확인하십시오.

프로시저

1 vRealize Automation에 로그인합니다.

2 컨테이너 탭을 클릭합니다.

3 왼쪽 창에서 **템플릿**을 클릭합니다.

4 템플릿 또는 이미지를 편집합니다.

옵션	설명
템플릿을 편집하려면 다음과 같이 하십시오.	<ul style="list-style-type: none"> 열려는 템플릿의 오른쪽 위 섹션에서 편집을 클릭합니다. 템플릿에 여러 템플릿이 포함되어 있는 경우 편집하려는 템플릿을 가리키고 열려는 템플릿의 오른쪽 위 섹션에서 편집을 클릭합니다.
이미지를 편집하려면 다음과 같이 하십시오.	이미지의 프로비저닝 버튼 옆의 화살표를 클릭하고 추가 정보 입력 을 클릭합니다.

5 정책 탭을 클릭합니다.

6 컨테이너 클러스터 크기를 설정합니다.

7 템플릿을 저장하거나 프로비저닝합니다.

옵션	설명
템플릿을 편집하는 경우	저장을 클릭합니다.
이미지를 편집하는 경우	<ul style="list-style-type: none"> a 비즈니스 그룹을 선택합니다. b 템플릿으로 저장을 클릭하여 설정을 저장하거나, 프로비저닝을 클릭하여 컨테이너를 배포합니다.

컨테이너에서 템플릿 및 이미지 구성 및 사용

컨테이너에서는 템플릿을 사용하여 컨테이너를 프로비저닝합니다.

템플릿은 컨테이너 하나 또는 일련의 컨테이너를 프로비저닝할 수 있도록 하는 재사용 가능한 구성입니다. 템플릿에서는 연결된 서비스로 구성된 다중 계층 애플리케이션을 정의할 수 있습니다.

서비스는 유형 또는 이미지가 같은 컨테이너 하나 이상으로 정의됩니다.

템플릿 페이지의 기존 템플릿을 토대로 사용자 지정 컨테이너 템플릿을 생성할 수도 있고, 올바른 형식의 YAML 파일을 가져올 수도 있습니다. 또한 컨테이너 템플릿 또는 이미지를 프로비저닝할 수 있습니다.

사용자 지정 컨테이너 템플릿 생성

사용자 지정 템플릿을 생성하여 컨테이너를 정의하는 데 사용할 수 있습니다.

템플릿은 컨테이너 또는 컨테이너 그룹을 프로비저닝하는 데 사용할 수 있는 재사용 가능 구성입니다.

정의하는 레지스트리를 기반으로 [템플릿] 페이지에 사용할 수 있는 템플릿 이미지가 표시됩니다. 기존 템플릿 이미지를 기반으로 사용자 지정 템플릿을 생성하거나 템플릿 또는 Docker Compose 파일을 가져올 수 있습니다. [컨테이너 템플릿 또는 Docker Compose 파일 가져오기](#) 항목을 참조하십시오.

[템플릿 또는 이미지에서 컨테이너 프로비저닝](#)에 설명된 대로 **프로비저닝 > 추가 정보 입력** 옵션을 사용하여 사용자 지정 템플릿 또는 이미지를 생성할 수도 있습니다.

필수 조건

- **컨테이너 관리자** 역할 권한이 있는지 확인하십시오.

프로시저

1 컨테이너 관리자로 vRealize Automation 콘솔에 로그인합니다.

2 컨테이너 탭을 클릭합니다.

3 왼쪽 창에서 **템플릿**을 클릭합니다.

목록에 프로비저닝에 대해 사용할 수 있는 템플릿 및 이미지가 표시됩니다.

- 이미지 보기에 구성된 템플릿이 표시됩니다.
- **템플릿** 보기에 기존 또는 사용자 지정 템플릿이 표시됩니다.
- 지정된 레지스트리를 기반으로 **모두** 보기에 사용할 수 있는 모든 템플릿 및 이미지가 표시됩니다.

가져오기 및 **내보내기** 옵션을 사용하여 템플릿 및 이미지를 내보내거나 가져올 수도 있습니다.

4 템플릿에 포함할 이미지의 **프로비저닝** 버튼 옆의 화살표를 클릭합니다.

5 **추가 정보 입력**을 클릭합니다.

6 **템플릿으로 저장**을 클릭하여 변경 내용을 vRealize Automation을 위한 컨테이너에 새 컨테이너 템플릿으로 저장합니다.

후속 작업

향후 프로비저닝을 위해 템플릿을 편집할 수 있습니다. 템플릿으로부터 프로비저닝된 기존 애플리케이션은 프로비저닝 후 템플릿에 가하는 변경 내용에 영향을 받지 않습니다.

컨테이너 템플릿 또는 Docker Compose 파일 가져오기

가져온 Docker Container 템플릿 또는 Docker Compose YAML 파일을 vRealize Automation의 컨테이너에서 사용자 지정 템플릿으로 사용할 수 있습니다.

YAML 파일을 사용하는 경우 YAML 파일의 콘텐츠를 텍스트로 입력하거나 YAML 파일을 찾아서 업로드합니다. YAML 파일은 템플릿, 다양한 컨테이너에 대한 구성 및 연결을 나타냅니다. 지원되는 형식 유형은 Docker Compose YAML 및 vRealize Automation의 컨테이너 YAML입니다.

vRealize Automation의 컨테이너 YAML은 Docker Compose와 유사하지만 vRealize Automation REST API 또는 vRealize CloudClient에서 표시할 수 있는 vRealize Automation Blueprint YAML 형식을 사용합니다. vRealize Automation의 컨테이너 YAML을 사용하면 기존 Docker Compose 애플리케이션을 가져와서 컨테이너를 사용하여 수정하고, 프로비저닝하고, 관리할 수 있습니다.

필수 조건

- 지원되는 vRealize Automation 배포에서 vRealize Automation의 컨테이너가 사용하도록 설정되었는지 확인하십시오.
- **컨테이너 관리자**로 vRealize Automation 콘솔에 로그인합니다.

vRealize Automation 서비스 REST API에서 사용되는 YAML 형식에 대한 자세한 내용은 vRealize Automation API 참조를 참조하십시오.

프로시저

1 컨테이너 탭을 클릭합니다.

2 왼쪽 창에서 **템플릿**을 클릭합니다.

목록에 프로비저닝에 대해 사용할 수 있는 템플릿 및 이미지가 표시됩니다.

- 이미지 보기에 구성된 템플릿이 표시됩니다.
- **템플릿** 보기에 기존 또는 사용자 지정 템플릿이 표시됩니다.
- 지정된 레지스트리를 기반으로 **모두** 보기에 사용할 수 있는 모든 템플릿 및 이미지가 표시됩니다.

가져오기 및 **내보내기** 옵션을 사용하여 템플릿 및 이미지를 내보내거나 가져올 수도 있습니다.

3 **템플릿 또는 Docker Compose 가져오기** 아이콘을 클릭합니다.

[템플릿 가져오기] 페이지가 나타납니다.

4 YAML 파일 콘텐츠를 입력합니다.

옵션	설명
파일에서 로드	파일에서 로드를 클릭하여 디렉토리에서 YAML 파일을 찾아 선택합니다.
템플릿 또는 Docker Compose 입력	템플릿 또는 Docker Compose 입력 텍스트 상자에 올바른 형식의 YAML 파일 콘텐츠를 붙여 넣습니다.

5 **가져오기**를 클릭합니다.

템플릿 보기에 새 템플릿이 나타납니다.

템플릿 또는 이미지에서 컨테이너 프로비저닝

[템플릿] 보기의 템플릿 또는 이미지에서 컨테이너를 프로비저닝할 수 있습니다.

프로비저닝 프로세스는 프로비저닝에 사용하는 템플릿 또는 이미지에 존재하는 구성 설정을 기반으로 컨테이너를 생성합니다.

템플릿 또는 이미지에서 기존 구성 설정을 사용하거나 구성 설정을 편집한 후 프로비저닝하여 컨테이너를 프로비저닝할 수 있습니다.

사용자 지정된 새로운 컨테이너 템플릿 또는 이미지를 생성하도록 구성 설정을 편집하고 저장할 수도 있습니다.

필수 조건

- 지원되는 vRealize Automation 배포에서 vRealize Automation의 컨테이너이 사용하도록 설정되었는지 확인하십시오.
- **컨테이너 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 컨테이너 탭을 클릭합니다.

2 왼쪽 창에서 **템플릿**을 클릭합니다.

목록에 프로비저닝에 대해 사용할 수 있는 템플릿 및 이미지가 표시됩니다.

- 이미지 보기에 구성된 템플릿이 표시됩니다.
- **템플릿** 보기에 기존 또는 사용자 지정 템플릿이 표시됩니다.
- 지정된 레지스트리를 기반으로 **모두** 보기에 사용할 수 있는 모든 템플릿 및 이미지가 표시됩니다.

가져오기 및 **내보내기** 옵션을 사용하여 템플릿 및 이미지를 내보내거나 가져올 수도 있습니다.

3 모두, 이미지 또는 템플릿 보기 옵션을 사용하여 프로비저닝할 이미지 또는 템플릿을 볼 수 있습니다.

4 템플릿 또는 이미지를 프로비저닝합니다.

옵션	설명
기존 설정을 사용하여 프로비저닝합니다.	<p>a 프로비저닝을 클릭합니다.</p> <p>[프로비저닝 요청] 보기는 프로비저닝 성공에 대한 정보를 표시합니다.</p>
설정을 편집하여 프로비저닝합니다.	<p>a 프로비저닝 버튼 옆의 화살표를 클릭합니다.</p> <p>b 추가 정보 입력을 클릭합니다.</p> <p>c 컨테이너 프로비저닝 양식에 컨테이너에 대한 추가 정보를 입력합니다.</p> <p>d 양식 업데이트가 완료되면 프로비저닝을 클릭하고 수정된 설정을 사용하여 프로비저닝합니다.</p> <p>e 템플릿으로 저장을 클릭하여 변경 내용을 vRealize Automation의 컨테이너에 새 컨테이너 템플릿으로 저장합니다.</p> <p>[프로비저닝 요청] 보기는 프로비저닝 성공에 대한 정보를 표시합니다.</p>

컨테이너 템플릿 또는 Docker Compose 파일 내보내기

컨테이너 템플릿을 Docker Compose YAML 파일 또는 vRealize Automation의 컨테이너 YAML 파일로 내보낼 수 있습니다.

템플릿을 가져와서 vRealize Automation REST API 또는 vRealize CloudClient를 사용하여 프로그래밍 방식으로 또는 컨테이너에서 그래프 방식으로 수정할 수 있습니다. 그런 다음 수정된 파일을 내보낼 수 있습니다. 예를 들어, Docker Compose 형식으로 가져와서 vRealize Automation 구성-서비스 API에 사용되는 Blueprint YAML 형식으로 내보낼 수 있습니다. 하지만 상태 구성 및 선호도 제약 조건과 같은 컨테이너 특유의 일부 구성은 Docker Compose 형식으로 템플릿을 내보내는 경우 포함되지 않습니다.

필수 조건

- 지원되는 vRealize Automation 배포에서 vRealize Automation의 컨테이너이 사용하도록 설정되었는지 확인하십시오.
- **컨테이너 관리자**로 vRealize Automation 콘솔에 로그인합니다.

vRealize Automation 서비스 REST API에서 사용되는 YAML 형식에 대한 자세한 내용은 vRealize Automation API 참조를 참조하십시오.

프로시저

1 컨테이너 탭을 클릭합니다.

2 왼쪽 창에서 **템플릿**을 클릭합니다.

목록에 프로비저닝에 대해 사용할 수 있는 템플릿 및 이미지가 표시됩니다.

- 이미지 보기에 구성된 템플릿이 표시됩니다.
- **템플릿** 보기에 기존 또는 사용자 지정 템플릿이 표시됩니다.
- 지정된 레지스트리를 기반으로 **모두** 보기에 사용할 수 있는 모든 템플릿 및 이미지가 표시됩니다.

가져오기 및 **내보내기** 옵션을 사용하여 템플릿 및 이미지를 내보내거나 가져올 수도 있습니다.

3 템플릿을 가리키고 **내보내기** 아이콘을 클릭합니다.

4 메시지가 표시되면 출력 형식 유형을 선택합니다.

■ YAML Blueprint

이 형식은 vRealize Automation 구성-서비스 API에 사용되는 Blueprint YAML 형식을 준수합니다.

■ Docker Compose

이 형식은 Docker Compose 애플리케이션에 사용되는 YAML 형식을 준수합니다.

5 **내보내기(Export)**를 클릭합니다.

6 메시지가 표시되면 파일을 저장하거나 적절한 애플리케이션을 사용하여 엽니다.

컨테이너 레지스트리 사용

Docker 레지스트리는 상태 비저장 서버 쪽 애플리케이션입니다. vRealize Automation의 컨테이너의 레지스트리를 사용하여 Docker 이미지를 저장 및 배포할 수 있습니다.

레지스트리를 구성하려면 해당 주소, 사용자 지정 레지스트리 이름, 그리고 원하는 경우 자격 증명을 제공해야 합니다. 주소는 레지스트리의 보안 여부를 지정하도록 HTTP 또는 HTTPS로 시작해야 합니다. 연결 유형을 제공하지 않으면 HTTPS가 기본적으로 사용됩니다.

참고 HTTP의 경우 포트 80을 선언하고, HTTPS의 경우에는 포트 443을 선언해야 합니다. 포트를 지정하지 않는 경우 Docker 엔진에서는 포트 5000을 예상하므로 연결이 끊어질 수 있습니다.

참고 HTTP는 안전하지 않은 것으로 간주되므로 HTTP 레지스트리는 사용하지 않는 것이 좋습니다. HTTP를 사용하려는 경우 각 호스트에서 DOCKER_OPTS 속성을 다음과 같이 수정해야 합니다.

```
DOCKER_OPTS="--insecure-registry myregistrydomain.com:5000"
```

자세한 내용은 Docker 설명서(<https://docs.docker.com/registry/insecure/>)를 참조하십시오.

컨테이너는 Docker 레지스트리 HTTP API V1 및 V2와 다음과 같은 방식으로 상호 작용할 수 있습니다.

HTTP를 통한 V1(비보안, 일반 HTTP 레지스트리)	이러한 종류의 레지스트리는 자유롭게 검색할 수 있지만 각각의 Docker 호스트를 --insecure-registry 플래그로 수동으로 구성하여 안전하지 않은 레지스트리의 이미지를 기반으로 컨테이너를 프로비저닝해야 합니다. 속성을 설정한 후에는 Docker 데몬을 다시 시작해야 합니다.
HTTPS를 통한 V1	NGINX 같은 역방향 프록시 뒤에 사용합니다. 표준 구현은 https://github.com/docker/docker-registry 에서 오픈 소스로 사용할 수 있습니다.
HTTPS를 통한 V2	표준 구현은 https://github.com/docker/distribution 에서 오픈 소스로 사용할 수 있습니다.
HTTPS를 통한 V2(기본 인증)	표준 구현은 https://github.com/docker/distribution 에서 오픈 소스로 사용할 수 있습니다.
HTTPS를 통한 V2(중앙 서비스를 통한 인증)	Docker 레지스트리를 권한 부여 상태를 확인하지 않는 독립형 모드에서 실행할 수 있습니다. 지원되는 타사 레지스트리는 JFrog Artifactory 및 Harbor입니다. Docker Hub는 모든 테넌트에 대해 기본적으로 사용하도록 설정되고 레지스트리 목록에 표시되지 않지만 시스템 속성을 통해 사용하지 않도록 설정할 수 있습니다.

참고 Docker는 알 수 없는 인증 기관에서 서명한 인증서로 구성된 보안 레지스트리와는 정상적으로 상호 작용하지 않습니다. 컨테이너 서비스는 이러한 상황을 처리하기 위해 신뢰할 수 없는 인증서를 모든 Docker 호스트로 자동으로 업로드하고 호스트가 이러한 레지스트리에 연결할 수 있도록 합니다. 지정한 호스트로 인증서를 업로드할 수 없으면 호스트가 자동으로 사용하지 않도록 설정됩니다.

컨테이너 레지스트리 생성 및 관리

여러 레지스트리를 구성하여 공용 및 개인 이미지에 대한 액세스를 얻을 수 있습니다.

레지스트리는 이미지를 업로드 또는 다운로드하는 공용 또는 개인 저장소입니다. 생성한 레지스트리를 사용하지 않도록 설정하고 편집하거나 삭제할 수 있습니다. **템플릿** 탭에 표시되는 이미지는 귀하가 정의하는 레지스트리를 기반으로 합니다.

[기존 레지스트리] 페이지에서 레지스트리를 생성 또는 관리하는 경우 **자격 증명** 또는 **인증서** 버튼을 클릭하여 자격 증명 및 인증서를 추가 또는 관리할 수 있습니다.

필수 조건

- **컨테이너 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 하나 이상의 호스트가 구성되었고 컨테이너 네트워크 구성에 대해 사용할 수 있는지 확인하십시오.

프로시저

- 1 **컨테이너** 탭을 클릭합니다.
- 2 [템플릿]을 클릭합니다.

3 레지스트리 관리를 클릭합니다.

[기존 레지스트리] 페이지가 나타납니다.

4 추가를 클릭합니다.

5 레지스트리 주소를 입력합니다.

6 레지스트리의 이름을 입력합니다.

7 드롭다운 목록에서 로그인 자격 증명을 선택합니다.

8 (선택 사항) 확인을 클릭하여 구성된 매개 변수가 유효함을 확인합니다.

9 저장을 클릭하여 레지스트리를 추가합니다.

컨테이너에 대해 네트워크 리소스 구성

vRealize Automation의 컨테이너 애플리케이션에서 네트워크 구성을 생성하고 수정하고 컨테이너 및 컨테이너 템플릿에 연결할 수 있습니다.

컨테이너를 프로비저닝할 때 네트워크 구성이 포함되고 사용할 수 있습니다. vRealize Automation Blueprint에 추가한 컨테이너 구성 요소에 대해 네트워크 설정을 사용자 지정할 수 있습니다.

컨테이너를 위한 새 네트워크 생성

적합한 네트워크 구성을 사용할 수 없는 경우 vRealize Automation에서 새 네트워크 구성을 생성할 수 있습니다.

필수 조건

- 컨테이너 관리자, 컨테이너 설계자 또는 IaaS 관리자 역할 권한이 있는지 확인하십시오.
- 하나 이상의 호스트가 구성되었고 컨테이너 네트워크 구성에 대해 사용할 수 있는지 확인하십시오.

프로시저

1 vRealize Automation에 로그인합니다.

2 컨테이너 탭을 클릭합니다.

3 왼쪽 창에서 네트워크를 선택합니다.

주 패널에 컨테이너 배포의 일부로 프로비저닝할 수 있는 기존 네트워크 구성이 표시됩니다. 네트워크 구성에는 추가된 Docker 호스트에서 수집된 항목과 vRealize Automation에서 생성된 항목이 모두 포함됩니다. 네트워크 구성을 나타내는 아이콘에 네트워크 및 IPAM 드라이버, 서브넷, 게이트웨이 및 IP 범위 정보, 네트워크 구성을 사용 중인 컨테이너 수 및 호스트 수가 표시됩니다.

4 네트워크 생성을 클릭합니다.

5 네트워크의 이름을 입력합니다.

새 구성 생성을 완료하면 고유 식별자가 있는 이름 값이 추가됩니다.

6 (선택 사항) 보다 세부적인 구성 설정을 추가하려면 고급 확인란을 선택합니다.

[네트워크 추가] 패널에 추가 네트워크 구성 설정이 나타납니다.

7 고급 네트워크 구성 설정을 구성합니다.

옵션	설명
IPAM 구성	서브넷 이 네트워크 구성에 고유한 서브넷 및 게이트웨이 주소를 입력합니다. 이들 값이 같은 컨테이너 호스트 상의 다른 네트워크와 겹치면 안 됩니다.
사용자 지정 속성	선택적으로, 새 네트워크 구성에 대한 사용자 지정 속성을 지정할 수 있습니다. <code>containers.ipam.driver</code> 컨테이너에만 사용할 수 있습니다. Blueprint에 컨테이너 네트워크 구성 요소를 추가할 때 사용될 IPAM 드라이버를 지정합니다. 지원되는 값은 드라이버가 사용되는 컨테이너 호스트 환경에 설치된 드라이버에 따라 다릅니다. 예를 들어 지원되는 값은 컨테이너 호스트에 설치된 IPAM 플러그인에 따라 infoblox 또는 calico 일 수 있습니다. 이 속성 이름 및 값은 대/소문자를 구분합니다. 속성 값을 추가하면 해당 값이 검증되지 않습니다. 프로비저닝 시 컨테이너 호스트에 지정된 드라이버가 없는 경우 오류 메시지가 반환되고 프로비저닝이 실패합니다. <code>containers.network.driver</code> 컨테이너에만 사용할 수 있습니다. Blueprint에 컨테이너 네트워크 구성 요소를 추가할 때 사용될 네트워크 드라이버를 지정합니다. 지원되는 값은 드라이버가 사용되는 컨테이너 호스트 환경에 설치된 드라이버에 따라 다릅니다. 기본적으로 VCH(가상 컨테이너 호스트) 제공 네트워크 드라이버에는 브리지 드라이버가 포함되는 반면 Docker 제공 네트워크 드라이버에는 브리지, 오버레이 및 macvlan이 포함됩니다. 컨테이너 호스트에 설치되어 있는 네트워크 플러그인에 따라 weave 및 calico와 같은 타사 네트워크 드라이버도 사용할 수 있습니다. 이 속성 이름 및 값은 대/소문자를 구분합니다. 속성 값을 추가하면 해당 값이 검증되지 않습니다. 프로비저닝 시 컨테이너 호스트에 지정된 드라이버가 없는 경우 오류 메시지가 반환되고 프로비저닝이 실패합니다.

참고 고급 설정 없이 네트워크를 생성하는 경우 vRealize Automation에서 설정을 자동으로 제공합니다.

8 드롭다운 메뉴에서 네트워크를 연결할 호스트를 선택합니다.

9 생성을 클릭합니다.

컨테이너 템플릿에 네트워크 추가

컨테이너 템플릿에 네트워크 구성을 추가하여 컨테이너를 서로 연결할 수 있습니다. 이 네트워크 구성은 템플릿을 사용하는 어떤 애플리케이션에 대해서든 자동으로 구현됩니다. 필요에 따라 기존 네트워크를 추가하거나 새 네트워크를 구성하고 추가할 수 있습니다.

필수 조건

- 사용 가능한 템플릿이 있는지 확인합니다. 없으면 사용 가능한 템플릿부터 먼저 만들어야 합니다.
- **컨테이너 관리자**, **컨테이너 설계자** 또는 **IaaS 관리자** 역할 권한이 있는지 확인하십시오.
- 하나 이상의 호스트가 구성되었고 컨테이너 네트워크 구성에 대해 사용할 수 있는지 확인하십시오.

프로시저

1 vRealize Automation에 로그인합니다.

2 **컨테이너** 탭을 클릭합니다.

3 왼쪽 창에서 **템플릿**을 클릭합니다.

일련의 아이콘이 프로비저닝에 사용 가능한 템플릿과 이미지를 표시합니다.

4 (선택 사항) 아이콘 위쪽의 상단 오른쪽 머리글에서 **보기: 템플릿**을 클릭하여 템플릿만 표시하도록 보기를 수정합니다.

5 사용자 지정하려는 템플릿의 상단 오른쪽 섹션에서 **편집**을 클릭합니다.

더하기 기호가 있는 빈 아이콘과 컨테이너 아이콘을 표시하는 [템플릿 편집] 페이지가 나타납니다.

6 빈 아이콘을 가리킵니다.

네트워크 추가 아이콘이 나타납니다.

7 **네트워크 추가** 아이콘을 클릭합니다.

[네트워크 추가] 패널이 나타납니다.

8 기존 네트워크를 추가하거나 새 네트워크를 생성하고 추가합니다.

옵션	설명
기존 네트워크를 추가합니다.	a 기존 확인란을 클릭합니다. b 이름 필드 내부를 클릭하여 기존 네트워크 목록을 표시합니다. c 사용할 네트워크를 선택하고 저장 을 클릭합니다.
새 네트워크를 구성하고 추가합니다.	a 네트워크의 이름을 입력합니다. b 보다 세부적인 구성 설정을 추가하려면 고급 확인란을 클릭합니다. c 저장 을 클릭합니다.

[네트워크 구성 추가] 패널이 사라지고 추가된 네트워크가 [템플릿 편집] 페이지의 컨테이너 아이콘 아래에 수평 방향 아이콘으로 나타납니다. 컨테이너 아이콘의 아래쪽 테두리에도 네트워크 아이콘이 나타납니다.

9 네트워크 커넥터 아이콘을 컨테이너에서 네트워크를 나타내는 수평 방향 아이콘의 임의의 지점으로 끌어서 네트워크를 컨테이너에 연결합니다.

컨테이너 볼륨 구성

vRealize Automation의 컨테이너 애플리케이션에서 볼륨을 생성하고 수정하고 컨테이너 및 컨테이너 템플릿에 연결할 수 있습니다.

vRealize Automation의 컨테이너는 영구 데이터 관리를 위해 Docker 볼륨을 사용합니다. 볼륨을 사용하면 다음과 같은 작업을 수행할 수 있습니다.

- 같은 호스트 내에 있는 서로 다른 컨테이너 사이에 볼륨을 공유합니다.
- 데이터를 즉시 업데이트합니다.
- 컨테이너가 삭제된 이후에 볼륨 데이터를 저장합니다.

컨테이너를 위한 새 볼륨 생성

컨테이너 스토리지를 확장하려면 먼저 데이터 볼륨을 생성해야 합니다.

필수 조건

- 컨테이너 관리자, 컨테이너 설계자 또는 IaaS 관리자 역할 권한이 있는지 확인하십시오.
- 하나 이상의 호스트가 구성되었고 컨테이너 볼륨 구성에 대해 사용할 수 있는지 확인하십시오.

프로시저

1 vRealize Automation에 로그인합니다.

2 컨테이너 탭을 클릭합니다.

3 왼쪽 창에서 리소스 > 볼륨을 선택합니다.

배포된 컨테이너에 연결할 수 있는 기존 볼륨 구성이 기본 패널에 표시됩니다. 볼륨 구성에는 추가된 Docker 호스트에서 수집된 항목과 vRealize Automation에서 생성된 항목이 모두 포함됩니다. 볼륨 인스턴스는 드라이버, 범위 및 드라이버 옵션을 표시합니다.

4 볼륨 생성을 클릭합니다.

5 볼륨 이름을 입력합니다.

구성 생성을 완료하면 이름 값에 고유 식별자가 추가됩니다.

6 드라이버 텍스트 상자에 사용할 볼륨 플러그인의 드라이버를 입력합니다. 아무 것도 입력하지 않으면 로컬 드라이버가 기본값으로 사용됩니다.

7 (선택 사항) 보다 세부적인 구성 설정을 추가하려면 고급 확인란을 클릭합니다.

추가적인 구성 설정이 나타납니다.

8 (선택 사항) 고급 볼륨 설정을 구성합니다.

옵션	설명
드라이버 옵션	사용할 드라이버 옵션을 지정합니다. 옵션은 현재 사용 중인 볼륨 플러그인에 따라 다릅니다.
사용자 지정 속성	새 구성의 사용자 지정 속성을 지정합니다.

9 드롭다운 메뉴에서 볼륨을 연결할 호스트를 선택합니다.

10 생성을 클릭합니다.

[볼륨 생성] 패널이 사라지고, 추가된 볼륨이 [볼륨] 탭에 나타납니다.

후속 작업

컨테이너 템플릿에 볼륨 추가

컨테이너 템플릿에 볼륨 추가

템플릿에 볼륨을 추가하여 볼륨을 컨테이너에 연결합니다.

필수 조건

- 사용 가능한 템플릿이 있는지 확인합니다. 없으면 사용 가능한 템플릿부터 먼저 만들어야 합니다.
- **컨테이너 관리자**, **컨테이너 설계자** 또는 **IaaS 관리자** 역할 권한이 있는지 확인하십시오.
- 하나 이상의 호스트가 구성되었고 컨테이너 볼륨 구성에 대해 사용할 수 있는지 확인하십시오.

프로시저

- 1 vRealize Automation에 로그인합니다.
- 2 **컨테이너** 탭을 클릭합니다.
- 3 왼쪽 창에서 **템플릿**을 클릭합니다.
 일련의 아이콘이 프로비저닝에 사용 가능한 템플릿과 이미지를 표시합니다.
- 4 (선택 사항) 아이콘 위쪽의 상단 오른쪽 머리글에서 **보기: 템플릿**을 클릭하여 템플릿만 표시하도록 보기를 수정합니다.
- 5 사용자 지정하려는 템플릿의 상단 오른쪽 섹션에서 **편집**을 클릭합니다.
 더하기 기호가 있는 빈 아이콘을 비롯하여, 컨테이너 아이콘을 표시하는 [템플릿 편집] 페이지가 나타납니다.
- 6 **볼륨 추가** 아이콘이 나타날 때까지 더하기 기호가 있는 빈 아이콘에 커서를 올려 놓습니다.
- 7 **볼륨 추가** 아이콘을 클릭합니다.
- 8 기존 볼륨을 추가하거나 새 볼륨을 생성하고 추가합니다.

옵션	설명
기존 볼륨을 추가합니다.	a 기존 확인란을 클릭합니다. b 이름 필드 내부를 클릭하여 기존 볼륨 목록을 표시합니다. c 사용할 볼륨을 선택하고 저장 을 클릭합니다.
새 볼륨을 구성하고 추가합니다.	a 볼륨 이름을 입력합니다. b 드라이버 텍스트 상자에 사용할 볼륨 플러그인의 드라이버를 입력합니다. 외부 스토리지 시스템을 사용 중인 경우 로컬 을 입력합니다. c 보다 세부적인 구성 설정을 추가하려면 고급 확인란을 클릭합니다. d 저장 을 클릭합니다.

[볼륨 추가] 패널이 사라지고 [템플릿 편집] 페이지의 컨테이너 아이콘 아래에 추가된 볼륨이 수평 방향 아이콘으로 나타납니다. 컨테이너 아이콘의 아래쪽 테두리에도 볼륨 아이콘이 표시됩니다.

- 9 볼륨 커넥터 아이콘을 컨테이너에서 볼륨을 나타내는 수평 방향 아이콘의 임의의 지점으로 끌어서 볼륨을 컨테이너에 연결합니다.
- 10 (선택 사항) 컨테이너 경로를 클릭해서 볼륨의 마운트 위치를 변경합니다.

후속 작업

템플릿 또는 이미지에서 컨테이너 프로비저닝

기본 vRealize Orchestrator 서버에 추가적인 플러그인 설치

vRealize Orchestrator 구성 인터페이스를 사용하여 기본 vRealize Orchestrator 서버에 추가 패키지와 플러그인을 설치할 수 있습니다.

추가 플러그인을 기본 vRealize Orchestrator 서버에 설치하고 XaaS에 워크플로를 사용할 수 있습니다.

기본 vRealize Orchestrator 서버에서 추가 패키지를 가져와 vRealize Automation 외부 IPAM 제공자 끝점 유형으로 구성할 수도 있습니다. 예를 들어 Infoblox IPAM 패키지 얻기, 가져오기 및 구성에 대한 자세한 내용은 [타사 IPAM 제공자 지원을 제공하기 위한 검사 목록](#) 항목을 참조하십시오.

패키지 파일(.package)과 플러그인 설치 파일(.vmoapp 또는 .dar)은 VMware Solution Exchange(https://solutionexchange.vmware.com/store/category_groups/cloud-management)에서 구할 수 있습니다. 플러그인 파일에 대한 자세한 내용은 vRealize Orchestrator 플러그인 설명서 (https://www.vmware.com/support/pubs/vco_plugins_pubs.html)를 참조하십시오.

새 플러그인 설치에 대한 자세한 내용은 VMware vCenter Orchestrator 설치 및 구성을 참조하십시오.

Active Directory 정책 사용

Active Directory 정책은 vRealize Automation Blueprint를 사용하여 레코드가 생성되는 조직 구성 단위와 함께 시스템 레코드의 속성(예: 도메인)을 정의합니다.

비즈니스 그룹에 정책을 적용하는 경우 비즈니스 그룹 구성원의 모든 시스템 요청이 지정된 조직 구성 단위에 추가됩니다. 조직 구성 단위별로 다양한 정책을 생성한 다음 다양한 정책을 다양한 비즈니스 그룹에 적용할 수 있습니다.

Active Directory 정책은 vRealize Automation 7.1의 기술 미리보기 기능으로, 운영 환경에서 사용되어서는 안 됩니다.

사용자 지정 속성을 사용하여 Active Directory 정책 재정의

제공된 Active Directory 사용자 지정 속성을 사용하여 Active Directory 정책, 도메인, 조직 구성 단위 및 기타 값을 배포할 때 특정 Blueprint에서 재정의할 수 있습니다.

제공된 Active Directory 사용자 지정 속성의 목록은 사용자 지정 속성 참조 자료에 포함되어 있습니다. 사용자 지정 속성 접두사는 ext.policy.activedirectory입니다.

제공된 속성 외에도 고유한 사용자 지정 속성을 생성할 수 있습니다. 사용자 지정 속성 앞에 ext.policy.activedirectory를 추가해야 합니다. 예를 들면 ext.policy.activedirectory.domain.extension 또는 ext.policy.activedirectory.yourproperty입니다. 속성은 사용자 지정 vRealize Orchestrator Active Directory 워크플로로 전달됩니다.

사용자 지정 속성에 대한 자세한 내용은 사용자 지정 속성 참조 자료 항목을 참조하십시오. 재정의하는 값에 따라 속성 정의를 생성해야 할 수 있습니다. 예를 들어 vRealize Automation에서 사용 가능한 Active Directory 정책을 검색하는 속성 정의를 생성할 수 있습니다. 또는 요청한 사용자가 2개 이상의 대체 조직 구성 단위에서 선택하도록 허용하는 정의를 생성할 수 있습니다. 사용자 지정 속성 참조 자료의 내용을 참조하십시오.

Active Directory 정책 생성 및 적용

다양한 비즈니스 그룹에 다양한 정책을 할당할 수 있도록 1개 이상의 Active Directory 정책을 생성합니다. 다양한 정책을 사용하여 비즈니스 그룹 구성원 자격을 기반으로 다양한 조직 구성 단위에 시스템 레코드를 추가할 수 있습니다.

필요한 경우 할당된 Active Directory 정책을 재정의할 수 있습니다.

프로시저

1 Active Directory 정책 생성

사용자가 시스템을 배포할 때 Active Directory 인스턴스에서 레코드가 추가되는 위치를 정의하는 Active Directory 정책을 생성합니다. 비즈니스 그룹에 정책을 할당하여 비즈니스 그룹 구성원에 의해 모든 시스템이 배포되어 지정된 조직 구성 단위로 레코드가 생성되도록 합니다.

2 시나리오: Blueprint에 사용자 지정 속성을 추가하여 Active Directory 정책 재정의

개발 비즈니스 그룹에 대한 Blueprint 설계자가 애플리케이션 시스템 및 데이터베이스 시스템이 포함된 Blueprint를 가지고 있습니다. 데이터베이스 시스템 레코드를 적용된 Active Directory 정책과 다른 조직 구성 단위에 추가하려고 합니다.

Active Directory 정책 생성

사용자가 시스템을 배포할 때 Active Directory 인스턴스에서 레코드가 추가되는 위치를 정의하는 Active Directory 정책을 생성합니다. 비즈니스 그룹에 정책을 할당하여 비즈니스 그룹 구성원에 의해 모든 시스템이 배포되어 지정된 조직 구성 단위로 레코드가 생성되도록 합니다.

다양한 비즈니스 그룹에 의해 배포된 시스템이 다양한 도메인을 갖거나 다양한 Active Directory 인스턴스에 추가되도록 하려면 다양한 Active Directory 정책을 생성합니다.

필수 조건

- Active Directory 끝점을 생성했는지 확인합니다. [Active Directory 플러그인을 끝점으로 구성](#) 항목을 참조하십시오.
- 외부 vRealize Orchestrator 서버를 사용하는 경우 서버가 올바르게 설정되어 있는지 확인하십시오. [외부 vRealize Orchestrator 서버 구성](#) 항목을 참조하십시오.
- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > AD 정책**을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.

3 Active Directory 정책 세부 정보를 구성합니다.

옵션	설명
ID	영구 값을 입력합니다. 값에는 공백이나 특수 문자를 포함할 수 없습니다. 나중에 이 값을 변경할 수 없습니다. 다른 ID로 정책을 다시 생성하는 것만 가능합니다.
설명	정책에 대한 설명입니다.
Active Directory 끝점	이 정책이 생성되는 Active Directory 끝점을 선택합니다.
도메인	루트 도메인을 입력합니다. 형식은 mycompany.com입니다.
조직 구성 단위	이 정책에 대한 조직 구성 단위 고유 이름을 입력합니다. 섬표로 구분된 목록으로 계층을 입력해야 합니다. 예를 들면 ou=development,dc=corp,dc=domain,dc=com입니다.

4 확인을 클릭합니다.

vRealize Orchestrator Active Directory 끝점이 목록에 추가됩니다. 비즈니스 그룹에 정책을 적용하거나 Blueprint 또는 비즈니스 그룹의 정책을 사용할 수 있습니다.

후속 작업

- 여러 정책 옵션을 제공하려면 더 많은 정책을 생성합니다.
- Blueprint가 배포될 때 비즈니스 그룹 구성원 자격을 기반으로 Active Directory에 레코드를 추가하려면 비즈니스 그룹에 적절한 Active Directory 정책을 추가합니다. [비즈니스 그룹 생성](#) 항목을 참조하십시오. 비즈니스 그룹을 생성할 때 정책을 적용하거나 나중에 추가할 수 있습니다.
- 특정 Blueprint의 비즈니스 그룹에 대한 Active Directory 정책을 재정의하려면 해당 Blueprint에 Active Directory 사용자 지정 속성을 추가합니다. [시나리오: Blueprint에 사용자 지정 속성을 추가하여 Active Directory 정책 재정의](#) 항목을 참조하십시오.

시나리오: Blueprint에 사용자 지정 속성을 추가하여 Active Directory 정책 재정의

개발 비즈니스 그룹에 대한 Blueprint 설계자가 애플리케이션 시스템 및 데이터베이스 시스템이 포함된 Blueprint를 가지고 있습니다. 데이터베이스 시스템 레코드를 적용된 Active Directory 정책과 다른 조직 구성 단위에 추가하려고 합니다.

개발 비즈니스 그룹에 적용되는 기존 정책이 있습니다. 이 정책은

ou=development,dc=corp,dc=domain,dc=com에 시스템 레코드를 추가합니다.

ou=databases,dc=corp,dc=domain,dc=com에 모든 데이터베이스 시스템을 추가하고자 합니다. 데이터베이스 서버가 포함된 Blueprint에서 Active Directory 조직 구성 단위를 재정의하여 ou=databases,dc=corp,dc=domain,dc=com에 데이터베이스 시스템 레코드를 추가합니다.

이 시나리오에서는 다음과 같이 가정합니다.

- Active Directory에 개발 및 데이터베이스에 대한 조직 구성 단위가 포함되어 있습니다.
- 서비스에 포함된 테스트 Blueprint가 있으며 서비스에 권한이 부여되었습니다.

정책을 재정의할 수 있는 방법에 대한 이 간단한 예 외에도 Active Directory 정책과 함께 사용자 지정 속성을 사용하여 Blueprint를 배포할 때 Active Directory에 대한 다른 변경을 수행할 수 있습니다. [Active Directory 정책 사용](#) 항목을 참조하십시오.

필수 조건

- 하나 이상의 Active Directory 정책이 있는지 확인합니다. [Active Directory 정책 생성](#) 항목을 참조하십시오. 예를 들어 ou=development,dc=corp,dc=domain,dc=com에 레코드를 추가하는 개발 정책을 생성합니다.
- Active Directory 정책을 적용한 비즈니스 그룹이 있는지 확인합니다. [비즈니스 그룹 생성](#) 항목을 참조하십시오. 예를 들어 개발 비즈니스 그룹은 개발 정책을 사용합니다.

프로시저

- 1 테스트 Blueprint에서 캔버스의 데이터베이스 시스템을 선택합니다.
- 2 **속성** 탭을 클릭합니다.
- 3 **사용자 지정 속성** 탭을 클릭합니다.
- 4 **새로 만들기** 아이콘(+)을 클릭합니다.
- 5 사용자 지정 속성을 추가하여 기본 조직 구성 단위를 변경합니다.
 - a **이름** 텍스트 상자에 `ext.policy.activedirectory.orgunit`을 입력합니다.
 - b **값** 텍스트 상자에 `ou=databases,dc=corp,dc=domain,dc=com`을 입력합니다.
 - c **재정의 가능**을 선택 해제합니다.
 - d **확인**을 클릭합니다.
- 6 **완료**를 클릭합니다.

테스트 Blueprint에는 사용자 지정 속성이 포함되어 있지만 사용자가 요청 양식에서 해당 사용자 지정 속성을 볼 수 없습니다.

후속 작업

테스트 Blueprint를 요청합니다. 데이터베이스 시스템에 대한 레코드가 데이터베이스 조직 구성 단위에 추가되었으며 애플리케이션 시스템에 대한 레코드가 개발 조직 구성 단위에 추가되었는지 확인합니다. 결과에 만족하는 경우 운영 Blueprint에 사용자 지정 속성을 추가할 수 있습니다.

사용자에게 서비스 Blueprint 제공

3

요청 시 서비스는 카탈로그 항목과 작업을 생성한 후, 사용 권한 및 승인 기능을 사용하여 해당 서비스를 요청할 수 있는 사용자를 신중하게 제어하는 방법으로 사용자에게 제공할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

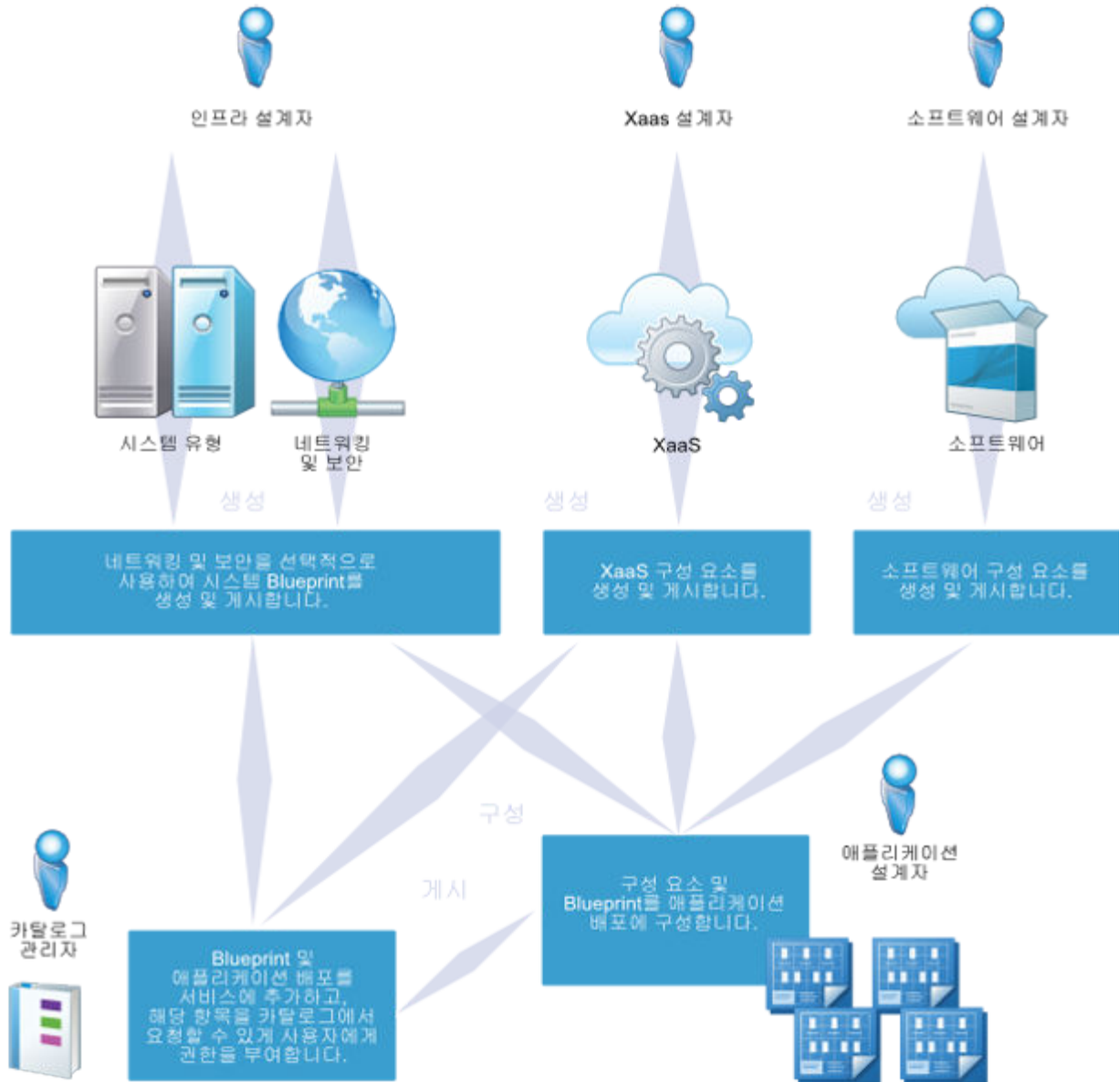
- [Blueprint 설계](#)
- [Blueprint와 콘텐츠 내보내기 및 가져오기](#)
- [설계 라이브러리 구축](#)
- [복합 Blueprint 구성](#)
- [서비스 카탈로그 관리](#)
- [배포된 카탈로그 항목 관리](#)

Blueprint 설계

Blueprint 설계자는 Software 구성 요소, 시스템 Blueprint 및 사용자 지정 XaaS Blueprint를 빌드하고 그러한 구성 요소를 사용자가 카탈로그에서 요청하는 항목을 정의하는 Blueprint에 구성합니다.

단일 시스템에 대한 Blueprint 또는 단일 사용자 지정 XaaS Blueprint를 생성 및 게시할 수 있지만 시스템 구성 요소와 XaaS Blueprint를 다른 빌딩 블록과 결합하여 여러 시스템, 네트워킹 및 보안, 전체 수명 주기를 지원하는 소프트웨어, 사용자 지정 XaaS 기능을 포함하는 정교한 카탈로그 항목 Blueprint를 설계할 수 있습니다.

정의하려는 카탈로그 항목에 따라 한 명의 인프라 설계자가 하나의 시스템 구성 요소를 Blueprint로 게시하는 간단한 프로세스가 될 수도 있고 프로세스에 여러 명의 설계자가 포함되어 사용자가 요청할 전체 애플리케이션 스택을 설계하기 위해 서로 다른 많은 유형의 구성 요소를 생성할 수도 있습니다.



Software 구성 요소

시스템 프로비저닝 프로세스 중에 소프트웨어를 설치하고 소프트웨어 수명 주기를 지원하기 위해 소프트웨어 구성 요소를 생성하고 게시할 수 있습니다. 예를 들어 개발자가 이미 설치 및 구성된 개발 환경을 사용하여 시스템을 요청하도록 Blueprint를 생성할 수 있습니다. 소프트웨어 구성 요소는 그 자체로 카탈로그 항목이 아니기 때문에 카탈로그 항목 Blueprint를 생성하려면 소프트웨어 구성 요소를 시스템 구성 요소와 결합해야 합니다.

시스템 Blueprint

단일 시스템을 프로비저닝하기 위해 간단한 Blueprint를 생성하고 게시하거나 추가 시스템 구성 요소를 포함하는 좀 더 복잡한 Blueprint를 생성할 수 있으며 필요한 경우 다음 구성 요소 유형을 원하는 대로 조합할 수 있습니다.

- Software 구성 요소
- 기존 Blueprint
- NSX 네트워크 및 보안 구성 요소
- XaaS 구성 요소
- 컨테이너 구성 요소
- 사용자 지정 또는 기타 구성 요소

XaaS Blueprint

vRealize Orchestrator 워크플로를 XaaS Blueprint로 게시할 수 있습니다. 예를 들어 Active Directory 사용자를 위한 사용자 지정 리소스를 생성하고 XaaS Blueprint를 설계하여 관리자가 해당 Active Directory 그룹에서 새 사용자를 프로비저닝하도록 허용할 수 있습니다. [설계] 탭 외부에서 XaaS 구성 요소를 생성 및 관리합니다. 최소 하나의 시스템 구성 요소와 결합하는 경우에만 게시된 XaaS Blueprint를 재사용하여 애플리케이션 Blueprint를 생성할 수 있습니다.

다중 시스템, XaaS 및 Software 구성 요소를 포함하는 애플리케이션 Blueprint

원하는 수만큼의 시스템 구성 요소, Software 구성 요소 및 XaaS Blueprint를 시스템 Blueprint에 추가하여 사용자에게 정교한 기능을 제공할 수 있습니다.

예를 들어, 관리자가 신입 사원 설정을 프로비저닝하도록 Blueprint를 생성할 수 있습니다. 새 Active Directory 사용자를 프로비저닝하기 위해 여러 시스템 구성 요소, 소프트웨어 구성 요소 및 XaaS Blueprint를 결합할 수 있습니다. QE 관리자가 신입 사원 카탈로그 항목을 요청하면 새로운 QE 직원이 Active Directory에서 프로비저닝되고 두 개의 작업 가상 시스템(하나는 Windows, 다른 하나는 Linux)이 지정되며 각각에는 이러한 환경에서 테스트 케이스를 실행하기 위한 모든 필수 소프트웨어가 포함됩니다.

Blueprint와 콘텐츠 내보내기 및 가져오기

vRealize Automation REST API 또는 vRealize CloudClient를 사용하여 한 vRealize Automation 환경의 Blueprint 및 콘텐츠를 다른 환경에 프로그래밍 방식으로 내보낼 수 있습니다.

예를 들어 개발 환경에서 Blueprint를 생성하고 테스트한 다음 이를 운영 환경으로 가져올 수 있습니다. 또는 커뮤니티 포럼에서 작성 vRealize Automation 테넌트 인스턴스로 속성 정의를 가져올 수 있습니다.

다음과 같은 vRealize Automation 콘텐츠 항목을 프로그래밍 방식으로 가져오고 내보낼 수 있습니다.

- 애플리케이션 Blueprint 및 모든 해당 구성 요소
- IaaS 시스템 Blueprint
- Software 구성 요소
- XaaS Blueprint
- 구성 요소 프로파일
- 속성 그룹

속성 그룹 정보는 테넌트별로 보유하고 속성 그룹이 대상 vRealize Automation 인스턴스에 이미 있는 경우에만 Blueprint와 함께 가져옵니다.

vRealize Automation 인스턴스 테넌트 사이에서 Blueprint를 내보내는 경우, 속성 그룹이 이미 대상 테넌트 인스턴스에 있는 경우가 아니면 해당 Blueprint에 정의된 속성 그룹 정보가 가져온 Blueprint에서 인식되지 않습니다. 예를 들어 사용자가 Blueprint를 가져온

vRealize Automation 인스턴스에 mica1 속성 그룹이 이미 있는 경우가 아니면 mica1이라는 속성 그룹이 있는 Blueprint를 가져오는 경우 mica1 속성 그룹이 가져온 Blueprint에 없습니다.

vRealize Automation 인스턴스 사이에서 Blueprint를 내보낼 때 속성 그룹 정보가 손실되지 않게 하려면 vRealize CloudClient를 사용하여 속성 그룹이 포함된 내보내기 패키지 zip 파일을 생성하고 Blueprint를 가져오기 전에 해당 패키지 zip 파일을 대상 테넌트로 가져옵니다.

vRealize CloudClient를 사용하여 속성 그룹은 물론 다른 vRealize Automation 항목을 나열하고 패키지로 만들고 내보내고 가져오는 작업에 대한 자세한 내용은 VMware Developer Center(<https://developercenter.vmware.com/tool/cloudclient>)를 참조하십시오.

표 3-1. 가져오기 및 내보내기 도구 선택

도구	추가 정보
vRealize CloudClient	https://developercenter.vmware.com/tool/cloudclient 에서 VMware 개발자 사이트를 참조하십시오.
vRealize Automation REST API	https://www.vmware.com/support/pubs/vcac-pubs.html 에서 vRealize Automation 정보 센터의 프로그래밍 가이드 항목을 참조하십시오.

참고 vRealize Automation 배포 간에 Blueprint를 프로그래밍 방식으로 내보내고 가져오는 경우(예: 테스트 환경에서 운영 환경으로 또는 특정 조직에서 다른 조직으로)에는 복제 템플릿 데이터가 패키지에 포함되었는지 확인하는 것이 중요합니다. Blueprint 패키지를 가져오면 패키지에 있는 기본 정보에 기반하여 기본 설정이 채워집니다. 예를 들어 복제 스타일 워크플로를 사용하여 생성된 Blueprint를 내보냈다가 가져올 경우, 해당 복제 데이터가 파생된 템플릿이 Blueprint를 가져오는 vRealize Automation 배포 내의 끝점에 없으면 일부 가져온 Blueprint 설정을 해당 배포에 적용할 수 없습니다.

시나리오: vSphere 샘플 애플리케이션용 Dukes Bank 가져오기 및 환경 구성

vRealize Automation을 평가하거나 학습하는 IT 전문가로서 사용 가능한 기능을 신속하게 살펴보고 현재 조직의 요구 사항을 충족할 수 있는 vRealize Automation Blueprint를 빌드하는 방법을 결정하기 위해 강력한 샘플 애플리케이션을 vRealize Automation 인스턴스로 가져오려고 합니다.

필수 조건

- CentOS 6.x Linux 참조 시스템을 준비하고, 해당 시스템을 템플릿으로 변환하고, 사용자 지정 규격을 생성합니다. [시나리오: vSphere 샘플 애플리케이션 Blueprint용 Dukes Bank 가져오기 준비](#) 항목을 참조하십시오.
- 게이트웨이 및 IP 주소 범위를 제공하기 위해 외부 네트워크 프로파일을 생성합니다. [타사 IPAM 제공자를 사용하여 외부 네트워크 프로파일 생성](#) 항목을 참조하십시오.
- 외부 네트워크 프로파일을 vSphere 예약에 매핑합니다. [Hyper-V, KVM, SCVMM, vSphere 또는 XenServer에 대한 예약 생성](#) 항목을 참조하십시오. 샘플 애플리케이션은 외부 네트워크 프로파일 없이 프로비저닝할 수 없습니다.
- **인프라 설계자** 및 **소프트웨어 설계자** 권한이 모두 있는지 확인합니다. Dukes Bank 샘플 애플리케이션을 가져오고 Dukes Bank Blueprint 및 소프트웨어 구성 요소와 상호 작용하려면 두 가지 역할이 모두 필요합니다.

프로시저

1 시나리오: vSphere 샘플 애플리케이션용 Dukes Bank 가져오기

vRealize Automation 장치에서 vSphere 애플리케이션용 Dukes Bank를 다운로드합니다. vRealize Automation 테넌트로 샘플 애플리케이션을 가져와서 네트워킹 및 소프트웨어 구성 요소와 함께 다중 시스템 구성 요소를 포함하는 다중 계층 vRealize Automation Blueprint의 작업 샘플을 봅니다.

2 시나리오: 환경에 맞게 Dukes Bank vSphere 샘플 구성 요소 구성

인프라 설계자 권한을 사용하여 환경을 위해 생성한 사용자 지정 규격, 템플릿 및 시스템 접두사를 사용하도록 Dukes Bank 시스템 구성 요소 각각을 구성합니다.

고유한 Blueprint를 직접 개발하기 위한 시작점, vRealize Automation을 평가하기 위한 도구 또는 vRealize Automation의 기능과 구성 요소를 이해하는 데 도움을 줄 수 있는 학습 리소스로 사용할 수 있도록 환경에 vSphere 샘플 애플리케이션용 Dukes Bank를 구성했습니다.

시나리오: vSphere 샘플 애플리케이션용 Dukes Bank 가져오기

vRealize Automation 장치에서 vSphere 애플리케이션용 Dukes Bank를 다운로드합니다. vRealize Automation 테넌트로 샘플 애플리케이션을 가져와서 네트워킹 및 소프트웨어 구성 요소와 함께 다중 시스템 구성 요소를 포함하는 다중 계층 vRealize Automation Blueprint의 작업 샘플을 봅니다.

프로시저

- 1 SSH를 사용하여 vRealize Automation 장치에 루트로 로그인합니다.
- 2 vRealize Automation 장치에서 /tmp로 vSphere 샘플 애플리케이션용 Dukes Bank를 다운로드합니다.

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn:5480/blueprints/DukesBankAppForvSphere.zip
```

패키지의 압축을 풀지 마십시오.

- 3 <http://developercenter.vmware.com/tool/cloudclient>에서 /tmp로 vRealize CloudClient를 다운로드합니다.
- 4 cloudclient-4x-dist.zip 패키지의 압축을 풉니다.
- 5 /bin 디렉토리에서 vRealize CloudClient를 실행합니다.

```
$>./bin/cloudclient.sh
```

- 6 메시지가 나타나면 라이선스 계약에 동의합니다.
- 7 vRealize CloudClient를 사용하여 **소프트웨어 설계자** 및 **인프라 설계자** 권한을 가진 사용자로 vRealize Automation 장치에 로그인합니다.

```
CloudClient>vra login userpass --server https://vRealize_VA_Hostname_fqdn --user <user@domain.com> --tenant <TenantName>
```

- 8 메시지가 나타나면 로그인 암호를 입력합니다.
- 9 DukesBankAppForvSphere.zip 콘텐츠를 사용할 수 있는지 확인합니다.

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run true --resolution OVERWRITE
```

OVERWRITE 항목은 대/소문자를 구분하며 대문자로 입력해야 합니다.

skip 대신 덮어쓰도록 확인을 구성하여 가능한 경우 vRealize Automation에서 충돌을 해결할 수 있도록 허용합니다.

- 10 Dukes Bank 샘플 애플리케이션을 가져옵니다.

