

VMware Cloud Director 서비스 제공자 관리자 포털 가이드