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run false --resolution OVERWRITE
```

OVERWRITE 항목은 대/소문자를 구분하며 대문자로 입력해야 합니다.

소프트웨어 설계자 및 인프라 설계자 권한을 가진 사용자로 vRealize Automation 콘솔에 로그인하면 **설계 > Blueprint** 탭과 **설계 > 소프트웨어 구성 요소** 탭에 Dukes Bank Blueprint와 소프트웨어 구성 요소가 표시됩니다.

시나리오: 환경에 맞게 Dukes Bank vSphere 샘플 구성 요소 구성

인프라 설계자 권한을 사용하여 환경을 위해 생성한 사용자 지정 규격, 템플릿 및 시스템 접두사를 사용하도록 Dukes Bank 시스템 구성 요소 각각을 구성합니다.

이 시나리오에서는 vSphere Web Client에서 생성한 템플릿에서 시스템을 복제하도록 시스템 구성 요소를 구성합니다. 스냅샷에 기반하여 가상 시스템의 공간 효율적인 복사본을 생성하려는 경우에 사용할 수 있도록 샘플 애플리케이션은 연결된 복제도 지원합니다. 연결된 복제는 델타 디스크 체인을 사용하여 상위 시스템과의 차이점을 추적하고, 신속하게 프로비저닝되며, 스토리지 비용을 절감하고 성능의 우선 순위가 높지 않은 경우에 사용하기 적합합니다.

프로시저

- 1 vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.

Dukes Bank 샘플 애플리케이션이 환경에서 **인프라 설계자** 역할로만 작동하도록 구성할 수 있지만 샘플 소프트웨어 구성 요소를 보거나 편집하려는 경우 **소프트웨어 설계자** 역할도 필요합니다.

- 2 **설계 > Blueprint**를 선택합니다.

- 3 **DukesBankApplication** Blueprint를 선택하고 **편집** 아이콘을 클릭합니다.

- 4 vRealize Automation이 이 시스템 구성 요소를 환경에 프로비저닝할 수 있도록 appserver-node를 편집합니다.

로드 밸런서 노드 기능을 확인할 수 있도록, Blueprint를 구성하여 이 시스템 구성 요소의 여러 인스턴스를 프로비저닝합니다.

- a 설계 캔버스에서 **appserver-node** 구성 요소를 클릭합니다.

아래쪽 패널에 구성 세부 정보가 나타납니다.

- b **시스템 접두사** 드롭다운 메뉴에서 시스템 접두사를 선택합니다.

- c 최소 2개에서 최대 10개의 인스턴스를 선택하여 이 노드의 인스턴스를 최소 2개에서 최대 10개까지 프로비저닝하도록 Blueprint를 구성합니다.

요청 양식에서 사용자는 최소 2개에서 최대 10개의 appserver 노드를 프로비저닝할 수 있습니다. 사용자에게 축소 및 확장 작업에 대한 권한이 부여된 경우 사용자는 변화하는 요구를 맞게 배포를 확장/축소할 수 있습니다.

- d **빌드 정보** 탭을 클릭합니다.

- e **프로비저닝 워크플로** 드롭다운 메뉴에서 **Cloneworkflow**를 선택합니다.

- f **복제 원본** 대화상자에서 **dukes_bank_template**을 선택합니다.

- g **사용자 지정 규격** 텍스트 상자에 **Customspecs_sample**을 입력합니다.

이 필드는 대/소문자를 구분합니다.

- h **시스템 리소스** 탭을 클릭합니다.

- i 메모리 설정이 2048MB 이상인지 확인합니다.

5 vRealize Automation이 이 시스템 구성 요소를 환경에 프로비저닝할 수 있도록 loadbalancer-node를 편집합니다.

- a 설계 캔버스에서 **loadbalancer-node** 구성 요소를 클릭합니다.
- b **시스템 접두사** 드롭다운 메뉴에서 시스템 접두사를 선택합니다.
- c **빌드 정보** 탭을 클릭합니다.
- d **프로비저닝 워크플로** 드롭다운 메뉴에서 **Cloneworkflow**를 선택합니다.
- e **복제 원본** 대화상자에서 **dukes_bank_template**을 선택합니다.
- f **사용자 지정 규격** 텍스트 상자에 **Customspecs_sample**을 입력합니다.
이 필드는 대/소문자를 구분합니다.
- g **시스템 리소스** 탭을 클릭합니다.
- h 메모리 설정이 2048MB 이상인지 확인합니다.

6 **database-node** 시스템 구성 요소에 대해 반복합니다.

7 **저장 및 종료**를 클릭합니다.

변경 내용이 저장되고 **Blueprint** 탭으로 돌아갑니다.

8 **DukesBankApplication** Blueprint를 선택하고 **게시**를 클릭합니다.

환경에 Dukes Bank 샘플 애플리케이션 Blueprint를 구성하고, 완성된 Blueprint를 게시했습니다.

후속 작업

게시된 Blueprint는 카탈로그 서비스를 구성하고, 서비스에 Blueprint를 추가하고 해당 Blueprint를 요청할 수 있는 권한을 사용자에게 부여해야만 사용자에게 표시됩니다. [서비스 카탈로그 구성을 위한 검사 목록](#) 항목을 참조하십시오.

Dukes Bank Blueprint가 카탈로그에 표시되도록 구성하고 나면 샘플 애플리케이션을 프로비저닝하도록 요청할 수 있습니다. [시나리오: Dukes Bank 샘플 애플리케이션 테스트](#) 항목을 참조하십시오.

시나리오: Dukes Bank 샘플 애플리케이션 테스트

Dukes Bank 카탈로그 항목을 요청하고 샘플 애플리케이션에 로그인하여 작업을 확인하고 vRealize Automation Blueprint 기능을 봅니다.

필수 조건

- Dukes Bank 샘플 애플리케이션을 가져오고 환경에서 작업할 Blueprint 구성 요소를 구성합니다. [시나리오: vSphere 샘플 애플리케이션용 Dukes Bank 가져오기 및 환경 구성](#) 항목을 참조하십시오.
- 서비스 카탈로그를 구성하고, 게시된 Dukes Bank Blueprint를 사용자가 요청할 수 있도록 설정합니다. [서비스 카탈로그 구성을 위한 검사 목록](#) 항목을 참조하십시오.
- 프로비저닝하는 가상 시스템이 YUM 저장소에 연결할 수 있는지 확인합니다.

프로시저

- 1 Dukes Bank 카탈로그 항목에 대해 사용 권한을 부여 받은 사용자로 vRealize Automation 콘솔에 로그인합니다.
- 2 **카탈로그** 탭을 클릭합니다.
- 3 Dukes Bank 샘플 애플리케이션 카탈로그 항목을 찾아서 **요청**을 클릭합니다.
- 4 빨간색 별표가 있는 각 구성 요소에 대해 필요한 요청 정보를 입력합니다.
 - a JBossAppServer 구성 요소로 이동하여 필요한 요청 정보를 입력합니다.
 - b **app_content_server_ip** 텍스트 상자에 vRealize Automation 장치의 정규화된 도메인 이름을 입력합니다.
 - c Dukes_Bank_App 소프트웨어 구성 요소로 이동하여 필요한 요청 정보를 입력합니다.
 - d **app_content_server_ip** 텍스트 상자에 vRealize Automation 장치의 정규화된 도메인 이름을 입력합니다.
- 5 **제출**을 클릭합니다.

네트워크 및 vCenter Server 인스턴스에 따라 Dukes Bank 샘플 애플리케이션이 완전히 프로비저닝되는 데에는 약 15~20분이 걸릴 수 있습니다. **요청** 탭 아래에서 상태를 모니터링할 수 있으며 애플리케이션 프로비저닝 후에는 **항목** 탭에서 카탈로그 항목 세부 정보를 볼 수 있습니다.
- 6 애플리케이션 프로비저닝 후에는 Dukes Bank 샘플 애플리케이션에 액세스할 수 있도록 로드 밸런서 서버의 IP 주소를 찾습니다.
 - a **항목 > 배포**를 선택합니다.
 - b Dukes Bank 샘플 애플리케이션 배포를 확장하고 Apache 로드 밸런서 서버를 선택합니다.
 - c **세부 정보 보기**를 클릭합니다.
 - d **네트워크** 탭을 선택합니다.
 - e IP 주소를 기록해 둡니다.
- 7 Dukes Bank 샘플 애플리케이션에 로그인합니다.
 - a `http://IP_Apache_Load_Balancer:8081/bank/main.faces`에서 로드 밸런서 서버로 이동합니다.

애플리케이션 서버에 직접 액세스하려는 경우 `http://IP_AppServer:8080/bank/main.faces`로 이동할 수 있습니다.
 - b **사용자 이름** 텍스트 상자에 **200**을 입력합니다.
 - c **암호** 텍스트 상자에 **foobar**를 입력합니다.

고유한 Blueprint를 개발하기 위한 시작점, vRealize Automation을 평가하기 위한 도구 또는 vRealize Automation의 기능과 구성 요소를 이해하는 데 도움을 줄 수 있는 학습 리소스로 사용할 수 있도록 Dukes Bank 샘플 애플리케이션을 구성했습니다.

설계 라이브러리 구축

정교한 요청 시 서비스를 사용자에게 제공하기 위해 설계자가 애플리케이션 Blueprint에 구성할 수 있는 재사용 가능한 Blueprint 구성 요소의 라이브러리를 구축할 수 있습니다.

최소 Blueprint 설계 구성 요소, 즉 시스템 Blueprint, Software 구성 요소, XaaS Blueprint의 라이브러리를 구축한 다음 이러한 기본 빌딩 블록을 새롭고 다른 방식으로 결합하여 높은 수준의 기능을 사용자에게 제공하는 정교한 카탈로그 항목을 생성합니다.

VMware Solution Exchange(<https://solutionexchange.vmware.com>) 및 <https://code.vmware.com>에서 샘플 Blueprint를 사용할 수 있습니다.

표 3-2. 설계 라이브러리 구축

카탈로그 항목	역할	구성 요소	설명	세부 정보
시스템	인프라 설계자	Blueprint 탭에 시스템 Blueprint를 생성합니다.	시스템 Blueprint를 생성하면 가상, 사설/공용 또는 하이브리드 클라우드 시스템을 사용자에게 신속하게 제공할 수 있습니다. 카탈로그 관리자는 게시된 시스템 Blueprint를 독립형 Blueprint로 카탈로그에 포함할 수 있지만 시스템 Blueprint를 다른 구성 요소와 결합하여 여러 시스템 Blueprint, Software 또는 XaaS Blueprint를 포함하는 더 정교한 카탈로그 항목을 생성할 수 있습니다.	시스템 Blueprint 구성
시스템의 NSX 네트워크 및 보안	인프라 설계자	NSX 네트워크 및 보안 구성 요소를 Blueprint 탭의 vSphere 시스템 Blueprint에 추가합니다.	물리적 네트워크와 가상 네트워크에서 가상 시스템끼리 안전하고 효율적으로 통신할 수 있도록 네트워크 프로파일 및 보안 그룹 같은 네트워크 및 보안 구성 요소를 구성할 수 있습니다. 네트워크 및 보안 구성 요소를 하나 이상의 vSphere 시스템 구성 요소와 결합해야만 카탈로그 관리자가 해당 구성 요소를 카탈로그에 포함할 수 있습니다. NSX 네트워크 및 보안 구성 요소는 vSphere 시스템 Blueprint에만 적용할 수 있습니다.	NSX 설정을 사용하여 Blueprint 설계
시스템의 소프트웨어	소프트웨어 설계자 설계 캔버스에 소프트웨어 구성 요소를 추가하려면 대상 카탈로그에 대해 비즈니스 그룹 구성원, 비즈니스 그룹 관리자 또는 테넌트 관리자 역할 액세스 권한도 있어야 합니다.	소프트웨어 탭에서 Software 구성 요소를 생성하고 게시한 다음 Blueprint 탭의 시스템 Blueprint와 결합합니다.	시스템 Blueprint에 Software 구성 요소를 추가하여 클라우드 환경에서 복잡한 애플리케이션을 표준화, 배포, 구성, 업데이트 및 확장합니다. 이러한 애플리케이션은 간단한 웹 애플리케이션부터 정교한 사용자 지정 애플리케이션 및 패키징된 애플리케이션에 이르기까지 다양합니다. Software 구성 요소는 카탈로그에 단독으로 나타날 수 없습니다. Software 구성 요소를 생성 및 게시한 다음 하나 이상의 시스템을 포함하는 애플리케이션 Blueprint를 구성해야 합니다.	Software 구성 요소 생성

표 3-2. 설계 라이브러리 구축 (계속)

카탈로그 항목	역할	구성 요소	설명	세부 정보
사용자 지정 IT 서비스	XaaS 설계자	XaaS 탭에서 XaaS Blueprint를 생성하고 게시합니다.	시스템, 네트워킹, 보안 및 소프트웨어 프로비저닝 이상으로 vRealize Automation 기능을 확장하는 XaaS 카탈로그 항목을 생성할 수 있습니다. 기존 vRealize Orchestrator 워크플로와 플러그인 또는 vRealize Orchestrator에서 개발하는 사용자 지정 스크립트를 사용하여 모든 IT 서비스의 제공을 자동화할 수 있습니다. 게시된 XaaS Blueprint는 카탈로그 관리자가 독립형 Blueprint에 포함할 때 사용할 수 있지만 Blueprint 탭의 다른 구성 요소와 결합하여 보다 정교한 카탈로그 항목을 생성하는 데도 사용될 수도 있습니다.	XaaS Blueprint 및 리소스 작업 설계
게시된 Blueprint 빌딩 블록을 새 카탈로그 항목에 구성합니다.	<ul style="list-style-type: none"> ■ 애플리케이션 설계자 ■ 인프라 설계자 ■ 소프트웨어 설계자 	추가 시스템 Blueprint, XaaS Blueprint 및 Software 구성 요소를 하나 이상의 시스템 구성 요소 또는 Blueprint 탭의 시스템 Blueprint와 결합합니다.	게시된 구성 요소 및 Blueprint를 재사용하고 새로운 방식으로 결합하여 사용자에게 정교한 기능을 제공하는 IT 서비스 패키지를 생성할 수 있습니다.	복합 Blueprint 구성

시스템 Blueprint 설계

시스템 Blueprint는 시스템의 전체 규격으로 시스템의 특성, 시스템이 프로비저닝되는 방식, 시스템의 정책 및 관리 설정을 결정합니다. 구축 중인 카탈로그 항목의 복잡도에 따라 Blueprint에 있는 하나 이상의 시스템 구성 요소를 설계 캔버스의 다른 구성 요소와 결합하여 네트워킹 및 보안, Software 구성 요소, XaaS 구성 요소 및 기타 Blueprint 구성 요소를 포함하는 더욱 정교한 카탈로그 항목을 생성할 수 있습니다.

가상 프로비저닝을 위한 공간 효율적인 스토리지

공간 효율적인 스토리지 기술은 시스템 작업에 실제로 필요한 스토리지만 사용하여 기존 스토리지 방식의 비효율성을 없앱니다. 일반적으로 시스템 작업에 필요한 스토리지는 시스템에 실제로 할당되는 스토리지의 일부에 불과합니다. vRealize Automation에서는 공간 효율적인 기술을 사용하여 두 가지 프로비저닝 방법인 썬 프로비저닝과 FlexClone 프로비저닝을 지원합니다.

표준 스토리지를 사용할 경우, 프로비저닝된 시스템에 할당된 스토리지는 시스템 전원이 꺼진 상태에서도 해당 시스템 전용으로 사용됩니다. 디스크의 100%를 모두 사용하여 작동하는 물리적 시스템이 몇 안 되는 것과 마찬가지로 할당된 스토리지를 실제로 모두 사용하는 가상 시스템은 몇 안 되기 때문에 이 방법의 경우 스토리지 리소스가 상당히 많이 낭비됩니다. 공간 효율적인 스토리지 기술을 사용하면 할당된 스토리지와 사용된 스토리지가 별개로 추적되고, 사용된 스토리지만 해당하는 프로비저닝된 시스템 전용으로 사용됩니다.

썸 프로비저닝

썸 프로비저닝은 모든 가상 프로비저닝 방법에 지원됩니다. 가상화 플랫폼, 스토리지 유형 및 기본 스토리지 구성에 따라 썸 프로비저닝은 시스템 프로비저닝 시 항상 사용될 수 있습니다. 예를 들어 NFS 스토리지를 사용하는 vSphere ESX Server 통합에는 썸 프로비저닝이 항상 사용됩니다. 그러나 로컬 스토리지나 iSCSI 스토리지를 사용하는 vSphere ESX Server 통합의 경우에는 VirtualMachine.Admin.ThinProvision 사용자 지정 속성을 Blueprint에 지정한 경우에만 시스템을 프로비저닝하는 데 썸 프로비저닝이 사용됩니다. 썸 프로비저닝에 대한 자세한 내용은 가상화 플랫폼에서 제공되는 설명서를 참조하십시오.

Net App FlexClone 프로비저닝

NFS(네트워크 파일 시스템) 스토리지와 FlexClone 기술을 사용하는 vSphere 환경에서 작업하는 경우에는 Net App FlexClone 프로비저닝을 위한 Blueprint를 생성할 수 있습니다.

NFS 스토리지만 사용해야 하며, 그렇지 않을 경우 시스템 프로비저닝이 실패합니다. 다른 시스템 프로비저닝 유형에 대해 FlexClone 스토리지 경로를 지정할 수 있지만 FlexClone 스토리지 경로는 표준 스토리지처럼 작동합니다.

다음은 FlexClone 기술을 사용하는 시스템을 프로비저닝하는 데 필요한 단계 순서의 간략한 개요입니다.

- 1 IaaS 관리자가 NetApp ONTAP 끝점을 만듭니다. [끝점 설정 참조](#) 항목을 참조하십시오.
- 2 IaaS 관리자가 끝점에서 데이터 수집을 실행하여 해당 끝점이 [계산 리소스] 및 [예약] 페이지에 나타나도록 합니다.

NetApp ONTAP 끝점이 있고 호스트가 가상 호스트이면 [예약] 페이지의 끝점 열에 FlexClone 옵션이 표시됩니다. NetApp ONTAP 끝점이 있으면 스토리지 경로에 할당된 끝점이 [예약] 페이지에 표시됩니다.

- 3 패브릭 관리자가 vSphere 예약을 생성하고, FlexClone 스토리지를 사용하도록 설정하고, FlexClone 기술을 사용하는 NFS 스토리지 경로를 지정합니다. [Hyper-V, KVM, SCVMM, vSphere 또는 XenServer에 대한 예약 생성](#) 항목을 참조하십시오.
- 4 인프라 설계자나 기타 권한이 있는 사용자가 FlexClone 프로비저닝을 위한 Blueprint를 만듭니다.

Blueprint 매개 변수화 이해 및 사용

Blueprint 매개 변수화를 위해 구성 요소 프로파일을 사용할 수 있습니다. 특정 배포 유형에 대해 소형, 중형 및 대형 Blueprint를 개별적으로 생성하는 대신 소형, 중형 또는 대형 가상 시스템을 선택할 수 있는 단일 Blueprint를 생성할 수 있습니다. 사용자는 카탈로그 항목을 배포할 때 이러한 크기 중 하나를 선택할 수 있습니다.

구성 요소 프로파일은 Blueprint 확장을 최소화하고 카탈로그 오퍼링을 간소화합니다. 구성 요소 프로파일을 사용하여 Blueprint에서 vSphere 시스템 구성 요소를 정의할 수 있습니다. 사용할 수 있는 구성 요소 프로파일 유형에는 Size와 Image가 있습니다. 구성 요소 프로파일을 시스템 구성 요소에 추가할 때 구성 요소 프로파일 설정은 시스템 구성 요소의 다른 설정(예: CPU 수 및 스토리지의 양)을 재정의합니다.

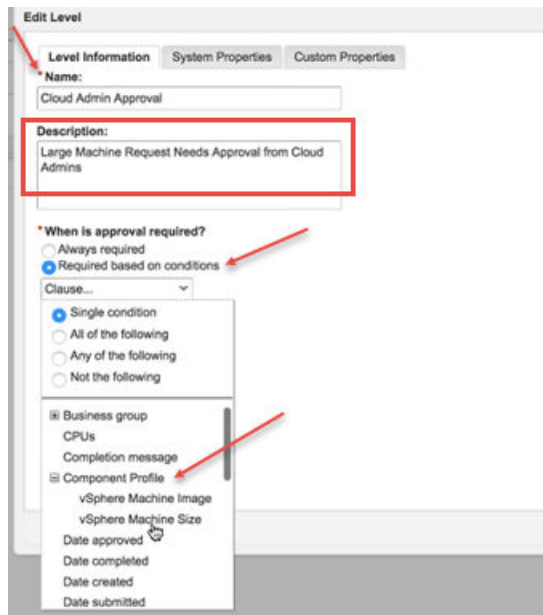
구성 요소 프로파일은 vSphere 시스템 구성 요소에 대해서만 사용할 수 있습니다.

Size 및 Image 구성 요소 프로파일의 값 집합 정의에 대한 자세한 내용은 사용자 지정 속성 참조 자료에서 를 참조하십시오.

Blueprint의 vSphere 시스템 구성 요소에 대해 구성 요소 프로파일 및 선택된 값 집합을 추가하는 것에 대한 자세한 내용은 [vSphere 시스템 구성 요소 설정](#)을 참조하십시오.

시스템 프로비저닝을 요청할 때 구성 요소 프로파일을 사용하는 것에 대한 자세한 내용은 [매개 변수화된 Blueprint를 사용하여 시스템 프로비저닝 요청](#)을 참조하십시오.

참고 Size 및 Image 구성 요소 프로파일에 대한 값 집합 조건과 관련된 Blueprint의 시스템 프로비저닝을 요청할 때 사전 승인이 필요하도록 승인 정책을 생성할 수 있습니다. 자세한 내용은 [가상 시스템 정책 유형에 기반한 승인 정책의 예](#)를 참조하십시오.



카탈로그에서 시스템 프로비저닝을 요청할 때 Blueprint 매개 변수화를 사용하는 것에 대한 자세한 내용은 [매개 변수화된 Blueprint를 사용하여 시스템 프로비저닝 요청](#)을 참조하십시오.

시스템 Blueprint 구성

다른 설계자가 애플리케이션 Blueprint의 구성 요소로 재사용할 수 있고 카탈로그 관리자가 카탈로그 서비스에 포함할 수 있는 독립형 Blueprint로 시스템 구성 요소를 구성하고 게시합니다.

필수 조건

- vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.

- 템플릿, WinPE 및 ISO 생성과 같은 프로비저닝을 위한 외부적 준비를 완료하거나 관리자로부터 외부적 준비에 관한 정보를 수집합니다.
- 테넌트를 구성합니다. [테넌트 설정 구성](#).
- IaaS 리소스를 구성합니다. [IaaS 리소스 구성을 위한 검사 목록](#).
- vRealize Automation 구성의 내용을 참조하십시오.

프로시저

- 1 **설계 > Blueprint**를 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 새 **Blueprint** 대화 상자에 표시되는 메시지에 따라 일반 설정을 구성합니다.
- 4 **확인**을 클릭합니다.
- 5 [범주] 영역에서 **시스템 유형**을 클릭하여 사용 가능한 시스템 유형 목록을 표시합니다.
- 6 프로비저닝하려는 시스템 유형을 설계 캔버스로 끌어옵니다.
- 7 각 탭의 안내 메시지에 따라 시스템 프로비저닝 세부 정보를 구성합니다.
- 8 **완료**를 클릭합니다.
- 9 Blueprint를 선택하고 **게시**를 클릭합니다.

시스템 구성 요소를 독립형 Blueprint로 구성하고 게시했습니다. 카탈로그 관리자는 카탈로그 서비스에 이 시스템 Blueprint를 포함하고 이 Blueprint 요청 권한을 사용자에게 제공할 수 있습니다. 다른 설계자는 이 시스템 Blueprint를 재사용하여 Software 구성 요소, XaaS Blueprint 또는 추가 시스템 Blueprint가 포함된 더 정교한 애플리케이션 Blueprint를 생성할 수 있습니다.

후속 작업

시스템 Blueprint를 Software 구성 요소, XaaS Blueprint 또는 추가 시스템 Blueprint와 결합하여 더 정교한 애플리케이션 Blueprint를 생성할 수 있습니다. [복합 Blueprint 구성](#) 항목을 참조하십시오.

시스템 Blueprint 설정

전체 Blueprint에 대해 구성 설정 및 사용자 지정 속성을 정의할 수 있습니다.

Blueprint 속성 설정

Blueprint를 생성할 때 새 **Blueprint** 페이지를 사용하여 전체 Blueprint에 적용되는 설정을 지정할 수 있습니다. Blueprint를 생성한 후에는 [Blueprint 속성] 페이지에서 이러한 설정을 편집할 수 있습니다.

일반 탭

지금 또는 나중에 추가하려는 모든 구성 요소를 포함하여 전체 Blueprint에서 설정을 적용합니다.

표 3-3. 일반 탭 설정

설정	설명
이름	Blueprint 이름을 입력합니다.
식별자	식별자 필드는 사용자가 입력한 이름에 따라 자동으로 채워집니다. 지금은 이 필드를 편집할 수 있지만 Blueprint를 저장한 후에는 이 필드를 변경할 수 없습니다. 식별자는 영구적이며 테넌트 내에서 고유하기 때문에 식별자를 사용하여 프로그래밍 방식으로 Blueprint와 상호 작용하고 속성 바인딩을 생성할 수 있습니다.
설명	다른 설계자를 위해 Blueprint를 요약합니다. 이 설명은 요청 양식의 사용자에게도 나타납니다.
아카이브 기간(일)	아카이브 기간을 지정하여 리스가 만료될 때 배포를 즉시 제거하지 않고 일시적으로 보존할 수 있습니다. 해당 리스가 만료될 때 배포를 제거하려면 0(기본값)을 지정합니다. 아카이브 기간은 리스 만료 날짜에 시작됩니다. 아카이브 기간이 종료되면 배포가 제거됩니다.
배포 제한	이 Blueprint가 시스템을 프로비저닝하는 데 사용될 때 생성될 수 있는 최대 배포 수를 지정합니다.
리스 기간(일): 최소 및 최대	사용자가 리스 기간 범위 내에서 선택할 수 있도록 최소값 및 최대값을 입력합니다. 리스가 종료되면 배포가 제거되거나 아카이브됩니다. 최소값이나 최대값을 지정하지 않는 경우 리스가 만료되지 않도록 설정됩니다.

NSX 설정 탭

NSX를 구성한 경우 Blueprint를 생성하거나 편집할 때 NSX 전송 영역, Edge 및 라우팅된 게이트웨이 예약 정책 그리고 App 분리 설정을 지정할 수 있습니다. 이러한 설정은 **Blueprint** 및 **Blueprint 속성** 페이지의 **NSX 설정** 탭에서 사용할 수 있습니다.

NSX 설정에 대한 자세한 내용은 [NSX를 사용하는 새 Blueprint 및 Blueprint 속성 페이지 설정](#) 항목을 참조하십시오.

속성 탭

Blueprint 수준에서 추가하는 사용자 지정 속성이 모든 구성 요소를 비롯한 전체 Blueprint에 적용됩니다. 하지만 해당 속성은 우선 순위 체인에서 나중에 할당된 사용자 지정 속성에 의해 재정의될 수 있습니다. 사용자 지정 속성의 우선 순위에 대한 자세한 내용은 사용자 지정 속성 참조 자료 항목을 참조하십시오.

표 3-4. 속성 탭 설정

탭	설정	설명
속성 그룹	속성 그룹	속성 그룹은 Blueprint에 사용자 지정 속성을 추가하는 프로세스를 간소화하기 위해 설계된 속성의 재사용 가능 그룹입니다. 테넌트 관리자 및 패브릭 관리자는 개별적으로 사용자 지정 속성을 삽입하는 대신 속성 그룹을 Blueprint에 추가할 수 있도록 자주 함께 사용되는 속성을 그룹화할 수 있습니다.
	추가	기존 속성 그룹을 하나 이상 추가하고 이것을 전체 Blueprint에 적용합니다. 다음 컨테이너 관련 속성 그룹이 제공됩니다. <ul style="list-style-type: none"> ■ 인증서 인증이 있는 컨테이너 호스트 속성 ■ 사용자/암호 인증이 있는 컨테이너 호스트 속성
	위로 이동/아래로 이동	그룹의 우선 순위를 지정함으로써 서로와 비교하여 각 속성 그룹에 지정된 우선 순위를 제어합니다. 목록의 첫 번째 그룹에 가장 높은 우선 순위가 있고 해당 사용자 지정 속성에 첫 번째 우선 순위가 있습니다. 또한 끝에서 끝으로 순서를 다시 지정할 수 있습니다.
	속성 보기	선택된 속성 그룹에서 사용자 지정 속성을 봅니다.
	병합된 속성 보기	사용자 지정 속성이 두 개 이상의 속성 그룹에 포함된 경우 가장 높은 우선 순위가 있는 속성 그룹에 포함된 값이 우선합니다. 속성 그룹 우선 순위 지정에 도움이 되도록 이러한 병합된 속성을 볼 수 있습니다.
사용자 지정 속성	속성 그룹 대신 개별 사용자 지정 속성을 추가할 수 있습니다.	
	새로운 문제	개별 사용자 지정 속성을 추가하고 이것을 전체 Blueprint에 적용합니다.
	이름	속성 이름을 입력합니다. 사용자 지정 속성 및 해당 정의 목록은 사용자 지정 속성 참조 자료를 참조하십시오.
	값	사용자 지정 속성의 값을 입력합니다.
	암호화됨	예를 들어 값이 암호인 경우 속성 값을 암호화하도록 선택할 수 있습니다.
	재정의 가능	속성 값을 속성을 사용하는 다음 사람 또는 나중 사람이 재정의할 수 있도록 지정할 수 있습니다. 일반적으로 이는 다른 설계자이지만 [요청에서 표시]를 선택하는 경우 비즈니스 사용자가 카탈로그 항목을 요청할 때 속성 값을 보고 편집할 수 있습니다.
	요청에서 표시	최종 사용자에게 속성 이름 및 값을 표시하려는 경우 시스템 프로비저닝을 요청할 때 요청 양식에 속성을 표시하도록 선택할 수 있습니다. 사용자가 값을 제공하길 원하는 경우 [재정의 가능]도 선택해야 합니다.

vSphere 시스템 구성 요소 설정

vRealize Automation Blueprint 설계 캔버스에서 vSphere 시스템 구성 요소에 대해 구성할 수 있는 설정과 옵션을 이해합니다. vSphere는 설계 캔버스에서 NSX 네트워크 및 보안 구성 요소 설정을 사용할 수 있는 유일한 시스템 구성 요소 유형입니다.

일반 탭

vSphere 시스템 구성 요소에 대한 일반 설정을 구성합니다.

표 3-5. 일반 탭 설정

설정	설명
ID	시스템 구성 요소의 이름을 입력하거나 기본값을 수락합니다.
설명	다른 설계자를 위해 시스템 구성 요소를 요약합니다.
요청에 위치 표시	vCloud Air와 같은 클라우드 환경에서는 이에 따라 사용자가 프로비저닝된 시스템에 대한 영역을 선택할 수 있습니다. vSphere와 같은 가상 환경의 경우 사용자가 요청된 시스템을 프로비저닝할 특정 데이터 센터 위치를 선택하도록 허용하기 위한 위치 기능을 구성할 수 있습니다. 이 옵션을 완전하게 구성하기 위해 시스템 관리자는 위치 파일에 데이터 센터 위치 정보를 추가하고 패브릭 관리자는 계산 리소스를 편집하여 위치와 연결합니다.
예약 정책	Blueprint에 예약 정책을 적용하여 해당 Blueprint에서 프로비저닝된 시스템이 사용 가능한 일부 예약으로 제한되도록 합니다. 예를 들어 여러 서비스 수준의 그룹에 리소스를 수집하거나 특정 용도에 특정한 유형의 리소스를 쉽게 사용할 수 있도록 만들기 위해, 패브릭 관리자는 예약 요청이 처리되는 방식을 제어하는 유용한 선택적 수단을 제공하도록 예약 정책을 생성합니다. 패브릭 관리자가 예약 정책을 구성하지 않은 경우 이 드롭다운 메뉴에는 사용 가능한 옵션이 표시되지 않습니다.
시스템 접두사	시스템 접두사는 패브릭 관리자에 의해 생성되며 프로비저닝된 시스템 이름을 생성하는 데 사용됩니다. 그룹 기본값 사용 을 선택하는 경우 Blueprint에서 프로비저닝된 시스템에는 사용자의 비즈니스 그룹에 대한 기본값으로 구성된 시스템 접두사에 따라 이름이 지정됩니다. 구성된 시스템 접두사가 없는 경우 비즈니스 그룹 이름을 기반으로 하나가 생성됩니다. 패브릭 관리자가 사용자가 선택하도록 기타 시스템 접두사를 구성하는 경우 사용자는 요청자가 누구인지 관계없이 해당 Blueprint에서 프로비저닝된 모든 시스템에 하나의 접두사를 적용할 수 있습니다.
인스턴스: 최소 및 최대	사용자가 하나의 배포 또는 하나의 확장/축소 작업에 대해 요청할 수 있는 최대 인스턴스 수와 최소 인스턴스 수를 구성합니다. 사용자가 선택할 수 있게 하지 않으려는 경우, 최소 및 최대 필드에 같은 값을 입력하면 프로비저닝할 인스턴스의 수가 정확하게 구성되고 이 시스템 구성 요소에 대한 확장/축소 작업이 사용되지 않도록 설정됩니다. XaaS 구성 요소는 확장/축소할 수 없고 확장/축소 작업 중 업데이트되지 않습니다. Blueprint에서 XaaS 구성 요소를 사용 중인 경우 사용자가 확장/축소 작업 후에 실행하도록 리소스 작업을 생성할 수 있으며 이 작업을 통해 필요에 맞게 XaaS 구성 요소를 확장/축소하거나 업데이트할 수 있습니다. 또는 각 시스템 구성 요소에 허용할 인스턴스 수를 정확하게 구성하여 확장/축소가 사용되지 않도록 설정할 수 있습니다.

빌드 정보 탭

vSphere 시스템 구성 요소에 대한 빌드 정보 설정을 구성합니다.

표 3-6. 빌드 정보 탭

설정	설명
Blueprint 유형	기록 보관 및 라이선싱 용도를 위해 이 Blueprint에서 프로비저닝된 시스템이 데스크톱 또는 서버로 분류되는지 선택합니다.
작업	<p>작업 드롭다운 메뉴에 표시되는 옵션은 선택하는 시스템 유형에 따라 다릅니다.</p> <p>다음과 같은 작업을 사용할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 생성 <p>복제 옵션을 사용하지 않고 시스템 구성 요소 규격을 생성합니다.</p> ■ 복제 <p>템플릿 및 사용자 지정 개체에서 가상 시스템의 복사본을 만듭니다.</p> ■ 연결된 복제 <p>가상 시스템의 공간 효율적인 복사본(연결된 복제라고 함)을 프로비저닝합니다. 연결된 복제는 VM의 스냅샷에 기반하며, 델타 디스크 체인을 사용하여 상위 시스템과의 차이점을 추적합니다.</p> <p>연결된 복제 VM을 프로비저닝하기 전에 Blueprint에서 식별되는 VM 스냅샷의 전원을 꺼야 합니다.</p> ■ NetApp FlexClone <p>패브릭 관리자가 NetApp FlexClone 스토리지를 사용하도록 예약을 구성한 경우 이 기술을 사용하여 공간 효율적인 시스템 사본을 복제할 수 있습니다.</p>

표 3-6. 빌드 정보 탭 (계속)

설정	설명
프로비저닝 워크플로	<p>프로비저닝 워크플로 드롭다운 메뉴에 표시되는 옵션은 선택하는 시스템 유형 및 선택하는 작업에 따라 다릅니다.</p> <ul style="list-style-type: none"> BasicVmWorkflow <p>게스트 운영 체제가 없는 시스템을 프로비저닝합니다.</p> ExternalProvisioningWorkflow <p>가상 시스템 인스턴스 또는 클라우드 기반 이미지부터 시작하여 시스템을 생성합니다.</p> LinuxKickstartWorkflow <p>ISO 이미지에서 부팅하여 시스템을 프로비저닝하며, kickstart 또는 autoYaSt 구성 파일과 Linux 배포 이미지를 사용하여 시스템에 운영 체제를 설치합니다.</p> VirtualSccmProvisioningWorkflow <p>시스템을 프로비저닝하고 제어 기능을 SCCM 작업 시퀀스에 전달하여 ISO 이미지에서 부팅하고, Windows 운영 체제를 배포하고, vRealize Automation 게스트 에이전트를 설치합니다.</p> WIMImageWorkflow <p>WinPE 환경으로 부팅하고, 기존 Windows 참조 시스템의 WIM(Windows Imaging File Format) 이미지를 사용하여 운영 체제를 설치하는 방법으로 시스템을 프로비저닝합니다.</p> <p>Blueprint에서 WIM 프로비저닝 워크플로를 사용하는 경우, 시스템에서 사용될 각 디스크의 크기를 고려하여 스토리지 값을 지정해야 합니다. 모든 디스크의 총 값을 시스템 구성 요소의 최소 스토리지 값으로 사용하십시오. 또한 운영 체제를 수용할 수 있을 정도로 크게 각 디스크의 크기를 지정해야 합니다.</p>
복제 원본	<p>복제 원본으로 사용할 시스템 템플릿을 선택합니다. 각 열 드롭다운 메뉴에서 필터 옵션(예: 이름 열의 필터 메뉴 옵션)을 사용하여 사용 가능한 템플릿 목록을 구체화할 수 있습니다.</p> <p>연결된 복제의 경우 복제 원본으로 사용 가능한 스냅샷이 있는 시스템 그리고 테넌트 관리자 또는 비즈니스 그룹 관리자로 관리하는 시스템만 표시됩니다.</p> <p>자신이 비즈니스 그룹 관리자 또는 테넌트 관리자로 관리하는 시스템에 있는 템플릿에서만 복제할 수 있습니다.</p>

표 3-6. 빌드 정보 탭 (계속)

설정	설명
스냅샷에서 복제	<p>연결된 복제의 경우 선택된 시스템 템플릿을 기반으로 복제 원본으로 사용할 기존 스냅샷을 선택합니다. 시스템은 이미 기존 스냅샷이 있으며 해당 시스템을 테넌트 관리자 또는 비즈니스 그룹 관리자로 관리하는 경우 목록에만 나타납니다.</p> <p>현재 스냅샷 사용을 선택하는 경우 복제가 가상 시스템의 최신 상태와 동일한 특성으로 정의됩니다. 그러지 않고 실제 스냅샷을 기준으로 복제하려는 경우에는 드롭다운 메뉴 옵션을 클릭하고 목록에서 특정 스냅샷을 선택합니다.</p> <p>참고 스냅샷이란 용어를 사용하는 것이 혼동을 일으킬 수 있습니다. 기존 스냅샷을 선택하는 경우 이 옵션을 선택하면 스냅샷이 상위 항목으로 지정되는 새 디스크가 생성됩니다. 현재 스냅샷 사용 옵션에서는 상위 디스크로 사용할 기본 디스크가 없고 전체 복제 작업이 자동으로 수행됩니다. 이에 대한 해결 방법으로서, 기본 디스크에 스냅샷을 만들거나, 스냅샷을 만든 다음에 스냅샷에서 즉시 복제하는 vRealize Orchestrator 워크플로를 사용할 수 있습니다.</p> <p>이 옵션은 연결된 복제 작업에 대해서만 사용할 수 있습니다.</p>
사용자 지정 규격	<p>사용 가능한 사용자 지정 규격을 지정합니다. 사용자 지정 규격은 정적 IP 주소로 복제할 경우에만 필요합니다.</p> <p>Windows 시스템은 사용자 지정 규격 없이 사용자 지정할 수 없습니다. Linux 복제 시스템의 경우 사용자 지정 규격, 외부 스크립트 또는 둘 다를 사용하여 사용자 지정을 수행할 수 있습니다.</p>

시스템 리소스 탭

vSphere 시스템 구성 요소에 대한 CPU, 메모리 및 스토리지 설정을 지정합니다.

표 3-7. 시스템 리소스 탭

설정	설명
CPU: 최소 및 최대	해당 시스템 구성 요소가 프로비저닝할 수 있는 CPU 수의 최소값 및 최대값을 입력합니다.
메모리(MB): 최소 및 최대	해당 시스템 구성 요소가 프로비저닝한 시스템이 사용할 수 있는 메모리 크기의 최소값 및 최대값을 입력합니다.
스토리지(GB): 최소 및 최대	<p>해당 시스템 구성 요소가 프로비저닝한 시스템이 사용할 수 있는 스토리지 크기의 최소값 및 최대값을 입력합니다.</p> <p>vSphere, KVM (RHEV), SCVMM, vCloud Air 및 vCloud Director의 경우 [스토리지] 탭에 입력하는 값을 기반으로 최소 스토리지가 설정됩니다.</p> <p>Blueprint에서 WIM 프로비저닝 워크플로를 사용하는 경우, 시스템에서 사용될 각 디스크의 크기를 고려하여 스토리지 값을 지정해야 합니다. 모든 디스크의 총 값을 시스템 구성 요소의 최소 스토리지 값으로 사용하십시오. 또한 운영 체제를 수용할 수 있을 정도로 크게 각 디스크의 크기를 지정해야 합니다.</p>

스토리지 탭

하나 이상의 스토리지 예약 정책을 포함한 스토리지 볼륨 설정을 시스템 구성 요소에 추가하여 스토리지 공간을 제어할 수 있습니다.

표 3-8. 스토리지 탭 설정

설정	설명
ID	스토리지 볼륨의 ID 또는 이름을 입력합니다.
용량(GB)	스토리지 볼륨의 스토리지 용량을 입력합니다.
드라이브 문자/마운트 경로	스토리지 볼륨의 드라이브 문자 또는 마운트 경로를 입력합니다.
레이블	스토리지 볼륨의 드라이브 문자 및 마운트 경로에 대한 레이블을 입력합니다.
스토리지 예약 정책	이 스토리지 볼륨에 사용할 기존 스토리지 예약 정책을 입력합니다.
사용자 지정 속성	이 스토리지 볼륨에 사용할 사용자 지정 속성을 모두 입력합니다.
최대 볼륨 수	시스템 구성 요소에서 프로비저닝할 때 사용할 수 있는 허용된 스토리지 볼륨의 최대 개수를 입력합니다. 다른 사용자가 스토리지 볼륨을 추가하는 것을 방지하려면 0을 입력합니다. 기본값은 60입니다.
사용자가 스토리지 예약 정책을 보고 변경할 수 있도록 허용	사용자가 연결된 예약 정책을 제거하도록 허용하거나 프로비저닝할 때 다른 예약 정책을 지정하려면 이 확인란을 선택합니다.

네트워크 탭

vRealize Automation 외부에서 구성된 NSX 네트워크 및 로드 밸런서 설정을 기반으로 vSphere 시스템 구성 요소에 대한 네트워크 설정을 구성할 수 있습니다. 설계 캔버스에 있는 하나 이상의 기존 및 요청 시 NSX 네트워크 구성 요소의 설정을 사용할 수 있습니다.

vSphere 시스템 구성 요소에서 네트워크 탭 설정을 사용하기 전에 NSX 네트워크 및 보안 구성 요소를 추가 및 구성하는 데 대한 자세한 내용은 [네트워크 및 보안 구성 요소 설정 구성](#) 항목을 참조하십시오.

vSphere 시스템 구성 요소에 적용되는 Blueprint 수준 NSX 설정을 지정하는 데 대한 자세한 내용은 [NSX를 사용하는 새 Blueprint 및 Blueprint 속성 페이지 설정](#) 항목을 참조하십시오.

표 3-9. 네트워크 탭 설정

설정	설명
네트워크	드롭다운 메뉴에서 네트워크 구성 요소를 선택합니다. 설계 캔버스에 이미 존재하는 네트워크 구성 요소만 나열됩니다.
할당 유형	네트워크 구성 요소에서 파생된 기본 할당 값을 그대로 사용하거나, 드롭다운 메뉴에서 할당 유형을 선택합니다. DHCP 및 정적 옵션 값은 네트워크 구성 요소의 설정에서 파생됩니다.
주소	네트워크의 IP 주소를 지정합니다. 이 옵션은 정적 주소 유형에 대해서만 사용할 수 있습니다.
로드 밸런싱	로드 밸런싱에 사용할 서비스를 입력합니다.

표 3-9. 네트워크 탭 설정 (계속)

설정	설명
사용자 지정 속성	선택된 네트워크 구성 요소 또는 네트워크 프로파일에 대해 구성된 사용자 지정 속성을 표시합니다.
최대 네트워크 어댑터 수	이 시스템 구성 요소에 허용할 네트워크 어댑터 또는 NIC의 최대 개수를 지정합니다. 기본값은 무제한입니다. 시스템 구성 요소에 대한 NIC 추가를 사용하지 않도록 설정하려면 0으로 설정합니다.

보안 탭

vRealize Automation 외부에서 구성된 NSX 설정을 기반으로 vSphere 시스템 구성 요소에 대한 보안 설정을 구성할 수 있습니다. 필요한 경우 설계 캔버스에 있는 기존 및 요청 시 NSX 보안 구성 요소의 설정을 선택적으로 사용할 수 있습니다.

설계 캔버스에 있는 기존 및 요청 시 보안 그룹과 보안 태그 구성 요소의 보안 설정은 자동으로 사용할 수 있습니다.

vSphere 시스템 구성 요소에서 보안 탭 설정을 사용하기 전에 NSX 네트워크 및 보안 구성 요소를 추가 및 구성하는 데 대한 자세한 내용은 [네트워크 및 보안 구성 요소 설정 구성](#) 항목을 참조하십시오.

vSphere 시스템 구성 요소에 적용되는 Blueprint 수준 NSX 정보 지정에 대한 자세한 내용은 [NSX를 사용하는 새 Blueprint 및 Blueprint 속성 페이지 설정](#) 항목을 참조하십시오.

표 3-10. 보안 탭 설정

설정	설명
이름	NSX 보안 그룹 또는 태그의 이름을 표시합니다. 이름은 설계 캔버스에 있는 보안 구성 요소에서 파생됩니다. 이 시스템 구성 요소에서 프로비저닝에 해당 그룹 또는 태그를 사용하려면 나열된 보안 그룹 또는 태그 옆의 확인란을 선택합니다.
유형	보안 요소가 요청 시 보안 그룹, 기존 보안 그룹 또는 보안 태그인지 나타냅니다.
설명	보안 그룹 또는 태그에 대해 정의된 설명을 표시합니다.
끝점	NSX 보안 그룹 또는 태그에 사용되는 끝점을 표시합니다.

속성 탭

필요한 경우 vSphere 시스템 구성 요소에 대한 사용자 지정 속성 및 속성 그룹 정보를 지정합니다.

속성 탭을 사용하면 개별 사용자 지정 속성 또는 사용자 지정 속성 그룹을 시스템 구성 요소에 추가할 수 있습니다. **새 Blueprint** 또는 **Blueprint 속성** 페이지를 각각 사용하여 Blueprint를 생성하거나 편집할 때도 속성 탭을 사용하여 사용자 지정 속성 및 속성 그룹을 전체 Blueprint에 추가할 수 있습니다.

사용자 지정 속성 탭에서는 기존 사용자 지정 속성에 대해 옵션을 추가하고 구성할 수 있습니다. 사용자 지정 속성이 vRealize Automation과 함께 제공되고 속성 정의를 생성할 수도 있습니다.

표 3-11. 속성 > 사용자 지정 속성 탭 설정

설정	설명
이름	사용자 지정 속성의 이름을 입력하거나, 사용 가능한 사용자 지정 속성을 드롭다운 메뉴에서 선택합니다. 예를 들어 사용자 지정 속성 이름 Machine.SSH를 입력하여 이 Blueprint를 사용하여 프로비저닝된 시스템이 SSH 연결을 허용하는지 여부를 지정합니다. 테넌트 관리자 또는 패브릭 관리자가 속성 정의를 생성한 경우 드롭다운 메뉴에 속성만 나타납니다.
값	사용자 지정 속성 이름에 연결할 값을 입력하거나 편집합니다. 예를 들어 값을 true로 설정하여 권한 있는 사용자가 Blueprint를 사용하여 프로비저닝된 시스템에 SSH를 사용하여 연결하도록 허용합니다.
암호화됨	예를 들어 값이 암호인 경우 속성 값을 암호화하도록 선택할 수 있습니다.
재정의 가능	속성 값을 속성을 사용하는 다음 사람 또는 나중 사람이 재정의할 수 있도록 지정할 수 있습니다. 일반적으로 이는 다른 설계자이지만 [요청에서 표시]를 선택하는 경우 비즈니스 사용자가 카탈로그 항목을 요청할 때 속성 값을 보고 편집할 수 있습니다.
요청에서 표시	최종 사용자에게 속성 이름 및 값을 표시하려는 경우 시스템 프로비저닝을 요청할 때 요청 양식에 속성을 표시하도록 선택할 수 있습니다. 사용자가 값을 제공하길 원하는 경우 [재정의 가능]도 선택해야 합니다.

속성 그룹 탭에서는 기존 사용자 지정 속성 그룹의 설정을 추가하고 구성할 수 있습니다. 고유한 속성 그룹을 생성하거나 기본적으로 제공되는 속성 그룹을 사용할 수 있습니다.

표 3-12. 속성 > 속성 그룹 탭 설정

설정	설명
이름	드롭다운 메뉴에서 사용 가능한 속성 그룹을 선택합니다.
위로 이동 및 아래로 이동	나열된 속성 그룹의 우선 순위 수준을 내림차순으로 제어합니다. 첫 번째로 나열되는 속성 그룹이 그 다음에 나오는 속성 그룹보다 우선 순위가 높습니다.
속성 보기	선택된 속성 그룹의 사용자 지정 속성을 표시합니다.
병합된 속성 보기	나열된 속성 그룹의 모든 사용자 지정 속성을 속성 그룹 목록에 나타나는 순서로 표시합니다. 둘 이상의 속성 그룹에 동일한 속성이 표시되는 경우, 해당 속성 이름은 목록에서 처음 나타나는 위치를 기준으로 한 번만 표시됩니다.

프로파일 탭

구성 요소 프로파일은 Blueprint를 매개 변수화하는 방법을 제공합니다. 예를 들어 소형, 중형, 대형의 Blueprint를 개별적으로 생성하는 대신 소형, 중형, 대형 기능을 가진 하나의 Blueprint를 생성하고 카탈로그 항목을 배포할 때 그 중 하나의 크기를 선택하여 사용할 수 있습니다. 구성 요소 프로파일은 Blueprint 확장을 최소화하고 카탈로그를 간소화할 목적으로 특별히 설계되었습니다.

제공된 vRealize Automation 구성 요소 프로파일 Size 및 Image에 대한 값 집합을 생성한 경우 Blueprint의 시스템 구성 요소에 대해 그러한 설정을 추가하고 구성할 수 있습니다. 또한 카탈로그 항목을 배포할 때 다른 값 집합을 선택할 수도 있습니다.

구성 요소 프로파일은 vSphere 시스템 구성 요소에 대해서만 사용할 수 있습니다.

Blueprint의 vSphere 시스템 구성 요소에 구성 요소 프로파일을 추가할 때, 프로파일의 선택된 값 집합에서 정의된 설정은 시스템 구성 요소의 다른 설정(예: CPU 수 및 스토리지)을 재정의합니다.

구성 요소 프로파일 값 집합은 클러스터의 모든 vSphere 시스템에 적용됩니다.

Size 또는 Image 구성 요소 프로파일을 사용하여 시스템을 재구성할 수 없지만 프로파일을 기반으로 계산된 CPU, 메모리 및 스토리지의 범위는 재구성 작업에 계속 사용할 수 있습니다. 예를 들어 소형(CPU 1개, 1024MB 메모리, 10GB 스토리지), 중형(CPU 3개, 2048MB 메모리, 12GB 스토리지) 및 대형(CPU 5개, 3072MB 메모리, 15GB 스토리지) Size 값 집합을 사용한 경우 시스템 재구성 동안 사용 가능한 범위는 CPU 1~5개, 1024~3072MB 메모리, 1~15GB 스토리지입니다.

구성 요소 프로파일에 대한 값 집합 정의와 관련한 자세한 내용은 사용자 지정 속성 참조 자료를 참조하십시오.

표 3-13. 프로파일 탭 설정

설정	설명
추가	Size 또는 Image 구성 요소 프로파일을 추가합니다.
값 집합 편집	선택된 구성 요소 프로파일에 대한 하나 이상의 값 집합을 정의된 값 집합 목록에서 선택하여 할당합니다. 값 집합 중 하나를 기본값으로 선택할 수 있습니다.
제거	Size 또는 Image 구성 요소 프로파일을 제거합니다.

vCloud Air 시스템 구성 요소 설정

vRealize Automation Blueprint 설계 캔버스에서 vCloud Air 시스템 구성 요소에 대해 구성할 수 있는 설정과 옵션을 이해합니다.

일반 탭

vCloud Air 시스템 구성 요소에 대한 일반 설정을 구성합니다.

표 3-14. 일반 탭 설정

설정	설명
ID	시스템 구성 요소의 이름을 입력하거나 기본값을 수락합니다.
설명	다른 설계자를 위해 시스템 구성 요소를 요약합니다.
요청에 위치 표시	vCloud Air와 같은 클라우드 환경에서는 이에 따라 사용자가 프로비저닝된 시스템에 대한 영역을 선택할 수 있습니다. vSphere와 같은 가상 환경의 경우 사용자가 요청된 시스템을 프로비저닝할 특정 데이터 센터 위치를 선택하도록 허용하기 위한 위치 기능을 구성할 수 있습니다. 이 옵션을 완전하게 구성하기 위해 시스템 관리자는 위치 파일에 데이터 센터 위치 정보를 추가하고 패브릭 관리자는 계산 리소스를 편집하여 위치와 연결합니다.

표 3-14. 일반 탭 설정 (계속)

설정	설명
예약 정책	Blueprint에 예약 정책을 적용하여 해당 Blueprint에서 프로비저닝된 시스템이 사용 가능한 일부 예약으로 제한되도록 합니다. 예를 들어 여러 서비스 수준의 그룹에 리소스를 수집하거나 특정 용도에 특정한 유형의 리소스를 쉽게 사용할 수 있도록 만들기 위해, 패브릭 관리자는 예약 요청이 처리되는 방식을 제어하는 유용한 선택적 수단을 제공하도록 예약 정책을 생성합니다. 패브릭 관리자가 예약 정책을 구성하지 않은 경우 이 드롭다운 메뉴에는 사용 가능한 옵션이 표시되지 않습니다.
시스템 접두사	<p>시스템 접두사는 패브릭 관리자에 의해 생성되며 프로비저닝된 시스템 이름을 생성하는 데 사용됩니다. 그룹 기본값 사용을 선택하는 경우 Blueprint에서 프로비저닝된 시스템에는 사용자의 비즈니스 그룹에 대한 기본값으로 구성된 시스템 접두사에 따라 이름이 지정됩니다. 구성된 시스템 접두사가 없는 경우 비즈니스 그룹 이름을 기반으로 하나가 생성됩니다.</p> <p>패브릭 관리자가 사용자가 선택하도록 기타 시스템 접두사를 구성하는 경우 사용자는 요청자가 누구인지 관계없이 해당 Blueprint에서 프로비저닝된 모든 시스템에 하나의 접두사를 적용할 수 있습니다.</p>
인스턴스: 최소 및 최대	<p>사용자가 하나의 배포 또는 하나의 확장/축소 작업에 대해 요청할 수 있는 최대 인스턴스 수와 최소 인스턴스 수를 구성합니다. 사용자가 선택할 수 있게 하지 않으려는 경우, 최소 및 최대 필드에 같은 값을 입력하면 프로비저닝할 인스턴스의 수가 정확하게 구성되고 이 시스템 구성 요소에 대한 확장/축소 작업이 사용하지 않도록 설정됩니다.</p> <p>XaaS 구성 요소는 확장/축소할 수 없고 확장/축소 작업 중 업데이트되지 않습니다. Blueprint에서 XaaS 구성 요소를 사용 중인 경우 사용자가 확장/축소 작업 후에 실행하도록 리소스 작업을 생성할 수 있으며 이 작업을 통해 필요에 맞게 XaaS 구성 요소를 확장/축소하거나 업데이트할 수 있습니다. 또는 각 시스템 구성 요소에 허용할 인스턴스 수를 정확하게 구성하여 확장/축소가 사용되지 않도록 설정할 수 있습니다.</p>

빌드 정보 탭

vCloud Air 시스템 구성 요소에 대한 빌드 정보 설정을 구성합니다.

표 3-15. 빌드 정보 탭

설정	설명
Blueprint 유형	기록 보관 및 라이선싱 용도를 위해 이 Blueprint에서 프로비저닝된 시스템이 데스크톱 또는 서버로 분류되는지 선택합니다.
작업	<p>작업 드롭다운 메뉴에 표시되는 옵션은 선택하는 시스템 유형에 따라 다릅니다.</p> <p>vCloud Air 시스템 구성 요소에서 수행할 수 있는 유일한 프로비저닝 작업은 복제입니다.</p> <ul style="list-style-type: none"> ■ 복제 <p>템플릿 및 사용자 지정 개체에서 가상 시스템의 복사본을 만듭니다.</p>

표 3-15. 빌드 정보 탭 (계속)

설정	설명
프로비저닝 워크플로	<p>프로비저닝 워크플로 드롭다운 메뉴에 표시되는 옵션은 선택하는 시스템 유형 및 선택하는 작업에 따라 다릅니다.</p> <p>vCloud Air 시스템 구성 요소에서 수행할 수 있는 유일한 프로비저닝 작업은 CloneWorkflow입니다.</p> <ul style="list-style-type: none"> CloneWorkflow <p>복제, 연결된 복제 또는 NetApp Flexclone으로 가상 시스템의 복사본을 만듭니다.</p>
복제 원본	<p>복제 원본으로 사용할 시스템 템플릿을 선택합니다. 각 열 드롭다운 메뉴에서 필터 옵션(예: 이름 열의 필터 메뉴 옵션)을 사용하여 사용 가능한 템플릿 목록을 구체화할 수 있습니다.</p> <p>연결된 복제의 경우 복제 원본으로 사용 가능한 스냅샷이 있는 시스템 그리고 테넌트 관리자 또는 비즈니스 그룹 관리자로 관리하는 시스템만 표시됩니다.</p> <p>자신이 비즈니스 그룹 관리자 또는 테넌트 관리자로 관리하는 시스템에 있는 템플릿에서만 복제할 수 있습니다.</p>

시스템 리소스 탭

vCloud Air 시스템 구성 요소에 대한 CPU, 메모리 및 스토리지 설정을 지정합니다.

표 3-16. 시스템 리소스 탭

설정	설명
CPU: 최소 및 최대	해당 시스템 구성 요소가 프로비저닝할 수 있는 CPU 수의 최소값 및 최대값을 입력합니다.
메모리(MB): 최소 및 최대	해당 시스템 구성 요소가 프로비저닝한 시스템이 사용할 수 있는 메모리 크기의 최소값 및 최대값을 입력합니다.
스토리지(GB): 최소 및 최대	<p>해당 시스템 구성 요소가 프로비저닝한 시스템이 사용할 수 있는 스토리지 크기의 최소값 및 최대값을 입력합니다.</p> <p>vSphere, KVM (RHEV), SCVMM, vCloud Air 및 vCloud Director의 경우 [스토리지] 탭에 입력하는 값을 기반으로 최소 스토리지가 설정됩니다.</p>

스토리지 탭

하나 이상의 스토리지 예약 정책을 포함한 스토리지 볼륨 설정을 시스템 구성 요소에 추가하여 스토리지 공간을 제어할 수 있습니다.

표 3-17. 스토리지 탭 설정

설정	설명
ID	스토리지 볼륨의 ID 또는 이름을 입력합니다.
용량(GB)	스토리지 볼륨의 스토리지 용량을 입력합니다.
드라이브 문자/마운트 경로	스토리지 볼륨의 드라이브 문자 또는 마운트 경로를 입력합니다.
레이블	스토리지 볼륨의 드라이브 문자 및 마운트 경로에 대한 레이블을 입력합니다.

표 3-17. 스토리지 탭 설정 (계속)

설정	설명
스토리지 예약 정책	이 스토리지 볼륨에 사용할 기존 스토리지 예약 정책을 입력합니다.
사용자 지정 속성	이 스토리지 볼륨에 사용할 사용자 지정 속성을 모두 입력합니다.
최대 볼륨 수	시스템 구성 요소에서 프로비저닝할 때 사용할 수 있는 허용된 스토리지 볼륨의 최대 개수를 입력합니다. 다른 사용자가 스토리지 볼륨을 추가하는 것을 방지하려면 0을 입력합니다. 기본값은 60입니다.
사용자가 스토리지 예약 정책을 보고 변경할 수 있도록 허용	사용자가 연결된 예약 정책을 제거하도록 허용하거나 프로비저닝할 때 다른 예약 정책을 지정하려면 이 확인란을 선택합니다.

속성 탭

필요한 경우 vCloud Air 시스템 구성 요소에 대한 사용자 지정 속성 및 속성 그룹 정보를 지정합니다.

속성 탭을 사용하면 개별 사용자 지정 속성 또는 사용자 지정 속성 그룹을 시스템 구성 요소에 추가할 수 있습니다. 새 **Blueprint** 또는 **Blueprint 속성** 페이지를 각각 사용하여 Blueprint를 생성하거나 편집할 때도 속성 탭을 사용하여 사용자 지정 속성 및 속성 그룹을 전체 Blueprint에 추가할 수 있습니다.

사용자 지정 속성 탭에서는 기존 사용자 지정 속성에 대해 옵션을 추가하고 구성할 수 있습니다. 사용자 지정 속성이 vRealize Automation과 함께 제공되고 속성 정의를 생성할 수도 있습니다.

표 3-18. 속성 > 사용자 지정 속성 탭 설정

설정	설명
이름	사용자 지정 속성의 이름을 입력하거나, 사용 가능한 사용자 지정 속성을 드롭다운 메뉴에서 선택합니다. 예를 들어 사용자 지정 속성 이름 Machine.SSH를 입력하여 이 Blueprint를 사용하여 프로비저닝된 시스템이 SSH 연결을 허용하는지 여부를 지정합니다. 테넌트 관리자 또는 패브릭 관리자가 속성 정의를 생성한 경우 드롭다운 메뉴에 속성만 나타납니다.
값	사용자 지정 속성 이름에 연결할 값을 입력하거나 편집합니다. 예를 들어 값을 true로 설정하여 권한 있는 사용자가 Blueprint를 사용하여 프로비저닝된 시스템에 SSH를 사용하여 연결하도록 허용합니다.
암호화됨	예를 들어 값이 암호인 경우 속성 값을 암호화하도록 선택할 수 있습니다.

표 3-18. 속성 > 사용자 지정 속성 탭 설정 (계속)

설정	설명
재정의 가능	속성 값을 속성을 사용하는 다음 사람 또는 나중 사람이 재정의할 수 있도록 지정할 수 있습니다. 일반적으로 이는 다른 설계자이지만 [요청에서 표시]를 선택하는 경우 비즈니스 사용자가 카탈로그 항목을 요청할 때 속성 값을 보고 편집할 수 있습니다.
요청에서 표시	최종 사용자에게 속성 이름 및 값을 표시하려는 경우 시스템 프로비저닝을 요청할 때 요청 양식에 속성을 표시하도록 선택할 수 있습니다. 사용자가 값을 제공하길 원하는 경우 [재정의 가능]도 선택해야 합니다.

속성 그룹 탭에서는 기존 사용자 지정 속성 그룹의 설정을 추가하고 구성할 수 있습니다. 고유한 속성 그룹을 생성하거나 기본적으로 제공되는 속성 그룹을 사용할 수 있습니다.

표 3-19. 속성 > 속성 그룹 탭 설정

설정	설명
이름	드롭다운 메뉴에서 사용 가능한 속성 그룹을 선택합니다.
위로 이동 및 아래로 이동	나열된 속성 그룹의 우선 순위 수준을 내림차순으로 제어합니다. 첫 번째로 나열되는 속성 그룹이 그 다음에 나오는 속성 그룹보다 우선 순위가 높습니다.
속성 보기	선택된 속성 그룹의 사용자 지정 속성을 표시합니다.
병합된 속성 보기	나열된 속성 그룹의 모든 사용자 지정 속성을 속성 그룹 목록에 나타나는 순서로 표시합니다. 둘 이상의 속성 그룹에 동일한 속성이 표시되는 경우, 해당 속성 이름은 목록에서 처음 나타나는 위치를 기준으로 한 번만 표시됩니다.

Amazon 시스템 구성 요소 설정

vRealize Automation Blueprint 설계 캔버스의 Amazon 시스템 구성 요소에 대해 구성할 수 있는 설정과 옵션을 이해합니다.

일반 탭

Amazon 시스템 구성 요소에 대한 일반 설정을 구성합니다.

표 3-20. 일반 탭 설정

설정	설명
ID	시스템 구성 요소의 이름을 입력하거나 기본값을 수락합니다.
설명	다른 설계자를 위해 시스템 구성 요소를 요약합니다.
요청에 위치 표시	vCloud Air와 같은 클라우드 환경에서는 이에 따라 사용자가 프로비저닝된 시스템에 대한 영역을 선택할 수 있습니다. vSphere와 같은 가상 환경의 경우 사용자가 요청된 시스템을 프로비저닝할 특정 데이터 센터 위치를 선택하도록 허용하기 위한 위치 기능을 구성할 수 있습니다. 이 옵션을 완전하게 구성하기 위해 시스템 관리자는 위치 파일에 데이터 센터 위치 정보를 추가하고 패브릭 관리자는 계산 리소스를 편집하여 위치와 연결합니다.

표 3-20. 일반 탭 설정 (계속)

설정	설명
예약 정책	Blueprint에 예약 정책을 적용하여 해당 Blueprint에서 프로비저닝된 시스템이 사용 가능한 일부 예약으로 제한되도록 합니다. 예를 들어 여러 서비스 수준의 그룹에 리소스를 수집하거나 특정 용도에 특정한 유형의 리소스를 쉽게 사용할 수 있도록 만들기 위해, 패브릭 관리자는 예약 요청이 처리되는 방식을 제어하는 유용한 선택적 수단을 제공하도록 예약 정책을 생성합니다. 패브릭 관리자가 예약 정책을 구성하지 않은 경우 이 드롭다운 메뉴에는 사용 가능한 옵션이 표시되지 않습니다.
시스템 접두사	<p>시스템 접두사는 패브릭 관리자에 의해 생성되며 프로비저닝된 시스템 이름을 생성하는 데 사용됩니다. 그룹 기본값 사용을 선택하는 경우 Blueprint에서 프로비저닝된 시스템에는 사용자의 비즈니스 그룹에 대한 기본값으로 구성된 시스템 접두사에 따라 이름이 지정됩니다. 구성된 시스템 접두사가 없는 경우 비즈니스 그룹 이름을 기반으로 하나가 생성됩니다.</p> <p>패브릭 관리자가 사용자가 선택하도록 기타 시스템 접두사를 구성하는 경우 사용자는 요청자가 누구인지 관계없이 해당 Blueprint에서 프로비저닝된 모든 시스템에 하나의 접두사를 적용할 수 있습니다.</p>
인스턴스: 최소 및 최대	<p>사용자가 하나의 배포 또는 하나의 확장/축소 작업에 대해 요청할 수 있는 최대 인스턴스 수와 최소 인스턴스 수를 구성합니다. 사용자가 선택할 수 있게 하지 않으려는 경우, 최소 및 최대 필드에 같은 값을 입력하면 프로비저닝할 인스턴스의 수가 정확하게 구성되고 이 시스템 구성 요소에 대한 확장/축소 작업이 사용하지 않도록 설정됩니다.</p> <p>XaaS 구성 요소는 확장/축소할 수 없고 확장/축소 작업 중 업데이트되지 않습니다. Blueprint에서 XaaS 구성 요소를 사용 중인 경우 사용자가 확장/축소 작업 후에 실행하도록 리소스 작업을 생성할 수 있으며 이 작업을 통해 필요에 맞게 XaaS 구성 요소를 확장/축소하거나 업데이트할 수 있습니다. 또는 각 시스템 구성 요소에 허용할 인스턴스 수를 정확하게 구성하여 확장/축소가 사용되지 않도록 설정할 수 있습니다.</p>

빌드 정보 탭

Amazon 시스템 구성 요소에 대한 빌드 정보 설정을 구성합니다.

표 3-21. 빌드 정보 탭

설정	설명
Blueprint 유형	기록 보관 및 라이선싱 용도를 위해 이 Blueprint에서 프로비저닝된 시스템이 데스크톱 또는 서버로 분류되는지 선택합니다.
프로비저닝 워크플로	<p>Amazon 시스템 구성 요소에는 CloudProvisioningWorkflow 프로비저닝 워크플로만 사용할 수 있습니다.</p> <ul style="list-style-type: none"> ■ CloudProvisioningWorkflow <p>가상 시스템 인스턴스 또는 클라우드 기반 이미지부터 시작하여 시스템을 생성합니다.</p>

표 3-21. 빌드 정보 탭 (계속)

설정	설명
Amazon 시스템 이미지	<p>사용 가능한 Amazon 시스템 이미지를 선택합니다. Amazon 시스템 이미지는 운영 체제를 포함한 소프트웨어 구성이 포함되어 있는 템플릿입니다. 시스템 이미지는 Amazon Web Services 계정을 통해 관리됩니다. AMI ID 열 드롭다운 메뉴에 있는 필터 옵션을 사용하여 표시되는 Amazon 시스템 이미지 이름 목록을 구체화할 수 있습니다.</p>
키 쌍	<p>Amazon Web Services를 사용하여 프로비저닝하는 경우에는 키 쌍이 필요합니다.</p> <p>키 쌍은 클라우드 인스턴스를 프로비저닝하고 클라우드 인스턴스에 연결하는 데 사용됩니다. 이는 Windows 암호를 해독하고 Linux 시스템에 로그인하는 데에도 사용됩니다.</p> <p>다음과 같은 키 쌍 옵션을 사용할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 지정되지 않음 <p>예약 수준이 아니라 Blueprint 수준에서 키 쌍의 동작을 제어합니다.</p> ■ 비즈니스 그룹별로 자동 생성됨 <p>동일한 비즈니스 그룹에 프로비저닝된 각 시스템이 동일한 키 쌍을 사용하도록 지정합니다. 시스템에서 동일한 계산 리소스와 비즈니스 그룹을 사용하는 경우, 다른 예약에 프로비저닝된 시스템도 여기에 포함됩니다. 키 쌍이 비즈니스 그룹과 연결되어 있기 때문에 비즈니스 그룹이 삭제될 때 키 쌍도 삭제됩니다.</p> ■ 시스템별로 자동 생성됨 <p>각 시스템에서 고유한 키 쌍을 사용하도록 지정합니다. 시스템 간에 키 쌍이 공유되지 않기 때문에 [시스템별로 자동 생성됨] 옵션은 가장 안전한 방법입니다.</p>
시스템에서 Amazon 네트워크 옵션 사용	<p>사용자가 요청을 제출할 때 VPC(Virtual Private Cloud) 또는 VPC 이외의 위치에서 시스템을 프로비저닝하도록 허용할지 선택합니다.</p>
인스턴스 유형	<p>Amazon 인스턴스 유형을 하나 이상 선택합니다. Amazon 인스턴스는 Amazon Web Services에서 애플리케이션을 실행할 수 있는 가상 서버입니다. 인스턴스는 Amazon 시스템 이미지에서 적절한 인스턴스 유형을 선택하여 생성됩니다. vRealize Automation은 프로비저닝에 사용할 수 있는 시스템 이미지 인스턴스 유형을 관리합니다.</p> <p>vRealize Automation에서 Amazon 인스턴스 유형 사용에 대한 자세한 내용은 Amazon 인스턴스 유형 이해 및 Amazon 인스턴스 유형 추가의 내용을 참조하십시오.</p>

시스템 리소스 탭

Amazon 시스템 구성 요소의 CPU, 메모리, 스토리지 및 EBS 볼륨 설정을 지정합니다.

배포에서 루트 볼륨을 제외한 모든 Amazon 시스템 스토리지 볼륨을 재구성할 수도 있습니다.

표 3-22. 시스템 리소스 탭

설정	설명
CPU: 최소 및 최대	해당 시스템 구성 요소가 프로비저닝할 수 있는 CPU 수의 최소값 및 최대값을 입력합니다.
메모리(MB): 최소 및 최대	해당 시스템 구성 요소가 프로비저닝한 시스템이 사용할 수 있는 메모리 크기의 최소값 및 최대값을 입력합니다.
스토리지(GB): 최소 및 최대	해당 시스템 구성 요소가 프로비저닝한 시스템이 사용할 수 있는 스토리지 크기의 최소값 및 최대값을 입력합니다. vSphere, KVM (RHEV), SCVMM, vCloud Air 및 vCloud Director의 경우 [스토리지] 탭에 입력하는 값을 기반으로 최소 스토리지가 설정됩니다.
EBS 스토리지(GB): 최소 및 최대	해당 시스템 구성 요소가 프로비저닝한 시스템 리소스가 사용할 수 있는 Amazon EBS(Elastic Block Store) 스토리지 볼륨 크기의 최소값 및 최대값을 입력합니다. Amazon 시스템 구성 요소가 포함된 배포를 제거 중인 경우, 수명 주기 동안 시스템에 추가된 모든 EBS 볼륨이 제거되지 않고 대신 분리됩니다. vRealize Automation은 EBS 볼륨 제거에 대한 옵션을 제공하지 않습니다.

속성 탭

필요한 경우 Amazon 시스템 구성 요소에 대해 사용자 지정 속성 및 속성 그룹 정보를 지정할 수 있습니다.

속성 탭을 사용하면 개별 사용자 지정 속성 또는 사용자 지정 속성 그룹을 시스템 구성 요소에 추가할 수 있습니다. 새 **Blueprint** 또는 **Blueprint 속성** 페이지를 각각 사용하여 Blueprint를 생성하거나 편집할 때도 속성 탭을 사용하여 사용자 지정 속성 및 속성 그룹을 전체 Blueprint에 추가할 수 있습니다.

사용자 지정 속성 탭에서는 기존 사용자 지정 속성에 대해 옵션을 추가하고 구성할 수 있습니다. 사용자 지정 속성이 vRealize Automation과 함께 제공되고 속성 정의를 생성할 수도 있습니다.

표 3-23. 속성 > 사용자 지정 속성 탭 설정

설정	설명
이름	사용자 지정 속성의 이름을 입력하거나, 사용 가능한 사용자 지정 속성을 드롭다운 메뉴에서 선택합니다. 예를 들어 사용자 지정 속성 이름 Machine.SSH를 입력하여 이 Blueprint를 사용하여 프로비저닝된 시스템이 SSH 연결을 허용하는지 여부를 지정합니다. 테넌트 관리자 또는 패브릭 관리자가 속성 정의를 생성한 경우 드롭다운 메뉴에 속성만 나타납니다.
값	사용자 지정 속성 이름에 연결할 값을 입력하거나 편집합니다. 예를 들어 값을 true로 설정하여 권한 있는 사용자가 Blueprint를 사용하여 프로비저닝된 시스템에 SSH를 사용하여 연결하도록 허용합니다.
암호화됨	예를 들어 값이 암호인 경우 속성 값을 암호화하도록 선택할 수 있습니다.

표 3-23. 속성 > 사용자 지정 속성 탭 설정 (계속)

설정	설명
재정의 가능	속성 값을 속성을 사용하는 다음 사람 또는 나중 사람이 재정의할 수 있도록 지정할 수 있습니다. 일반적으로 이는 다른 설계자이지만 [요청에서 표시]를 선택하는 경우 비즈니스 사용자가 카탈로그 항목을 요청할 때 속성 값을 보고 편집할 수 있습니다.
요청에서 표시	최종 사용자에게 속성 이름 및 값을 표시하려는 경우 시스템 프로비저닝을 요청할 때 요청 양식에 속성을 표시하도록 선택할 수 있습니다. 사용자가 값을 제공하길 원하는 경우 [재정의 가능]도 선택해야 합니다.

속성 그룹 탭에서는 기존 사용자 지정 속성 그룹의 설정을 추가하고 구성할 수 있습니다. 고유한 속성 그룹을 생성하거나 기본적으로 제공되는 속성 그룹을 사용할 수 있습니다.

표 3-24. 속성 > 속성 그룹 탭 설정

설정	설명
이름	드롭다운 메뉴에서 사용 가능한 속성 그룹을 선택합니다.
위로 이동 및 아래로 이동	나열된 속성 그룹의 우선 순위 수준을 내림차순으로 제어합니다. 첫 번째로 나열되는 속성 그룹이 그 다음에 나오는 속성 그룹보다 우선 순위가 높습니다.
속성 보기	선택된 속성 그룹의 사용자 지정 속성을 표시합니다.
병합된 속성 보기	나열된 속성 그룹의 모든 사용자 지정 속성을 속성 그룹 목록에 나타나는 순서로 표시합니다. 둘 이상의 속성 그룹에 동일한 속성이 표시되는 경우, 해당 속성 이름은 목록에서 처음 나타나는 위치를 기준으로 한 번만 표시됩니다.

OpenStack 시스템 구성 요소 설정

vRealize Automation Blueprint 설계 캔버스에서 OpenStack 시스템 구성 요소에 대해 구성할 수 있는 설정과 옵션을 이해합니다.

일반 탭

OpenStack 시스템 구성 요소에 대한 일반 설정을 구성합니다.

표 3-25. 일반 탭 설정

설정	설명
ID	시스템 구성 요소의 이름을 입력하거나 기본값을 수락합니다.
설명	다른 설계자를 위해 시스템 구성 요소를 요약합니다.
요청에 위치 표시	vCloud Air와 같은 클라우드 환경에서는 이에 따라 사용자가 프로비저닝된 시스템에 대한 영역을 선택할 수 있습니다. vSphere와 같은 가상 환경의 경우 사용자가 요청된 시스템을 프로비저닝할 특정 데이터 센터 위치를 선택하도록 허용하기 위한 위치 기능을 구성할 수 있습니다. 이 옵션을 완전하게 구성하기 위해 시스템 관리자는 위치 파일에 데이터 센터 위치 정보를 추가하고 패브릭 관리자는 계산 리소스를 편집하여 위치와 연결합니다.

표 3-25. 일반 탭 설정 (계속)

설정	설명
예약 정책	Blueprint에 예약 정책을 적용하여 해당 Blueprint에서 프로비저닝된 시스템이 사용 가능한 일부 예약으로 제한되도록 합니다. 예를 들어 여러 서비스 수준의 그룹에 리소스를 수집하거나 특정 용도에 특정한 유형의 리소스를 쉽게 사용할 수 있도록 만들기 위해, 패브릭 관리자는 예약 요청이 처리되는 방식을 제어하는 유용한 선택적 수단을 제공하도록 예약 정책을 생성합니다. 패브릭 관리자가 예약 정책을 구성하지 않은 경우 이 드롭다운 메뉴에는 사용 가능한 옵션이 표시되지 않습니다.
시스템 접두사	<p>시스템 접두사는 패브릭 관리자에 의해 생성되며 프로비저닝된 시스템 이름을 생성하는 데 사용됩니다. 그룹 기본값 사용을 선택하는 경우 Blueprint에서 프로비저닝된 시스템에는 사용자의 비즈니스 그룹에 대한 기본값으로 구성된 시스템 접두사에 따라 이름이 지정됩니다. 구성된 시스템 접두사가 없는 경우 비즈니스 그룹 이름을 기반으로 하나가 생성됩니다.</p> <p>패브릭 관리자가 사용자가 선택하도록 기타 시스템 접두사를 구성하는 경우 사용자는 요청자가 누구인지 관계없이 해당 Blueprint에서 프로비저닝된 모든 시스템에 하나의 접두사를 적용할 수 있습니다.</p>
인스턴스: 최소 및 최대	<p>사용자가 하나의 배포 또는 하나의 확장/축소 작업에 대해 요청할 수 있는 최대 인스턴스 수와 최소 인스턴스 수를 구성합니다. 사용자가 선택할 수 있게 하지 않으려는 경우, 최소 및 최대 필드에 같은 값을 입력하면 프로비저닝할 인스턴스의 수가 정확하게 구성되고 이 시스템 구성 요소에 대한 확장/축소 작업이 사용하지 않도록 설정됩니다.</p> <p>XaaS 구성 요소는 확장/축소할 수 없고 확장/축소 작업 중 업데이트되지 않습니다. Blueprint에서 XaaS 구성 요소를 사용 중인 경우 사용자가 확장/축소 작업 후에 실행하도록 리소스 작업을 생성할 수 있으며 이 작업을 통해 필요에 맞게 XaaS 구성 요소를 확장/축소하거나 업데이트할 수 있습니다. 또는 각 시스템 구성 요소에 허용할 인스턴스 수를 정확하게 구성하여 확장/축소가 사용되지 않도록 설정할 수 있습니다.</p>

빌드 정보 탭

OpenStack 시스템 구성 요소에 대한 빌드 정보 설정을 구성합니다.

표 3-26. 빌드 정보 탭

설정	설명
Blueprint 유형	기록 보관 및 라이선싱 용도를 위해 이 Blueprint에서 프로비저닝된 시스템이 데스크톱 또는 서버로 분류되는지 선택합니다.
프로비저닝 워크플로	<p>OpenStack 시스템 구성 요소에 대해서는 다음과 같은 프로비저닝 워크플로를 사용할 수 있습니다.</p> <ul style="list-style-type: none"> ■ CloudLinuxKickstartWorkflow ISO 이미지에서 부팅하여 시스템을 프로비저닝하며, kickstart 또는 autoYaSt 구성 파일과 Linux 배포 이미지를 사용하여 시스템에 운영 체제를 설치합니다. ■ CloudProvisioningWorkflow 가상 시스템 인스턴스 또는 클라우드 기반 이미지부터 시작하여 시스템을 생성합니다. ■ CloudWIMImageWorkflow WinPE 환경으로 부팅하고, 기존 Windows 참조 시스템의 WIM(Windows Imaging File Format) 이미지를 사용하여 운영 체제를 설치하는 방법으로 시스템을 프로비저닝합니다. Blueprint에서 WIM 프로비저닝 워크플로를 사용하는 경우, 시스템에서 사용될 각 디스크의 크기를 고려하여 스토리지 값을 지정해야 합니다. 모든 디스크의 총 값을 시스템 구성 요소의 최소 스토리지 값으로 사용하십시오. 또한 운영 체제를 수용할 수 있을 정도로 크게 각 디스크의 크기를 지정해야 합니다.
OpenStack 이미지	<p>사용 가능한 OpenStack 이미지를 선택합니다.</p> <p>OpenStack 이미지는 운영 체제를 포함한 소프트웨어 구성이 포함되어 있는 템플릿입니다. 이미지는 OpenStack 계정을 통해 관리됩니다. 이름 옆 드롭다운 메뉴에 있는 필터 옵션을 사용하여 표시되는 OpenStack 이미지 이름 목록을 구체화할 수 있습니다.</p>

표 3-26. 빌드 정보 탭 (계속)

설정	설명
키 쌍	<p>OpenStack을 사용하여 프로비저닝하는 경우에는 키 쌍이 선택 사항입니다.</p> <p>키 쌍은 클라우드 인스턴스를 프로비저닝하고 클라우드 인스턴스에 연결하는 데 사용됩니다. 이는 Windows 암호를 해독하고 Linux 시스템에 로그인하는 데에도 사용됩니다.</p> <p>다음과 같은 키 쌍 옵션을 사용할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 지정되지 않음 <p>예약 수준이 아니라 Blueprint 수준에서 키 쌍의 동작을 제어합니다.</p> ■ 비즈니스 그룹별로 자동 생성됨 <p>동일한 비즈니스 그룹에 프로비저닝된 각 시스템이 동일한 키 쌍을 사용하도록 지정합니다. 시스템에서 동일한 계산 리소스와 비즈니스 그룹을 사용하는 경우, 다른 예약에 프로비저닝된 시스템도 여기에 포함됩니다. 키 쌍이 비즈니스 그룹과 연결되어 있기 때문에 비즈니스 그룹이 삭제될 때 키 쌍도 삭제됩니다.</p> ■ 시스템별로 자동 생성됨 <p>각 시스템에서 고유한 키 쌍을 사용하도록 지정합니다. 시스템 간에 키 쌍이 공유되지 않기 때문에 [시스템별로 자동 생성됨] 옵션은 가장 안전한 방법입니다.</p>
플레이버	<p>하나 이상의 OpenStack 플레이버를 선택합니다.</p> <p>OpenStack 플레이버는 OpenStack에서 프로비저닝된 인스턴스에 대한 시스템 리소스 규격을 정의하는 가상 하드웨어 템플릿입니다. 플레이버는 OpenStack 제공자 내에서 관리되며 데이터 수집 시 가져옵니다.</p>

시스템 리소스 탭

OpenStack 시스템 구성 요소에 대한 CPU, 메모리 및 스토리지 설정을 지정합니다.

표 3-27. 시스템 리소스 탭

설정	설명
CPU: 최소 및 최대	해당 시스템 구성 요소가 프로비저닝할 수 있는 CPU 수의 최소값 및 최대값을 입력합니다.
메모리(MB): 최소 및 최대	해당 시스템 구성 요소가 프로비저닝한 시스템이 사용할 수 있는 메모리 크기의 최소값 및 최대값을 입력합니다.
스토리지(GB): 최소 및 최대	<p>해당 시스템 구성 요소가 프로비저닝한 시스템이 사용할 수 있는 스토리지 크기의 최소값 및 최대값을 입력합니다.</p> <p>vSphere, KVM (RHEV), SCVMM, vCloud Air 및 vCloud Director의 경우 [스토리지] 탭에 입력하는 값을 기반으로 최소 스토리지가 설정됩니다.</p> <p>Blueprint에서 WIM 프로비저닝 워크플로를 사용하는 경우, 시스템에서 사용될 각 디스크의 크기를 고려하여 스토리지 값을 지정해야 합니다. 모든 디스크의 총 값을 시스템 구성 요소의 최소 스토리지 값으로 사용하십시오. 또한 운영 체제를 사용할 수 있을 정도로 크게 각 디스크의 크기를 지정해야 합니다.</p>

속성 탭

필요한 경우 OpenStack 시스템 구성 요소에 대한 사용자 지정 속성 및 속성 그룹 정보를 지정합니다.

속성 탭을 사용하면 개별 사용자 지정 속성 또는 사용자 지정 속성 그룹을 시스템 구성 요소에 추가할 수 있습니다. 새 **Blueprint** 또는 **Blueprint 속성** 페이지를 각각 사용하여 Blueprint를 생성하거나 편집할 때도 속성 탭을 사용하여 사용자 지정 속성 및 속성 그룹을 전체 Blueprint에 추가할 수 있습니다.

사용자 지정 속성 탭에서는 기존 사용자 지정 속성에 대해 옵션을 추가하고 구성할 수 있습니다. 사용자 지정 속성이 vRealize Automation과 함께 제공되고 속성 정의를 생성할 수도 있습니다.

표 3-28. 속성 > 사용자 지정 속성 탭 설정

설정	설명
이름	사용자 지정 속성의 이름을 입력하거나, 사용 가능한 사용자 지정 속성을 드롭다운 메뉴에서 선택합니다. 예를 들어 사용자 지정 속성 이름 Machine.SSH를 입력하여 이 Blueprint를 사용하여 프로비저닝된 시스템이 SSH 연결을 허용하는지 여부를 지정합니다. 테넌트 관리자 또는 패브릭 관리자가 속성 정의를 생성한 경우 드롭다운 메뉴에 속성만 나타납니다.
값	사용자 지정 속성 이름에 연결할 값을 입력하거나 편집합니다. 예를 들어 값을 true로 설정하여 권한 있는 사용자가 Blueprint를 사용하여 프로비저닝된 시스템에 SSH를 사용하여 연결하도록 허용합니다.
암호화됨	예를 들어 값이 암호인 경우 속성 값을 암호화하도록 선택할 수 있습니다.

표 3-28. 속성 > 사용자 지정 속성 탭 설정 (계속)

설정	설명
재정의 가능	속성 값을 속성을 사용하는 다음 사람 또는 나중 사람이 재정의할 수 있도록 지정할 수 있습니다. 일반적으로 이는 다른 설계자이지만 [요청에서 표시]를 선택하는 경우 비즈니스 사용자가 카탈로그 항목을 요청할 때 속성 값을 보고 편집할 수 있습니다.
요청에서 표시	최종 사용자에게 속성 이름 및 값을 표시하려는 경우 시스템 프로비저닝을 요청할 때 요청 양식에 속성을 표시하도록 선택할 수 있습니다. 사용자가 값을 제공하길 원하는 경우 [재정의 가능]도 선택해야 합니다.

속성 그룹 탭에서는 기존 사용자 지정 속성 그룹의 설정을 추가하고 구성할 수 있습니다. 고유한 속성 그룹을 생성하거나 기본적으로 제공되는 속성 그룹을 사용할 수 있습니다.

표 3-29. 속성 > 속성 그룹 탭 설정

설정	설명
이름	드롭다운 메뉴에서 사용 가능한 속성 그룹을 선택합니다.
위로 이동 및 아래로 이동	나열된 속성 그룹의 우선 순위 수준을 내림차순으로 제어합니다. 첫 번째로 나열되는 속성 그룹이 그 다음에 나오는 속성 그룹보다 우선 순위가 높습니다.
속성 보기	선택된 속성 그룹의 사용자 지정 속성을 표시합니다.
병합된 속성 보기	나열된 속성 그룹의 모든 사용자 지정 속성을 속성 그룹 목록에 나타나는 순서로 표시합니다. 둘 이상의 속성 그룹에 동일한 속성이 표시되는 경우, 해당 속성 이름은 목록에서 처음 나타나는 위치를 기준으로 한 번만 표시됩니다.

네트워크 사용자 지정 속성 사용

Blueprint 또는 시스템 구성 요소 수준에서 네트워크 사용자 지정 속성을 사용하여 NSX가 포함되지 않은 vSphere 및 Blueprint 이외의 시스템 구성 요소에 대한 네트워크 및 보안 정보를 지정할 수 있습니다.

네트워크 및 보안 구성 요소는 오직 vSphere 시스템 구성 요소와 함께 사용할 수 있습니다.

vSphere 이외의 시스템 구성 요소에는 **네트워크** 또는 **보안** 탭이 포함되어 있지 않습니다.

네트워크 또는 **보안** 탭이 없는 시스템 구성 요소의 경우 네트워크 및 보안 사용자 지정 속성(예: VirtualMachine.Network0.Name)을 해당 설계 캔버스의 **속성** 탭에 추가할 수 있습니다. NSX 네트워크, 보안 및 로드 밸런서 속성은 vSphere 시스템에만 적용할 수 있습니다.

설계 캔버스의 시스템 구성 요소를 구성할 때 **속성** 탭을 사용하여 기존 속성 그룹의 일부로 또는 개별적으로 사용자 지정 속성을 정의할 수 있습니다. 시스템 구성 요소에 대해 정의하는 사용자 지정 속성은 Blueprint에서 프로비저닝된 유형의 시스템에 적용됩니다.

사용 가능한 사용자 지정 속성에 대한 자세한 내용은 사용자 지정 속성 참조 자료 항목을 참조하십시오.

복제 및 연결된 복제에 대한 Blueprint 문제 해결

연결된 복제 또는 복제 Blueprint를 생성할 때 시스템 또는 템플릿이 누락됩니다. 공유된 복제 Blueprint를 사용하여 시스템을 요청하면 시스템 프로비저닝이 실패합니다.

문제점

복제 또는 연결된 복제 Blueprint로 작업할 때 다음 문제 중 하나가 발생할 수 있습니다.

- 연결된 복제 Blueprint를 생성할 때 복제할 목록에 시스템이 나타나지 않거나 복제하려는 시스템이 나타나지 않습니다.
- 복제 Blueprint를 생성할 때 복제할 템플릿 목록에 템플릿이 나타나지 않거나 원하는 템플릿이 나타나지 않습니다.
- 공유된 복제 Blueprint를 사용하여 시스템을 요청할 때 프로비저닝이 실패합니다.
- 데이터 수집 시간으로 인해 사용자가 연결된 복제 Blueprint를 생성 또는 편집할 때 제거된 템플릿이 사용자에게 계속 표시됩니다.

원인

일반적인 복제 및 연결된 복제 Blueprint 문제의 가능한 원인에는 여러 가지가 있습니다.

Blueprint를 생성할 때 사용할 수 있는 **현재 스냅샷 사용** 옵션을 비롯하여 **복제 원본** 및 **스냅샷에서 복제** 옵션에 대한 관련 정보는 [vSphere 시스템 구성 요소 설정](#) 항목을 참조하십시오.

표 3-30. 일반적인 복제 및 연결된 복제 Blueprint 문제의 원인

문제	원인	솔루션
시스템 누락	테넌트 관리자 또는 비즈니스 그룹 관리자로서 관리하는 시스템을 사용할 때 연결된 복제 Blueprint만 생성할 수 있습니다.	<p>테넌트 또는 비즈니스 그룹의 사용자는 vSphere 시스템을 요청해야 합니다. 적절한 역할을 가진 경우 이 작업을 직접 수행할 수 있습니다.</p> <p>이 대화상자에서 관리되지 않는 시스템을 볼 수도 있습니다.</p> <p>관리되는 시스템을 가져왔을 수 있습니다.</p> <p>vRealize Automation에서 프로비저닝된 시스템을 이 대화상자에 표시해야 하는 요구 사항은 없습니다.</p>
템플릿 누락	지정된 끝점에서 데이터 수집이 실패했거나 구성 요소의 플랫폼에 대해 끝점을 사용할 수 없습니다.	<ul style="list-style-type: none"> ■ 끝점이 클러스터링되고 여러 계산 리소스를 포함하는 경우에는 IaaS 관리자가 템플릿이 포함된 클러스터를 패브릭 그룹에 추가했는지 확인하십시오. ■ 새 템플릿의 경우 IT가 패브릭 그룹에 포함된 동일한 클러스터에 템플릿을 배치했는지 확인하십시오.

표 3-30. 일반적인 복제 및 연결된 복제 Blueprint 문제의 원인 (계속)

문제	원인	솔루션
공유된 Blueprint 사용 시 프로비저닝 실패	Blueprint의 경우 공유된 복제 Blueprint에서 시스템을 프로비저닝하기 위해 사용되는 예약에 선택한 템플릿이 있는지 확인하기 위한 검증을 사용할 수 없습니다.	사용 권한을 사용하여 템플릿이 있는 계산 리소스를 예약한 사용자만 Blueprint를 제한하는 방법을 고려하십시오.
게스트 에이전트 사용 시 프로비저닝 실패	게스트 운영 체제 사용자 지정이 완료되었지만 게스트 에이전트 작업 항목이 완료되기 전에 가상 시스템이 재부팅되어 프로비저닝이 실패할 수 있습니다. 사용자 지정 속성 <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> 를 사용하여 시간 지연을 늘릴 수 있습니다.	사용자 지정 속성 <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> 를 추가했는지 확인합니다. 값은 HH:MM:SS 형식이어야 합니다. 값을 설정하지 않는 경우 기본값은 1분 (00:01:00)입니다.
SDRS를 사용할 경우 연결된 복제 프로비저닝이 실패함	연결된 복제 프로비저닝 및 SDRS를 사용할 경우 새 시스템이 동일한 클러스터에 상주해야 합니다. 소스 시스템의 디스크가 한 클러스터에 있고 다른 클러스터에서 시스템 프로비저닝을 요청할 경우 프로비저닝 오류가 발생합니다.	SDRS 및 연결된 복제 프로비저닝을 사용할 경우 연결된 복제 소스와 동일한 클러스터에 시스템을 프로비저닝하십시오. 다른 클러스터에 프로비저닝하지 마십시오.
복제의 기반이 되는 템플릿을 찾을 수 없어서 복제 또는 연결된 복제 Blueprint 프로비저닝이 실패합니다.	더 이상 존재하지 않는 템플릿에서 복제된 Blueprint에서 시스템을 프로비저닝하는 것은 불가능합니다. vRealize Automation은 정기적으로 데이터 수집을 실행합니다(기본값: 24시간마다). 템플릿이 제거되어도 다음 데이터 수집 시점까지 변경 내용이 반영되지 않으므로 존재하지 않는 템플릿을 기반으로 Blueprint를 생성하게 될 수 있습니다.	기존 템플릿을 사용하여 Blueprint를 다시 정의한 다음 프로비저닝을 요청합니다. 하나의 예방 조치로 그리고 해당하는 경우 복제 또는 연결된 복제 Blueprint를 정의하기 전에 데이터 수집을 실행할 수 있습니다.

NSX 설정을 사용하여 Blueprint 설계

vRealize Automation과 통합된 NSX 인스턴스가 있는 경우에는 네트워크 및 보안 가상화를 위해 NSX를 사용하도록 vSphere Blueprint를 구성할 수 있습니다.

NSX와의 vRealize Automation 통합을 구성한 경우 설계 캔버스에서 네트워크, 보안 및 로드 밸런서 구성 요소를 사용하여 시스템 프로비저닝을 위한 Blueprint를 구성할 수 있습니다. 또한 새 Blueprint를 생성하거나 기존 Blueprint를 편집할 때 다음 NSX 네트워크 및 보안 설정을 전체 Blueprint에 추가할 수 있습니다.

- 전송 영역 - 프로비저닝된 시스템 배포에 사용되는 네트워크를 포함합니다.
- Edge 및 라우팅된 게이트웨이 예약 정책 - 프로비저닝된 시스템 배포를 위한 네트워크 통신을 관리합니다.
- App 분리 - 프로비저닝된 시스템 배포에 사용되는 시스템 간의 내부 트래픽만 허용합니다.

vRealize Automation 및 NSX 통합 그리고 vRealize Automation Blueprint에서의 NSX 네트워크 및 보안 구성 요소의 사용에 대한 추가 정보는 [vRA 및 NSX - 네트워크 및 보안 자동화 소개](#) 블로그 문서를 참조하십시오.

NSX 설정은 vSphere 시스템 구성 요소 유형에만 적용할 수 있습니다.

NSX 를 사용하는 새 Blueprint 및 Blueprint 속성 페이지 설정

Blueprint를 생성할 때 새 **Blueprint** 페이지를 사용하여 전체 Blueprint에 적용되는 설정(일부 NSX 설정 포함)을 지정할 수 있습니다. Blueprint를 생성한 후에는 [Blueprint 속성] 페이지에서 이러한 설정을 편집할 수 있습니다.

일반 탭

지금 또는 나중에 추가하려는 모든 구성 요소를 포함하여 전체 Blueprint에서 설정을 적용합니다.

표 3-31. 일반 탭 설정

설정	설명
이름	Blueprint 이름을 입력합니다.
식별자	식별자 필드는 사용자가 입력한 이름에 따라 자동으로 채워집니다. 지금은 이 필드를 편집할 수 있지만 Blueprint를 저장한 후에는 이 필드를 변경할 수 없습니다. 식별자는 영구적이며 테넌트 내에서 고유하기 때문에 식별자를 사용하여 프로그래밍 방식으로 Blueprint와 상호 작용하고 속성 바인딩을 생성할 수 있습니다.
설명	다른 설계자를 위해 Blueprint를 요약합니다. 이 설명은 요청 양식의 사용자에게도 나타납니다.
아카이브 기간(일)	아카이브 기간을 지정하여 리스가 만료될 때 배포를 즉시 제거하지 않고 일시적으로 보존할 수 있습니다. 해당 리스가 만료될 때 배포를 제거하려면 0(기본값)을 지정합니다. 아카이브 기간은 리스 만료 날짜에 시작됩니다. 아카이브 기간이 종료되면 배포가 제거됩니다.
배포 제한	이 Blueprint가 시스템을 프로비저닝하는 데 사용될 때 생성될 수 있는 최대 배포 수를 지정합니다.
리스 기간(일): 최소 및 최대	사용자가 리스 기간 범위 내에서 선택할 수 있도록 최소값 및 최대값을 입력합니다. 리스가 종료되면 배포가 제거되거나 아카이브됩니다. 최소값이나 최대값을 지정하지 않는 경우 리스가 만료되지 않도록 설정됩니다.

NSX 설정 탭

NSX를 구성한 경우 Blueprint를 생성하거나 편집할 때 NSX 전송 영역, Edge 및 라우팅된 게이트웨이 예약 정책 그리고 App 분리 설정을 지정할 수 있습니다. 이러한 설정은 **Blueprint** 및 **Blueprint 속성** 페이지의 **NSX 설정** 탭에서 사용할 수 있습니다.

NSX 구성에 대한 자세한 내용은 NSX 관리 가이드를 참조하십시오.

표 3-32. NSX 설정 탭 설정

설정	설명
전송 영역	<p>프로비저닝된 시스템 배포가 사용할 수 있는 네트워크를 포함하려면 기존 NSX 전송 영역을 선택합니다.</p> <p>전송 영역은 네트워크가 걸쳐 있을 수 있는 클러스터를 정의합니다. 시스템을 프로비저닝할 때 예약 및 Blueprint에 전송 영역이 지정되어 있으면 전송 영역 값이 일치해야 합니다.</p> <p>전송 영역은 요청 시 네트워크를 사용하는 Blueprint에만 필요합니다. 보안 그룹, 보안 태그 및 로드 밸런서의 경우 전송 영역은 선택 사항입니다. 전송 영역을 지정하지 않는 경우 끝점이 보안 그룹의 위치, 보안 태그의 위치 또는 로드 밸런서가 연결되는 네트워크에 의해 결정됩니다.</p>
Edge 및 라우팅된 게이트웨이 예약 정책	<p>NSX Edge 또는 라우팅된 게이트웨이 예약 정책을 선택합니다. 이 예약 정책은 라우팅된 게이트웨이 및 프로비저닝의 일부로 배포된 모든 Edge에 적용됩니다. 배포당 프로비저닝된 Edge가 하나만 있습니다.</p> <p>라우팅된 네트워크의 경우 Edge가 프로비저닝되지 않지만 예약 정책을 사용하여 라우팅된 네트워크 프로비저닝에 사용할 라우팅된 게이트웨이와 함께 예약을 선택할 수 있습니다.</p> <p>vRealize Automation은 NAT 또는 라우팅된 네트워킹으로 시스템을 프로비저닝할 때 라우팅된 게이트웨이를 네트워크 라우터로 프로비저닝합니다. Edge 또는 라우팅된 게이트웨이는 다른 가상 시스템처럼 계산 리소스를 사용하는 관리 시스템이지만 해당 배포에 속한 모든 시스템 사이의 네트워크 통신을 관리합니다. Edge 또는 라우팅된 게이트웨이를 프로비저닝하는 데 사용되는 예약은 NAT 및 로드 밸런서 가상 IP 주소에 사용되는 외부 네트워크를 결정합니다. NSX Edge와 같이 관리 시스템에 대해 별도의 관리 클러스터를 사용하는 것이 가장 좋습니다.</p>
App 분리	<p>NSX에 구성된 App 분리 보안 정책을 사용하려면 App 분리 확인란을 선택합니다. App 분리 정책은 Blueprint의 모든 vSphere 시스템 구성 요소에 적용됩니다. 선택적으로 vRealize Orchestrator가 분리된 네트워크 구성을 열어 App 분리 안팎으로 추가 경로를 허용하도록 NSX 보안 그룹 및 태그를 추가할 수 있습니다.</p>

속성 탭

Blueprint 수준에서 추가하는 사용자 지정 속성이 모든 구성 요소를 비롯한 전체 Blueprint에 적용됩니다. 하지만 해당 속성은 우선 순위 체인에서 나중에 할당된 사용자 지정 속성에 의해 재정의될 수 있습니다. 사용자 지정 속성의 우선 순위에 대한 자세한 내용은 사용자 지정 속성 참조 자료 항목을 참조하십시오.

표 3-33. 속성 탭 설정

탭	설정	설명
속성 그룹	속성 그룹	속성 그룹은 Blueprint에 사용자 지정 속성을 추가하는 프로세스를 간소화하기 위해 설계된 속성의 재사용 가능 그룹입니다. 테넌트 관리자 및 패브릭 관리자는 개별적으로 사용자 지정 속성을 삽입하는 대신 속성 그룹을 Blueprint에 추가할 수 있도록 자주 함께 사용되는 속성을 그룹화할 수 있습니다.
	추가	기존 속성 그룹을 하나 이상 추가하고 이것을 전체 Blueprint에 적용합니다. 다음 컨테이너 관련 속성 그룹이 제공됩니다. <ul style="list-style-type: none"> ■ 인증서 인증이 있는 컨테이너 호스트 속성 ■ 사용자/암호 인증이 있는 컨테이너 호스트 속성
	위로 이동/아래로 이동	그룹의 우선 순위를 지정함으로써 서로와 비교하여 각 속성 그룹에 지정된 우선 순위를 제어합니다. 목록의 첫 번째 그룹에 가장 높은 우선 순위가 있고 해당 사용자 지정 속성에 첫 번째 우선 순위가 있습니다. 또한 끝에서 끝으로 순서를 다시 지정할 수 있습니다.
	속성 보기	선택된 속성 그룹에서 사용자 지정 속성을 봅니다.
	병합된 속성 보기	사용자 지정 속성이 두 개 이상의 속성 그룹에 포함된 경우 가장 높은 우선 순위가 있는 속성 그룹에 포함된 값이 우선합니다. 속성 그룹 우선 순위 지정에 도움이 되도록 이러한 병합된 속성을 볼 수 있습니다.
사용자 지정 속성	속성 그룹 대신 개별 사용자 지정 속성을 추가할 수 있습니다.	
	새로운 문제	개별 사용자 지정 속성을 추가하고 이것을 전체 Blueprint에 적용합니다.
	이름	속성 이름을 입력합니다. 사용자 지정 속성 및 해당 정의 목록은 사용자 지정 속성 참조 자료를 참조하십시오.
	값	사용자 지정 속성의 값을 입력합니다.
	암호화됨	예를 들어 값이 암호인 경우 속성 값을 암호화하도록 선택할 수 있습니다.
	재정의 가능	속성 값을 속성을 사용하는 다음 사람 또는 나중 사람이 재정의할 수 있도록 지정할 수 있습니다. 일반적으로 이는 다른 설계자이지만 [요청에서 표시]를 선택하는 경우 비즈니스 사용자가 카탈로그 항목을 요청할 때 속성 값을 보고 편집할 수 있습니다.
	요청에서 표시	최종 사용자에게 속성 이름 및 값을 표시하려는 경우 시스템 프로비저닝을 요청할 때 요청 양식에 속성을 표시하도록 선택할 수 있습니다. 사용자가 값을 제공하길 원하는 경우 [재정의 가능]도 선택해야 합니다.

Blueprint에 NSX 전송 영역 적용

NSX 관리자는 네트워크의 클러스터 사용을 제어하기 위한 전송 영역을 생성할 수 있습니다.

Blueprint에 요청 시 네트워크가 있으면 프로비저닝된 시스템 배포에 사용되는 네트워크가 있는 NSX 전송 영역을 지정해야 합니다. 동일한 전송 영역이 예약에 지정되어 있어야 합니다.

Blueprint에 NSX Edge 또는 라우팅된 게이트웨이 예약 정책 적용

Blueprint를 통해 프로비저닝된 시스템에 대해 네트워크 통신을 관리하기 위한 예약 정책을 지정할 수 있습니다. 시스템 프로비저닝을 요청하는 경우 예약 정책이 배포에 대해 고려될 수 있는 예약을 그룹화하는 데 사용됩니다. 라우팅된 게이트웨이 예약 정책은 Edge 예약 정책이라고도 합니다.

네트워킹 정보는 각 예약에 포함되어 있습니다. 시스템이 프로비저닝될 때 Edge 또는 라우팅된 게이트웨이가 배포의 프로비저닝된 시스템에 대해 네트워크 통신을 관리하기 위한 네트워크 라우터로 할당됩니다. Blueprint 속성 페이지를 사용하여 Blueprint 수준 속성을 추가하거나 편집할 수 있습니다.

라우팅된 게이트웨이 예약 정책은 선택 사항입니다. 해당 정책은 Blueprint에 지정된 요청 시 네트워킹 및 요청 시 로드 밸런서 구성 요소에 연결되어 있는 NSX Edge를 프로비저닝하는 데 사용할 수 있는 예약을 제어합니다.

예약 정책을 사용하여 예약 선택을 제어합니다. Blueprint의 가상 시스템 정의에서 예약 정책을 선택한 다음 해당 정책을 가상 시스템에서 사용할 예약에 할당합니다.

여러 비즈니스 그룹 간에 예약을 공유할 수 없습니다.

vRealize Automation은 NAT 네트워크 및 로드 밸런서에 대해 라우팅된 게이트웨이(예: ESG(Edge 서비스 게이트웨이))를 프로비저닝합니다. 라우팅된 네트워크의 경우 vRealize Automation은 기존 분산 라우터를 사용합니다.

NAT 네트워크 프로파일 및 로드 밸런서를 통해 vRealize Automation이 NSX Edge 서비스 게이트웨이를 배포할 수 있습니다. 라우팅된 네트워크 프로파일은 NSX DLR(논리적 분산 라우터)를 사용합니다. vRealize Automation에서 DLR을 사용하려면 먼저 NSX에서 DLR이 생성되어야 합니다. vRealize Automation은 DLR을 생성할 수 없습니다. vRealize Automation은 데이터 수집 후 가상 시스템 프로비저닝에 DLR을 사용할 수 있습니다.

Edge 또는 라우팅된 게이트웨이를 프로비저닝하는 데 사용되는 예약은 NAT 및 라우팅된 네트워크 프로파일뿐만 아니라 로드 밸런서 가상 IP 주소에 사용되는 외부 네트워크를 결정합니다.

시스템 배포를 프로비저닝하기 위해 Blueprint를 사용할 때 vRealize Automation은 지정된 예약 정책과 연결된 예약만 사용하여 Edge 또는 라우팅된 게이트웨이를 프로비저닝하려고 시도합니다.

Blueprint에 NSX App 분리 보안 정책 적용

NSX App 분리 정책은 배포의 프로비저닝된 시스템과의 모든 인바운드 및 아웃바운드 트래픽을 차단하기 위한 방화벽 역할을 합니다. 정의된 NSX App 분리 정책을 지정하는 경우 Blueprint를 통해 프로비저닝된 시스템이 다른 시스템과 통신할 수 있지만 방화벽 외부에 연결할 수는 없습니다.

새 **Blueprint** 또는 **Blueprint 속성** 페이지를 사용하여 Blueprint 수준에서 App 분리를 적용할 수 있습니다.

NSX App 분리 정책을 사용하는 경우 Blueprint에 의해 프로비저닝된 시스템 간의 내부 트래픽만 허용됩니다. 프로비저닝을 요청하는 경우 프로비저닝할 시스템에 대해 보안 그룹이 생성됩니다. App 분리 보안 정책이 NSX에서 생성되고 보안 그룹에 적용됩니다. 배포 내 구성 요소 간의 내부 트래픽만 허용하도록 방화벽 규칙이 보안 정책에 정의됩니다. 관련 정보는 [NSX 끝점을 생성하고 vSphere 끝점에 연결](#) 항목을 참조하십시오.

참고 NSX Edge 로드 밸런서와 NSX App 분리 보안 정책을 모두 사용하는 Blueprint로 프로비저닝하는 경우 동적으로 프로비저닝된 로드 밸런서가 보안 그룹에 추가되지 않습니다. 이것은 로드 밸런서가 연결을 처리하는 시스템과 통신하지 못하도록 방지합니다. Edge는 NSX 분산 방화벽에서 제외되기 때문에 보안 그룹에 추가될 수 없습니다. 로드 밸런싱이 제대로 작동되도록 하려면, 다른 보안 그룹을 사용하거나 로드 밸런싱을 위해 필요한 트래픽을 구성 요소 VM에 허용하는 보안 정책을 사용하십시오.

App 분리 정책은 NSX의 다른 보안 정책보다 우선 순위가 낮습니다. 예를 들어 프로비저닝된 배포에 웹 구성 요소 시스템과 App 구성 요소 시스템이 포함되어 있으며 웹 구성 요소 시스템이 웹 서비스를 호스팅하는 경우 해당 서비스가 포트 80 및 443의 인바운드 트래픽을 허용해야 합니다. 이 경우 사용자는 이러한 포트에 대한 들어오는 트래픽을 허용하도록 정의된 방화벽 규칙이 포함된 웹 보안 정책을 NSX에 생성해야 합니다. vRealize Automation에서 사용자는 프로비저닝된 시스템 배포의 웹 구성 요소에 웹 보안 정책을 적용해야 합니다.

참고 Blueprint에 로드 밸런서가 하나 이상 포함되어 있고 Blueprint에 대해 App 분리가 사용되도록 설정되어 있으면 로드 밸런서 VIP가 App 분리 보안 그룹에 IPSet로 추가됩니다. 시스템 계층에 연결되어 있는 요청 시 보안 그룹이 Blueprint에 포함되어 있고, 이 시스템 계층이 로드 밸런서에도 연결되어 있는 경우, 요청 시 보안 그룹에는 로드 밸런서 VIP가 있는 IPSet과 시스템 계층이 포함됩니다.

웹 구성 요소 시스템이 포트 8080 및 8443에서 로드 밸런서를 사용하여 App 구성 요소 시스템에 액세스해야 하는 경우, 웹 보안 정책은 포트 80 및 443에 대한 인바운드 트래픽을 허용하는 기존 방화벽 규칙 외에도 포트 8080 및 8443에 대한 아웃바운드 트래픽을 허용하는 방화벽 규칙도 포함해야 합니다.

Blueprint의 시스템 구성 요소에 적용할 수 있는 보안 기능에 대한 자세한 내용은 [설계 캔버스에서 보안 구성 요소 사용](#)을 참조하십시오.

네트워크 및 보안 구성 요소 설정 구성

vRealize Automation은 NSX 플랫폼을 기반으로 하는 가상화된 네트워크를 지원합니다. 통합된 vRealize Automation의 컨테이너 네트워크도 지원됩니다.

vRealize Automation으로 네트워크 및 보안을 통합하려면 IaaS 관리자가 vSphere 및 NSX 끝점을 구성해야 합니다.

외부적 준비에 대한 자세한 내용은 vRealize Automation 구성 항목을 참조하십시오.

예약 및 설계 캔버스의 네트워크 설정을 지정하는 네트워크 프로파일을 생성할 수 있습니다. 외부 네트워크 프로파일은 기존의 물리적 네트워크를 정의합니다. NAT 및 라우팅된 프로파일은 가상 시스템을 프로비저닝하고 NSX Edge 디바이스를 구성할 때 새 네트워크 경로를 위해 그리고 네트워크 경로에 연결할 목적으로 네트워크 인터페이스를 구성하기 위해 NSX 논리적 스위치와 적절한 라우팅 설정을 구축하는 템플릿입니다.

설계 캔버스에 추가하는 네트워크 및 보안 구성 요소 설정은 NSX 구성에서 파생됩니다. 이러한 설정을 사용하려면 vSphere 클러스터의 NSX 인벤토리에 대해 데이터 수집을 실행해야 합니다. 네트워크 및 보안 구성 요소는 NSX에만 해당하며 vSphere 시스템 구성 요소와만 사용할 수 있습니다. NSX 구성에 대한 자세한 내용은 NSX 관리 가이드를 참조하십시오.

네트워크 또는 **보안** 탭이 없는 시스템 구성 요소의 경우 네트워크 및 보안 사용자 지정 속성(예: VirtualMachine.Network0.Name)을 해당 설계 캔버스의 **속성** 탭에 추가할 수 있습니다. NSX 네트워크, 보안 및 로드 밸런서 속성은 vSphere 시스템에만 적용할 수 있습니다.

예약과 Blueprint에 네트워크 프로파일을 지정하는 경우, Blueprint 값이 우선합니다. 예를 들어, VirtualMachine.NetworkN.ProfileName 사용자 지정 속성을 사용하여 Blueprint에 또는 Blueprint에 사용되는 예약에 네트워크 프로파일을 지정하면 Blueprint에 지정된 네트워크 프로파일이 우선합니다. 하지만 Blueprint에서 사용자 지정 속성이 사용되지 않고 사용자가 시스템 NIC를 위한 네트워크 프로파일을 선택하는 경우, vRealize Automation에서는 네트워크 프로파일이 지정되는 시스템 NIC에 대한 예약 네트워크 경로를 사용합니다.

계산 리소스에 따라, vSphere 끝점을 식별하는 전송 영역을 선택할 수 있습니다. 전송 영역은 영역 내에 생성되는 논리적 스위치와 연결될 수 있는 호스트와 클러스터를 지정합니다. 전송 영역은 여러 vSphere 클러스터로 확장될 수 있습니다. 프로비저닝에 사용되는 Blueprint와 예약은 전송 영역 설정이 동일해야 합니다. 전송 영역은 NSX 환경에서 정의됩니다. 자세한 내용은 NSX 관리 가이드를 참조하십시오.

예약, Blueprint 또는 게스트 에이전트 스크립트에 정보를 지정하여 가상 시스템에 대한 보안 설정이 프로비저닝되도록 구성할 수 있습니다. 프로비저닝될 시스템에 게스트 에이전트가 필요한 경우 예약 또는 Blueprint에 대한 요구 사항을 포함하는 보안 규칙을 추가해야 합니다. 예를 들어, 모든 시스템 간의 통신을 거부하는 기본 보안 정책을 사용하고 별도의 보안 정책에 의존하여 특정 시스템 간의 통신을 허용하는 경우 게스트 에이전트는 사용자 지정 단계 중 vRealize Automation과 통신하지 못할 수 있습니다. 시스템 프로비저닝 중에 이러한 문제를 피하려면 사용자 지정 단계 중 통신을 허용하는 기본 보안 정책을 사용합니다.

Blueprint에 컨테이너 네트워크 구성 요소를 추가할 수도 있습니다.

설계 캔버스에서 네트워크 구성 요소 사용

하나 이상의 NSX 네트워크 구성 요소를 설계 캔버스에 추가하고 Blueprint에서 vSphere 시스템 구성 요소에 대한 해당 설정을 구성할 수 있습니다.

네트워크 구성 요소를 설계 캔버스에 추가하여 Blueprint의 시스템 구성 요소 하나 이상이 해당 구성 설정을 사용 가능하도록 할 수 있습니다.

설계 캔버스에 추가하는 네트워크 및 보안 구성 요소 설정은 NSX 구성에서 파생됩니다. 이러한 설정을 사용하려면 vSphere 클러스터의 NSX 인벤토리에 대해 데이터 수집을 실행해야 합니다. 네트워크 및 보안 구성 요소는 NSX에만 해당하며 vSphere 시스템 구성 요소와만 사용할 수 있습니다. NSX 구성에 대한 자세한 내용은 NSX 관리 가이드를 참조하십시오.

기존 네트워크 구성 요소 추가

Blueprint에서 하나 이상의 vSphere 시스템 구성 요소에 해당 설정 연결을 준비하는 과정에서 설계 캔버스에 기존 NSX 네트워크 구성 요소를 추가할 수 있습니다.

기존 네트워크 구성 요소를 사용하여 NSX 네트워크를 설계 캔버스에 추가하고 vSphere 시스템 구성 요소 및 vSphere와 관련된 Software 또는 XaaS 구성 요소에 사용할 해당 설정을 구성할 수 있습니다.

기존 네트워크 구성 요소 또는 요청 시 네트워크 구성 요소를 시스템 구성 요소에 연결하면 시스템 구성 요소에 NIC 정보가 저장됩니다. 지정하는 네트워크 프로파일 정보는 네트워크 구성 요소와 함께 저장됩니다.

설계 캔버스에 네트워크 및 보안 구성 요소를 여러 개 추가할 수 있습니다.

네트워크 또는 **보안** 탭이 없는 시스템 구성 요소의 경우 네트워크 및 보안 사용자 지정 속성(예: VirtualMachine.Network0.Name)을 해당 설계 캔버스의 **속성** 탭에 추가할 수 있습니다. NSX 네트워크, 보안 및 로드 밸런서 속성은 vSphere 시스템에만 적용할 수 있습니다.

필수 조건

- NSX를 위한 네트워크 설정을 생성하고 구성합니다. 자세한 내용은 vRealize Automation 구성 및 NSX 관리 가이드를 참조하십시오.
- 클러스터에 대해 NSX 인벤토리가 실행되었는지 확인합니다.
vRealize Automation에서 NSX 구성을 사용하려면 데이터 수집을 실행해야 합니다.
- 네트워크 프로파일을 생성합니다.
- vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.
- **설계** 탭을 사용하여 설계 캔버스에서 새로운 Blueprint 또는 기존 Blueprint를 엽니다.

프로시저

- 1 범주 섹션에서 **네트워크 및 보안**을 클릭하여 사용 가능한 네트워크 및 보안 구성 요소 목록을 표시합니다.
- 2 **기존 네트워크** 구성 요소를 설계 캔버스에 끌어다 놓습니다.
- 3 **기존 네트워크** 텍스트 상자를 클릭하고 기존 네트워크 프로파일을 선택합니다.
설명, 서브넷 마스크 및 게이트웨이 값은 선택한 네트워크 프로파일에 기반하여 채워집니다.
- 4 (선택 사항) **DNS/WINS** 탭을 클릭합니다.
- 5 (선택 사항) 네트워크 프로파일에 대해 제공된 DNS 및 WINS 설정을 수락하거나 지정합니다.
 - 기본 DNS
 - 보조 DNS
 - DNS 접미사
 - 기본 설정 WINS

- 대체 WINS

기존 네트워크의 DNS 또는 WINS 설정은 변경할 수 없습니다.

6 (선택 사항) IP 범위 탭을 클릭합니다.

네트워크 프로파일에 지정된 IP 범위가 표시됩니다. 정렬 순서 또는 열 표시를 변경할 수 있습니다. NAT 네트워크의 경우 IP 범위 값을 변경할 수도 있습니다.

7 완료를 클릭하여 Blueprint를 초안으로 저장하거나 계속하여 Blueprint를 구성합니다.

후속 작업

추가적인 네트워크 구성 요소를 추가하고 설계 캔버스에서 vSphere 시스템 구성 요소의 **네트워크** 탭에 있는 설정을 선택하면 네트워크 설정을 계속 구성할 수 있습니다.

NAT 규칙 생성 및 사용

NAT 네트워크 구성 요소가 클러스터되지 않은 vSphere 시스템 구성 요소 또는 요청 시 NSX 로드 밸런서 구성 요소와 연결되어 있는 경우 Blueprint의 일대다 NAT 네트워크 구성 요소에 NAT 규칙을 추가할 수 있습니다.

모든 NSX 지원 프로토콜에 대해 NAT 규칙을 정의할 수 있습니다. Edge의 외부 IP 주소에서 NAT 네트워크 구성 요소의 개인 IP 주소로 포트 또는 포트 범위를 매핑할 수 있습니다.

- vSphere 시스템 구성 요소

클러스터되지 않은 vSphere 시스템 구성 요소에 연결된 NAT 일대다 네트워크 구성 요소에 대해 NAT 규칙을 생성할 수 있습니다.

예를 들어 두 시스템이 Blueprint의 NAT 일대다 네트워크 구성 요소에 연결되어 있는 경우 TCP 프로토콜을 사용하여 NAT 네트워크의 포트 80을 통해 외부 IP의 포트 443이 시스템에 연결할 수 있도록 허용하는 NAT 규칙을 정의할 수 있습니다.

- NSX 로드 밸런서 구성 요소

NSX 로드 밸런서 구성 요소의 VIP 네트워크와 연결된 NAT 일대다 네트워크 구성 요소에 대해 NAT 규칙을 생성할 수 있습니다.

예를 들어 NAT 네트워크 구성 요소가 세 개의 시스템을 로드 밸런싱하는 로드 밸런서 구성 요소에 연결되어 있는 경우 외부 IP의 포트 90이 UDP 프로토콜을 사용하여 NAT 네트워크의 포트 80을 통해 로드 밸런서 VIP에 연결할 수 있도록 허용하는 NAT 규칙을 정의할 수 있습니다.

원하는 수의 NAT 규칙을 생성할 수 있으며 규칙이 처리되는 순서를 제어할 수 있습니다.

다음 요소는 NAT 규칙에 지원되지 않습니다.

- 현재 네트워크에 없는 NIC
- DHCP를 사용하여 IP 주소를 가져오도록 구성된 NIC
- 시스템 클러스터

Blueprint의 NAT 네트워크 구성 요소에 NAT 규칙을 추가하려면 [요청 시 NAT 또는 요청 시 라우팅된 네트워크 구성 요소 추가](#) 항목을 참조하십시오.

NAT 규칙 사용에 대한 관련 정보는 이 [vmwarelab 블로그 게시물](#)과 같은 공개 문서를 참조하십시오.

요청 시 NAT 또는 요청 시 라우팅된 네트워크 구성 요소 추가

Blueprint에서 하나 이상의 vSphere 시스템 구성 요소에 해당 설정 연결을 준비하는 과정에서 설계 캔버스에 NSX 요청 시 NAT 네트워크 구성 요소 또는 NSX 요청 시 라우팅된 네트워크 구성 요소를 추가할 수 있습니다.

기존 네트워크 구성 요소 또는 요청 시 네트워크 구성 요소를 시스템 구성 요소에 연결하면 시스템 구성 요소에 NIC 정보가 저장됩니다. 지정하는 네트워크 프로파일 정보는 네트워크 구성 요소와 함께 저장됩니다.

설계 캔버스에 네트워크 및 보안 구성 요소를 여러 개 추가할 수 있습니다.

단일 Blueprint에 2개 이상의 요청 시 네트워크 구성 요소를 포함할 수 있습니다. 하지만 Blueprint에 사용되는 모든 요청 시 네트워크 프로파일은 동일한 외부 네트워크 프로파일을 참조해야 합니다.

네트워크 또는 **보안** 탭이 없는 시스템 구성 요소의 경우 네트워크 및 보안 사용자 지정 속성(예: VirtualMachine.Network0.Name)을 해당 설계 캔버스의 **속성** 탭에 추가할 수 있습니다. NSX 네트워크, 보안 및 로드 밸런서 속성은 vSphere 시스템에만 적용할 수 있습니다.

필수 조건

- NSX를 위한 네트워크 설정을 생성하고 구성합니다. 자세한 내용은 vRealize Automation 구성 및 NSX 관리 가이드를 참조하십시오.
- 클러스터에 대해 NSX 인벤토리가 실행되었는지 확인합니다.
vRealize Automation에서 NSX 구성을 사용하려면 데이터 수집을 실행해야 합니다.
- 요청 시 네트워크 프로파일을 생성합니다. [네트워크 프로파일 생성](#) 항목을 참조하십시오.
예를 들어 요청 시 NAT 네트워크 구성 요소를 추가하는 경우 [요청 시 네트워크를 위한 NAT 네트워크 프로파일 생성](#)을 참조하십시오.
- vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.
- **설계** 탭을 사용하여 설계 캔버스에서 새로운 Blueprint 또는 기존 Blueprint를 엽니다.
- NAT 네트워크 구성 요소에 대해 NAT 규칙을 지정하려면 NAT 일대다 네트워크 프로파일을 사용해야 합니다. [제공된 IPAM 끝점을 사용하여 NAT 네트워크 프로파일 생성](#) 또는 [타사 IPAM 끝점을 사용하여 NAT 네트워크 프로파일 생성](#)를 참조하십시오. NAT 규칙에 대한 자세한 내용은 [NAT 규칙 생성 및 사용](#)을 참조하십시오.

프로시저

- 1 범주 섹션에서 **네트워크 및 보안**을 클릭하여 사용 가능한 네트워크 및 보안 구성 요소 목록을 표시합니다.
- 2 요청 시 NAT 또는 요청 시 라우팅된 네트워크 구성 요소를 설계 캔버스에 끌어다 놓습니다.

- 3 ID 텍스트 상자에 구성 요소 이름을 입력하여 설계 캔버스에서 구성 요소에 고유한 레이블을 지정합니다.

- 4 **상위 네트워크 프로파일** 드롭다운 메뉴에서 적절한 네트워크 프로파일을 선택합니다. 예를 들어 NAT 네트워크 구성 요소를 추가하려면 의도된 네트워크 설정을 지원하도록 구성된 NAT 네트워크 프로파일을 선택합니다.

NAT 네트워크 구성 요소에 NAT 규칙을 지정하려면 NAT 일대다에 대해 구성된 상위 네트워크 프로파일을 사용해야 합니다.

선택하는 프로파일 유형에 따라 네트워크 프로파일 선택에 기반하여 다음 네트워크 설정이 채워집니다. 이러한 값은 네트워크 프로파일에서 변경해야 합니다.

- 외부 네트워크 프로파일 이름
- NAT 유형(요청 시 NAT 네트워크)
- 서브넷 마스크
- 서브넷 마스크 범위(요청 시 라우팅된 네트워크)
- 서브넷 마스크 범위(요청 시 라우팅된 네트워크)
- 기본 IP 주소(요청 시 라우팅된 네트워크)

- 5 (선택 사항) **설명** 텍스트 상자에 구성 요소 설명을 입력합니다.

- 6 (선택 사항) **DNS/WINS** 탭을 클릭합니다.

- 7 (선택 사항) 네트워크 프로파일에 대해 제공된 DNS 및 WINS 설정을 수락하거나 지정합니다.

- 기본 DNS
- 보조 DNS
- DNS 접미사
- 기본 설정 WINS
- 대체 WINS

기존 네트워크의 DNS 또는 WINS 설정은 변경할 수 없습니다.

- 8 **IP 범위** 탭을 클릭합니다.

네트워크 프로파일에 지정된 IP 범위가 표시됩니다. 정렬 순서 또는 열 표시를 변경할 수 있습니다. NAT 네트워크의 경우 IP 범위 값을 변경할 수도 있습니다.

a **IP 범위 시작** 텍스트 상자에 시작 IP 주소 값을 입력합니다.

b **IP 범위 시작** 텍스트 상자에 시작 IP 주소 값을 입력합니다.

- 9 정적 IP 범위를 사용하는 일대다 NAT 네트워크 프로파일에 기반하는 NAT 네트워크를 사용 중인 경우 **NAT 규칙** 탭을 사용하여 외부 IP가 내부 NAT 네트워크의 구성 요소에 액세스할 수 있게 하는 규칙을 추가할 수 있습니다.

NAT 일대다 네트워크의 경우 Blueprint에 NAT 네트워크 구성 요소를 추가할 때 구성할 수 있고 배포에서 NAT 네트워크를 편집할 때 변경할 수 있는 NAT 규칙을 정의할 수 있습니다.

선택할 수 있는 옵션은 NAT 네트워크 구성 요소에 연결한 vSphere 시스템 또는 NSX 로드 밸런서 구성 요소를 기반으로 합니다.

- **이름** - 고유한 규칙 이름을 입력합니다.
- **구성 요소** - NAT 네트워크가 연결된 관련 vSphere 시스템 또는 로드 밸런서 구성 요소 목록에서 선택합니다.
- **소스 포트** - [임의] 옵션을 선택하고 유효한 포트 또는 포트 범위를 입력하거나 유효한 속성 바인딩을 지정합니다.
- **대상 포트** - [임의] 옵션을 선택하고 유효한 포트 또는 포트 범위를 입력하거나 유효한 속성 바인딩을 지정합니다.
- **프로토콜** - 유효한 NSX 지원 프로토콜을 입력하거나 [TCP], [UDP] 또는 [임의] 옵션을 선택합니다.
- **설명** - NAT 규칙이 수행할 작업에 대해 간단한 설명을 입력합니다.

10 완료를 클릭하여 Blueprint를 초안으로 저장하거나 계속하여 Blueprint를 구성합니다.

후속 작업

추가적인 네트워크 구성 요소를 추가하고 설계 캔버스에서 vSphere 시스템 구성 요소의 **네트워크** 탭에 있는 설정을 선택하면 네트워크 설정을 계속 구성할 수 있습니다.

설계 캔버스에서 로드 밸런서 구성 요소 사용

설계 캔버스에 요청 시 NSX 로드 밸런서 구성 요소를 하나 이상 추가하여 Blueprint의 vSphere 시스템 구성 요소 설정을 구성할 수 있습니다.

설계 캔버스에 추가하는 네트워크 및 보안 구성 요소 설정은 NSX 구성에서 파생됩니다. 이러한 설정을 사용하려면 vSphere 클러스터의 NSX 인벤토리에 대해 데이터 수집을 실행해야 합니다. 네트워크 및 보안 구성 요소는 NSX에만 해당하며 vSphere 시스템 구성 요소와만 사용할 수 있습니다. NSX 구성에 대한 자세한 내용은 NSX 관리 가이드를 참조하십시오.

다음 규칙이 Blueprint의 VIP 네트워크 설정 및 로드 밸런서 풀에 적용됩니다.

- 풀 네트워크 프로파일이 NAT인 경우 VIP 네트워크 프로파일은 NAT 네트워크 프로파일의 일부가 될 수 있습니다.
- 풀 네트워크 프로파일이 라우팅된 경우 VIP 네트워크 프로파일은 동일한 라우팅된 네트워크에만 있을 수 있습니다.
- 풀 네트워크 프로파일이 외부 네트워크 프로파일인 경우, VIP 네트워크 프로파일은 반드시 동일한 외부 네트워크 프로파일이어야 합니다.

각 로드 밸런서 구성 요소는 로드 밸런서 서비스라고도 하는 가상 서버를 여러 개 포함할 수 있습니다. 로드 밸런서 구성 요소에 있는 각 가상 서버는 하나의 포트와 프로토콜을 가집니다. 예를 들어 HTTP 서비스 또는 HTTPS 서비스를 로드 밸런싱할 수 있습니다. 로드 밸런서가 로드 밸런싱하는 서비스는 여러 개일 수 있습니다.

NSX Edge는 로드 밸런서 가상 서버를 포함하는 네트워크 디바이스입니다. Blueprint에 둘 이상의 로드 밸런서 구성 요소가 있을 수 있지만 배포를 프로비저닝하면 각 로드 밸런서 구성 요소에 정의된 가상 서버가 단일 NSX Edge에 포함됩니다.

Blueprint에 로드 밸런서가 하나 이상 포함되어 있고 Blueprint에 대해 App 분리가 사용되도록 설정되어 있으면 로드 밸런서 VIP가 App 분리 보안 그룹에 IPSet로 추가됩니다. 시스템 계층에 연결되어 있는 요청 시 보안 그룹이 Blueprint에 포함되어 있고, 이 시스템 계층이 로드 밸런서에도 연결되어 있는 경우, 요청 시 보안 그룹에는 로드 밸런서 VIP가 있는 IPSet와 시스템 계층이 포함됩니다.

기존 배포에서 로드 밸런서 설정을 재구성하여 가상 서버를 추가, 편집 또는 제거할 수 있습니다. 자세한 정보는 [배포에서 로드 밸런서 재구성](#)의 내용을 참조하십시오.

업그레이드 또는 마이그레이션 후 로드 밸런서 구성 요소 작업에 대한 자세한 내용은 [업그레이드 또는 마이그레이션된 로드 밸런서 구성 요소 사용 시 고려 사항](#) 항목을 참조하십시오.

업그레이드 또는 마이그레이션된 로드 밸런서 구성 요소 사용 시 고려 사항

대상 vRealize Automation 릴리스의 NSX 로드 밸런서 구성 요소와 관련하여 다음과 같은 고려 사항을 이해하고 이에 대한 작업을 수행하는 것이 중요합니다.

이 정보는 이 vRealize Automation 릴리스로 업그레이드 또는 마이그레이션된 NSX 로드 밸런서 구성 요소에 적용됩니다.

- 로드 밸런서 재구성 작업 실행 시 문제가 발생하지 않도록 하려면 이 릴리스로의 업그레이드 또는 마이그레이션 전과 후에 NSX 네트워크 및 보안 인벤토리 데이터 수집을 실행해야 합니다. 새 배포에 대한 로드 밸런서 재구성 작업에는 영향을 미치지 않습니다.

자세한 내용은 vRealize Automation 7.1 또는 7.2에서 7.3으로 업그레이드 및 vRealize Automation 7.3으로 마이그레이션 항목을 참조하십시오.

- vRealize Automation 7.3부터 로드 밸런서를 재구성할 수 있습니다. 필요한 카탈로그 사용 권한은 [재구성(로드 밸런서)]입니다. 관련 정보는 [배포에서 로드 밸런서 재구성](#) 항목을 참조하십시오.
- vRealize Automation 7.x에서 이 vRealize Automation 릴리스로 업그레이드 또는 마이그레이션된 배포의 경우 로드 밸런서 재구성은 단일 로드 밸런서가 포함된 배포로만 제한됩니다.
- vRealize Automation 6.2.x에서 이 vRealize Automation 릴리스로 업그레이드 또는 마이그레이션된 배포에 대해서는 로드 밸런서 재구성 작업이 지원되지 않습니다.

요청 시 로드 밸런서 구성 요소 추가

NSX 요청 시 로드 밸런서 구성 요소를 끌어서 설계 캔버스에 놓고 Blueprint의 vSphere 시스템 구성 요소 및 컨테이너 구성 요소에 사용할 해당 설정을 구성할 수 있습니다.

특정 네트워크 트래픽 유형의 동작을 정의하기 위해 NSX 애플리케이션 프로파일을 생성하는 것과 관련된 정보는 https://www.vmware.com/support/pubs/nsx_pubs.html에서 현재 릴리스에 대한 NSX 관리 가이드를 참조하십시오.

프로시저

1 로드 밸런서 구성원 설정 정의

요청 시 NSX 로드 밸런서 구성 요소를 정의하여 네트워크의 프로비저닝된 vSphere 구성원 시스템 또는 컨테이너 시스템에 걸쳐 작업 처리를 분산할 수 있습니다.

2 가상 서버 일반 설정 정의

로드 밸런서에 대한 단일 가상 서버 프로토콜 및 포트를 정의하거나 더 많은 가상 서버를 추가하여 추가 NSX 로드 밸런서 옵션을 사용자 지정할 수 있습니다.

3 가상 서버 배포 설정 정의

일반 탭에서 **사용자 지정** 옵션을 선택하면 구성원이 트래픽을 수신하는 포트, NSX 로드 밸런서가 포트에 액세스하는 데 사용할 수 있는 프로토콜 유형, 로드 밸런싱에 사용되는 알고리즘 및 지속성 설정과 같은 풀 구성원에 대한 정보를 지정할 수 있습니다.

4 가상 서버 상태 점검 설정 정의

일반 탭에서 **사용자 지정** 옵션을 선택하면 NSX 로드 밸런서가 가상 서버 내의 풀 구성원에 대한 상태 점검을 수행하는 방법 또는 수행 여부를 지정할 수 있습니다.

5 가상 서버 고급 설정 정의

일반 탭에서 **사용자 지정** 옵션을 선택하면 NSX 로드 밸런서 구성 요소를 사용자 지정하여 단일 풀 구성원이 인식할 수 있는 동시 연결 수 및 가상 서버가 처리할 수 있는 최대 동시 연결 수와 같은 설정을 지정할 수 있습니다.

6 로드 밸런서 로깅 옵션 정의

로드 밸런서 로그에 캡처 및 기록되는 로드 밸런서 로깅 작업 유형을 정의할 수 있습니다.

로드 밸런서 구성원 설정 정의

요청 시 NSX 로드 밸런서 구성 요소를 정의하여 네트워크의 프로비저닝된 vSphere 구성원 시스템 또는 컨테이너 시스템에 걸쳐 작업 처리를 분산할 수 있습니다.

로드 밸런서 구성 요소를 설계 캔버스의 Blueprint에 추가하는 경우 로드 밸런서 구성 요소의 가상 서버 정의를 생성 또는 편집할 때 기본 또는 사용자 지정 옵션을 선택할 수 있습니다. 기본 옵션을 사용하면 가상 서버 프로토콜, 포트 및 설명을 지정하고 다른 모든 설정에 기본값을 사용할 수 있습니다. 사용자 지정 옵션을 사용하면 세부 정보의 추가 수준을 정의할 수 있습니다.

로드 밸런서가 외부 네트워크로 프로비저닝된 경우 VIP(**VIP 네트워크**로 지정됨)와 구성원 풀(**구성원 네트워크**로 지정됨)이 동일한 기존 네트워크에 있어야 합니다. VIP와 풀이 동일한 외부 네트워크에 있지 않으면 프로비저닝 중에 오류가 발생합니다.

필수 조건

- NSX를 위한 로드 밸런서 설정을 생성하고 구성합니다. 자세한 내용은 vRealize Automation 구성 및 NSX 관리 가이드를 참조하십시오.
- 클러스터에 대해 NSX 인벤토리가 실행되었는지 확인합니다.
vRealize Automation에서 NSX 구성을 사용하려면 데이터 수집을 실행해야 합니다.
- 네트워크 프로파일을 생성합니다.

- vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.
- **설계** 탭을 사용하여 설계 캔버스에서 새로운 Blueprint 또는 기존 Blueprint를 엽니다.
- 하나 이상의 vSphere 시스템 구성 요소 또는 컨테이너 구성 요소가 Blueprint에 있는지 확인합니다.

프로시저

- 1 범주 섹션에서 **네트워크 및 보안**을 클릭하여 사용 가능한 네트워크 및 보안 구성 요소 목록을 표시합니다.
- 2 **요청 시 로드 밸런서** 구성 요소를 설계 캔버스에 끌어다 놓습니다.
- 3 **ID** 텍스트 상자에 구성 요소 이름을 입력하여 설계 캔버스에서 구성 요소에 고유한 레이블을 지정합니다.
- 4 **구성원** 드롭다운 메뉴에서 vSphere 시스템 구성 요소 또는 컨테이너 구성 요소 이름을 선택합니다.

목록에는 활성 Blueprint의 vSphere 시스템 구성 요소 및 컨테이너 구성 요소만 포함됩니다.

- 5 **구성원 네트워크** 드롭다운 메뉴에서 로드 밸런싱할 NIC를 선택합니다.
목록에는 선택한 vSphere 시스템 구성원에 대해 정의된 NIC가 포함됩니다.
- 6 **VIP 네트워크** 드롭다운 메뉴에서 사용 가능한 가상 IP 주소를 선택합니다. 예를 들면 사용 가능한 외부 또는 NAT 네트워크를 선택합니다.

Blueprint에 여러 개의 NSX 로드 밸런서와 NSX 요청 시 네트워크 구성 요소를 포함할 수 있지만 이러한 구성 요소 모두가 동일한 VIP 네트워크에 연결되어 있어야 합니다.

- 7 (선택 사항) **IP 주소** 텍스트 상자에 NIC의 올바른 IP 주소를 입력합니다.

기본 설정은 VIP 네트워크에 연결된 정적 IP 주소입니다. 다른 IP 주소 또는 IP 주소 범위를 지정할 수 있습니다. 기본적으로 연결된 VIP 네트워크에서 사용 가능한 다음 IP 주소가 할당됩니다.

프로비저닝 도중 연결된 VIP 네트워크에서 IP 주소를 할당할 수 있도록 하려면 IP 주소 필드를 비워 둡니다.

NAT 네트워크에서 VIP를 만든 경우에만 IP 주소를 지정할 수 있습니다.

- 8 가상 서버 정의를 생성하려면 **새로 만들기**를 클릭하고 **가상 서버 일반 설정 정의**를 참조하십시오.
각 로드 밸런서 구성 요소에는 하나 이상의 가상 서버가 필요합니다.
로깅 옵션을 지정하려면 **로드 밸런서 로깅 옵션 정의**를 참조하십시오.

가상 서버 일반 설정 정의

로드 밸런서에 대한 단일 가상 서버 프로토콜 및 포트를 정의하거나 더 많은 가상 서버를 추가하여 추가 NSX 로드 밸런서 옵션을 사용자 지정할 수 있습니다.

예를 들어 로드 밸런서 구성 요소를 사용자 지정하여 상태 점검 프로토콜 및 포트, 알고리즘, 지속성 및 투명성과 같은 설정을 정의할 수 있습니다.

필수 조건

로드 밸런서 구성원 설정 정의.

프로시저

- 1 새로운 가상 서버 페이지에서 **일반** 탭을 클릭합니다.
- 2 **프로토콜** 드롭다운 메뉴에서 가상 서버를 로드 밸런싱하는 데 사용할 네트워크 트래픽 프로토콜을 선택합니다.

프로토콜 옵션은 HTTP, HTTPS, TCP 및 UDP입니다.

- 3 **포트** 텍스트 상자에 포트 값을 입력합니다.

선택된 프로토콜은 기본 포트 설정을 결정합니다.

프로토콜	기본 포트
HTTP	80
HTTPS	443
TCP	8080
UDP	기본값 없음

HTTP, HTTPS 및 TCP 프로토콜은 UDP와 포트를 공유할 수 있습니다. 예를 들어 서비스 1이 포트 80에서 TCP, HTTP 또는 HTTPS를 사용하는 경우 서비스 2는 포트 80에서 UDP를 사용할 수 있습니다. 하지만 서비스 1이 포트 80에서 UDP를 사용하는 경우 서비스 2는 포트 80에서 UDP를 사용할 수 없습니다.

- 4 (선택 사항) 가상 서버 구성 요소에 대한 설명을 입력합니다.
- 5 설정 옵션 중 하나를 선택합니다.

- 다른 모든 설정에 기본값 사용

다른 모든 기본 설정을 수락합니다. **확인**을 클릭하여 로드 밸런서 구성 요소 정의를 완료하고 Blueprint에서 작업을 계속합니다.

사용자 지정을 클릭하고 추가 탭 옵션을 검토하여 기본값을 표시할 수 있습니다. 기본 설정이 허용되면 **일반** 탭에서 **다른 모든 설정에 기본값 사용**을 클릭합니다.

- 사용자 지정

상태 모니터링을 위한 다양한 프로토콜 또는 구성원 트래픽 모니터링을 위한 다양한 포트를 정의하기 위해 추가 설정으로 로드 밸런서 구성 요소를 구성합니다.

사용자 지정된 설정을 추가할 수 있는 추가 탭이 표시됩니다.

다른 모든 설정에 기본값 사용을 선택하고 **확인**을 클릭한 경우 작업이 완료되며, 계속해서 설계 캔버스에서 Blueprint를 정의하거나 편집할 수 있습니다. **사용자 지정**을 선택한 경우 단계를 계속합니다.

- 6 **배포** 탭을 클릭하고 **가상 서버 배포 설정 정의** 항목을 진행하여 NSX 로드 밸런서 구성 요소에서 가상 서버 정의를 계속합니다.

가상 서버 배포 설정 정의

일반 탭에서 **사용자 지정** 옵션을 선택하면 구성원이 트래픽을 수신하는 포트, NSX 로드 밸런서가 포트에 액세스하는 데 사용할 수 있는 프로토콜 유형, 로드 밸런싱에 사용되는 알고리즘 및 지속성 설정과 같은 풀 구성원에 대한 정보를 지정할 수 있습니다.

풀은 로드 밸런싱되고 있는 시스템의 클러스터를 나타냅니다. 풀 구성원은 해당 클러스터에 있는 하나의 시스템을 나타냅니다.

기본 구성원 프로토콜 및 구성원 포트 설정은 **일반** 페이지의 프로토콜 및 포트 설정과 일치합니다.

구성원 시스템의 풀은 Blueprint 로드 밸런서 구성 요소 사용자 인터페이스의 **구성원** 옵션 값에 표시됩니다. **구성원** 항목은 시스템의 풀 또는 클러스터로 설정됩니다.

필수 조건

가상 서버 일반 설정 정의.

프로시저

- 1 (선택 사항) **구성원 프로토콜** 설정은 **일반** 탭에서 지정한 프로토콜과 일치합니다. 이 설정은 풀 구성원이 네트워크 트래픽을 수신하는 방법을 정의합니다.
- 2 (선택 사항) **구성원 포트** 텍스트 상자에 포트 번호를 입력하여 풀 구성원이 네트워크 트래픽을 수신할 포트를 지정합니다.

예를 들어 로드 밸런서 VIP(가상 IP) 주소의 수신 요청이 포트 80에 있는 경우 풀 구성원에서 요청을 다른 포트(예: 포트 8080)로 라우팅하려 할 수도 있습니다.

- 3 (선택 사항) 이 풀에 대한 알고리즘 밸런싱 메서드를 선택합니다.

알고리즘 옵션 및 옵션에 필요한 알고리즘 매개 변수가 다음 테이블에 설명되어 있습니다.

옵션	설명 및 알고리즘 매개 변수
ROUND_ROBIN	<p>각 서버에 할당된 가중치 순서대로 서버가 사용됩니다.</p> <p>로드 밸런서가 vRealize Automation에서 생성된 경우 가중치는 모든 구성원에 대해 동일합니다.</p> <p>이는 서버의 처리 시간이 균일하게 분산된 상태를 유지하는 경우 가장 유연하고 공정한 알고리즘입니다.</p> <p>이 옵션에 대해서는 알고리즘 매개 변수가 사용되지 않도록 설정됩니다.</p>
IP-HASH	<p>소스 IP 주소의 해시와 실행 중인 모든 서버의 총 가중치에 따라 서버를 선택합니다.</p> <p>이 옵션에 대해서는 알고리즘 매개 변수가 사용되지 않도록 설정됩니다.</p>
LEASTCONN	<p>서버에 이미 있는 연결 수를 기반으로 하여 클라이언트 요청을 여러 서버로 분산합니다.</p> <p>새 연결은 연결 수가 가장 적은 서버로 전송됩니다.</p> <p>이 옵션에 대해서는 알고리즘 매개 변수가 사용되지 않도록 설정됩니다.</p>

옵션	설명 및 알고리즘 매개 변수
URI	<p>URI의 왼쪽 부분(물음표 앞부분)이 해시되고 실행 중인 서버의 총 가중치로 나누어집니다.</p> <p>결과에 따라 요청을 받는 서버가 지정됩니다. 이 경우 켜지거나 꺼지는 서버가 없는 한 URI는 항상 동일한 서버로 연결됩니다.</p> <p>URI 알고리즘 매개 변수에는 <code>uriLength=<len></code> 및 <code>uriDepth=<dep></code>의 두 가지 옵션이 있습니다. 알고리즘 매개 변수 텍스트 상자의 별도의 줄에 <code>length</code> 및 <code>depth</code> 매개 변수를 입력합니다.</p> <p><code>length</code> 및 <code>depth</code> 매개 변수 다음에는 양의 정수가 옵니다. 이러한 옵션은 URI 시작 부분에 따라서만 서버 밸런스를 유지합니다.</p> <p><code>length</code> 매개 변수는 알고리즘에서 해시 계산을 위해 URI 시작 부분에 정의된 문자만 고려해야 함을 나타냅니다. <code>length</code> 매개 변수 범위는 $1 \leq \text{len} < 256$이어야 합니다.</p> <p><code>depth</code> 매개 변수는 해시 계산에 사용될 최대 디렉토리 깊이를 나타냅니다. 요청의 각 슬래시는 1개의 수준으로 계산됩니다. <code>depth</code> 매개 변수 범위는 $1 \leq \text{dep} < 10$이어야 합니다.</p> <p>두 매개 변수를 모두 지정하면 두 매개 변수 중 하나에 도달할 때 평가가 중지됩니다.</p>
HTTPHEADER	<p>HTTP 헤더 이름은 각 HTTP 요청에서 조회됩니다.</p> <p>괄호로 묶인 헤더 이름은 ACL <code>'hdr()'</code> 함수와 마찬가지로 대소문자를 구분하지 않습니다.</p> <p>HTTPHEADER 알고리즘 매개 변수에는 하나의 옵션 <code>headerName=<name></code>이 있습니다. 예를 들어 host를 HTTPHEADER 알고리즘 매개 변수로 사용할 수 있습니다.</p> <p>헤더가 없거나 값을 포함하지 않으면 라운드 로빈 알고리즘이 적용됩니다.</p>
URL	<p>인수에 지정된 URL 매개 변수는 각 HTTP GET 요청의 쿼리 문자열에서 조회됩니다.</p> <p>URL 알고리즘 매개 변수에는 하나의 옵션 <code>urlParam=<url></code>이 있습니다.</p> <p>매개 변수 다음에 등호(=)와 값이 나오면 해당 값은 해시되고 실행 중인 서버의 총 가중치로 나누어집니다. 결과에 따라 요청을 받는 서버가 지정됩니다. 이 프로세스는 요청의 사용자 식별자를 추적하는 데 사용되고, 켜지거나 꺼지는 서버가 없는 한 동일한 사용자 ID가 항상 동일한 서버로 전송되도록 합니다.</p> <p>값이나 매개 변수가 없으면 라운드 로빈 알고리즘이 적용됩니다.</p>

4 (선택 사항) 이 풀에 대한 지속성 메서드를 선택합니다.

지속성을 통해 클라이언트 요청에 서비스를 지원한 특정 풀 구성원과 같은 세션 데이터를 추적하고 저장합니다. 지속성을 사용하면 세션이 실행되는 전체 기간 또는 이후 세션이 실행되는 동안 클라이언트 요청이 동일한 풀 구성원으로 전달됩니다.

프로토콜	지원되는 지속성 메서드
HTTP	없음, 쿠키, 소스 IP
HTTPS	없음, 소스 IP 및 SSL 세션 ID

프로토콜	지원되는 지속성 메서드
TCP	없음, 소스 IP, MSRDp
UDP	없음, 소스 IP

- 쿠키를 선택하여 클라이언트가 사이트에 처음 액세스할 때 세션을 식별하기 위한 고유한 쿠키를 삽입합니다. 이 쿠키는 해당 서버에 대한 연결을 지속하기 위해 후속 요청에서 참조됩니다.
- 소스 IP 주소를 기준으로 세션을 추적하려면 **소스 IP**를 선택합니다. 클라이언트가 소스 주소 선호도 지속성을 지원하는 가상 서버에 대한 연결을 요청할 경우 로드 밸런서는 해당 클라이언트가 이전에 연결한 적이 있는지 여부를 확인한 후 연결한 적이 있으면 클라이언트를 동일한 풀 구성원에 반환합니다.
- **SSL 세션 ID**를 선택하고 SSL 패스스루 HTTPS 트래픽 패턴을 선택합니다.
 - SSL 패스스루 - 클라이언트 -> HTTPS -> LB(SSL 패스스루) -> HTTPS -> 서버
 - 클라이언트 - HTTP-> LB -> HTTP -> 서버

참고 vRealize Automation에서는 현재 SSL 패스스루만 지원합니다. SSL 패스스루 방법은 선택하는 옵션과 관계없이 사용됩니다.

- Windows 클라이언트와 Microsoft RDP(원격 데스크톱 프로토콜) 서비스를 실행하는 서버 간에 지속적인 세션을 유지하려면 **MSRDp**를 선택합니다. MSRDp 지속성을 사용하는 권장 시나리오는 지원되는 Windows Server를 실행하는 구성원으로 구성되어 있고, 모든 구성원이 Windows 클러스터에 속해 있고, Windows 세션 디렉토리에 참가하는 로드 밸런싱 풀을 생성하기 위한 것입니다.
 - 세션 작업이 후속 리콜에 대해 저장되지 않도록 지정하려면 **없음**을 선택합니다.
- 5 쿠키 지속성 설정을 사용하는 경우 쿠키 이름을 입력합니다.
- 6 (선택 사항) **모드** 드롭다운 메뉴에서 쿠키가 삽입되는 모드를 선택합니다.

옵션	설명
삽입	NSX Edge가 쿠키를 보냅니다. 서버가 하나 이상의 쿠키를 보내면 클라이언트는 하나의 추가 쿠키를 수신합니다(서버 쿠키 + NSX Edge 쿠키). 서버가 쿠키를 보내지 않을 경우 클라이언트는 NSX Edge 쿠키를 수신합니다.
접두사	서버가 쿠키를 전송합니다. 클라이언트가 둘 이상의 쿠키를 지원하지 않을 경우 이 옵션을 사용합니다. 하나의 쿠키만 지원하는 독점 클라이언트를 사용하는 독점 애플리케이션이 있는 경우 웹 서버는 쿠키를 보내지만 NSX Edge는 서버 쿠키 값에 해당 쿠키 정보를 접두사로 삽입합니다.
애플리케이션 세션	서버가 쿠키를 보내지 않습니다. 대신 사용자 세션 정보를 URL로 전송합니다. 예를 들어 http://mysite.com/admin/UpdateUserServlet;jsessionid=X000X0XXX0XXXX와 같습니다. 여기서 jsessionid는 사용자 세션 정보이며 지속성에 사용됩니다.

- 7 (선택 사항) 쿠키에 대한 지속성 만료 시간을 초 단위로 입력합니다.

예를 들어 TCP 소스 IP가 포함된 L7 로드 밸런싱의 경우 지정된 만료 시간 동안 새로운 TCP 연결이 생성되지 않는 경우 기존 연결이 아직 유효하더라도 지속성 항목의 시간이 초과됩니다.

- 8 (선택 사항) **상태 점검** 탭을 클릭하고 **가상 서버 상태 점검 설정 정의** 항목을 진행하여 NSX 로드 밸런서 구성 요소에서 가상 서버 정의를 계속합니다.

가상 서버 상태 점검 설정 정의

일반 탭에서 **사용자 지정** 옵션을 선택하면 NSX 로드 밸런서가 가상 서버 내의 풀 구성원에 대한 상태 점검을 수행하는 방법 또는 수행 여부를 지정할 수 있습니다.

기본 상태 점검 프로토콜 및 상태 점검 포트 설정은 **일반** 탭의 프로토콜 및 포트 설정과 일치합니다.

관련 정보는 https://www.vmware.com/support/pubs/nsx_pubs.html의 NSX 제품 설명서에서 서비스 모니터링 생성을 참조하십시오. NSX 설명서는 가상 서버 구성원을 풀 구성원으로 참조합니다.

필수 조건

가상 서버 일반 설정 정의.

프로시저

- 1 (선택 사항) **상태 점검 프로토콜** 드롭다운 메뉴에서 상태 점검 프로토콜을 선택하여 로드 밸런서가 풀 구성원의 상태를 결정하기 위해 수신할 때 풀 구성원이 액세스되는 방법을 지정합니다.

프로토콜 옵션은 **HTTP, HTTPS, TCP, ICMP, UDP** 및 **없음**입니다.

[일반] 탭에 지정된 기본 프로토콜을 수락할 수도 있습니다.

- 2 (선택 사항) **상태 점검 포트** 상자에 값을 입력하여 가상 서버 구성원 또는 풀 구성원의 상태를 모니터링하기 위해 로드 밸런서가 수신할 포트를 지정합니다.

NSX 설명서는 가상 서버 구성원을 풀 구성원으로 참조합니다.

HTTP, HTTPS 및 TCP 프로토콜은 UDP와 포트를 공유할 수 있습니다. 예를 들어 서비스 1이 포트 80에서 TCP, HTTP 또는 HTTPS를 사용하는 경우 서비스 2는 포트 80에서 UDP를 사용할 수 있습니다. 하지만 서비스 1이 포트 80에서 UDP를 사용하는 경우 서비스 2는 포트 80에서 UDP를 사용할 수 없습니다.

- 3 서버를 ping할 **간격** 값을 초 단위로 입력합니다.
- 4 서버의 응답을 수신해야 하는 최대 **시간 초과** 값을 초 단위로 입력합니다.
- 5 **최대 재시도 횟수** 값은 다운된 것으로 선언하기 전에 서버를 ping해야 하는 횟수로 입력합니다.
- 6 선택한 **상태 점검 프로토콜**을 기반으로 추가 상태 점검 설정을 지정합니다.
- a 서버 상태 감지에 사용할 **메서드**를 입력합니다. 옵션은 GET, OPTIONS 및 POST입니다.
 - b 서버 상태 감지 요청에 사용할 **URL**을 입력합니다. 이것은 GET 및 POST(기본적으로 "/") 메서드 옵션에 사용되는 URL입니다.

c **보내기** 텍스트 상자에 연결이 설정된 후 서버에 보낼 문자열을 입력합니다.

보내기 텍스트 상자에 연결이 설정된 후 서버에 보낼 문자열을 입력합니다.

d **받기** 텍스트 상자에 서버로부터 수신할 것으로 예상되는 문자열을 입력합니다.

수신된 문자열이 이 정의와 일치할 때에만 서버가 작동 상태인 것으로 간주됩니다.

문자열은 머리글이거나 응답 본문에 있을 수 있습니다.

7 **고급** 탭을 클릭하고 **가상 서버 고급 설정 정의** 항목을 진행하여 NSX 로드 밸런서 구성 요소에서 가상 서버 정의를 계속합니다.

로깅 옵션을 지정하려면 **로드 밸런서 로깅 옵션 정의**를 참조하십시오.

가상 서버 고급 설정 정의

일반 탭에서 **사용자 지정** 옵션을 선택하면 NSX 로드 밸런서 구성 요소를 사용자 지정하여 단일 풀 구성원이 인식할 수 있는 동시 연결 수 및 가상 서버가 처리할 수 있는 최대 동시 연결 수와 같은 설정을 지정할 수 있습니다.

필수 조건

가상 서버 일반 설정 정의.

프로시저

1 **연결 제한** 텍스트 상자에 값을 입력하여 가상 서버가 처리할 수 있는 NSX의 최대 동시 연결 수를 지정합니다.

이 설정에는 모든 구성원 연결 수가 고려됩니다.

제한을 지정하지 않으려면 값을 0으로 입력합니다.

2 **연결 속도 제한** 텍스트 상자에 값을 입력하여 초당 수락될 수 있는 NSX의 수신 연결 요청의 최대 수를 지정합니다.

이 설정에는 모든 구성원 연결 수가 고려됩니다.

제한을 지정하지 않으려면 값을 0으로 입력합니다.

3 (선택 사항) 각 VIP(가상 IP)가 L7 로드 밸런서가 아닌 더 빠른 L4 로드 밸런서를 사용하도록 지정하려면 **가속 활성화** 확인란을 선택합니다.

4 (선택 사항) 로드 밸런서 풀 구성원이 로드 밸런서를 호출하는 시스템의 IP 주소를 볼 수 있도록 허용하려면 **투명** 확인란을 선택합니다.

이 옵션을 선택하지 않으면 로드 밸런서 풀의 구성원이 트래픽 소스 IP 주소를 로드 밸런서 내부 IP 주소로 봅니다.

5 **최대 연결** 텍스트 상자에 값을 입력하여 단일 풀 구성원이 인식할 수 있는 최대 동시 연결 수를 지정합니다.

수신 요청의 수가 이 값보다 큰 경우 요청은 대기열에 들어가고 연결이 해제될 때 수신된 순서대로 처리됩니다.

최대값을 지정하지 않으려면 값을 0으로 입력합니다.

- 6 최소 연결 수** 텍스트 상자에 값을 입력하여 단일 풀 구성원이 항상 수락해야 하는 최소 동시 연결 수를 지정합니다.

최소값을 지정하지 않으려면 값을 0으로 입력합니다.

- 7 확인**을 클릭하여 가상 서버 정의를 완료합니다.

- 8** 로깅 옵션을 지정하려면 **로드 밸런서 로깅 옵션 정의**를 참조하십시오. 그렇지 않으면 **저장** 또는 **완료**를 클릭합니다.

로드 밸런서 로깅 옵션 정의

로드 밸런서 로그에 캡처 및 기록되는 로드 밸런서 로깅 작업 유형을 정의할 수 있습니다.

로드 밸런서 구성 요소를 정의한 후 또는 로드 밸런서 구성 요소를 정의하는 중 로드 밸런서 트래픽 로그 수집을 위한 로깅 수준을 지정할 수 있습니다. Blueprint의 모든 로드 밸런서 구성 요소에 대해 정의하는 로깅 수준은 Blueprint에서 정의된 모든 로드 밸런서에 적용됩니다.

로깅 수준에는 디버그, 정보, 주의, 오류 및 위험이 포함됩니다. 디버그 및 정보 옵션은 사용자 요청을 로깅하지만 주의, 오류 및 위험 옵션은 사용자 요청을 로깅하지 않습니다.

NSX 로드 밸런서 로깅에 대한 추가 정보는 NSX 관리 가이드를 참조하십시오.

필수 조건

로드 밸런서 구성원 설정 정의.

프로시저

- 1 설계 캔버스에서 로드 밸런서 구성 요소의 **글로벌** 탭을 선택합니다.
- 2 **로깅 수준** 드롭다운 메뉴에서 하나 이상의 로깅 옵션을 선택합니다.

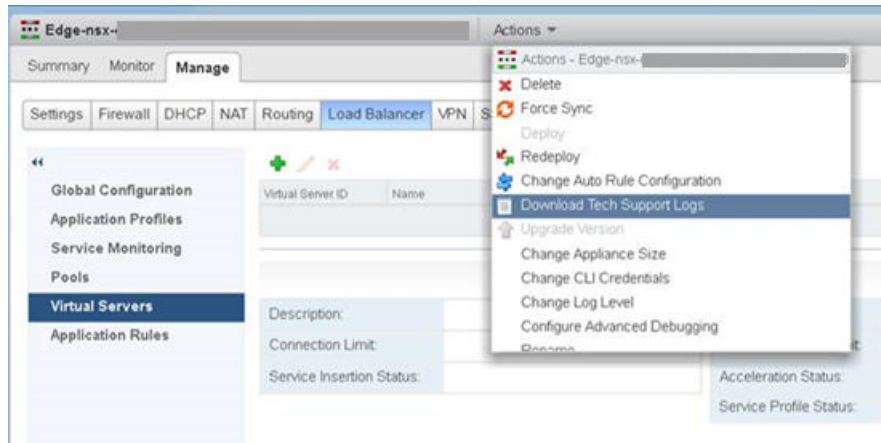
로드 밸런서 트래픽 로그 수집을 위한 로깅 수준을 선택합니다. 이 설정은 Blueprint의 모든 NSX 로드 밸런서 구성 요소에 적용됩니다.

로깅 설정은 vSphere Web Client에서 정의됩니다.

- 없음
- 정보
- 긴급
- 경고
- 위험
- 오류
- 경고
- 알림
- 디버그

- 3 **저장**을 클릭합니다.

https://www.vmware.com/support/pubs/nsx_pubs.html에 있는 NSX 제품 설명서의 NSX Edge에 대한 기술 지원 로그 다운로드에 설명된 대로 NSX Edge의 **작업** 메뉴를 사용하여 vSphere Web Client에서 로그를 보고 다운로드할 수 있습니다.



설계 캔버스에서 보안 구성 요소 사용

NSX 보안 구성 요소를 설계 캔버스에 추가하여 구성된 해당 설정을 Blueprint의 vSphere 시스템 구성 요소 하나 이상에서 사용할 수 있도록 설정할 수 있습니다.

NSX 애플리케이션에서 보안 그룹, 태그 및 정책은 vRealize Automation 외부에서 구성됩니다.

설계 캔버스에 추가하는 네트워크 및 보안 구성 요소 설정은 NSX 구성에서 파생됩니다. 이러한 설정을 사용하려면 vSphere 클러스터의 NSX 인벤토리에 대해 데이터 수집을 실행해야 합니다. 네트워크 및 보안 구성 요소는 NSX에만 해당하며 vSphere 시스템 구성 요소와만 사용할 수 있습니다. NSX 구성에 대한 자세한 내용은 NSX 관리 가이드를 참조하십시오.

NSX에서 vSphere 계산 리소스에 대한 보안 그룹, 태그 및 정책을 구성하여 Blueprint에 보안 제어를 추가할 수 있습니다. 데이터 수집을 실행한 후에는 vRealize Automation에서 보안 구성을 선택할 수 있습니다.

보안 그룹

보안 그룹은 보안 정책 집합에 매핑되는 vSphere 인벤토리의 그룹 개체 또는 자산 모음으로, 바이러스 백신, 침입 탐지와 같은 타사 보안 서비스 통합 및 분산 방화벽 규칙을 그 예로 들 수 있습니다. 그룹화 기능을 사용하면 사용자 지정 컨테이너를 생성하여 분산 방화벽으로 보호할 리소스(예: 가상 시스템 및 네트워크 어댑터)를 해당 컨테이너에 할당할 수 있습니다. 그룹을 정의한 후 방화벽 규칙에 그룹을 소스 또는 대상으로 추가하여 보호할 수 있습니다.

예약에 지정된 보안 그룹 외에도 Blueprint에 기존 NSX 또는 요청 시 보안 그룹을 추가할 수 있습니다.

요청 시 보안 그룹을 하나 이상 생성할 수 있습니다. 보안 그룹에 구성할 보안 정책을 하나 이상 선택할 수 있습니다.

보안 그룹은 소스 리소스에서 관리됩니다. 다양한 리소스 유형에 대해 보안 그룹을 관리하는 데 대한 자세한 내용은 NSX 설명서를 참조하십시오.

Blueprint에 로드 밸런서가 하나 이상 포함되어 있고 Blueprint에 대해 App 분리가 사용되도록 설정되어 있으면 로드 밸런서 VIP가 App 분리 보안 그룹에 IPSet로 추가됩니다. 시스템 계층에 연결되어 있는 요청 시 보안 그룹이 Blueprint에 포함되어 있고, 이 시스템 계층이 로드 밸런서에도 연결되어 있는 경우, 요청 시 보안 그룹에는 로드 밸런서 VIP가 있는 IPSet와 시스템 계층이 포함됩니다.

보안 태그

보안 태그는 그룹화 메커니즘으로 사용할 수 있는 한정자 개체 또는 분류 항목입니다. 생성 중인 보안 그룹에 추가되기 위해 개체가 충족해야 하는 조건을 정의합니다. 이를 통해 검색 조건에 일치시키기 위한 여러 지원 매개 변수로 필터 조건을 정의함으로써 시스템을 포함시킬 수 있습니다. 예를 들어 지정된 보안 태그가 태그 지정된 모든 시스템을 보안 그룹에 추가할 수 있습니다.

보안 태그를 설계 캔버스에 추가할 수 있습니다.

보안 정책

보안 정책은 보안 그룹에 적용할 수 있는 끝점, 방화벽 및 네트워크 검사 서비스의 집합입니다. Blueprint에서 요청 시 보안 그룹을 사용하여 보안 정책을 vSphere 가상 시스템에 추가할 수 있습니다. 보안 정책을 예약에 직접 추가할 수는 없습니다. 데이터 수집 후 계산 리소스에 대해 NSX에 정의된 보안 정책을 Blueprint에서 선택할 수 있습니다.

App 분리

App 분리를 사용하도록 설정하는 경우 개별 보안 정책이 생성됩니다. App 분리는 논리적 방화벽을 사용하여 Blueprint의 애플리케이션에 대한 모든 인바운드 및 아웃바운드 트래픽을 차단합니다. App 분리 정책을 포함하는 Blueprint에 의해 프로비저닝되는 구성 요소 시스템은 서로 통신할 수 있지만 다른 보안 그룹이 액세스를 허용하는 보안 정책과 함께 Blueprint에 추가되는 경우가 아니면 방화벽 외부에서 연결할 수 없습니다.

기존 보안 그룹 구성 요소 추가

Blueprint에서 하나 이상의 시스템 구성 요소 또는 기타 사용 가능한 구성 요소 유형에 해당 설정 연결을 준비하는 과정에서 설계 캔버스에 기존 NSX 보안 그룹 구성 요소를 추가할 수 있습니다.

기존 보안 그룹 구성 요소를 사용하여 NSX 보안 그룹을 설계 캔버스에 추가하고 vSphere 시스템 구성 요소 및 vSphere와 관련된 Software 또는 XaaS 구성 요소에 사용할 해당 설정을 구성할 수 있습니다.

설계 캔버스에 네트워크 및 보안 구성 요소를 여러 개 추가할 수 있습니다.

필수 조건

- NSX에서 보안 그룹을 생성하고 구성합니다. 자세한 내용은 vRealize Automation 구성 및 NSX 관리 가이드를 참조하십시오.
- 클러스터에 대해 NSX 인벤토리가 실행되었는지 확인합니다.
vRealize Automation에서 NSX 구성을 사용하려면 데이터 수집을 실행해야 합니다.
- 보안 구성 요소 개념을 검토합니다. [설계 캔버스에서 보안 구성 요소 사용](#) 항목을 참조하십시오.
- vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.
- **설계** 탭을 사용하여 설계 캔버스에서 새로운 Blueprint 또는 기존 Blueprint를 엽니다.

프로시저

- 1 범주 섹션에서 **네트워크 및 보안**을 클릭하여 사용 가능한 네트워크 및 보안 구성 요소 목록을 표시합니다.
- 2 **기존 보안 그룹** 구성 요소를 설계 캔버스에 끌어다 놓습니다.
- 3 **보안 그룹** 드롭다운 메뉴에서 기존 보안 그룹을 선택합니다.
- 4 **확인**을 클릭합니다.
- 5 **완료**를 클릭하여 Blueprint를 초안으로 저장하거나 계속하여 Blueprint를 구성합니다.

추가적인 보안 구성 요소를 추가하고 설계 캔버스에서 vSphere 시스템 구성 요소의 **보안** 탭에 있는 설정을 선택하면 보안 설정을 계속 구성할 수 있습니다.

요청 시 보안 그룹 구성 요소 추가

Blueprint에서 하나 이상의 vSphere 시스템 구성 요소 또는 기타 사용 가능한 구성 요소 유형에 해당 설정 연결을 준비하는 과정에서 설계 캔버스에 요청 시 NSX 보안 그룹 구성 요소를 추가할 수 있습니다.

필수 조건

- NSX에서 보안 정책을 생성 및 구성합니다. 자세한 내용은 NSX 관리 가이드를 참조하십시오.
- 클러스터에 대해 NSX 인벤토리가 실행되었는지 확인합니다.
vRealize Automation에서 NSX 구성을 사용하려면 데이터 수집을 실행해야 합니다.
- 보안 구성 요소 개념을 검토합니다. [설계 캔버스에서 보안 구성 요소 사용](#) 항목을 참조하십시오.
- vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.
- **설계** 탭을 사용하여 설계 캔버스에서 새로운 Blueprint 또는 기존 Blueprint를 엽니다.

프로시저

- 1 범주 섹션에서 **네트워크 및 보안**을 클릭하여 사용 가능한 네트워크 및 보안 구성 요소 목록을 표시합니다.
- 2 **요청 시 보안 그룹** 구성 요소를 설계 캔버스에 끌어다 놓습니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 4 하나 이상의 보안 정책을 추가합니다. **보안 정책** 영역에서 추가 아이콘을 클릭하고 사용 가능한 보안 정책을 선택하면 됩니다.
- 5 **확인**을 클릭합니다.
- 6 **완료**를 클릭하여 Blueprint를 초안으로 저장하거나 계속하여 Blueprint를 구성합니다.

추가적인 보안 구성 요소를 추가하고 설계 캔버스에서 vSphere 시스템 구성 요소의 **보안** 탭에 있는 설정을 선택하면 보안 설정을 계속 구성할 수 있습니다.

기존 보안 태그 구성 요소 추가

Blueprint에서 하나 이상의 시스템 구성 요소에 해당 설정 연결을 준비하는 과정에서 Blueprint 설계 캔버스에 NSX 보안 태그 구성 요소를 추가할 수 있습니다.

보안 태그 구성 요소를 사용하여 NSX 보안 태그를 설계 캔버스에 추가하고 vSphere와 관련된 vSphere 시스템 구성 요소 및 Software 구성 요소에 사용할 해당 설정을 구성할 수 있습니다.

설계 캔버스에 네트워크 및 보안 구성 요소를 여러 개 추가할 수 있습니다.

필수 조건

- NSX에서 보안 태그를 생성하고 구성합니다. 자세한 내용은 vRealize Automation 구성 및 NSX 관리 가이드를 참조하십시오.
- 클러스터에 대해 NSX 인벤토리가 실행되었는지 확인합니다.
vRealize Automation에서 NSX 구성을 사용하려면 데이터 수집을 실행해야 합니다.
- vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.
- **설계** 탭을 사용하여 설계 캔버스에서 새로운 Blueprint 또는 기존 Blueprint를 엽니다.

프로시저

- 1 범주 섹션에서 **네트워크 및 보안**을 클릭하여 사용 가능한 네트워크 및 보안 구성 요소 목록을 표시합니다.
- 2 **기존 보안 태그** 구성 요소를 설계 캔버스에 끌어다 놓습니다.
- 3 **보안 태그** 텍스트 상자를 클릭하고 기존 보안 태그를 선택합니다.
- 4 **확인**을 클릭합니다.
- 5 **완료**를 클릭하여 Blueprint를 초안으로 저장하거나 계속하여 Blueprint를 구성합니다.

추가적인 보안 구성 요소를 추가하고 설계 캔버스에서 vSphere 시스템 구성 요소의 **보안** 탭에 있는 설정을 선택하면 보안 설정을 계속 구성할 수 있습니다.

네트워크 및 보안 구성 요소 연결

네트워크 및 보안 구성 요소를 설계 캔버스에 끌어다 놓아 Blueprint의 시스템 구성 요소 구성에 대해 해당 설정을 사용할 수 있도록 할 수 있습니다. 시스템에 대한 네트워크 및 보안 설정을 정의한 후 로드 밸런서 구성 요소의 설정을 선택적으로 연결할 수 있습니다.

설계 캔버스에 NSX 네트워크 또는 보안 구성 요소를 추가하고 사용 가능한 설정을 정의한 후 캔버스에서 vSphere 시스템 구성 요소의 [네트워크 및 보안] 탭을 열고 해당 설정을 구성할 수 있습니다.

요청 시 NAT 네트워크 구성 요소를 끌어서 설계 캔버스에 놓고 이것을 Blueprint의 vSphere 시스템 구성 요소 또는 NSX 로드 밸런서 구성 요소와 연결할 수 있습니다.

설계 캔버스에 추가하는 네트워크 및 보안 구성 요소 설정은 NSX 구성에서 파생됩니다. 이러한 설정을 사용하려면 vSphere 클러스터의 NSX 인벤토리에 대해 데이터 수집을 실행해야 합니다. 네트워크 및 보안 구성 요소는 NSX에만 해당하며 vSphere 시스템 구성 요소와만 사용할 수 있습니다. NSX 구성에 대한 자세한 내용은 NSX 관리 가이드를 참조하십시오.

참고 Blueprint에 로드 밸런서가 하나 이상 포함되어 있고 Blueprint에 대해 App 분리가 사용되도록 설정되어 있으면 로드 밸런서 VIP가 App 분리 보안 그룹에 IPSet로 추가됩니다. 시스템 계층에 연결되어 있는 요청 시 보안 그룹이 Blueprint에 포함되어 있고, 이 시스템 계층이 로드 밸런서에도 연결되어 있는 경우, 요청 시 보안 그룹에는 로드 밸런서 VIP가 있는 IPSet와 시스템 계층이 포함됩니다.

TCP 또는 UDP 포트가 Edge(소스 포트)의 외부 IP 주소에서 NAT 네트워크 구성 요소(대상 포트)의 개인 IP 주소로 매핑되도록 NAT 규칙을 사용하는 방법에 대한 자세한 내용은 [NAT 규칙 생성 및 사용](#)을 참조하십시오.

Blueprint에서 컨테이너 구성 요소 사용

Blueprint에서 컨테이너 구성 요소를 구성하고 사용할 수 있습니다.

컨테이너 관리자가 vRealize Automation의 컨테이너에서 컨테이너 정의를 만들면 컨테이너 설계자가 설계 캔버스에서 vRealize Automation Blueprint에 대한 컨테이너 구성 요소를 추가하고 구성할 수 있습니다.

컨테이너 구성 요소 설정

vRealize Automation 설계 캔버스에서 vRealize Automation의 컨테이너 컨테이너 구성 요소에 대한 Blueprint 설정 및 옵션을 구성할 수 있습니다.

일반 탭

설계 캔버스에서 Blueprint 컨테이너 구성 요소에 대한 일반 설정을 구성합니다.

표 3-34. 일반 탭 설정

설정	설명
이름	Blueprint의 컨테이너 구성 요소에 대한 이름을 입력합니다.
설명	다른 설계자를 위해 컨테이너 구성 요소를 요약합니다.
이미지	개인 레지스트리 또는 Docker Hub 레지스트리(예: registry.hub.docker.com/library/python)와 같은 관리되는 레지스트리의 이미지 전체 이름을 입력합니다.
명령	python app.py와 같은 지정된 이미지에 적용되는 명령을 입력합니다. 해당 명령은 컨테이너 프로비저닝 프로세스가 시작되면 실행됩니다.
링크	링크는 단일 호스트에서 또는 호스트 간 컨테이너를 연결하는 다른 방법을 제공합니다. redis 또는 datadog와 같은 이 컨테이너가 연결될 서비스를 하나 이상 입력합니다.

네트워크 탭

설계 캔버스의 Blueprint 컨테이너 구성 요소에 대한 네트워크 설정을 구성합니다.

컨테이너를 네트워크에 연결할 수 있습니다. 네트워크가 설계 캔버스에서 컨테이너 네트워크 구성 요소로 나타납니다. 사용할 수 있는 네트워크에 대한 자세한 내용은 컨테이너 구성 요소 양식의 네트워크 페이지에 지정되어 있습니다.

표 3-35. 네트워크 탭 설정

설정	설명
네트워크	선택한 이미지에 대해 정의된 기존 네트워크를 지정합니다. 새 네트워크를 생성할 수도 있습니다. 설계 양식에 네트워크 컨테이너 구성 요소를 추가하는 경우 여기에 지정하는 네트워크가 선택에 대해 사용할 수 있는 옵션으로 나열됩니다.
포트 바인딩	선택한 네트워크에 대한 포트 바인딩을 지정합니다. 프로토콜 호스트, 호스트 포트 및 컨테이너 포트 구성된 바인딩을 가리킵니다.
모든 포트 게시	확인란을 선택하여 컨테이너 이미지에서 사용된 포트를 모든 사용자에게 노출합니다.
호스트 이름	컨테이너 호스트 이름을 지정합니다. 이름을 지정하지 않는 경우 값이 Blueprint의 컨테이너 구성 요소 이름 기본값으로 설정됩니다.
네트워크 모드	컨테이너의 네트워킹 스택을 지정합니다. 값을 지정하지 않는 경우 컨테이너가 브리지 네트워크 모드에서 구성됩니다.

스토리지 탭

설계 캔버스의 Blueprint 컨테이너 구성 요소에 대한 스토리지 설정을 구성합니다.

표 3-36. 스토리지 탭 설정

설정	설명
볼륨	컨테이너가 사용하도록 호스트에서 매핑된 스토리지 볼륨을 지정합니다.
상속 볼륨	다른 컨테이너에서 상속할 스토리지 볼륨을 지정합니다.
작업 디렉토리	명령을 실행할 디렉토리를 지정합니다.

정책 탭

설계 캔버스에서 Blueprint 컨테이너 구성 요소에 대한 배포 정책 및 선호도 제약 조건과 같은 정책 설정을 구성합니다.

표 3-37. 정책 탭 설정

설정	설명
배포 정책	이 컨테이너 배포에 사용할 호스트 집합에 대한 기본 설정을 설정하기 위한 배포 정책을 지정합니다. 배포 정책을 호스트, 정책과 호스트, 정책 및 컨테이너 배포 시 할될량에 대한 기본 설정을 설정하기 위한 컨테이너 정의에 연결할 수 있습니다. vRealize Automation에서 컨테이너 탭을 사용하여 배포 정책을 추가할 수 있습니다.
클러스터 크기	이 컨테이너에서 클러스터로 생성할 인스턴스 수를 지정합니다.
다시 시작 정책	종료 시 컨테이너를 다시 시작하는 방법에 대한 다시 시작 정책을 지정합니다.
최대 다시 시작	다시 시작 정책으로 [실패 시]를 선택한 경우 다시 시도 최대 횟수를 지정할 수 있습니다.
CPU 공유	프로비저닝된 리소스에 대해 할당된 CPU 공유 수를 지정합니다.
메모리 제한	0과 배치 영역에서 사용할 수 있는 메모리 간 숫자를 지정합니다. 이 배치의 리소스에 대해 사용할 수 있는 전체 메모리입니다. 0은 제한이 없음을 의미합니다.
메모리 스왑	총 메모리 제한입니다.
선호도 제약 조건	<p>동일한 호스트 또는 다른 호스트의 컨테이너 프로비저닝에 대한 규칙을 정의합니다.</p> <ul style="list-style-type: none"> ■ 선호도 유형 <p>반선호도의 경우 컨테이너가 다른 호스트에 배치되어 있지 않으면 동일한 호스트에 배치되어 있습니다.</p> ■ 서비스 <p>일반 탭의 이름 필드에 지정된 컨테이너 구성 요소 이름과 일치하는 드롭다운 메뉴에서 사용할 수 있는 서비스 이름입니다.</p> ■ 제약 조건 <p>강한 제약 조건은 제약 조건이 충족되지 않는 경우 프로비저닝이 실패하도록 지정합니다. 약한 제약 조건은 제약 조건이 충족되지 않는 경우 프로비저닝을 계속하도록 지정합니다.</p>

환경 탭

설계 캔버스의 Blueprint 컨테이너 구성 요소에 대한 속성 바인딩과 같은 환경 설정을 구성합니다.

표 3-38. 환경 탭 설정

설정	설명
이름	변수 이름입니다.
바인딩	템플릿의 일부인 다른 속성에 변수를 바인딩합니다. 바인딩을 선택할 경우 _resource~TemplateComponent~TemplateComponentProperty 구문에 값을 입력해야 합니다.
값	환경 변수의 값 또는 바인딩을 선택한 경우, 바인딩할 속성의 값입니다.

속성 탭

설계 캔버스의 Blueprint 컨테이너 구성 요소에 대한 개별 및 그룹 사용자 지정 속성을 구성합니다.

속성 그룹 탭을 선택하고 **추가**를 클릭하면 다음 옵션을 사용할 수 있습니다.

- 인증서 인증이 있는 컨테이너 호스트 속성
- 사용자/암호 인증이 있는 컨테이너 호스트 속성

추가 속성 그룹이 정의된 경우 해당 속성 그룹도 나열됩니다.

사용자 지정 속성 탭을 선택하고 **추가**를 클릭하면 컨테이너 구성 요소에 개별 사용자 지정 속성을 추가할 수 있습니다.

표 3-39. 사용자 지정 속성을 위한 속성 탭 설정

설정	설명
이름	사용자 지정 속성의 이름을 입력하거나, 사용 가능한 사용자 지정 속성을 드롭다운 메뉴에서 선택합니다.
값	사용자 지정 속성 이름에 연결할 값을 입력하거나 편집합니다.
암호화됨	예를 들어 값이 암호인 경우 속성 값을 암호화하도록 선택할 수 있습니다.
재정의 가능	속성 값을 속성을 사용하는 다음 사람 또는 나중 사람이 재정의할 수 있도록 지정할 수 있습니다. 일반적으로 이는 다른 설계자이지만 [요청에서 표시]를 선택하는 경우 비즈니스 사용자가 카탈로그 항목을 요청할 때 속성 값을 보고 편집할 수 있습니다.
요청에서 표시	최종 사용자에게 속성 이름 및 값을 표시하려는 경우 시스템 프로비저닝을 요청할 때 요청 양식에 속성을 표시하도록 선택할 수 있습니다. 사용자가 값을 제공하길 원하는 경우 재정의 가능성 도 선택해야 합니다.

상태 구성 탭

설계 캔버스의 Blueprint 컨테이너 구성 요소에 대한 상태 구성 모드를 지정합니다.

표 3-40. 상태 구성 탭 설정

모드 설정	설명
없음	기본값. 상태 점검이 구성되지 않습니다.
HTTP	<p>HTTP를 선택하는 경우 액세스할 API, 사용할 HTTP 방법 및 버전을 입력해야 합니다. API는 상대적이며 컨테이너의 주소를 입력할 필요가 없습니다. 작업에 대한 시간 초과 기간을 지정하고 상태 임계값을 설정할 수도 있습니다.</p> <p>예를 들어 정상 상태 임계값 2는 컨테이너가 정상이고 실행 중 상태로 간주되려면 연속 호출 성공이 2회 발생해야 한다는 것을 의미합니다. 비정상 상태 임계값 2는 컨테이너가 비정상이고 오류 상태로 간주되려면 호출 실패가 2회 발생해야 한다는 것을 의미합니다. 정상 상태 및 비정상 상태 임계값 사이의 모든 상태의 경우 컨테이너 상태는 저하됩니다.</p>
TCP 연결	<p>TCP 연결을 선택하는 경우 컨테이너에 대한 포트만 입력해야 합니다. 상태 점검이 제공된 포트에서 컨테이너와의 TCP 연결 설정을 시도합니다. 작업에 대한 시간 초과 값을 지정하고 HTTP로 정상 또는 비정상 상태 임계값을 설정할 수도 있습니다.</p>
명령	<p>명령을 선택하는 경우 컨테이너에서 실행될 명령을 입력해야 합니다. 상태 점검 성공 여부는 명령 종료 상태로 결정됩니다.</p>
프로비저닝 시 상태 점검 무시	<p>프로비저닝 시 상태 점검을 강제하려면 이 옵션을 선택 취소합니다. 강제하면 하나의 성공적인 상태 점검이 통과될 때까지 컨테이너가 프로비저닝된 것으로 고려되지 않습니다.</p>
자동 배포	<p>컨테이너가 오류 상태일 때 컨테이너를 자동으로 다시 배포합니다.</p>

로그 구성 탭

설계 캔버스의 Blueprint 컨테이너 구성 요소에 대한 로깅 모드 및 로깅 옵션 선택 사항을 지정합니다.

표 3-41. 로그 구성 탭 설정

설정	설명
드라이버	드롭다운 메뉴에서 로깅 형식을 선택합니다.
옵션	로깅 형식을 준수하는 이름 및 값 형식을 사용하여 드라이버 옵션을 입력합니다.

Blueprint의 컨테이너 속성 및 속성 그룹 사용

미리 정의된 속성 그룹을 vRealize Automation Blueprint의 컨테이너 구성 요소에 추가할 수 있습니다. 이러한 속성이 포함된 Blueprint를 사용하여 프로비저닝한 시스템은 Docker Container 호스트 시스템으로 등록됩니다.

vRealize Automation의 컨테이너에서는 컨테이너 관련 사용자 지정 속성으로 구성된 다음과 같은 두 가지 속성 그룹을 제공합니다. Blueprint에 컨테이너 구성 요소를 추가하는 경우 이러한 속성 그룹을 컨테이너에 추가하여 프로비저닝된 시스템을 컨테이너 호스트로 등록할 수 있습니다.

- 인증서 인증이 있는 컨테이너 호스트 속성

■ 사용자/암호 인증이 있는 컨테이너 호스트 속성

이러한 속성 그룹은 vRealize Automation에서 **관리 > 속성 사전 > 속성 그룹**을 선택하면 표시됩니다.

모든 테넌트에서 속성 그룹을 공유하기 때문에 다중 테넌트 환경에서 작업하는 경우에는 속성을 복제 및 사용자 지정하는 것을 고려하십시오. 속성 그룹 및 그룹의 속성에 고유한 이름을 지정하면 이를 편집하여 특정 테넌트에서 사용하도록 사용자 지정 값을 정의할 수 있습니다.

가장 일반적으로 사용되는 속성은 컨테이너 관리자가 컨테이너 호스트를 통한 인증에 사용할 클라이언트 인증서를 제공하는 `Container.Auth.PublicKey` 및 `Container.Auth.PrivateKey`입니다.

표 3-42. 컨테이너 사용자 지정 속성

속성	설명
<code>containers.ipam.driver</code>	컨테이너에만 사용할 수 있습니다. Blueprint에 컨테이너 네트워크 구성 요소를 추가할 때 사용될 IPAM 드라이버를 지정합니다. 지원되는 값은 드라이버가 사용되는 컨테이너 호스트 환경에 설치된 드라이버에 따라 다릅니다. 예를 들어 지원되는 값은 컨테이너 호스트에 설치된 IPAM 플러그인에 따라 <code>infoblox</code> 또는 <code>calico</code> 일 수 있습니다.
<code>containers.network.driver</code>	컨테이너에만 사용할 수 있습니다. Blueprint에 컨테이너 네트워크 구성 요소를 추가할 때 사용될 네트워크 드라이버를 지정합니다. 지원되는 값은 드라이버가 사용되는 컨테이너 호스트 환경에 설치된 드라이버에 따라 다릅니다. 기본적으로 VCH(가상 컨테이너 호스트) 제공 네트워크 드라이버에는 브리지 드라이버가 포함되는 반면 Docker 제공 네트워크 드라이버에는 브리지, 오버레이 및 <code>macvlan</code> 이 포함됩니다. 컨테이너 호스트에 설치되어 있는 네트워크 플러그인에 따라 <code>weave</code> 및 <code>calico</code> 와 같은 타사 네트워크 드라이버도 사용할 수 있습니다.
<code>Container</code>	컨테이너에만 사용할 수 있습니다. 기본값은 <code>App.Docker</code> 이며 필수입니다. 이 속성을 수정하지 마십시오.
<code>Container.Auth.User</code>	컨테이너에만 사용할 수 있습니다. 컨테이너 호스트에 연결하기 위한 사용자 이름을 지정합니다.
<code>Container.Auth.Password</code>	컨테이너에만 사용할 수 있습니다. 사용될 사용자 이름에 대한 암호나 공용 또는 개인 키 암호를 지정합니다. 암호화된 속성 값이 지원됩니다.
<code>Container.Auth.PublicKey</code>	컨테이너에만 사용할 수 있습니다. 컨테이너 호스트에 연결하기 위한 공용 키를 지정합니다.
<code>Container.Auth.PrivateKey</code>	컨테이너에만 사용할 수 있습니다. 컨테이너 호스트에 연결하기 위한 개인 키를 지정합니다. 암호화된 속성 값이 지원됩니다.
<code>Container.Connection.Protocol</code>	컨테이너에만 사용할 수 있습니다. 통신 프로토콜을 지정합니다. 기본값은 <code>API</code> 이며 필수입니다. 이 속성을 수정하지 마십시오.
<code>Container.Connection.Scheme</code>	컨테이너에만 사용할 수 있습니다. 통신 체계를 지정합니다. 기본값은 <code>https</code> 입니다.
<code>Container.Connection.Port</code>	컨테이너에만 사용할 수 있습니다. 컨테이너 연결 포트를 지정합니다. 기본값은 <code>2376</code> 입니다.

표 3-42. 컨테이너 사용자 지정 속성 (계속)

속성	설명
Extensibility.Lifecycle.Properties.VMPSMasterWorkflow32.MachineActivated	컨테이너에만 사용할 수 있습니다. 모든 컨테이너 속성을 노출하고 프로비저닝된 호스트를 등록하는 데 사용되는 이벤트 브로커 속성을 지정합니다. 기본값은 Container*이며 필수입니다. 이 속성을 수정하지 마십시오.
Extensibility.Lifecycle.Properties.VMPSMasterWorkflow32.Disposing	컨테이너에만 사용할 수 있습니다. 위의 모든 컨테이너 속성을 노출하고 프로비저닝된 호스트를 등록 해제하는 데 사용되는 이벤트 브로커 속성을 지정합니다. 기본값은 Container*이며 필수입니다. 이 속성을 수정하지 마십시오.

설계 캔버스에서 컨테이너 네트워크 구성 요소 사용

컨테이너 네트워크 구성 요소 하나 이상을 설계 캔버스에 추가하고 Blueprint의 vSphere 시스템 구성 요소에 대한 해당 구성 요소의 설정을 구성할 수 있습니다.

컨테이너 구성 요소를 Blueprint에 추가하는 경우 containers.ipam.driver 및 containers.network.driver를 구성 요소에 추가할 수 있습니다.

컨테이너 네트워크 구성 요소 추가

컨테이너 구성 요소를 포함한 vRealize Automation Blueprint에 컨테이너 네트워크 정보를 추가할 수 있습니다.

vRealize Automation **컨테이너** 탭을 사용하여 vRealize Automation의 컨테이너에 컨테이너를 구성할 수 있습니다. vRealize Automation **설계** 탭의 옵션을 사용하여 이런 컨테이너와 그 네트워크 설정을 Blueprint의 구성 요소로 추가할 수 있습니다.

필수 조건

- **컨테이너 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- **설계** 탭을 사용하여 설계 캔버스에서 새로운 Blueprint 또는 기존 Blueprint를 엽니다.

프로시저

- 1 범주 섹션에서 **네트워크 및 보안**을 클릭하여 사용 가능한 네트워크 및 보안 구성 요소 목록을 표시합니다.
- 2 **컨테이너 네트워크** 구성 요소를 설계 캔버스에 끌어다 놓습니다.
- 3 **이름** 텍스트 상자에 이름을 입력하여 설계 캔버스에서 구성 요소에 고유한 레이블을 지정합니다.
- 4 (선택 사항) **설명** 텍스트 상자에 구성 요소 설명을 입력합니다.
- 5 (선택 사항) 외부 IPAM 설정을 지정하지 않으려면 **외부** 확인란을 선택합니다.
외부 확인란을 선택하면 **IPAM 구성** 탭이 제거됩니다.

- 6 IPAM 구성** 탭을 클릭하여 Blueprin의 컨테이너 구성 요소에 지정된 네트워크에 대한 서브넷, IP 범위 및 게이트웨이를 새로 지정하거나 기존 설정을 편집합니다.

IPAM 구성은 Docker나 지원되는 다른 컨테이너 애플리케이션에서 이전에 생성된 것들과는 반대로 vRealize Automation에 의해 생성되는 새 네트워크에 적용됩니다. 이런 설정은 유효성 검사되지 않고 설정이 다른 네트워크와 겹칠 경우 프로비저닝이 실패합니다. 예를 들어, 서브넷과 게이트웨이는 컨테이너 호스트 내에서 고유해야 합니다.

- 7 속성** 탭을 클릭하여 구성 요소에 대한 사용자 지정 속성을 지정합니다.

속성 그룹 탭을 선택하고 **추가**를 클릭하면 다음 옵션을 사용할 수 있습니다.

- 인증서 인증이 있는 컨테이너 호스트 속성
- 사용자/암호 인증이 있는 컨테이너 호스트 속성

추가 속성 그룹이 정의된 경우 해당 속성 그룹도 나열됩니다.

사용자 지정 속성 탭을 선택하고 **추가**를 클릭하면 컨테이너 구성 요소에 개별 사용자 지정 속성을 추가할 수 있습니다.

표 3-43. 사용자 지정 속성을 위한 속성 탭 설정

설정	설명
이름	사용자 지정 속성의 이름을 입력하거나, 사용 가능한 사용자 지정 속성을 드롭다운 메뉴에서 선택합니다.
값	사용자 지정 속성 이름에 연결할 값을 입력하거나 편집합니다.
암호화됨	예를 들어 값이 암호인 경우 속성 값을 암호화하도록 선택할 수 있습니다.
재정의 가능	속성 값을 속성을 사용하는 다음 사람 또는 나중 사람이 재정의할 수 있도록 지정할 수 있습니다. 일반적으로 이는 다른 설계자이지만 [요청에서 표시]를 선택하는 경우 비즈니스 사용자가 카탈로그 항목을 요청할 때 속성 값을 보고 편집할 수 있습니다.
요청에서 표시	최종 사용자에게 속성 이름 및 값을 표시하려는 경우 시스템 프로비저닝을 요청할 때 요청 양식에 속성을 표시하도록 선택할 수 있습니다. 사용자가 값을 제공하길 원하는 경우 재정의 가능 도 선택해야 합니다.

- 8 완료**를 클릭하여 Blueprint를 초안으로 저장하거나 계속하여 Blueprint를 구성합니다.

후속 작업

설계 캔버스에서 컨테이너 구성 요소의 **네트워크** 탭에서 컨테이너 네트워크 설정을 계속 구성할 수 있습니다.

Blueprint에서 사용을 위해 컨테이너 템플릿 푸시

컨테이너 템플릿을 vRealize Automation Blueprint에서 사용할 수 있도록 만들 수 있습니다.

컨테이너 템플릿은 여러 컨테이너를 포함할 수 있습니다. 다중 컨테이너 템플릿을 vRealize Automation에 푸시하면 템플릿이 vRealize Automation에 다중 구성 요소 Blueprint로 생성됩니다.

컨테이너 템플릿에 추가하는 컨테이너별 속성은 vRealize Automation Blueprint에서 인식됩니다. [Blueprint의 컨테이너 속성 및 속성 그룹 사용](#) 항목을 참조하십시오.

vRealize Automation 카탈로그에 게시된 Blueprint를 프로비저닝하도록 요청하면 해당 Blueprint에 대한 소스 컨테이너 애플리케이션이 프로비저닝됩니다.

vRealize Automation Blueprint에는 다음 구성 요소 유형을 비롯한 기타 구성 요소를 추가할 수 있습니다.

- 시스템 유형
- 소프트웨어 구성 요소
- 기타 Blueprint
- NSX 네트워크 및 보안 구성 요소
- XaaS 구성 요소
- 사용자 지정 구성 요소

컨테이너에서 vRealize Automation으로 템플릿을 푸시할 수 있습니다. vRealize Automation Blueprint에 변경하는 내용은 컨테이너 템플릿에 영향을 미치지 않습니다.

컨테이너 템플릿에 이후 변경 내용을 적용하고 vRealize Automation에서 Blueprint를 덮어쓰도록 다시 푸시합니다. 템플릿을 vRealize Automation에 푸시하면 Blueprint를 덮어쓰고 푸시 사이에 vRealize Automation에서 Blueprint에 변경한 내용은 손실됩니다. Blueprint 변경 내용이 손실되는 것을 방지하려면 vRealize CloudClient를 사용하여 새 Blueprint를 복제하거나 Blueprint를 내보냅니다.

Blueprint에서 Docker Container 또는 호스트 프로비저닝

vRealize Automation Blueprint를 생성하여 등록된 Docker Container 호스트로 시스템을 프로비저닝하는 데 사용할 수 있습니다.

프로비저닝된 시스템을 컨테이너 호스트로 등록하려면 다음 요구 사항을 충족해야 합니다.

- 시스템이 컨테이너별 사용자 지정 속성을 포함하는 Blueprint에 의해 프로비저닝됩니다.

컨테이너별 필수 사용자 지정 속성은 두 개의 속성 그룹으로 제공됩니다. [Blueprint의 컨테이너 속성 및 속성 그룹 사용](#) 항목을 참조하십시오.

vRealize Automation의 사용자 지정 속성 및 속성 그룹 사용에 대한 자세한 내용은 사용자 지정 속성 참조 자료 항목을 참조하십시오.

- 시스템은 네트워크를 통해 액세스할 수 있습니다.

예를 들어 시스템에 유효한 IP 주소가 있어야 하고 전원이 켜져 있어야 합니다.

Blueprint를 사용하여 프로비저닝될 때 시스템을 컨테이너 호스트로 지정하는 특정 사용자 지정 속성을 포함하도록 vRealize Automation Blueprint를 정의할 수 있습니다.

필수 Blueprint 속성이 있는 시스템이 성공적으로 프로비저닝되면 컨테이너에 등록되고 vRealize Automation으로부터 이벤트 및 작업을 수신합니다.

Microsoft Azure Blueprint 및 통합 리소스 작업 생성

클라우드 또는 패브릭 관리자로서 비즈니스 그룹 관리자가 소비자를 위한 사용자 지정 프로비저닝된 시스템을 생성하기 위해 빌드 블록으로 사용하는 Microsoft Azure 가상 시스템 Blueprint를 생성할 수 있습니다. DevOps 관리자도 Azure 시스템 Blueprint를 생성하거나 복합 Blueprint 생성 시 기존 Azure 시스템 Blueprint를 사용할 수 있습니다.

■ Microsoft Azure용 Blueprint 생성

Azure 가상 시스템 리소스에 대한 액세스를 제공하는 Microsoft Azure 가상 시스템 Blueprint를 생성할 수 있습니다.

■ Azure 사용자 지정 리소스 작업 생성

사용자 지정 리소스 작업을 생성 및 사용하여 Azure 가상 시스템을 제어할 수 있습니다.

Microsoft Azure용 Blueprint 생성

Azure 가상 시스템 리소스에 대한 액세스를 제공하는 Microsoft Azure 가상 시스템 Blueprint를 생성할 수 있습니다.

기본 Azure 시스템 템플릿이 vRealize Automation Blueprint 편집 페이지의 **시스템 유형** 범주에 표시됩니다. 이 가상 시스템 템플릿은 다음 절차에 설명된 대로 Azure Blueprint의 기반으로 사용할 수 있습니다. Azure Blueprint를 생성한 후에는 설계된 대로 게시하고 배포하거나 사용자 지정 Azure 리소스 또는 다른 Blueprint와 함께 사용하여 복합 Blueprint를 생성할 수 있습니다.

Blueprint를 생성 및 게시한 후 적절한 권한이 있는 사용자는 vRealize Automation 서비스 카탈로그를 통해 Azure 인스턴스를 요청하고 프로비저닝할 수 있습니다.

Azure Blueprint는 가상 시스템 요구 사항을 정의합니다. vRealize Automation에서는 이러한 요구 사항을 사용하여 배포에 가장 적절한 예약을 선택합니다.

[새 Blueprint] 대화상자의 [NSX 설정] 및 [속성] 탭에 대한 자세한 내용은 vRealize Automation 구성 항목을 참조하십시오.

단일 배포로 두 개의 가상 시스템을 동시에 생성하려면 각각 두 개의 네트워크 인터페이스 이름과 가상 시스템 이름을 생성해야 합니다.

필수 조건

- Blueprint 생성에 필요할 수 있는 유효한 Azure 구독 ID 및 관련 정보(리소스 그룹, 스토리지 계정 및 가상 네트워크 정보 등)를 확보합니다.
- vRealize Automation 배포에 사용하기 위한 Azure에 대한 연결을 생성하도록 Azure 끝점을 구성합니다.
- 비즈니스 그룹에 맞게 Azure 예약을 구성합니다.

프로시저

- 1 설계 > **Blueprint**를 선택합니다.
- 2 새로 만들기 아이콘(+)을 클릭합니다.
- 3 이름 텍스트 상자에 Blueprint 이름을 입력합니다.

이름을 입력하면 ID 텍스트 상자도 채워집니다. 대부분의 경우 **NSX 설정** 및 **속성** 탭을 무시할 수 있습니다.

- 4 **확인**을 클릭합니다.
- 5 [범주] 메뉴에서 **시스템 유형**을 클릭합니다.
- 6 **Azure 시스템** 가상 시스템 템플릿을 설계 캔버스로 끕니다.

사용자 지정 Azure 리소스를 Blueprint의 기반으로 사용하기 위해 생성해둔 경우에는 범주 목록의 할당된 범주에서 해당 리소스를 선택할 수 있습니다.

- 7 Azure 시스템 템플릿을 설계 캔버스로 끌어 놓을 때 표시되는 설계 캔버스의 하반부에서 탭 페이지의 텍스트 상자에 Azure 가상 시스템에 필요한 정보를 입력합니다.

이러한 모든 탭의 텍스트 상자 및 기타 매개 변수에서 사용할 수 있는 선택 항목은 Blueprint의 기반으로 구성된 Azure 끝점에 의해 주로 결정됩니다.

대부분의 매개 변수는 매개 변수 이름 옆에 있는 텍스트 상자를 클릭하면 페이지 오른쪽에 새 창이 열립니다. 이 창에서 **값** 텍스트 상자에 매개 변수 값을 입력하고 이 값이 **필수**인지 여부를 나타낼 수 있습니다. 경우에 따라서는 **최소값** 및 **최대값**을 입력할 수도 있습니다. 오른쪽 창에서 **적용**을 클릭하여 초기 텍스트 상자를 채웁니다.

그림 3-1. Azure Blueprint 오른쪽 메뉴

The screenshot shows the 'Storage' tab of the 'Azure_Machine_1' configuration. The 'Resource Group' section has two radio buttons: 'Create New' and 'Use Existing'. The 'Resource Group Name' is 'RG1-vAficionado'. The 'Availability Set' section has three radio buttons: 'None', 'Create New', and 'Use Existing'. A red arrow points from the 'Value' field in the 'Required' dropdown to the 'Value' field in the 'Resource Group Name' field.

대부분의 매개 변수에는 **고급 옵션** 버튼도 있습니다. 이러한 옵션을 사용하여 매개 변수 길이를 지정하고 최종 사용자로부터 매개 변수를 숨길 수도 있습니다.

참고 Blueprint 구성을 계속하려면 각 탭에서 필수 매개 변수를 채워야 합니다. 필드를 비워두려면 저장하기 전에 뒤로 돌아가서 입력 내용을 삭제합니다.

탭	설명	중요 매개 변수
일반	사용할 끝점과 같은 Azure 가상 시스템에 대한 기본 연결 정보를 선택합니다.	<p>ID - 생성 중인 Azure 가상 시스템을 나타냅니다. 이 이름을 변경하면 설계 캔버스에 있는 Azure 가상 시스템 이미지도 자동으로 업데이트됩니다.</p> <p>설명 - 생성 중인 가상 시스템을 나타내고 그 시스템이 필수인지 여부도 나타냅니다.</p> <p>인스턴스 - 이 선택 항목에서는 확장/축소 가능한 가상 시스템을 생성할 수 있습니다. 최소 및 최대 필드를 사용하여 이 시스템으로 부터 생성될 수 있는 Azure 인스턴스 수를 나타냅니다.</p> <p>암호 인증 사용: 암호 인증을 사용하려면 [예]를 선택하고 SSH를 사용하려면 [아니요]를 선택합니다.</p> <p>관리자 사용자 이름 - 이 필드는 비워 둡니다. 시스템을 프로비저닝하는 사용자가 할당할 수 있습니다.</p> <p>Admin 암호 - 이 필드는 비워 둡니다. 시스템을 프로비저닝하는 개인이 적절한 암호를 제공할 수 있습니다.</p>
빌드 정보	생성 중인 가상 시스템에 대한 정보를 구성할 수 있습니다.	<p>위치 - 이 가상 시스템이 배포될 지리적 위치를 선택합니다.</p> <p>시스템 접두사 - 연결된 비즈니스 그룹의 시스템 접두사를 사용할지 또는 사용자 지정 접두사를 생성할지 여부를 나타내도록 적절한 라디오 버튼을 선택합니다. 사용자 지정 접두사를 사용하려면 사용자 지정 시스템 접두사 텍스트 상자에 사용자 지정 접두사를 입력합니다.</p> <p>가상 시스템 이미지 유형 - 사용자 지정 또는 보관 가상 시스템 이미지 중에 적절한 라디오 버튼을 선택합니다. 사용자 지정 가상 시스템이 Azure 클래식 배포로부터 생성되고 클라우드 서비스, 스토리지 계정 및 가용성 집합과 관련하여 더 많은 구성 옵션이 제공됩니다.</p> <p>가상 시스템 이미지 - Blueprint의 기반으로 사용할 Azure 가상 시스템 이미지를 나타냅니다.</p> <ul style="list-style-type: none"> ■ 보관 가상 시스템 이미지의 경우 시스템 이미지 URN이 (게시자):(제공):(sku):(버전) 형식을 충족해야 합니다. ■ 사용자 지정 가상 시스템 이미지의 경우 시스템 이미지 URN이 다음 형식을 충족해야 합니다. <p><code>https://storageaccount.blob.core.windows.net/container/image.vhd</code></p> <p>사용자 지정 이미지의 경우 [운영 체제 이미지 유형(Windows 또는 Linux)] 텍스트 상자도 완료해야 합니다.</p> <p>관리자 - 이 Blueprint를 기반으로 가상 시스템에 구성되어 있는 지정된 관리자의 이름을 입력합니다. 또는 여기에서 비워두고 요청 양식에서 입력할 수 있습니다.</p> <p>인증 - 이 Blueprint를 기반으로 하는 가상 시스템에 암호가 필요한지 또는 SSH 인증이 필요한지를 나타내도록 적절한 라디오 버튼을 선택합니다.</p> <p>Admin 암호 - 가상 시스템 인스턴스에 대한 관리자 암호입니다.</p> <p>시리즈 - 가상 시스템 인스턴스의 일반 크기를 정의합니다. 시리즈 정보는 Azure 설명서(https://azure.microsoft.com/ko-kr/documentation/articles/virtual-machines-windows-sizes/)를 참조하십시오.</p>

탭	설명	중요 매개 변수
		<p>크기 - 시리즈에 포함된 구체적인 가상 시스템 인스턴스 크기를 정의합니다. [크기]는 선택된 시리즈와 관련되어 있습니다. Azure 인스턴스에 대한 유효한 연결이 있는 경우 사용 가능한 크기는 구독 및 선택된 위치 및 시리즈를 기반으로 동적으로 채워집니다. 크기 정보는 Azure 설명서를 참조하십시오.</p> <p>인스턴스 크기 세부 정보 - 가상 시스템 인스턴스 시리즈 및 크기에 대한 선택적인 정보입니다.</p>
시스템 리소스	<p>버킷에 가상 시스템 리소스를 구성합니다. 리소스 그룹은 웹사이트, 계정, 데이터베이스, 네트워크와 같은 가상 시스템 리소스를 그룹화하는 조직적 구성체입니다.</p> <p>가용성 설정은 이중화 지원을 위해 둘 이상의 가상 시스템을 관리하기 위한 메커니즘입니다. Azure 가용성 설정에 대한 자세한 내용은 https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-manage-availability/ 항목을 참조하십시오.</p> <p>참고 Azure 인스턴스의 최대 수가 1보다 큰 값으로 설정된 상태에서 Blueprint를 구성하는 경우에는 리소스 그룹 및 가용성 집합을 새로 생성하기 보다는 기존 리소스 그룹 및 가용성 집합을 사용하는 것이 좋습니다. 동일한 배포에 포함된 둘 이상의 인스턴스에서 새 리소스 그룹 또는 새 가용성 집합을 사용하는 경우 로드 밸런서와 연결되면 오류 및 기타 문제가 발생하게 됩니다.</p>	<p>리소스 그룹 생성 또는 재사용: - 기존 Azure 리소스 그룹을 사용할지 또는 새 리소스 그룹을 생성할지를 나타내는 적절한 라디오 버튼을 선택합니다. 기존 리소스 그룹의 이름은 Azure 포털의 리소스 그룹 페이지에서 찾을 수 있습니다. 새 리소스 그룹을 생성하도록 선택하면 새 그룹에 적합한 이름이 리소스 그룹 텍스트 상자에 자동으로 표시됩니다.</p> <p>가용성 집합 생성 또는 재사용: 원하는 작업의 내용에 따라 적절한 라디오 버튼을 선택합니다. [새로 생성]을 선택하면 새 가용성 집합 정보에 적합한 정보가 텍스트 상자에 표시됩니다.</p>

탭	설명	중요 매개 변수
스토리지	<p>Azure 스토리지 계정을 구성할 수 있습니다. 스토리지 계정은 Azure Blob, 대기열 테이블, 파일 스토리지 등 서로 다른 유형의 Azure 스토리지에 대한 액세스를 제공합니다. 대부분의 Blueprint에 대해 기본값을 그대로 사용할 수 있습니다.</p>	<p>스토리지 계정 - 해당하는 경우 가상 시스템에 대한 스토리지 계정 이름을 입력합니다. Azure 가상 시스템 운영 체제 디스크가 이 스토리지 계정에 배포됩니다. Azure 포털에서 스토리지 그룹 정보를 찾을 수 있습니다. 스토리지 계정은 하나 이상 가질 수 있습니다.</p> <p>참고 스토리지 계정 이름에 밑줄 또는 기타 특수 문자가 포함된 경우 오류가 발생할 수 있습니다.</p> <p>진단 스토리지 추가 - Azure 인스턴스에 진단 데이터를 사용하는 경우 이 확인란을 선택합니다.</p> <p>스토리지 디스크 수 - 가상 시스템에 사용하기에 적절한 데이터 스토리지 디스크 수를 선택합니다. 디스크는 최대 4개까지 지정할 수 있습니다. 이 디스크는 스토리지 계정 텍스트 상자에 지정된 운영 체제 디스크 외에 추가적인 디스크입니다.</p> <p>스토리지 디스크 #</p> <ul style="list-style-type: none"> ■ 디스크 이름 - 디스크에 할당된 이름을 나타냅니다. ■ 디스크 유형 - 스토리지 디바이스 유형입니다. ■ 디스크 크기 - 스토리지 크기입니다. ■ 복제 - 디스크 백업에 사용되는 복제 방법입니다. ■ 호스트 캐시 - 성능을 높이기 위해 읽기/쓰기를 캐시할지 여부를 나타냅니다.
네트워크	<p>가상 시스템 Blueprint에 대한 네트워킹을 선택할 수 있습니다. 대부분의 Blueprint에 대해 기본값을 그대로 사용할 수 있으며 배포 중에 소비자가 적절한 네트워크 정보를 입력하게 됩니다.</p> <p>참고 인터페이스당 가상 시스템을 하나만 생성할 수 있지만 각 가상 시스템은 인터페이스를 최대 4개까지 가질 수 있습니다.</p>	<p>페이지에서 테이블을 클릭하면 다음 필드와 함께 편집할 수 있는 다른 테이블이 포함된 대화상자가 오른쪽에 열립니다.</p> <ul style="list-style-type: none"> ■ 로드 밸런서 이름 - Azure 인스턴스에 사용되는 로드 밸런서입니다. ■ 네트워크 인터페이스 수 - Azure 인스턴스에 사용되는 네트워크 인터페이스 수를 선택합니다. 네트워크 인터페이스 수는 [스토리지] 탭에 선택되어 있는 가상 시스템 크기에서 지원되어야 합니다. ■ 네트워크 인터페이스 - 가상 시스템 Blueprint에 적합한 네트워크 인터페이스를 선택합니다. 기존 네트워크를 입력하는 경우 기타 네트워크 탭을 모두 무시할 수 있습니다. 존재하지 않는 네트워크 인터페이스 이름을 입력하면 해당 이름으로 새 인터페이스가 생성되고 다른 네트워크 탭을 사용하여 인터페이스를 구성할 수 있습니다. ■ NIC 이름 접두사 - 네트워크 인터페이스 카드의 접두사입니다. ■ IP 주소 유형 - 가상 시스템이 정적 IP 주소를 사용하는지 또는 동적 IP 주소를 사용하는지 나타냅니다. ■ 네트워킹 구성 - 적절한 네트워킹 구성을 입력합니다. 네트워크 프로파일이 지원됩니다. Azure 네트워크 지정 및 네트워크 프로파일 사용이라는 두 가지 옵션이 있으며 이후 필드는 선택하는 옵션에 따라 변경됩니다. <ul style="list-style-type: none"> ■ Azure 네트워크 지정을 선택하면 다음 옵션을 사용할 수 있습니다. 이 텍스트 상자를 비워두면 해당되는 예약에 지정된 정보를 기반으로 기본 네트워크 구성체가 사용됩니다. <ul style="list-style-type: none"> ■ vNet 이름 - 가상 네트워크의 이름입니다.

탭	설명	중요 매개 변수
		<ul style="list-style-type: none"> ■ 서브넷 이름 - Azure 서브넷의 도메인 이름입니다.
		<p>참고 2일차 작업 동안 Azure에 대해 공용 IP 주소를 설정할 수 있습니다.</p>
		<ul style="list-style-type: none"> ■ 네트워크 프로파일 사용을 선택하면 네트워크 구성이 기본 Azure 구성체로부터 분리되고 대신 vRealize Automation 네트워킹 프로파일과 한 쌍으로 연결됩니다. ■ 네트워크 프로파일 텍스트 상자를 비워두면 기본 Azure vNet 및 서브넷 쌍은 네트워크 프로파일이 지정되어 있는 해당 예약을 기반으로 확인됩니다. ■ 네트워크 프로파일을 입력하면 Azure vNet 및 서브넷은 일치하는 예약을 기반으로 확인됩니다.

8 완료 버튼을 클릭하여 Blueprint 구성을 저장하고 기본 Blueprint 페이지로 돌아갑니다.

후속 작업

VPN 터널을 지원하기 위해 Azure 예약에서 사용자 지정 속성을 구성한 경우 Azure Blueprint에 소프트웨어 구성 요소를 추가할 수 있습니다.

- 1 범주 메뉴에서 **소프트웨어 구성 요소**를 선택합니다. Azure Blueprint에 구성된 소프트웨어 구성 요소가 아래 창에 나타납니다.
- 2 컨테이너 드롭다운 값에서 [Azure 가상 시스템]을 선택합니다.
- 3 원하는 소프트웨어 구성 요소를 선택하고 끌어서 설계 캔버스의 Azure 가상 시스템에 놓습니다.
- 4 소프트웨어 구성 요소에 필요한 속성이 있는 경우 설계 캔버스 아래의 해당하는 매개 변수 텍스트 상자에 입력합니다.
- 5 **저장**을 클릭합니다.

Blueprint를 게시하려면 기본 Blueprint 페이지에서 Blueprint를 선택하고 **게시**를 클릭합니다. 게시된 Blueprint는 [카탈로그 항목] 페이지에서 사용할 수 있습니다. 또한 비즈니스 그룹 관리자 또는 이에 상응하는 담당자는 게시된 Blueprint를 복합 Blueprint의 기반으로 사용할 수 있습니다.

Azure 사용자 지정 리소스 작업 생성

사용자 지정 리소스 작업을 생성 및 사용하여 Azure 가상 시스템을 제어할 수 있습니다.

vRealize Automation Azure 구현에는 기본적으로 두 개의 사용자 지정 리소스 작업이 제공됩니다.

- 가상 시스템 시작
- 가상 시스템 중지

또한 vRealize Automation 인터페이스의 vRealize Orchestrator 라이브러리를 통해 액세스할 수 있는 워크플로를 사용하여 사용자 지정 리소스 작업을 생성할 수 있습니다.

vRealize Automation에서 기타 XaaS 리소스 작업을 사용하는 것과 마찬가지로 Azure 리소스 작업을 사용할 수 있습니다. XaaS 리소스 작업에 대한 자세한 내용은 vRealize Automation 구성에서 XaaS Blueprint 및 리소스 작업 생성 및 vRealize Automation에서 vRealize Orchestrator 통합을 참조하십시오.

필수 조건

vRealize Automation 배포에 대해 올바른 Azure 끝점을 구성합니다.

프로시저

- 1 **설계 > XaaS > 리소스 작업**을 선택합니다.
- 2 **새로 만들기**를 클릭합니다.
- 3 vRealize Orchestrator 워크플로 라이브러리에서 **Orchestrator > 라이브러리 > Azure**로 이동합니다.
- 4 원하는 폴더와 워크플로를 선택합니다.
- 5 기타 XaaS 리소스 작업과 마찬가지로 방식으로 필요에 맞게 작업을 구성합니다.

Puppet 사용 vSphere Blueprint 생성

vSphere 가상 시스템의 Puppet 기반 구성 관리를 지원하는 Puppet 사용 vSphere Blueprint를 생성할 수 있습니다.

Puppet 기반 구성 관리는 일반적으로 역할 및 환경을 사용하여 소프트웨어 구성을 정의 및 관리합니다. Puppet에서 역할 및 환경의 의미는 보다 일반적인 IT의 의미와 다르니 유의해야 합니다.

끝점은 기존 Puppet Enterprise 배포와의 연결을 설정합니다. 끝점이 생성되면

vRealize Automation은 지정한 배포와 관련된 환경 및 역할 목록을 검색합니다. 이러한 환경 및 역할은 Puppet 사용 가상 시스템 Blueprint를 구성할 때 컴파일 시 바인딩 또는 런타임 시 바인딩 시나리오에 사용할 수 있습니다.

참고 Puppet 구성 요소는 현재 vSphere Blueprint 및 가상 시스템에서만 지원됩니다.

vSphere Blueprint에 Puppet 구성 요소 추가

Puppet 구성 관리 구성 요소를 vSphere Blueprint에 추가하면 Puppet Master를 사용하여 vSphere 가상 시스템의 적용된 관리를 용이하게 할 수 있습니다.

Puppet 구성 요소를 vSphere Blueprint에 추가하면 해당 Blueprint에서 생성된 가상 시스템에 Puppet 에이전트가 추가됩니다.

Puppet 사용 vSphere Blueprint를 생성하는 경우 컴파일 시 바인딩 구성을 생성할지 또는 런타임 시 바인딩 구성을 생성할지 선택해야 합니다.

컴파일 시 바인딩의 경우 Puppet 구성 요소가 Blueprint에 추가될 때 사용자가 특정 Blueprint를 기반으로 모든 가상 시스템에 대한 Puppet 역할 및 환경 설정을 정의합니다. 이러한 설정은 Blueprint의 수명 기간 동안 정적으로 유지됩니다. 런타임 시 바인딩의 경우 몇 가지 옵션을 사용할 수 있습니다.

- Blueprint에서 **Puppet 환경** 및 **Puppet 역할** 텍스트 상자를 비워 두고 사용자가 이러한 설정을 요청 시 입력하도록 합니다.
- **Puppet 환경**을 지정하고 **Puppet 역할** 상자는 비워 둡니다. 요청 시 사용자가 역할을 지정해야 합니다.

필수 조건

적절한 vSphere Blueprint를 생성합니다. 자세한 내용은 [vSphere 시스템 구성 요소 설정](#)을 참조하십시오.

프로시저

- 1 **설계 > Blueprint**를 선택합니다.
- 2 Blueprint에 대한 [설계] 페이지의 [범주] 메뉴에서 **구성 관리**를 선택합니다.
- 3 Puppet 구성 요소를 선택하고 설계 캔버스의 vSphere 구성 요소로 끌어 놓습니다.
- 4 페이지 맨 아래의 [일반] 탭에서 Puppet 구성 요소의 **ID** 및 **설명**을 입력합니다.
ID 및 설명은 임의의 값입니다.
- 5 [서버] 탭을 클릭합니다.
- 6 드롭다운을 클릭하고 Blueprint에 적합한 Puppet Master를 선택합니다.
- 7 이 구성 요소에 대해 컴파일 시 바인딩을 사용하려면 적합한 **Puppet 환경** 및 **Puppet 역할**을 선택합니다.

컴파일 시 바인딩을 구성하려면 Puppet 환경 및 역할을 선택합니다. 런타임 시 바인딩으로 구성 요소를 생성하려면 **Puppet 환경**을 선택하거나, **Puppet 환경** 및 **Puppet 역할** 텍스트 상자를 비워 두고 **요청 양식에서 설정** 확인란을 선택합니다.

참고 요청 양식에서 **설정** 확인란은 함께 연결되어 있습니다. 하나를 선택하면 다른 확인란이 자동으로 선택됩니다.

- 8 **완료**를 클릭하여 Puppet 구성 요소 구성을 저장하고 기본 Blueprint [설계] 페이지로 돌아갑니다.

Windows 시스템 Blueprint에 RDP 연결 지원 추가

카탈로그 관리자가 Windows Blueprint에 대해 [RDP를 사용하여 연결] 작업에 대한 사용 권한을 사용자에게 부여하도록 허용하려면 RDP 사용자 지정 속성을 Blueprint에 추가하고 시스템 관리자가 준비한 RDP 파일을 참조합니다.

참고 패브릭 관리자가 필수 사용자 지정 속성이 포함된 속성 그룹을 생성하고 사용자가 이 그룹을 Blueprint에 포함시키는 경우 사용자는 개별적으로 사용자 지정 속성을 Blueprint에 추가할 필요가 없습니다.

필수 조건

- **테넌트 관리자** 또는 **비즈니스 그룹 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 시스템 관리자가 생성한 사용자 지정 RDP 파일의 이름을 가져옵니다. [프로비저닝된 시스템에 대한 RDP 연결 지원을 위해 사용자 지정 RDP 파일 생성](#) 항목을 참조하십시오.
- Windows 시스템 Blueprint를 최소 하나 생성합니다.

프로시저

- 1 **설계 > Blueprint**를 선택합니다.
- 2 업데이트할 Blueprint를 가리키고 **편집**을 클릭합니다.
- 3 세부 정보를 편집하려면 캔버스에서 시스템 구성 요소를 선택합니다.
- 4 **속성** 탭을 클릭합니다.
- 5 **사용자 지정 속성** 탭을 클릭합니다.

6 RDP 설정을 구성합니다.

- a 새 속성을 클릭합니다.
- b 이름 텍스트 상자에 RDP 사용자 지정 속성 이름을 입력하고 해당하는 값을 값 텍스트 상자에 입력합니다.

옵션	설명 및 값
(필수) RDP.FileName	설정을 가져올 RDP 파일을 지정합니다(예: My_RDP_Settings.rdp). 이 파일은 vRealize Automation 설치 디렉토리의 WebsiteWRdp 하위 디렉토리에 있어야 합니다.
(필수) VirtualMachine.Rdp.SettingN	시스템에 대한 RDP 링크를 열 때 사용할 RDP 설정을 지정합니다. N은 특정 RDP 설정을 다른 RDP 설정과 구분하는 데 사용되는 고유한 번호입니다. 예를 들어 인증 요구 사항이 지정되지 않도록 RDP 인증 수준을 지정하려면 사용자 지정 속성 VirtualMachine.Rdp.Setting1을 정의하고 값을 authentication level:i:3으로 설정합니다. 사용 가능한 RDP 설정과 해당 구문에 대한 자세한 내용은 RDP Settings for Remote Desktop Services in Windows Server 와 같은 Microsoft Windows RDP 설명서를 참조하십시오.
VirtualMachine.Admin.NameCompletion	사용자 인터페이스 옵션인 RDP를 사용하여 연결 또는 SSH를 사용하여 연결 옵션에 대해 RDP 또는 SSH 파일이 생성하는 시스템의 정규화된 도메인 이름에 포함할 도메인 이름을 지정합니다. 예를 들어 RDP 또는 SSH 파일에서 정규화된 도메인 이름 <i>my-machine-name.myCompany.com</i> 을 생성하려면 값을 myCompany.com으로 설정합니다.

- c 저장을 클릭합니다.

7 Blueprint 행을 선택하고 게시를 클릭합니다.

카탈로그 관리자가 Blueprint에서 프로비저닝된 시스템에 대해 **RDP를 사용하여 연결** 작업에 대한 사용 권한을 사용자에게 부여할 수 있습니다. 이 작업에 대한 권한이 사용자에게 없는 경우 사용자는 RDP를 사용하여 연결할 수 없습니다.

시나리오: CentOS Blueprint에 Active Directory 정리 추가

IaaS 설계자로서, 프로비저닝된 시스템이 하이퍼바이저에서 제거될 때마다 Active Directory 환경을 정리하도록 vRealize Automation을 구성합니다. 따라서 기존 vSphere CentOS Blueprint를 편집하여 Active Directory 정리 플러그인을 구성합니다.

Active Directory 정리 플러그인을 사용하여 시스템이 하이퍼바이저에서 삭제될 때 다음과 같은 Active Directory 계정 작업이 발생하도록 지정할 수 있습니다.

- AD 계정 삭제
- AD 계정을 사용하지 않도록 설정
- AD 계정 이름 변경
- AD 계정을 다른 AD OU(조직 구성 단위)로 이동

필수 조건

참고 이 정보는 Amazon Web Services에는 적용되지 않습니다.

- vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.
- Active Directory 환경에 대한 다음과 같은 정보를 수집합니다.
 - AD 계정을 삭제하거나, 사용하지 않도록 설정하거나, 이름을 변경하거나, 이동할 수 있는 충분한 권한을 가진 Active Directory 계정의 사용자 이름과 암호. 사용자 이름은 domain\username 형식이어야 합니다.
 - (선택 사항) 제거된 시스템을 이동할 OU의 이름
 - (선택 사항) 제거된 시스템에 추가할 접두사
- 시스템 Blueprint를 생성합니다. Rainpole의 vRealize Automation 설치 및 구성 시나리오의 내용을 참조하십시오.

프로시저

- 1 **설계 > Blueprint**를 선택합니다.
- 2 **vSphere CentOS** Blueprint를 가리키고 **편집**을 클릭합니다.
- 3 [세부 정보] 탭을 표시하려면 캔버스에서 시스템 구성 요소를 선택합니다.
- 4 **속성** 탭을 클릭합니다.
- 5 **사용자 지정 속성** 탭을 클릭하고 Active Directory 정리 플러그인을 구성합니다.
 - a **새 속성**을 클릭합니다.
 - b **이름** 텍스트 상자에 Plugin.AdMachineCleanup.Execute를 입력합니다.
 - c **값** 텍스트 상자에 **true**를 입력합니다.
 - d **저장** 아이콘(🟢)을 클릭합니다.
- 6 사용자 지정 속성을 추가하여 Active Directory 정리 플러그인을 구성합니다.

옵션	설명 및 값
Plugin.AdMachineCleanup.UserName	값 텍스트 상자에 Active Directory 계정 사용자 이름을 입력합니다. 이 사용자에게는 Active Directory 계정을 삭제하고, 사용하지 않도록 설정하고, 이동하고, 이름을 변경할 수 있는 충분한 권한이 있어야 합니다. 사용자 이름은 domain\username 형식이어야 합니다.
Plugin.AdMachineCleanup.Password	값 텍스트 상자에 Active Directory 계정 사용자 이름에 대한 암호를 입력합니다.
Plugin.AdMachineCleanup.Delete	제거된 시스템의 계정을 사용하지 않도록 설정하는 대신 삭제하려면 True로 설정합니다.
Plugin.AdMachineCleanup.MoveToOu	제거된 시스템의 계정을 새 Active Directory 조직 구성 단위로 이동합니다. 이 값은 계정을 이동하는 조직 구성 단위입니다. 이 값은 ou=OU, dc=dc 형식이어야 합니다(예: ou=trash,cn=computers,dc=lab,dc=local).
Plugin.AdMachineCleanup.RenamePrefix	접두사를 추가하여 제거된 시스템 계정의 이름을 바꿉니다. 이 값은 이름 앞에 붙을 접두사 문자열입니다(예: destroyed_).

7 확인을 클릭합니다.

Blueprint에서 프로비저닝된 시스템이 하이퍼바이저에서 삭제될 때마다 Active Directory 환경이 업데이트됩니다.

시나리오: 요청자가 시스템 호스트 이름을 지정할 수 있도록 허용

Blueprint 설계자는 사용자가 Blueprint를 요청할 때 자신들의 시스템 이름을 선택하도록 허용할 수 있습니다. 이렇게 하려면 기존 CentOS vSphere Blueprint를 편집하여 사용자 요청 중 사용자에게 값 제공을 요구하도록 호스트 이름 사용자 지정 속성을 추가하고 구성합니다.


참고 패브릭 관리자가 필수 사용자 지정 속성이 포함된 속성 그룹을 생성하고 사용자가 이 그룹을 Blueprint에 포함시키는 경우 사용자는 개별적으로 사용자 지정 속성을 Blueprint에 추가할 필요가 없습니다.

필수 조건

- vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.
- 시스템 Blueprint를 생성합니다. Rainpole의 vRealize Automation 설치 및 구성 시나리오의 내용을 참조하십시오.

프로시저

- 1 **설계 > Blueprint**를 선택합니다.
- 2 **vSphere CentOS** Blueprint를 가리키고 **편집**을 클릭합니다.
- 3 [세부 정보] 탭을 표시하려면 캔버스에서 시스템 구성 요소를 선택합니다.
- 4 **속성** 탭을 클릭합니다.
- 5 **새 속성**을 클릭합니다.
- 6 **이름** 텍스트 상자에 **호스트 이름**을 입력합니다.
- 7 **값** 텍스트 상자는 비워 둡니다.
- 8 요청 중 사용자에게 호스트 이름 값 제공을 요구하도록 vRealize Automation를 구성합니다.
 - a **재정의 가능**을 선택합니다.
 - b **요청에서 표시**를 선택합니다.

호스트 이름은 고유해야 하므로 사용자는 이 Blueprint에서 한 번에 하나의 시스템만 요청할 수 있습니다.
- 9 **저장** 아이콘()을 클릭합니다.
- 10 **확인**을 클릭합니다.

설계자 Blueprint에서 시스템을 요청하는 사용자는 자신들의 시스템에 대한 호스트 이름을 지정해야 합니다. vRealize Automation는 지정된 호스트 이름이 고유한지 확인합니다.

시나리오: 영역 간 배포에 사용할 데이터 센터 위치를 사용자가 선택할 수 있도록 허용

Blueprint 설계자로서, 사용자가 시스템 프로비저닝을 보스턴 인프라에서 할지 아니면 런던 인프라에서 할지 선택할 수 있도록 허용하려고 합니다. 이에 위치 기능을 사용하도록 기존 vSphere CentOS Blueprint를 편집합니다.



런던과 보스턴에 데이터 센터가 있으며 보스턴의 사용자가 런던 인프라에서 시스템을 프로비저닝하거나 런던의 사용자가 보스턴 인프라에서 시스템을 프로비저닝하지 않길 바랍니다. 보스턴 사용자가 보스턴 인프라에서 프로비저닝하고 런던 사용자가 런던 인프라에서 프로비저닝하도록 사용자가 시스템을 요청할 때 프로비저닝을 위한 적합한 위치를 선택하도록 허용하고자 합니다.

필수 조건

- vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.
- 시스템 관리자는 데이터 센터 위치를 정의합니다. **시나리오: 영역 간 배포를 위한 데이터 센터 위치 추가** 항목을 참조하십시오.
- 패브릭 관리자로서 적합한 위치를 계산 리소스에 적용합니다. **시나리오: 영역 간 배포를 위한 계산 리소스에 위치 적용** 항목을 참조하십시오.
- 시스템 Blueprint를 생성합니다. Rainpole의 vRealize Automation 설치 및 구성 시나리오의 내용을 참조하십시오.

프로시저

- 1 **설계 > Blueprint**를 선택합니다.
- 2 **vSphere CentOS** Blueprint를 가리키고 **편집**을 클릭합니다.
- 3 **일반** 세부 정보 탭을 표시하려면 캔버스에서 시스템 구성 요소를 선택합니다.
- 4 **요청에 위치 표시** 확인란을 선택합니다.
- 5 **완료**를 클릭합니다.
- 6 **vSphere CentOS** Blueprint를 가리키고 **게시**를 클릭합니다.

이제 비즈니스 그룹 사용자가 Blueprint에서 프로비저닝될 시스템을 요청하면 데이터 센터 위치를 선택하도록 메시지가 표시됩니다.

Software 구성 요소 설계

소프트웨어 설계자는 재사용 가능한 소프트웨어 구성 요소를 생성하여 구성 속성을 표준화하고, 작업 스크립트를 사용하여 구성 요소가 설치, 구성, 제거, 배포 확장/축소 작업 중 업데이트되는 방식을 정확하게 지정합니다. 이러한 작업 스크립트를 언제라도 다시 작성하고 게시하여 변경 내용을 프로비저닝된 소프트웨어 구성 요소에 푸시할 수 있습니다.

소프트웨어 속성이라고 하는 이름 및 값 쌍을 정의 및 사용하고 이를 작업 스크립트에 매개 변수로 전달하여 작업 스크립트가 일반적이고 재사용 가능한 스크립트가 되도록 설계할 수 있습니다. 소프트웨어 속성에 알 수 없는 값이 있거나 소프트웨어 속성을 나중에 정의해야 하는 경우 다른 Blueprint 설계자 또는 최종 사용자가 값을 제공하도록 지정 또는 허용할 수 있습니다. Blueprint에서 다른 구성 요소의 값이 필요한 경우(예: 시스템의 IP 주소) 소프트웨어 속성을 해당 시스템의 IP 주소 속성과 바인딩할 수 있습니다. 소프트웨어 속성을 사용하여 작업 스크립트를 매개 변수화하면 일반적이고 재사용 가능한 작업 스크립트를 만들 수 있기 때문에 스크립트를 수정하지 않고도 서로 다른 환경에 소프트웨어 구성 요소를 배포할 수 있습니다.

표 3-44. 수명 주기 작업

수명 주기 작업	설명
설치	소프트웨어를 설치합니다. 예를 들어 Tomcat 서버 설치 비트를 다운로드하여 Tomcat 서비스를 설치할 수 있습니다. 설치 수명 주기 작업에 대해 작성하는 스크립트는 초기 배포 요청 동안 또는 확장의 일부로 소프트웨어가 처음 프로비저닝될 때 실행됩니다.
구성	소프트웨어를 구성합니다. Tomcat을 예로 들면 JAVA_OPTS 및 CATALINA_OPTS를 설정할 수 있습니다. 구성 스크립트는 설치 작업이 완료된 후에 실행됩니다.
시작	소프트웨어를 시작합니다. 예를 들어 Tomcat 서버에서 시작 명령을 사용하여 Tomcat 서비스를 시작할 수 있습니다. 시작 스크립트는 구성 작업이 완료된 후에 실행됩니다.
업데이트	확장 가능 Blueprint를 지원하도록 소프트웨어 구성 요소를 설계 중인 경우 축소 또는 확장 작업 후에 필요한 모든 업데이트를 처리합니다. 예를 들어 확장/축소된 배포에 대해 클러스터 크기를 변경하고 로드 밸런서를 사용하여 클러스터된 노드를 관리할 수 있습니다. 여러 번 실행되고 (idempotent) 축소 및 확장을 모두 처리할 수 있도록 업데이트 스크립트를 설계합니다. 축소/확장 작업이 수행되면 모든 종속 소프트웨어 구성 요소에 대해 업데이트 스크립트가 실행됩니다.
제거	소프트웨어를 제거합니다. 예를 들어 배포가 제거되기 전에 애플리케이션에서 특정 작업을 수행할 수 있습니다. 제거 스크립트는 소프트웨어 구성 요소가 제거될 때마다 실행됩니다.

VMware Solution Exchange에서 다양한 미들웨어 서비스 및 애플리케이션에 대해 미리 정의된 Software 구성 요소를 다운로드할 수 있습니다. vRealize CloudClient 또는 vRealize Automation REST API를 사용하여 미리 정의된 Software 구성 요소를 vRealize Automation 인스턴스로 프로그래밍 방식으로 가져올 수 있습니다.

- VMware Solution Exchange를 방문하려면 https://solutionexchange.vmware.com/store/category_groups/cloud-management 항목을 참조하십시오.
- vRealize Automation REST API에 대한 자세한 내용은 프로그래밍 가이드 및 vRealize Automation API 참조 항목을 참조하십시오.
- vRealize CloudClient에 대한 자세한 내용은 <https://developercenter.vmware.com/tool/cloudclient> 항목을 참조하십시오.

속성 유형 및 설정 옵션

소프트웨어 속성이라고 하는 이름 및 값 쌍을 정의 및 사용하고 이를 작업 스크립트에 매개 변수로 전달하여 작업 스크립트가 일반적이고 재사용 가능한 스크립트가 되도록 설계할 수 있습니다. 문자열, 어레이, 콘텐츠, 부울 또는 정수 값을 필요로 하는 소프트웨어 속성을 생성할 수 있습니다. 직접 값을 제공하거나, 다른 사람이 값을 제공하도록 하거나, 바인딩을 생성하여 다른 Blueprint 구성 요소에서 값을 검색할 수 있습니다.

속성 옵션

[계산됨] 확인란을 선택하여 모든 문자열 속성의 값을 계산할 수 있으며 Software 속성을 구성할 때 해당하는 확인란을 선택하여 모든 속성을 암호화하거나, 재정의 가능하게 하거나, 필수로 설정할 수 있습니다. 다른 용도로 사용하려면 이러한 옵션을 원하는 값과 결합합니다. 예를 들어 Blueprint 설계자가 암호 값을 제공하고 Blueprint에서 소프트웨어 구성 요소를 사용할 때 해당 값을 암호화하도록 요구할 수 있습니다. 암호 속성을 생성하고 값 텍스트 상자는 비워 둡니다. [재정의 가능], [필수], 및 [암호화됨]을 선택합니다. 필요한 암호가 최종 사용자에게 속하는 경우 Blueprint 설계자는 **요청에서 표시**를 선택하여 사용자가 요청 양식을 작성할 때 암호를 입력하도록 요구할 수 있습니다.

옵션	설명
암호화됨	암호화된 속성으로 표시하여 값을 마스킹하고 vRealize Automation에서 별표로 표시합니다. 속성을 암호화됨에서 암호화되지 않음으로 변경하면 vRealize Automation이 속성 값을 재설정합니다. 보안상의 이유로 속성 값을 새로 설정해야 합니다.
재정의 가능	설계자가 애플리케이션 Blueprint를 구성하는 동안 이 속성 값을 편집할 수 있도록 허용합니다. 값을 입력하면 해당 값이 기본값으로 표시됩니다.
필수	설계자가 이 속성 값을 직접 지정하거나, 사용자가 제공한 기본값을 수락하도록 요구합니다.
계산됨	계산된 속성의 값은 INSTALL, CONFIGURE, START 또는 UPDATE 수명 주기 스크립트에 의해 할당됩니다. 할당된 값은 사용 가능한 후속 수명 주기 단계 및 Blueprint에서 이러한 속성에 바인딩하는 구성 요소로 전파됩니다. 문자열 속성이 아닌 속성에 대해 [계산됨]을 선택하면 속성 유형이 문자열로 변경됩니다.

[계산됨] 속성 옵션을 선택하는 경우 사용자 지정 속성 값을 비워 둡니다. 계산된 값에 대한 스크립트를 설계합니다.

표 3-45. 계산된 속성 옵션에 대한 스크립팅 예

샘플 문자열 속성	스크립트 구문	샘플 사용법
my_unique_id = ""	Bash - \$my_unique_id	<pre>export my_unique_id="0123456789"</pre>
	Windows CMD - %my_unique_id%	<pre>set my_unique_id=0123456789</pre>
	Windows PowerShell - \$my_unique_id	<pre>\$my_unique_id = "0123456789"</pre>

문자열 속성

문자열 속성에는 문자열 값이 필요합니다. 직접 문자열을 제공하거나, 다른 사람이 값을 제공하도록 하거나, 다른 문자열 속성에 대한 바인딩을 생성하여 다른 Blueprint 구성 요소에서 값을 검색할 수 있습니다. 문자열 값에는 모든 ASCII 문자가 포함될 수 있습니다. 속성 바인딩을 생성하려면 설계 캔버스에서 **속성** 탭을 사용하여 바인딩에 적합한 속성을 선택합니다. 그러면 속성 값이 작업 스크립트에 원시 문자열 데이터로 전달됩니다. Blueprint 문자열 속성에 바인딩하는 경우 바인딩하는 Blueprint 구성 요소가 클러스터 가능하지 않아야 합니다. 구성 요소가 클러스터되는 경우 문자열 값이 어레이가 되어 필요한 값을 검색할 수 없습니다.

샘플 문자열 속성	스크립트 구문	샘플 사용법
admin_email = "admin@email987.com"	Bash - \$admin_email	<pre>echo \$admin_email</pre>
	Windows CMD - %admin_email%	<pre>echo %admin_email%</pre>
	Windows PowerShell - \$admin_email	<pre>write-output \$admin_email</pre>

어레이 속성

어레이 속성에는 ["value1", "value2", "value3"...]으로 정의된 문자열, 정수, 십진수 또는 부울 값의 어레이가 필요합니다. 직접 값을 제공하거나, 다른 사람이 값을 제공하도록 하거나, 속성 바인딩을 생성하여 다른 Blueprint 구성 요소에서 값을 검색할 수 있습니다.

데이터 유형이 정수 또는 소수인 어레이 유형의 소프트웨어 속성을 생성할 때 로케일에 관계없이 어레이 요소 구분 기호로 세미콜론을 사용해야 합니다. 쉼표(,)나 점(.)은 사용하지 마십시오. 일부 로케일의 경우 쉼표(.)를 소수 구분 기호로 사용할 수 있습니다. 예:

- 프랑스어에 대한 올바른 어레이는 다음과 유사합니다. [1,11;2,22;3,33]
- 영어에 대한 올바른 어레이는 다음과 유사합니다. [1.11,2.22,3.33]

어레이에 큰 숫자를 전달할 때 그룹화 형식을 사용하지 마십시오. 예를 들어 로케일별 형식을 포함하는 데이터 파일이 다른 로케일이 있는 시스템으로 전송되면 잘못 해석될 수 있으므로 **4444 444.000**(프랑스어), **4.444.444,000**(이탈리아어) 또는 **4,444,444.000**(영어)를 사용하지 마십시오. **4,444,444.000**과 같은 숫자는 세 개의 개별 숫자로 간주되므로 그룹화 형식은 허용되지 않습니다. 대신 **4444444.000**을 입력하십시오.

어레이 속성 값을 정의할 때는 어레이를 대괄호로 묶어야 합니다. 문자열 어레이의 경우 어레이 요소의 값에는 모든 ASCII 문자가 포함될 수 있습니다. 어레이 속성 값에서 백슬래시 문자를 올바르게 인코딩하려면 백슬래시를 하나 더 추가합니다(예: ["c:WWtest1WWtest2"]). 바인딩 속성의 경우 설계 캔버스에서 **속성** 탭을 사용하여 바인딩에 적합한 속성을 선택합니다. 어레이에 바인딩하는 경우 소프트웨어 구성 요소가 값 어레이를 특정 순서로 요청하지 않도록 소프트웨어 구성 요소를 설계해야 합니다.

예를 들어 애플리케이션 서버 가상 시스템의 클러스터에 대한 로드 균형화를 조정하는 로드 밸런서 가상 시스템을 가정해 보겠습니다. 이러한 경우 어레이 속성은 로드 밸런서 서비스에 대해 정의되고 애플리케이션 서버 가상 시스템의 IP 주소 어레이로 설정됩니다.

이러한 로드 밸런서 서비스 구성 스크립트는 어레이 속성을 사용하여 Red Hat, Windows 및 Ubuntu 운영 체제에서 적절한 로드 밸런싱 체계를 구성합니다.

샘플 어레이 속성	스크립트 구문	샘플 사용법
operating_systems = ["Red Hat", "Windows", "Ubuntu"]	Bash - \${operating_systems[@]} - 전체 문자열 어레이용 \${operating_systems[N]} - 개별 어레이 요소용	for ((i = 0 ; i < \$ {#operating_systems[@]}; i++)); do echo \${operating_systems[\$i]} done
	Windows CMD - %operating_systems_% 여기서 N은 어레이 요소의 위치를 나타냅니다.	for /F "delims== tokens=2" %A in ('set operating_systems_') do (echo %A)
	Windows PowerShell - \$operating_systems - 전체 문자열 어레이용 \$operating_systems[N] - 개별 어레이 요소용	foreach (\$os in \$operating_systems){ write-output \$os }

컨텐츠 속성

컨텐츠 속성 값은 컨텐츠를 다운로드할 파일의 URL입니다. Software 에이전트는 URL의 컨텐츠를 가상 시스템으로 다운로드하고 가상 시스템의 로컬 파일 위치를 스크립트에 전달합니다.

컨텐츠 속성은 HTTP 또는 HTTPS 프로토콜을 사용하여 유효한 URL로 정의해야 합니다. 예를 들어 Dukes Bank 샘플 애플리케이션의 JBOSS 애플리케이션 서버 Software 구성 요소는 컨텐츠 속성 cheetah_tgz_url을 지정합니다. 아티팩트가 Software 장치에서 호스팅되고 URL은 장치에서 해당 위치를 가리킵니다. Software 에이전트는 지정된 위치의 아티팩트를 배포된 가상 시스템으로 다운로드합니다.

컨텐츠 속성과 함께 사용할 수 있는 software.http.proxy 설정에 대한 자세한 내용은 사용자 지정 속성 참조 자료 항목을 참조하십시오.

샘플 문자열 속성	스크립트 구문	샘플 사용법
cheetah_tgz_url = "http://app_content_server_ip:port/artifacts/software/jboss/cheetah-2.4.4.tar.gz"	Bash - \$cheetah_tgz_url	tar -zxvf \$cheetah_tgz_url
	Windows CMD - %cheetah_tgz_url %	start /wait c:Wunzip.exe %cheetah_tgz_url %
	Windows PowerShell - \$cheetah_tgz_url	& c:Wunzip.exe \$cheetah_tgz_url

부울 속성

[값] 드롭다운 메뉴에서 True 및 False를 선택하려면 부울 속성 유형을 사용합니다.

정수 속성

0, 양의 정수, 음의 정수에는 정수 속성 유형을 사용합니다.

십진수 속성

반복되지 않는 소수를 나타내는 값에는 십진수 속성 유형을 사용합니다.

Software 구성 요소에 다른 구성 요소의 정보가 필요한 경우

여러 배포 시나리오에서 구성 요소 자체를 사용자 지정하려면 다른 구성 요소의 속성 값이 필요합니다. vRealize Automation에서 속성 바인딩을 생성하여 이 작업을 수행할 수 있습니다. 속성 바인딩에 대해 Software 작업 스크립트를 설계할 수 있지만 실제 바인딩은 Blueprint를 구성하는 설계자가 구성합니다.

속성을 하드 코딩된 값으로 설정하는 것 외에도 소프트웨어 설계자, IaaS 설계자 또는 애플리케이션 설계자는 IP 주소 또는 설치 위치와 같은 Software 구성 요소 속성을 Blueprint의 다른 속성에 바인딩할 수 있습니다. Software 속성을 다른 속성에 바인딩하는 경우 다른 구성 요소 속성 또는 가상 시스템 속성의 값을 기반으로 스크립트를 사용자 지정할 수 있습니다. 예를 들어 WAR 구성 요소에는 Apache Tomcat 서버의 설치 위치가 필요할 수 있습니다. 스크립트에서는 server_home 속성 값을 스크립트의 Apache Tomcat 서버 install_path 속성 값으로 설정하도록 WAR 구성 요소를 구성할 수 있습니다. Blueprint를 구성하는 설계자가 server_home 속성을 Apache Tomcat 서버 install_path 속성에 바인딩하는 한 server_home 속성 값은 올바르게 설정됩니다.

작업 스크립트에서는 해당 스크립트에서 정의하는 속성만 사용할 수 있으며 문자열 및 어레이 값으로만 속성 바인딩을 생성할 수 있습니다. Blueprint 속성 어레이는 특정 순서로 반환되지 않기 때문에 클러스터 가능 또는 확장 가능 구성 요소에 바인딩할 때 필요한 값이 생성되지 않을 수 있습니다. 예를 들어 소프트웨어 구성 요소에 시스템 클러스터의 각 시스템 ID가 필요하며, 사용자가 1-10개 시스템으로 구성된 클러스터를 요청하고 배포를 1-10개 시스템에 확장할 수 있도록 허용한다고 가정합니다. 소프트웨어 속성을 문자열 유형으로 구성하면 클러스터로부터 임의로 선택된 하나의 시스템 ID를 갖게 됩니다. 소프트웨어 속성을 어레이 유형으로 구성하면 특정 순서 없이 클러스터의 모든 시스템 ID 어레이

를 갖게 됩니다. 사용자가 배포를 확장하면 값의 순서가 작업별로 다를 수 있습니다. 클러스터된 구성 요소의 값이 손실되지 않도록 모든 소프트웨어 속성에 대해 어레이 유형을 사용할 수 있습니다. 하지만 소프트웨어 구성 요소가 값 어레이를 특정 순서로 요청하지 않도록 소프트웨어 구성 요소를 설계해야 합니다.

다른 유형의 속성에 바인딩하는 경우 문자열 속성 바인딩의 예 테이블에서 문자열 속성 값의 예를 참조하십시오.

표 3-46. 문자열 속성 바인딩의 예

샘플 속성 유형	바인딩할 속성 유형	바인딩 결과(A가 B에 바인딩)
문자열(속성 A)	문자열(속성 B="Hi")	A="Hi"
문자열(속성 A)	컨텐츠(속성 B="http://my.com/content")	A="http://my.com/content"
문자열(속성 A)	어레이(속성 B=["1","2"])	A=["1","2"]
문자열(속성 A)	계산(속성 B="Hello")	A="Hello"

다른 유형의 속성에 바인딩하는 경우 어레이 속성 바인딩의 예 테이블에서 어레이 속성 값의 예를 참조하십시오.

표 3-47. 어레이 속성 바인딩의 예

샘플 속성 유형	바인딩할 속성 유형	바인딩 결과(A가 B에 바인딩)
어레이(속성 A)	문자열(속성 B="Hi")	A="Hi"
어레이(속성 A)	컨텐츠(속성 B="http://my.com/content")	A="http://my.com/content"
어레이(속성 A)	계산(속성 B="Hello")	A="Hello"

지원되는 속성 유형에 대한 자세한 설명은 [속성 유형 및 설정 옵션](#) 항목을 참조하십시오.

수명 주기 단계 사이에 속성 값 전달

작업 스크립트를 사용하여 수명 주기 단계 사이에 속성 값을 수정하고 전달할 수 있습니다.

계산된 속성의 경우 속성 값을 수정하고 해당 값을 작업 스크립트의 다음 수명 주기 단계로 전달할 수 있습니다. 예를 들어 구성 요소 A의 progress_status 값이 스테이징됨으로 정의된 경우 설치 및 구성 수명 주기 단계에서는 해당 작업 스크립트에서 이 속성 값을 progress_status=installed로 변경할 수 있습니다. 구성 요소 B가 구성 요소 A에 바인딩되어 있으면 작업 스크립트의 수명 주기 단계에서 progress_status의 속성 값이 구성 요소 A와 동일하게 유지됩니다.

소프트웨어 구성 요소에서 구성 요소 B가 구성 요소 A에 종속된다고 정의하면 이 종속성 정의에 따라 구성 요소 A와 B가 같은 노드에 있는지 아니면 서로 다른 노드에 있든지에 관계없이 두 구성 요소 사이에 올바른 속성 값이 전달됩니다.

예를 들어 지원되는 스크립트를 사용하여 작업 스크립트에서 속성 값을 업데이트할 수 있습니다.

- Bash progress_status="completed"
- Windows CMD set progress_status=completed

- Windows PowerShell \$progress_status="completed"

참고 어레이 및 콘텐츠 속성의 경우에는 수명 주기 단계의 작업 스크립트 간에 수정된 속성 값이 전달되지 않습니다.

구성 요소 개발에 대한 모범 사례

속성 및 작업 스크립트 정의를 위한 모범 사례를 숙지하기 위해 VMware Solution Exchange에서 Software 구성 요소 및 애플리케이션 Blueprint를 다운로드하고 가져올 수 있습니다.

Software 구성 요소를 개발할 때는 다음 모범 사례를 따릅니다.

- 스크립트가 중단 없이 실행되도록 하려면 반환 값이 0으로 설정되어야 합니다. 이렇게 설정하면 에이전트가 속성을 모두 캡처하여 Software 서버로 보낼 수 있습니다.
- 일부 설치 관리자에서는 tty 콘솔에 액세스해야 할 수 있습니다. /dev/console의 입력을 리디렉션합니다. 예를 들어 RabbitMQ Software 구성 요소는 해당 설치 스크립트에 `./rabbitmq_rhel.py --setup-rabbitmq < /dev/console` 명령을 사용할 수 있습니다.
- 구성 요소가 여러 수명 주기 단계를 사용하는 경우 설치 수명 주기 단계에서 속성 값이 변경될 수 있습니다. 새 값은 다음 수명 주기 단계로 전송됩니다. 작업 스크립트에서는 배포 중 속성 값을 계산하여 다른 종속 스크립트에 값을 제공할 수 있습니다. 예를 들어 Clustered Dukes Bank 샘플 애플리케이션에서 JBossAppServer 서비스는 설치 수명 주기 단계 동안 JVM_ROUTE 속성을 계산합니다. 이 속성은 JBossAppServer 서비스에서 수명 주기를 구성하는 데 사용됩니다. 그런 다음 Apache 로드 밸런서 서비스는 JVM_ROUTE 속성에 바인딩하여 node0 및 node1의 최종 계산 값을 얻습니다. 애플리케이션 배포를 완료하기 위해 구성 요소에 다른 구성 요소의 속성 값이 필요한 경우 애플리케이션 Blueprint에서 종속성을 명시적으로 규정해야 합니다.

참고 여러 수명 주기 단계를 사용하는 구성 요소의 콘텐츠 속성 값은 변경할 수 없습니다.

Software 구성 요소 생성

다른 소프트웨어 설계자, IaaS 설계자, 애플리케이션 설계자가 애플리케이션 Blueprint를 구성하는데 사용할 수 있는 Software 구성 요소를 구성하고 게시합니다.

필수 조건

소프트웨어 설계자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **설계 > 소프트웨어 구성 요소**를 선택합니다.
- 2 **추가** 아이콘(+)을 클릭합니다.

3 이름을 입력하고 원하는 경우 설명을 입력합니다.

vRealize Automation은 사용자가 Software 구성 요소에 지정한 이름을 사용하여 테넌트 내에서 고유한 ID를 Software 구성 요소에 대해 생성합니다. 지금은 이 필드를 편집할 수 있지만 Blueprint를 저장한 후에는 이 필드를 변경할 수 없습니다. ID는 영구적이며 테넌트 내에서 고유하기 때문에 ID를 사용하여 프로그래밍 방식으로 Blueprint와 상호 작용하고 속성 바인딩을 생성할 수 있습니다.

4 (선택 사항) Software 구성 요소가 Blueprint에 포함되는 방식을 제어하려면 **컨테이너** 드롭다운 메뉴에서 컨테이너 유형을 선택합니다.

옵션	설명
시스템	Software 구성 요소를 시스템에 직접 배치해야 합니다.
게시된 Software 구성 요소 중 하나	특정 Software 구성 요소를 설계하여 다른 Software 구성 요소 위에 특별히 설치하려는 경우 해당 Software 구성 요소를 목록에서 선택합니다. 예를 들어 EAR 구성 요소를 설계하여 이전에 생성한 JBOSS 구성 요소 위에 설치하려는 경우 목록에서 JBOSS 구성 요소를 선택합니다.
소프트웨어 구성 요소	시스템에 직접 설치되어서는 안 되지만 서로 다른 여러 Software 구성 요소 위에 설치될 수 있는 Software 구성 요소를 설계 중인 경우에는 해당하는 소프트웨어 구성 요소 옵션을 선택합니다. 예를 들어 WAR 구성 요소를 설계 중이고 이 구성 요소를 Tomcat Server Software 구성 요소 및 Tcserver Software 구성 요소 위에 설치하려는 경우 해당 소프트웨어 구성 요소 컨테이너 유형을 선택합니다.

5 다음을 클릭합니다.

6 작업 스크립트에서 사용하려는 속성을 정의합니다.

- 추가** 아이콘(+)을 클릭합니다.
- 속성의 이름을 입력합니다.
- 속성에 대한 설명을 입력합니다.

이 설명은 Blueprint에서 사용자의 Software 구성 요소를 사용하는 설계자에게 표시됩니다.

- d 속성 값에 대한 예상 유형을 선택합니다.
- e 속성에 대한 값을 정의합니다.

옵션	설명
지금 제공하는 값 사용	<ul style="list-style-type: none"> ■ 값을 입력합니다. ■ 재정의 가능을 선택 해제합니다. ■ 필수를 선택합니다.
설계자가 값을 제공해야 함	<ul style="list-style-type: none"> ■ 기본값을 제공하려면 값을 입력합니다. ■ 재정의 가능을 선택합니다. ■ 필수를 선택합니다.
선택하는 경우 설계자가 값을 제공하도록 허용	<ul style="list-style-type: none"> ■ 기본값을 제공하려면 값을 입력합니다. ■ 재정의 가능을 선택합니다. ■ 필수를 선택 해제합니다.

설계자는 요청 양식에서 사용자에게 표시되도록 Software 속성을 구성할 수 있습니다. 설계자는 [요청에서 표시] 옵션을 사용하여 [재정의 가능]으로 표시한 속성의 값을 사용자가 채우도록 설정 또는 요청할 수 있습니다.

- 7 메시지에 따라 최소 하나의 소프트웨어 수명 주기 작업에 대한 스크립트를 제공합니다.

표 3-48. 수명 주기 작업

수명 주기 작업	설명
설치	소프트웨어를 설치합니다. 예를 들어 Tomcat 서버 설치 비트를 다운로드하여 Tomcat 서비스를 설치할 수 있습니다. 설치 수명 주기 작업에 대해 작성하는 스크립트는 초기 배포 요청 동안 또는 확장의 일부로 소프트웨어가 처음 프로비저닝될 때 실행됩니다.
구성	소프트웨어를 구성합니다. Tomcat을 예로 들면 JAVA_OPTS 및 CATALINA_OPTS를 설정할 수 있습니다. 구성 스크립트는 설치 작업이 완료된 후에 실행됩니다.
시작	소프트웨어를 시작합니다. 예를 들어 Tomcat 서버에서 시작 명령을 사용하여 Tomcat 서비스를 시작할 수 있습니다. 시작 스크립트는 구성 작업이 완료된 후에 실행됩니다.
업데이트	확장 가능 Blueprint를 지원하도록 소프트웨어 구성 요소를 설계 중인 경우 축소 또는 확장 작업 후에 필요한 모든 업데이트를 처리합니다. 예를 들어 확장/축소된 배포에 대해 클러스터 크기를 변경하고 로드 밸런서를 사용하여 클러스터된 노드를 관리할 수 있습니다. 여러 번 실행되고(idempotent) 축소 및 확장을 모두 처리할 수 있도록 업데이트 스크립트를 설계합니다. 축소/확장 작업이 수행되면 모든 종속 소프트웨어 구성 요소에 대해 업데이트 스크립트가 실행됩니다.
제거	소프트웨어를 제거합니다. 예를 들어 배포가 제거되기 전에 애플리케이션에서 특정 작업을 수행할 수 있습니다. 제거 스크립트는 소프트웨어 구성 요소가 제거될 때마다 실행됩니다.

작업 스크립트에 종료 코드와 상태 코드를 포함합니다. 지원되는 각 스크립트 유형에는 고유한 종료 코드 및 상태 코드 요구 사항이 있습니다.

스크립트 유형	성공 상태	오류 상태	지원되지 않는 명령
Bash	<ul style="list-style-type: none"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	없음
Windows CMD	exit /b 0	exit /b non-zero	exit 0 또는 exit non-zero 코드를 사용하지 마십시오.

스크립트 유형	성공 상태	오류 상태	지원되지 않는 명령
PowerShell	exit 0	exit non-zero;	warning, verbose, debug 또는 host 호출을 사용하지 마십시오.

8 시스템 재부팅이 필요한 모든 스크립트에 대해 **재부팅** 확인란을 선택합니다.

스크립트를 실행하면 다음 수명 주기 스크립트가 시작되기 전에 시스템이 재부팅됩니다.

9 **완료**를 클릭합니다.

10 Software 구성 요소를 선택하고 **게시**를 클릭합니다.

Software 구성 요소를 구성하고 게시했습니다. 다른 소프트웨어 설계자, IaaS 설계자 및 애플리케이션 설계자가 이 Software 구성 요소를 사용하여 애플리케이션 Blueprint에 소프트웨어를 추가할 수 있습니다.

후속 작업

게시된 Software 구성 요소를 애플리케이션 Blueprint에 추가합니다. [복합 Blueprint 구성](#) 항목을 참조하십시오.

Software 구성 요소 설정

일반 설정을 구성하고, 속성을 생성하고, 프로비저닝된 시스템에서 Software 구성 요소를 설치, 구성, 업데이트 또는 제거하는 사용자 지정 작업 스크립트를 작성합니다.

소프트웨어 설계자는 **설계 > 소프트웨어 구성 요소**를 클릭한 후 **추가** 아이콘을 클릭하여 새 Software 구성 요소를 생성합니다.

새 Software 일반 설정

Software 구성 요소에 일반 설정을 적용합니다.

표 3-49. 새 Software 일반 설정

설정	설명
이름	Software 구성 요소의 이름을 입력합니다.
ID	vRealize Automation은 사용자가 Software 구성 요소에 지정한 이름을 사용하여 테넌트 내에서 고유한 ID를 Software 구성 요소에 대해 생성합니다. 지금은 이 필드를 편집할 수 있지만 Blueprint를 저장한 후에는 이 필드를 변경할 수 없습니다. ID는 영구적이며 테넌트 내에서 고유하기 때문에 ID를 사용하여 프로그래밍 방식으로 Blueprint와 상호 작용하고 속성 바인딩을 생성할 수 있습니다.

표 3-49. 새 Software 일반 설정 (계속)

설정	설명
설명	다른 설계자의 편의를 위해 Software 구성 요소를 요약합니다.
컨테이너	<p>설계 캔버스에서, Blueprint 설계자는 선택한 컨테이너 유형 내부에만 Software 구성 요소를 배치할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 설계자가 설계 캔버스의 시스템 구성 요소에 Software 구성 요소를 직접 배치하도록 하려면 시스템을 선택합니다. ■ 시스템 구성 요소에 직접 배치되어서는 안 되지만 서로 다른 여러 개의 Software 구성 요소 중 하나의 내부에 중첩될 수 있는 Software 구성 요소를 설계 중인 경우 소프트웨어 구성 요소를 선택합니다. ■ 생성한 다른 Software 구성 요소 내부에 특별히 중첩되도록 Software 구성 요소를 설계 중인 경우 게시된 특정 Software 구성 요소를 선택합니다. ■ 특별히 Azure Blueprint를 위한 Software 구성 요소를 설계 중인 경우에는 Azure 가상 시스템을 선택합니다.

새 Software 속성

Software 구성 요소 속성은 정의된 속성을 시스템에서 실행되는 스크립트에 환경 변수로 전달하기 위해 스크립트를 매개 변수화하는 데 사용됩니다. 프로비저닝된 시스템에 있는 Software 에이전트는 스크립트를 실행하기 전에 vRealize Automation과 통신하여 속성을 확인합니다. 그런 후 에이전트는 이러한 속성에서 스크립트 관련 변수를 생성하여 스크립트에 전달합니다.

표 3-50. 새 Software 속성

설정	설명
이름	Software 속성의 이름을 입력합니다. 속성 이름은 대/소문자를 구분하며 영문자, 숫자, 하이픈(-) 또는 밑줄(_) 문자만 포함할 수 있습니다.
설명	다른 사용자의 편의를 위해 속성 및 값에 대한 요구 사항을 요약합니다.
유형	Software는 문자열, 어레이, 컨테츠, 부울 및 정수 유형을 지원합니다. 지원되는 속성 유형에 대한 자세한 설명은 속성 유형 및 설정 옵션 항목을 참조하십시오. 속성 바인딩에 대한 자세한 내용은 Software 구성 요소에 다른 구성 요소의 정보가 필요한 경우 및 Blueprint 구성 요소 간 속성 바인딩 생성 항목을 참조하십시오.

표 3-50. 새 Software 속성 (계속)

설정	설명
값	<ul style="list-style-type: none"> ■ 지금 제공하는 값 사용: <ul style="list-style-type: none"> ■ 값을 입력합니다. ■ 필수를 선택합니다. ■ 재정의의 기능을 선택 해제합니다. ■ 설계자가 값을 제공해야 함: <ul style="list-style-type: none"> ■ (선택 사항) 기본값을 제공하려면 값을 입력합니다. ■ 재정의의 기능을 선택합니다. ■ 필수를 선택합니다. ■ 설계자가 값을 제공하거나 값을 비워 두도록 허용: <ul style="list-style-type: none"> ■ (선택 사항) 기본값을 제공하려면 값을 입력합니다. ■ 재정의의 기능을 선택합니다. ■ 필수를 선택 해제합니다.
암호화됨	<p>암호화된 속성으로 표시하여 값을 마스킹하고 vRealize Automation에서 별표로 표시합니다. 속성을 암호화됨에서 암호화되지 않음으로 변경하면 vRealize Automation이 속성 값을 재설정합니다. 보안상의 이유로 속성 값을 새로 설정해야 합니다.</p> <p>중요 echo 명령이나 다른 유사한 명령을 사용하여 스크립트에서 보안 속성을 출력하는 경우 이러한 값은 로그 파일에서 일반 텍스트로 표시됩니다. 로그 파일의 값은 마스킹되지 않습니다.</p>
재정의의 가능	설계자가 애플리케이션 Blueprint를 구성하는 동안 이 속성 값을 편집할 수 있도록 허용합니다. 값을 입력하면 해당 값이 기본값으로 표시됩니다.
필수	설계자가 이 속성 값을 직접 지정하거나, 사용자가 제공한 기본값을 수락하도록 요구합니다.
계산됨	계산된 속성의 값은 INSTALL, CONFIGURE, START 또는 UPDATE 수명 주기 스크립트에 의해 할당됩니다. 할당된 값은 사용 가능한 후속 수명 주기 단계 및 Blueprint에서 이러한 속성에 바인딩하는 구성 요소로 전파됩니다. 문자열 속성이 아닌 속성에 대해 [계산됨]을 선택하면 속성 유형이 문자열로 변경됩니다.

새 Software 작업

구성 요소가 설치, 구성, 제거 또는 배포 확장/축소 작업 중 업데이트되는 방식을 정확하게 지정하도록 Bash, Windows CMD 또는 PowerShell 작업 스크립트를 생성합니다.

표 3-51. 수명 주기 작업

수명 주기 작업	설명
설치	소프트웨어를 설치합니다. 예를 들어 Tomcat 서버 설치 비트를 다운로드하여 Tomcat 서비스를 설치할 수 있습니다. 설치 수명 주기 작업에 대해 작성하는 스크립트는 초기 배포 요청 동안 또는 확장의 일부로 소프트웨어가 처음 프로비저닝될 때 실행됩니다.
구성	소프트웨어를 구성합니다. Tomcat을 예로 들면 JAVA_OPTS 및 CATALINA_OPTS를 설정할 수 있습니다. 구성 스크립트는 설치 작업이 완료된 후에 실행됩니다.

표 3-51. 수명 주기 작업 (계속)

수명 주기 작업	설명
시작	소프트웨어를 시작합니다. 예를 들어 Tomcat 서버에서 시작 명령을 사용하여 Tomcat 서비스를 시작할 수 있습니다. 시작 스크립트는 구성 작업이 완료된 후에 실행됩니다.
업데이트	확장 가능 Blueprint를 지원하도록 소프트웨어 구성 요소를 설계 중인 경우 축소 또는 확장 작업 후에 필요한 모든 업데이트를 처리합니다. 예를 들어 확장/축소된 배포에 대해 클러스터 크기를 변경하고 로드 밸런서를 사용하여 클러스터된 노드를 관리할 수 있습니다. 여러 번 실행되고 (idempotent) 축소 및 확장을 모두 처리할 수 있도록 업데이트 스크립트를 설계합니다. 축소/확장 작업이 수행되면 모든 종속 소프트웨어 구성 요소에 대해 업데이트 스크립트가 실행됩니다.
제거	소프트웨어를 제거합니다. 예를 들어 배포가 제거되기 전에 애플리케이션에서 특정 작업을 수행할 수 있습니다. 제거 스크립트는 소프트웨어 구성 요소가 제거될 때마다 실행됩니다.

시스템 재부팅이 필요한 모든 스크립트에 대해 **재부팅** 확인란을 선택합니다. 스크립트를 실행하면 다음 수명 주기 스크립트가 시작되기 전에 시스템이 재부팅됩니다. 작업 스크립트가 실행 중일 때 사용자 상호 작용을 요구하는 프로세스가 없는지 확인합니다. 중단이 발생하면 스크립트가 일시 중지되어 무기한으로 유휴 상태로 남아 결과적으로 실패할 수 있습니다. 또한 스크립트에는 애플리케이션 배포에 적용할 수 있는 적절한 종료 코드가 포함되어야 합니다. 스크립트에 종료 및 반환 코드가 없으면 스크립트에서 마지막으로 실행된 명령이 종료 상태가 됩니다. 종료 및 반환 코드는 지원되는 스크립트 유형 (Bash, Windows CMD, PowerShell)에 따라 다릅니다.

스크립트 유형	성공 상태	오류 상태	지원되지 않는 명령
Bash	<ul style="list-style-type: none"> return 0 exit 0 	<ul style="list-style-type: none"> return non-zero exit non-zero 	없음
Windows CMD	exit /b 0	exit /b non-zero	exit 0 또는 exit non-zero 코드를 사용하지 마십시오.
PowerShell	exit 0	exit non-zero;	warning, verbose, debug 또는 host 호출을 사용하지 마십시오.

XaaS Blueprint 및 리소스 작업 설계

XaaS Blueprint는 카탈로그 항목으로 게시하거나 Blueprint 설계 캔버스에서 사용될 수 있습니다. 리소스 작업은 배포된 항목에서 실행하는 작업입니다.

XaaS는 vRealize Orchestrator를 사용하여 항목을 프로비저닝하거나 작업을 실행하는 워크플로를 실행합니다. 예를 들어 vSphere 가상 시스템, 그룹의 Active Directory 사용자를 생성하거나 PowerShell 스크립트 실행을 위해 워크플로를 구성할 수 있습니다. 사용자 지정 vRealize Orchestrator 워크플로를 생성하는 경우 이 워크플로를 서비스 카탈로그에서 하나의 항목으로 제공하여 권한 있는 사용자가 워크플로를 실행하도록 할 수 있습니다.

XaaS Blueprint를 설계 캔버스에서 생성하는 Blueprint의 구성 요소로 사용하거나 서비스 카탈로그에 직접 게시할 수 있습니다.

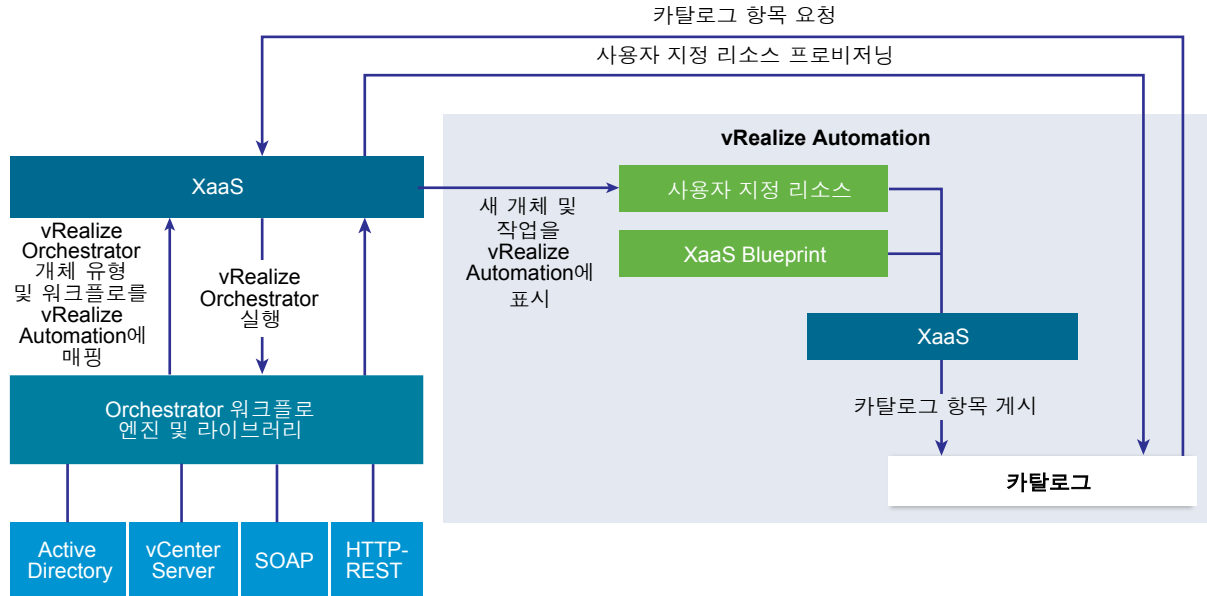
Blueprint를 다른 Blueprint의 구성 요소로 사용하는 경우 배포된 Blueprint가 확대 또는 축소될 때 확대/축소되도록 구성할 수 있습니다.

vRealize Automation 에서 vRealize Orchestrator 통합

vRealize Orchestrator는 vRealize Automation에 통합되어 있는 워크플로 엔진입니다.

vRealize Automation와 함께 배포되는 vRealize Orchestrator 서버는 미리 구성되어 있기 때문에 시스템 관리자가 vRealize Automation 장치를 배포하면 vRealize Orchestrator 서버가 자동으로 실행됩니다.

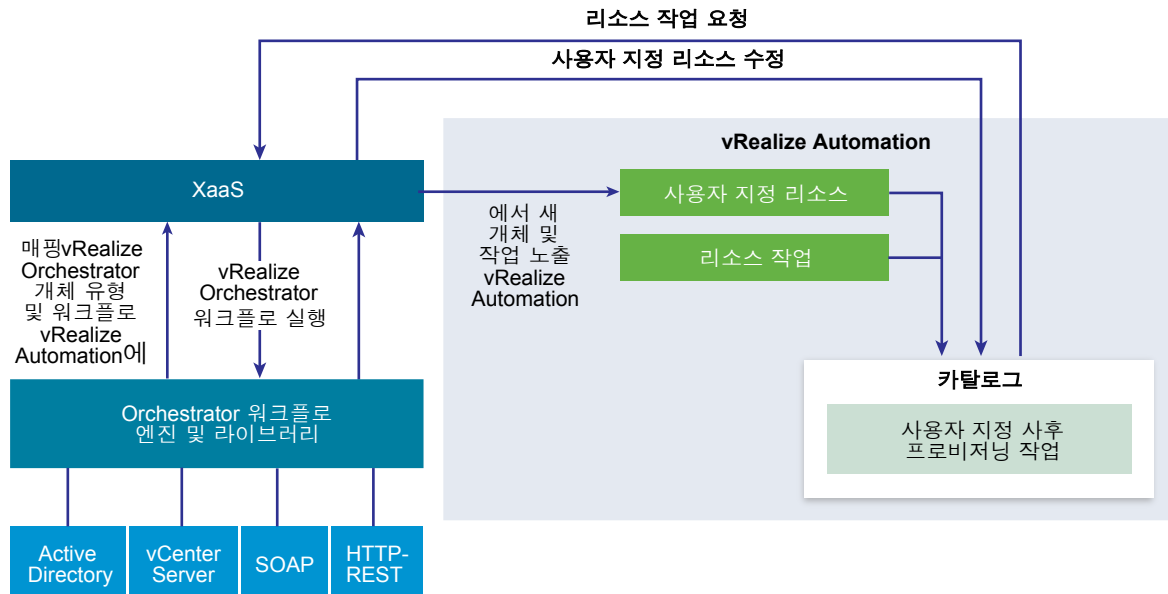
그림 3-2. 사용자 지정 리소스 프로비저닝을 위해 XaaS에 포함된 카탈로그 항목 생성 및 요청



XaaS 설계자는 지원되는 끝점 및 제공된 워크플로와 관련된 사용자 지정 리소스를 추가한 다음 그러한 리소스를 기반으로 XaaS Blueprint와 작업을 생성합니다. 테넌트 관리자와 비즈니스 그룹 관리자는 서비스 카탈로그에 XaaS Blueprint와 작업을 추가할 수 있습니다. XaaS Blueprint는 Blueprint 디자이너에서도 사용될 수 있습니다.

서비스 카탈로그 사용자가 항목을 요청하면 vRealize Automation에서 vRealize Orchestrator 워크플로를 실행하여 사용자 지정 리소스를 프로비저닝합니다.

그림 3-3. 사용자 지정 리소스 수정을 위해 사용자 지정 리소스 작업 생성 및 요청



XaaS 설계자는 리소스 작업으로 vRealize Orchestrator 워크플로를 추가하여 vRealize Automation 기능을 확장할 수 있습니다. 서비스 카탈로그 사용자가 사용자 지정 리소스를 프로비저닝한 후에는 사후 프로비저닝 작업을 실행할 수 있습니다. 이러한 방식으로 소비자는 vRealize Orchestrator 워크플로를 실행하고 프로비저닝된 사용자 지정 리소스를 수정합니다.

서비스 카탈로그 사용자가 카탈로그 항목으로 XaaS Blueprint 또는 리소스 작업을 요청하는 경우 XaaS 서비스는 해당하는 vRealize Orchestrator 워크플로를 실행하여 다음 데이터를 글로벌 매개 변수로 워크플로에 전달합니다.

표 3-52. XaaS 글로벌 매개 변수

매개 변수	설명
__asd_tenantRef	워크플로를 요청하는 사용자의 테넌트입니다.
__asd_subtenantRef	워크플로를 요청하는 사용자의 비즈니스 그룹입니다.
__asd_catalogRequestId	이 워크플로 실행을 위한 카탈로그의 요청 ID입니다.
__asd_requestedFor	요청의 대상 사용자입니다. 특정 사용자를 대신한 요청인 경우 이 사용자는 워크플로를 요청하는 사람을 대신한 사용자이며 그렇지 않으면 워크플로를 요청하는 사용자입니다.
__asd_requestedBy	워크플로를 요청하는 사용자입니다.

XaaS Blueprint 또는 리소스 작업에서 사용자 상호 작용 스키마 요소가 들어 있는 vRealize Orchestrator 워크플로를 사용하는 경우 소비자가 서비스를 요청하면 워크플로는 실행을 일시 중단하고 사용자가 필요한 데이터를 제공할 때까지 기다립니다. 대기 중인 사용자 상호 작용에 응답하기 위해 사용자는 **받은 편지함 > 수동 사용자 작업**으로 이동해야 합니다.

기본 vRealize Orchestrator 서버 인벤토리는 모든 테넌트에서 공유되며 테넌트별로 사용될 수 없습니다. 예를 들어, 서비스 설계자가 클러스터 계산 리소스 생성을 위해 서비스 Blueprint를 생성하는 경우 서로 다른 테넌트의 소비자는 자신이 속한 테넌트와 관계없이 모든 vCenter Server 인스턴스의 인벤토리 항목을 탐색해야 합니다.

시스템 관리자는 vRealize Orchestrator를 설치하거나 vRealize Orchestrator Appliance를 개별적으로 배포하여 외부 vRealize Orchestrator 인스턴스를 설정하고 이 외부 vRealize Orchestrator 인스턴스와 작업하도록 vRealize Automation을 구성할 수 있습니다.

또한 시스템 관리자는 테넌트별로 vRealize Orchestrator 워크플로 범주를 구성하고 각 테넌트에서 사용할 수 있는 워크플로를 정의할 수 있습니다.

이 외에, 테넌트 관리자는 자신의 테넌트에 한정하여 외부 vRealize Orchestrator 인스턴스를 구성할 수도 있습니다.

외부 vRealize Orchestrator 인스턴스 및 vRealize Orchestrator 워크플로 범주 구성에 대한 자세한 내용은 vCenter Orchestrator 및 플러그인 구성을 참조하십시오.

vRealize Orchestrator 플러그인 목록

플러그인을 사용하면 vRealize Orchestrator를 사용하여 외부 기술과 애플리케이션을 액세스하고 제어할 수 있습니다. vRealize Orchestrator 플러그인에서 외부 기술을 노출시킴으로써 외부 기술의 개체와 기능에 액세스하는 워크플로에서 개체와 기능을 통합할 수 있습니다.

플러그인을 사용하여 액세스할 수 있는 외부 기술에는 가상화 관리 도구, 이메일 시스템, 데이터베이스, 디렉토리 서비스, 원격 제어 인터페이스 등이 포함될 수 있습니다.

vRealize Orchestrator 플러그인의 표준 집합을 사용하여 vCenter Server API 및 이메일 기능과 같은 외부 기술을 워크플로에 통합할 수 있습니다. 또한 vRealize Orchestrator 개방형 플러그인 아키텍처를 사용하여 다른 애플리케이션에 액세스하는 플러그인을 개발할 수 있습니다.

표 3-53. vRealize Orchestrator 에 기본적으로 포함되는 플러그인

플러그인	용도
vCenter Server	vCenter Server API에 대한 액세스를 제공하여 모든 vCenter Server 개체와 기능을 vRealize Orchestrator로 자동화하는 관리 프로세스에 통합할 수 있도록 합니다.
구성	vRealize Orchestrator 인증, 데이터베이스 연결, SSL 인증서 등을 구성하기 위한 워크플로를 제공합니다.
vCO Library	클라이언트 프로세스의 사용자 지정 및 자동화를 위한 기본적인 빌딩 블록으로 작동하는 워크플로를 제공합니다. 워크플로 라이브러리에는 수명 주기 관리, 프로비저닝, 재해 복구, 핫 백업 및 기타 표준 프로세스에 대한 템플릿이 포함됩니다. 템플릿을 복사하고 편집하여 필요에 따라 수정할 수 있습니다.
SQL	Java 프로그래밍 언어와 광범위한 데이터베이스 간의 데이터베이스 독립적인 연결을 위한 산업 표준인 JDBC(Java Database Connectivity) API를 제공합니다. 데이터베이스에는 SQL 데이터베이스와 스프레드시트 또는 폴렛 파일과 같은 기타 표 형식 데이터 소스가 포함됩니다. JDBC API는 워크플로에서 SQL 기반 데이터베이스 액세스를 위한 호출 수준 API를 제공합니다.
SSH	SSH-2(보안 셸 v2) 프로토콜에 대한 구현을 제공합니다. 워크플로에서 암호 및 공용 키 기반 인증을 사용하는 원격 명령 및 파일 전송 세션을 허용합니다. 키보드를 사용한 대화형 인증을 지원합니다. 선택적으로 SSH 플러그인은 vRealize Orchestrator 클라이언트 인벤토리에서 직접 원격 파일 시스템 찾아보기를 제공할 수 있습니다.
XML	워크플로에서 구현할 수 있는 완전한 DOM(문서 개체 모델) XML 파서입니다. 또는, vRealize Orchestrator JavaScript API에서 E4X(ECMAScript for XML) 구현을 사용할 수도 있습니다.
Mail	SMTP(Simple Mail Transfer Protocol)를 사용하여 워크플로에서 이메일을 전송합니다.
Net	Jakarta Apache Commons Net 라이브러리를 래핑합니다. Telnet, FTP, POP3 및 IMAP 구현을 제공합니다. POP3와 IMAP는 이메일을 읽는데 사용됩니다. Net 플러그인은 Mail 플러그인과 함께 워크플로에서 완벽한 이메일 전송 및 수신 기능을 제공합니다.
Enumeration	다른 플러그인이 워크플로에서 사용할 수 있는 공통의 열거된 유형을 제공합니다.
Workflow documentation	워크플로 또는 워크플로 범주에 대해 PDF 형식으로 정보를 생성하는 데 사용할 수 있는 워크플로를 제공합니다.
HTTP-REST	vCenter Orchestrator 및 REST 호스트 간 상호 작용을 제공하여 REST 웹 서비스를 관리할 수 있습니다.
SOAP	vCenter Orchestrator 및 SOAP 호스트 간 상호 작용을 제공하여 SOAP 웹 서비스를 관리할 수 있습니다.
AMQP	브로커라고도 하는 AMQP(Advanced Message Queuing Protocol) 서버와 상호 작용할 수 있습니다.

표 3-53. vRealize Orchestrator 에 기본적으로 포함되는 플러그인 (계속)

플러그인	용도
SNMP	vCenter Orchestrator가 SNMP를 사용하도록 설정된 시스템 및 장치에 연결하여 정보를 수신하도록 설정합니다.
Active Directory	vCenter Orchestrator 및 Microsoft Active Directory 간 상호 작용을 제공합니다.
vCO WebOperator	웹 브라우저를 사용하여 vRealize Orchestrator 라이브러리의 워크플로에 액세스하고 네트워크 전체에서 워크플로와 상호 작용할 수 있는 웹 보기입니다.
Dynamic Types	동적 유형을 정의하고 이러한 동적 유형을 생성 및 사용할 수 있습니다.
PowerShell	PowerShell 호스트를 관리하고 사용자 지정 PowerShell 작업을 실행할 수 있습니다.
Multi-Node	계층 오케스트레이션, Orchestrator 인스턴스 관리, Orchestrator 작업의 확장을 위한 워크플로를 포함합니다.
vRealize Automation	vRealize Orchestrator 및 vRealize Automation 간 상호 작용을 위한 워크플로를 생성 및 실행할 수 있습니다.

VMware에서 개발하고 배포하는 vRealize Orchestrator 플러그인에 대한 자세한 내용은 VMware vRealize™ Orchestrator™ 설명서 시작 페이지를 참조하십시오.

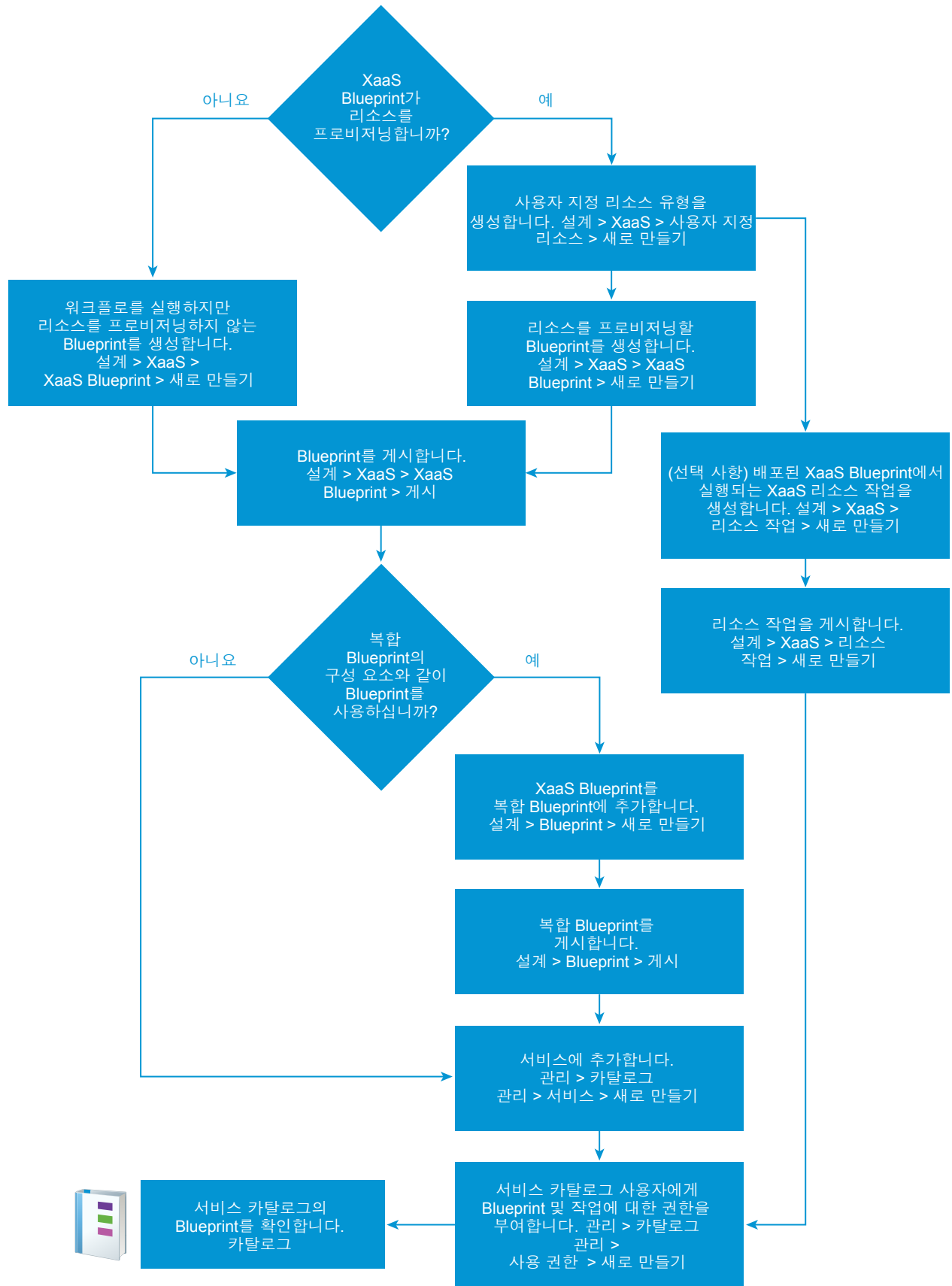
XaaS Blueprint 및 리소스 작업 생성

카탈로그 항목으로 XaaS Blueprint에 대한 사용 권한을 사용자에게 부여하거나 이러한 Blueprint를 설계 캔버스를 사용하여 복합 Blueprint에 구성할 수 있습니다. 항목이 프로비저닝된 후 항목을 관리하기 위해 프로비저닝된 항목에서 리소스 작업을 실행합니다.

예를 들어 XaaS Blueprint를 사용하여 그룹에서 Active Directory 사용자를 생성할 수 있습니다. 그런 다음 사용자의 암호 변경을 위한 리소스 작업을 사용할 수 있습니다.

XaaS Blueprint 워크플로

XaaS Blueprint를 생성하기 위해 따르는 워크플로 및 리소스 작업 선택 사항은 Blueprint를 사용하는 방법에 따라 다릅니다. 다음 워크플로에서는 기본 프로세스를 제공합니다.



XaaS Blueprint 용어

XaaS Blueprint는 리소스를 프로비저닝하거나, 프로비저닝된 리소스를 변경하거나, 환경에서 작업을 수행하는 서비스 역할을 할 수 있는 vRealize Orchestrator 워크플로입니다. Blueprint와 리소스 작업은 서비스 카탈로그 사용자를 위해 Blueprint를 설계할 때 이해하고 있어야 하는 몇 가지 미묘한 차이가 있습니다.

다음 정의는 XaaS Blueprint로 작업할 때 사용되는 용어를 이해하는 데 도움이 됩니다.

사용자 지정 리소스

vRealize Orchestrator 플러그인의 API를 통해 리소스로 표시되는 vRealize Orchestrator 개체 유형입니다. 사용자 지정 리소스를 생성하여 XaaS 프로비저닝 Blueprint의 출력 매개 변수를 정의하고 리소스 작업의 입력 매개 변수를 정의합니다.

XaaS Blueprint 구성 요소

Blueprint 설계 캔버스에서 사용할 수 있는 프로비저닝 또는 비프로비저닝 Blueprint입니다. 이 Blueprint는 독립형 XaaS Blueprint일 수도 있습니다.

독립형 XaaS Blueprint

서비스 카탈로그로 바로 게시되고 이에 대한 사용 권한이 부여되는 프로비저닝 또는 비프로비저닝 Blueprint입니다.

프로비저닝 Blueprint

끝점에 vRealize Orchestrator 플러그인 API를 사용하여 대상 끝점에서 리소스를 프로비저닝하는 vRealize Orchestrator 워크플로를 실행하는 프로비저닝 Blueprint입니다. vSphere에서 네트워크 디바이스에 가상 NIC를 추가하는 경우를 예로 들 수 있습니다. 프로비저닝 Blueprint를 생성하려면 vRealize Orchestrator 리소스 유형을 정의하는 사용자 지정 리소스가 있어야 합니다.

서비스 카탈로그 사용자가 이 유형의 카탈로그 항목을 요청하는 경우 워크플로에서는 항목을 프로비저닝하며 배포된 항목은 **항목** 탭에 저장됩니다. 이 유형의 프로비저닝된 리소스에 대해서는 사후 프로비저닝 작업을 정의할 수 있습니다. 필요에 따라 인스턴스를 추가 또는 제거하여 Blueprint를 확장/축소할 수도 있습니다.

비프로비저닝 Blueprint

비프로비저닝 Blueprint는 vRealize Orchestrator 워크플로를 실행하여 API를 통해 끝점을 변경할 필요가 없는 작업을 수행합니다. 실행되는 워크플로가 보고서를 작성한 후 대상 통신 시스템에 게시하거나 이메일로 보내는 워크플로를 예로 들 수 있습니다.

서비스 카탈로그 사용자가 이 유형의 카탈로그 항목을 요청하는 경우 워크플로가 실행되어 스크립트로 작성된 작업을 수행하지만 항목이 **항목** 탭에 추가되지 않습니다. 이 유형의 Blueprint에 대해서는 사후 프로비저닝 작업을 수행할 수 없습니다. 비프로비저닝 Blueprint는 확장 가능 Blueprint에서 지원 워크플로로 사용할 수 있습니다. 고가용성 로드 밸런서를 업데이트하는 Blueprint를 생성하는 경우를 예로 들 수 있습니다.

복합 Blueprint

설계 캔버스를 사용하여 생성한 Blueprint입니다. 복합 Blueprint에서는 구성 요소를 하나 이상 사용합니다. 구성 요소의 예로는 시스템 구성 요소, 소프트웨어 구성 요소, XaaS 구성 요소 등이 있습니다. 서비스에 추가하면 배포로 나열됩니다. 서비스 카탈로그 사용자가 활용할 수 있도록 사용 권한에 추가하면 복합 Blueprint로 나열됩니다. 복합 Blueprint에는 Blueprint 구성 요소 하나가 있을 수도 있고, 여러 시스템, 소프트웨어 및 네트워킹이 있는 전체 애플리케이션이 포함될 수도 있습니다.

리소스 작업

배포된 프로비저닝 Blueprint에서 실행할 수 있는 워크플로입니다. 배포된 Blueprint는 XaaS Blueprint 또는 Blueprint 구성 요소일 수도 있고, vRealize Orchestrator 리소스 유형에 매핑된 시스템 유형일 수도 있습니다.

XaaS Blueprint 설계 고려 사항

XaaS Blueprint를 생성하기 전에 Blueprint의 의도를 파악해야 리소스를 올바르게 프로비저닝하는 Blueprint를 생성할 수 있습니다.

XaaS Blueprint는 설계 캔버스에서 Blueprint 구성 요소로 생성하여 사용할 수도 있고 독립형 Blueprint로 생성하여 사용할 수도 있습니다. Blueprint는 프로비저닝 Blueprint이거나 비프로비저닝 Blueprint일 수 있습니다.

표 3-54. XaaS Blueprint 유형 및 결과

XaaS Blueprint 유형	사용자 지정 리소스가 필요합니까?	Blueprint를 배포에서 확장/축소할 수 있습니까?	배포된 Blueprint에서 리소스 작업을 실행할 수 있습니까?
리소스를 프로비저닝하는 Blueprint 구성 요소	예	예. 확장/축소하도록 구성되어 있는 경우 배포와 함께 확장/축소됩니다.	예. 배포와 함께 확장/축소되며, 배포된 구성 요소에서 다른 리소스 작업을 실행할 수 있습니다. Blueprint 구성 요소는 [항목] 탭에 표시됩니다.
워크플로를 실행하지만 리소스를 프로비저닝하지 않는 Blueprint 구성 요소	아니요. Blueprint는 vRealize Orchestrator 서버 구성을 사용하지만 XaaS 사용자 지정 리소스가 필요하지는 않습니다.	아니요. 리소스를 프로비저닝하지는 않지만 확장/축소 작업의 일부로 실행할 수 있습니다. 확장/축소 작업을 기반으로 로드 밸런서를 새 구성으로 업데이트하는 경우를 예로 들 수 있습니다.	아니요. 비프로비저닝 구성 요소에서는 리소스 작업을 실행할 수 없습니다.

표 3-54. XaaS Blueprint 유형 및 결과 (계속)

XaaS Blueprint 유형	사용자 지정 리소스가 필요합니까?	Blueprint를 배포에서 확장/축소할 수 있습니까?	배포된 Blueprint에서 리소스 작업을 실행할 수 있습니까?
리소스를 프로비저닝하는 독립형 Blueprint	예	아니요. 인스턴스를 추가 또는 삭제하려면 리소스 작업을 생성해야 합니다.	예. 배포된 리소스에서는 확장/축소를 지원하기 위해 만든 작업을 비롯한 리소스 작업을 실행할 수 있습니다. Blueprint는 [항목] 탭에 표시됩니다.
워크플로를 실행하지만 리소스를 프로비저닝하지 않는 독립형 Blueprint	아니요. Blueprint는 vRealize Orchestrator 서버 구성을 사용하지만 XaaS 사용자 지정 리소스가 필요하지는 않습니다.	아니요. 리소스를 프로비저닝하지는 않지만 리소스 작업의 일부로 실행할 수 있습니다.	아니요. 비프로비저닝 구성 요소에서는 리소스 작업을 실행할 수 없습니다.

XaaS 사용자 지정 리소스 추가

사용자 지정 리소스를 생성하여 프로비저닝을 위한 XaaS 항목을 정의합니다. XaaS Blueprint 또는 작업을 생성하려면 Blueprint 또는 작업 워크플로의 개체 유형과 호환되는 사용자 지정 리소스가 있어야 합니다.

사용자 지정 리소스를 생성하여 vRealize Orchestrator 플러그인의 API를 통해 표시되는 개체 유형을 리소스로 매핑합니다. 사용자 지정 리소스는 프로비저닝을 위한 XaaS Blueprint의 출력 매개 변수를 정의하고 리소스 작업의 입력 매개 변수를 정의합니다.

Blueprint 또는 리소스 작업 워크플로가 리소스를 프로비저닝하지 않거나 배포된 Blueprint에서 실행되는 경우 사용자 지정 리소스를 생성하지 않아도 됩니다. 예를 들어 워크플로가 프로비저닝 작업 후 데이터베이스 값을 업데이트하거나 이메일 메시지를 보내는 경우 사용자 지정 리소스가 없어도 됩니다.

사용자 지정 리소스를 생성하면 프로비저닝된 항목의 세부 정보에서 읽기 전용 양식 필드를 지정할 수 있습니다. [사용자 지정 리소스 양식 설계](#) 항목을 참조하십시오.

필수 조건

- vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.
- 사용자 지정 리소스를 구성하려면 세부적인 옵션 정보를 사용합니다. [XaaS 사용자 지정 리소스 마법사 옵션](#) 항목을 참조하십시오.

프로시저

- 1 설계 > XaaS > 사용자 지정 리소스를 선택합니다.
- 2 새로 만들기 아이콘(+)을 클릭합니다.

3 리소스 유형 탭의 값을 구성합니다.

- a **Orchestrator 유형** 텍스트 상자에서 vRealize Orchestrator 개체 유형을 입력 또는 선택합니다.

예를 들어 문자 v가 포함된 유형을 보려면 v를 입력합니다. 모든 유형을 보려면 빈 칸을 입력합니다.

- b 이름을 입력하고 원하는 경우 설명을 입력합니다.
- c 버전을 입력합니다.

지원되는 형식은 major.minor.micro-revision으로 확장됩니다.

- d 다음을 클릭합니다.

4 필요에 따라 세부 정보 양식 탭을 편집합니다.

요소를 삭제, 편집 및 재정렬하여 사용자 지정 리소스 양식을 편집할 수 있습니다. 또한 양식과 양식 페이지를 추가하고 요소를 새 양식과 양식 페이지에 끌어서 놓을 수 있습니다.

5 완료를 클릭합니다.

사용자 지정 리소스를 생성했습니다. 이 리소스를 [사용자 지정 리소스] 페이지에서 볼 수 있습니다. 이 사용자 지정 리소스를 기반으로 XaaS Blueprint 또는 작업을 생성할 수 있습니다.

후속 작업

- XaaS Blueprint를 생성합니다. [XaaS Blueprint 추가](#) 항목을 참조하십시오.
- XaaS 리소스 작업을 생성합니다. [XaaS 리소스 작업 생성](#) 항목을 참조하십시오.

XaaS 사용자 지정 리소스 마법사 옵션

이러한 사용자 지정 리소스 옵션을 통해 사용자 지정 리소스를 생성하거나 수정하여 리소스를 프로비저닝하거나 프로비저닝된 리소스를 수정하는 XaaS Blueprint 및 리소스 작업 워크플로를 실행할 수 있습니다.

사용자 지정 리소스는 개체 유형당 하나씩만 생성할 수 있습니다. 또한 여러 Blueprint 및 리소스 작업에 대해 사용할 수 있습니다.

사용자 지정 리소스 작업을 생성하려면 **설계 > XaaS > 사용자 지정 리소스**를 선택합니다.

리소스 유형

구성된 vRealize Orchestrator 인스턴스에 설치된 플러그인에 따라 **리소스 유형** 탭에 표시되는 사용 가능한 개체 유형의 목록입니다. vRealize Automation은 구성된 vRealize Orchestrator 인스턴스에서 값을 수집합니다.

표 3-55. 리소스 유형 옵션

옵션	설명
Orchestrator 유형	<p>프로비저닝하는 데 사용하는 워크플로를 지원하는 유형을 입력하거나 선택합니다.</p> <p>이 유형은 스크립팅 API에 나타나는 플러그인 이름(예: vCenter를 뜻하는 VC) 및 개체 유형(예: VirtualMachine)으로 구성됩니다. 이 예에서는 API가 값 VC:VirtualMachine을 사용합니다.</p> <p>이 유형은 Blueprint 워크플로 출력 매개 변수이거나 리소스 작업 워크플로 입력 매개 변수일 수 있습니다.</p>
이름	XaaS Blueprint 또는 리소스 작업을 생성할 때 식별할 수 있도록 정보가 반영된 사용자 지정 리소스 이름을 입력합니다.
설명	세부 정보 표시 설명을 입력합니다.
버전	지원되는 양식은 major.minor.micro-revision으로 확장됩니다.

세부 정보 양식

이러한 양식 필드는 서비스 카탈로그 사용자가 이 사용자 지정 리소스를 사용하는 항목을 프로비저닝할 때 읽기 전용 값으로 나타납니다. 기존 필드를 수정하고 외부에서 정의된 새 필드를 추가할 수 있습니다.

양식 구성에 대한 자세한 내용은 [사용자 지정 리소스 양식 설계](#) 항목을 참조하십시오.

사용된 위치

개체 유형당 사용자 지정 리소스를 하나만 생성할 수 있기 때문에 마법사의 이 페이지를 통해 사용자 지정 리소스가 사용되는 방식을 파악할 수 있습니다.

이 탭은 저장된 사용자 지정 리소스에 대해 사용할 수 있으며, 리소스를 생성할 때는 표시되지 않습니다.

표 3-56. 사용된 위치 옵션

옵션	설명
XaaS Blueprint	<p>이 사용자 지정 리소스를 사용하도록 구성된 Blueprint의 목록입니다.</p> <p>이 페이지에서는 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 편집. Blueprint를 열어 구성을 확인하거나 수정할 수 있습니다. ■ 게시/게시 취소. 복합 Blueprint에서 사용하거나 서비스에 추가할 수 있도록 하여 Blueprint의 상태를 변경합니다. Blueprint의 게시를 취소하는 경우 복합 Blueprint에서 사용할 수 없도록 하거나, 서비스에 추가하거나, 서비스 카탈로그에서 사용할 수 없도록 할 수 있습니다. ■ 삭제. 시스템에서 이 Blueprint를 제거합니다.
리소스 작업	<p>이 사용자 지정 리소스를 사용하도록 구성된 리소스 작업의 목록입니다.</p> <p>이 페이지에서는 다음 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 편집. 리소스 작업을 열어 구성을 확인하거나 수정할 수 있습니다. ■ 게시/게시 취소. 사용 권한에서 사용할 수 있도록 하여 리소스 작업의 상태를 변경합니다. 리소스 작업의 게시를 취소하는 경우 서비스에 추가할 수 없도록 하거나, 배포된 Blueprint에서 실행할 수 없도록 할 수 있습니다. ■ 삭제. 시스템에서 이 리소스 작업을 제거합니다.

XaaS Blueprint 생성

XaaS Blueprint는 프로비저닝 또는 비 프로비저닝 Blueprint입니다. 제공된 vRealize Orchestrator 프로비저닝 워크플로의 일부에는 가상 시스템 생성, Active Directory에 사용자 추가 또는 가상 시스템 스냅샷 생성이 포함됩니다. 귀하가 생성할 수 있는 비 프로비저닝 워크플로 중 일부에는 로드 밸런서를 업데이트하거나 보고서를 작성해 받는 사람에게 보내는 작업이 포함됩니다.

vRealize Orchestrator에서 제공되는 워크플로를 기반으로 XaaS Blueprint를 생성하거나 자신의 환경과 관련된 목표를 달성하기 위해 생성하는 워크플로를 사용할 수 있습니다.

프로시저

1 XaaS Blueprint 추가

XaaS Blueprint는 귀하의 환경에서 대상 시스템을 변경하는 vRealize Orchestrator 워크플로를 실행하기 위한 규격입니다. 이 Blueprint에는 상기 워크플로가 포함되며, 이 워크플로는 입력 매개 변수, 제출 및 읽기 전용 양식, 작업 시퀀스, 그리고 프로비저닝 작업이나 비 프로비저닝 작업을 포함할 수 있습니다.

2 복합 Blueprint에 XaaS Blueprint 추가

설계 캔버스에 다른 Blueprint 구성 요소를 추가하는 방법과 유사하게 XaaS Blueprint를 복합 Blueprint의 구성 요소로 추가합니다.

XaaS Blueprint 추가

XaaS Blueprint는 귀하의 환경에서 대상 시스템을 변경하는 vRealize Orchestrator 워크플로를 실행하기 위한 규격입니다. 이 Blueprint에는 상기 워크플로가 포함되며, 이 워크플로는 입력 매개 변수, 제출 및 읽기 전용 양식, 작업 시퀀스, 그리고 프로비저닝 작업이나 비 프로비저닝 작업을 포함할 수 있습니다.

다음 중 한 가지 이상의 방법으로 사용할 XaaS Blueprint를 생성할 수 있습니다.

- XaaS Blueprint 구성 요소를 생성합니다. 구성 요소 Blueprint는 복합 Blueprint의 일부로서 Blueprint 설계 캔버스에서 사용할 수 있는 프로비저닝 또는 비 프로비저닝 Blueprint입니다. 이 Blueprint를 구성 요소로 사용할 경우 배포되는 복합 Blueprint에서 축소 및 확장 작업을 지원하는 구성 요소 수명 주기 옵션을 구성해야 합니다.

이 Blueprint 유형은 독립형 Blueprint로 게시될 수도 있습니다.

- 독립형 XaaS Blueprint를 생성합니다. 독립형 Blueprint는 서비스 카탈로그에 직접 게시되고 권한이 부여되는 프로비저닝 또는 비 프로비저닝 Blueprint입니다.

XaaS Blueprint를 사용하여 Active Directory 사용자를 만드는 방법을 보여 주는 예는 [사용자 생성 및 수정을 위해 XaaS Blueprint 및 작업 생성](#) 항목을 참조하십시오.

필수 조건

- vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.
- Blueprint가 리소스를 프로비저닝해야 하는 경우, 서비스 Blueprint의 출력 매개 변수에 해당하는 사용자 지정 리소스를 생성합니다. [XaaS 사용자 지정 리소스 추가](#) 항목을 참조하십시오. 이 Blueprint가 vRealize Orchestrator 플러그인 API를 사용하지 않는 경우에는 사용자 지정 리소스를 구성할 필요가 없습니다.
- XaaS Blueprint를 생성하여 vRealize Orchestrator 워크플로를 잠재적인 구성 요소 Blueprint 또는 카탈로그 항목으로 게시합니다. Blueprint는 귀하가 편집할 수 있는 양식을 포함합니다. [XaaS Blueprint 양식 설계](#) 항목을 참조하십시오.
- 자세한 옵션 정보를 사용하여 Blueprint를 구성합니다. [XaaS Blueprint 새로 만들기 또는 편집 마법사 옵션](#) 항목을 참조하십시오.

프로시저

- 1 **설계 > XaaS > XaaS Blueprint**를 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 **워크플로** 탭에서 Blueprint가 리소스를 프로비저닝할 때 실행되는 워크플로를 선택합니다.

Blueprint를 편집할 경우에는 이 탭을 사용할 수 없습니다.

- a vRealize Orchestrator 워크플로 라이브러리에서 탐색하여 사용자 지정 리소스에 관련된 워크플로를 선택합니다.
- b 나중에 정확한 값을 제공할 수 있도록 입력 및 출력 매개 변수를 검토하십시오.
- c **다음**을 클릭합니다.

4 일반 탭에서 옵션을 구성하고 다음을 클릭합니다.

- 이름 텍스트 상자에는 이 Blueprint를 유사한 Blueprint와 구분하는 이름을 입력합니다.
- 이 Blueprint를 복합 Blueprint의 구성 요소로 사용하지 않으려면 **설계 캔버스에서 구성 요소로 사용할 수 있도록 설정** 확인란을 선택 취소합니다.

5 Blueprint 양식 탭에서 필요에 따라 양식을 편집하고 다음을 클릭합니다.

6 프로비저닝된 리소스 페이지에서 값을 선택하고 다음을 클릭합니다.

옵션	설명
프로비저닝 없음	워크플로가 리소스를 프로비저닝하지 않을 경우 이 옵션을 선택하거나 필드를 비워둔 채로 둘 수 있습니다.
<이전에 생성한 사용자 지정 리소스>	이 프로비저닝 워크플로를 지원하는 사용자 지정 리소스를 선택합니다.

7 구성 요소 수명 주기 탭에서 축소, 확장 및 삭제 작업 중 이 Blueprint의 동작 방식을 정의합니다.

이러한 워크플로는 이 Blueprint를 구성 요소로 포함하는 배포된 복합 Blueprint에서 실행됩니다. 다양한 옵션의 가용성은 Blueprint에 따라 다릅니다. 모든 Blueprint 워크플로에서 모든 옵션을 지원하거나 요구하는 것은 아닙니다.

8 완료를 클릭합니다.

9 Blueprint에 대한 행을 선택하고 게시를 클릭합니다.

XaaS Blueprint가 생성되고 게시됩니다.

후속 작업

- 이 Blueprint를 서비스 카탈로그에 독립형 Blueprint로 직접 추가하려면 서비스를 추가하고 서비스에 Blueprint를 추가하십시오. [서비스 추가](#) 항목을 참조하십시오.
- 이 Blueprint를 복합 Blueprint의 한 구성 요소로 사용하는 방법은 [복합 Blueprint에 XaaS Blueprint 추가](#) 항목을 참조하십시오.

XaaS Blueprint 새로 만들기 또는 편집 마법사 옵션

이러한 옵션을 사용하여 Blueprint가 배포될 때 vRealize Orchestrator 워크플로를 실행하는 XaaS Blueprint를 생성할 수 있습니다. 이 워크플로를 통해 환경의 대상 시스템이 변경됩니다.

Blueprint를 생성하기 위해 수행하는 단계에 대해서는 [XaaS Blueprint 추가](#) 항목을 참조하십시오.

이 마법사를 사용하려면 **설계 > XaaS > XaaS Blueprint**를 선택합니다.

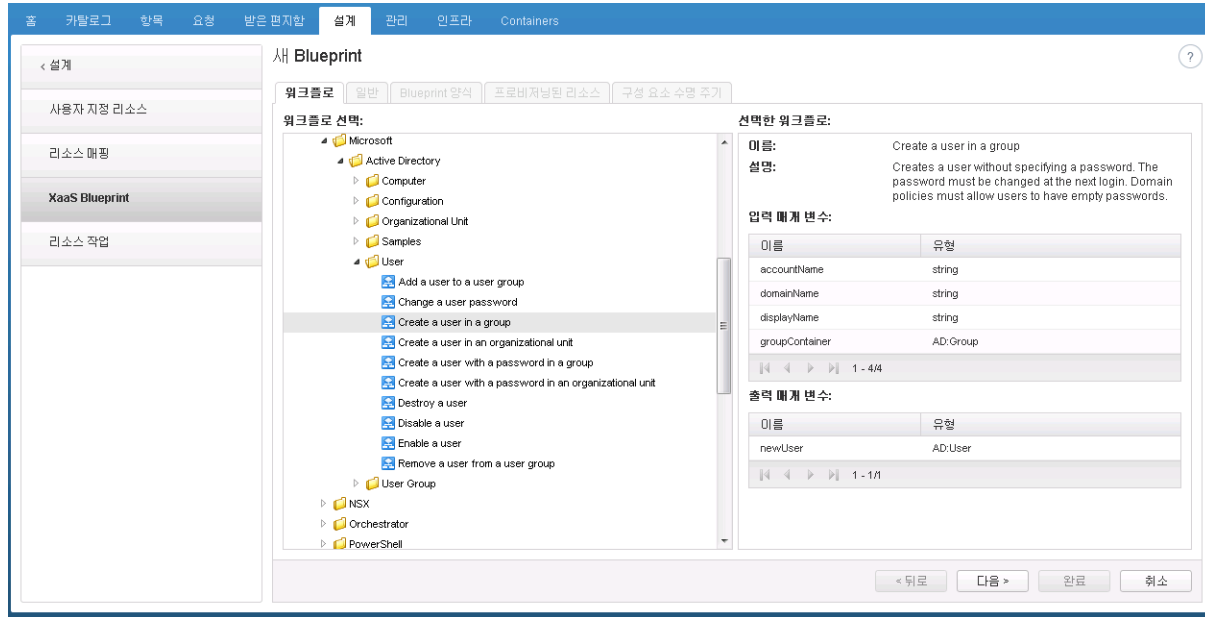
워크플로 탭

Blueprint가 리소스를 프로비저닝할 때 실행되는 워크플로를 선택합니다.

Blueprint를 편집할 경우에는 이 탭을 사용할 수 없습니다.

다음 그림에서 워크플로 트리는 왼쪽에, 매개 변수는 오른쪽에 있습니다.

그림 3-4. XaaS Blueprint 마법사의 워크플로 탭



입력 및 출력 매개 변수를 검토하여 자신 또는 서비스 카탈로그 사용자가 다음과 같은 상황에서 올바른 값을 제공할 수 있는지 확인합니다.

- 이 마법사 또는 Blueprint 설계 캔버스에서 Blueprint 양식을 사용자 지정하는 경우.
- 모든 입력 매개 변수를 비워 두는 경우 서비스 카탈로그 사용자가 값을 설정할 수 있습니다.

일반 탭

Blueprint의 동작에 대한 메타데이터를 구성합니다.

표 3-57. 일반 탭 옵션

옵션	설명
이름	<p>다음 위치에 나타나도록 하려는 Blueprint의 이름입니다.</p> <ul style="list-style-type: none"> ■ 설계 캔버스. [설계 캔버스에서 구성 요소로 사용하도록 설정]을 선택하는 경우 이 값은 범주 목록에 표시되는 이름입니다. ■ 서비스. 이 Blueprint를 독립형 Blueprint로 사용하는 경우 이 값은 서비스에 카탈로그 항목을 추가할 때 표시되는 이름입니다. ■ 사용 권한. Blueprint에 개별 항목으로 사용 권한을 부여하는 경우 이 값은 [항목 추가] 목록에 표시되는 이름입니다.
설명	<p>비슷한 항목을 구분하는 데 도움이 되는 세부 정보 표시 설명을 제공합니다.</p>
카탈로그 요청 정보 페이지 숨기기	<p>서비스 카탈로그 소비자가 항목을 요청할 때 설명과 이유를 제공할 필요가 없도록 하려면 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있습니다.</p>

표 3-57. 일반 탭 옵션 (계속)

옵션	설명
버전	지원되는 형식은 major.minor.micro-revision으로 확장됩니다.
설계 캔버스에서 구성 요소로 사용할 수 있도록 설정	<p>Blueprint를 설계 캔버스 Blueprint에서 구성 요소로 사용하려는 경우 이 옵션을 선택합니다.</p> <p>게시된 Blueprint는 사용자 지정 리소스를 구성할 때 선택한 범주에서 사용할 수 있습니다.</p> <p>이 옵션을 선택하지 않으면 Blueprint가 설계 캔버스에 나타나지 않습니다. 하지만 계속해서 서비스에 추가하고 독립형 Blueprint로 배포하도록 사용자에게 사용 권한을 부여할 수 있습니다.</p>

Blueprint 양식 탭

마법사의 이 페이지에 표시되는 필드는 워크플로 입력 매개 변수입니다. 다음과 같은 변경 작업을 하나 이상 수행할 수 있습니다.

- 필드를 양식에 추가합니다.
- 필드를 삭제 또는 재정렬하여 기존 필드를 수정합니다.
- 기본값을 입력 매개 변수로 제공합니다.

변경 내용은 다음에 대상에게 제공되는 양식에 영향을 줍니다.

- 이 XaaS Blueprint가 Blueprint 구성 요소로 사용되는 경우 설계 캔버스에서 작업하는 애플리케이션 설계자.
- 이 Blueprint가 독립형 Blueprint로 게시되는 경우 서비스 카탈로그 사용자.

양식 구성에 대한 자세한 내용은 [XaaS Blueprint 양식 설계](#) 항목을 참조하십시오.

프로비저닝된 리소스

프로비저닝된 리소스는 **설계 > XaaS > 사용자 지정 리소스**의 [사용자 지정 리소스] 페이지에서 구성한 관련된 XaaS 사용자 지정 리소스에 Blueprint를 연결합니다.

표 3-58. 프로비저닝된 리소스 옵션

옵션	설명
이전에 생성한 사용자 지정 리소스	<p>프로비저닝 Blueprint를 실행하는 데 필요한 vRealize Orchestrator 리소스 유형을 정의하는 사용자 지정 리소스를 선택합니다.</p> <p>프로비저닝 Blueprint는 끝점에 vRealize Orchestrator 플러그인 API를 사용하여 대상 끝점에서 리소스를 프로비저닝하는 vRealize Orchestrator 워크플로를 실행합니다. vSphere에서 네트워크 디바이스에 가상 NIC를 추가하는 경우를 예로 들 수 있습니다.</p> <p>이 유형의 프로비저닝된 리소스에 대해서는 사후 프로비저닝 작업을 정의할 수 있습니다. 필요에 따라 인스턴스를 추가 또는 제거하여 Blueprint를 확장/축소할 수도 있습니다.</p> <p>결과</p> <ul style="list-style-type: none"> ■ Blueprint를 확장/축소할 수 있습니다. ■ Blueprint가 설계 캔버스에서 선택한 사용자 지정 리소스에 대해 지정된 범주에 나타납니다. ■ Blueprint는 이를 포함하는 Blueprint를 배포할 때 항목 탭에 표시되며, 배포 후에는 항목에 대해 어떤 작업이든 실행할 수 있습니다.
프로비저닝 없음	<p>비프로비저닝 Blueprint는 vRealize Orchestrator 워크플로를 실행하여 API를 통해 끝점을 변경할 필요가 없는 작업을 수행합니다. 보고서를 작성하고 대상 통신 시스템에 게시하거나 이메일로 보내는 경우를 예로 들 수 있습니다.</p> <p>결과</p> <ul style="list-style-type: none"> ■ Blueprint를 확장/축소할 수 없습니다. 비프로비저닝 Blueprint는 확장 가능 Blueprint에서 지원 워크플로로 사용할 수 있습니다. 고가용성 로드 밸런서를 업데이트하는 Blueprint를 생성하는 경우를 예로 들 수 있습니다. ■ Blueprint는 설계 캔버스에서 XaaS 범주에 표시됩니다. ■ Blueprint는 이를 포함하는 Blueprint를 배포할 때 항목 탭에 표시되지 않을 뿐 아니라, 배포 후에 항목에 대해 어떤 작업도 실행할 수 없습니다.

구성 요소 수명 주기 탭

[구성 요소 수명 주기] 탭은 **일반** 탭에서 **설계 캔버스에서 구성 요소로 사용할 수 있도록 설정**을 선택한 경우에 사용할 수 있습니다.

이러한 옵션을 통해 이 Blueprint가 복합 Blueprint에서 구성 요소로 사용되는 경우 확장/축소 작업 도중 배포 후 작업을 처리하는 방식을 지정합니다.

각 옵션의 사용 가능 여부는 Blueprint에 따라 다릅니다. 모든 Blueprint 워크플로에서 모든 옵션을 지원하거나 요구하는 것은 아닙니다. XaaS는 복합 Blueprint에서 사용될 수도 있기 때문에 Blueprint가 올바르게 확장/축소되도록 하려면 업데이트 및 삭제 옵션은 물론, 할당 및 할당 해제 옵션(Blueprint에 사용할 수 있는 경우)도 구성해야 합니다.

표 3-59. 구성 요소 수명 주기 옵션

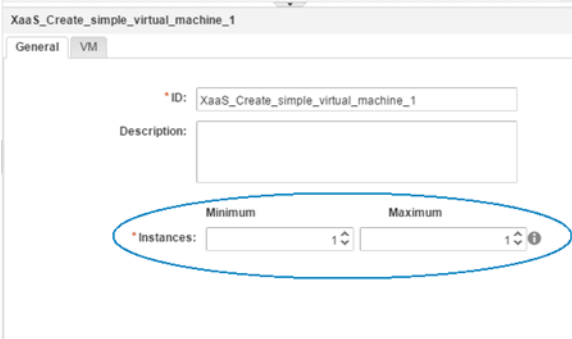
옵션	설명
확장 가능	<p>이 옵션을 선택하여 배포 후 축소 또는 확장 작업 도중 서비스 카탈로그 사용자가 이 Blueprint 구성 요소의 인스턴스 수를 변경할 수 있습니다.</p> <p>이 옵션은 [프로비저닝된 리소스] 탭에서 사용자 지정 리소스를 선택한 경우에 사용할 수 있습니다. [프로비저닝 없음] 옵션을 선택한 경우에는 사용할 수 없습니다.</p> <p>이 Blueprint를 확장/축소할 수 있도록 설정하면 설계 캔버스의 [일반] 탭에 [인스턴스] 옵션이 추가됩니다. 아래의 예를 참조하십시오. [확장 가능]을 선택하지 않으면 설계 캔버스에서 [인스턴스] 옵션을 사용할 수 없습니다.</p> 
프로비저닝 워크플로	<p>프로비저닝 또는 확장 작업 도중 실행되는 워크플로입니다. 이 워크플로는 이 Blueprint를 생성할 때 선택된 것이며, 값을 편집할 수는 없습니다.</p>
할당 워크플로	<p>모든 초기 프로비저닝 또는 확장 작업 이전에 실행되는 워크플로를 선택합니다.</p> <p>이 수명 주기 워크플로 유형은 Azure 할당에 사용할 수 있습니다. 확장/축소 작업에 대한 할당 워크플로를 생성하는 경우 다음 값을 포함해야 합니다.</p> <ul style="list-style-type: none"> ■ 입력 매개 변수 <ul style="list-style-type: none"> ■ 매개 변수 이름은 requestData이고 매개 변수 유형은 Properties입니다. ■ 매개 변수 이름은 subtenant이고 매개 변수 유형은 Properties입니다. ■ reservations 및 매개 변수 유형은 Arrays/Properties입니다. ■ 출력 매개 변수 <ul style="list-style-type: none"> ■ 매개 변수 유형이 Properties인 경우 매개 변수를 포함해야 합니다.

표 3-59. 구성 요소 수명 주기 옵션 (계속)

옵션	설명
업데이트 워크플로	<p>구성 요소를 확장/축소할 수 없지만 업데이트할 수 있는 경우 확장 또는 축소 작업을 포함하여 업데이트 작업 도중 실행되는 워크플로를 선택합니다.</p> <p>예를 들어 복합 Blueprint에 있는 구성 요소의 경우 확장 또는 축소 작업을 통해 생성된 새 구성으로 로드 밸런서가 업데이트됩니다.</p> <p>업데이트 워크플로는 확장/축소된 구성 요소에 바인딩되어 있지만 그 자체를 확장/축소할 수는 없는 구성 요소에 적용될 수 있습니다. 이 업데이트 워크플로는 업데이트 작업을 토대로 확장/축소가 불가능한 구성 요소를 변경합니다.</p> <p>확장/축소 작업에 대한 업데이트 워크플로를 생성하는 경우 다음 값을 포함해야 합니다.</p> <ul style="list-style-type: none"> ■ 입력 매개 변수. <ul style="list-style-type: none"> ■ 매개 변수의 이름과 관계없이 프로비저닝 워크플로의 출력 매개 변수 유형과 일치하는 매개 변수를 포함해야 합니다. ■ 매개 변수 이름은 data이고 매개 변수 유형은 Properties입니다.
삭제 워크플로	<p>축소 또는 삭제 작업 도중 실행되는 워크플로를 선택합니다.</p> <p>확장/축소 작업에 대한 삭제 워크플로를 생성하는 경우 다음 값을 포함해야 합니다.</p> <ul style="list-style-type: none"> ■ 입력 매개 변수. <ul style="list-style-type: none"> ■ 매개 변수의 이름과 관계없이 프로비저닝 워크플로의 출력 매개 변수 유형과 일치하는 매개 변수를 포함해야 합니다. <p>예를 들어 [단순한 가상 시스템 프로비저닝 워크플로 생성]에 출력 매개 변수 VC:VirtualMachine이 포함되어 있으면 삭제 워크플로에는 유형이 VC:VirtualMachine인 입력 매개 변수가 포함되어 있어야 합니다.</p>
할당 해제 워크플로	<p>삭제 또는 축소 작업 후에 실행되는 워크플로를 선택합니다.</p> <p>작업 도중 할당 해제가 실패하더라도 삭제 워크플로는 예상대로 계속 실행됩니다.</p> <p>할당 해제는 복합 Blueprint를 축소 또는 삭제하는 경우 수행하는 마지막 프로세스입니다. 이 프로세스는 삭제 작업 후 실행되어 리소스를 해제합니다.</p> <p>이 수명 주기 워크플로 유형은 Azure 할당에 사용할 수 있습니다. 확장/축소 작업에 대한 할당 해제 워크플로를 생성하는 경우 다음 값을 포함해야 합니다.</p> <ul style="list-style-type: none"> ■ 입력 매개 변수. <ul style="list-style-type: none"> ■ 매개 변수 이름은 data이고 매개 변수 유형은 Properties입니다.
범주	<p>설계 캔버스에서 XaaS Blueprint가 표시되는 위치를 지정하려면 설계 캔버스 범주 드롭다운 메뉴에서 값을 선택합니다.</p> <p>범주를 선택하지 않으면 계시된 Blueprint가 XaaS 범주에 추가됩니다.</p>

복합 Blueprint에 XaaS Blueprint 추가

설계 캔버스에 다른 Blueprint 구성 요소를 추가하는 방법과 유사하게 XaaS Blueprint를 복합 Blueprint의 구성 요소로 추가합니다.

이 방법을 사용하여 XaaS를 복합 Blueprint에 추가합니다. 이 Blueprint가 애플리케이션 Blueprint를 구성하는 유일한 Blueprint 구성 요소일 수도 있고, 여러 구성 요소 중 하나일 수도 있습니다.

사용자에게 XaaS Blueprint만 제공하려는 경우 이 Blueprint를 복합 Blueprint에 추가하지 않고 서비스에 추가한 다음 사용자에게 Blueprint에 대한 사용 권한을 부여할 수 있습니다.

배포된 애플리케이션 Blueprint에서 축소 및 확장 작업을 실행하는 경우 XaaS Blueprint의 규모는 Blueprint 수명 주기 옵션의 구성 방식에 따라 결정됩니다.

필수 조건

- vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.
- XaaS Blueprint를 생성하고 발행합니다. [XaaS Blueprint 생성](#) 항목을 참조하십시오. Blueprint를 만들 때 설계 캔버스에서 Blueprint의 위치를 나타내는 범주를 지정했습니다.
- 복합 Blueprint에서 XaaS Blueprint 양식을 사용자 지정하는 방법을 검토합니다. [XaaS Blueprint 및 작업을 위한 양식 설계](#) 항목을 참조하십시오.

프로시저

- 1 **설계 > Blueprint**를 선택합니다.
- 2 XaaS를 추가하려는 Blueprint의 이름을 선택합니다.
설계 캔버스가 나타납니다. 여기에는 현재 애플리케이션 구성 요소 Blueprint와 기타 구성 요소가 들어 있습니다.
- 3 [범주] 목록에서 Blueprint를 찾습니다.
- 4 Blueprint를 캔버스로 끕니다.
- 5 [일반] 및 [생성] 탭에서 기본값을 구성합니다.
이러한 값은 사용자가 항목을 요청할 때 서비스 카탈로그 양식에 나타나는 기본 값입니다.
- 6 **완료**를 클릭합니다.
- 7 Blueprint를 선택하고 **게시**를 클릭합니다.

이제 XaaS Blueprint가 복합 Blueprint의 일부가 되었습니다.

후속 작업

복합 Blueprint를 서비스에 추가합니다. [서비스 카탈로그 관리](#) 항목을 참조하십시오.

XaaS 리소스 작업 생성

vRealize Orchestrator 워크플로를 사용하여 프로비저닝된 항목을 관리할 수 있도록 리소스 작업을 생성합니다.

필수 조건

- vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.
- 작업을 지원하는 사용자 지정 리소스가 있는지 확인합니다. [XaaS 사용자 지정 리소스 추가](#) 항목을 참조하십시오.
- XaaS 카탈로그 항목으로 프로비저닝되지 않은 항목에서 실행할 작업을 생성 중인 경우에는 대상 리소스를 매핑했는지 확인합니다. [XaaS 리소스 작업에 대해 작업하기 위해 다른 리소스 매핑](#) 항목을 참조하십시오.

프로시저

1 리소스 작업 생성

리소스 작업은 서비스 카탈로그 사용자가 프로비저닝된 카탈로그 항목에서 실행할 수 있는 XaaS 워크플로입니다. XaaS 설계자는 리소스 작업을 생성하여 소비자가 프로비저닝된 항목에 대해 수행할 수 있는 작업을 정의할 수 있습니다.

2 리소스 작업 게시

새로 생성한 리소스 작업은 초안 상태이며, 리소스 작업을 게시해야 합니다.

3 XaaS 리소스 작업에 아이콘 할당

리소스 작업을 생성하고 게시한 후 이 작업을 편집하고 이 작업에 아이콘을 할당할 수 있습니다.

리소스 작업 생성

리소스 작업은 서비스 카탈로그 사용자가 프로비저닝된 카탈로그 항목에서 실행할 수 있는 XaaS 워크플로입니다. XaaS 설계자는 리소스 작업을 생성하여 소비자가 프로비저닝된 항목에 대해 수행할 수 있는 작업을 정의할 수 있습니다.

리소스 작업을 생성함으로써 vRealize Orchestrator 워크플로를 사후 프로비저닝 작업으로 연결합니다. 이 프로세스 동안 기본 제출 양식과 읽기 전용 양식을 편집할 수 있습니다. [리소스 작업 양식 설계](#) 항목을 참조하십시오.

필수 조건

- vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.
- 리소스 작업의 입력 매개 변수에 해당하는 사용자 지정 리소스를 생성합니다.

프로시저

1 설계 > XaaS > 리소스 작업을 선택합니다.

2 새로 만들기 아이콘(+)을 클릭합니다.

3 vRealize Orchestrator 워크플로 라이브러리에서 탐색하여 사용자 지정 리소스에 관련된 워크플로를 선택합니다.

vRealize Orchestrator에서 정의된 대로, 선택한 워크플로의 이름과 설명 및 입력과 출력 매개 변수를 볼 수 있습니다.

4 다음을 클릭합니다.

- 5 이전에 **리소스 유형** 드롭다운 메뉴에서 생성한 사용자 지정 리소스를 선택합니다.
- 6 **입력 매개 변수** 드롭다운 메뉴에서 리소스 작업에 대한 입력 매개 변수를 선택합니다.
- 7 **다음**을 클릭합니다.
- 8 이름을 입력하고 원하는 경우 설명을 입력합니다.

이름 및 설명 텍스트 상자에는 vRealize Orchestrator에서 정의된 대로 워크플로의 이름과 설명이 미리 채워져 있습니다.

- 9 (선택 사항) 이 리소스 작업 요청에 대한 설명과 이유를 입력하라는 메시지가 소비자에게 나타나지 않게 하려면 **카탈로그 요청 정보 페이지 숨기기 페이지** 확인란을 선택합니다.
- 10 버전을 입력합니다.
지원되는 형식은 major.minor.micro-revision으로 확장됩니다.
- 11 (선택 사항) 작업 유형을 선택합니다.

옵션	설명
삭제	리소스 작업 워크플로의 입력 매개 변수가 삭제되고 해당 항목이 항목 탭에서 제거됩니다. 예를 들어 리소스 작업이 프로비저닝된 시스템을 삭제하기 위한 것입니다.
프로비저닝	리소스 작업이 프로비저닝하기 위한 것입니다. 예를 들어 리소스 작업이 카탈로그 항목을 복사하기 위한 것입니다. 드롭다운 메뉴에서 출력 매개 변수를 선택합니다. 소비자가 이 리소스 작업을 요청할 때 프로비저닝된 항목이 항목 탭에 추가되도록 사용자 지정 리소스를 선택할 수 있습니다. 프로비저닝 없음 옵션만 있는 경우 리소스 작업이 프로비저닝을 위한 것이 아니거나 출력 매개 변수를 위한 올바른 사용자 지정 리소스를 생성한 것이 아니므로 계속 진행할 수 없습니다.

작업 워크플로에 따라 옵션 중 하나 또는 둘 다를 선택할 수 있거나 어느 것도 선택하지 못할 수 있습니다.

- 12 리소스 작업이 사용자에게 사용 가능한 조건을 선택하고 **다음**을 클릭합니다.
- 13 (선택 사항) **양식** 탭에서 리소스 작업 양식을 편집합니다.

리소스 작업 양식은 vRealize Orchestrator 워크플로 프레젠테이션을 매핑합니다. 요소를 삭제, 편집 및 재정렬하여 양식을 변경할 수 있습니다. 또한 새 양식 및 양식 페이지를 추가하고 필요한 요소를 새 양식 및 양식 페이지에 끌어서 놓습니다.

옵션	작업
양식 추가	양식 이름 옆의 새 양식 아이콘(+)을 클릭하고 필수 정보를 제공하고 제출 을 클릭합니다.
양식 편집	양식 이름 옆의 편집 아이콘(✎)을 클릭하고 필요한 내용을 변경하고 제출 을 클릭합니다.
워크플로 프레젠테이션 재생성	양식 이름 옆의 재구축 아이콘(🔄)을 클릭하고 확인 을 클릭합니다.
양식 삭제	양식 이름 옆의 삭제 아이콘(✖)을 클릭하고 확인 대화 상자에서 확인 을 클릭합니다.

옵션	작업
양식 페이지 추가	양식 페이지 이름 옆의 새 페이지 아이콘(+)을 클릭하고 필수 정보를 제공하고 제출 을 클릭합니다.
양식 페이지 편집	양식 페이지 이름 옆의 편집 아이콘(✎)을 클릭하고 필요한 내용을 변경하고 제출 을 클릭합니다.
양식 페이지 삭제	양식 이름 옆의 삭제 아이콘(✖)을 클릭하고 확인 대화 상자에서 확인 을 클릭합니다.
양식 페이지에 요소 추가	왼쪽의 새 필드 창에서 요소를 끌어서 오른쪽의 창에 놓습니다. 그런 다음 필수 정보를 제공하고 제출 을 클릭할 수 있습니다.
요소 편집	편집할 요소 옆의 편집 아이콘(✎)을 클릭하고 필요한 내용을 변경하고 제출 을 클릭합니다.
요소 삭제	삭제할 요소 옆의 삭제 아이콘(✖)을 클릭하고 확인 대화 상자에서 확인 을 클릭합니다.

14 완료를 클릭합니다.

리소스 작업을 생성했습니다. 이 리소스 작업을 리소스 작업 페이지에서 볼 수 있습니다.

후속 작업

리소스 작업을 게시합니다. [리소스 작업 게시](#) 항목을 참조하십시오.

리소스 작업 게시

새로 생성한 리소스 작업은 초안 상태이며, 리소스 작업을 게시해야 합니다.

필수 조건

vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.

프로시저

- 1 **설계 > XaaS > 리소스 작업**을 선택합니다.
- 2 리소스 작업에 해당하는 행을 선택하고 **게시**를 클릭합니다.

리소스 작업의 상태가 [게시됨]으로 변경됩니다.

후속 작업

리소스 작업에 아이콘을 할당합니다. [XaaS 리소스 작업에 아이콘 할당](#)를 참조하십시오. 이렇게 하면 비즈니스 그룹 관리자와 테넌트 관리자가 사용 권한을 생성할 때 해당 작업을 사용할 수 있습니다.

XaaS 리소스 작업에 아이콘 할당

리소스 작업을 생성하고 게시한 후 이 작업을 편집하고 이 작업에 아이콘을 할당할 수 있습니다.

필수 조건

vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.

프로시저

- 1 **관리 > 카탈로그 관리 > 작업**을 선택합니다.
- 2 생성한 리소스 작업을 선택합니다.
- 3 **구성**을 클릭합니다.
- 4 **찾아보기**를 클릭하고 추가할 아이콘을 선택합니다.
- 5 **열기**를 클릭합니다.
- 6 **업데이트**를 클릭합니다.

리소스 작업에 아이콘을 할당했습니다. 비즈니스 그룹 관리자 및 테넌트 관리자는 사용 권한의 리소스 작업을 사용할 수 있습니다.

XaaS 리소스 작업에 대해 작업하기 위해 다른 리소스 매핑

XaaS로 프로비저닝되지 않은 항목을 매핑하여 그러한 항목에서 실행되도록 리소스 작업을 실행할 수 있습니다.

리소스 매핑 스크립트 작업 및 워크플로

vSphere, vCloud Director 또는 vCloud Air 가상 시스템에 대해 제공된 리소스 매핑을 사용하거나 사용자 지정 vRealize Orchestrator 스크립트 작업 또는 워크플로를 생성하여 다른 vRealize Automation 카탈로그 리소스 유형을 vRealize Orchestrator 인벤토리 유형에 매핑할 수 있습니다.

vRealize Automation 와 함께 제공되는 리소스 매핑

vRealize Automation에는 IaaS vSphere 가상 시스템, IaaS vCloud Director 및 배포를 위한 리소스 매핑이 포함되어 있습니다.

vRealize Automation에는 제공된 XaaS 리소스 매핑 각각에 대한 vRealize Orchestrator 리소스 매핑 스크립트 작업이 포함되어 있습니다. 제공된 리소스 매핑에 대한 스크립트 작업은 포함된 vRealize Orchestrator 서버의 `com.vmware.vcac.asd.mappings` 패키지에 위치해 있습니다.

입력 매개 변수 `VCACAFE:CatalogResource`와 함께 vRealize Orchestrator 워크플로를 사용하는 배포된 복합 Blueprint에서 실행되는 리소스 작업을 생성할 때 [배포] 매핑이 입력 리소스 유형으로 적용됩니다. [배포] 매핑은 선택된 워크플로에 입력 매개 변수로 `VCACAFE:CatalogResource`가 포함되어 있는 경우에만 적용됩니다. 예를 들어 사용자를 대신하여 리소스 작업을 요청하는 작업을 생성하는 경우가 워크플로에서 `VCACAFE:CatalogResource`를 사용하므로 [입력 리소스] 탭의 리소스 유형은 [배포]가 됩니다.

작업에서 IaaS vCD VM 및 IaaS VC VirtualMachine 리소스 매핑이 사용되면 IaaS 리소스와 일치하는 가상 시스템이 vRealize Orchestrator vSphere 또는 vCloud Director 가상 시스템에 매핑됩니다.

리소스 매핑 개발

사용 중인 vRealize Orchestrator 버전에 따라 vRealize Orchestrator 워크플로 또는 스크립트 작업 중 하나를 생성하여 vRealize Orchestrator 및 vRealize Automation 간의 리소스를 매핑할 수 있습니다.

리소스 매핑을 개발하려면 프로비저닝된 리소스를 정의하는 키 값 쌍이 포함된 Properties 유형의 입력 매개 변수와 해당 vRealize Orchestrator 플러그인이 예상하는 vRealize Orchestrator 인벤토리 유형의 출력 매개 변수를 사용합니다. 매핑에 사용할 수 있는 속성은 리소스 유형에 따라 다릅니다. 예를 들어 EXTERNAL_REFERENCE_ID 속성은 개별 가상 시스템을 정의하는 일반적인 키 매개 변수이고 이 속성을 사용하여 카탈로그 리소스를 쿼리할 수 있습니다. EXTERNAL_REFERENCE_ID를 사용하지 않는 리소스에 대해 매핑을 생성하는 경우 개별 가상 시스템에 대해 전달된 다른 속성 중 하나를 사용할 수 있습니다. 예를 들어 이름, 설명 등이 포함됩니다.

워크플로 및 스크립트 작업 개발에 대한 자세한 내용은 VMware vCenter Orchestrator를 사용한 개발을 참조하십시오.

리소스 매핑 생성

vRealize Automation은 vSphere, vCloud Director 및 vCloud Air 시스템에 대한 리소스 매핑을 제공합니다. 다른 유형의 카탈로그 리소스에 대해서 추가적인 리소스 매핑을 생성할 수 있습니다.

필수 조건

- vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.
- vRealize Orchestrator에서 매핑 스크립트 또는 워크플로를 사용할 수 있는지 확인합니다. [리소스 매핑 스크립트 작업 및 워크플로](#) 항목을 참조하십시오.

프로시저

- 1 **설계 > XaaS > 리소스 매핑**을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 4 버전을 입력합니다.
지원되는 형식은 major.minor.micro-revision으로 확장됩니다.
- 5 **카탈로그 리소스 유형** 텍스트 상자에 카탈로그 리소스의 유형을 입력하고 Enter 키를 누릅니다.
카탈로그 리소스 유형이 프로비저닝된 항목의 세부 정보 보기에 나타납니다.
- 6 **Orchestrator 유형** 텍스트 상자에 vRealize Orchestrator 개체 유형을 입력하고 Enter 키를 누릅니다.
이것이 리소스 매핑 워크플로의 출력 매개 변수입니다.

- 7 (선택 사항) 이 리소스 매핑으로 생성된 리소스 작업의 가용성을 제한하는 대상 기준을 추가합니다.

리소스 작업은 승인 및 사용 권한에 따라 제한을 받기도 합니다.

- a 조건에 따라 사용 가능을 선택합니다.
- b 조건 유형을 선택합니다.

옵션	설명
다음 중 모두	정의하는 모든 절이 만족스러운 경우 이 리소스 매핑으로 생성된 리소스 작업을 사용자가 사용할 수 있습니다.
다음 중 일부	정의하는 일부 절이 만족스러운 경우 이 리소스 매핑으로 생성된 리소스 작업을 사용자가 사용할 수 있습니다.
다음 제외	정의하는 절이 존재하는 경우 이 리소스 매핑으로 생성된 리소스 작업을 사용자가 사용할 수 없습니다.

- c 메시지에 따라 절을 작성하고 조건을 완성합니다.

- 8 vRealize Orchestrator 라이브러리에서 리소스 매핑 스크립트 작업 또는 워크플로를 선택합니다.

- 9 확인을 클릭합니다.

XaaS Blueprint 및 작업을 위한 양식 설계

XaaS에는 Blueprint와 리소스 작업의 제출 및 세부 정보 양식을 설계하는 데 사용할 수 있는 양식 디자이너가 포함되어 있습니다. 워크플로의 프레젠테이션을 기반으로 양식 디자이너는 사용자가 기본 양식을 수정하는 데 사용할 수 있는 기본 양식 및 필드를 동적으로 생성합니다.

사용자가 카탈로그 항목 및 리소스 작업의 제출을 위해 완성할 수 있는 대화형 양식을 생성할 수 있습니다. 또한 사용자가 카탈로그 항목이나 프로비저닝된 리소스에 대한 세부 정보 보기에서 볼 수 있는 정보를 정의하는 읽기 전용 양식도 생성할 수 있습니다.

XaaS 사용자 지정 리소스, XaaS Blueprint 및 리소스 작업을 생성할 때 일반적인 사용 사례를 위한 양식이 생성됩니다.

표 3-60. XaaS 개체 유형 및 연결된 양식

개체 유형	기본 양식	추가 양식
사용자 지정 리소스	vRealize Orchestrator 플러그인 인벤토리 유형(읽기 전용)의 특성을 기반으로 하는 리소스 세부 정보 양식입니다.	■ 없음
XaaS Blueprint	선택한 워크플로의 모양을 기반으로 하는 요청 제출 양식입니다.	■ 카탈로그 항목 세부 정보(읽기 전용) ■ 제출된 요청 세부 정보(읽기 전용)
리소스 작업	선택한 워크플로의 모양을 기반으로 하는 작업 제출 양식입니다.	■ 제출된 작업 세부 정보(읽기 전용)

기본 양식을 수정하고 새로운 양식을 설계할 수 있습니다. 필드를 끌어서 양식에 추가하고 다시 정렬할 수 있습니다. 특정 필드의 값에 제약 조건을 지정하거나, 기본값을 지정하거나, 양식을 완성하는 최종 사용자를 위한 지침 텍스트를 제공할 수 있습니다.

용도가 다양하기 때문에 읽기 전용 양식을 설계하기 위해 수행할 수 있는 작업은 제출 양식을 설계하기 위한 작업에 비해 제한되어 있습니다.

양식 디자이너의 필드

리소스 작업 및 XaaS Blueprint의 기본 생성 양식에 미리 정의된 새 필드를 추가하여 워크플로 프레젠테이션 및 기능을 확장할 수 있습니다.

입력 매개 변수가 vRealize Orchestrator 워크플로에 정의된 경우 vRealize Automation에서 기본 생성 양식에 표시됩니다. 양식의 기본 생성 필드를 사용하지 않으려는 경우 삭제한 후 팔레트에서 새 필드를 끌어서 놓을 수 있습니다. 바꾸려는 필드와 동일한 ID를 사용하는 경우 워크플로 매핑을 끊지 않고 기본 생성 필드를 바꿀 수 있습니다.

vRealize Orchestrator 워크플로 입력을 기반으로 생성된 필드와 다른 새 필드를 추가하여 다음과 같은 경우에 워크플로 프레젠테이션 및 기능을 확장할 수도 있습니다.

■ 기존 필드에 제약 조건 추가

예를 들어 새 드롭다운 메뉴를 생성하고 이름을 **dd**로 지정할 수 있습니다. 또한 골드, 실버, 브론즈 및 사용자 지정의 미리 정의된 옵션을 생성할 수도 있습니다. CPU와 같은 미리 정의된 필드가 있는 경우 이 필드에 다음과 같은 제약 조건을 추가할 수 있습니다.

- dd가 골드와 같으면 CPU가 2000MHz임
- dd가 실버와 같으면 CPU가 1000MHz임
- dd가 브론즈와 같으면 CPU가 500MHz임
- dd가 사용자 지정과 같으면 CPU 필드를 편집할 수 있으며 소비자가 사용자 지정 값을 지정할 수 있음

■ 필드에 외부 값 정의 추가

필드에 외부 값 정의를 추가하여 vRealize Orchestrator 스크립트 작업을 실행하고 설계한 양식에 소비자에 대한 추가 정보를 제공할 수 있습니다. 예를 들어 워크플로를 생성하여 가상 시스템의 방화벽 설정을 변경하고자 할 수 있습니다. 리소스 작업 요청 페이지에서 사용자에게 열린 포트 설정을 변경하는 기능을 제공하면서 열려 있는 포트에 대한 옵션을 제한하고자 할 수 있습니다. 이 중 목록 필드에 외부 값 정의를 추가하고 열린 포트를 관리하는 사용자 지정

vRealize Orchestrator 스크립트 작업을 선택할 수 있습니다. 요청 양식이 로드되면 스크립트 작업이 실행되고 열린 포트가 사용자에게 옵션으로 제공됩니다.

■ vRealize Orchestrator 워크플로에서 처리되는 새 필드를 글로벌 매개 변수로 추가

예를 들어 워크플로가 타사 시스템과의 통합을 제공하고 워크플로 개발자가 일반적인 경우에 처리될 입력 매개 변수를 정의했으며 사용자 지정 필드를 전달하기 위한 방법도 제공했습니다. 예를 들어 스크립팅 상자에서 **my3rdparty**로 시작하는 모든 글로벌 매개 변수가 처리됩니다. 그런 다음 XaaS 설계자가 소비자에 대해 제공할 특정 값을 전달하려는 경우 XaaS 설계자가 이름이 **my3rdparty_CPU**로 지정된 새 필드를 추가할 수 있습니다.

표 3-61. 리소스 작업 또는 XaaS Blueprint 양식의 새 필드

필드	설명
텍스트 필드	한 줄 텍스트 상자
텍스트 영역	여러 줄 텍스트 상자
링크	소비자가 URL을 입력하는 필드
이메일	소비자가 이메일 주소를 입력하는 필드
암호 필드	소비자가 암호를 입력하는 필드
정수 필드	소비자가 정수를 입력하는 텍스트 상자 이 필드를 최소값 및 최대값과 증분이 있는 슬라이더로 만들 수 있습니다.
십진수 필드	소비자가 십진수를 입력하는 텍스트 상자 이 필드를 최소값 및 최대값과 증분이 있는 슬라이더로 만들 수 있습니다.
날짜 및 시간	소비자가 일정 메뉴에서 날짜를 선택하여 날짜를 지정하고 위쪽 및 아래쪽 화살표를 사용하여 시간을 선택할 수도 있는 텍스트 상자
이중 목록	소비자가 2개 목록 사이에서 미리 정의된 값 집합을 이동하는 목록 빌더로 첫 번째 목록에는 선택되지 않은 모든 옵션이 포함되어 있고 두 번째 목록에는 사용자의 선택 사항이 포함되어 있습니다.
확인란	확인란
예/아니오	예 또는 아니오 를 선택하기 위한 드롭다운 메뉴
드롭다운	드롭다운 메뉴
목록	목록
확인란 목록	확인란 목록
라디오 버튼 그룹	라디오 버튼 그룹
검색	쿼리를 자동으로 완성하고 소비자가 개체를 선택하는 검색 텍스트 상자
트리	소비자가 사용 가능한 개체를 탐색하고 선택하는 데 사용하는 트리
맵	소비자가 속성에 대한 키-값 쌍을 정의하는 데 사용하는 맵 테이블

또한 **섹션 머리글** 양식 필드를 사용하여 양식 페이지를 별도의 머리글이 있는 섹션으로 분할하고 **텍스트** 양식 필드를 사용하여 읽기 전용 정보 텍스트를 추가할 수 있습니다.

양식 디자인어의 제약 조건 및 값

리소스 작업 양식 또는 Blueprint의 요소를 편집할 때 요소에 다양한 제약 조건 및 값을 적용할 수 있습니다.

제약 조건

요소에 적용할 수 있는 제약 조건은 편집 중인 또는 양식에 추가 중인 요소의 유형에 따라 다릅니다. vRealize Orchestrator 워크플로에 일부 제약 조건 값이 구성되어 있을 수 있습니다. 그러한 값은 워크플로 실행 시 평가되는 조건에 종속되는 경우가 많기 때문에 [제약 조건] 탭에 나타나지 않습니다. Blueprint 양식에 대해 구성하는 제약 조건 값은 vRealize Orchestrator 워크플로에 포함된 모든 제약 조건을 재정의합니다.

요소에 적용하는 각 제약 조건에 대해, 다음 옵션 중 하나를 선택하여 제약 조건을 정의할 수 있습니다.

설정 안 함	vRealize Orchestrator 워크플로 프레젠테이션에서 속성을 가져옵니다.
상수	편집 중인 요소를 필수 또는 선택 사항으로 설정합니다.
필드	요소를 양식의 다른 요소와 결합합니다. 예를 들어, 다른 요소(예: 확인란)가 선택되었을 때만 필요한 요소를 설정할 수 있습니다.
조건부	조건을 적용합니다. 조건을 사용하여 다양한 결과 식을 생성하고 이를 요소의 상태 또는 제약 조건에 적용합니다.
외부	값을 정의하는 vRealize Orchestrator 스크립트 작업을 선택합니다.

표 3-62. 양식 디자인어의 제약 조건

제약 조건	설명
필요	요소가 필요한지 여부를 나타냅니다.
읽기 전용	필드가 읽기 전용인지 여부를 나타냅니다.
값	요소에 대한 값을 설정합니다.
표시 가능	<p>소비자가 요소를 볼 수 있는지 여부를 나타냅니다.</p> <p>vRealize Orchestrator 워크플로의 표시 그룹에 가시성 제약 조건을 적용하면 XaaS [제출된 요청 세부 정보] 양식에서 제약 조건이 무시되며 숨기고 싶은 필드가 양식에 나타납니다.</p> <p>[제출된 요청 세부 정보] 양식에 표시하지 않으려는 필드와 요청한 사용자에게 필요하지 않은 필드를 숨기려면 XaaS Blueprint Designer의 [Blueprint 양식] 탭에 있는 [제출된 요청 세부 정보] 양식에서 해당 필드를 제거합니다. 이 탭을 찾으려면 새 XaaS Blueprint 양식 추가 항목을 참조하십시오.</p>
최소 길이	문자열 입력 요소의 최소 문자 수를 설정합니다.
최대 길이	문자열 입력 요소의 허용되는 최대 문자 수를 설정합니다.
최소값	숫자 입력 요소의 최소값을 설정합니다.
최대값	숫자 입력 요소의 최대값을 설정합니다.
증분	<p>십진수 또는 정수 필드와 같은 요소에 대해 증분을 설정합니다. 예를 들어 정수 필드를 슬라이더로 렌더링하려는 경우 단계의 값을 사용할 수 있습니다.</p>

표 3-62. 양식 디자이너의 제약 조건 (계속)

제약 조건	설명
최소 개수	선택 가능한 요소 항목의 최소 개수를 설정합니다. 예를 들어, 확인란 목록 을 추가 또는 편집할 때 소비자가 계속하기 위해 선택해야 하는 최소 확인란 수를 설정할 수 있습니다.
최대 개수	선택 가능한 요소 항목의 최대 개수를 설정합니다. 예를 들어, 확인란 목록 을 추가 또는 편집할 때 소비자가 계속하기 위해 선택해야 하는 최대 확인란 수를 설정할 수 있습니다.

값

값을 요소의 일부에 적용하고 일부 필드에 대해 소비자에게 표시할 내용을 정의할 수 있습니다. 사용 가능한 옵션은 편집 중인 또는 양식에 추가 중인 요소의 유형에 따라 다릅니다.

표 3-63. 양식 디자이너의 값

값	설명
설정 안 함	vRealize Orchestrator 워크플로 프레젠테이션에서 편집 중인 요소의 값을 가져옵니다.
미리 정의된 값	vRealize Orchestrator 인벤토리의 관련 개체 목록에서 값을 선택합니다.
값	레이블을 사용하여 정적 사용자 지정 값을 정의합니다.
외부 값	워크플로에 의해 직접 표시되지 않는 정보와 함께 값을 정의하는 vRealize Orchestrator 스크립트 작업을 선택합니다.

양식 디자이너의 외부 값 정의

양식 디자이너의 일부 요소를 편집하는 경우 워크플로에서 직접 제공되지 않는 정보를 제공하는 사용자 지정 vRealize Orchestrator 스크립트 작업을 사용하는 외부 값 정의를 할당할 수 있습니다.

예를 들어 프로비저닝된 시스템에 소프트웨어를 설치하는 리소스 작업을 게시하려고 할 수 있습니다. 소비자에게 다운로드 가능한 모든 소프트웨어의 정적 목록을 제공하는 대신 시스템의 운영 체제와 관련된 소프트웨어, 사용자가 이전에 시스템에 설치하지 않은 소프트웨어 또는 시스템에서 최신 버전이 아니며 업데이트가 필요한 소프트웨어로 해당 목록을 동적으로 채울 수 있습니다.

소비자를 위한 사용자 지정 동적 콘텐츠를 제공하려면 소비자에게 표시하고자 하는 정보를 검색하는 vRealize Orchestrator 스크립트 작업을 생성합니다. 스크립트 작업을 양식 디자이너의 필드에 외부 값 정의로 할당합니다. 리소스 또는 서비스 Blueprint 양식이 소비자에게 제공될 때 스크립트 작업이 사용자 지정 정보를 검색하고 이를 소비자에게 표시합니다.

외부 값 정의를 사용하여 기본 또는 읽기 전용 값을 제공하고 부울 식을 작성하고 제약 조건을 정의하거나 소비자에게 양식 목록, 확인란 등을 선택하기 위한 옵션을 제공할 수 있습니다.

양식 디자이너 사용

XaaS Blueprint, 사용자 지정 리소스 작업 및 사용자 지정 리소스를 생성할 때 양식 디자이너를 사용하여 Blueprint, 작업 및 리소스의 양식을 편집할 수 있습니다. 표현을 편집하여 소비자가 카탈로그 항목을 요청하거나 프로비저닝 후 작업을 실행할 때 항목 또는 작업의 소비자에게 표시되는 항목을 정의할 수 있습니다.

기본적으로 모든 XaaS Blueprint, 리소스 작업 또는 사용자 지정 리소스 양식은 vRealize Orchestrator의 워크플로 프레젠테이션에 기반하여 생성됩니다.

vRealize Orchestrator 표현의 단계는 양식 페이지로 표현되며 vRealize Orchestrator 표현 그룹은 별도 섹션으로 표현됩니다. 선택된 워크플로의 입력 유형이 양식에 여러 필드로 표시됩니다. 예를 들어 vRealize Orchestrator 유형 string은 텍스트 상자로 표현됩니다. VC:VirtualMachine과 같은 복잡한 유형은 검색 상태 또는 트리로 표현되므로 소비자는 영숫자 값을 입력하여 가상 시스템을 검색하거나 찾아보기를 수행하여 가상 시스템을 선택할 수 있습니다.

Create cluster - Blueprint 편집

양식 디자이너에서 개체가 표현되는 방법을 편집할 수 있습니다. 예를 들어 기본 VC:VirtualMachine 표현을 편집하여 검색 상자 대신 트리로 만들 수 있습니다. 또한 확인란, 드롭다운 메뉴 등과 같은 새 필드를 추가하고 다양한 제약 조건을 적용할 수 있습니다. 추가하는 새 필드가 유효하지 않거나 vRealize Orchestrator 워크플로 입력에 올바르게 매핑되지 않은 경우에는 소비자가 워크플로를 실행할 때 vRealize Orchestrator가 잘못되거나 매핑되지 않은 필드를 건너뛸 것입니다.

사용자 지정 리소스 양식 설계

사용자 지정 리소스를 프로비저닝할 때 리소스 세부 정보 양식의 모든 필드가 항목 세부 정보 페이지에서 소비자에게 읽기 전용으로 표시됩니다. 필드 삭제, 수정 또는 재정렬과 같은 기본적인 양식 편집 작업을 수행하거나 vRealize Orchestrator 스크립트 작업을 사용하는 외부에서 정의된 새 필드를 추가하여 소비자에게 읽기 전용 정보를 추가로 제공할 수 있습니다.

■ 사용자 지정 리소스 요소 편집

사용자 지정 리소스 세부 정보 양식 페이지에서 요소의 일부 특성을 편집할 수 있습니다. 페이지의 각 기본 필드는 사용자 지정 리소스의 속성을 나타냅니다. 속성의 유형이나 기본값을 변경할 수는 없지만 이름, 크기, 설명을 편집할 수 있습니다.

■ 새 사용자 지정 리소스 양식 페이지 추가

새 페이지를 추가하여 양식을 여러 탭으로 재정렬할 수 있습니다.

■ 사용자 지정 리소스 양식에 섹션 머리글 삽입

섹션 머리글을 삽입하면 양식을 섹션으로 분할할 수 있습니다.

■ 사용자 지정 리소스 양식에서 텍스트 요소 추가

텍스트 상자를 삽입하여 해당 양식에 일부 설명 텍스트를 추가할 수 있습니다.

■ 외부에서 정의된 필드를 사용자 지정 리소스 양식에 삽입

새 필드를 삽입하고 외부 값 정의를 할당하면 사용자 지정 리소스를 프로비저닝할 때 소비자가 항목 세부 정보 페이지에서 볼 수 있는 읽기 전용 정보를 동적으로 제공할 수 있습니다.

사용자 지정 리소스 요소 편집

사용자 지정 리소스 세부 정보 양식 페이지에서 요소의 일부 특성을 편집할 수 있습니다. 페이지의 각 기본 필드는 사용자 지정 리소스의 속성을 나타냅니다. 속성의 유형이나 기본값을 변경할 수는 없지만 이름, 크기, 설명을 편집할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- **XaaS 사용자 지정 리소스** 추가.

프로시저

- 1 **설계 > XaaS > 사용자 지정 리소스**를 선택합니다.
- 2 사용자 지정 리소스를 클릭하여 편집합니다.
- 3 **세부 정보 양식** 탭을 클릭합니다.
- 4 편집할 요소를 가리키고 **편집** 아이콘을 클릭합니다.

- 5 **레이블** 텍스트 상자에서 필드에 대한 새 이름을 입력하여 레이블을 변경합니다.
- 6 **설명** 텍스트 상자에서 설명을 편집합니다.
- 7 **크기** 드롭다운 메뉴에서 옵션을 선택하여 요소 크기를 변경합니다.
- 8 **레이블 크기** 드롭다운 메뉴에서 옵션을 선택하여 레이블 크기를 변경합니다.
- 9 **제출**을 클릭합니다.
- 10 **마침**을 클릭합니다.

새 사용자 지정 리소스 양식 페이지 추가

새 페이지를 추가하여 양식을 여러 탭으로 재정렬할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- **XaaS 사용자 지정 리소스 추가**.

프로시저

- 1 **설계 > XaaS > 사용자 지정 리소스**를 선택합니다.
- 2 사용자 지정 리소스를 클릭하여 편집합니다.
- 3 **세부 정보 양식** 탭을 클릭합니다.
- 4 **양식 페이지** 이름 옆의 **새 페이지** 아이콘(+)을 클릭합니다.
- 5 사용되지 않는 화면 유형을 선택하고 **제출**을 클릭합니다.

리소스 세부 정보 또는 리소스 목록 보기를 이미 가지고 있다면 같은 유형 두 개를 생성할 수는 없습니다.

- 6 **제출**을 클릭합니다.
- 7 양식을 구성합니다.
- 8 **마침**을 클릭합니다.

원래 양식 페이지에서 요소 중 일부를 삭제하고 새 양식 페이지에 해당 요소를 삽입하거나, vRealize Orchestrator 워크플로가 직접 표시하지 않는 정보를 소비자에게 제공하기 위해 외부 값 정의를 사용하는 새 필드를 추가할 수 있습니다.

사용자 지정 리소스 양식에 섹션 머리글 삽입

섹션 머리글을 삽입하면 양식을 섹션으로 분할할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- **XaaS 사용자 지정 리소스 추가**.

프로시저

- 1 설계 > **XaaS** > **사용자 지정 리소스**를 선택합니다.
- 2 사용자 지정 리소스를 클릭하여 편집합니다.
- 3 **세부 정보 양식** 탭을 클릭합니다.
- 4 양식 창의 **섹션 머리글** 요소를 양식 페이지 창으로 끌어다 놓습니다.
- 5 해당 섹션의 이름을 입력합니다.
- 6 요소 바깥쪽을 클릭하여 변경 내용을 저장합니다.
- 7 **마침**을 클릭합니다.

사용자 지정 리소스 양식에서 텍스트 요소 추가

텍스트 상자를 삽입하여 해당 양식에 일부 설명 텍스트를 추가할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- [XaaS 사용자 지정 리소스 추가](#).

프로시저

- 1 설계 > **XaaS** > **사용자 지정 리소스**를 선택합니다.
- 2 사용자 지정 리소스를 클릭하여 편집합니다.
- 3 **세부 정보 양식** 탭을 클릭합니다.
- 4 양식 창의 **텍스트** 요소를 양식 페이지 창으로 끌어다 놓습니다.
- 5 추가하려는 텍스트를 입력합니다.
- 6 요소 바깥쪽을 클릭하여 변경 내용을 저장합니다.
- 7 **마침**을 클릭합니다.

외부에서 정의된 필드를 사용자 지정 리소스 양식에 삽입

새 필드를 삽입하고 외부 값 정의를 할당하면 사용자 지정 리소스를 프로비저닝할 때 소비자가 항목 세부 정보 페이지에서 볼 수 있는 읽기 전용 정보를 동적으로 제공할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- [XaaS 사용자 지정 리소스 추가](#).
- 소비자에게 제공할 정보를 검색하는 vRealize Orchestrator 스크립트 작업을 개발하거나 가져옵니다.

프로시저

- 1 설계 > **XaaS** > **사용자 지정 리소스**를 선택합니다.

- 2 사용자 지정 리소스를 클릭하여 편집합니다.
 - 3 세부 정보 양식 탭을 클릭합니다.
 - 4 새 필드 창에서 요소를 끌어서 양식 페이지 창에 놓습니다.
 - 5 요소 ID를 ID 텍스트 상자에 입력합니다.
 - 6 레이블 텍스트 상자에 레이블을 입력합니다.
레이블은 양식에서 소비자에게 표시됩니다.
 - 7 (선택 사항) 유형 드롭다운 메뉴에서 필드의 유형을 선택합니다.
 - 8 vRealize Orchestrator 스크립트 작업의 결과 유형을 엔티티 유형 검색 상자에 입력하고 Enter 키를 누릅니다.
예를 들어, 현재 사용자를 표시하는 스크립트 작업을 사용하고, 이 스크립트가 LdapUser라는 vRealize Orchestrator 결과 유형을 반환하는 경우에는 엔티티 유형 검색 상자에 LdapUser를 입력하고 Enter 키를 누릅니다.
 - 9 외부 값 추가를 클릭합니다.
 - 10 사용자 지정 vRealize Orchestrator 스크립트 작업을 선택합니다.
 - 11 제출을 클릭합니다.
 - 12 제출을 다시 클릭합니다.
 - 13 마침을 클릭합니다.
- 소비자에게 양식이 표시되면 스크립트 작업이 사용자 지정 정보를 검색하여 소비자에게 표시합니다.

XaaS Blueprint 양식 설계

XaaS Blueprint를 생성할 때 양식에 새 필드를 추가하거나, 기존 필드를 수정하거나, 필드를 삭제 또는 재정렬하는 방식으로 Blueprint의 양식을 편집할 수 있습니다. 또한 새 양식과 양식 페이지를 생성하고 새 필드를 여기에 끌어다 놓을 수 있습니다.

■ 새 XaaS Blueprint 양식 추가

XaaS Blueprint로 게시하려는 워크플로의 기본 생성 양식을 편집할 때 새 XaaS Blueprint 양식을 추가할 수 있습니다.

■ XaaS Blueprint 요소 편집

XaaS Blueprint의 Blueprint 양식 페이지에서 요소의 일부 특성을 편집할 수 있습니다. 요소의 유형, 기본값을 변경하고 다양한 제약 조건과 값을 적용할 수 있습니다.

■ 새 요소 추가

XaaS Blueprint의 기본 생성 양식을 편집할 때 양식에 미리 정의된 새 요소를 추가할 수 있습니다. 예를 들어 기본 생성 필드를 사용하지 않으려는 경우 해당 필드를 삭제한 후 새 필드로 바꿀 수 있습니다.

■ XaaS Blueprint 양식에 섹션 머리글 삽입

섹션 머리글을 삽입하면 양식을 섹션으로 분할할 수 있습니다.

■ XaaS Blueprint 양식에 텍스트 요소 추가

텍스트 상자를 삽입하여 해당 양식에 일부 설명 텍스트를 추가할 수 있습니다.

새 XaaS Blueprint 양식 추가

XaaS Blueprint로 게시하려는 워크플로의 기본 생성 양식을 편집할 때 새 XaaS Blueprint 양식을 추가할 수 있습니다.

새 XaaS Blueprint 양식을 추가하여, 카탈로그 항목 세부 정보 및 제출된 요청 세부 정보 페이지의 모양과 느낌을 정의합니다. 카탈로그 항목 세부 정보 및 제출된 요청 세부 정보 양식을 추가하지 않는 경우 소비자에게는 요청 양식에 정의된 내용이 표시됩니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- **XaaS Blueprint 추가**.

프로시저

- 1 **설계 > XaaS > XaaS Blueprint**를 선택합니다.
- 2 편집할 XaaS Blueprint를 클릭합니다.
- 3 **Blueprint 양식** 탭을 클릭합니다.
- 4 **새 양식** 아이콘(+)을 클릭합니다.
- 5 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 6 **화면 유형** 메뉴에서 화면 유형을 선택합니다.

옵션	설명
카탈로그 항목 세부 정보	소비자가 카탈로그 항목을 클릭하면 표시되는 카탈로그 항목 세부 정보 페이지입니다.
요청 양식	기본 XaaS Blueprint 양식입니다. 소비자가 카탈로그 항목을 요청하면 요청 양식이 표시됩니다.
제출된 요청 세부 정보	소비자가 항목을 요청하고 요청 탭에서 요청 세부 정보를 보려고 하면 표시되는 요청 세부 정보 페이지입니다.

- 7 **제출**을 클릭합니다.

후속 작업

새 필드 창에서 원하는 필드를 끌어서 양식 페이지 창에 놓아 해당 필드를 추가합니다.

XaaS Blueprint 요소 편집


XaaS Blueprint의 Blueprint 양식 페이지에서 요소의 일부 특성을 편집할 수 있습니다. 요소의 유형, 기본값을 변경하고 다양한 제약 조건과 값을 적용할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.

■ XaaS Blueprint 추가.

프로시저

- 1 **설계 > XaaS > XaaS Blueprint**를 선택합니다.
- 2 편집할 XaaS Blueprint를 클릭합니다.
- 3 **Blueprint 양식** 탭을 클릭합니다.
- 4 편집할 요소를 찾습니다.
- 5 **편집** 아이콘()을 클릭합니다.
- 6 **레이블** 텍스트 상자에 필드의 새 이름을 입력하여 소비자에게 표시되는 레이블을 변경합니다.
- 7 **설명** 텍스트 상자에서 설명을 편집합니다.
- 8 **유형** 드롭다운 메뉴에서 옵션을 선택하여 요소의 표시 유형을 변경합니다.
옵션은 편집하는 요소 유형에 따라 다릅니다.
- 9 **크기** 드롭다운 메뉴에서 옵션을 선택하여 요소 크기를 변경합니다.
- 10 **레이블 크기** 드롭다운 메뉴에서 옵션을 선택하여 레이블 크기를 변경합니다.
- 11 요소의 기본값을 편집합니다.

옵션	설명
설정 안 함	vRealize Orchestrator 워크플로 프레젠테이션에서 편집할 요소의 값을 가져옵니다.
상수	지정하는 상수 값으로 편집할 요소의 기본값을 설정합니다.
필드	표현에서 다른 요소의 매개 변수에 요소의 기본값을 바인딩합니다.
조건부	조건을 적용합니다. 조건을 사용하여 다양한 결과 표현식을 생성하고 요소에 적용할 수 있습니다.
외부	vRealize Orchestrator 스크립트 작업을 선택하여 값을 정의합니다.

- 12 **제약 조건** 탭에서 요소에 제약 조건을 적용합니다.

옵션	설명
설정 안 함	vRealize Orchestrator 워크플로 프레젠테이션에서 편집할 요소의 값을 가져옵니다.
상수	지정하는 상수 값으로 편집할 요소의 기본값을 설정합니다.
필드	표현에서 다른 요소의 매개 변수에 요소의 기본값을 바인딩합니다.
조건부	조건을 적용합니다. 조건을 사용하여 다양한 결과 표현식을 생성하고 요소에 적용할 수 있습니다.
외부	vRealize Orchestrator 스크립트 작업을 선택하여 값을 정의합니다.

13 값 탭에서 요소에 대한 값을 하나 이상 추가합니다.

사용 가능한 옵션은 편집할 요소 유형에 따라 다릅니다.

옵션	설명
설정 안 함	vRealize Orchestrator 워크플로 프레젠테이션에서 편집할 요소의 값을 가져옵니다.
미리 정의된 값	vRealize Orchestrator 인벤토리의 관련 개체 목록에서 값을 선택합니다. a 미리 정의된 값 검색 상자에 값을 입력하여 vRealize Orchestrator 인벤토리를 검색합니다. b 검색 결과에서 값을 선택하고 Enter 키를 누릅니다.
값	레이블을 사용하여 사용자 지정 값을 정의합니다. a 값 텍스트 상자에 값을 입력합니다. b 레이블 텍스트 상자에 값의 레이블을 입력합니다. c 추가 아이콘(+)을 클릭합니다.
외부 값	vRealize Orchestrator 스크립트 작업을 선택하여 워크플로에 의해 직접 표시되지 않는 정보와 함께 값을 정의합니다. ■ 외부 값 추가 를 선택합니다. ■ vRealize Orchestrator 스크립트 작업을 선택합니다. ■ 제출 을 클릭합니다.

14 제출을 클릭합니다.

15 마침을 클릭합니다.

새 요소 추가

XaaS Blueprint의 기본 생성 양식을 편집할 때 양식에 미리 정의된 새 요소를 추가할 수 있습니다. 예를 들어 기본 생성 필드를 사용하지 않으려는 경우 해당 필드를 삭제한 후 새 필드로 바꿀 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- **XaaS Blueprint 추가**.

프로시저

- 1 **설계 > XaaS > XaaS Blueprint**를 선택합니다.
- 2 편집할 XaaS Blueprint를 클릭합니다.
- 3 **Blueprint 양식** 탭을 클릭합니다.
- 4 새 필드 창에서 요소를 끌어서 양식 페이지 창에 놓습니다.
- 5 **ID** 텍스트 상자에 워크플로 입력 매개 변수의 ID를 입력합니다.
- 6 **레이블** 텍스트 상자에 레이블을 입력합니다.
레이블은 양식에서 소비자에게 표시됩니다.
- 7 (선택 사항) **유형** 드롭다운 메뉴에서 필드의 유형을 선택합니다.

- 8 엔티티 유형** 텍스트 상자에 vRealize Orchestrator 개체를 입력하고 Enter 키를 누릅니다.
이 단계는 일부 필드 유형에서 필요하지 않습니다.

옵션	설명
결과 유형	스크립트 작업을 사용하여 필드에 대한 외부 값을 정의하는 경우 vRealize Orchestrator 스크립트 작업의 결과 유형을 입력합니다.
입력 매개 변수	이 필드를 사용하여 소비자 입력을 수락하고 매개 변수를 vRealize Orchestrator로 다시 전달하는 경우 vRealize Orchestrator 워크플로에 의해 수락되는 입력 매개 변수의 유형을 입력합니다.
출력 매개 변수	이 필드를 사용하여 소비자에게 정보를 표시하는 경우 vRealize Orchestrator 워크플로의 출력 매개 변수의 유형을 입력합니다.

- 9** (선택 사항) 소비자가 두 개 이상의 개체를 선택할 수 있게 하려면 **다중 값** 확인란을 선택합니다.
이 옵션은 일부 필드 유형에서 사용 가능하지 않습니다.

10 제출을 클릭합니다.

11 업데이트를 클릭합니다.

후속 작업

요소를 편집하여 기본 설정을 변경하고 다양한 제약 조건 또는 값을 적용할 수 있습니다.

XaaS Blueprint 양식에 섹션 머리글 삽입

섹션 머리글을 삽입하면 양식을 섹션으로 분할할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- [XaaS Blueprint 추가](#).

프로시저

- 1** 설계 > XaaS > XaaS Blueprint를 선택합니다.
- 2** 편집할 XaaS Blueprint를 클릭합니다.
- 3** Blueprint 양식 탭을 클릭합니다.
- 4** 양식 창의 **섹션 머리글** 요소를 양식 페이지 창으로 끌어다 놓습니다.
- 5** 해당 섹션의 이름을 입력합니다.
- 6** 요소 바깥쪽을 클릭하여 변경 내용을 저장합니다.
- 7** 업데이트를 클릭합니다.

XaaS Blueprint 양식에 텍스트 요소 추가

텍스트 상자를 삽입하여 해당 양식에 일부 설명 텍스트를 추가할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.

■ XaaS Blueprint 추가.

프로시저

- 1 설계 > XaaS > XaaS Blueprint를 선택합니다.
- 2 편집할 XaaS Blueprint를 클릭합니다.
- 3 Blueprint 양식 탭을 클릭합니다.
- 4 새 필드 창의 텍스트 요소를 양식 페이지 창으로 끌어다 놓습니다.
- 5 추가하려는 텍스트를 입력합니다.
- 6 요소 바깥쪽을 클릭하여 변경 내용을 저장합니다.
- 7 업데이트를 클릭합니다.

리소스 작업 양식 설계

리소스 작업을 생성할 때 양식에 새 필드를 추가하거나, 기존 필드를 수정하거나, 필드를 삭제 또는 재정렬하는 방식으로 작업의 양식을 편집할 수 있습니다. 또한 새 양식과 양식 페이지를 생성하고 새 필드를 여기에 끌어다 놓을 수 있습니다.

새 리소스 작업 양식 추가

리소스 작업으로 게시하려는 워크플로의 기본 생성 양식을 편집할 때 새 리소스 작업 양식을 추가할 수 있습니다.

새 리소스 작업 양식을 추가하여, 제출된 작업 세부 정보 페이지의 모양을 정의합니다. 제출된 작업 세부 정보 양식을 추가하지 않는 경우 소비자에게는 작업 양식에 정의된 내용이 표시됩니다.

필수 조건

- 데몬트 관리자 또는 XaaS 설계자로 vRealize Automation 콘솔에 로그인합니다.
- 리소스 작업 생성.

프로시저

- 1 설계 > XaaS > 리소스 작업을 선택합니다.
- 2 편집할 리소스 작업을 클릭합니다.
- 3 양식 탭을 클릭합니다.
- 4 새 양식 아이콘(+)을 클릭합니다.
- 5 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 6 화면 유형 메뉴에서 화면 유형을 선택합니다.

옵션	설명
작업 양식	소비자가 사후 프로비저닝 작업을 실행하도록 결정하는 경우 표시되는 기본 리소스 작업 양식입니다.
제출된 작업 세부 정보	소비자가 작업을 요청하고 요청 탭에서 요청 세부 정보를 보려고 하면 표시되는 요청 세부 정보 페이지입니다.

7 제출을 클릭합니다.

후속 작업

새 필드 창에서 원하는 필드를 끌어서 양식 페이지 창에 놓아 해당 필드를 추가합니다.

리소스 작업 양식에 새 요소 추가

리소스 작업의 기본 생성 양식을 편집할 때 양식에 미리 정의된 새 요소를 추가할 수 있습니다. 예를 들어 기본 생성 필드를 사용하지 않으려는 경우 해당 필드를 삭제한 후 새 필드로 바꿀 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- **리소스 작업 생성**.

프로시저

- 1 **설계 > XaaS > 리소스 작업**을 선택합니다.
- 2 편집할 리소스 작업을 클릭합니다.
- 3 **양식** 탭을 클릭합니다.
- 4 새 필드 창에서 요소를 끌어서 양식 페이지 창에 놓습니다.
- 5 **ID** 텍스트 상자에 워크플로 입력 매개 변수의 ID를 입력합니다.
- 6 **레이블** 텍스트 상자에 레이블을 입력합니다.
레이블은 양식에서 소비자에게 표시됩니다.
- 7 (선택 사항) **유형** 드롭다운 메뉴에서 필드의 유형을 선택합니다.
- 8 **엔티티 유형** 텍스트 상자에 vRealize Orchestrator 개체를 입력하고 Enter 키를 누릅니다.
이 단계는 일부 필드 유형에서 필요하지 않습니다.

옵션	설명
결과 유형	스크립트 작업을 사용하여 필드에 대한 외부 값을 정의하는 경우 vRealize Orchestrator 스크립트 작업의 결과 유형을 입력합니다.
입력 매개 변수	이 필드를 사용하여 소비자 입력을 수락하고 매개 변수를 vRealize Orchestrator로 다시 전달하는 경우 vRealize Orchestrator 워크플로에 의해 수락되는 입력 매개 변수의 유형을 입력합니다.
출력 매개 변수	이 필드를 사용하여 소비자에게 정보를 표시하는 경우 vRealize Orchestrator 워크플로의 출력 매개 변수의 유형을 입력합니다.

- 9 (선택 사항) 소비자가 두 개 이상의 개체를 선택할 수 있게 하려면 **다중 값** 확인란을 선택합니다.
이 옵션은 일부 필드 유형에서 사용 가능하지 않습니다.
- 10 **제출**을 클릭합니다.
- 11 **마침**을 클릭합니다.

후속 작업

요소를 편집하여 기본 설정을 변경하고 다양한 제약 조건 또는 값을 적용할 수 있습니다.


리소스 작업 요소 편집

리소스 작업 양식 페이지에서 요소의 일부 특성을 편집할 수 있습니다. 요소의 유형, 기본값을 변경하고 다양한 제약 조건과 값을 적용할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- **리소스 작업 생성**.

프로시저

- 1 **설계 > XaaS > 리소스 작업**을 선택합니다.
- 2 편집할 리소스 작업을 클릭합니다.
- 3 **양식** 탭을 클릭합니다.
- 4 편집할 요소를 찾습니다.
- 5 **편집** 아이콘()을 클릭합니다.
- 6 **레이블** 텍스트 상자에 필드의 새 이름을 입력하여 소비자에게 표시되는 레이블을 변경합니다.
- 7 **설명** 텍스트 상자에서 설명을 편집합니다.
- 8 **유형** 드롭다운 메뉴에서 옵션을 선택하여 요소의 표시 유형을 변경합니다.
옵션은 편집하는 요소 유형에 따라 다릅니다.
- 9 **크기** 드롭다운 메뉴에서 옵션을 선택하여 요소 크기를 변경합니다.
- 10 **레이블 크기** 드롭다운 메뉴에서 옵션을 선택하여 레이블 크기를 변경합니다.
- 11 요소의 기본값을 편집합니다.

옵션	설명
설정 안 함	vRealize Orchestrator 워크플로 프레젠테이션에서 편집할 요소의 값을 가져옵니다.
상수	지정하는 상수 값으로 편집할 요소의 기본값을 설정합니다.
필드	표현에서 다른 요소의 매개 변수에 요소의 기본값을 바인딩합니다.
조건부	조건을 적용합니다. 조건을 사용하여 다양한 결과 표현식을 생성하고 요소에 적용할 수 있습니다.
외부	vRealize Orchestrator 스크립트 작업을 선택하여 값을 정의합니다.

12 제약 조건 탭에서 요소에 제약 조건을 적용합니다.

옵션	설명
설정 안 함	vRealize Orchestrator 워크플로 프레젠테이션에서 편집할 요소의 값을 가져옵니다.
상수	지정하는 상수 값으로 편집할 요소의 기본값을 설정합니다.
필드	표현에서 다른 요소의 매개 변수에 요소의 기본값을 바인딩합니다.
조건부	조건을 적용합니다. 조건을 사용하여 다양한 결과 표현식을 생성하고 요소에 적용할 수 있습니다.
외부	vRealize Orchestrator 스크립트 작업을 선택하여 값을 정의합니다.

13 값 탭에서 요소에 대한 값을 하나 이상 추가합니다.

사용 가능한 옵션은 편집할 요소 유형에 따라 다릅니다.

옵션	설명
설정 안 함	vRealize Orchestrator 워크플로 프레젠테이션에서 편집할 요소의 값을 가져옵니다.
미리 정의된 값	vRealize Orchestrator 인벤토리의 관련 개체 목록에서 값을 선택합니다. a 미리 정의된 값 검색 상자에 값을 입력하여 vRealize Orchestrator 인벤토리를 검색합니다. b 검색 결과에서 값을 선택하고 Enter 키를 누릅니다.
값	레이블을 사용하여 사용자 지정 값을 정의합니다. a 값 텍스트 상자에 값을 입력합니다. b 레이블 텍스트 상자에 값의 레이블을 입력합니다. c 추가 아이콘(+)을 클릭합니다.
외부 값	vRealize Orchestrator 스크립트 작업을 선택하여 워크플로에 의해 직접 표시되지 않는 정보와 함께 값을 정의합니다. ■ 외부 값 추가 를 선택합니다. ■ vRealize Orchestrator 스크립트 작업을 선택합니다. ■ 제출 을 클릭합니다.

14 제출을 클릭합니다.

15 업데이트를 클릭합니다.

리소스 작업 양식에 섹션 머리글 삽입

섹션 머리글을 삽입하면 양식을 섹션으로 분할할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- **리소스 작업 생성**.

프로시저

- 1 **설계 > XaaS > 리소스 작업**을 선택합니다.
- 2 편집할 리소스 작업을 클릭합니다.

- 3 양식 탭을 클릭합니다.
- 4 양식 창의 **섹션 머리글** 요소를 양식 페이지 창으로 끌어다 놓습니다.
- 5 해당 섹션의 이름을 입력합니다.
- 6 요소 바깥쪽을 클릭하여 변경 내용을 저장합니다.
- 7 **마침**을 클릭합니다.

리소스 작업 양식에 텍스트 요소 추가

텍스트 상자를 삽입하여 해당 양식에 일부 설명 텍스트를 추가할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **XaaS 설계자**로 vRealize Automation 콘솔에 로그인합니다.
- **리소스 작업 생성**.

프로시저

- 1 **설계 > XaaS > 리소스 작업**을 선택합니다.
- 2 편집할 리소스 작업을 클릭합니다.
- 3 **양식** 탭을 클릭합니다.
- 4 새 필드 창의 **텍스트** 요소를 양식 페이지 창으로 끌어다 놓습니다.
- 5 추가하려는 텍스트를 입력합니다.
- 6 요소 바깥쪽을 클릭하여 변경 내용을 저장합니다.
- 7 **마침**을 클릭합니다.

XaaS 예제 및 시나리오

예제와 시나리오는 XaaS Blueprint와 리소스 작업을 사용하여 일반 작업을 수행하는 데 vRealize Automation를 사용할 수 있는 권장 방법을 제시합니다.

사용자 생성 및 수정을 위해 XaaS Blueprint 및 작업 생성

XaaS를 사용하여 그룹의 사용자를 프로비저닝하기 위한 카탈로그 항목을 작성하고 게시할 수 있습니다. 프로비저닝된 사용자에게 새 사후 프로비저닝 작업을 연결할 수도 있습니다. 예를 들어 서비스 카탈로그 사용자가 사용자 암호를 변경할 수 있도록 하는 작업입니다.

XaaS 설계자로서 사용자 지정 리소스, XaaS Blueprint를 생성하고 사용자를 생성하기 위해 카탈로그 항목을 게시합니다. 또한 사용자 암호 변경을 위한 리소스 작업도 생성합니다.

카탈로그 관리자는 서비스를 생성하고 서비스에 Blueprint 카탈로그 항목을 포함합니다. 또한 양식 디자인을 사용하여 카탈로그 항목의 워크플로 프레젠테이션을 편집하고 소비자가 요청 양식을 보는 방식을 변경합니다.

비즈니스 그룹 관리자 또는 테넌트 관리자는 새로 생성된 서비스, 카탈로그 항목 및 리소스 작업에 대한 사용 권한을 소비자에게 부여합니다.

필수 조건

Active Directory 플러그인이 제대로 구성되었고 Active Directory에서 사용자를 생성할 권한이 있는지 확인합니다.

프로시저

1 사용자 지정 리소스로 테스트 사용자 생성

사용자 지정 리소스를 생성하고 이것을 vRealize Orchestrator 개체 유형 AD:User에 매핑할 수 있습니다.

2 사용자 생성을 위한 XaaS Blueprint 생성

Active Directory 사용자를 추가하고 Active Directory 그룹에 사용자를 할당하는 워크플로를 실행할 수 있도록 그룹에서 사용자 생성 XaaS Blueprint를 생성합니다. Blueprint를 독립형 XaaS Blueprint 또는 Blueprint 구성 요소로 생성할 수 있습니다. 이 시나리오에서는 독립형 Blueprint를 생성합니다.

3 리소스 작업을 생성하여 사용자 암호 변경

리소스 작업을 생성하여 XaaS의 소비자가 사용자를 프로비저닝한 후 사용자 Blueprint를 생성하여 사용자의 암호를 변경하도록 허용할 수 있습니다.

4 서비스 생성 및 서비스에 테스트 사용자 Blueprint 생성 추가

서비스를 생성하여 서비스 카탈로그에서 사용자 카탈로그 항목 생성을 표시할 수 있습니다.

5 소비자에게 서비스 및 리소스 작업에 대한 사용 권한 부여

비즈니스 그룹 관리자 및 테넌트 관리자는 서비스 및 리소스 작업의 권한을 사용자 또는 사용자 그룹에 부여할 수 있습니다. 사용자에게 권한이 부여된 후 사용자의 카탈로그에서 서비스를 볼 수 있고 서비스에 포함된 테스트 사용자 생성 카탈로그 항목을 요청할 수 있습니다. 소비자가 항목을 프로비저닝한 후 사용자 암호를 변경하도록 요청할 수 있습니다.

사용자 지정 리소스로 테스트 사용자 생성

사용자 지정 리소스를 생성하고 이것을 vRealize Orchestrator 개체 유형 AD:User에 매핑할 수 있습니다.

필수 조건

vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.

프로시저

1 설계 > XaaS > 사용자 지정 리소스를 선택합니다.

2 새로 만들기 아이콘(+)을 클릭합니다.

3 Orchestrator 유형 텍스트 상자에 AD:User를 입력하고 Enter 키를 누릅니다.

4 목록에서 AD:User를 선택합니다.

5 리소스의 이름을 입력합니다.

예를 들어, **Test User**라고 입력합니다.

6 리소스에 대한 설명을 입력합니다.

예를 들어

그룹에서 사용자를 생성하기 위해 내 카탈로그 항목에 대해 사용할 테스트 사용자 지정 리소스입니다.라고 입력합니다.

7 다음을 클릭합니다.

8 양식의 기본값을 그대로 둡니다.

9 완료를 클릭합니다.

Test User라는 사용자 지정 리소스를 생성했습니다. 이 리소스를 사용자 지정 리소스 페이지에서 볼 수 있습니다.

후속 작업

XaaS Blueprint를 생성합니다.

사용자 생성을 위한 XaaS Blueprint 생성

Active Directory 사용자를 추가하고 Active Directory 그룹에 사용자를 할당하는 워크플로를 실행할 수 있도록 그룹에서 사용자 생성 XaaS Blueprint를 생성합니다. Blueprint를 독립형 XaaS Blueprint 또는 Blueprint 구성 요소로 생성할 수 있습니다. 이 시나리오에서는 독립형 Blueprint를 생성합니다.

필수 조건

- Active Directory 사용자 프로비저닝을 지원하는 사용자 지정 리소스 작업을 생성하는지 확인합니다. [사용자 지정 리소스로 테스트 사용자 생성](#) 항목을 참조하십시오.
- vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.

프로시저

1 설계 > XaaS > XaaS Blueprint를 선택합니다.

2 새로 만들기 아이콘(+)을 클릭합니다.

3 [워크플로 선택] 창에서 **Orchestrator > 라이브러리 > Microsoft > Active Directory > 사용자**로 이동하여 **그룹에서 사용자 생성** 워크플로를 선택합니다.

4 다음을 클릭합니다.

5 일반 탭 옵션을 구성합니다.

a Blueprint의 이름을 **Create a test user**로 변경하고 설명은 그대로 둡니다.

b 설계 캔버스에서 **구성 요소로 사용할 수 있도록 설정** 확인란을 선택 해제합니다.

이 Blueprint를 설계 캔버스에서 Blueprint 구성 요소로 사용하는 대신 서비스 카탈로그에 직접 게시합니다. 축소 또는 확장 워크플로를 구성하지 않아도 됩니다.

사용자 인터페이스에서 **구성 요소 수명 주기** 탭이 제거됩니다.

6 다음을 클릭합니다.

7 Blueprint 양식을 편집합니다.

- a **Win2000** 양식의 **도메인 이름**을 클릭합니다.
- b **제약 조건** 탭을 클릭합니다.
- c **값** 드롭다운 화살표를 클릭하고 드롭다운 메뉴에서 **상수**를 선택한 다음 **test.domain**을 입력합니다.
- d **표시 가능** 드롭다운 화살표를 클릭하고 드롭다운 메뉴에서 **상수**를 선택한 다음 드롭다운 메뉴에서 **아니요**를 선택합니다.

카탈로그 항목의 소비자가 도메인 이름을 볼 수 없도록 설정했습니다.

- e **적용**을 클릭하여 변경 내용을 저장합니다.

8 다음을 클릭합니다.

9 프로비저닝할 출력 매개 변수로 **newUser [Test User]**를 선택합니다.

10 다음을 클릭합니다.

11 완료를 클릭합니다.

12 **XaaS Blueprints** 페이지에서 **테스트 사용자 생성** 행을 선택하고 **게시**를 클릭합니다.

테스트 사용자를 생성하기 위한 Blueprint를 생성했고 해당 Blueprint를 서비스에 추가할 수 있도록 했습니다.

후속 작업

프로비저닝된 사용자 계정에서 실행할 작업을 생성합니다. [리소스 작업을 생성하여 사용자 암호 변경](#) 항목을 참조하십시오.

리소스 작업을 생성하여 사용자 암호 변경

리소스 작업을 생성하여 XaaS의 소비자가 사용자를 프로비저닝한 후 사용자 Blueprint를 생성하여 사용자의 암호를 변경하도록 허용할 수 있습니다.

필수 조건

- vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.
- Active Directory 사용자 프로비저닝을 지원하는 사용자 지정 리소스 작업을 생성하는지 확인합니다. [사용자 지정 리소스로 테스트 사용자 생성](#) 항목을 참조하십시오.

프로시저

- 1 **설계 > XaaS > 리소스 작업**을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 vRealize Orchestrator 워크플로 라이브러리에서 **Orchestrator > 라이브러리 > Microsoft > Active Directory > 사용자**로 이동하고 **사용자 암호 변경** 워크플로를 선택합니다.
- 4 다음을 클릭합니다.

5 리소스 유형 드롭다운 메뉴에서 **테스트 사용자**를 선택합니다.

이 선택은 이전에 생성한 사용자 지정 리소스입니다.

6 입력 매개 변수 드롭다운 메뉴에서 **사용자**를 선택합니다.

7 다음을 클릭합니다.

8 리소스 작업의 이름을 **테스트 사용자의 암호 변경**으로 변경하고 **세부 정보** 탭에 나타나면 설명을 그대로 둡니다.

9 다음을 클릭합니다.

10 (선택 사항) 양식을 그대로 둡니다.

11 완료를 클릭합니다.

12 [리소스 작업] 페이지에서 **테스트 사용자의 암호 변경** 행을 선택하고 **게시**를 클릭합니다.

사용자의 암호를 변경하기 위한 리소스 작업을 생성했고 사용 권한에 추가할 수 있도록 했습니다.

후속 작업

서비스에 테스트 사용자 생성 Blueprint를 추가합니다. [서비스 생성 및 서비스에 테스트 사용자 Blueprint 생성 추가](#) 항목을 참조하십시오.

서비스 생성 및 서비스에 테스트 사용자 Blueprint 생성 추가

서비스를 생성하여 서비스 카탈로그에서 사용자 카탈로그 항목 생성을 표시할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **카탈로그 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- XaaS Blueprint를 생성했는지 확인합니다. [사용자 생성을 위한 XaaS Blueprint 생성](#) 항목을 참조하십시오.

테넌트 관리자 또는 **카탈로그 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 카탈로그 관리 > 서비스**를 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 서비스 이름으로 **Active Directory 테스트 사용자**를 입력합니다.
- 4 **상태** 드롭다운 메뉴에서 **활성**을 선택합니다.
- 5 다른 텍스트 상자는 비워 둡니다.
- 6 **확인**을 클릭합니다.
- 7 서비스 목록에서 **Active Directory 테스트 사용자** 행을 선택하고 **카탈로그 항목 관리**를 클릭합니다.
- 8 **새로 만들기** 아이콘(+)을 클릭합니다.

9 테스트 사용자 생성을 선택하고 확인을 클릭합니다.

카탈로그 항목 목록에 테스트 사용자 생성 XaaS Blueprint가 추가됩니다.

10 닫기를 클릭합니다.

Active Directory 테스트 사용자 서비스에 테스트 사용자 생성 Blueprint가 포함됩니다. 서비스에 작업을 추가하지 않아도 됩니다.

후속 작업

사용자에게 Blueprint를 요청하고 작업을 실행할 수 있는 권한을 부여할 수 있습니다. [소비자에게 서비스 및 리소스 작업에 대한 사용 권한 부여](#) 항목을 참조하십시오.

소비자에게 서비스 및 리소스 작업에 대한 사용 권한 부여

비즈니스 그룹 관리자 및 테넌트 관리자는 서비스 및 리소스 작업의 권한을 사용자 또는 사용자 그룹에 부여할 수 있습니다. 사용자에게 권한이 부여된 후 사용자의 카탈로그에서 서비스를 볼 수 있고 서비스에 포함된 테스트 사용자 생성 카탈로그 항목을 요청할 수 있습니다. 소비자가 항목을 프로비저닝한 후 사용자 암호를 변경하도록 요청할 수 있습니다.

필수 조건

- 테넌트 관리자 또는 비즈니스 그룹 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 사용자 생성 Blueprint가 서비스에 추가되었는지 확인합니다. [서비스 생성 및 서비스에 테스트 사용자 Blueprint 생성 추가](#) 항목을 참조하십시오.
- 사용자 암호 변경 리소스 작업이 존재하는지 확인합니다. [리소스 작업을 생성하여 사용자 암호 변경](#) 항목을 참조하십시오.

프로시저

- 1 **관리 > 카탈로그 관리 > 사용 권한**을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 이름 텍스트 상자에 **Active Directory 사용자 생성**을 입력합니다.
- 4 **설명** 및 **만료 날짜** 텍스트 상자를 비워 둡니다.
- 5 **상태** 드롭다운 메뉴에서 **활성**을 선택합니다.
- 6 **비즈니스 그룹** 드롭다운 메뉴에서 대상 비즈니스 그룹을 선택합니다.
예를 들어, IT 계정 관리자를 선택합니다.
- 7 **모든 사용자 및 그룹**을 선택하여 해당 비즈니스 그룹(예: IT 계정 관리자)의 모든 구성원에게 사용자 계정을 생성할 권한을 부여합니다.

선택한 사용자는 카탈로그의 서비스에 포함된 서비스 및 카탈로그 항목을 볼 수 있습니다. 이들은 사용자 계정이 생성된 후에 암호 변경 작업을 실행할 수 있습니다.
- 8 **다음**을 클릭합니다.

9 권한 있는 서비스 텍스트 상자에 **Active Directory 테스트 사용자**를 입력하고 Enter 키를 누릅니다.

10 권한 있는 작업 텍스트 상자에 **테스트 사용자의 암호 변경**을 입력하고 Enter 키를 누릅니다.

11 완료를 클릭합니다.

IT 계정 관리자 비즈니스 그룹의 구성원인 사용자가 사용자를 생성할 수 있도록 활성 사용 권한을 생성했습니다. 사용자가 프로비저닝된 후 프로비저닝된 사용자 계정에서 암호 변경 리소스 작업을 실행할 수 있습니다.

후속 작업

Active Directory 사용자를 생성할 권한이 있는 사용자로 로그인합니다. **카탈로그** 탭에서 XaaS Blueprint가 예상대로 사용자를 생성하는지 확인합니다. 사용자가 생성된 후 **항목** 탭에서 암호 변경 작업을 실행합니다.

가상 시스템을 마이그레이션하도록 XaaS 작업 생성 및 게시

소비자가 IaaS에서 프로비저닝된 vSphere 가상 시스템에서 수행할 수 있는 작업을 확장하기 위한 XaaS 리소스 작업을 생성하고 게시할 수 있습니다.

이 시나리오에서 vSphere 가상 시스템의 빠른 마이그레이션을 위한 리소스 작업을 생성합니다.

필수 조건

vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.

프로시저

1 리소스 작업을 생성하여 vSphere 가상 시스템 마이그레이션

사용자 지정 리소스 작업을 생성하여 소비자가 IaaS로 vSphere 가상 시스템을 프로비저닝한 후 vSphere 가상 시스템을 마이그레이션하도록 허용할 수 있습니다.

2 vSphere 가상 시스템의 마이그레이션 작업 게시

[가상 시스템의 빠른 마이그레이션] 리소스 작업을 사후 프로비저닝 작업으로 사용하려면 해당 작업을 게시해야 합니다.

리소스 작업을 생성하여 vSphere 가상 시스템 마이그레이션

사용자 지정 리소스 작업을 생성하여 소비자가 IaaS로 vSphere 가상 시스템을 프로비저닝한 후 vSphere 가상 시스템을 마이그레이션하도록 허용할 수 있습니다.

프로시저

1 설계 > XaaS > 리소스 작업을 선택합니다.

2 추가(+)를 클릭합니다.

3 vRealize Orchestrator 워크플로 라이브러리에서 **Orchestrator > 라이브러리 > vCenter > 가상 시스템 관리 > 이동 및 마이그레이션**으로 이동하고 **가상 시스템의 빠른 마이그레이션** 워크플로를 선택합니다.

4 다음을 클릭합니다.

- 5 리소스 유형 드롭다운 메뉴에서 **laaS VC VirtualMachine**을 선택합니다.
- 6 입력 매개 변수 드롭다운 메뉴에서 **vm**을 선택합니다.
- 7 다음을 클릭합니다.
- 8 리소스 작업의 이름과 설명이 **세부 정보** 탭에 나타나면 그대로 둡니다.
- 9 다음을 클릭합니다.
- 10 양식을 그대로 둡니다.
- 11 마침을 클릭합니다.

가상 시스템 마이그레이션을 위한 리소스 작업을 생성했습니다. 이 리소스 작업을 리소스 작업 페이지에서 볼 수 있습니다.

후속 작업

[vSphere 가상 시스템의 마이그레이션 작업 게시](#)

vSphere 가상 시스템의 마이그레이션 작업 게시

[가상 시스템의 빠른 마이그레이션] 리소스 작업을 사후 프로비저닝 작업으로 사용하려면 해당 작업을 게시해야 합니다.

프로시저

- 1 **설계 > XaaS > 리소스 작업**을 선택합니다.
- 2 [가상 시스템의 빠른 마이그레이션] 리소스 작업에 해당하는 행을 선택하고 **게시** 버튼을 클릭합니다.

리소스 작업으로 vRealize Orchestrator 워크플로를 생성하고 게시했습니다. **관리 > 카탈로그 관리 > 작업**으로 이동하고 작업 목록에서 가상 시스템의 빠른 마이그레이션 리소스 작업을 볼 수 있습니다. 리소스 작업에 아이콘을 할당할 수 있습니다. [XaaS 리소스 작업에 아이콘 할당](#) 항목을 참조하십시오.

후속 작업

laaS 프로비저닝 vSphere 가상 시스템을 포함하는 사용 권한에 작업을 추가합니다. [사용자에게 서비스, 카탈로그 항목 및 작업에 대한 사용 권한 부여](#) 항목을 참조하십시오.

vMotion을 사용하여 가상 시스템을 마이그레이션하도록 XaaS 작업 생성

XaaS를 사용하여 vMotion으로 laaS에서 프로비저닝된 가상 시스템을 마이그레이션하기 위한 리소스 작업을 생성하고 게시할 수 있습니다.

이 시나리오에서 vMotion으로 vSphere 가상 시스템을 마이그레이션하기 위한 리소스 작업을 생성합니다. 또한 양식 디자이너를 사용하여 워크플로 프레젠테이션을 편집하고 소비자가 작업 요청 시 작업을 보는 방식을 변경합니다.

필수 조건

vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.

프로시저

1 vMotion을 사용하여 vSphere 가상 시스템을 마이그레이션하도록 작업 생성

사용자 지정 리소스 작업을 생성하여 서비스 카탈로그 사용자가 IaaS로 시스템을 프로비저닝한 후 vMotion으로 vSphere 가상 시스템을 마이그레이션하도록 허용할 수 있습니다.

2 리소스 작업 양식 편집

리소스 작업 양식은 vRealize Orchestrator 워크플로 프레젠테이션을 매핑합니다. 양식을 편집하여 리소스 작업의 소비자가 사후 프로비저닝 작업을 실행하기로 결정할 때 볼 것을 정의합니다.

3 제출된 작업 세부 정보 양식 추가 및 작업 저장

vMotion 리소스 작업을 사용하여 가상 시스템 마이그레이션에 새 양식을 추가하여 소비자가 사후 프로비저닝 작업을 실행하도록 요청한 후 표시되는 내용을 정의할 수 있습니다.

4 vMotion을 사용하는 가상 시스템의 마이그레이션 작업 게시

[vMotion을 사용하는 가상 시스템 마이그레이션] 리소스 작업을 사후 프로비저닝 작업으로 사용하려면 해당 작업을 게시해야 합니다.

vMotion을 사용하여 vSphere 가상 시스템을 마이그레이션하도록 작업 생성

사용자 지정 리소스 작업을 생성하여 서비스 카탈로그 사용자가 IaaS로 시스템을 프로비저닝한 후 vMotion으로 vSphere 가상 시스템을 마이그레이션하도록 허용할 수 있습니다.

프로시저

1 **설계 > XaaS > 리소스** 작업을 선택합니다.

2 **추가(+)**를 클릭합니다.

3 vRealize Orchestrator 워크플로 라이브러리에서 **Orchestrator > 라이브러리 > vCenter > 가상 시스템 관리 > 이동 및 마이그레이션**으로 이동하고 **vMotion으로 가상 시스템 마이그레이션** 워크플로를 선택합니다.

4 **다음**을 클릭합니다.

5 **리소스 유형** 드롭다운 메뉴에서 **IaaS VC VirtualMachine**을 선택합니다.

6 **입력 매개 변수** 드롭다운 메뉴에서 **vm**을 선택합니다.

7 **다음**을 클릭합니다.

8 리소스 작업의 이름과 설명이 **세부 정보** 탭에 나타나면 그대로 둡니다.

9 **다음**을 클릭합니다.

후속 작업

[리소스 작업 양식 편집](#).

리소스 작업 양식 편집

리소스 작업 양식은 vRealize Orchestrator 워크플로 프레젠테이션을 매핑합니다. 양식을 편집하여 리소스 작업의 소비자가 사후 프로비저닝 작업을 실행하기로 결정할 때 볼 것을 정의합니다.

프로시저

1 삭제 아이콘(✖)을 클릭하여 풀 요소를 삭제합니다.

2 호스트 요소를 편집합니다.

- a 호스트 필드 옆의 편집 아이콘(✎)을 클릭합니다.
- b 레이블 텍스트 상자에 대상 호스트를 입력합니다.
- c 유형 드롭다운 메뉴에서 검색을 선택합니다.
- d 제약 조건 탭을 클릭합니다.
- e 필수 드롭다운 메뉴에서 상수를 선택하고 예를 선택합니다.
호스트 필드를 항상 필요한 것으로 지정했습니다.
- f 제출을 클릭합니다.

3 우선 순위 요소를 편집합니다.

- a 우선 순위 필드 옆의 편집 아이콘(✎)을 클릭합니다.
- b 레이블 텍스트 상자에 작업의 우선 순위를 입력합니다.
- c 유형 드롭다운 메뉴에서 라디오 버튼 그룹을 선택합니다.
- d 값 탭을 클릭하고 설정 안 함 확인란을 선택 해제합니다.
- e 미리 정의된 값 검색 텍스트 상자에 낮은 우선 순위를 입력하고 Enter 키를 누릅니다.
- f 미리 정의된 값 검색 텍스트 상자에 기본 우선 순위를 입력하고 Enter 키를 누릅니다.
- g 미리 정의된 값 검색 텍스트 상자에 높은 우선 순위를 입력하고 Enter 키를 누릅니다.
- h 제출을 클릭합니다.

소비자가 리소스 작업을 요청하면 낮은 우선 순위, 기본 우선 순위 및 높은 우선 순위의 3개 라디오 버튼이 있는 라디오 버튼 그룹이 표시됩니다.

4 상태 요소를 편집합니다.

- a 상태 필드 옆의 편집 아이콘(✎)을 클릭합니다.
- b 레이블 텍스트 상자에 가상 시스템 상태를 입력합니다.
- c 유형 드롭다운 메뉴에서 드롭다운을 선택합니다.
- d 값 탭을 클릭하고 설정 안 함 확인란을 선택 해제합니다.
- e 미리 정의된 값 검색 텍스트 상자에 전원 꺼짐을 입력하고 Enter 키를 누릅니다.
- f 미리 정의된 값 검색 텍스트 상자에 전원 켜짐을 입력하고 Enter 키를 누릅니다.

g **미리 정의된 값** 검색 텍스트 상자에 **일시 중단됨**을 입력하고 Enter 키를 누릅니다.

h **제출**을 클릭합니다.

소비자가 리소스 작업을 요청하면 **전원 꺼짐**, **전원 켜짐** 및 **일시 중단됨**의 3개 옵션이 있는 드롭다운 메뉴가 표시됩니다.

vMotion으로 가상 시스템 마이그레이션 워크플로의 워크플로 프레젠테이션을 편집했습니다.



후속 작업

제출된 작업 세부 정보 양식 추가 및 작업 저장.

제출된 작업 세부 정보 양식 추가 및 작업 저장

vMotion 리소스 작업을 사용하여 가상 시스템 마이그레이션에 새 양식을 추가하여 소비자가 사후 프로비저닝 작업을 실행하도록 요청한 후 표시되는 내용을 정의할 수 있습니다.

프로시저

- 1 새 양식 아이콘() (양식 드롭다운 메뉴 옆에 있음)을 클릭합니다.
- 2 이름 텍스트 상자에 **제출된 작업**을 입력합니다.
- 3 설명 필드는 비워 둡니다.
- 4 화면 유형 메뉴에서 **제출된 작업 세부 정보**를 선택합니다.
- 5 제출을 클릭합니다.
- 6 양식 페이지 드롭다운 메뉴 옆의 편집 아이콘()을 클릭합니다.
- 7 머릿글 텍스트 상자에 **세부 정보**를 입력합니다.
- 8 제출을 클릭합니다.
- 9 양식 창의 텍스트 요소를 끌어다 양식 페이지에 놓습니다.
- 10 다음을 입력합니다.
vMotion을 사용하여 시스템을 마이그레이션하는 요청을 제출했습니다. 이 프로세스가 완료될 때까지 기다리십시오.
- 11 텍스트 상자 바깥쪽을 클릭하여 변경 내용을 저장합니다.
- 12 제출을 클릭합니다.
- 13 추가를 클릭합니다.

vMotion을 사용하여 가상 시스템을 마이그레이션하는 리소스 작업을 생성한 후, 리소스 작업 페이지에 이 요청이 나열된 것을 볼 수 있습니다.

후속 작업

vMotion을 사용하는 가상 시스템의 마이그레이션 작업 게시.

vMotion을 사용하는 가상 시스템의 마이그레이션 작업 게시

[vMotion을 사용하는 가상 시스템 마이그레이션] 리소스 작업을 사후 프로비저닝 작업으로 사용하려면 해당 작업을 게시해야 합니다.

프로시저

- 1 **설계 > XaaS > 리소스** 작업을 선택합니다.
- 2 [vMotion을 사용하는 가상 시스템 마이그레이션] 작업에 해당하는 행을 선택하고 **게시** 버튼을 클릭합니다.

리소스 작업으로 vRealize Orchestrator 워크플로를 생성하고 게시했습니다. **관리 > 카탈로그 관리 > 작업**으로 이동하고 작업 목록에서 vMotion으로 가상 시스템 마이그레이션 리소스 작업을 볼 수 있습니다. 리소스 작업에 아이콘을 할당할 수 있습니다. [XaaS 리소스 작업에 아이콘 할당](#) 항목을 참조하십시오.

또한 워크플로의 프레젠테이션을 편집하고 작업의 모양과 느낌을 정의했습니다.

후속 작업

비즈니스 그룹 관리자 및 테넌트 관리자는 사용 권한에 vMotion으로 가상 시스템 마이그레이션 리소스 작업을 포함시킬 수 있습니다. 가상 플랫폼에 대한 IaaS Blueprint를 생성하고 게시하는 방법에 대한 자세한 내용은 [시스템 Blueprint 설계](#) 항목을 참조하십시오.

스냅샷을 생성하도록 XaaS 작업 생성 및 게시

XaaS를 사용하여 IaaS로 프로비저닝된 vSphere 가상 시스템의 스냅샷을 생성하기 위한 리소스 작업을 생성하고 게시할 수 있습니다.

이 시나리오에서 IaaS로 프로비저닝된 vSphere 가상 시스템의 스냅샷을 생성하기 위한 리소스 작업을 생성합니다. 또한 양식 디자인너를 사용하여 워크플로 프레젠테이션을 편집하고 소비자가 작업 요청 시 작업을 보는 방식을 변경합니다.

필수 조건

vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.

프로시저

- 1 **vSphere 가상 시스템의 스냅샷을 생성하도록 작업 생성**
사용자 지정 리소스 작업을 생성하여 소비자가 IaaS로 시스템을 프로비저닝한 후 vSphere 가상 시스템의 스냅샷을 생성하도록 허용할 수 있습니다.
- 2 **스냅샷을 작성하는 작업 게시**
[스냅샷 생성] 리소스 작업을 사후 프로비저닝 작업으로 사용하려면 해당 작업을 게시해야 합니다.

vSphere 가상 시스템의 스냅샷을 생성하도록 작업 생성

사용자 지정 리소스 작업을 생성하여 소비자가 IaaS로 시스템을 프로비저닝한 후 vSphere 가상 시스템의 스냅샷을 생성하도록 허용할 수 있습니다.

프로시저

- 1 **설계 > XaaS > 리소스** 작업을 선택합니다.
- 2 **추가(+)**를 클릭합니다.
- 3 vRealize Orchestrator 워크플로 라이브러리에서 **Orchestrator > 라이브러리 > vCenter > 가상 시스템 관리 > 스냅샷**으로 이동하고 **스냅샷 생성** 워크플로를 선택합니다.
- 4 **다음**을 클릭합니다.
- 5 **리소스 유형** 드롭다운 메뉴에서 **IaaS VC VirtualMachine**을 선택합니다.
- 6 **입력 매개 변수** 드롭다운 메뉴에서 **vm**을 선택합니다.
- 7 **다음**을 클릭합니다.
- 8 리소스 작업의 이름과 설명이 **세부 정보** 탭에 나타나면 그대로 둡니다.
- 9 **다음**을 클릭합니다.
- 10 양식을 그대로 둡니다.
- 11 **추가**를 클릭합니다.

가상 시스템의 스냅샷 생성을 위한 리소스 작업을 생성했습니다. 이 리소스 작업을 리소스 작업 페이지에서 볼 수 있습니다.

후속 작업

[스냅샷을 작성하는 작업 게시](#).

스냅샷을 작성하는 작업 게시

[스냅샷 생성] 리소스 작업을 사후 프로비저닝 작업으로 사용하려면 해당 작업을 게시해야 합니다.

프로시저

- 1 **설계 > XaaS > 리소스** 작업을 선택합니다.
- 2 [스냅샷 생성] 작업에 해당하는 행을 선택하고 **게시** 버튼을 클릭합니다.

리소스 작업으로 vRealize Orchestrator 워크플로를 생성하고 게시했습니다. **관리 > 카탈로그 관리 > 작업**으로 이동하고 작업 목록에서 스냅샷 생성 리소스 작업을 볼 수 있습니다. 리소스 작업에 아이콘을 할당할 수 있습니다. [XaaS 리소스 작업에 아이콘 할당](#) 항목을 참조하십시오.

후속 작업

비즈니스 그룹 관리자 및 테넌트 관리자는 사용 권한에 스냅샷 생성 리소스 작업을 포함시킬 수 있습니다. 가상 플랫폼에 대한 IaaS Blueprint를 생성하고 게시하는 방법에 대한 자세한 내용은 [시스템 Blueprint 설계](#) 항목을 참조하십시오.

Amazon 가상 시스템을 시작하도록 XaaS 작업 생성 및 게시

XaaS를 사용하여 소비자가 타사에서 프로비저닝된 리소스에서 수행할 수 있는 작업을 확장하기 위한 작업을 생성하고 게시할 수 있습니다.

이 시나리오에서 Amazon 가상 시스템의 빠른 시작을 위한 리소스 작업을 생성하고 게시합니다.

필수 조건

- 기본 vRealize Orchestrator 서버에 Amazon Web Services를 위한 vRealize Orchestrator 플러그인을 설치합니다.
- Amazon 인스턴스의 리소스 매핑을 위해 vRealize Orchestrator 워크플로를 생성하거나 가져옵니다.

프로시저

1 Amazon 인스턴스에 대한 리소스 매핑 생성

IaaS를 사용하여 프로비저닝된 Amazon 인스턴스를 Amazon Web Services 플러그인이 제공하는 vRealize Orchestrator 유형 AWS:EC2Instance와 연결하기 위한 리소스 매핑을 생성할 수 있습니다.

2 리소스 작업을 생성하여 Amazon 가상 시스템 시작

리소스 작업을 생성하여 소비자가 프로비저닝된 Amazon 가상 시스템을 시작할 수 있도록 할 수 있습니다.

3 Amazon 인스턴스 시작 작업 게시

새로 생성한 [인스턴스 시작] 리소스 작업을 Amazon 가상 시스템에서 사후 프로비저닝 작업으로 사용하려면 해당 작업을 게시해야 합니다.

Amazon 인스턴스에 대한 리소스 매핑 생성

IaaS를 사용하여 프로비저닝된 Amazon 인스턴스를 Amazon Web Services 플러그인이 제공하는 vRealize Orchestrator 유형 AWS:EC2Instance와 연결하기 위한 리소스 매핑을 생성할 수 있습니다.

필수 조건

- vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.
- vRealize Orchestrator 리소스 매핑 워크플로 또는 스크립트 작업을 생성하거나 가져옵니다.

프로시저

- 1 **설계 > XaaS > 리소스 매핑**을 선택합니다.
- 2 **추가(+)**를 클릭합니다.
- 3 **이름** 텍스트 상자에 **EC2 인스턴스**를 입력합니다.
- 4 **카탈로그 리소스 유형** 텍스트 상자에 **클라우드 시스템**을 입력합니다.
- 5 **Orchestrator 유형** 텍스트 상자에 **AWS:EC2Instance**를 입력합니다.
- 6 **항상 사용 가능**을 선택합니다.

- 7 사용할 리소스 매핑의 유형을 선택합니다.
- 8 vRealize Orchestrator 라이브러리에서 사용자 지정 리소스 매핑 스크립트 작업 또는 워크플로를 선택합니다.
- 9 **추가**를 클릭합니다.

Amazon 리소스 매핑을 사용하여 IaaS로 프로비저닝된 Amazon 시스템에 대한 리소스 작업을 생성할 수 있습니다.

후속 작업

리소스 작업을 생성하여 [Amazon 가상 시스템 시작](#).

리소스 작업을 생성하여 Amazon 가상 시스템 시작

리소스 작업을 생성하여 소비자가 프로비저닝된 Amazon 가상 시스템을 시작할 수 있도록 할 수 있습니다.

필수 조건

vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.

프로시저

- 1 **설계 > XaaS > 리소스 작업**을 선택합니다.
- 2 **추가(+)**를 클릭합니다.
- 3 **Orchestrator > 라이브러리 > Amazon Web Services > Elastic Cloud > 인스턴스**를 선택하고 워크플로 폴더에서 **인스턴스 시작** 워크플로를 선택합니다.
- 4 **다음**을 클릭합니다.
- 5 **리소스 유형** 드롭다운 메뉴에서 **EC2 인스턴스**를 선택합니다.
이것은 이전에 생성한 리소스 매핑의 이름입니다.
- 6 **입력 매개 변수** 드롭다운 메뉴에서 **인스턴스**를 선택합니다.
이것은 리소스 매핑을 일치시킬 리소스 작업 워크플로의 입력 매개 변수입니다.
- 7 **다음**을 클릭합니다.
- 8 이름과 설명은 그대로 두십시오.
리소스 작업의 기본 이름은 [인스턴스 시작]입니다.
- 9 **다음**을 클릭합니다.
- 10 **양식** 탭에서 필드를 그대로 둡니다.
- 11 **추가**를 클릭합니다.

Amazon 가상 시스템 시작을 위한 리소스 작업을 생성했습니다. 이 리소스 작업을 리소스 작업 페이지에서 볼 수 있습니다.

후속 작업

[Amazon 인스턴스 시작 작업 게시](#).

Amazon 인스턴스 시작 작업 게시

새로 생성한 [인스턴스 시작] 리소스 작업을 Amazon 가상 시스템에서 사후 프로비저닝 작업으로 사용하려면 해당 작업을 게시해야 합니다.

필수 조건

vRealize Automation 콘솔에 **XaaS 설계자**로 로그인합니다.

프로시저

- 1 설계 > **XaaS** > 리소스 작업을 선택합니다.
- 2 [인스턴스 시작] 리소스 작업에 해당하는 행을 선택하고 **게시**를 클릭합니다.

[인스턴스 시작] 리소스 작업의 상태가 [게시됨]으로 변경됩니다.

후속 작업

Amazon 카탈로그 항목을 포함하는 사용 권한에 인스턴스 시작 작업을 추가합니다. [사용자에게 서비스, 카탈로그 항목 및 작업에 대한 사용 권한 부여](#) 항목을 참조하십시오.

XaaS Blueprint의 잘못된 악센트 기호 및 특수 문자 문제 해결

ASCII가 아닌 문자열을 사용하는 언어에 대해 XaaS Blueprint를 생성할 때 악센트 기호 및 특수 문자가 사용 불가능한 문자열로 표시됩니다.

원인

기본적으로 설정되지 않는 vRealize Orchestrator 구성 속성이 설정되어 있을 수 있습니다.

해결 방법

- 1 Orchestrator 서버 시스템에서 `/etc/vco/app-server/`로 이동합니다.
- 2 텍스트 편집기에서 `vmo.properties` 구성 파일을 엽니다.
- 3 다음 속성을 사용하지 않도록 설정했는지 확인합니다.

```
com.vmware.o11n.webview.htmlescaping.disabled
```

- 4 `vmo.properties` 파일을 저장합니다.
- 5 vRealize Orchestrator 서버를 다시 시작합니다.

Blueprint 게시

Blueprint는 초안 상태로 저장되며, 카탈로그 항목으로 구성하거나 설계 캔버스의 Blueprint 구성 요소로 사용하기 위해서는 수동으로 게시해야 합니다.

Blueprint를 게시한 이후에는 서비스 카탈로그에서 프로비저닝 요청에 사용할 수 있게 Blueprint에 사용 권한을 부여할 수 있습니다.

Blueprint는 한 번만 게시하면 됩니다. 게시된 Blueprint에서 변경한 내용이 카탈로그와 중첩된 Blueprint 구성 요소에 자동으로 반영됩니다.

Blueprint 게시

Blueprint는 시스템 프로비저닝에 사용하고, 필요한 경우 다른 Blueprint에 재사용하기 위해 게시할 수 있습니다. 시스템 프로비저닝을 요청하는 데 Blueprint를 사용하려면 Blueprint를 게시한 이후에 사용 권한을 부여해야 합니다. 다른 Blueprint의 구성 요소로 사용되는 Blueprint에는 사용 권한이 필요하지 않습니다.

필수 조건

- vRealize Automation 콘솔에 **인프라 설계자**로 로그인합니다.
- Blueprint를 생성합니다. vRealize Automation Blueprint 생성 검사 목록을 참조하십시오.

프로시저

- 1 **설계** 탭을 클릭합니다.
- 2 **Blueprint**를 클릭합니다.
- 3 게시할 Blueprint를 가리키고 **게시**를 클릭합니다.
- 4 **확인**을 클릭합니다.

Blueprint가 카탈로그 항목으로 게시되지만, 사용자들이 서비스 카탈로그에서 사용할 수 있으려면 Blueprint에 사용 권한을 먼저 부여해야 합니다.

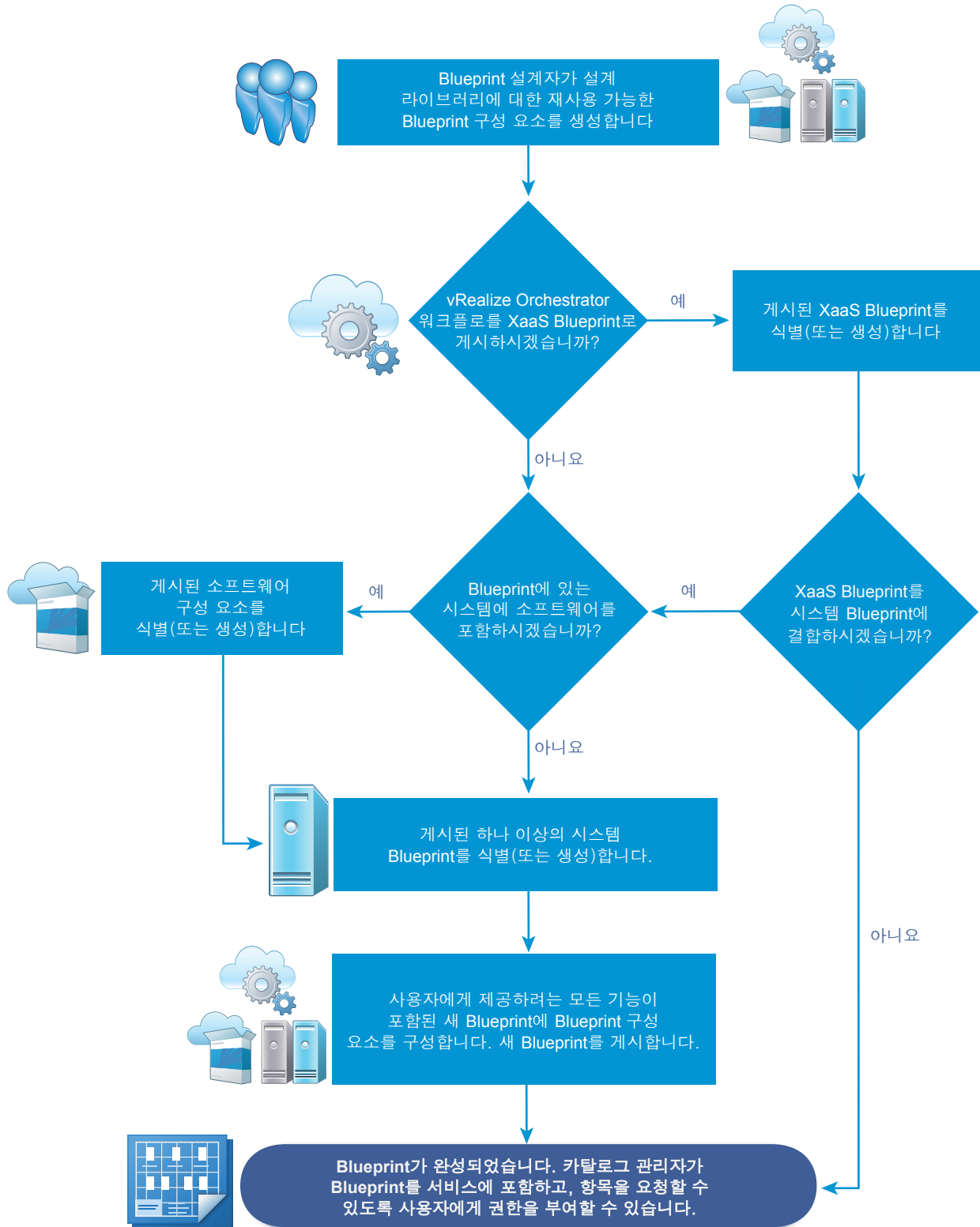
후속 작업

Blueprint를 카탈로그 서비스에 추가하고, Blueprint에 정의된 대로 카탈로그 항목을 시스템 프로비저닝을 위해 요청할 수 있도록 사용자에게 사용 권한을 부여합니다.

복합 Blueprint 구성

게시된 Blueprint 및 Blueprint 구성요소를 재사용하고 새로운 방식으로 결합하여 사용자에게 정교한 기능을 제공하는 IT 서비스 패키지를 생성할 수 있습니다.

그림 3-5. 복합 Blueprint 구성 워크플로



■ 중첩된 Blueprint 동작 이해

Blueprint를 다른 Blueprint 안에 구성 요소로 중첩하여 Blueprint를 재사용할 수 있습니다. 시스템 프로비저닝 시 재사용 및 모듈성 제어를 위해 Blueprint를 중첩하지만 중첩된 Blueprint를 사용할 때에는 특정 규칙과 고려 사항이 있습니다.

■ Software 구성 요소를 지원하는 시스템 구성 요소 선택

Blueprint를 구성할 때 지원되는 시스템 구성 요소 위에 Software 구성 요소를 배치하여 해당 구성 요소를 전달합니다.

■ Blueprint 구성 요소 간 속성 바인딩 생성

여러 배포 시나리오에서 구성 요소 자체를 사용자 지정하려면 다른 구성 요소의 속성 값이 필요합니다. XaaS, 시스템, Software의 속성 및 사용자 지정 속성을 Blueprint의 다른 속성에 바인딩할 수 있습니다.

■ 명시적 종속성 생성 및 프로비저닝 순서 제어

Blueprint의 한 구성 요소의 프로비저닝을 완료하기 위해 다른 구성 요소의 정보가 필요한 경우 종속 구성 요소가 너무 이르게 프로비저닝되지 않도록 설계 캔버스에 명시적 종속성을 설정하여 프로비저닝에 시차를 둘 수 있습니다. 명시적 종속성은 배포의 빌드 순서를 제어하고 확장/축소 작업 중에 항상 종속 업데이트를 트리거합니다.

중첩된 Blueprint 동작 이해

Blueprint를 다른 Blueprint 안에 구성 요소로 중첩하여 Blueprint를 재사용할 수 있습니다. 시스템 프로비저닝 시 재사용 및 모듈성 제어를 위해 Blueprint를 중첩하지만 중첩된 Blueprint를 사용할 때에는 특정 규칙과 고려 사항이 있습니다.

중첩된 Blueprint를 하나 이상 포함하는 Blueprint를 외부 Blueprint라고 합니다. 다른 Blueprint를 생성 또는 편집하는 동안 하나의 Blueprint 구성 요소를 설계 캔버스에 추가하는 경우 이 Blueprint 구성 요소를 중첩된 Blueprint라고 하며 이 Blueprint가 추가되는 컨테이너 Blueprint를 외부 Blueprint라고 합니다.

중첩된 Blueprint를 사용할 때에는 고려해야 할 점이 명확하지 않은 경우가 종종 발생합니다. 시스템 프로비저닝 기능을 최대한 활용하려면 규칙 및 고려 사항을 이해하는 것이 중요합니다.

Blueprint 중첩을 위한 일반 규칙 및 고려 사항

- Blueprint 복잡성을 최소화하려면 Blueprint의 깊이를 세 개 수준으로 제한하고 최상위 Blueprint가 이 세 개 수준 중 하나가 되도록 하는 것이 좋습니다.
- 외부 Blueprint에 대한 사용 권한을 부여받은 사용자는 이 Blueprint의 중첩된 Blueprint에 대한 사용 권한도 부여받습니다.
- Blueprint에 승인 정책을 적용할 수 있습니다. 승인된 경우 중첩된 Blueprint를 포함하여 Blueprint 카탈로그 항목과 모든 해당 구성 요소가 프로비저닝됩니다. 다른 구성 요소에 다른 승인 정책을 적용할 수도 있습니다. 요청된 Blueprint가 프로비저닝되기 전에 모든 승인 정책이 승인되어야 합니다.

- 게시된 Blueprint를 편집할 때 해당 Blueprint를 사용하여 이미 프로비저닝된 배포는 변경되지 않습니다. 따라서 프로비저닝할 때 배포는 중첩된 Blueprint를 포함하여 Blueprint에서 현재 값을 읽어옵니다. 프로비저닝된 배포에 전달할 수 있는 유일한 변경 내용은 소프트웨어 구성 요소에 대한 편집입니다(예: 업데이트 또는 제거 스크립트에 대한 편집).
- 외부 Blueprint에 정의된 설정은 중첩된 Blueprint에 구성된 설정에 우선하지만 다음과 같은 예외가 있습니다.
 - 중첩된 Blueprint의 이름은 변경할 수 있지만 중첩된 Blueprint 내부의 시스템 구성 요소 또는 기타 구성 요소의 이름은 변경할 수 없습니다.
 - 중첩된 Blueprint의 시스템 구성 요소에 대한 사용자 지정 속성을 추가 또는 삭제할 수 없습니다. 하지만 그러한 사용자 지정 속성을 편집할 수는 있습니다. 중첩된 Blueprint의 시스템 구성 요소에 대한 속성 그룹을 추가, 편집 또는 삭제할 수 없습니다.
- 귀하 또는 다른 설계자가 중첩된 Blueprint 설정에 대해 변경한 내용은 외부 Blueprint에서 그러한 설정을 재정의한 경우가 아니면 외부 Blueprint에 나타납니다.
- 외부 Blueprint의 최대 리스 시간을 구성 요소 Blueprint의 가장 낮은 최대 리스 값으로 제한합니다.

중첩된 Blueprint와 외부 Blueprint에 지정되는 리스 시간을 아무 값으로 설정할 수 있지만, 외부 Blueprint의 최대 리스 시간은 중첩된 Blueprint의 가장 낮은 최대 리스 값으로 제한되어야 합니다. 그러면 애플리케이션 설계자는 인프라 설계자가 식별한 제약 조건 이내에서 균일하면서 가변적인 리스 값을 갖는 복합 Blueprint를 설계할 수 있습니다. 중첩된 Blueprint에 정의된 최대 리스 값이 외부 Blueprint에 정의된 값보다 작은 경우 프로비저닝 요청이 실패합니다.

- 외부 Blueprint에서 작업할 때 중첩된 Blueprint의 시스템 구성 요소에 대해 구성되는 시스템 리소스 설정을 재정의할 수 있습니다.
- 외부 Blueprint에서 작업할 때 소프트웨어 구성 요소를 중첩된 Blueprint 내의 시스템 구성 요소 위로 끌어올 수 있습니다.
- 중첩된 Blueprint의 시스템 구성 요소가 제거되었거나 해당 ID가 변경되었고 해당 시스템 구성 요소가 현재 Blueprint의 구성 요소와 연결되어 있는 Blueprint를 열면 연결된 구성 요소가 제거되고 다음과 같은 메시지가 나타납니다.

현재 Blueprint의 구성 요소에서 참조되는 중첩된 Blueprint의 시스템 구성 요소가 제거되었거나 해당 시스템 구성 요소 ID가 변경되었습니다. 누락되거나 변경된 시스템 구성 요소 ID와 연결된 현재 Blueprint의 모든 구성 요소가 제거되었습니다. 중첩된 Blueprint의 누락 또는 변경된 시스템 구성 요소 ID와 현재 Blueprint 구성 요소 간의 연결 기록을 유지하고 중첩된 Blueprint에서 문제를 해결하려면 [취소]를 클릭합니다. 중첩된 Blueprint를 열고 누락된 시스템 구성 요소를 원래 ID로 다시 추가하거나 시스템 구성 요소 ID를 원래 ID로 변경합니다. 중첩된 Blueprint의 누락 또는 변경된 시스템 구성 요소 ID와 현재 Blueprint 구성 요소 간의 연결 기록을 모두 제거하려면 [저장]을 클릭합니다.

Blueprint 중첩을 위한 네트워킹 및 보안 규칙 및 고려 사항

- 외부 Blueprint의 네트워킹 및 보안 구성 요소는 중첩된 Blueprint에서 정의된 시스템과 연결될 수 있습니다.

- NSX 네트워크, 보안, 로드 밸런서 구성 요소 및 해당 설정은 중첩된 Blueprint에서 지원되지 않습니다.
- 외부 Blueprint에서 App 분리가 적용되는 경우, 이것은 중첩된 Blueprint에 지정된 App 분리 설정을 재정의합니다.
- 외부 Blueprint에서 정의된 전송 영역 설정은 중첩된 Blueprint에 지정된 전송 영역 설정을 재정의합니다.
- 외부 Blueprint에서 작업할 때 내부 또는 중첩된 Blueprint에서 구성되는 시스템 구성 요소 설정 및 네트워크 구성 요소 설정과 관련된 로드 밸런서 설정을 구성할 수 있습니다.
- 요청 시 NAT 네트워크 구성 요소가 포함된 중첩된 Blueprint의 경우, 요청 시 NAT 네트워크 구성 요소에 지정된 IP 범위는 외부 Blueprint에서 편집할 수 없습니다.
- 외부 Blueprint는 요청 시 네트워크 설정 또는 요청 시 로드 밸런서 설정이 포함된 내부 Blueprint를 포함할 수 없습니다. NSX 요청 시 네트워크 구성 요소 또는 NSX 로드 밸런서 구성 요소가 포함된 내부 Blueprint의 사용은 지원되지 않습니다.
- NSX 네트워크 또는 보안 구성 요소가 포함된 중첩된 Blueprint의 경우, 중첩된 Blueprint에 지정된 네트워크 프로파일 또는 보안 정책 정보를 변경할 수 없습니다. 하지만 외부 Blueprint에 추가하는 다른 vSphere 시스템 구성 요소에 대한 설정은 재사용할 수 있습니다.
- 중첩된 Blueprint의 NSX 네트워크 및 보안 구성 요소가 복합 Blueprint에서 고유하게 명명되도록 vRealize Automation은 아직 고유하지 않은 네트워크 및 보안 구성 요소 이름 앞에 중첩된 Blueprint ID를 접두사로 추가합니다. 예를 들어 외부 Blueprint에 ID 이름이 xbp_1인 Blueprint를 추가했고 두 Blueprint 모두에 OD_Security_Group_1이라는 요청 시 보안 그룹 구성 요소가 포함된 경우 중첩된 Blueprint 구성 요소의 이름이 Blueprint 설계 캔버스에서 xbp_1_OD_Security_Group_1로 변경됩니다. 외부 Blueprint의 네트워크 및 보안 구성 요소 이름에는 접두사가 추가되지 않습니다.
- 구성 요소가 어느 Blueprint에 있는지에 따라 구성 요소 설정이 변경될 수 있습니다. 예를 들어 보안 그룹, 보안 태그 또는 요청 시 네트워크를 내부 및 외부 Blueprint 수준 모두에 포함하는 경우 외부 Blueprint의 설정이 내부 Blueprint의 설정을 재정의합니다. 네트워크 및 보안 구성 요소는 내부 Blueprint 수준에서 작동하는 기존 네트워크만 예외로 하고 외부 Blueprint 수준에서만 지원됩니다. 이 문제를 방지하려면 모든 보안 그룹, 보안 태그 또는 요청 시 네트워크를 외부 Blueprint에만 추가합니다.

Blueprint 중첩을 위한 소프트웨어 구성 요소 고려 사항

확장 가능 Blueprint의 경우 다른 Blueprint를 재사용하지 않는 단일 계층 Blueprint를 생성하는 것이 좋습니다. 일반적으로, 확장/축소 작업 중의 업데이트 프로세스는 소프트웨어 속성을 시스템 속성에 바인딩할 때 생성하는 종속성과 같은 명시적 종속성에 의해 트리거됩니다. 하지만 중첩된 Blueprint의 경우 명시적 종속성이 항상 업데이트 프로세스를 트리거하는 것은 아닙니다. 확장 가능 Blueprint에서 중첩된 Blueprint를 사용하려는 경우 중첩된 Blueprint의 구성 요소 간에 수동으로 종속성을 설정하여 업데이트를 항상 트리거하는 명시적 종속성을 생성할 수 있습니다.

Software 구성 요소를 지원하는 시스템 구성 요소 선택

Blueprint를 구성할 때 지원되는 시스템 구성 요소 위에 Software 구성 요소를 배치하여 해당 구성 요소를 전달합니다.

Software 구성 요소를 지원하려면 선택하는 시스템 Blueprint에 게스트 에이전트 및 Software 부트스트랩 에이전트가 포함된 Amazon 시스템 이미지, 템플릿 또는 스냅샷을 기반으로 한 시스템 구성 요소가 포함되어야 하며 지원되는 프로비저닝 방법을 사용해야 합니다.

Software 에이전트는 IPv6(인터넷 프로토콜 버전 6)을 지원하지 않기 때문에 IPv4 설정을 사용합니다.

확장 가능한 Blueprint를 설계 중인 경우 다른 Blueprint를 재사용하지 않는 단일 계층 Blueprint를 생성하는 것이 좋습니다. 일반적으로 확장 작업 중에 사용되는 업데이트 프로세스는 속성 바인딩과 같은 암시적 종속성에 의해 트리거됩니다. 하지만 중첩된 Blueprint의 경우 명시적 종속성이 항상 업데이트 프로세스를 트리거하는 것은 아닙니다.

Blueprint 구성은 IaaS 설계자, 애플리케이션 설계자, 소프트웨어 설계자가 모두 수행할 수 있지만 시스템 구성 요소 구성은 IaaS 설계자만 수행할 수 있습니다. IaaS 설계자가 아닌 경우 고유한 시스템 구성 요소를 구성할 수 없지만 IaaS 설계자가 생성 및 게시한 시스템 Blueprint를 재사용할 수 있습니다.

설계 캔버스에 소프트웨어 구성 요소를 추가하려면 대상 카탈로그에 대해 비즈니스 그룹 구성원, 비즈니스 그룹 관리자 또는 테넌트 관리자 역할 액세스 권한도 있어야 합니다.

확장 가능 Blueprint에서 중첩된 Blueprint를 사용하려는 경우 중첩된 Blueprint의 구성 요소 간에 수동으로 종속성을 설정하여 업데이트를 항상 트리거하는 명시적 종속성을 생성할 수 있습니다.

표 3-64. Software 를 지원하는 프로비저닝 방법

시스템 유형	프로비저닝 방법
vSphere	복제
vSphere	연결된 복제
vCloud Director	복제
vCloud Air	복제
Amazon AWS	Amazon 시스템 이미지

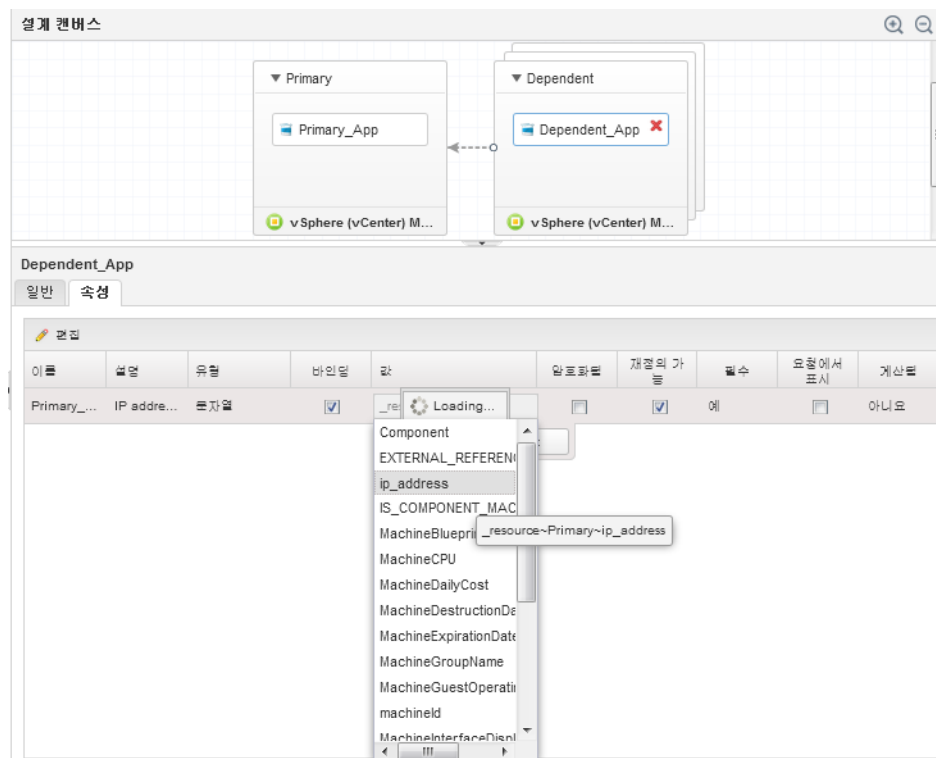
Blueprint 구성 요소 간 속성 바인딩 생성

여러 배포 시나리오에서 구성 요소 자체를 사용자 지정하려면 다른 구성 요소의 속성 값이 필요합니다. XaaS, 시스템, Software의 속성 및 사용자 지정 속성을 Blueprint의 다른 속성에 바인딩할 수 있습니다.

예를 들어 소프트웨어 설계자는 WAR 구성 요소의 수명 주기 스크립트의 속성 정의를 수정할 수 있습니다. WAR 구성 요소에는 Apache Tomcat 서버 구성 요소의 설치 위치가 필요할 수 있으므로 소프트웨어 설계자가 server_home 속성 값을 Apache Tomcat 서버 install_path 속성 값으로 설정하도록 WAR 구성 요소를 구성합니다. 설계자가 Blueprint를 구성할 때 Software 구성 요소가 성공적으로 프로비저닝되도록 server_home 속성을 Apache Tomcat 서버 install_path 속성에 바인딩해야 합니다.

Blueprint에서 구성 요소를 구성할 때 속성 바인딩을 설정합니다. [Blueprint] 페이지에서 구성 요소를 캔버스에 끌어다 놓고 **속성** 탭을 클릭합니다. 속성을 Blueprint의 다른 속성에 바인딩하려면 **바인딩** 확인란을 선택합니다. 값 텍스트 상자에 ComponentName~PropertyName을 입력하거나 아래쪽 화살표를 사용하여 사용 가능한 바인딩 옵션 목록을 생성할 수 있습니다. 물결표 문자(~)를 구성 요소와 속성 간의 구분 기호로 사용합니다. 예를 들어 속성 dp_port에 바인딩하려면 MySQL 소프트웨어 구성 요소에서 mysql~db_port를 입력할 수 있습니다. 시스템의 IP 주소 또는 Software 구성 요소의 호스트 이름과 같이 프로비저닝 중 구성된 속성에 바인딩하려면 _resource~ComponentName~PropertyName을 입력합니다. 예를 들어 시스템의 예약 이름에 바인딩하려면 _resource~vSphere_Machine_1~MachineReservationName을 입력할 수 있습니다.

그림 3-6. 시스템의 IP 주소에 소프트웨어 속성 바인딩



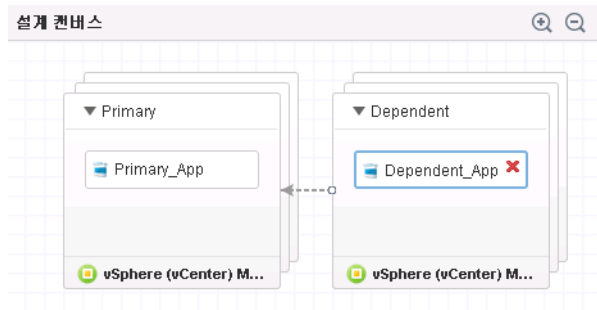
명시적 종속성 생성 및 프로비저닝 순서 제어

Blueprint의 한 구성 요소의 프로비저닝을 완료하기 위해 다른 구성 요소의 정보가 필요한 경우 종속 구성 요소가 너무 이르게 프로비저닝되지 않도록 설계 캔버스에 명시적 종속성을 설정하여 프로비저닝에 시차를 둘 수 있습니다. 명시적 종속성은 배포의 빌드 순서를 제어하고 확장/축소 작업 중에 항상 종속 업데이트를 트리거합니다.

여러 개의 시스템과 애플리케이션이 포함된 Blueprint를 설계하는 경우, 한 시스템에서 애플리케이션 설치를 완료하기 위해 다른 시스템의 속성이 필요할 수 있습니다. 예를 들어 웹 서버를 구축하는 경우에는 데이터베이스 서버의 호스트 이름을 알고 있어야 애플리케이션을 설치하고 데이터베이스 테이블을 인스턴스화할 수 있습니다. 명시적 종속성을 매핑하는 경우 웹 서버에서 프로비저닝이 완료되면 데이터베이스 서버가 프로비저닝을 시작합니다.

설계 캔버스에서 종속성을 매핑하려면 종속 구성 요소와 사용자가 종속되는 구성 요소를 잇는 선을 그립니다. 완료하면 두 번째로 구축할 구성 요소에 맨 처음 구축한 구성 요소를 가리키는 화살표가 표시됩니다. 예를 들어 '종속성을 매핑하여 빌드 순서 제어' 그림에서 종속 시스템은 기본 시스템이 구축될 때까지 프로비저닝되지 않습니다. 또는 두 시스템을 동시에 프로비저닝하되 소프트웨어 구성 요소 간에 종속성을 설정하도록 구성할 수 있습니다.

그림 3-7. 종속성을 매핑하여 빌드 순서 제어

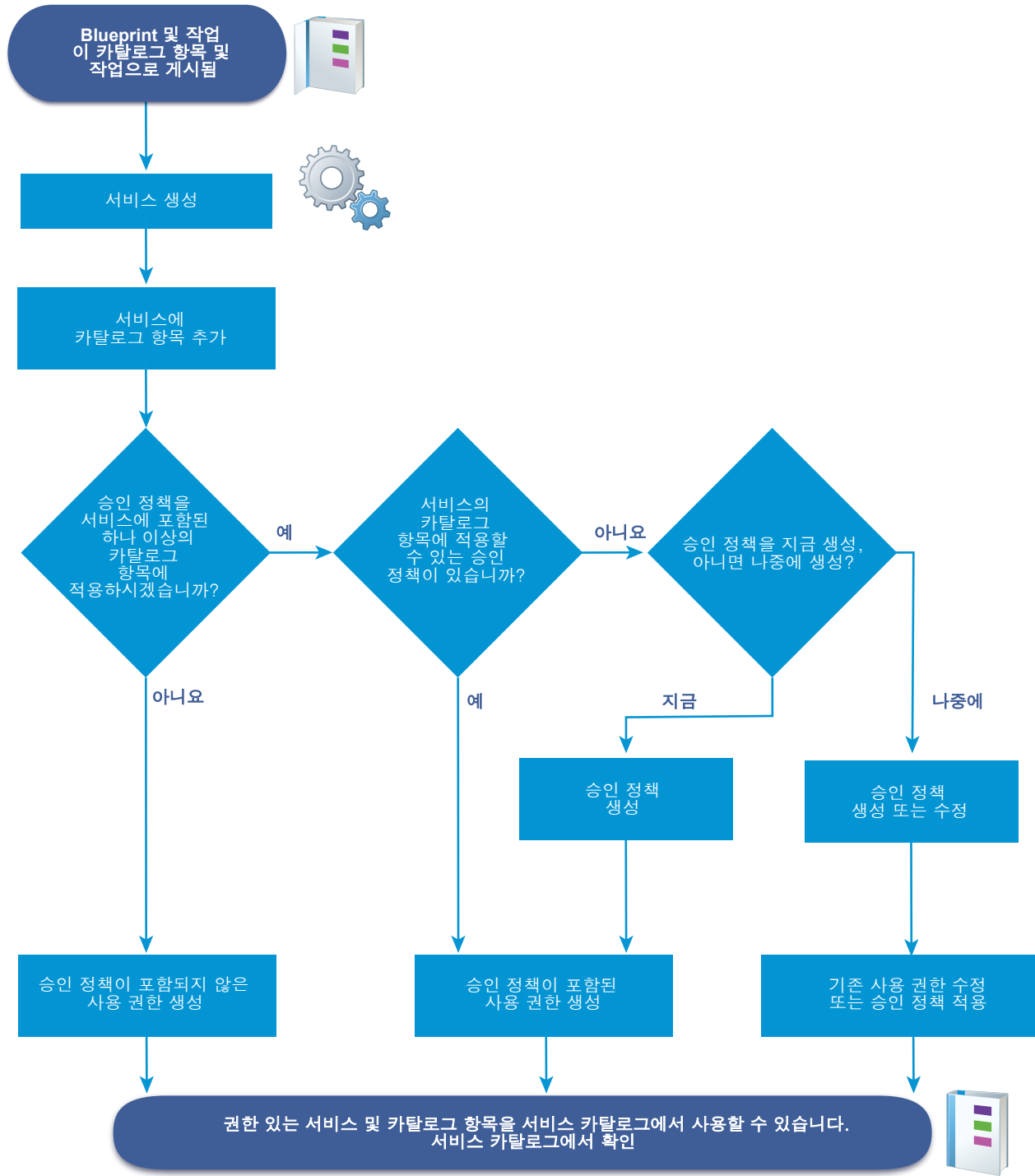


확장 가능한 Blueprint를 설계 중인 경우 다른 Blueprint를 재사용하지 않는 단일 계층 Blueprint를 생성하는 것이 좋습니다. 일반적으로, 확장/축소 작업 중의 업데이트 프로세스는 소프트웨어 속성을 시스템 속성에 바인딩할 때 생성하는 종속성과 같은 명시적 종속성에 의해 트리거됩니다. 하지만 중첩된 Blueprint의 경우 명시적 종속성이 항상 업데이트 프로세스를 트리거하는 것은 아닙니다. 확장 가능 Blueprint에서 중첩된 Blueprint를 사용하려는 경우 중첩된 Blueprint의 구성 요소 간에 수동으로 종속성을 설정하여 업데이트를 항상 트리거하는 명시적 종속성을 생성할 수 있습니다.

서비스 카탈로그 관리

서비스 카탈로그는 사용자가 시스템 및 기타 항목을 프로비저닝하기 위해 요청하는 곳입니다. 서비스를 구축하고, 사용자에게 하나 이상의 항목에 대한 사용 권한을 부여하고 거버넌스를 적용하는 방법에 기반하여 서비스 카탈로그 항목에 대한 사용자 액세스를 관리합니다.

서비스 카탈로그에 항목을 추가하기 위해 따르는 워크플로는 승인 정책을 생성 및 적용하는지 여부에 따라 다릅니다.



서비스 카탈로그 구성을 위한 검사 목록

Blueprint와 작업을 생성하고 게시한 후에 vRealize Automation 서비스를 생성하고, 카탈로그 항목을 구성하고, 사용 권한 및 승인을 할당할 수 있습니다.

서비스 카탈로그 검사 목록 구성은 카탈로그를 구성하는 데 필요한 단계에 대한 개괄적인 개요를 제공하고 각 단계에 대한 자세한 지침 또는 결정 시점에 대한 링크를 제공합니다.

표 3-65. 서비스 카탈로그 검사 목록 구성

작업	필요한 역할	세부 정보
<input type="checkbox"/> 서비스를 추가합니다.	테넌트 관리자 또는 카탈로그 관리자	서비스 추가 항목을 참조하십시오.
<input type="checkbox"/> 서비스에 카탈로그 항목을 추가합니다.	테넌트 관리자 또는 카탈로그 관리자	서비스에 카탈로그 항목 추가 항목을 참조하십시오.
<input type="checkbox"/> 서비스에서 카탈로그 항목을 구성합니다.	테넌트 관리자 또는 카탈로그 관리자	카탈로그 항목 구성 항목을 참조하십시오.
<input type="checkbox"/> 사용 권한을 생성하고 카탈로그 항목에 적용합니다.	테넌트 관리자 또는 비즈니스 그룹 관리자	사용자에게 서비스, 카탈로그 항목 및 작업에 대한 사용 권한 부여 항목을 참조하십시오.
<input type="checkbox"/> 승인 정책을 생성하고 카탈로그 항목에 적용합니다.	테넌트 관리자 또는 승인 관리자가 승인 정책을 생성할 수 있음 테넌트 관리자 또는 비즈니스 그룹 관리자가 승인 정책을 적용할 수 있음	승인 정책 생성 항목을 참조하십시오.

서비스 생성

서비스는 서비스 카탈로그에 포함하려는 카탈로그 항목 그룹입니다. 서비스에 대한 사용 권한을 부여할 수 있고(연결된 모든 카탈로그 항목에 대한 사용 권한이 비즈니스 그룹 사용자에게 부여됨) 서비스에 승인 정책을 적용할 수 있습니다.

서비스는 카탈로그 항목의 동적 그룹으로 작동합니다. 서비스에 대한 사용 권한을 부여하면 지정된 사용자가 서비스와 연결된 모든 카탈로그 항목을 서비스 카탈로그에서 사용할 수 있으며 서비스에 추가 또는 서비스에서 제거한 카탈로그 항목이 서비스 카탈로그에 영향을 미칩니다.

서비스를 생성할 때 이를 서비스 범주로 사용하여 서비스 카탈로그 사용자를 위한 서비스 오퍼링을 구성할 수 있습니다. 예를 들어 Windows 7, 8 및 10 운영 체제 카탈로그 항목을 포함하는 Windows 데스크톱 서비스 또는 CentOS 및 RHEL 운영 체제 항목을 포함하는 Linux 서비스를 구성할 수 있습니다.

서비스 추가

서비스를 추가하여 서비스 카탈로그 사용자가 카탈로그 항목을 사용할 수 있게 합니다. 사용자에게 항목에 대한 권한을 부여할 수 있도록 모든 카탈로그 항목을 서비스와 연결해야 합니다.

사용자에 대한 서비스 사용 권한이 부여되는 경우 서비스 카탈로그에 카탈로그 항목이 함께 나타납니다. 사용자에게 개별 카탈로그 항목에 대한 사용 권한을 부여할 수도 있습니다.

필수 조건

테넌트 관리자 또는 카탈로그 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 관리 > 카탈로그 관리 > 서비스를 선택합니다.

2 새로 만들기 아이콘(+)을 클릭합니다.

3 이름과 설명을 입력합니다.

해당 값은 카탈로그 사용자에게 대한 서비스 카탈로그에 나타납니다.

4 서비스 카탈로그의 서비스에 대한 특정 아이콘을 추가하려면 **찾아보기**를 클릭하고 이미지를 선택합니다.

지원되는 이미지 파일 형식은 GIF, JPG 및 PNG입니다. 표시되는 이미지는 40 x 40픽셀입니다. 사용자 지정 이미지를 선택하지 않는 경우 서비스 카탈로그에 기본 아이콘이 나타납니다.

5 상태 드롭다운 메뉴에서 상태를 선택합니다.

옵션	설명
비활성	서비스가 서비스 카탈로그에서 사용 가능하지 않습니다. 서비스가 이 상태인 경우 카탈로그 항목을 서비스와 연결할 수 있지만 사용자에게 서비스에 대한 사용 권한을 부여할 수는 없습니다. 활성이며 사용 권한이 부여된 서비스에 대해 비활성 을 선택하는 경우 해당 서비스가 재활성화할 때까지 서비스 카탈로그에서 제거됩니다.
활성	(기본값) 서비스 및 연결된 카탈로그 항목에 대한 사용 권한을 사용자에게 부여할 수 있으며 사용 권한이 부여된 경우 서비스 및 연결된 카탈로그 항목을 해당 사용자에게 대한 서비스 카탈로그에서 사용할 수 있습니다.
삭제됨	vRealize Automation에서 서비스가 제거됩니다. 연결된 모든 카탈로그 항목이 여전히 존재하지만 서비스 카탈로그의 서비스와 연결된 항목을 카탈로그 사용자가 사용할 수 없습니다.

6 서비스 설정을 구성합니다.

다음 설정은 서비스 카탈로그 사용자에게 정보를 제공합니다. 이 설정은 서비스 가용성에 영향을 미치지 않습니다.

옵션	설명
시간	지원 팀의 가용성에 맞게 시간을 구성합니다. 시간은 현지 시간을 기반으로 합니다. 서비스 시간은 어떤 날에서 다른 날까지 이어질 수 없습니다. 예를 들어 서비스 시간을 오후 4:00에서 오전 4:00로 설정할 수 없습니다. 자정을 넘기려면 2개의 사용 권한을 생성합니다. 하나는 오후 4:00에서 오전 12:00까지의 사용 권한이고 다른 하나는 오전 12:00에서 오전 4:00까지의 사용 권한입니다.
소유자	서비스 및 연결된 카탈로그 항목의 기본 소유자인 사용자 또는 사용자 그룹을 지정합니다.
지원 팀	서비스 카탈로그 사용자가 서비스를 사용하여 항목을 프로비저닝할 때 발생하는 문제에 대해 지원할 수 있는 사용자 지정 사용자 그룹 또는 사용자를 지정합니다.
기간 변경	서비스를 변경할 계획인 날짜와 시간을 선택합니다. 지정된 날짜와 시간은 정보 제공용이며 서비스 가용성에 영향을 미치지 않습니다.

7 추가를 클릭합니다.

후속 작업

사용자에게 항목에 대한 사용 권한을 부여할 수 있도록 카탈로그 항목을 서비스와 연결합니다. [서비스에 카탈로그 항목 추가](#) 항목을 참조하십시오.

서비스에 카탈로그 항목 추가

사용자에게 서비스 카탈로그의 항목을 요청하는 권한을 부여할 수 있도록 서비스에 카탈로그 항목을 추가합니다. 카탈로그 항목은 하나의 서비스와만 연결할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **카탈로그 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 서비스가 존재하는지 확인합니다. [서비스 추가](#) 항목을 참조하십시오.
- 하나 이상의 카탈로그 항목이 게시되었는지 확인합니다. [카탈로그 항목 구성](#) 항목을 참조하십시오.

프로시저

- 1 **관리 > 카탈로그 관리 > 서비스**를 선택합니다.
- 2 카탈로그 항목을 추가할 서비스를 선택하고 **카탈로그 항목 관리**를 클릭합니다.
- 3 **카탈로그 항목** 아이콘(+)을 클릭합니다.
 - a 이 서비스에 포함할 카탈로그 항목을 선택합니다.
[카탈로그 항목 선택] 대화상자에는 서비스와 연결되지 않은 항목만 표시됩니다.
 - b **추가**를 클릭합니다.
- 4 **닫기**를 클릭합니다.

후속 작업

- 서비스 카탈로그의 항목과 함께 나타나게 되는 카탈로그 항목에 사용자 지정 아이콘을 추가할 수 있습니다. [카탈로그 항목 구성](#) 항목을 참조하십시오.
- 사용자가 서비스 카탈로그의 서비스 또는 카탈로그 항목을 요청할 수 있도록 사용자에게 이러한 항목에 대한 권한을 부여합니다. [사용 권한 생성](#) 항목을 참조하십시오.

카탈로그 항목 및 작업 사용

카탈로그 항목은 시스템, 소프트웨어 구성 요소 및 기타 개체에 대한 게시된 Blueprint입니다. 카탈로그 관리 영역의 작업은 프로비저닝된 카탈로그 항목에서 실행할 수 있는 게시된 작업입니다. 목록을 사용하여 서비스 카탈로그 사용자가 사용할 수 있도록 게시할 Blueprint 및 작업을 결정할 수 있습니다.

게시된 카탈로그 항목

카탈로그 항목은 게시된 Blueprint입니다. 게시된 Blueprint는 다른 Blueprint에서도 사용될 수 있습니다. 다른 Blueprint에서의 Blueprint 재사용은 카탈로그 항목 목록에 표시되지 않습니다.

게시된 카탈로그 항목에는 Blueprint의 구성 요소로만 구성된 항목도 포함될 수 있습니다. 예를 들어 게시된 소프트웨어 구성 요소는 카탈로그 항목으로 나열되지만 배포의 일부로만 사용할 수 있습니다.

권한 있는 사용자가 서비스 카탈로그에서 사용할 수 있도록 하려면 배포 카탈로그 항목을 서비스에 연결해야 합니다. 서비스 카탈로그에는 활성 항목만 나타납니다. 카탈로그 항목을 다른 서비스로 구성하고, 서비스 카탈로그에서 임시로 제거하려는 경우 사용되지 않도록 설정하고, 카탈로그에 표시되는 사용자 지정 아이콘을 추가할 수 있습니다.

게시된 작업

작업은 프로비저닝된 카탈로그 항목에 대해 수행할 수 있는 변경입니다. 예를 들어 가상 시스템을 재부팅할 수 있습니다.

작업에는 기본 작업 또는 XaaS를 사용하여 생성된 작업이 포함될 수 있습니다. 기본 작업은 시스템 또는 다른 제공된 Blueprint를 추가할 때 추가됩니다. XaaS 작업을 생성하고 게시해야 합니다.

작업은 서비스에 연결되어 있지 않습니다. 작업이 실행되는 카탈로그 항목이 포함된 사용 권한에 작업을 포함해야 합니다. 사용자에게 권한이 있는 작업은 서비스 카탈로그에 나타나지 않습니다. 작업은 항목과 항목의 현재 상태에 적용 가능한지 여부에 따라 서비스 카탈로그 사용자의 **항목** 탭에서 프로비저닝된 항목에 사용 가능합니다.

항목 탭에 나타나는 작업에 사용자 지정 아이콘을 추가할 수 있습니다.

카탈로그 항목 구성

카탈로그 항목은 사용자에게 사용 권한을 부여할 수 있는 게시된 Blueprint입니다. 카탈로그 항목 옵션을 사용하면 상태 또는 연결된 서비스를 변경할 수 있습니다. 또한 선택된 카탈로그 항목이 포함된 사용 권한을 볼 수도 있습니다.

서비스에 연결되고 사용자에게 사용 권한이 부여된 카탈로그 항목만 서비스 카탈로그에 나타납니다. 카탈로그 항목은 하나의 서비스에만 연결될 수 있습니다.

카탈로그 항목을 사용 권한 또는 게시된 카탈로그 항목 목록에서 제거하지 않고도 서비스 카탈로그에 표시되지 않게 하려면 해당 항목을 비활성화합니다. 비활성화된 카탈로그 항목은 그리드에서 회수된 상태이고 구성 세부 정보에서는 비활성 상태입니다. 이 항목은 나중에 활성화할 수 있습니다.

필수 조건

- **데넌트 관리자** 또는 **카탈로그 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 하나 이상의 Blueprint를 카탈로그 항목으로 게시했는지 확인합니다. **Blueprint 게시** 항목을 참조하십시오.

프로시저

- 1 **관리 > 카탈로그 관리 > 카탈로그 항목**을 선택합니다.
- 2 카탈로그 항목을 선택하고 **구성**을 클릭합니다.

3 카탈로그 항목 설정을 구성합니다.

옵션	설명
아이콘	이미지를 찾습니다. 지원되는 이미지 파일 형식은 GIF, JPG 및 PNG입니다. 표시되는 이미지는 40 x 40픽셀입니다. 사용자 지정 이미지를 선택하지 않는 경우 서비스 카탈로그에 기본 카탈로그 아이콘이 나타납니다.
상태	가능한 값은 활성 , 비활성 및 스테이징 입니다. <ul style="list-style-type: none"> ■ 활성. 카탈로그 항목이 서비스 카탈로그에 나타나고 권한 있는 사용자는 이것을 사용하여 리소스를 프로비저닝할 수 있습니다. 항목은 카탈로그 항목 목록에 [게시됨]으로 나타납니다. ■ 비활성. 카탈로그 항목을 서비스 카탈로그에서 사용할 수 없습니다. 항목은 카탈로그 항목 목록에 [회수됨]으로 나타납니다. ■ 스테이징. 카탈로그 항목을 서비스 카탈로그에서 사용할 수 없습니다. 항목이 비활성화된 상태에서 스테이징을 사용하여 항목의 재활성화를 고려 중임을 나타내려는 경우 이 메뉴 항목을 선택합니다. 항목은 카탈로그 항목 목록에 [스테이징]으로 나타납니다.
서비스	서비스를 선택합니다. 권한 있는 사용자가 볼 수 있도록 서비스 카탈로그에서 표시하려면 모든 카탈로그 항목을 서비스에 연결해야 합니다. 목록에는 활성 서비스와 비활성 서비스가 포함됩니다.
새 항목 및 주목할 만한 항목	카탈로그 항목이 홈 페이지의 [새 항목 및 주목할 만한 항목] 영역에 나타납니다.

4 사용자에게 카탈로그 항목을 제공할 수 있는 사용 권한을 보려면 **사용 권한** 탭을 클릭합니다.

5 업데이트를 클릭합니다.

후속 작업

- 서비스 카탈로그에서 카탈로그 항목을 사용할 수 있게 하려면 항목에 연결된 서비스 또는 개별 항목에 대한 사용 권한을 사용자에게 부여해야 합니다. **사용 권한 생성** 항목을 참조하십시오.
- 개별 사용자에게 대한 승인 정책이 올바르게 적용되도록 사용 권한 처리 순서를 지정하려면 동일한 비즈니스 그룹의 여러 사용 권한에 대해 우선 순위를 설정합니다. **사용 권한의 우선 순위 지정** 항목을 참조하십시오.

서비스 카탈로그에 대한 작업 구성

작업은 프로비저닝된 항목에서 실행될 수 있는 변경 사항 또는 워크플로입니다. 아이콘을 추가하거나 선택된 작업이 포함된 사용 권한을 볼 수 있습니다.

작업은 프로비저닝된 시스템, 네트워크 및 기타 Blueprint 구성 요소에 대한 기본 작업이거나 게시된 XaaS 작업입니다.

아이콘의 경우, GIF, JPG 및 PNG 이미지 파일 형식이 지원됩니다. 표시되는 이미지는 40 x 40픽셀입니다. 사용자 지정 이미지를 선택하지 않는 경우 **항목** 탭에 기본 작업 아이콘이 나타납니다.

필수 조건

- **테넌트 관리자** 또는 **카탈로그 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 게시된 하나 이상의 작업이 있는지 확인합니다. **Blueprint 게시** 및 **리소스 작업 게시** 항목을 참조하십시오.

프로시저

- 1 **관리 > 카탈로그 관리 > 작업**을 선택합니다.
- 2 공유 작업을 선택하고 **세부 정보 보기**를 클릭합니다.
- 3 이미지를 찾습니다.
- 4 작업이 사용자에게 제공되는 사용 권한을 보려면 **사용 권한** 탭을 클릭합니다.
- 5 **업데이트**를 클릭합니다.

후속 작업

사용자에게 서비스, 카탈로그 항목 및 작업에 대한 사용 권한 부여.

사용 권한 생성

사용 권한은 선택된 비즈니스 그룹 구성원에 대해 서비스 카탈로그에서 사용 가능한 항목 및 작업을 제어합니다. 항목이 서비스 카탈로그에 표시되려면 해당 항목에 대한 사용 권한이 활성화 상태여야 합니다. 규정 준수가 필요한 항목이 있는 경우 사용 권한을 사용하여 각기 다른 항목에 승인 정책을 적용할 수 있습니다.

사용 권한을 구성하려면 서비스에 카탈로그 항목을 포함해야 합니다. 사용 권한에는 여러 개의 서비스, 다른 사용 권한에 포함된 서비스의 카탈로그 항목, 그리고 배포된 카탈로그 항목에서 실행할 수 있는 작업이 포함될 수 있습니다.

사용 권한 옵션 상호 작용 이해

사용 권한을 구성하는 방식에 따라 서비스 카탈로그에 표시되는 항목이 결정됩니다. 서비스, 카탈로그 항목 및 구성 요소, 작업, 승인 정책의 상호 작용은 사용자가 요청할 수 있는 서비스 카탈로그가 무엇이고 승인 정책이 어떻게 적용되는지에 영향을 미칩니다.

사용 권한을 생성할 때 서비스, 카탈로그 항목, 작업 및 승인의 상호 작용을 고려해야 합니다.

■ 사용 권한의 서비스

권한 있는 서비스는 카탈로그 항목의 동적 그룹으로 작동합니다. 카탈로그 항목이 권한이 부여된 후 서비스에 추가되는 경우 추가 구성 없이 지정된 사용자가 새 카탈로그 항목을 사용할 수 있습니다.

■ 사용 권한의 카탈로그 항목 및 구성 요소

권한 있는 카탈로그 항목은 서비스 카탈로그에서 요청할 수 있는 Blueprint입니다. 권한 있는 구성 요소는 Blueprint의 일부이지만, 서비스 카탈로그에서 구체적으로 요청할 수 없습니다.

■ 사용 권한의 작업

작업은 배포된 카탈로그 항목에서 실행됩니다. 프로비저닝된 카탈로그 항목과, 해당 항목에서 실행할 수 있는 권한이 부여된 작업이 [항목] 탭에 표시됩니다. 배포된 항목에서 작업을 실행하려면 작업이 서비스 카탈로그에서 항목을 프로비저닝한 카탈로그 항목과 동일한 사용 권한에 포함되어야 합니다.

■ 사용 권한의 승인 정책

환경에서 리소스를 관리할 수 있도록 사용 권한에서 승인 정책이 적용됩니다.

사용 권한의 서비스

권한 있는 서비스는 카탈로그 항목의 동적 그룹으로 작동합니다. 카탈로그 항목이 권한이 부여된 후 서비스에 추가되는 경우 추가 구성 없이 지정된 사용자가 새 카탈로그 항목을 사용할 수 있습니다.

서비스에 승인 정책을 적용하는 경우 요청 시 모든 항목이 동일한 승인 정책의 영향을 받습니다.

사용 권한의 카탈로그 항목 및 구성 요소

권한 있는 카탈로그 항목은 서비스 카탈로그에서 요청할 수 있는 Blueprint입니다. 권한 있는 구성 요소는 Blueprint의 일부이지만, 서비스 카탈로그에서 구체적으로 요청할 수 없습니다.

권한 있는 카탈로그 항목 및 구성 요소에는 다음 항목이 포함될 수 있습니다.

카탈로그 항목

- 권한 있는 사용자에게 제공하려는 서비스의 항목(서비스가 현재 사용 권한에 포함되지 않은 경우에도).

예를 들어 카탈로그 관리자로서 여러 각기 다른 버전의 Red Hat Enterprise Linux를 Red Hat 서비스와 연결했으며 해당 서비스에 대한 사용 권한을 제품 A에 대한 품질 엔지니어에게 부여했습니다. 그런 다음 교육 팀을 위해 최신 버전의 Linux 기반 운영 체제만 포함하는 서비스 카탈로그 항목을 생성해 달라는 요청을 받습니다. 서비스에서 최신 버전의 기타 운영 체제를 포함하는 교육 팀에 대한 사용 권한을 생성합니다. 이미 다른 서비스와 연결된 최신 버전의 RHEL이 있으므로 전체 Red Hat 서비스를 추가하는 대신 RHEL을 카탈로그 항목으로 추가합니다.

- 현재 사용 권한에 포함된 서비스에 포함되어 있지만 서비스에 적용한 정책과 다른 승인 정책을 개별 카탈로그 항목에 적용하고자 하는 항목.

예를 들어 비즈니스 그룹 관리자로서 개발 팀에게 3개의 가상 시스템 카탈로그 항목을 포함하는 서비스에 대한 사용 권한을 부여합니다. 5개 이상의 CPU가 있는 시스템에 대해 가상 인프라 관리자의 승인을 필요로 하는 승인 정책을 적용합니다. 가상 시스템 중 하나는 성능 테스트에 사용되므로 이를 카탈로그 항목으로 추가하고 동일한 사용자 그룹에 대해 덜 제한적인 승인 정책을 적용합니다.

구성 요소

- 구성 요소는 카탈로그 항목의 일부이기 때문에 서비스 카탈로그에서 이름으로 사용할 수 없습니다. 구성 요소가 포함된 카탈로그 항목과 다른 특정 승인 정책을 적용할 수 있도록 구성 요소에 대한 사용 권한을 개별적으로 부여합니다.

예를 들어 항목에는 시스템과 소프트웨어가 포함됩니다. 시스템은 프로비저닝 가능 항목으로 사용할 수 있으며 사이트 관리자 승인이 필요한 승인 정책이 있습니다. 소프트웨어는 독립형 프로비저닝 가능 항목으로 사용할 수 없으며 시스템 요청의 일부로만 소프트웨어에 대한 승인 정책은 조직의 소프트웨어 라이선싱 관리자의 승인을 필요로 합니다. 시스템은 서비스 카탈로그에서 요청되는 경우 프로비저닝되기 전에 사이트 관리자와 소프트웨어 라이선싱 관리자의 승인을 받아야 합니다. 프로비저닝된 후 소프트웨어 항목이 있는 시스템이 시스템의 일부로 요청자의 [항목] 탭에 표시됩니다.

사용 권한의 작업

작업은 배포된 카탈로그 항목에서 실행됩니다. 프로비저닝된 카탈로그 항목과, 해당 항목에서 실행할 수 있는 권한이 부여된 작업이 [항목] 탭에 표시됩니다. 배포된 항목에서 작업을 실행하려면 작업이 서비스 카탈로그에서 항목을 프로비저닝한 카탈로그 항목과 동일한 사용 권한에 포함되어야 합니다.

예를 들어 사용 권한 1에는 vSphere 가상 시스템 및 스냅샷 생성 작업이 포함되지만 사용 권한 2에는 vSphere 가상 시스템만 포함됩니다. 사용 권한 1에서 vSphere 시스템을 배포하는 경우 스냅샷 생성 작업을 사용할 수 있습니다. 사용 권한 2에서 vSphere 시스템을 배포하는 경우 작업이 없습니다. 사용 권한 2 사용자가 작업을 사용할 수 있게 하려면 사용 권한 2에 스냅샷 생성 작업을 추가합니다.

사용 권한의 카탈로그 항목에 적용되지 않는 작업을 선택하는 경우 항목 탭에 작업으로 표시되지 않습니다. 예를 들어 사용 권한에 vSphere 시스템이 포함되며 클라우드 시스템에 대해 제거 작업에 대한 사용 권한을 부여합니다. 제거 작업은 프로비저닝된 시스템에서 실행할 수 없습니다.

사용 권한에서 카탈로그 항목에 적용된 정책과 다른 승인 정책을 작업에 적용할 수 있습니다.

서비스 카탈로그 사용자가 여러 비즈니스 그룹의 구성원이며 한 그룹에만 전원을 켜고 끌 수 있는 사용 권한이 부여되었고 다른 그룹에는 제거 권한만 있다면 이 사용자는 프로비저닝된 해당 시스템에 대해 세 가지 작업을 모두 수행할 수 있습니다.

사용자에게 작업에 대한 사용 권한을 부여할 때의 모범 사례

Blueprint는 복잡하며 프로비저닝된 Blueprint에서 실행되는 사용 권한 부여 작업에는 예기치 않은 동작이 발생할 수 있습니다. 프로비저닝된 항목에 대한 작업 실행을 위해 서비스 카탈로그 사용자에게 사용 권한을 부여하려는 경우에는 다음 모범 사례를 사용합니다.

- 사용자에게 시스템 제거 작업에 대한 사용 권한을 부여하려는 경우 배포 제거 작업에 대한 사용 권한을 부여합니다. 프로비저닝된 Blueprint는 배포입니다.

배포에는 시스템이 포함될 수 있습니다. 서비스 카탈로그 사용자가 시스템 제거 작업을 실행할 권한은 있지만 배포 제거 작업을 실행할 권한은 없는 경우 이 사용자가 배포의 마지막 또는 유일한 시스템에 대해 시스템 제거 작업을 실행하면 사용자에게 작업을 실행할 사용 권한이 없음을 나타내는 메시지가 표시됩니다. 두 작업에 대한 사용 권한을 모두 부여하면 환경에서 배포가 제거됩니다. 배포 제거 작업에서 거버넌스를 관리하기 위해 사전 승인 정책을 생성하고 이 정책을 작업에 적용할 수 있습니다. 이 정책을 사용하면 지정된 승인자가 배포 제거 요청을 실행하기 전에 이를 검증할 수 있습니다.
- 서비스 카탈로그 사용자에게 시스템 및 배포에 적용될 수 있는 리스 변경, 소유자 변경, 만료, 재구성 및 기타 작업에 대한 사용 권한을 부여할 때에는 두 작업 모두에 대한 사용 권한을 부여합니다.

사용 권한의 승인 정책

환경에서 리소스를 관리할 수 있도록 사용 권한에서 승인 정책이 적용됩니다.

사용 권한을 생성할 때 승인 정책을 적용하려면 정책이 이미 존재해야 합니다. 그렇지 않은 경우 이 사용 권한의 카탈로그 항목과 작업에 필요한 승인 정책을 생성하고 나중에 정책을 적용할 때까지 사용 권한을 생성하고 초안 상태 또는 비활성 상태에 둘 수 있습니다.

항목 또는 작업에 승인 정책을 적용하지 않아도 됩니다. 승인 정책이 적용되지 않은 경우 요청된 항목 및 작업이 승인 요청을 트리거하지 않은 채 배포됩니다.

사용자에게 서비스, 카탈로그 항목 및 작업에 대한 사용 권한 부여

서비스, 카탈로그 항목 또는 작업을 사용 권한에 추가하는 경우 사용 권한에서 식별된 사용자가 서비스 카탈로그의 프로비저닝 가능 항목을 요청할 수 있습니다. 작업은 항목과 연결되며 요청하는 사용자에게 대한 **항목** 탭에 표시됩니다.

비즈니스 그룹에 대한 사용 권한을 생성할 수 있는 사용 권한이 있는 여러 사용자 역할이 있습니다.

- 테넌트 관리자는 자신이 관리하는 테넌트에 속해 있는 모든 비즈니스 그룹에 대해 사용 권한을 생성할 수 있습니다.
- 비즈니스 그룹 관리자는 자신이 관리하는 그룹에 대해 사용 권한을 생성할 수 있습니다.
- 카탈로그 관리자는 자신이 관리하는 테넌트에 속해 있는 모든 비즈니스 그룹에 대해 사용 권한을 생성할 수 있습니다.

사용 권한을 생성할 때는 사용 권한에 대해 비즈니스 그룹 및 비즈니스 그룹의 구성원을 선택해야 합니다.

승인을 통해 서비스, 카탈로그 항목 및 작업의 상호 작용을 사용할 수 있도록 사용 권한을 생성하는 방법을 이해하려면 [사용 권한 생성](#) 항목을 참조하십시오.

필수 조건

- **테넌트 관리자** 또는 **카탈로그 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- 사용자에게 사용 권한을 부여하는 카탈로그 항목이 서비스와 연결되어 있는지 확인합니다. [서비스에 카탈로그 항목 추가](#) 항목을 참조하십시오.
- 사용 권한을 정의하는 비즈니스 그룹이 존재하며 구성원 사용자 및 사용자 그룹이 정의되어 있는지 확인합니다. [비즈니스 그룹 생성](#) 항목을 참조하십시오.
- 승인을 추가하려고 하는 경우 이 사용 권한을 생성할 때 승인 정책이 존재하는지 확인합니다. [승인 정책 생성](#) 항목을 참조하십시오. 사용자에게 승인 없이 서비스 카탈로그의 항목에 대한 사용 권한을 부여하는 경우 나중에 승인을 추가하도록 사용 권한을 수정할 수 있습니다.

프로시저

- 1 **관리 > 카탈로그 관리 > 사용 권한**을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 **세부 정보** 옵션을 구성합니다.

세부 정보는 사용 권한이 사용 권한 목록에 표시되는 방법과 서비스 카탈로그의 항목에 대한 액세스 권한이 있는 사용자를 결정합니다.

옵션	설명
이름 및 설명	사용 권한 목록에 표시되는 사용 권한에 대한 정보입니다.
만료 날짜	사용 권한이 특정 날짜에 비활성화되기를 원하는 경우 날짜 및 시간을 설정합니다.

옵션	설명
상태	<p>가능한 값에는 활성, 비활성 및 삭제됨이 포함됩니다.</p> <ul style="list-style-type: none"> ■ 활성: 항목이 서비스 카탈로그에서 사용 가능합니다. 이 옵션은 사용 권한을 추가하거나 편집할 때 사용 가능합니다. ■ 비활성: 항목을 서비스 카탈로그에서 사용할 수 없습니다. 사용 권한이 만료 날짜 또는 사용자에 의해 비활성화되었습니다. ■ 삭제됨: 사용 권한이 삭제되었습니다.
비즈니스 그룹	<p>비즈니스 그룹을 선택합니다. 하나의 비즈니스 그룹에 대해서만 사용 권한을 생성할 수 있으며 권한 있는 사용자는 비즈니스 그룹의 구성원이어야 합니다.</p> <p>사용 권한을 모든 사용자가 사용할 수 있도록 하려면 모든 사용자 비즈니스 그룹이 있거나 각 비즈니스 그룹에 대해 사용 권한을 생성해야 합니다.</p> <p>비즈니스 그룹 관리자로 로그인한 경우 비즈니스 그룹에 대해서만 사용 권한을 생성할 수 있습니다.</p>
사용자 및 그룹	<p>모든 사용자 및 그룹을 선택하여 비즈니스 그룹의 모든 구성원에게 카탈로그 항목 및 작업에 대한 권한을 부여하거나 개별 사용자 또는 그룹에게 사용 권한을 부여할 수 있습니다. 사용 권한을 활성화하려면 비즈니스 그룹 사용자 또는 그룹을 하나 이상 선택해야 합니다.</p>

4 다음을 클릭합니다.

5 새로 만들기 아이콘(+)을 클릭하여 이 사용 권한으로 사용자에게 서비스, 카탈로그 항목 또는 작업에 대한 사용 권한을 부여합니다.

서비스, 항목 및 작업의 다양한 조합으로 사용 권한을 생성할 수 있습니다.

옵션	설명
권한 있는 서비스	<p>권한 있는 사용자가 서비스와 연결된 모든 게시된 카탈로그 항목에 액세스할 수 있도록 허용하려는 경우 서비스를 추가합니다.</p> <p>권한 있는 서비스는 동적 사용 권한입니다. 나중에 항목이 서비스에 추가되는 경우 권한 있는 사용자에게 대한 서비스 카탈로그에 이 항목이 추가됩니다. 사용 권한에는 서비스와 개별 카탈로그 항목을 모두 포함할 수 있습니다.</p>
권한 있는 카탈로그 항목 및 구성 요소	<p>권한 있는 사용자가 사용할 수 있는 개별 항목을 추가합니다.</p> <p>사용 권한에는 서비스와 개별 카탈로그 항목을 모두 포함할 수 있습니다. 서비스에 포함된 항목에 다른 승인 정책을 적용하려면 이 정책을 카탈로그 항목으로 추가합니다. 동일한 사용 권한에 있는 경우 항목의 승인 정책이 항목이 속한 서비스의 승인 정책에 우선합니다. 다른 사용 권한에 있는 경우 순서는 설정된 우선 순위를 기반으로 합니다.</p> <p>카탈로그 항목은 서비스 카탈로그에서 사용 가능한 서비스와 연결해야 합니다. 카탈로그 항목은 현재 사용 권한의 서비스 외에도 다른 모든 서비스와 연결될 수 있습니다.</p> <p>구성 요소는 카탈로그 항목의 일부이지만 서비스 카탈로그에서 이름으로 사용할 수 없습니다. 예를 들어 MySQL 소프트웨어는 CentOS 가상 시스템 카탈로그 항목의 구성 요소입니다. 구성 요소에는 카탈로그 항목에 대한 사용 권한이 부여됩니다. 소프트웨어별 승인 정책을 적용하려는 경우, 사용자가 항목에 대한 사용 권한을 개별적으로 부여합니다. 그렇지 않으면, 상위 항목과 함께 배포되도록 구성 요소에 대한 사용 권한을 부여할 필요가 없습니다.</p>

옵션	설명
권한 있는 작업	<p>사용자가 프로비저닝된 항목에 대한 작업을 실행하도록 허용하려면 작업을 추가합니다.</p> <p>이 사용 권한에서 프로비저닝된 항목에서 실행할 작업은 동일한 사용 권한에 포함되어야 합니다.</p> <p>권한 있는 작업은 서비스 카탈로그에 나타나지 않습니다. 이 작업은 프로비저닝된 항목의 항목 탭에 나타납니다.</p>
이 사용 권한에 정의된 항목에만 작업 적용	<p>권한 있는 작업이 모든 적용 가능한 서비스 카탈로그 항목에 부여되는지 아니면 이 사용 권한에 포함된 항목에 대해서만 부여되는지 결정합니다.</p> <p>선택된 경우, 해당 작업은 이 사용 권한의 적용 가능한 항목에 대해 비즈니스 그룹 구성원에게 사용 권한이 부여됩니다. 이러한 작업 사용 권한 부여 방법은 특정 항목에 대해 작업을 지정할 수 있도록 해줍니다.</p> <p>이 옵션이 선택되지 않은 경우 이 사용 권한에 항목이 포함되어 있는지 여부와 상관없이 사용 권한에 지정된 사용자에게 모든 적용 가능한 카탈로그 항목에 대한 작업 사용 권한이 부여됩니다. 또한 이러한 작업에 대한 모든 적용된 승인 정책은 활성화됩니다.</p>

6 각 섹션의 드롭다운 메뉴를 사용하여 사용 가능한 항목을 필터링합니다.

7 항목을 사용 권한에 포함하려면 확인란을 선택합니다.

8 선택된 서비스, 항목 또는 작업에 승인 정책을 추가하려면 **선택한 항목에 적용할 정책** 드롭다운 메뉴에서 승인 정책을 선택합니다.

서비스에 승인 정책을 적용하는 경우 해당 서비스의 모든 항목이 동일한 승인 정책을 갖습니다. 항목에 다른 정책을 적용하려면 카탈로그 항목으로 추가한 다음 적합한 정책을 적용합니다.

9 **확인**을 클릭합니다.

서비스, 항목 또는 작업이 사용 권한에 추가됩니다.

10 **완료**를 클릭하여 사용 권한을 저장합니다.

사용 권한 상태가 활성화인 경우 서비스 및 항목이 서비스 카탈로그에 추가됩니다.

후속 작업

권한 있는 서비스 및 카탈로그 항목이 권한 있는 사용자에게 대한 서비스 카탈로그에 표시되며 요청된 항목이 예상대로 대상 개체를 프로비저닝하는지 확인합니다. 선택된 사용자 대신 항목을 요청할 수 있습니다.

사용 권한의 우선 순위 지정

같은 비즈니스 그룹에 대해 사용 권한이 여러 개 있는 경우에는 서비스 카탈로그 사용자가 요청을 했을 때 지정한 순서대로 사용 권한 및 관련 승인 정책이 처리되도록 사용 권한의 우선 순위를 지정할 수 있습니다.

사용자 그룹의 승인 정책을 구성하는 경우, 그룹 구성원이 서비스, 카탈로그 항목 또는 작업 중 하나 이상에 대해 고유한 정책을 갖도록 하려면 그룹 사용 권한보다 구성된 사용 권한의 우선 순위를 높게 지정해야 합니다. 구성원이 서비스 카탈로그의 항목을 요청하면 비즈니스 그룹에 대한 사용 권한 우선 순위 순서에 기반하여 승인 정책이 적용됩니다. 사용자 지정 사용자 그룹의 일부로든 개별 사용자로든 이 구성원의 이름이 처음으로 발견되면 해당 승인 정책이 적용됩니다.

예를 들어 같은 카탈로그 항목에 대해 두 개의 사용 권한을 생성하여 회계 사용자 그룹을 위한 승인 정책 하나와 이 그룹의 구성원인 Chris를 위한 또 다른 승인 정책을 적용할 수 있습니다.

표 3-66. 사용 권한 예제

사용 권한 1	사용 권한 2
비즈니스 그룹: 재무	비즈니스 그룹: 재무
사용자 및 그룹: 회계 그룹	사용자 및 그룹: Chris
카탈로그 항목 1: 정책 A	카탈로그 항목 1: 정책 C

Chris가 서비스 카탈로그에 있는 카탈로그 항목 1을 요청합니다. 재무 비즈니스 그룹에 대한 사용 권한의 우선 순위 순서에 따라 Chris의 요청에 대해 다른 정책이 적용됩니다.


표 3-67. 예제 결과

구성 및 결과	우선 순위 순서	우선 순위 순서
우선 순위 순서	1: 사용 권한 1 2: 사용 권한 2	1: 사용 권한 2 2: 사용 권한 1
적용되는 정책	정책 A가 적용됩니다. Chris는 회계 사용자 그룹의 구성원입니다. Chris를 사용 권한이 있는 사용자로 검색하는 작업이 사용 권한 1에서 중지되고, 해당 승인 정책이 적용됩니다.	정책 C가 적용됩니다. Chris를 사용 권한이 있는 사용자로 검색하는 작업이 사용 권한 2에서 중지되고, 해당 승인 정책이 적용됩니다.

필수 조건

테넌트 관리자 또는 카탈로그 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 카탈로그 관리 > 사용 권한**을 선택합니다.
- 2 **우선 순위 지정** 아이콘()을 클릭합니다.
- 3 **비즈니스 그룹** 드롭다운 목록에서 비즈니스 그룹을 선택합니다.
- 4 사용 권한의 우선 순위를 변경하려면 해당 사용 권한을 목록 내의 새 위치로 끌어옵니다.
- 5 업데이트 방법을 선택합니다.

옵션	설명
업데이트	변경 내용을 저장합니다.
업데이트 및 닫기	변경 내용을 저장하고 요소 우선 순위 지정 창을 닫습니다.

승인 정책 사용

승인 정책은 환경에서 리소스를 관리할 수 있도록 서비스 카탈로그 요청에 추가하는 거버넌스입니다. 각 정책은 사용자에게 서비스, 카탈로그 항목 및 작업에 대한 사용 권한을 부여할 때 해당 항목에 적용할 수 있는 정의된 조건 집합입니다.

승인 정책 프로세스

우선, 테넌트 관리자 또는 승인 관리자가 프로비저닝 거버넌스가 필요한 승인 정책을 생성합니다.

승인 정책은 승인 정책 유형 또는 특정 항목에 대해 생성됩니다. 정책이 정책 유형을 기반으로 하는 경우 일치하는 카탈로그 항목 유형에 정책을 적용할 수 있습니다. 예를 들어 정책이 소프트웨어 정책 유형을 기반으로 한다면 사용 권한의 모든 소프트웨어 항목에 대해 정책을 정의하고 적용할 수 있습니다. 정책이 특정 항목을 위한 것이라면 해당 항목에 대해서만 정책을 적용해야 합니다. 예를 들어 항목이 특정 소프트웨어 항목인 경우 사용 권한의 해당하는 특정 데이터베이스 소프트웨어에 대해서만 정책을 적용해야 합니다.

정책에는 사전 승인 요구 사항과 사후 승인 요구 사항이 포함될 수 있습니다. 사전 승인의 경우 요청된 항목이 프로비저닝되기 전에 요청이 승인되어야 합니다. 사후 승인 정책의 경우에는 프로비저닝된 항목이 요청하는 사용자에게 제공되기 전에 승인자가 요청을 수락해야 합니다.

사전 및 사후 승인 구성은 승인 정책이 트리거되는 시간과 요청 승인 주체 또는 방법을 결정하는 하나 이상의 수준으로 이루어져 있습니다. 여러 개의 수준을 포함할 수 있습니다. 예를 들어 승인 정책에는 관리자 승인 수준 하나와 그 다음에 나오는 재무 승인 수준이 포함될 수 있습니다.

그 다음, 테넌트 관리자 또는 비즈니스 그룹 관리자가 승인 정책을 서비스, 카탈로그 항목 및 작업에 적절하게 적용합니다.

마지막으로, 서비스 카탈로그 사용자가 승인 정책이 적용되는 항목을 요청하면 승인자가 **승인** 페이지의 **받은 편지함** 탭에서 요청을 승인하거나 거부합니다. 요청하는 사용자는 특정 요청에 대한 승인 상태를 해당 **요청** 탭에서 추적할 수 있습니다.

가상 시스템 정책 유형에 기반한 승인 정책의 예

동일한 카탈로그 항목 유형에 적용할 수 있는 승인 정책을 생성할 수 있지만 항목이 서비스 카탈로그에서 요청될 때 해당 정책이 각기 다른 결과를 생성할 수 있습니다. 승인 정책이 정의 및 적용되는 방법에 따라 서비스 카탈로그 사용자 및 승인자에 대한 영향이 다릅니다.

다음 표에는 모두 동일한 승인 정책 유형을 기반으로 하는 각기 다른 승인 정책의 예가 포함되어 있습니다. 이러한 예는 각기 다른 유형의 거버넌스를 수행하도록 승인 정책을 구성할 수 있는 몇 가지 방식을 보여 줍니다.

표 3-68. 승인 정책 및 결과의 예

거버넌스 목표	선택된 정책 유형	사전 또는 사후 승인	승인이 필요한 시기	승인자	정책이 사용 권한에 적용되는 방법	항목이 서비스 카탈로그에서 요청될 때의 결과
비즈니스 그룹 관리자는 모든 가상 시스템 요청을 승인해야 합니다. 승인 정책은 여러 사용 권한의 여러 비즈니스 그룹에 적용할 수 있어야 합니다.	서비스 카탈로그 - 카탈로그 항목 요청 - 가상 시스템	사전 승인 탭에 추가	항상 필요 선택	요청에서 승인자 결정을 선택합니다. 조건 비즈니스 그룹 > 관리자 > 사용자 > 관리자 를 선택합니다. 누구나 승인 가능 을 선택합니다.	사용 권한은 비즈니스 그룹을 기반으로 합니다. 이 승인은 가상 시스템에 대해 관리자 승인이 필요한 모든 사용 권한에서 사용할 수 있습니다.	서비스 카탈로그 그 사용자가 이 승인이 적용된 가상 시스템을 요청하는 경우 비즈니스 그룹 관리자가 시스템이 프로비저닝되기 전에 요청을 승인해야 합니다.
가상 인프라 관리자는 가상 시스템의 올바른 프로비저닝을 확인하고 가상 시스템이 요청한 사용자에게 릴리스되기 전에 요청을 승인해야 합니다.	서비스 카탈로그 - 카탈로그 항목 요청 - 가상 시스템	사후 승인 탭에 추가	항상 필요 선택	특정 사용자 및 그룹 을 선택합니다. 가상 인프라 관리자 사용자 지정 사용자 그룹을 선택합니다. 누구나 승인 가능 을 선택합니다.	이 승인은 가상 인프라 관리자가 가상 시스템이 프로비저닝된 후 vCenter Server의 가상 시스템을 확인하길 원하는 모든 사용 권한에서 사용할 수 있습니다.	서비스 카탈로그 그 사용자가 이 승인이 적용된 가상 시스템을 요청하는 경우 가상 시스템이 프로비저닝됩니다. VI 관리 그룹의 각 구성원이 요청을 승인하는 경우 시스템이 사용자에게 릴리스됩니다.
가상 인프라 리소스를 관리하고 가격을 제어하려면 시스템 리소스와 일별 시스템 가격에 대한 2개의 사전 승인 수준을 추가합니다.	서비스 카탈로그 - 카탈로그 항목 요청 - 가상 시스템	사전 승인 탭에 추가	수준 1 조건에 따라 필요 를 선택합니다. CPU > 6 또는 메모리 > 8 또는 스토리지 > 100GB인 조건을 구성합니다.	요청에서 승인자 결정을 선택합니다. 요청자 > 관리자 조건을 선택합니다. 시스템 속성을 클릭하고 CPU, 메모리 및 스토리지 를 선택하여 승인자가 값을 허용 가능한 수준으로 변경할 수 있도록 합니다.	이 승인 정책은 요청한 사용자의 관리자 와 재무 부서의 구성원이 요청을 승인하길 원하는 사용 권한에서 사용할 수 있습니다.	서비스 카탈로그 그 사용자가 가상 시스템을 요청하는 경우 요청된 CPU, 메모리 또는 스토리지 양이 수준 1에서 지정된 양을 초과하는지 여부를 결정하기 위해 요청이 평가됩니다. 그렇지 않은 경우 수준 2 조건이 평가됩니다. 요청이 수준 1 조건 중 하나 이상을 초과하는 경우 관리자가 요청을 승인해야 합니다. 관리자는 요청

표 3-68. 승인 정책 및 결과의 예 (계속)

거버넌스 목표	선택된 정책 유형	사전 또는 사후 승인	승인이 필요한 시기	승인자	정책이 사용 권한에 적용되는 방법	항목이 서비스 카탈로그에서 요청될 때의 결과
			수준 2 조건에 따라 필요를 선택합니다. 가격 > 일별 15.00 조건을 구성합니다.	특정 사용자 및 그룹을 선택합니다. 재무 사용자 지정 사용자 그룹을 선택합니다. 누구나 승인 기능을 선택합니다.		된 구성 양을 줄이고 승인하거나 요청을 거부할 수 있습니다.
매개 변수화된 Blueprint 카탈로그 항목의 경우 클라우드 관리자가 vSphere 시스템 구성 요소 프로파일의 size가 large로 설정된 배포 요청을 승인해야 합니다.	서비스 카탈로그 - 항목 요청 - 가상 시스템	사전 승인 탭에 추가	수준 1 조건에 따라 필요를 선택합니다. 수준 2 단일 조건을 선택합니다. 구성 요소 프로파일 > vSphere 시스템 크기를 선택합니다. size = large 조건을 구성합니다.	특정 사용자 및 그룹을 선택합니다. 요청을 승인할 수 있는 사용자 및 그룹을 선택합니다. 누구나 승인 기능을 선택합니다.	이 승인 정책은 클라우드 관리자가 프로비저닝 요청을 승인하게 하려는 사용 권한에서 사용할 수 있습니다.	서비스 카탈로그 사용자가 이 승인이 적용된 가상 시스템을 요청하는 경우 클라우드 관리자가 시스템이 프로비저닝되기 전에 요청을 승인해야 합니다.

복합 배포에서 승인 정책이 적용되는 작업의 예

복합 Blueprint의 다양한 구성 요소에서 실행될 수 있는 작업에 승인 정책을 적용하는 경우 사용 권한이 구성되는 방식과 승인 정책이 적용되는 방식에 따라 승인 프로세스가 다릅니다.

이 예에서는 특정 세부 정보를 사용하여 Blueprint를 빌드한 다음 다른 사용 권한의 프로비저닝된 Blueprint의 서비스 카탈로그에서 실행할 수 있는 작업에 승인 정책을 적용합니다. Blueprint는 다른 Blueprint가 포함된 복합 Blueprint입니다. 작업은 프로비저닝된 항목을 제거하고 Blueprint에 대한 배포를 제거하고 시스템에 대한 가상 시스템을 제거하기 위해 사용되었습니다. 결과 동작에는 제거된 항목과 적용된 승인 정책이 승인 요청을 트리거한 시점이 포함되어 있습니다.

Blueprint 예

이 예에서는 가상 시스템과 함께 중첩된 Blueprint가 포함된 Blueprint를 구성합니다.

- Blueprint 1 - 연속 통합 Blueprint
 - Blueprint 2 - 운영 전단계 Blueprint
 - 가상 시스템 1 - TestAsAService vSphere VM

제거 작업에 대한 승인 정책

프로비저닝된 항목을 제거하기 위한 2개의 승인 정책을 구성합니다. 제거 - 배포 작업은 이 예의 Blueprint 1 또는 Blueprint 2에서 실행될 수 있습니다. 제거 - 가상 시스템 작업은 가상 시스템 1에서 실행될 수 있습니다. 사용 권한의 작업에 적용할 수 있도록 승인 정책을 생성합니다.

승인 정책 이름	승인 정책 유형
승인 정책 A	서비스 카탈로그 - 리소스 작업 요청 - 제거 - 배포
승인 정책 B	서비스 카탈로그 - 리소스 작업 요청 - 제거 - 가상 시스템

사용 권한 및 작업에 적용되는 승인 정책

3개의 사용 권한을 구성합니다. 각 사용 권한에는 복합 Blueprint가 포함됩니다. 각 사용 권한에서 제거 작업을 추가하고 승인 정책을 적용합니다.

사용 권한 이름	프로비저닝된 시스템에 대한 권한 있는 작업	적용된 승인 정책
사용 권한 1	제거 - 배포	승인 정책 A
사용 권한 2	제거 - 가상 시스템	승인 정책 B
사용 권한 3	제거 - 배포 제거 - 가상 시스템	승인 정책 A 승인 정책 B

서비스 카탈로그의 사용자 작업

서비스 카탈로그 사용자가 작업을 실행하는 경우 사용자가 작업을 실행한 항목에 따라 Blueprint 또는 시스템이 제거됩니다.

서비스 카탈로그의 사용자 작업	선택된 작업	제거된 Blueprint 또는 시스템
작업 1	제거 - 배포 작업이 Blueprint 1 - 연속 통합 Blueprint에서 실행됨	Blueprint 1, Blueprint 2 및 가상 시스템 1
작업 2	제거 - 배포 작업이 중첩된 Blueprint 2 - 운영 전단계 Blueprint에서 실행됨	Blueprint 2 및 가상 시스템 1
작업 3	제거 - 가상 시스템 작업이 배포, 가상 시스템 1 - TestAsAService vSphere VM 내부의 시스템에서 실행됨	가상 시스템 1

사용 권한의 작업에 적용되는 승인 정책

승인 정책을 적용하고 승인자가 서비스 카탈로그 사용자가 작업을 실행한 Blueprint 또는 시스템에 따라 승인 요청을 수신합니다.

사용 권한 이름	작업에 대한 승인 정책	사용자 작업	트리거된 승인 요청	승인된 경우, 제거된 Blueprint 또는 시스템
사용 권한 1 - 배포 제거 승인 정책	제거 - 배포 작업에만 해당하는 정책 A(배포 제거 승인 정책)	작업 1(Blueprint 1에 대해 제거 - 배포 작업 실행)	승인 요청이 Blueprint 1에 대해서만 트리거됨	Blueprint 1, Blueprint 2 및 가상 시스템 1
		작업 2(Blueprint 2에 대해 제거 - 배포 작업 실행)	승인 요청이 Blueprint 2에 대해서만 트리거됨	Blueprint 2 및 가상 시스템 1
		작업 3 (제거 - 가상 시스템 작업은 가상 시스템 1에서 실행됨)	승인 요청이 트리거되지 않음	가상 시스템 1
사용 권한 2	제거 - 가상 시스템 작업에만 해당하는 정책 B(제거 - 가상 시스템 정책)	작업 1(Blueprint 1에 대해 제거 - 배포 작업 실행)	승인 요청이 트리거되지 않음	Blueprint 1, Blueprint 2 및 가상 시스템 1
		작업 2(Blueprint 2에 대해 제거 - 배포 작업 실행)	승인 요청이 트리거되지 않음	Blueprint 2 및 가상 시스템 1
		작업 3 (제거 - 가상 시스템 작업은 가상 시스템 1에서 실행됨)	승인 요청이 가상 시스템 1에 대해서만 트리거됨	가상 시스템 1
사용 권한 3	제거 - 배포 작업에 대한 정책 A(배포 제거 승인 정책)와 제거 - 가상 시스템 작업에 대한 정책 B(제거 - 가상 시스템 정책)	작업 1(Blueprint 1에 대해 제거 - 배포 작업 실행)	승인 요청이 Blueprint 1에 대해서만 트리거됨	Blueprint 1, Blueprint 2 및 가상 시스템 1
		작업 2(Blueprint 2에 대해 제거 - 배포 작업 실행)	승인 요청이 Blueprint 2에 대해서만 트리거됨	Blueprint 2 및 가상 시스템 1
		작업 3 (제거 - 가상 시스템 작업은 가상 시스템 1에서 실행됨)	승인 요청이 가상 시스템 1에 대해서만 트리거됨	가상 시스템 1

여러 사용 권한의 승인 정책 예

승인 정책을 비즈니스 그룹의 동일한 사용자에게 사용 권한이 부여된 여러 사용 권한에서 사용된 항목에 적용하는 경우 승인 정책이 명시적으로 사용 권한에 적용되지 않은 서비스에서도 항목에 대해 승인 정책이 트리거됩니다.

예를 들어 다음과 같은 Blueprint, 서비스, 승인 정책 및 사용 권한을 생성합니다.

Blueprint

- RHEL vSphere 가상 시스템
- QE 테스트에 RHEL vSphere 가상 시스템이 포함됨
- QE 교육에 RHEL vSphere 가상 시스템이 포함됨

서비스

- QE 테스트 Blueprint가 테스트 서비스와 연결됨
- QE 교육 Blueprint가 교육 서비스와 연결됨

사용 권한

- 사용 권한 1
- 사용 권한 2

표 3-69. 사용 권한 구성

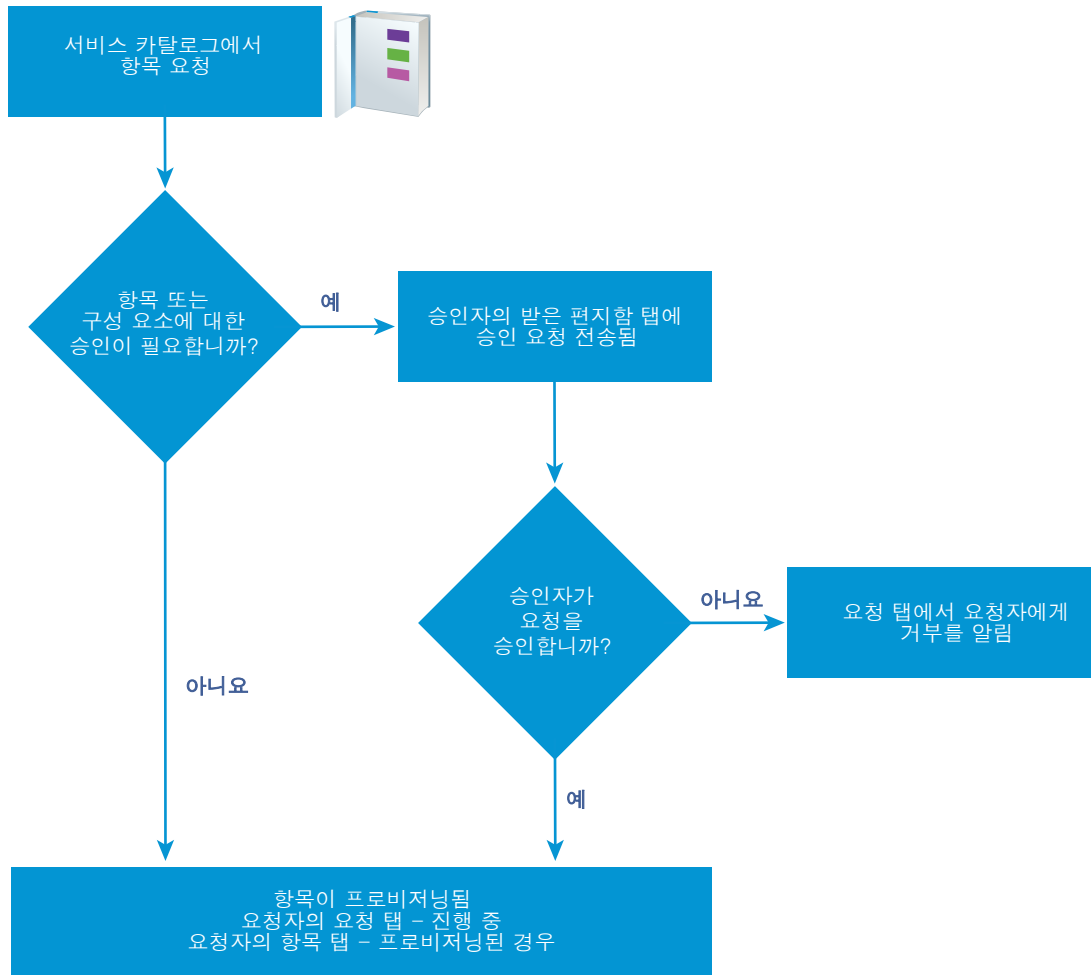
사용 권한 이름	비즈니스 그룹	권한 있는 서비스	권한 있는 항목
사용 권한 1	QE	테스트	카탈로그 항목 요청 - 가상 시스템이 가상 시스템 구성 요소에 적용됨
사용 권한 2	QE	교육	

결과

사용자가 서비스 카탈로그에서 QE 교육을 선택하는 경우 QE 교육 Blueprint에서 사용되는 가상 시스템 구성 요소를 기반으로 하는 Blueprint이기 때문에 승인 정책이 RHEL vSphere 가상 시스템에 대해 트리거됩니다.

서비스 카탈로그에서 승인 정책 처리

사용자가 승인 정책이 적용된 서비스 카탈로그에서 항목을 요청하는 경우 이 요청은 다음 워크플로와 유사하게 승인자 및 요청하는 사용자에게 의해 처리됩니다.



승인 정책 생성

테넌트 관리자와 승인 관리자는 승인 정책을 정의하고 사용 권한에서 이러한 정책을 사용할 수 있습니다. 사전 승인 및 사후 승인 이벤트에 대해 여러 수준이 포함된 승인 정책을 구성할 수 있습니다.

소프트웨어 구성 요소 Blueprint의 설정을 수정하고 승인 정책에서 이 설정을 사용하여 승인 요청을 트리거하는 경우 승인 정책이 예상과 다르게 작동할 수 있습니다. 구성 요소의 설정을 수정해야 하는 경우에는 변경 내용이 하나 이상의 승인 정책에 영향을 미치지 않는지 확인하십시오.

필수 조건

테넌트 관리자 또는 승인 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 승인 정책 정보 지정

승인 정책을 생성할 때 승인 정책 유형, 이름, 설명 및 상태를 정의합니다.

2 승인 수준 생성

승인 정책을 생성할 때 사전 승인 및 사후 승인 수준을 추가할 수 있습니다.

3 시스템 및 사용자 지정 속성을 포함하도록 승인 양식 구성

승인 양식에 나타나는 시스템 및 사용자 지정 속성을 추가할 수 있습니다. 이러한 속성을 추가하여 승인자가 CPU, 리스 또는 메모리 같은 시스템 리소스 설정에 대한 시스템 속성 값을 변경하고 승인 요청을 완료하기 전에 속성을 사용자 지정할 수 있도록 합니다.

4 승인 정책 설정

승인 정책을 생성하는 경우 서비스 카탈로그 사용자가 요청하는 항목이 승인되어야 하는 시점을 결정하는 다양한 옵션을 구성할 수 있습니다. 요청이 프로비저닝을 시작하기 전에 또는 항목이 프로비저닝된 후 요청한 사용자에게 릴리스되기 전에 승인이 필요할 수 있습니다.

승인 정책 정보 지정

승인 정책을 생성할 때 승인 정책 유형, 이름, 설명 및 상태를 정의합니다.

필수 조건

테넌트 관리자 또는 승인 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 승인 정책**을 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 정책 유형 또는 소프트웨어 구성 요소를 선택합니다.

옵션	설명
승인 정책 유형 선택	<p>정책 요청 유형을 기반으로 승인 정책을 생성합니다.</p> <p>해당 유형의 모든 카탈로그 항목에 적용할 수 있는 승인 정책을 정의하려면 이 옵션을 선택합니다. 요청 유형은 일반 요청, 카탈로그 항목 요청 또는 리소스 작업 요청일 수 있습니다.</p> <p>사용 가능한 조건 구성 옵션은 유형에 따라 다릅니다. 유형이 구체적일수록 구성 필드도 구체적입니다. 예를 들어 서비스 카탈로그 - 카탈로그 항목 요청은 모든 카탈로그 항목 요청에 공통으로 해당하는 필드만 제공하지만 서비스 카탈로그 - 카탈로그 항목 요청 - 가상 시스템에는 공통 옵션과 가상 시스템과 관련된 옵션도 포함되어 있습니다.</p> <p>요청 유형은 승인 정책을 적용할 수 있는 카탈로그 항목 또는 작업을 제한합니다.</p>
항목 선택	<p>특정 항목을 기반으로 승인 정책을 생성합니다.</p> <p>시스템 또는 기타 배포의 일부로만 서비스 카탈로그에서 개별 항목으로 사용할 수 없는 특정 항목에 적용할 수 있는 승인 정책을 정의하려면 이 옵션을 선택합니다. 예를 들어 소프트웨어 구성 요소입니다.</p> <p>사용 가능한 조건 구성 필드는 항목과 관련되며 정책 유형 항목에 대해 제공된 기준보다 세부적일 수 있습니다.</p>
목록	<p>사용 가능한 정책 유형 또는 카탈로그 항목을 나열합니다.</p> <p>열을 검색하거나 정렬하여 특정 항목 또는 유형을 찾습니다.</p>

- 4 **확인**을 클릭합니다.
- 5 이름을 입력하고 원하는 경우 설명을 입력합니다.

6 상태 드롭다운 메뉴에서 정책 상태를 선택합니다.

옵션	설명
초안	편집 가능한 상태로 승인 정책을 저장합니다.
활성	사용자가 사용 권한에서 사용할 수 있는 읽기 전용 상태로 승인 정책을 저장합니다.
비활성	사용자가 승인 정책을 활성화할 때까지 사용 권한에서 사용할 수 없는 읽기 전용 상태로 승인 정책을 저장합니다.

후속 작업

사전 승인 및 사후 승인 수준을 생성합니다.

승인 수준 생성

승인 정책을 생성할 때 사전 승인 및 사후 승인 수준을 추가할 수 있습니다.

승인 정책에 대해 여러 승인 수준을 생성할 수 있습니다. 서비스 카탈로그 사용자가 여러 수준이 포함된 승인 정책이 적용되는 항목을 요청하는 경우 승인 요청이 다음 승인자에게 전송되기 전에 각각의 첫 번째 수준이 승인되어야 합니다. [승인 정책 사용](#) 항목을 참조하십시오.

필수 조건

[승인 정책 정보 지정](#).

프로시저

- 1 사전 승인 또는 사후 승인 탭에서 **새로 만들기** 아이콘(+)을 클릭합니다.
- 2 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 3 승인 요구 사항을 선택합니다.

옵션	설명
항상 필요	승인 정책이 모든 요청에 대해 트리거됩니다.
조건에 따라 필요	<p>승인 정책이 하나 이상의 조건 절을 기반으로 합니다.</p> <p>이 옵션을 선택하는 경우 조건을 생성해야 합니다. 이 승인 정책이 사용 권한의 적합한 서비스, 카탈로그 항목 또는 작업에 적용되는 경우 조건이 평가됩니다. 조건이 True인 경우 요청이 프로비저닝되기 전에 지정된 승인자 방법에 의해 승인되어야 합니다. 조건이 False인 경우 승인을 요청하지 않고 요청이 프로비저닝됩니다. 예를 들어 4개 이상의 CPU가 포함된 가상 시스템에 대한 모든 요청은 가상 인프라 관리자에 의해 승인되어야 합니다.</p> <p>조건이 기반으로 하는 필드의 가용성은 선택된 승인 정책 유형 또는 카탈로그 항목에 의해 결정됩니다.</p> <p>조건에 대한 값을 입력하는 경우 값은 대/소문자를 구분합니다.</p> <p>2개 이상의 조건 절을 구성하려면 절에 대해 부울 연산을 선택합니다.</p>

4 승인자를 선택합니다.

옵션	작업
특정 사용자 및 그룹	선택된 사용자에게 승인 요청을 전송합니다.
요청에서 승인자 결정	정의된 조건을 기반으로 사용자에게 승인 요청을 전송합니다.
이벤트 구독 사용	정의된 이벤트 구독을 기반으로 승인 요청을 처리합니다. 워크플로 구독은 관리 > 이벤트 > 구독 에서 정의되어야 합니다. 적용 가능한 워크플로 구독은 사전 승인 및 사후 승인입니다.

5 요청 또는 작업을 승인해야 하는 사람을 나타냅니다.

옵션	설명
누구나 승인 가능	요청이 처리되기 전에 승인자 중 한 명만 승인해야 합니다. 항목이 서비스 카탈로그에서 요청되는 경우 승인을 위한 요청이 모든 승인자에게 전송됩니다. 한 승인자가 요청을 승인하는 경우 요청이 승인되고 승인을 위한 요청이 다른 승인자의 받은 편지함에서 제거됩니다.
모두가 승인해야 함	요청이 처리되기 전에 지정된 모든 승인자가 승인해야 합니다.

6 승인 양식에 속성을 추가하거나 수준을 저장합니다.

- 승인 양식에 속성을 추가하려면 **시스템 속성** 또는 **사용자 지정 속성**을 클릭합니다.
- 수준을 저장하려면 **확인**을 클릭합니다.

후속 작업

승인 양식에 속성을 추가하려면 **시스템 및 사용자 지정 속성을 포함하도록 승인 양식 구성** 항목을 참조하십시오.

시스템 및 사용자 지정 속성을 포함하도록 승인 양식 구성

승인 양식에 나타나는 시스템 및 사용자 지정 속성을 추가할 수 있습니다. 이러한 속성을 추가하여 승인자가 CPU, 리스 또는 메모리 같은 시스템 리소스 설정에 대한 시스템 속성 값을 변경하고 승인 요청을 완료하기 전에 속성을 사용자 지정할 수 있도록 합니다.

사용 가능한 시스템 속성은 승인 정책 유형과 Blueprint 구성 방법에 따라 다릅니다. 일부 속성의 경우, 속성이 시스템 속성 목록에 나타나기 전에 Blueprint의 구성 필드에 최소값과 최대값이 포함되어야 합니다.

사용자 지정 속성은 승인 수준을 추가하면 추가될 수 있습니다. 사용자 지정 속성이 구성되어 Blueprint에 포함된 경우 승인 양식에 추가하는 사용자 지정 속성은 해당 사용자 지정 속성의 다른 모든 인스턴스(예: Blueprint의 속성 그룹 또는 끝점)를 덮어씁니다.

승인자는 승인 양식에서 선택 또는 구성된 속성을 수정할 수 있습니다.

필수 조건

- **테넌트 관리자** 또는 **승인 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- **승인 수준 생성**.

프로시저

- 1 사전 승인 또는 사후 승인 탭에서 **새로 만들기** 아이콘(+)을 클릭합니다.
- 2 시스템 속성 탭을 클릭합니다.
- 3 승인 프로세스 중에 승인자가 구성하기를 원하는 각 시스템 속성에 대한 확인란을 선택합니다.
- 4 사용자 지정 속성을 구성합니다.

승인 프로세스 중에 승인자가 구성하기를 원하는 하나 이상의 사용자 지정 속성을 추가합니다.

- a 사용자 지정 속성 탭을 클릭합니다.
- b 새로 만들기 아이콘(+)을 클릭합니다.
- c 사용자 지정 속성 값을 입력합니다.

옵션	설명
이름	속성 이름을 입력합니다.
Label	승인 양식에서 승인자에게 제공된 레이블을 입력합니다.
설명	승인자에 대한 확장된 정보를 입력합니다. 이 정보는 양식에서 필드 도구 설명으로 나타납니다.

- d 저장을 클릭합니다.
- e 여러 사용자 지정 속성을 삭제하려면 행을 선택하고 삭제를 클릭합니다.

5 확인을 클릭합니다.

후속 작업

- 추가적인 사전 승인 또는 사후 승인 수준을 추가합니다.
- 승인 정책을 저장합니다. **사용 권한**의 서비스, 항목 또는 작업에 적용하려면 정책이 활성 상태여야 합니다.

승인 정책 설정

승인 정책을 생성하는 경우 서비스 카탈로그 사용자가 요청하는 항목이 승인되어야 하는 시점을 결정하는 다양한 옵션을 구성할 수 있습니다. 요청이 프로비저닝을 시작하기 전에 또는 항목이 프로비저닝된 후 요청한 사용자에게 릴리스되기 전에 승인이 필요할 수 있습니다.

관리 > 승인 정책을 선택합니다. **새로 만들기**를 클릭합니다.

■ 승인 정책 유형 설정

승인 정책 유형은 승인 정책이 구성되는 방식과 사용 권한에서 적용할 수 있는 항목 또는 작업을 결정합니다. 승인 수준을 추가하는 경우 정책 유형 또는 항목이 승인 수준에 대한 조건을 생성하는 데 사용할 수 있는 필드에 영향을 미칩니다.

■ 승인 정책 설정 추가

정책을 관리할 수 있도록 정책의 상태를 비롯하여 승인 정책에 대한 기본 정보를 구성합니다.

■ 승인 정책 설정에 수준 정보 추가

승인 수준에는 서비스 카탈로그 사용자가 항목을 요청할 때 승인 프로세스를 트리거하는 조건 그리고 포함하고 싶은 시스템 속성과 사용자 지정 속성이 포함됩니다. 트리거되면, 승인 요청이 지정된 승인자에게 전송됩니다.

■ 승인 정책 설정에 시스템 속성 추가

승인 양식에 추가하려는 그리고 승인자의 값 수정을 허용하는 시스템 속성을 선택했습니다.

■ 승인 정책 설정에 사용자 지정 속성 추가

승인자의 값 수정을 허용하도록 승인 양식에 추가하려는 사용자 지정 속성을 구성합니다.

승인 정책 유형 설정

승인 정책 유형은 승인 정책이 구성되는 방식과 사용 권한에서 적용할 수 있는 항목 또는 작업을 결정합니다. 승인 수준을 추가하는 경우 정책 유형 또는 항목이 승인 수준에 대한 조건을 생성하는 데 사용할 수 있는 필드에 영향을 미칩니다.

관리 > 승인 정책을 선택합니다. **새로 만들기**를 클릭합니다.

표 3-70. 승인 정책 유형 옵션

옵션	설명
승인 정책 유형 선택	<p>정책 요청 유형을 기반으로 승인 정책을 생성합니다.</p> <p>해당 유형의 모든 카탈로그 항목에 적용할 수 있는 승인 정책을 정의하려면 이 옵션을 선택합니다. 요청 유형은 일반 요청, 카탈로그 항목 요청 또는 리소스 작업 요청일 수 있습니다.</p> <p>사용 가능한 조건 구성 옵션은 유형에 따라 다릅니다. 유형이 구체적일수록 구성 필드도 구체적입니다. 예를 들어 서비스 카탈로그 - 카탈로그 항목 요청은 모든 카탈로그 항목 요청에 공통으로 해당하는 필드만 제공하지만 서비스 카탈로그 - 카탈로그 항목 요청 - 가상 시스템에는 공통 옵션과 가상 시스템과 관련된 옵션도 포함되어 있습니다.</p> <p>요청 유형은 승인 정책을 적용할 수 있는 카탈로그 항목 또는 작업을 제한합니다.</p>
항목 선택	<p>특정 항목을 기반으로 승인 정책을 생성합니다.</p> <p>시스템 또는 기타 배포의 일부로만 서비스 카탈로그에서 개별 항목으로 사용할 수 없는 특정 항목에 적용할 수 있는 승인 정책을 정의하려면 이 옵션을 선택합니다. 예를 들어 소프트웨어 구성 요소입니다.</p> <p>사용 가능한 조건 구성 필드는 항목과 관련되며 정책 유형 항목에 대해 제공된 기준보다 세부적일 수 있습니다.</p>
목록	<p>사용 가능한 정책 유형 또는 카탈로그 항목을 나열합니다.</p> <p>열을 검색하거나 정렬하여 특정 항목 또는 유형을 찾습니다.</p>

승인 정책 설정 추가

정책을 관리할 수 있도록 정책의 상태를 비롯하여 승인 정책에 대한 기본 정보를 구성합니다.

기본 승인 정책 정보를 정의하려면 **관리 > 승인 정책**을 선택합니다. **새로 만들기**를 클릭합니다. 정책 유형을 선택하고 **확인**을 클릭합니다.

표 3-71. 승인 정책 옵션

옵션	설명
이름	사용 권한에 승인 정책을 적용할 때 나타나는 이름.
설명	승인 정책 구성 방법에 대한 세부 정보 표시 설명을 제공합니다. 이 정보는 승인 정책을 관리하는 데 도움이 됩니다.
상태	가능한 값은 다음과 같습니다. <ul style="list-style-type: none"> ■ 초안. 사용 권한에 적용할 승인 정책을 사용할 수 없습니다. 정책을 활성화한 후에는 초안 상태로 되돌릴 수 없습니다. ■ 활성. 사용 권한에 적용할 승인 정책을 사용할 수 있습니다. ■ 비활성. 사용 권한에 적용할 승인 정책을 사용할 수 없습니다. 정책이 사용 권한에 적용되지 않은 상태에서 정책을 비활성화한 경우 정책을 삭제할 수 있지만 다시 활성화할 수는 없습니다. 정책이 적용된 상태에서 정책을 비활성화한 경우 정책이 적용되는 항목을 다른 정책에 연결해야 합니다. 그렇지 않으면 항목이 연결 해제됩니다. 연결 해제된 항목과 작업에 대한 권한은 여전히 사용자에게 있지만 여기에 승인 정책이 적용되지는 않습니다.
정책 유형	승인 정책 요청 유형을 표시합니다. 승인 정책의 기반이 되는 카탈로그 항목을 선택한 경우 연결된 요청 유형이 표시됩니다.
항목	선택된 카탈로그 항목을 표시합니다. 승인 정책의 기반이 되는 요청 유형을 선택한 경우 이 필드는 비어 있습니다.
마지막으로 업데이트한 사용자	승인 정책을 변경한 사용자의 이름.
마지막 업데이트 날짜	승인 정책을 마지막으로 변경한 날짜.
사전 승인 수준	요청된 항목이 프로비저닝되거나 작업이 실행되기 전에 승인이 필요한 경우 서비스 카탈로그 사용자가 항목을 요청할 때 승인 프로세스를 트리거하는 하나 이상의 조건을 구성합니다.
사후 승인 수준	항목이 프로비저닝되었지만 프로비저닝 또는 수정된 항목이 요청한 서비스 카탈로그 사용자에게 릴리스되기 전에 승인이 필요한 경우 승인 프로세스를 트리거하는 하나 이상의 조건을 구성합니다. 예를 들어 가상 인프라 관리자는 가상 시스템을 서비스 카탈로그 사용자에게 릴리스하기 전에 해당 시스템이 작업 가능한 상태인지 확인합니다.
연결된 사용 권한 보기	승인 정책이 서비스, 카탈로그 항목 또는 작업에 적용되는 모든 사용 권한을 표시합니다. 한 사용 권한의 항목을 다른 정책에 연결할 수 있습니다. 이 옵션은 활성 승인 정책을 볼 때만 사용할 수 있습니다.

승인 정책 설정에 수준 정보 추가

승인 수준에는 서비스 카탈로그 사용자가 항목을 요청할 때 승인 프로세스를 트리거하는 조건 그리고 포함하고 싶은 시스템 속성과 사용자 지정 속성이 포함됩니다. 트리거되면, 승인 요청이 지정된 승인자에게 전송됩니다.

기본 승인 정책 정보를 정의하려면 **관리 > 승인 정책**을 선택합니다. **새로 만들기**를 클릭합니다. 정책 유형을 선택하고 **확인**을 클릭합니다. 사전 승인 또는 사후 승인 탭에서 **새로 만들기** 아이콘(+)을 클릭합니다.

처리하려는 순서에 따라 수준의 우선 순위를 지정합니다. 승인 정책이 트리거되는 경우 첫 번째 승인 수준이 거부되면 요청이 거부됩니다.

표 3-72. 수준 정보 옵션

옵션	설명
이름	이름을 입력합니다. 승인 정책이 포함된 요청을 검토 중일 때 수준 이름이 나타납니다.
설명	수준 설명을 입력합니다. 예를 들어 CPU>4 to VI Admin입니다.
승인이 언제 필요합니까?	승인 정책이 트리거되는 시점을 선택합니다.
항상 필요	승인 정책이 모든 요청에 대해 트리거됩니다. 이 옵션을 선택하고 이 승인 정책을 사용 권한의 적합한 서비스, 카탈로그 항목 또는 작업에 적용하는 경우 요청이 프로비저닝되기 전에 지정된 승인자 방법에 의해 승인되어야 합니다. 예를 들어 모든 요청은 요청한 사용자의 관리자에 의해 승인되어야 합니다.
조건에 따라 필요	승인 정책이 하나 이상의 조건 절을 기반으로 합니다. 이 옵션을 선택하는 경우 조건을 생성해야 합니다. 이 승인 정책이 사용 권한의 적합한 서비스, 카탈로그 항목 또는 작업에 적용되는 경우 조건이 평가됩니다. 조건이 True인 경우 요청이 프로비저닝되기 전에 지정된 승인자 방법에 의해 승인되어야 합니다. 조건이 False인 경우 승인을 요청하지 않고 요청이 프로비저닝됩니다. 예를 들어 4개 이상의 CPU가 포함된 가상 시스템에 대한 모든 요청은 가상 인프라 관리자에 의해 승인되어야 합니다. 조건이 기반으로 하는 필드의 가용성은 선택된 승인 정책 유형 또는 카탈로그 항목에 의해 결정됩니다. 조건에 대한 값을 입력하는 경우 값은 대/소문자를 구분합니다. 2개 이상의 조건 절을 구성하려면 절에 대해 부울 연산을 선택합니다. <ul style="list-style-type: none"> ■ 다음 중 모두. 모든 절이 True인 경우 승인이 트리거됩니다. 이는 각 절 간의 부울 AND 연산자입니다. ■ 다음 중 일부. 하나 이상의 절이 True인 경우 승인 수준이 트리거됩니다. 이는 각 절 간의 부울 OR 연산자입니다. ■ 다음 제외. True인 절이 없는 경우 승인 수준이 트리거됩니다. 이는 각 절 간의 부울 NOT 연산자입니다.
승인자	승인자 방법을 선택합니다.

표 3-72. 수준 정보 옵션 (계속)

옵션	설명
특정 사용자 및 그룹	<p>선택된 사용자에게 승인 요청을 전송합니다.</p> <p>요청이 프로비저닝되거나 작업을 실행하기 전에 서비스 카탈로그 요청을 승인해야 하는 사용자 또는 사용자 그룹을 선택합니다. 예를 들어 요청은 누구나 승인 가능이 선택된 가상 인프라 관리자 그룹으로 이동합니다.</p>
요청에서 사용자 결정	<p>정의된 조건을 기반으로 사용자에게 승인 요청을 전송합니다.</p> <p>예를 들어 비즈니스 그룹에 걸쳐 이 승인 정책을 적용하고 비즈니스 그룹 관리자가 해당 요청을 승인하기를 원하는 경우 비즈니스 그룹 > 소비자 > 사용자 > 관리자를 선택합니다.</p>
이벤트 구독 사용	<p>정의된 이벤트 구독을 기반으로 승인 요청을 처리합니다.</p> <p>워크플로 구독은 관리 > 이벤트 > 구독에서 정의되어야 합니다. 적용 가능한 워크플로 구독은 사전 승인 및 사후 승인입니다.</p>
누구나 승인 가능	<p>요청이 처리되기 전에 승인자 중 한 명만 승인해야 합니다.</p> <p>항목이 서비스 카탈로그에서 요청되는 경우 승인을 위한 요청이 모든 승인자에게 전송됩니다. 한 승인자가 요청을 승인하는 경우 요청이 승인되고 승인을 위한 요청이 다른 승인자의 받은 편지함에서 제거됩니다.</p> <p>첫 번째 승인자가 요청을 거부하는 경우 요청한 사용자에게 거부에 대한 알림이 전달되고 승인 요청이 승인자의 받은 편지함에서 제거됩니다.</p> <p>첫 번째 승인자가 요청을 승인하고 승인 요청이 두 번째 승인자의 콘솔에 열려 있는 경우 승인자가 승인 요청을 제출할 수 없습니다. 첫 번째 승인자 응답으로 완료된 것으로 고려되었습니다.</p> <p>특정 사용자 및 그룹 또는 요청에서 승인자 결정을 선택하고 승인자가 두 명 이상 있는 경우의 추가 옵션 중 하나입니다. 승인자가 한 명만 있는 경우 이 옵션은 적용되지 않습니다.</p>
모두가 승인해야 함	<p>요청이 처리되기 전에 지정된 모든 승인자가 승인해야 합니다.</p> <p>특정 사용자 및 그룹 또는 요청에서 승인자 결정을 선택하고 승인자가 두 명 이상 있는 경우의 추가 옵션 중 하나입니다. 승인자가 한 명만 있는 경우 이 옵션은 적용되지 않습니다.</p>

승인 정책 설정에 시스템 속성 추가

승인 양식에 추가하려는 그리고 승인자의 값 수정을 허용하는 시스템 속성을 선택했습니다.

예를 들어 가상 시스템 승인의 경우 승인자가 6개 CPU에 대한 요청을 4개 CPU로 수정하도록 허용하려면 CPU를 선택합니다.

시스템 속성을 선택하려면 **관리 > 승인 정책**을 선택합니다. **새로 만들기**를 클릭합니다. 정책 유형을 선택하고 **확인**을 클릭합니다. 사전 승인 또는 사후 승인 탭에서 **새로 만들기** 아이콘(+)을 클릭하고 **시스템 속성** 탭을 클릭합니다.

표 3-73. 시스템 속성 옵션

옵션	설명
속성	<p>사용 가능한 시스템 속성 목록은 선택된 요청 유형 또는 카탈로그 항목 및 시스템 속성이 항목에 대해 존재하는지 여부에 따라 다릅니다.</p> <p>Blueprint가 특정 방식으로 구성된 경우에만 일부 속성을 사용할 수 있습니다. 예를 들어 CPU입니다. CPU 시스템 속성과 함께 승인 정책을 적용할 Blueprint는 범위로 구성되어야 합니다. 예를 들어 CPU 최소값은 2이고 최대값은 8입니다.</p>

승인 정책 설정에 사용자 지정 속성 추가

승인자의 값 수정을 허용하도록 승인 양식에 추가하려는 사용자 지정 속성을 구성합니다.

예를 들어 가상 시스템 승인의 경우 승인자가 vCenter Server에서 시스템이 추가될 폴더를 지정하도록 허용하려면 `VMware.VirtualCenter.Folder`를 추가합니다.

이 승인 정책 양식과 관련된 사용자 지정 속성을 추가할 수도 있습니다.

시스템 속성을 선택하려면 **관리 > 승인 정책**을 선택합니다. **새로 만들기**를 클릭합니다. 정책 유형을 선택하고 **확인**을 클릭합니다. 사전 승인 또는 사후 승인 탭에서 **새로 만들기** 아이콘(+)을 클릭하고 **사용자 지정 속성** 탭을 클릭합니다.

표 3-74. 사용자 지정 속성

옵션	설명
이름	속성 이름을 입력합니다.
레이블	승인 양식에서 승인자에게 제공된 레이블을 입력합니다.
설명	<p>승인자에 대한 확장된 정보를 입력합니다.</p> <p>이 정보는 양식에서 필드 도구 설명으로 나타납니다.</p>

승인 정책 수정

활성 또는 비활성 승인 정책을 수정할 수 없습니다. 원래 정책의 복사본을 생성하고 필요한 결과를 생성하지 않는 정책을 바꿔야 합니다. 활성 및 비활성 승인 정책은 읽기 전용입니다. 승인 정책은 초안 상태에 있을 때 수정할 수 있습니다.

승인 정책의 복사본을 만드는 경우 새 정책은 원래 정책 유형을 기반으로 합니다. 정책 유형을 제외한 모든 특성을 편집할 수 있습니다. 수준을 수정, 추가 또는 제거하기 위해 승인 수준을 수정하거나 양식에 시스템 또는 사용자 지정 속성을 추가하려는 경우 이렇게 할 수 있습니다.


사전 승인 또는 사후 승인 수준을 생성할 수 있습니다. 승인 수준 생성에 대한 지침은 [승인 수준 생성](#) 항목을 참조하십시오.

필수 조건

테넌트 관리자 또는 승인 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 **관리 > 승인 정책**을 선택합니다.

- 2 복사할 승인 정책의 행을 선택합니다.
- 3 **복사** 아이콘()을 클릭합니다.
승인 정책의 복사본이 생성됩니다.
- 4 편집할 새 승인 정책을 선택합니다.
- 5 **이름** 텍스트 상자에 이름을 입력합니다.
- 6 (선택 사항) **설명** 텍스트 상자에 설명을 입력합니다.
- 7 **상태** 드롭다운 메뉴에서 정책 상태를 선택합니다.

옵션	설명
초안	편집 가능한 상태로 승인 정책을 저장합니다.
활성	사용자가 사용 권한에서 사용할 수 있는 읽기 전용 상태로 승인 정책을 저장합니다.
비활성	사용자가 승인 정책을 활성화할 때까지 사용 권한에서 사용할 수 없는 읽기 전용 상태로 승인 정책을 저장합니다.

- 8 사전 승인 및 사후 승인 수준을 편집합니다.
- 9 **확인**을 클릭합니다.
기존 승인 정책을 기반으로 새 승인 정책을 생성했습니다.

후속 작업

사용 권한에 새 승인 정책을 적용합니다. [사용자에게 서비스, 카탈로그 항목 및 작업에 대한 사용 권한 부여](#) 항목을 참조하십시오.

승인 정책 비활성화

승인 정책이 오래되었다고 확인되면 프로비저닝 중에 사용할 수 없도록 해당 정책을 비활성화할 수 있습니다.

승인 정책을 비활성화하려면 현재 승인 정책이 적용되고 있는 각 사용 권한에 대해 새 정책을 할당해야 합니다.

비활성화된 승인 정책을 나중에 다시 활성화하거나 비활성화된 정책을 삭제할 수 있습니다.

필수 조건

테넌트 관리자 또는 **승인 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 승인 정책**을 선택합니다.
- 2 승인 정책 이름을 클릭합니다.

3 연결된 사용 권한 보기를 클릭합니다.

- a **모두 바꿀 내용** 드롭다운 메뉴에서 새 승인 정책을 선택합니다.

목록에 2개 이상의 사용 권한이 포함되어 있는 경우 새 승인 정책이 나열된 모든 사용 권한에 적용됩니다.

- b **확인**을 클릭합니다.

4 승인 정책에 연결된 사용 권한이 없음을 확인한 후 [상태] 드롭다운 메뉴에서 **비활성**을 선택합니다.

5 **확인**을 클릭합니다.

6 승인 정책을 삭제하려면 비활성 정책을 포함하는 행을 선택합니다.

- a **삭제**를 클릭합니다.

- b **확인**을 클릭합니다.

승인 정책이 사용되고 비활성화된 사용 권한에서 승인 정책이 연결 해제됩니다. 나중에 승인 정책을 재 활성화하고 사용 권한의 항목에 다시 적용할 수 있습니다.

후속 작업

더 이상 승인 정책이 필요하지 않은 경우 삭제할 수 있습니다. [승인 정책 삭제](#) 항목을 참조하십시오.

승인 정책 삭제

비활성화했거나 필요하지 않은 승인 정책이 있는 경우 vRealize Automation에서 해당 정책을 삭제할 수 있습니다.

필수 조건

- 승인 정책 연결을 해제하고 비활성화합니다. [승인 정책 비활성화](#) 항목을 참조하십시오.
- **테넌트 관리자** 또는 **승인 관리자**로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 승인 정책**을 선택합니다.
- 2 비활성 정책이 들어 있는 행을 선택합니다.
- 3 **삭제**를 클릭합니다.
- 4 **확인**을 클릭합니다.

승인 정책이 삭제됩니다.

시나리오: MySQL이 설치된 CentOS 승인 정책 생성 및 적용

개발 및 품질 엔지니어링 비즈니스 그룹의 테넌트 관리자로서, 카탈로그 항목 요청에 엄격한 거버넌스를 적용하려고 합니다. 사용자가 MySQL이 설치된 CentOS 카탈로그 항목을 프로비저닝하기 전에 vSphere 가상 인프라 관리자가 시스템 요청을 승인하고 소프트웨어 관리자가 소프트웨어 요청을 승인하도록 지정합니다.

특정 조건을 기반으로 시스템에 대해 vSphere 가상 인프라 관리자의 승인을 요청하도록 MySQL이 설치된 vSphere CentOS 서비스 카탈로그 요청에 대한 하나의 승인 정책을 생성 및 적용하고 모든 요청에 대해 소프트웨어 관리자의 승인을 요청하도록 MySQL Software 구성 요소에 대한 다른 승인 정책을 생성하고 적용합니다.

승인 관리자는 승인 생성만 가능하며 비즈니스 그룹 관리자는 승인을 사용 권한에 적용할 수 있습니다. 테넌트 관리자는 승인 생성 및 사용 권한 적용이 모두 가능합니다.

필수 조건

- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다. 테넌트 관리자만 승인 정책을 생성하고 적용할 수 있습니다.
- MySQL이 설치된 CentOS 카탈로그 항목이 서비스에 포함되어 있는지 확인합니다. **시나리오: 서비스 카탈로그에서 MySQL이 설치된 CentOS 애플리케이션 Blueprint를 사용할 수 있도록 설정** 항목을 참조하십시오.

시나리오: MySQL이 설치된 CentOS 가상 시스템 승인 정책 생성

테넌트 관리자로서 환경 내에서 적절하게 프로비저닝된 가상 시스템이 개발 및 품질 엔지니어링 그룹에 제공되고 있는지 확인하려고 합니다. 따라서 특정 요청 유형에 대해 사전 승인이 필요한 승인 정책을 생성합니다.

MySQL이 설치된 CentOS 가상 시스템은 vCenter Server 리소스를 사용하므로 리소스가 효율적으로 사용될 수 있도록 요청된 메모리가 2048MB를 초과하거나 CPU가 3개 이상인 경우 vSphere 가상 인프라 관리자가 요청을 승인하도록 지정하려고 합니다. 또한 요청을 승인하기 전에 승인자에게 요청된 CPU와 메모리 값을 수정할 수 있는 권한을 부여합니다.


프로시저

- 1 **관리 > 승인 정책**을 선택합니다.
- 2 가상 시스템 프로비저닝에 대한 승인 정책을 생성합니다.
 - a **새로 만들기** 아이콘(+)을 클릭합니다.
 - b **승인 정책 유형 선택**을 선택합니다.
 - c 목록에서 **서비스 카탈로그 - 카탈로그 항목 요청 - 가상 시스템**을 선택합니다.
 - d **확인**을 클릭합니다.
 - e 다음 옵션을 구성합니다.

옵션	구성
이름	CentOS on vSphere CPU or Memory VM을 입력합니다.
설명	Requires VI Admin approval for CPU>2 or Memory>2048을 입력합니다.
상태	활성을 선택합니다.

- 3 **사전 승인** 탭에서 **추가** 아이콘(+)을 클릭합니다.

4 트리거 조건 및 승인 작업을 사용하여 **수준 정보** 탭을 구성합니다.

- a **이름** 텍스트 상자에 **CPU>2 or Memory>2048 - VI Admin**을 입력합니다.
- b **설명** 텍스트 상자에 **VI Admin approval for CPU and Memory**를 입력합니다.
- c **조건에 따라 필요**를 선택합니다.
- d [절] 드롭다운 목록에서 **다음 중 일부**를 선택합니다.
- e 새로운 [절] 드롭다운 목록에서 **CPU**를 선택하고 값 **CPU > 2**로 절을 구성합니다.
- f **표현식 추가**를 클릭하고 값 **Memory (MB) > 2048**로 절을 구성합니다.
- g **특정 사용자 및 그룹**을 선택합니다.
- h 검색 텍스트 상자에 vSphere 가상 인프라 관리자 또는 관리자 그룹의 이름을 입력하고 검색 아이콘()을 클릭합니다.
- i 사용자 또는 그룹을 선택합니다.
- j **누구나 승인 가능**을 선택합니다.

이 요청은 단 한 명의 가상 인프라 관리자만 리소스를 확인하고 요청을 승인하면 됩니다.

5 **시스템 속성** 탭을 클릭하고 승인자가 요청을 승인하기 전에 요청된 CPU 및 메모리 값을 수정하도록 허용하는 속성을 선택합니다.

- a **CPU 및 메모리(MB)** 확인란을 선택합니다.
- b **확인**을 클릭합니다.

6 **확인**을 클릭합니다.

가상 시스템 요청을 위한 승인 정책을 생성했지만 여전히 MySQL 구성 요소에 대한 승인을 생성해야 합니다. 정책을 사용 권한에 적용할 때까지 어떠한 승인도 트리거되지 않습니다.

시나리오: MySQL Software 구성 요소 승인 정책 생성

소프트웨어 관리자가 테넌트 관리자인 사용자에게 라이선싱 사용량을 추적할 수 있도록 MySQL 설치를 위한 승인 정책을 생성하고 적용하도록 요청했습니다. 이에 Linux 가상 시스템용 MySQL Software 구성 요소를 요청할 때마다 소프트웨어 라이선스 관리자에게 알리도록 지정하는 정책을 생성합니다.

일부 환경에서, 소프트웨어 관리자가 라이선스 키를 제공해야 하기 때문에 이러한 유형의 승인이 필요할 수 있습니다. 이 시나리오에서는 소프트웨어 관리자가 요청을 추적 및 승인할 수 있도록 하기만 하면 됩니다. 승인 정책을 생성한 후 해당 정책을 Linux 가상 시스템용 MySQL 카탈로그 항목에 적용합니다. 이 승인 정책은 매우 제한적인 것으로, 사용 권한의 Linux 가상 시스템용 MySQL Software 구성 요소에만 적용될 수 있습니다.

프로시저

1 **관리 > 승인 정책**을 선택합니다.

2 MySQL Software 구성 요소에 대한 승인 정책을 생성합니다.

- 새로 만들기** 아이콘(+)을 클릭합니다.
- 항목 선택**을 선택합니다.
- Linux 가상 시스템용 MySQL**을 선택합니다.
- 확인**을 클릭합니다.
- 다음 옵션을 구성합니다.

옵션	구성
이름	MySQL tracking approval을 입력합니다.
설명	Approval request sent to software manager를 입력합니다.
상태	활성을 선택합니다.

3 사전 승인 탭에서 추가 아이콘(+)을 클릭합니다.

4 트리거 조건 및 승인 작업을 사용하여 수준 정보 탭을 구성합니다.

- 이름** 텍스트 상자에 **MySQL software deployment notice**를 입력합니다.
 - 설명** 텍스트 상자에 **Software mgr approval of software installation**을 입력합니다.
 - 항상 필요**를 선택합니다.
 - 특정 사용자 및 그룹**을 선택합니다.
 - 검색 텍스트 상자에 소프트웨어 관리자의 이름을 입력하고 검색 아이콘(🔍)을 클릭한 다음 사용자를 선택합니다.
 - 누구나 승인 가능**을 선택합니다.
- 한 명의 소프트웨어 관리자만 요청을 승인하면 됩니다.
- 확인**을 클릭합니다.

5 확인을 클릭합니다.

가상 시스템 및 Linux 가상 시스템용 MySQL Software 구성 요소를 위한 승인 정책을 생성했습니다. 승인 정책을 사용 권한에 적용할 때까지 어떠한 승인도 트리거되지 않습니다.

시나리오: MySQL이 설치된 CentOS 구성 요소에 승인 정책 적용

테넌트 관리자로서 승인 정책 및 사용 권한을 생성할 수 있습니다. 생성한 승인 정책을 적용하도록 개발 및 QE 사용 권한을 수정하여 서비스 카탈로그 사용자가 항목 요청 시 승인이 트리거되도록할 수 있습니다.

전체 카탈로그 서비스에 대한 사용 권한을 비즈니스 그룹에 부여하는 것이 더 쉬울 수 있지만 이 경우 카탈로그 항목에 대한 개별 사용 권한을 생성할 때와 동일한 제어와 거버넌스를 가질 수는 없습니다. 예를 들어 사용자에게 특정 서비스에 대한 사용 권한을 부여하면 사용자는 현재 서비스에 속해 있는 모든 카탈로그 항목 그리고 나중에 서비스에 추가될 모든 항목을 요청할 수 있습니다. 이것은 또한 항상 관리자에게 승인을 요청하는 것과 같은, 서비스의 모든 카탈로그 항목에 적용되는 매우 개괄적인 승인

정책만 사용할 수 있음을 의미합니다. 카탈로그 항목에 대한 사용 권한을 개별적으로 부여하도록 선택하는 경우 각 항목에 매우 한정적인 승인 정책을 생성 및 적용할 수 있고 누가 서비스의 어떤 품목을 요청할 수 있는지 긴밀하게 제어할 수 있습니다. 카탈로그 항목의 개별 구성 요소에 대한 사용 권한을 개별적으로 부여하도록 선택하는 경우 더 효과적으로 제어할 수 있습니다.

사용 권한에서 항목에 적용할 승인 정책을 모르는 경우 나중에 돌아와 적용할 수 있습니다. 이 시나리오에서는 게시된 동일한 애플리케이션 Blueprint의 구성 요소 두 개에 서로 다른 승인 정책을 적용합니다.

프로시저

- 1 **관리 > 카탈로그 관리 > 사용 권한**을 선택합니다.
- 2 **개발 및 QE 사용 권한**을 클릭합니다.
- 3 **항목 및 승인** 탭을 클릭합니다.
- 4 MySQL이 설치된 CentOS 시스템을 추가하고 승인 정책을 적용합니다.
 - a 권한 있는 항목 머리글 옆에 있는 **항목 추가** 아이콘(+)을 클릭합니다.
 - b **MySQL이 설치된 CentOS** 확인란을 선택합니다.
 - c **선택한 항목에 적용할 정책** 드롭다운 화살표를 클릭합니다.
vSphere CentOS CPU 및 메모리 정책이 목록에 없습니다.
 - d **모두 표시**를 클릭하고 아래쪽 화살표를 클릭하여 모든 승인 정책을 봅니다.
 - e **vSphere CentOS CPU 및 메모리 [서비스 카탈로그 - 카탈로그 항목 요청 - 가상 시스템]**을 선택합니다.
vSphere CentOS 시스템은 애플리케이션 Blueprint의 시스템 Blueprint입니다. 정책 이름을 검토하고 카탈로그 항목 유형에 적합한 하나의 이름을 선택합니다. 잘못된 정책을 적용하는 경우 승인 정책이 실패하거나 잘못된 조건을 기반으로 승인 요청을 트리거합니다.
 - f **확인**을 클릭합니다.
- 5 Linux 가상 시스템용 MySQL 소프트웨어 구성 요소를 항목으로 추가하고 MySQL 항목에 승인 정책을 적용합니다.
 - a [권한 있는 카탈로그 항목 및 구성 요소] 머리글 옆에 있는 **카탈로그 항목 및 구성 요소 추가** 아이콘(+)을 클릭합니다.
 - b **카탈로그 항목 및 구성 요소** 드롭다운 메뉴에서 **아니요**를 선택합니다.
소프트웨어 구성 요소가 항상 시스템과 연결됩니다. 서비스 카탈로그에서 개별적으로 요청할 수는 없습니다.
 - c **Linux 가상 시스템용 MySQL** 확인란을 선택합니다.
 - d **선택한 항목에 적용할 정책** 드롭다운 화살표를 클릭합니다.

- e **MySQL 추적 승인 [서비스 카탈로그 - 카탈로그 항목 요청 - 소프트웨어 구성 요소]**를 선택합니다.

승인 정책이 가상 시스템에 추가되어 있는 이 특정 소프트웨어 구성 요소에 대해 생성되었기 때문에 고급 옵션은 필요하지 않습니다.

- f **확인**을 클릭합니다.

6 사용자가 프로비저닝된 시스템에서 실행할 수 있는 작업을 추가합니다.

이 시나리오에서는 작업에 승인 정책이 적용되지 않습니다.

- a [권한 있는 작업] 머리글 옆에 있는 **작업 추가** 아이콘(+)을 클릭합니다.

- b 다음 작업을 선택합니다.

이름/유형	설명
스냅샷 생성/가상 시스템	설치된 소프트웨어를 포함하여 가상 시스템의 스냅샷을 생성합니다. 개발자가 개발 중 되돌릴 수 있는 스냅샷을 생성할 수 있습니다.
제거/배포	시스템뿐만 아니라 전체 프로비저닝된 Blueprint를 제거합니다. 이 작업을 사용하여 구성 요소가 분리되는 것을 방지합니다.
전원 끄기/시스템	가상 시스템의 전원을 끕니다.
전원 켜기/시스템	가상 시스템의 전원을 켭니다.
스냅샷으로 되돌리기/가상 시스템	이전에 생성한 스냅샷으로 되돌립니다.

- c **확인**을 클릭합니다.

7 완료를 클릭합니다.

이 사용 권한을 사용하면 서로 다른 Blueprint에서 서로 다른 승인을 요구할 수 있습니다.

후속 작업

서비스 카탈로그에서 MySQL이 설치된 CentOS 항목을 비즈니스 그룹의 구성원으로 요청하여 사용 권한 및 승인이 예상대로 동작하는지 확인합니다.

매개 변수화된 Blueprint를 사용하여 시스템 프로비저닝 요청

크기 또는 이미지 구성 요소 프로파일을 포함하도록 설계된 vSphere 시스템 Blueprint에 대한 시스템 프로비저닝을 요청할 경우 사용 가능한 값 집합을 선택하여 프로비저닝 설정을 지정합니다.

카탈로그에서 프로비저닝을 요청할 때 Size 및 Image 구성 요소 프로파일에 대해 사용 가능한 값 집합 옵션 중에서 선택할 수 있습니다. 값 집합 중 하나를 선택하면 해당하는 속성 값이 요청에 바인딩됩니다.

구성 요소 프로파일 값 집합은 클러스터의 모든 vSphere 시스템에 적용됩니다.

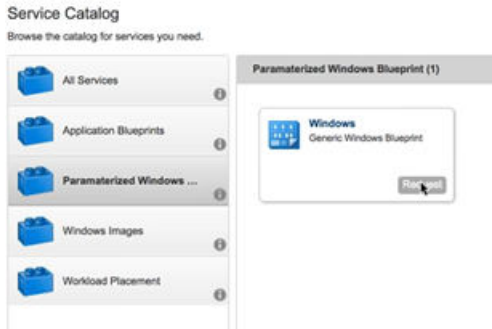
구성 요소 프로파일 구성에 대한 자세한 내용은 [Blueprint 매개 변수화 이해 및 사용](#) 항목을 참조하십시오.

필수 조건

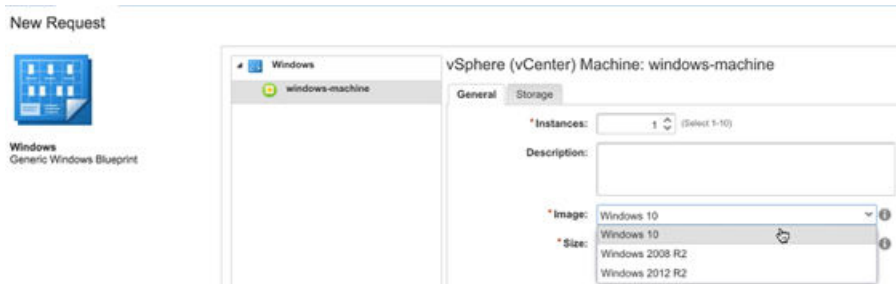
- Size 또는 Image 구성 요소 프로파일에 대한 값 집합을 정의합니다. 사용자 지정 속성 참조 자료에서 및 항목을 참조하십시오.
- Image 또는 Size 구성 요소 프로파일이 포함된 vSphere 시스템 구성 요소를 포함하는 Blueprint를 생성합니다. [시스템 Blueprint 구성](#) 및 [vSphere 시스템 구성 요소 설정](#) 항목을 참조하십시오.
- Blueprint를 카탈로그에 게시합니다. [Blueprint 게시](#) 항목을 참조하십시오.
- 카탈로그에서 Blueprint를 구성합니다. [서비스 카탈로그 구성을 위한 검사 목록](#) 및 [가상 시스템 정책 유형에 기반한 승인 정책의 예](#) 항목을 참조하십시오.

프로시저

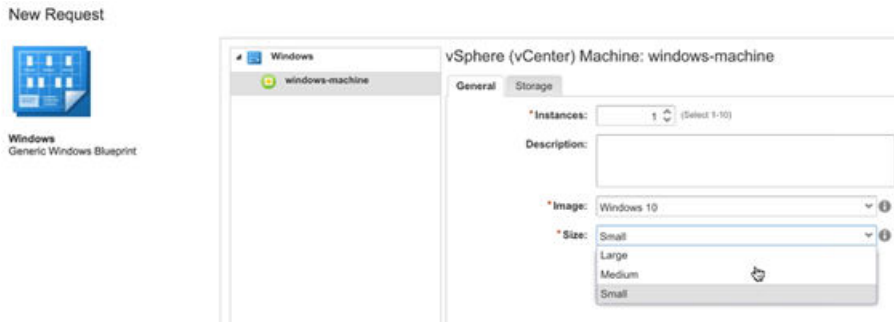
- 1 카탈로그를 클릭합니다.
- 2 요청할 카탈로그 서비스를 선택하고 **요청**을 클릭합니다.



- 3 프로비저닝할 vSphere 시스템 구성 요소를 선택하고 프로비저닝할 인스턴스 수를 지정합니다.
- 4 **이미지** 드롭다운 메뉴에서 이미지 값 집합 옵션을 선택합니다.



5 크기 드롭다운 메뉴에서 크기 값 집합 옵션을 선택합니다.



6 제출을 클릭합니다.

후속 작업

Size 및 Image 구성 요소 프로파일에 대해 정의한 값 집합을 이제 카탈로그 프로비저닝 요청 양식의 카탈로그 탭에 있는 이미지 및 크기 드롭다운 메뉴에서 사용할 수 있습니다.

시나리오: 서비스 카탈로그에서 MySQL이 설치된 CentOS 애플리케이션 Blueprint를 사용할 수 있도록 설정

테넌트 관리자로서, Blueprint 설계자에게 개발 및 품질 엔지니어링 그룹에서 테스트 케이스를 실행할 수 있도록 카탈로그 항목을 생성하여 CentOS MySQL 가상 시스템을 제공해 달라고 요청했습니다. 소프트웨어 설계자가 사용자를 위해 카탈로그 항목이 준비되었음을 알렸습니다. 비즈니스 사용자가 항목을 사용할 수 있도록 Blueprint와 Software 구성 요소를 카탈로그 서비스와 연결한 다음 비즈니스 그룹 구성원에게 카탈로그 항목 요청 권한을 부여해야 합니다.

필수 조건

- 테넌트 관리자 또는 카탈로그 관리자로 vRealize Automation 콘솔에 로그인합니다.
- vSphere CentOS 가상 시스템에서 MySQL을 제공하도록 Blueprint를 게시합니다. Rainpole의 vRealize Automation 설치 및 구성 시나리오의 내용을 참조하십시오.
- 개발 환경에서 Blueprint를 생성하는 경우 Blueprint를 운영 환경으로 가져옵니다. [Blueprint와 콘텐츠 내보내기 및 가져오기](#) 항목을 참조하십시오.
- vSphere 리소스를 개발 및 QE 비즈니스 그룹에 할당하기 위해 예약을 생성합니다. [Hyper-V, KVM, SCVMM, vSphere 또는 XenServer에 대한 예약 생성](#) 항목을 참조하십시오.

프로시저

1 시나리오: 개발 및 품질 엔지니어링 카탈로그 서비스 생성

테넌트 관리자로서, 개발 및 품질 엔지니어링 그룹을 위한 별도의 카탈로그 서비스를 생성하여 재무, 인사와 같은 다른 그룹에서 특수한 카탈로그 항목을 확인하지 못하도록 하려고 합니다. 개발 및 QE 서비스라는 이름의 카탈로그 서비스를 생성하여 테스트 케이스를 실행하기 위한 모든 카탈로그 항목 개발 및 엔지니어링 요구를 게시합니다.

2 시나리오: 개발 및 QE 서비스에 MySQL이 설치된 CentOS 추가

테넌트 관리자로서 개발 및 QE 서비스에 MySQL이 설치된 CentOS 카탈로그 항목을 추가하려고 합니다.

3 시나리오: 사용자에게 개발 및 QE 서비스를 카탈로그 항목으로 요청할 수 있는 권한 부여

테넌트 관리자로서 개발 및 QE 사용 권한을 생성하고 카탈로그 항목과 일부 관련 작업을 추가하여 개발 및 품질 엔지니어링 사용자가 MySQL이 설치된 CentOS 카탈로그 항목을 요청하고 시스템 및 배포에 대해 작업을 실행할 수 있도록 합니다.

시나리오: 개발 및 품질 엔지니어링 카탈로그 서비스 생성

테넌트 관리자로서, 개발 및 품질 엔지니어링 그룹을 위한 별도의 카탈로그 서비스를 생성하여 재무, 인사와 같은 다른 그룹에서 특수한 카탈로그 항목을 확인하지 못하도록 하려고 합니다. 개발 및 QE 서비스라는 이름의 카탈로그 서비스를 생성하여 테스트 케이스를 실행하기 위한 모든 카탈로그 항목 개발 및 엔지니어링 요구를 게시합니다.

프로시저

- 1 **관리 > 카탈로그 관리 > 서비스**를 선택합니다.
- 2 **새로 만들기** 아이콘(+)을 클릭합니다.
- 3 **이름** 텍스트 상자에 **Dev and QE Service**라는 이름을 입력합니다.
- 4 **설명** 텍스트 상자에 **Dev and QE application catalog items for test cases**라는 설명을 입력합니다.
- 5 **상태** 드롭다운 메뉴에서 **활성**을 선택합니다.
- 6 서비스를 생성하는 카탈로그 관리자로서, 검색 옵션을 사용하여 자신의 이름을 소유자로 추가합니다.
- 7 지원 팀 사용자 지정 사용자 그룹을 추가합니다.
예를 들어 IaaS 설계자와 소프트웨어 설계자를 포함하는 사용자 지정 사용자 그룹을 추가하여 카탈로그 항목 프로비저닝에 문제가 발생하는 경우 자신과 서비스 카탈로그 사용자가 문의할 수 있도록 합니다.
- 8 **확인**을 클릭합니다.

개발 및 QE 카탈로그 서비스를 생성하고 활성화했지만 아직 카탈로그 항목이 포함되지는 않았습니다.

시나리오: 개발 및 QE 서비스에 MySQL이 설치된 CentOS 추가

테넌트 관리자로서 개발 및 QE 서비스에 MySQL이 설치된 CentOS 카탈로그 항목을 추가하려고 합니다.

프로시저

- 1 **관리 > 카탈로그 관리 > 서비스**를 선택합니다.
- 2 **서비스** 목록에서 [개발 및 QE 서비스] 행을 선택하고 **카탈로그 항목 관리**를 클릭합니다.

3 새로 만들기 아이콘(+)을 클릭합니다.

4 MySQL이 설치된 CentOS를 선택합니다.

아직 서비스에 연결되지 않은 게시된 Blueprint와 구성 요소만 목록에 나타납니다. Blueprint가 표시되지 않으면 Blueprint가 게시되었는지 또는 다른 서비스에 포함된 것은 아닌지 확인합니다.

5 확인을 클릭합니다.

6 닫기를 클릭합니다.

MySQL이 설치된 CentOS 카탈로그 항목을 개발 및 QE 서비스에 게시했지만 사용자에게 항목 또는 서비스에 대한 사용 권한을 부여할 때까지 누구도 항목을 보거나 요청할 수 없습니다.

시나리오: 사용자에게 개발 및 QE 서비스를 카탈로그 항목으로 요청할 수 있는 권한 부여

테넌트 관리자로서 개발 및 QE 사용 권한을 생성하고 카탈로그 항목과 일부 관련 작업을 추가하여 개발 및 품질 엔지니어링 사용자가 MySQL이 설치된 CentOS 카탈로그 항목을 요청하고 시스템 및 배포에 대해 작업을 실행할 수 있도록 합니다.

이 시나리오에서, 이 서비스에 추가되는 향후 카탈로그 항목에 대한 권한을 사용자에게 부여합니다. 또한 사용자가 프로비저닝된 배포를 관리하도록 허용할 것이므로 전원 켜기 및 끄기, 스냅샷 생성, 배포 제거와 같은 작업을 사용 권한에 추가합니다.

프로시저

1 관리 > 카탈로그 관리 > 사용 권한을 선택합니다.

2 새로 만들기 아이콘(+)을 클릭합니다.

3 세부 정보를 구성합니다.

a 이름 텍스트 상자에 Dev and QE Entitlement라는 이름을 입력합니다.

b 상태 드롭다운 메뉴에서 활성을 선택합니다.

c 비즈니스 그룹 드롭다운 메뉴에서 개발 및 QE 그룹을 선택합니다.

d 사용자 및 그룹 영역에서 하나 이상의 사용자를 추가합니다.

Blueprint가 제대로 작동한다고 확신하는 경우가 아니면 자기 자신만 추가합니다. 제대로 작동한다면 개별 사용자와 사용자 지정 사용자 그룹을 추가할 수 있습니다.

e 다음을 클릭합니다.

4 서비스를 추가합니다.

CentOS 및 MySQL 카탈로그 항목을 개별적으로 추가하는 중이지만 서비스 카탈로그의 비즈니스 그룹 구성원은 나중에 서비스에 추가하는 추가 항목을 사용할 수 있습니다.

- [권한 있는 서비스] 머리글 옆에 있는 **서비스 추가** 아이콘(+)을 클릭합니다.
- 개발 및 QE 서비스**를 선택합니다.
- 확인**을 클릭합니다.

[개발 및 QE 서비스]가 [권한 있는 서비스] 목록에 추가됩니다.

5 작업을 추가합니다.

- [권한 있는 작업] 머리글 옆에 있는 **작업 추가** 아이콘(+)을 클릭합니다.
- 목록을 정렬하려면 [유형] 열 머리글을 클릭합니다.

유형에 따라 다음과 같은 작업을 선택합니다. 이러한 작업은 테스트 케이스 시스템에서 작업하는 개발 및 품질 엔지니어링 사용자에게 유용하며 이 시나리오에서 이러한 비즈니스 그룹 구성원이 사용할 유일한 작업입니다.

유형	작업 이름
시스템	전원 켜기
시스템	전원 끄기
가상 시스템	스냅샷 생성
가상 시스템	스냅샷으로 되돌리기
배포	제거
배포 제거 작업은 가상 시스템뿐만 아니라 전체 배포를 제거합니다.	

- 확인**을 클릭합니다.

5개의 작업이 권한 있는 작업 목록에 추가됩니다.

6 마침을 클릭합니다.

MySQL이 설치된 CentOS 카탈로그 항목을 새 개발 및 QE 카탈로그 서비스에 추가했고 항목을 요청 및 관리할 수 있는 권한을 비즈니스 그룹 구성원에게 부여했습니다.

후속 작업

MySQL이 설치된 CentOS 카탈로그 항목을 프로비저닝하여 작업을 확인한 후에 추가 사용자를 사용 권한에 추가하여 개발 및 품질 엔지니어링 사용자가 공개적으로 카탈로그 항목을 사용하게 할 수 있습니다. 환경의 리소스에 대한 프로비저닝을 추가로 제어하려는 경우 MySQL Software 구성 요소와 소프트웨어 테스트 시스템용 CentOS에 대한 승인 정책을 생성할 수 있습니다. [시나리오: MySQL이 설치된 CentOS 승인 정책 생성 및 적용](#) 항목을 참조하십시오.

배포된 카탈로그 항목 관리

시스템, 로드 밸런서, 네트워크, 기타 배포 리소스를 포함하여 프로비저닝된 배포를 보고 이에 대해 작업을 수행할 수 있습니다.

프로비저닝된 리소스에 대한 작업 실행

프로비저닝된 리소스에 대해 사용 가능한 작업은 리소스 유형, 작업이 프로비저닝된 항목에 대해 구성되고 사용할 수 있게 된 방식, 항목의 작동 상태에 따라 다릅니다.

프로비저닝된 시스템 또는 배포에 대해 사용 가능한 구성된 작업이 **항목** 탭의 선택된 리소스에 대한 **작업** 메뉴에 나타납니다.

항목이 IaaS 시스템 Blueprint를 사용하여 IaaS에 의해 프로비저닝된 경우 사용 가능한 작업의 목록이 Blueprint가 생성되었을 때 시스템 유형 구성 요소에 대해 **작업** 탭에서 선택된 항목 그리고 시스템 유형 또는 상태를 기반으로 적용되는 항목에 의해 결정됩니다.

항목이 XaaS Blueprint를 사용하여 프로비저닝된 경우 항목을 프로비저닝하는 데 사용되는 동일한 서비스에서 리소스 작업을 생성하고 게시하고 사용 권한을 부여해야 합니다. 사용 가능한 작업의 목록은 항목 유형과 항목의 현재 상태에 의해 결정됩니다.

작업이 항목에 매핑된 경우 IaaS 시스템으로 프로비저닝된 항목에 대해 사용 가능한 작업에는 XaaS 리소스 작업도 포함될 수 있습니다.

프로비저닝된 리소스에 대한 작업 메뉴 명령

작업은 프로비저닝된 리소스에 대해 수행할 수 있는 변경입니다. vRealize Automation 작업은 리소스의 수명 주기를 관리하는 데 사용됩니다.

프로비저닝된 리소스에 대한 **작업** 메뉴의 명령에는 Blueprint에서 지정된 작업이 포함되어 있으며 서비스 설계자가 생성한 사용자 지정 메뉴 작업이 포함되어 있을 수 있습니다. 사용 가능한 작업은 비즈니스 그룹 관리자 또는 테넌트 관리자가 작업이 실행되는 리소스가 포함된 사용 권한을 구성한 방식에 따라 다릅니다.

vRealize Automation에서 관리하는 NSX 개체를 vRealize Automation 외부에서 관리해서는 안 됩니다. 예를 들어 vRealize Automation이 아니라 NSX에서 배포된 NSX 로드 밸런서의 구성원 포트를 수정하는 경우 NSX 데이터 수집은 배포된 시스템과 다른 방법으로 연결된 해당 로드 밸런서 구성원 풀 간의 연결을 끊습니다. 배포된 로드 밸런서 구성원 포트가 vRealize Automation 외부에서 변경되는 경우 축소 및 확장 작업도 예기치 않은 결과를 가져옵니다.

표 3-75. 작업 메뉴 명령

작업	리소스 유형	설명
부동 소수점 IP 연결	시스템 (OpenStack)	부동 소수점 IP 주소를 OpenStack 시스템과 연결합니다.
재구성 취소	시스템	실행 중인 재구성 작업을 취소합니다.

표 3-75. 작업 메뉴 명령 (계속)

작업	리소스 유형	설명
리스 변경	배포 및 시스템	배포에 포함된 모든 리소스 또는 특정 시스템에 대한 리스에서 남은 일수를 변경합니다. 값을 제공하지 않는 경우 리스가 만료되지 않습니다.
소유자 변경	배포	배포 및 포함된 모든 리소스의 소유자를 변경합니다. 비즈니스 그룹 관리자 및 지원 사용자만 배포의 소유권을 변경할 수 있습니다. 소유자 변경 작업을 시작할 때 시스템은 [켜짐], [꺼짐] 또는 [활성] 상태여야 합니다. 그렇지 않으면 작업이 실패하고 다음 메시지가 표시됩니다. 시스템에 대한 작업이 잘못되었습니다.
VMRC를 사용하여 연결	시스템	VMRC 8.x 애플리케이션을 사용하여 가상 시스템에 연결합니다. 이 작업을 사용하려면 해당 작업을 실행 중인 서비스 카탈로그 사용자의 로컬 시스템에 VMRC 애플리케이션을 설치해야 합니다. 설치 및 사용자 지침은 VMware Remote Console 설명서 를 참조하십시오. 다운로드하려면 VMware Remote Console 다운로드 를 참조하십시오. VMRC 8.x는 이전 VMware Remote Console을 대체합니다.
원격 콘솔에 연결	시스템	VMware Remote Console을 사용하여 선택된 시스템에 연결합니다. 가상 시스템 콘솔이 브라우저에 표시됩니다. VMRC 8.x는 VMware Remote Console을 대체합니다.
콘솔 티켓을 사용하여 연결	시스템 (OpenStack 및 KVM)	VMware Remote Console 연결에 대한 콘솔 티켓을 사용하여 OpenStack 또는 KVM 가상 시스템에 연결합니다.
ICA를 사용하여 연결	시스템 (Citrix)	Independent Computing Architecture를 사용하여 Citrix 시스템에 연결합니다.
RDP를 사용하여 연결	시스템	Microsoft Remote Desktop Protocol을 사용하여 시스템에 연결합니다.

표 3-75. 작업 메뉴 명령 (계속)

작업	리소스 유형	설명
SSH를 사용하여 연결	시스템	<p>SSH를 사용하여 선택된 시스템에 연결합니다.</p> <p>SSH를 사용하여 연결 옵션을 사용하려면 브라우저에 Mozilla Firefox 및 Google Chrome을 위한 FireSSH SSH 터미널 클라이언트 등 SSH를 지원하는 플러그인이 있어야 합니다. 해당 플러그인이 있는 경우, SSH를 사용하여 연결을 선택하면 SSH 콘솔이 표시되고 관리자 자격 증명을 묻는 메시지가 나타납니다.</p> <p>이 작업을 사용하려면 Machine.SSH 사용자 지정 속성이 포함되어야 하며 속성 그룹 또는 개별 사용자 지정 속성의 Blueprint의 시스템 구성 요소에서 True로 설정되어야 합니다.</p>
가상 데스크톱을 사용하여 연결	시스템	Microsoft 가상 데스크톱을 사용하여 선택된 시스템에 연결합니다.
스냅샷 생성	가상 시스템	가상 시스템의 스냅샷을 생성합니다. 2개의 스냅샷만 허용되고 이미 이를 가진 경우 스냅샷을 삭제할 때까지 이 명령을 사용할 수 없습니다.
스냅샷 삭제	가상 시스템	가상 시스템의 스냅샷을 삭제합니다.

표 3-75. 작업 메뉴 명령 (계속)

작업	리소스 유형	설명
제거	클라우드 시스템, 배포, 가상 시스템 및 NSX Edge	<p>프로비저닝된 리소스를 즉시 제거합니다. 제거 중인 배포의 일부이더라도 XaaS 리소스를 제거하려면 이 작업을 실행해야 합니다. 해당 리스 또는 아카이브 기간이 종료될 때 다른 리소스가 제거됩니다.</p> <p>XaaS를 제외하고 배포의 구성 요소를 제거하는 것은 모범 사례가 아닙니다. 축소 작업을 사용하여 배포의 시스템 수를 줄이거나 전체 배포를 제거하십시오.</p> <p>제거 작업은 다음 배포 상황에서 사용할 수 없습니다.</p> <ul style="list-style-type: none"> ■ 물리적 시스템 배포 ■ NSX 기존 네트워크 또는 NSX 기존 보안 리소스가 포함된 배포 ■ NSX 요청 시 로드 밸런서 리소스가 포함된 배포 <p>NSX 로드 밸런서가 요청 시 NSX Edge의 속성이므로 NSX Edge가 제거되면 로드 밸런서 리소스도 제거되며 리소스가 해제됩니다. 로드 밸런싱된 시스템 계층이 제거되면 해당 NSX Edge의 로드 밸런서 풀에서도 제거됩니다.</p> <p>비즈니스 그룹 관리자는 배포 요청이 실패한 후 배포를 강제 제거하도록 선택할 수 있습니다. 강제 제거는 배포를 제거하는 동안 vRealize Automation이 개별 리소스 제거 실패를 무시하도록</p>

표 3-75. 작업 메뉴 명령 (계속)

작업	리소스 유형	설명
		<p>지정합니다. 강제 제거 사용에 대한 자세한 내용은 실패한 제거 요청 후 배포 강제 제거를 참조하십시오.</p> <p>참고 예약에 의해 프로비저닝된 시스템에 할당된 스토리지와 메모리는 해당 시스템이 vRealize Automation에서 [제거] 작업에 의해 삭제될 때 해제됩니다. 시스템이 vCenter Server에서 삭제되는 경우에는 스토리지와 메모리가 해제되지 않습니다.</p> <p>Amazon 시스템 구성 요소가 포함된 배포를 제거 중인 경우, 수명 주기 동안 시스템에 추가된 모든 EBS 볼륨이 제거되지 않고 대신 분리됩니다. vRealize Automation은 EBS 볼륨 제거에 대한 옵션을 제공하지 않습니다.</p>
기존 네트워크 제거	기존 네트워크	네트워크를 제거합니다.
VMware NSX 로드 밸런서 제거	VMware NSX 로드 밸런서	NSX 로드 밸런서를 제거합니다.
VMware NSX 네트워크 제거	VMware NSX 네트워크	NSX 네트워크를 제거합니다.
VMware NSX 보안 그룹 제거	VMware NSX 보안 그룹	NSX 보안 그룹을 제거합니다.
VMware NSX 보안 태그 제거	VMware NSX 보안 태그	NSX 보안 태그를 제거합니다.
부동 소수점 IP 연결 끊기	시스템 (OpenStack)	OpenStack 시스템에서 부동 소수점 IP를 제거합니다.
재구성 실행	시스템	스케줄링된 재구성을 재정의하거나 실패한 재구성을 다시 실행하거나 다시 스케줄링합니다.
만료	배포 및 시스템	배포에 포함된 모든 리소스에 대한 배포 또는 시스템 리스를 종료합니다.
인증서 내보내기	시스템	클라우드 시스템에서 인증서를 내보냅니다.
만료 미리 알림 받기	시스템	현재 리스 만료 날짜에 대한 일정 이벤트 파일을 다운로드합니다.
VMware Tools 설치	시스템	vSphere 가상 시스템에 VMware Tools를 설치합니다.
전원 주기	시스템	시스템 전원을 켜다가 다시 끕니다.

표 3-75. 작업 메뉴 명령 (계속)

작업	리소스 유형	설명
전원 끄기	시스템	게스트 운영 체제를 종료하지 않고 시스템 전원을 끕니다.
전원 켜기	시스템	시스템 전원을 켭니다. 시스템이 일시 중단된 경우, 시스템이 일시 중단된 지점에서 정상 작동이 재개됩니다.
재부팅	시스템	vSphere 가상 시스템에서 게스트 운영 체제를 재부팅합니다. 이 작업을 사용할 시스템에 VMware Tools를 설치해야 합니다.
재구성	시스템	<p>비즈니스 그룹 관리자, 지원 사용자 또는 시스템 소유자는 선택된 vSphere 시스템에 대해 다음과 같은 재구성 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 설명 변경 ■ CPU, 메모리, 네트워크 및 디스크 설정 변경 ■ 사용자 지정 속성 및 속성 그룹 추가, 편집 및 삭제 ■ 보안 태그 및 보안 그룹 추가, 편집 또는 삭제 ■ NAT 포트 포워딩 규칙 추가, 편집, 순서 다시 지정 또는 삭제 ■ 종료 재구성 ■ 시스템 소유자 변경(비즈니스 그룹 관리자 및 지원 사용자에게 대해서만 가능) <p>스토리지 예약 정책을 변경할 수 없습니다. 변경할 경우 디스크의 스토리지 프로파일이 변경됩니다.</p>
재구성	로드 밸런서	<p>권한 있는 시스템 소유자, 지원 사용자, 테넌트 관리자 또는 비즈니스 그룹 관리자는 가상 서버의 설정을 변경할 수 있고 NSX 로드 밸런서에서 가상 서버를 추가 또는 제거할 수 있습니다.</p> <p>로드 밸런서의 가상 서버 설정에 대한 자세한 내용은 요청 시 로드 밸런서 구성 요소 추가를 참고하십시오.</p>
VDI 등록	가상 시스템(XenServer)	XenServer 항목에 가상 디스크 이미지를 등록합니다.

표 3-75. 작업 메뉴 명령 (계속)

작업	리소스 유형	설명
재프로비저닝	시스템	<p>시스템을 제거한 다음 프로비저닝 워크플로를 시작하여 동일한 이름의 시스템을 생성합니다.</p> <p>시스템을 재프로비저닝하도록 요청하면 알려진 문제로 인해 vRealize Automation이 실제 상태가 [진행 중]일 때 재프로비저닝 상태를 카탈로그에 [완료]로 표시합니다. 시스템 재프로비저닝 요청을 제출한 후 다음 시퀀스 중 하나를 사용하여 재프로비저닝된 시스템의 상태를 확인할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 인프라 > 관리되는 시스템 ■ 항목 > 항목 세부 정보 ■ 관리 > 이벤트 > 이벤트 로그 <p>참고 Amazon 시스템은 재프로비저닝할 수 없습니다.</p> <p>관련 정보는 http://kb.vmware.com/kb/2065873의 VMware 기술 자료 문서 재프로비저닝된 시스템 작업...(2065873)을 참조하십시오.</p>
스냅샷 되돌리기	가상 시스템	<p>시스템의 이전 스냅샷으로 되돌립니다. 이 작업을 사용하려면 기존 스냅샷이 있어야 합니다.</p>

표 3-75. 작업 메뉴 명령 (계속)

작업	리소스 유형	설명
축소	배포	<p>줄어드는 용량 요구 사항에 맞게 조정하기 위해 배포에서 시스템의 불필요한 인스턴스를 제거합니다. 해당 시스템에 설치된 시스템 구성 요소 및 소프트웨어 구성 요소가 제거됩니다. 종속 소프트웨어 구성 요소 및 네트워킹 및 보안 구성 요소가 새 배포 구성에 대해 업데이트됩니다. XaaS 구성 요소는 확장/축소할 수 없고 확장/축소 작업 중 업데이트되지 않습니다.</p> <p>배포 확장/축소를 다시 시도하여 부분적으로 성공한 확장/축소 작업을 복구해 볼 수 있습니다. 하지만 배포를 현재 크기로 확장/축소할 수는 없으며 부분적으로 성공한 확장/축소를 이러한 방식으로 수정하면 현수 리소스가 할당 해제되지 않습니다. 요청 실행 세부 정보 화면을 보고 실패한 작업과 해당 작업이 위치한 노드를 확인하여 부분적으로 성공한 확장/축소를 다른 확장/축소 작업으로 수정할지 여부를 결정할 수 있습니다. 실패한 그리고 부분적으로 성공한 확장/축소 작업은 원래 배포의 기능에 영향을 주지 않으며 문제를 해결하는 동안 계속해서 카탈로그 항목을 사용할 수 있습니다.</p>

표 3-75. 작업 메뉴 명령 (계속)

작업	리소스 유형	설명
확장	배포	<p>확장하는 용량 요구 사항에 맞게 조정하기 위해 배포에서 시스템의 추가 인스턴스를 프로비저닝합니다. 해당 시스템에 설치된 시스템 구성 요소 및 소프트웨어 구성 요소가 프로비저닝됩니다. 종속 소프트웨어 구성 요소 및 네트워킹 및 보안 구성 요소가 새 배포 구성에 대해 업데이트됩니다. XaaS 구성 요소는 확장/축소할 수 없고 확장/축소 작업 중 업데이트되지 않습니다.</p> <p>배포 확장/축소를 다시 시도하여 부분적으로 성공한 확장/축소 작업을 복구해 볼 수 있습니다. 하지만 배포를 현재 크기로 확장/축소할 수는 없으며 부분적으로 성공한 확장/축소를 이러한 방식으로 수정하면 현수 리소스가 할당 해제되지 않습니다. 요청 실행 세부 정보 화면을 보고 실패한 작업과 해당 작업이 위치한 노드를 확인하여 부분적으로 성공한 확장/축소를 다른 확장/축소 작업으로 수정할지 여부를 결정할 수 있습니다. 실패한 그리고 부분적으로 성공한 확장/축소 작업은 원래 배포의 기능에 영향을 주지 않으며 문제를 해결하는 동안 계속해서 카탈로그 항목을 사용할 수 있습니다.</p>
종료	시스템	게스트 운영 체제를 종료한 후 시스템 전원을 끕니다. 이 작업을 사용할 시스템에 VMware Tools를 설치해야 합니다.
일시 중단	시스템	시스템을 사용할 수 없고 시스템에서 사용 중인 스토리지 이외의 다른 시스템 리소스를 사용하지 않도록 시스템을 일시 중지합니다.
등록 취소	시스템	인벤토리에서 시스템을 제거합니다. 등록 취소된 시스템은 사용할 수 없습니다.
VDI 등록 취소	가상 시스템(XenServer)	XenServer 항목에 가상 디스크 이미지를 등록 취소합니다.

메트릭 제공자 구성

vSphere 가상 시스템에 대해 vRealize Operations Manager 상태 및 리소스 메트릭을 사용하도록 vRealize Automation을 구성할 수 있습니다.

vRealize Operations Manager 상태 배지 및 메트릭에 대한 자세한 내용은 vRealize Operations Manager 설명서를 참조하십시오.

필수 조건

- **테넌트 관리자, 비즈니스 그룹 관리자 또는 시스템 소유자**로 vRealize Automation 콘솔에 로그인합니다.
- vRealize Automation과 통합하는 모든 vSphere 서버에 대해 보기 권한 및 리소스 메트릭 쿼리 권한을 가진 vRealize Operations Manager 사용자 계정을 생성합니다.
- vRealize Automation에서 끝점으로 추가하는 모든 vSphere 서버에 대해 vRealize Operations Manager 어댑터 인스턴스를 생성합니다. 어댑터 인스턴스 생성에 대한 자세한 내용은 vRealize Operations Manager 설명서를 참조하십시오.

프로시저

- 1 **관리 > 회수 > 메트릭 제공자**를 선택합니다.
- 2 메트릭 제공자를 선택합니다.

옵션	설명
(기본값) vRealize Automation 메트릭 제공자	vRealize Operations Manager 인스턴스가 없는 경우 vRealize Automation에서 기본 시스템 메트릭을 제공합니다.
vRealize Operations Manager 끝점	vSphere 가상 시스템에 대해 메트릭 제공자로 사용하려는 vRealize Operations Manager 인스턴스에 대한 연결 정보를 제공합니다.

- 3 **연결 테스트**를 클릭합니다.
- 4 **저장**을 클릭합니다.

시스템이 있는 그룹의 비즈니스 그룹 관리자, 테넌트 관리자, 시스템 소유자는 vSphere 가상 시스템의 항목 세부 정보 페이지에서 상태 배지와 상태 경고를 볼 수 있습니다. 회수 페이지에서 플랫폼 유형 vSphere를 기준으로 필터링하여 vRealize Operations Manager 메트릭과 상태 배지를 볼 수도 있습니다.

후속 작업

[회수 요청 보내기](#).

회수 요청 보내기

배포를 보고 관리하는 것은 물론, 배포 소유자에게 회수 요청을 보낼 수도 있습니다. 회수 요청에는 세 리스 기간(일), 배포 포소유자에게 제공되는 응답 기한 및 회수 대상 시스템이 지정됩니다.

필수 조건

- **테넌트 관리자**로 vRealize Automation 콘솔에 로그인합니다.
- (선택 사항) 상태 배지를 보거나 vRealize Operations Manager가 제공하는 메트릭을 보려면 [메트릭 제공자 구성](#) 항목을 참조하십시오.

프로시저

- 1 **관리 > 회수 > 배포**를 선택합니다.

2 검색 기준과 일치하는 가상 시스템 배포를 찾습니다.

vRealize Operations Manager가 제공하는 메트릭을 보려면 vSphere 플랫폼 유형을 선택해야 합니다.

- a **고급 검색** 아래쪽 화살표를 클릭하여 검색 상자를 엽니다.
- b 검색 값을 하나 이상 입력하거나 선택합니다.

옵션	작업
가상 시스템 이름 포함 항목	텍스트 상자에 일치하는 가상 시스템 이름을 찾기 위한 문자를 하나 이상 입력합니다.
소유자 이름 포함 항목	텍스트 상자에 일치하는 소유자 이름을 찾기 위한 이름을 입력합니다.
비즈니스 그룹 이름 포함 항목	텍스트 상자에 일치하는 비즈니스 그룹 이름을 찾기 위한 이름을 입력합니다.
플랫폼 유형	드롭다운 메뉴에서 플랫폼 유형을 선택합니다. vRealize Operations Manager가 제공하는 메트릭을 보려면 vSphere를 선택합니다. vRealize Operations Manager에 필요합니다.
전원 상태	드롭다운 메뉴에서 전원 상태가 일치하는 가상 시스템을 찾기 위한 전원 상태 값을 선택합니다.
만료 날짜 범위	일정 아이콘을 클릭하고 범위 내에서 만료 날짜를 찾기 위한 시작 날짜와 종료 날짜를 선택합니다.
CPU 사용량	드롭다운 메뉴에서 높은 CPU 활용도(80% 초과), 낮은 CPU 활용도(5% 미만) 또는 없음(값 없음)을 나타내는 가상 시스템을 찾기 위한 값을 선택합니다. vRealize Operations Manager 메트릭을 질의하는 경우에는 질의에 이 필터를 사용할 수 없으며, CPU 사용량을 기준으로 결과를 정렬할 수 없습니다.
메모리 사용량	드롭다운 메뉴에서 높은 메모리 활용도(80% 초과), 낮은 메모리 활용도(10% 미만) 또는 없음(값 없음)을 나타내는 가상 시스템을 찾기 위한 값을 선택합니다. vRealize Operations Manager 메트릭을 질의하는 경우에는 질의에 이 필터를 사용할 수 없으며, 메모리 사용량을 기준으로 결과를 정렬할 수 없습니다.
디스크 사용	드롭다운 메뉴에서 낮은 하드 디스크 활용도(2KB/초 미만) 또는 없음(값 없음)을 나타내는 가상 시스템을 찾기 위한 값을 선택합니다. vRealize Operations Manager 메트릭을 질의하는 경우에는 질의에 이 필터를 사용할 수 없으며, 디스크 사용량을 기준으로 결과를 정렬할 수 없습니다.

옵션	작업
네트워크 사용	드롭다운 메뉴에서 낮은 네트워크 활용도(1KB/초 미만) 또는 없음(값 없음)을 나타내는 가상 시스템을 찾기 위한 값을 선택합니다. vRealize Operations Manager 메트릭을 질의하는 경우에는 질의에 이 필터를 사용할 수 없으며, 네트워크 사용량을 기준으로 결과를 정렬할 수 없습니다.
복합 메트릭	드롭다운 메뉴에서 복합 메트릭에 기반하여 가상 시스템을 찾기 위한 값을 선택합니다. 예를 들어 CPU, 네트워크, 메모리 및 디스크 사용량 값이 모두 20% 미만인 시스템을 찾으려면 [유휴]를 선택합니다. vRealize Operations Manager 메트릭을 질의하는 경우에는 이 필터를 사용할 수 없습니다.

C 검색 아이콘()을 클릭합니다.

- [배포] 페이지에서 해당 상위 배포를 회수하려는 시스템을 하나 이상 선택합니다.

현재 결과 페이지에 표시되어 선택된 시스템만 회수됩니다.

- 회수를 클릭합니다.

현재 페이지에서 선택한 가상 시스템으로 구성된 배포가 요청에 포함됩니다.

참고 [배포 회수] 페이지에는 회수할 수 없는 시스템(예: 리스가 만료된 시스템)이 나열될 수 있습니다. 회수할 수 없는 시스템을 지정하면 다음과 같은 오류를 수신하게 됩니다.

Selection Error: Virtual machine *name* is not in valid state for reclamation.

- 새 리스 기간(일) 텍스트 상자에 새 리스의 기간을 입력합니다.

최소 기간은 1일이며 최대 기간은 365일입니다. 기본값은 7일입니다.

- 리스 적용 전 대기 기간(일) 텍스트 상자에 리스가 강제 적용되기 전 배포 소유자가 회수 요청에 응답할 수 있는 시간(일)을 입력합니다.

이 시간이 끝나면 새 리스 기간을 사용하는 새 리스가 배포에 적용됩니다. 최소 대기 기간은 1일이며 최대 기간은 365일입니다. 기본값은 3일입니다.

- 요청한 이유 텍스트 상자에 요청의 이유를 입력합니다.

- 제출을 클릭합니다.

- 확인을 클릭합니다.

회수 요청을 보내면 배포 소유자의 [받은 편지함]에 나타납니다. 요청한 일 수 이내에 소유자가 응답하지 않으면 지정한 기간의 새 리스가 배포에 적용됩니다(현재 리스가 더 짧은 경우 제외). 소유자가 회수 요청에서 **사용 중인 항목**을 클릭하면 배포의 리스가 변경되지 않고 유지됩니다. 소유자가 **회수를 위해 해제**를 클릭하면 배포 리스가 즉시 만료됩니다.

후속 작업

[회수 요청 추적](#).

회수 요청 추적

회수 요청의 현재 상태 및 기타 세부 정보를 추적할 수 있습니다.

다음은 최근 회수 요청을 확인하는 데 사용할 수 있는 대체 방법입니다.

- **받은 편지함** 탭을 클릭하고 **회수 요청**을 선택하여 회수 요청 정보를 봅니다.
- **회수 요청** 탭을 클릭하고 최근 요청 목록을 봅니다.
- **항목** 탭을 클릭하고 **배포**를 클릭하여 최근 배포 변경 내용을 봅니다.


필수 조건

테넌트 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 **관리 > 회수 > 회수 요청**을 선택합니다.
- 2 검색 조건에 일치하는 가상 시스템을 찾습니다.
 - a **고급 검색** 아래쪽 화살표를 클릭하여 검색 상자를 엽니다.
 - b 하나 이상의 검색 값을 입력하거나 선택합니다.

옵션	작업
가상 시스템 이름 포함 항목	텍스트 상자에 하나 이상의 문자를 입력하여 이에 일치하는 가상 시스템 이름을 찾습니다.
소유자 이름 포함 항목	텍스트 상자에 하나 이상의 문자를 입력하여 이에 일치하는 소유자 이름을 찾습니다.
요청 이유 포함 항목	텍스트 상자에 하나 이상의 문자를 입력하여 이에 일치하는 요청 이유를 찾습니다.
요청 상태	드롭다운 메뉴에서 요청 상태 값을 선택하여 요청 상태가 이 값에 일치하는 가상 시스템을 찾습니다.

- c **검색** 아이콘()을 클릭하거나 Enter를 눌러 검색을 시작합니다.
 - d **고급 검색** 위쪽 화살표를 클릭하여 검색 상자를 닫습니다.
- 3 (선택 사항) **데이터 새로 고침**을 클릭하여 회수 요청의 표시를 업데이트합니다.

관리되는 시스템의 예약 변경

관리되는 시스템에 대한 예약 또는 스토리지 설정을 변경할 수 있습니다. 이 기능은 시스템이 현재 예약에서 사용할 수 없는 새 스토리지 경로로 이동하는 경우 유용합니다. 단일 시스템 배포의 경우, 시스템에 대한 비즈니스 그룹을 변경할 수도 있습니다.

시스템 소유자가 대상 비즈니스 그룹의 구성원인 경우에는 단일 시스템 배포의 시스템을 다른 비즈니스 그룹으로 이동할 수 있습니다. 원래 및 대상 비즈니스 그룹의 비즈니스 그룹 관리자여야 비즈니스 그룹 설정을 변경할 수 있습니다.

참고 시스템에 할당된 예약 정책이 있는 경우에는 비즈니스 그룹을 변경할 수 없습니다.

관리 > 계산 리소스 메뉴 옵션을 사용하여 연결된 계산 리소스에 대한 추가 예약을 생성할 수 있습니다.

예약에 의해 프로비저닝된 시스템에 할당된 스토리지와 메모리는 해당 시스템이 vRealize Automation에서 [제거] 작업에 의해 삭제될 때 해제됩니다. 시스템이 vCenter Server에서 삭제되는 경우에는 스토리지와 메모리가 해제되지 않습니다.

예를 들어 기존 배포에 포함된 시스템과 연결되어 있는 예약은 삭제할 수 없습니다. vCenter Server에서 배포된 시스템을 수동으로 이동하거나 삭제할 경우, vRealize Automation에서는 배포된 시스템을 라이브 상태로 계속 인식하기 때문에 연결된 예약을 삭제하지 못합니다.

예약을 변경할 시 vCenter Server의 시스템이 vRealize Automation의 해당 시스템 예약의 일부가 아닌 새로운 스토리지 경로로 이동되는 경우, 시스템의 예약을 변경하기 전에 대상 또는 새로운 스토리지 경로가 시스템의 대상 예약에서 선택되었는지 확인합니다.

필수 조건

패브릭 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

1 **인프라 > 관리되는 시스템**을 선택합니다.

2 변경할 예약이 있는 시스템을 찾습니다.

3 드롭다운 메뉴에서 **예약 변경**을 클릭합니다.

드롭다운 메뉴에서 **보기**를 클릭하여 연결된 Blueprint 및 계산 리소스와 같은 관리되는 시스템에 대한 정보를 볼 수 있습니다.

4 (선택 사항) **비즈니스 그룹** 드롭다운 메뉴에서 비즈니스 그룹을 선택합니다.

5 (선택 사항) **예약** 드롭다운 메뉴에서 예약을 선택합니다.

6 (선택 사항) **스토리지** 드롭다운 메뉴에서 스토리지 정책을 선택합니다.

7 **확인**을 클릭합니다.

시스템의 스냅샷 생성

관리자가 환경을 어떻게 구성했는지에 따라 가상 시스템의 스냅샷을 생성할 수 있습니다. 스냅샷이란 특정 시간의 가상 시스템 이미지입니다. 이것은 원래 VM 이미지의 공간 효율적인 복사본입니다. 스냅샷을 사용하면 시스템 손상, 데이터 손실 또는 보안 위협으로부터 시스템을 쉽게 복구할 수 있습니다. 가상 시스템의 스냅샷을 생성했다면 나중에 이 스냅샷을 적용하여 스냅샷이 생성되었을 때의 지점으로 시스템을 다시 재설정할 수 있습니다.

메모리 스냅샷을 생성할 때 스냅샷은 가상 시스템 전원 설정의 상태와 선택적으로 가상 시스템 메모리의 상태를 캡처합니다. 가상 시스템의 메모리 상태를 캡처할 경우 스냅샷 작업을 완료하는 데 더 오랜 시간이 소요됩니다. 네트워크를 통해 응답할 때 약간의 시간이 걸릴 수도 있습니다.

필수 조건

- 전원이 켜져 있거나, 꺼져 있거나, 일시 중단된 기존의 가상 시스템.
- 가상 시스템이 하나 이상의 독립 디스크에 대해 구성되어 있는 경우 스냅샷을 생성하기 전에 시스템을 끄십시오. 전원이 켜져 있을 때에는 스냅샷을 생성할 수 없습니다. 디스크 구성 정보는 사용자 지정 속성 V 테이블을 참조하십시오.
- 테넌트 관리자 또는 비즈니스 그룹 관리자가 스냅샷 작업에 대한 사용 권한을 부여했습니다.

프로시저

- 1 항목 > 시스템을 선택합니다.
또는 항목 > 배포를 선택하고 배포의 시스템으로 이동할 수 있습니다.
- 2 스냅샷을 생성할 시스템을 찾습니다.
- 3 작업 열에서 아래쪽 화살표를 클릭하고 **자세히 보기**를 클릭합니다.
- 4 [작업] 메뉴에서 **스냅샷 생성**을 클릭합니다.
- 5 이름을 입력하고 원하는 경우 설명을 입력합니다.
- 6 시스템의 메모리 및 전원 설정을 캡처하려면 **메모리 포함**을 선택합니다.
- 7 **제출**을 클릭합니다.

시스템에 원격으로 연결

vRealize Automation 콘솔에서 원격으로 시스템에 연결할 수 있습니다.

필수 조건

- 시스템 소유자, 테넌트 관리자 또는 비즈니스 그룹 관리자로 vRealize Automation 콘솔에 로그인합니다.
- VMware Tools가 설치되어 있는지 확인합니다.
VMware Remote Console과 연결할 때 완전히 작동하는 액세스를 지원하려면 vRealize Automation 클라이언트에 VMware Tools를 설치해야 합니다. VMware Tools가 설치되지 않은 경우에는 대상 시스템 연결 후 마우스 포인터와 마우스 키가 작동하지 않는 등의 문제가 발생합니다. 지원되는 VMware Tools 버전에 대한 자세한 내용은 vRealize Automation 지원 매트릭스 항목을 참조하십시오.
- 프로비저닝된 시스템의 전원이 켜져 있는지 확인합니다.

프로시저

- 1 항목 > 배포를 선택합니다.

- 2 시스템 이름 행에서 **작업**을 클릭하거나 시스템을 선택하고 해당 시스템 페이지에서 **작업**을 클릭합니다.
- 3 원격 연결 방법을 선택합니다.
 - RDP를 사용하여 연결하려면 **RDP를 사용하여 연결**을 선택합니다.
 - VMware Remote Console을 사용하여 연결하려면 **원격 콘솔에 연결**을 선택합니다. 프롬프트에 응답합니다.
- 4 지시에 따라 **연결**을 클릭하고 시스템에 로그인합니다.
- 5 완료되었으면 로그아웃하고 브라우저 창을 닫습니다.

신뢰할 수 없는 인증서를 사용하는 vSphere 에 대한 원격 콘솔 구성

vRealize Automation 배포에서 신뢰할 수 없는 인증서를 사용하는 경우

VMware Remote Console과 함께 원격 콘솔을 사용하려면 인증서를 신뢰하도록 클라이언트 브라우저를 구성해야 합니다. 이를 위한 단계는 브라우저별로 다릅니다.

환경에서 신뢰할 수 있는 SSL 인증서를 사용하여 vRealize Automation을 구성한 경우에는 클라이언트 브라우저에서 VMware Remote Console을 위한 추가 구성이 필요하지 않습니다.

vRealize Automation 장치 인증서가 교체되고 신뢰할 수 있는 인증서인 경우에는 웹 브라우저 클라이언트에 대해 인증서 정보를 업데이트할 필요가 없습니다.

인증서를 교체하려는 경우에는 vRealize Automation에 대한 시스템 관리 가이드에서 vRealize Automation 장치 인증서 교체에 관한 항목을 참조하십시오.

vSphere에 프로비저닝된 시스템에 대해 VMware Remote Console을 사용하는 원격 연결은 프록시 콘솔을 통해 vRealize Automation 장치 인증서가 보호합니다. VMware Remote Console을 사용하려면 브라우저에서 WebSocket을 지원해야 하며 브라우저가 vRealize Automation 장치 인증서를 신뢰해야 합니다. <https://vra-va.eng.mycompany.com/> 형식의 주소에서 루트 수준 가상 장치로 이동하여 인증서를 가져올 수 있습니다.

브라우저 및 vSphere의 지원 요구 사항에 대한 자세한 내용은 vRealize Automation 지원 매트릭스의 내용을 참조하십시오.

vRealize Automation 의 인증서를 신뢰하도록 Firefox 구성

vSphere에서 프로비저닝된 클라이언트의 VMware Remote Console을 지원하려면 신뢰할 수 없는 vRealize Automation 장치 인증서를 클라이언트 브라우저에 수동으로 가져와야 합니다.

지원되는 Firefox 버전에 대한 자세한 내용은 vRealize Automation [정보 센터](#)에서 VMware vRealize 지원 매트릭스를 참조하십시오.

참고 환경에서 신뢰할 수 있는 SSL 인증서를 사용하여 vRealize Automation을 구성한 경우에는 클라이언트 브라우저에서 VMware Remote Console을 위한 추가 구성이 필요하지 않습니다.

프로시저

- 1 Firefox 브라우저에서 vRealize Automation 장치에 로그인합니다.
인증서를 신뢰할 수 없다는 메시지가 나타납니다.

- 2 현재 연결 정보를 표시하려면 옵션을 선택합니다. **인증서 보기(View Certificate)**를 클릭하여 현재 SSL 인증서를 표시하고 [인증서 뷰어](Certificate Viewer)에서 **세부 정보(Detail)**를 클릭합니다.
- 3 **추가 정보(More Information)**를 클릭하고 [페이지 정보](Page Info) 페이지에서 **보안(Security)** 탭을 클릭합니다.
- 4 [인증서 계층](Certificate Hierarchy) 창에서 인증서를 선택합니다.

옵션	작업
인증 기관에서 발급한 인증서 (Certificate Authority issued certificates)	최상위 vRealize Automation 인증서를 선택합니다.
자체 서명된 인증서(Self-signed certificates)	vRealize Automation 인증서를 선택합니다.

- 5 **내보내기(Export)**를 클릭합니다.
- 6 [파일로 인증서 저장] 텍스트 상자에 인증서 정보를 구성합니다.
 - a **다른 이름으로 저장(Save As)** 텍스트 상자에 인증서 이름을 입력합니다. 인증서 이름은 .crt, .cert 또는 .cer로 끝나야 합니다.
 - b 파일을 저장할 위치를 선택합니다.
 - c 형식으로 **X.509 인증서(PEM)(X.509 Certificate (PEM))**를 선택합니다.
- 7 **저장**을 클릭합니다.
- 8 [인증서 관리] 텍스트 상자에서 **권한** 탭을 클릭합니다.

옵션	작업
Windows	Firefox 메뉴에서 기본 설정(Preference) > 고급(Advanced) > 인증서(Certificates) 를 선택합니다.
iOS	Firefox 메뉴에서 기본 설정(Preference) > 고급(Advanced) > 인증서(Certificates) 를 선택하고 인증서 보기(View Certificates) 를 클릭합니다.

- 9 **권한(Authorities)** 탭을 클릭하고 **가져오기(Import)**를 클릭합니다.
- 10 앞에서 저장한 인증서 파일을 선택하고 텍스트 상자에서 **열기**를 클릭합니다.
- 11 신뢰 설정을 편집합니다.

옵션	작업
자체 서명된 인증서(Self-signed certificates)	이 인증서는 웹 사이트를 식별할 수 있음(This certificate can identify websites)을 선택합니다.
인증 기관에서 발급한 인증서 (Certificates issued by a Certificate Authority)	웹 사이트 식별을 위해 이 CA 신뢰(Trust this CA to identify websites)를 선택합니다.

- 12 **확인(OK)**을 클릭하고 브라우저를 다시 시작합니다.

인증서 오류 없이 원격 콘솔에 연결할 수 있습니다.

vRealize Automation 장치의 인증서를 신뢰하도록 Internet Explorer 구성

vSphere에서 프로비저닝된 클라이언트의 VMware Remote Console을 지원하려면 신뢰할 수 없는 vRealize Automation 장치 인증서를 클라이언트 브라우저에 수동으로 가져와야 합니다.

참고 환경에서 신뢰할 수 있는 SSL 인증서를 사용하여 vRealize Automation을 구성한 경우에는 클라이언트 브라우저에서 VMware Remote Console을 위한 추가 구성이 필요하지 않습니다.

이 절차의 단계는 자체 서명된 인증서와 인증 기관에서 발급한 인증서에 적용됩니다.

지원되는 Internet Explorer 버전에 대한 자세한 내용은 VMware 웹 사이트에서 VMware vRealize 지원 매트릭스를 참조하십시오.

프로시저

- 1 Internet Explorer 브라우저에서 vRealize Automation 장치에 로그인합니다.
- 2 브라우저 주소 표시줄에 나타나는 인증서 오류 메시지에서 **인증서 보기**를 클릭합니다.
- 3 [인증서 정보] 창에서 **일반** 탭을 클릭합니다.
- 4 인증서에 대한 정보가 올바른지 확인하고 **인증서 설치**를 클릭합니다.
- 5 [인증서 저장소] 대화 상자에서 **모든 인증서를 다음 저장소에 저장**을 선택합니다.
- 6 **찾아보기**를 클릭하여 인증서 저장소를 찾습니다.
- 7 **신뢰할 수 있는 루트 인증 기관**을 선택하고 **확인**을 클릭합니다.
- 8 [인증서 저장소] 대화 상자에서 **다음**을 클릭합니다.
- 9 [보안 경고] 대화 상자에서 **예**를 클릭하여 인증서를 설치합니다.
- 10 브라우저를 다시 시작합니다.

인증서 오류 없이 원격 콘솔에 연결할 수 있습니다.

vRealize Automation 장치의 인증서를 신뢰하도록 Chrome 구성

vSphere에서 프로비저닝된 클라이언트의 VMware Remote Console을 지원하려면 신뢰할 수 없는 vRealize Automation 장치 인증서를 클라이언트 브라우저에 수동으로 가져와야 합니다.

지원되는 Chrome 버전에 대한 자세한 내용은 VMware 웹 사이트에서 VMware vRealize 지원 매트릭스를 참조하십시오.

참고 환경에서 신뢰할 수 있는 SSL 인증서를 사용하여 vRealize Automation을 구성한 경우에는 클라이언트 브라우저에서 VMware Remote Console을 위한 추가 구성이 필요하지 않습니다.

Windows의 경우 Chrome과 Internet Explorer가 동일한 인증서 저장소를 사용합니다. 이것은 Internet Explorer에서 신뢰하는 인증서는 Chrome에서도 신뢰한다는 것을 의미합니다. 신뢰할 수 있는 Chrome용 인증서를 설정하려면 Internet Explorer를 통해 해당 인증서를 가져옵니다. 이 절차에 대한 자세한 내용은 [vRealize Automation 장치의 인증서를 신뢰하도록 Internet Explorer 구성](#) 항목을 참조하십시오.

절차가 완료되면 Chrome을 다시 시작합니다.

Macintosh 운영 체제에서 인증서를 영구적으로 신뢰하려면 인증서 파일을 다운로드하고 인증서를 인증서 관리 도구에서 신뢰할 수 있는 인증서로 설치합니다.

프로시저

- 1 Chrome 브라우저에서 vRealize Automation 장치에 로그인합니다.
- 2 주소 표시줄에서 아이콘을 클릭합니다.
- 3 인증서 정보 링크를 클릭합니다.
- 4 인증서 아이콘을 바탕 화면으로 끌어서 인증서를 저장합니다.
- 5 키체인 접근(Keychain Access) 애플리케이션을 시작합니다.
- 6 **파일(File) > 항목 가져오기(Import Items)**를 클릭합니다.
- 7 키체인 접근(Keychain Access) 화면에서, 앞에서 저장한 인증서 파일을 선택합니다.
대상 키(Destination Key)의 값을 시스템(System)으로 설정합니다.
- 8 **열기(Open)**를 클릭하여 인증서를 가져옵니다.
- 9 브라우저를 다시 시작합니다.

실패한 제거 요청 후 배포 강제 제거

실패한 제거 요청으로 인해 일관되지 않은 상태인 배포를 강제로 제거할 수 있습니다.

배포 제거 작업 중에 vRealize Automation이 배포 리소스를 제거하지 못한 경우 나머지 배포 리소스를 제거하지 않고 배포 제거 작업이 즉시 중지됩니다. 이 실패로 인해 배포가 일관되지 않은 상태가 되고, 배포를 제거할 수 있는 방법이 없는 상태로 리소스가 사용됩니다. 비즈니스 그룹 관리자는 이렇게 일관되지 않은 상태로 남아 있는 배포를 강제 제거할 수 있습니다.

필수 조건

vRealize Automation에 **비즈니스 그룹 관리자**로 로그인했는지 확인합니다.

프로시저

- 1 **항목** 탭에서 **배포**를 클릭하고 제거할 배포를 선택합니다.
- 2 **작업**을 클릭하고 **제거**를 클릭합니다.
- 3 요청에 대한 설명과 이유를 입력합니다.
- 4 **강제 제거**를 선택하고 **제출**을 클릭합니다.

vRealize Automation은 배포를 모든 리소스와 함께 완전히 제거하려고 시도합니다. 하지만 제거할 수 없는 배포 리소스가 있는 경우 vRealize Automation은 해당 리소스를 건너 뛰고 배포의 나머지 리소스를 계속 제거합니다.

후속 작업

요청 탭을 클릭하고 배포의 모든 리소스가 제거되었는지 확인합니다. 강제 제거 중에 제거되지 않은 모든 리소스는 수동으로 제거해야 합니다. 프로비저닝된 모든 가상 시스템 개체가 삭제되었는지도 확인합니다. vRealize Automation이 후속 작업 중에 해당 호스트 이름, IP 주소 및 기타 구성 세부 정보를 재사용하려고 시도할 수 있기 때문입니다.

리소스 작업 메뉴에서 누락된 작업 문제 해결

시스템 또는 리소스 소유자는 프로비저닝된 항목에 대한 모든 권한 있는 작업이 보이지 않습니다.

문제점

작업이 사용자 또는 비즈니스 그룹에 대해 사용 권한이 부여되었음을 아는 환경에서는 **항목** 목록에서 항목을 선택할 때 모든 작업을 볼 것으로 예상합니다.

원인

작업의 가용성은 프로비저닝된 리소스의 유형, 리소스의 작동 상태 및 작업이 구성되고 사용할 수 있게 된 방식에 따라 다릅니다. 다음 목록은 구성된 모든 작업이 보이지 않는 몇 가지 이유를 제공합니다.

- 프로비저닝된 리소스의 현재 상태를 기반으로 작업을 적용할 수 없습니다. 예를 들어 시스템의 전원이 켜진 경우에만 전원 끄기를 사용할 수 있습니다.
- 선택된 항목 유형에 작업을 적용할 수 없습니다. 항목이 작업을 지원하지 않는 경우 목록에 나타나지 않습니다. 예를 들어 스냅샷 생성 작업은 물리적 시스템에 대해 사용할 수 없으며 RDP를 사용하여 연결 작업은 선택된 항목이 Linux 시스템인 경우 사용할 수 없습니다.
- 프로비저닝된 리소스 유형에 대해 작업을 적용할 수 있지만 작업이 인프라 Blueprint에서 사용하지 않도록 설정되었습니다. 작업이 사용하지 않도록 설정된 경우 Blueprint를 사용하여 프로비저닝된 항목에 대해 사용 가능한 작업으로 나타나지 않습니다.
- 작업이 작업을 실행해야 하는 항목을 프로비저닝하는 데 사용된 사용 권한에 포함되어 있지 않습니다. 권한 있는 작업만 IaaS Blueprint의 일부 또는 XaaS 리소스 작업으로 작업 메뉴에 나타날 수 있습니다.
- 작업이 XaaS 리소스 작업으로 생성되었지만 작업을 실행해야 하는 항목을 프로비저닝하는 데 사용된 사용 권한에 포함되지 않았습니다. 권한 있는 작업만 작업 메뉴에 나타납니다.
- 작업이 XaaS 리소스 작업 또는 리소스 매핑에 대해 구성된 대상 기준을 기반으로 프로비저닝된 IaaS 시스템으로 제한될 수 있습니다.

해결 방법

- 작업을 프로비저닝된 항목 또는 프로비저닝된 항목의 상태에 적용할 수 있는지 확인합니다.
- 작업이 구성되었으며 항목을 프로비저닝하는 데 사용된 사용 권한에 포함되었는지 확인합니다.

vRealize Orchestrator 워크플로가 포함된 실패한 배포 문제 해결

실패한 Blueprint 배포에 vRealize Orchestrator 워크플로가 포함된 경우 토큰 ID를 사용하여 워크플로 관련 문제를 해결할 수 있습니다. vRealize Orchestrator에서 토큰 ID를 사용하여 로그를 찾습니다.

해결 방법

- 1 실패한 워크플로의 토큰 ID를 찾습니다.
 - a vRealize Automation에서 **요청** 탭을 클릭합니다.
 - b [요청] 열의 번호를 클릭합니다.
요청은 배포 또는 작업일 수 있습니다.
 - c **일반** 탭을 클릭합니다.
Blueprint가 vRealize Orchestrator 워크플로에 기반하는 경우 페이지 제목은 vRealize Orchestrator 워크플로 실행 세부 정보입니다.
 - d 토큰 ID를 찾아 클립보드 또는 텍스트 파일에 복사합니다.
예를 들어 ff8080815a685352015a6c8d450801ee와 같은 형태입니다.
- 2 제어 센터를 사용하여 vRealize Orchestrator에서 워크플로 로그 찾기
 - a 브라우저 검색 상자에 vRealize Automation에 대한 기본 URL을 입력합니다.
VMware vRealize Automation 장치 페이지가 나타납니다.
 - b **vRealize Orchestrator 제어 센터**를 클릭합니다.
 - c 루트 권한이 있는 사용자로 로그인합니다.
 - d **워크플로 검사**를 클릭합니다.
 - e **완료된 워크플로**를 클릭합니다.
 - f 워크플로 토큰을 [토큰 ID] 텍스트 상자에 붙여 넣습니다.
목록에 토큰 ID와 일치하는 워크플로가 표시됩니다.
 - g 행을 클릭하고 로그에서 실패의 원인을 검토합니다.

재구성에 대한 시스템 재구성 설정 및 고려 사항 지정

vSphere, vCloud Air 및 vCloud Director 플랫폼은 배포의 기존 시스템을 재구성하여 CPU, 메모리 및 스토리지 같은 사양을 수정하도록 지원합니다.

재구성 요청은 Blueprint에서 시스템 구성 요소에 대해 사용하도록 설정된 사용 권한, 정책 및 작업을 기준으로 승인을 받아야 합니다.

요청 시 네트워크에 할당된 가상 시스템 재구성은 지원되지 않습니다. 요청 시 네트워크에 연결된 NIC는 재구성할 수 없습니다. 요청 시 NAT 또는 라우팅된 네트워크를 재구성하려고 시도하면 'Original network [<network>] is not selected in the machine's reservation. 오류가 표시되고, 시스템의 네트워크는 그대로 유지되며, 시스템의 IP 주소는 변경되지 않습니다.

(시스템) 재구성 취소 및 (시스템) 재구성 실행 작업에 대한 권한이 부여된 경우 재구성을 취소하거나 실패한 재구성을 재시도할 수 있습니다.

연결된 클론 Blueprint에서 프로비저닝된 VM에서 디스크 확장은 지원되지 않습니다.

Size 또는 Image 구성 요소 프로파일을 사용하여 시스템을 재구성할 수 없지만 프로파일을 기반으로 계산된 CPU, 메모리 및 스토리지의 범위는 재구성 작업에 계속 사용할 수 있습니다. 예를 들어 소형 (CPU 1개, 1024MB 메모리, 10GB 스토리지), 중형 (CPU 3개, 2048MB 메모리, 12GB 스토리지) 및 대형 (CPU 5개, 3072MB 메모리, 15GB 스토리지) Size 값 집합을 사용한 경우 시스템 재구성 동안 사용 가능한 범위는 CPU 1~5개, 1024~3072MB 메모리, 1~15GB 스토리지입니다.

vRealize Automation은 배포 시 Blueprint 스냅샷을 생성합니다. 배포의 CPU 및 RAM 같은 시스템 속성을 업데이트할 때 재구성 문제가 발생한 경우에는 기술 자료 문서 [2150829 vRA 7.x Blueprint 스냅샷 생성](#)을 참조하십시오.

필수 조건

- 시스템 소유자, 지원 사용자, 공유 액세스 역할을 가진 비즈니스 그룹 사용자 또는 비즈니스 그룹 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 재구성하려는 시스템은 상태가 [켜짐] 또는 [꺼짐]이어야 하며 활성 상태의 재구성 작업이 없어야 합니다.
- NSX 설정이 vSphere에 적용되지만 시스템 유형은 vSphere, vCloud Air 또는 vCloud Director여야 합니다.
- 시스템을 재구성할 권한이 있는지 확인합니다.

프로시저

- 1 항목 > 시스템을 선택합니다.

또는 항목 > 배포를 선택하고 배포의 시스템으로 이동할 수 있습니다.

- 2 재구성할 시스템을 선택합니다.



- 3 작업 메뉴에서 재구성을 선택합니다.
- 4 재구성하려는 설정에 해당하는 탭을 선택합니다.

표 3-76. 재구성 변경 요청

탭	항목
일반	CPU 및 메모리 재구성
스토리지	스토리지 설정 편집
네트워크	네트워크 설정 변경 NAT 규칙을 변경하려면 배포에서 NAT 규칙 변경 항목을 참조하십시오.
보안	보안 설정을 재구성하려면 배포에서 보안 항목 추가 또는 제거 항목을 참조하십시오.
속성	사용자 지정 속성 및 속성 그룹 설정 변경

후속 작업

[요청된 시스템 재구성 실행](#).

CPU 및 메모리 재구성

프로비저닝 Blueprint에 의해 설정된 제한 내에서 프로비저닝된 시스템에서 사용하는 메모리 및 스토리지의 양 또는 CPU 수를 변경할 수 있습니다.

프로비저닝된 Amazon 배포에서는 루트 볼륨을 제외한 모든 스토리지 볼륨을 재구성할 수 있습니다. 연결된 클론 Blueprint에서 프로비저닝된 VM에서 디스크 확장은 지원되지 않습니다.

필수 조건

[재구성에 대한 시스템 재구성 설정 및 고려 사항 지정](#).

프로시저

- 1 일반 탭을 클릭합니다.
- 2 CPU 수 텍스트 상자에 CPU 수를 입력합니다.
- 3 메모리(MB) 텍스트 상자에 메모리 양을 입력합니다.
- 4 스토리지(GB) 텍스트 상자에 스토리지 양을 입력합니다.

후속 작업

추가적인 시스템 재구성 설정을 지정합니다. 시스템 설정 변경을 완료한 경우 시스템 재구성 요청을 시작합니다. [요청된 시스템 재구성 실행](#) 항목을 참조하십시오.

스토리지 설정 편집

프로비저닝된 가상 시스템에서 스토리지 볼륨을 추가 또는 삭제하거나 크기를 변경할 수 있습니다.

IDE 디스크 유형에 대해서는 스토리지를 재구성할 수 없습니다.

예약에 의해 프로비저닝된 시스템에 할당된 스토리지와 메모리는 해당 시스템이 vRealize Automation에서 [제거] 작업에 의해 삭제될 때 해제됩니다. 시스템이 vCenter Server에서 삭제되는 경우에는 스토리지와 메모리가 해제되지 않습니다.

예를 들어 기존 배포에 포함된 시스템과 연결되어 있는 예약은 삭제할 수 없습니다. vCenter Server에서 배포된 시스템을 수동으로 이동하거나 삭제할 경우, vRealize Automation에서는 배포된 시스템을 라이브 상태로 계속 인식하기 때문에 연결된 예약을 삭제하지 못합니다.

필수 조건

[재구성에 대한 시스템 재구성 설정 및 고려 사항 지정](#).


프로비저닝된 Amazon 배포에서는 루트 볼륨을 제외한 모든 스토리지 볼륨을 재구성할 수 있습니다.

프로시저


- 1 스토리지 탭을 클릭합니다.

스토리지의 허용 가능한 범위가 [스토리지 볼륨] 테이블 아래에 표시됩니다.

2 사용 가능한 스토리지 볼륨 설정을 추가하거나 편집합니다.

- a 새 볼륨을 클릭합니다.
- b 용량(GB) 텍스트 상자에 용량을 입력합니다.
- c 스토리지 예약 정책 드롭다운 메뉴에서 스토리지 예약 정책을 선택합니다.
- d 저장 아이콘()을 클릭합니다.



3 볼륨을 삭제합니다.

- a 볼륨을 찾습니다.
- b 삭제 아이콘()을 클릭합니다.

선택할 수 없는 아이콘은 연결된 복제의 볼륨과 같이 삭제할 수 없는 볼륨을 나타냅니다.

4 볼륨의 크기를 늘립니다.

기존 볼륨의 크기를 줄일 수는 없습니다. 볼륨 크기는 Blueprint에 지정된 스토리지의 총 양으로 제한되며 다른 볼륨에 할당된 양보다 작습니다.

- a 볼륨을 찾습니다.
- b 편집 아이콘()을 클릭합니다.
- c 용량(GB) 텍스트 상자에 새 크기를 입력합니다.
- d 저장 아이콘()을 클릭합니다.

후속 작업

추가적인 시스템 재구성 설정을 지정합니다. 시스템 설정 변경을 완료한 경우 시스템 재구성 요청을 시작합니다. [요청된 시스템 재구성 실행](#) 항목을 참조하십시오.

네트워크 설정 변경

네트워크 어댑터를 추가, 제거 또는 편집할 수 있습니다.

시스템 재구성 프로세스 중에 다음과 같은 네트워크 설정을 변경할 수 있습니다.

- NIC를 추가 또는 제거합니다.
- 기존 NIC의 IP 주소를 할당 또는 해제합니다.
- 네트워크가 요청 시 NAT 또는 요청 시 라우팅된 네트워크가 아닌 경우 NIC에 새 IP 주소를 할당합니다.

요청 시 라우팅된 네트워크 또는 요청 시 NAT 네트워크는 재구성할 수 없습니다.

네트워크를 재구성하려면 예약에서 소스 및 대상 네트워크를 선택해야 합니다.

NIC를 추가하면 IP 주소가 할당됩니다. NIC를 제거하면 IP 주소가 해제됩니다.

예약 및 네트워크 프로파일 정보를 기반으로 네트워크 설정을 변경하면 새 네트워크 IP가 vRealize Automation에 할당되지만 배포된 시스템은 끝점에서 새 IP 정보로 업데이트되지 않습니다. 재구성 프로세스가 완료된 후 시스템에 IP를 수동으로 할당해야 합니다.

요청 시 네트워크에 할당된 가상 시스템 재구성은 지원되지 않습니다. 요청 시 네트워크에 연결된 NIC는 재구성할 수 없습니다. 요청 시 NAT 또는 라우팅된 네트워크를 재구성하려고 시도하면 'Original network [<network>] is not selected in the machine's reservation. 오류가 표시되고, 시스템의 네트워크는 그대로 유지되며, 시스템의 IP 주소는 변경되지 않습니다.

vRealize Automation 6.2.x에서 이 vRealize Automation 릴리스로 업그레이드 또는 마이그레이션된 배포에는 NSX 네트워크 설정 변경이 지원되지 않습니다.

필수 조건

재구성에 대한 시스템 재구성 설정 및 고려 사항 지정.

프로시저

- 1 네트워크 탭을 클릭합니다.
- 2 (선택 사항) 네트워크 어댑터를 추가합니다.
 - a 새 네트워크 어댑터를 클릭합니다.
 - b 네트워크 경로 드롭다운 메뉴에서 네트워크를 선택합니다.
시스템의 예약에 선택된 모든 네트워크를 사용할 수 있습니다.
 - c 주소 텍스트 상자에 네트워크의 정적 IP 주소를 입력합니다.
IP 주소는 예약에 할당된 네트워크 프로파일에서 할당이 취소된 상태여야 합니다.
 - d 저장 아이콘(🟢)을 클릭합니다.
- 3 (선택 사항) 네트워크 어댑터를 제거합니다.
 - a 네트워크 어댑터를 찾습니다.
 - b 삭제 아이콘(🗑️)을 클릭합니다.
네트워크 어댑터 0은 제거할 수 없습니다.
- 4 (선택 사항) 네트워크 어댑터를 편집합니다.
 - a 네트워크 어댑터를 찾습니다.
 - b 편집 아이콘(✎)을 클릭합니다.
 - c 네트워크 경로 드롭다운 메뉴에서 네트워크를 선택합니다.
 - d 저장 아이콘(🟢)을 클릭합니다.

후속 작업

추가적인 시스템 재구성 설정을 지정합니다. 시스템 설정 변경을 완료한 경우 시스템 재구성 요청을 시작합니다. [요청된 시스템 재구성 실행](#) 항목을 참조하십시오.

사용자 지정 속성 및 속성 그룹 설정 변경

배포된 시스템에서 사용자 지정 속성을 편집, 추가 또는 삭제할 수 있습니다.

볼륨 디스크 번호, 용량, 레이블 또는 스토리지 예약 정책에 대한 값을 입력하는 데는 사용자 지정 속성을 사용할 수 없습니다. 이러한 값은 [스토리지 볼륨] 테이블에서 볼륨을 추가하거나 편집하는 방법으로 입력해야 합니다. [스토리지 설정 편집](#) 항목을 참조하십시오.

필수 조건

[재구성에 대한 시스템 재구성 설정 및 고려 사항 지정](#).

프로시저

- 1 속성 탭을 클릭합니다.
- 2 속성을 추가하려면 **새 속성**을 클릭합니다.
- 3 **이름** 텍스트 상자에 속성 이름을 입력합니다.
- 4 **값** 텍스트 상자에 속성 값을 입력합니다.
- 5 값을 암호화하려면 **암호화됨** 확인란을 선택합니다.
- 6 사용자가 시스템을 요청할 때 사용자에게 값을 확인하려면 **사용자에게 확인** 확인란을 선택합니다.
- 7 다른 속성을 추가하거나, 기존 속성을 편집하거나, 속성을 삭제합니다.

후속 작업

추가적인 시스템 재구성 설정을 지정합니다. 시스템 설정 변경을 완료한 경우 시스템 재구성 요청을 시작합니다. [요청된 시스템 재구성 실행](#) 항목을 참조하십시오.

요청된 시스템 재구성 실행

요청된 시스템 재구성을 즉시 시작하거나 특정 날짜와 시간에 시작하도록 예약할 수 있습니다. 또한 시스템을 재구성하기 전에 전원 옵션을 지정할 수도 있습니다.

필수 조건

[재구성에 대한 시스템 재구성 설정 및 고려 사항 지정](#).

프로시저

- 1 **실행** 탭이 표시되는 경우 이 탭을 선택하여 추가적인 재구성 설정을 지정할 수 있습니다. 이 탭이 표시되지 않는 경우 **제출**을 클릭하여 시스템 재구성을 시작합니다.
- 2 **실행** 탭에 표시되는 경우 **실행**을 클릭하여 재구성 작업을 예약합니다.
- 3 (선택 사항) **요청 실행** 드롭다운 메뉴에서 옵션을 선택합니다.

옵션	설명
즉시	승인 후 최대한 빨리 재구성을 시작합니다.
예약됨	지정한 날짜와 시간에 재구성을 시작합니다. 표시되는 텍스트 상자에서 날짜와 시간을 선택하거나 직접 입력합니다.

예약된 시간은 vRealize Automation 웹 서버가 있는 위치의 로컬 시간입니다. **요청 실행**을 사용할 수 없으면 재구성이 즉시 시작됩니다.

4 (선택 사항) 전원 동작 드롭다운 메뉴에서 전원 동작을 선택합니다.

옵션	설명
필요한 경우 재부팅	(기본값) 필요한 경우 시스템을 재구성하기 전에 재부팅합니다.
재부팅	재부팅이 필요한지 여부에 관계없이 시스템을 재구성하기 전에 재부팅합니다.
재부팅하지 않음	재부팅이 필요하더라도 시스템을 재구성하기 전에 재부팅하지 않습니다.

다음과 같은 조건에서는 시스템을 재구성하기 전에 재부팅해야 합니다.

- Hot Add가 지원되지 않거나 사용하지 않도록 설정된 경우의 CPU 변경
- 핫 메모리가 지원되지 않거나 사용하지 않도록 설정된 경우의 메모리 변경
- 핫 스토리지가 사용하지 않도록 설정된 경우의 스토리지 변경

시스템은 종료 상태일 때는 재부팅되지 않습니다.

참고 VirtualMachine.Reconfigure.DisableHotCpu 사용자 지정 속성을 사용하면 vSphere Hot Add 옵션을 사용하지 않도록 설정할 수 있습니다.

5 확인을 클릭합니다.

후속 작업

사용자 인터페이스에 표시되는 워크플로 상태를 관찰하는 방법으로 재구성의 진행률을 모니터링할 수 있습니다. [재구성 작업의 워크플로 상태](#) 항목을 참조하십시오.

재구성 작업의 워크플로 상태

재구성이 시작되고 워크플로에서 진행 중인 동안 [편집] 페이지에서 진행률을 모니터링할 수 있습니다.

표 3-77. 재구성 작업의 워크플로 상태

상태	설명
재구성 보류 중	[상태 작업]이 생성되었습니다.
예약됨	DEM(Distributed Execution Manager)에 대해 예약된 워크플로가 생성되었습니다.
재구성	인터페이스별 워크플로가 실행 중입니다.
재구성이 실패했으며 재시도를 기다리는 중입니다.	재구성이 실패했으며 소유자가 재시도를 요청할 때까지 기다리는 중입니다. 시스템 소유자가 재구성 실행 또는 재구성 취소 같은 작업에 대한 사용 권한을 가지고 있는 경우, 소유자가 재구성을 재시도하거나 취소할 수 있습니다.
재구성이 실패함	재구성이 실패했으며 RVG 워크플로가 다음 작업을 수행할 때까지 기다리는 중입니다.
재구성이 성공함	재구성이 성공했으며 RVG 워크플로가 다음 작업을 수행할 때까지 기다리는 중입니다.
취소됨	사용자가 재구성을 취소했습니다. 재구성 취소 작업에 대한 사용 권한을 가진 시스템 소유자는 재구성을 취소할 수 있습니다.
완료	완료 워크플로는 RVG 워크플로가 상태 작업 및 승인을 정리할 수 있도록, 정리를 완료한 이후에 이 상태를 설정합니다. 완료 상태는 vRealize Automation에서 보낸 요청을 마쳤음을 나타내지만 시스템 재구성이 성공적으로 완료되었음을 나타내지는 않습니다.

배포에서 로드 밸런서 재구성

배포된 NSX 로드 밸런서에서 가상 서버를 추가, 편집 또는 삭제할 수 있습니다.

다음 고려 사항은 vRealize Automation 7.2 이전 버전에서 시작된 배포에 적용됩니다.

- 로드 밸런서 재구성은 단일 로드 밸런서가 포함된 배포로 제한됩니다.
- 배포의 모든 로드 밸런서에 대한 항목 세부 정보 페이지에는 배포의 모든 로드 밸런서에 사용되는 가상 서버가 표시됩니다. 자세한 내용은 [기술 자료 문서 2150276](#)을 참조하십시오.

업그레이드된 로드 밸런서 및 최신 vRealize Automation 릴리스에 배포된 로드 밸런서의 경우에는 가상 서버 편집 및 가상 서버 추가 작업을 같은 요청에서 수행하지 마십시오. 자세한 내용은 [기술 자료 문서 2150240](#)을 참조하십시오.

배포에 대한 확장 작업이 진행 중인 때와 같이, 배포에서 다른 작업이 수행되는 동안 로드 밸런서를 재구성하는 요청을 제출하면 재구성이 실패하고 지원 메시지가 나타납니다. 이 경우 작업이 완료될 때까지 기다린 다음 재구성 요청을 제출할 수 있습니다.

vRealize Automation 6.2.x에서 이 vRealize Automation 릴리스로 업그레이드 또는 마이그레이션된 배포에 대해서는 로드 밸런서 재구성 작업이 지원되지 않습니다.

vRealize Automation에서 관리하는 NSX 개체를 vRealize Automation 외부에서 관리해서는 안 됩니다. 예를 들어 vRealize Automation이 아니라 NSX에서 배포된 NSX 로드 밸런서의 구성원 포트를 수정하는 경우 NSX 데이터 수집은 배포된 시스템과 다른 방법으로 연결된 해당 로드 밸런서 구성원 풀 간의 연결을 끊습니다. 배포된 로드 밸런서 구성원 포트가 vRealize Automation 외부에서 변경되는 경우 축소 및 확장 작업도 예기치 않은 결과를 가져옵니다.

알려진 문제는 vRealize Automation [릴리스 정보](#)를 참조하십시오.

가상 서버를 추가 또는 편집할 때 사용할 수 있는 설정에 대한 자세한 내용은 [요청 시 로드 밸런서 구성 요소 추가](#) 항목을 참조하십시오.

vRealize Automation에서 로드 밸런서를 재구성하는 경우 NSX에서 구성했지만 vRealize Automation에서 설정으로 사용할 수 없는 일부 설정이 기본값으로 돌아갑니다. vRealize Automation에서 로드 밸런서 재구성 작업을 실행한 후 NSX에서 다음 설정을 확인하고 필요에 따라 업데이트합니다.

- HTTP 헤더의 Insert-X-Forwarded
- HTTP 리디렉션 URL
- 서비스 모니터링 확장

필수 조건

- 시스템 소유자, 지원 사용자, 공유 액세스 역할을 가진 비즈니스 그룹 사용자 또는 비즈니스 그룹 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 배포에서 로드 밸런서를 재구성할 수 있는 권한이 있는지 확인합니다. 필요한 카탈로그 사용 권한은 [재구성(로드 밸런서)]입니다.

프로시저

- 1 항목 > 배포를 선택합니다.
- 2 배포를 찾아서 해당 하위 구성 요소를 표시합니다.



- 3 편집할 NSX 로드 밸런서를 선택합니다.



- 4 작업 메뉴에서 재구성을 선택합니다.
- 5 가상 서버를 추가, 편집 또는 제거합니다.

Virtual servers:

Protocol	Port	Description	Member Protocol	Member Port	Health Check Protocol	Health Check Port
HTTP	80		HTTP	80	HTTP	80
HTTP	81		HTTP	81	HTTP	81

- 6 가상 서버 추가, 편집 또는 삭제를 마쳤으면 제출을 클릭하여 재구성 요청을 제출합니다.

배포에서 NAT 규칙 변경

배포된 일대다 NAT 네트워크에서 기존 NSX NAT 규칙을 추가, 편집 및 삭제할 수 있습니다. NAT 규칙이 처리되는 순서도 변경할 수 있습니다.

NAT 규칙에 대한 자세한 내용은 [NAT 규칙 생성 및 사용 및 요청 시 NAT 또는 요청 시 라우팅된 네트워크 구성 요소 추가](#)를 참조하십시오.

NAT 규칙 변경 작업은 vRealize Automation 6.2.x에서 이 vRealize Automation 릴리스로 업그레이드되거나 마이그레이션된 배포에 대해서는 지원되지 않습니다.

Infoblox와 같은 타사 IPAM 끝점에 매핑되어 있는 배포에 NAT 규칙을 추가할 수 없습니다.

알려진 문제는 vRealize Automation [릴리스 정보](#)를 참조하십시오.

필수 조건

- 시스템 소유자, 지원 사용자, 공유 액세스 역할을 가진 비즈니스 그룹 사용자 또는 비즈니스 그룹 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 네트워크에서 NAT 규칙을 변경할 권한이 부여되어 있는지 확인합니다.
- NAT 네트워크는 NAT 일대다 네트워크로 구성되어야 합니다. NAT 일대일 네트워크에 대해서는 작업을 수행할 수 없습니다. 다음을 참조하십시오.

프로시저

- 1 항목 > 배포를 선택합니다.

- 2 배포를 찾아서 해당 하위 구성 요소를 표시합니다.



- 3 편집할 NAT 네트워크 구성 요소를 선택합니다.



- 4 작업 메뉴에서 **NAT 규칙 변경**을 클릭합니다.



- 5 새 NAT 포트 포워딩 규칙을 추가하거나, 규칙 순서를 다시 지정하거나, 기존 규칙을 편집하거나, 규칙을 삭제합니다.
- 6 변경을 완료하면 **저장**을 클릭하거나 **제출**을 클릭하여 재구성 요청을 제출합니다.

배포에서 보안 항목 추가 또는 제거

시스템 배포에서 기존 NSX 보안 그룹 및 보안 태그를 추가 또는 제거할 수 있습니다. 요청 시 보안 그룹은 추가할 수 없지만 제거할 수 있습니다.

보안 변경 작업은 시스템 구성 요소 또는 클러스터를 기반으로 합니다. 예를 들어 보안이 2개의 시스템으로 구성된 AppTier2라는 클러스터에 연결되어 있는 경우 클러스터 내의 개별 시스템이 아닌 AppTier2 클러스터에서 보안 변경 작업을 수행합니다.

보안 변경 작업은 vRealize Automation 6.2.x에서 이 vRealize Automation 릴리스로 업그레이드되거나 마이그레이션된 배포에 대해서는 지원되지 않습니다.

필수 조건

- 시스템 소유자, 지원 사용자, 공유 액세스 역할을 가진 비즈니스 그룹 사용자 또는 비즈니스 그룹 관리자로 vRealize Automation 콘솔에 로그인합니다.
- 배포에서 보안을 변경할 권한이 부여되었는지 확인합니다. 필요한 카탈로그 사용 권한은 보안 변경 (배포)입니다.

프로시저

- 1 항목 > 배포를 선택합니다.
- 2 배포를 찾아서 해당 하위 구성 요소를 표시합니다.



- 3 작업 메뉴에서 **보안 변경**을 클릭합니다.



- 4 보안 항목을 추가 또는 제거할 배포된 시스템 구성 요소 또는 클러스터를 선택합니다.



- 5 필요에 맞게 배포에서 각 시스템 구성 요소 또는 클러스터의 기존 보안 그룹 및 보안 태그를 추가 또는 제거합니다.
- 6 필요에 맞게 배포에서 각 시스템 구성 요소 또는 클러스터의 요청 시 보안 그룹을 제거합니다.
- 7 (선택 사항) **이유** 탭을 클릭하고 요청 이유를 입력합니다.
- 8 변경을 완료하면 **저장**을 클릭하거나 **제출**을 클릭하여 변경 요청을 제출합니다.

기존 NSX Edge의 모든 NAT 규칙 표시

활성 배포에 사용되는 NSX Edge에 대한 NAT 규칙 정보를 표시할 수 있습니다.

NAT 규칙은 배포에 사용되는 모든 NAT 규칙의 집계로 Edge 보기에 표시됩니다. Edge 보기에서 규칙이 반드시 처리되는 순서대로 표시되지는 않습니다.

NAT 일대다 네트워크에서 NAT 규칙이 처리되는 순서를 보고 필요에 따라 변경하려면 [배포에서 NAT 규칙 변경](#)을 참조하십시오.

필수 조건

- 시스템 소유자, 지원 사용자, 공유 액세스 역할을 가진 비즈니스 그룹 사용자 또는 비즈니스 그룹 관리자로 vRealize Automation 콘솔에 로그인합니다.

프로시저

- 1 항목 > 배포를 선택합니다.
- 2 배포를 찾아서 해당 하위 구성 요소를 표시합니다.



- 3 보려는 NSX Edge를 선택합니다.



- 4 완료했으면 **닫기**를 클릭합니다.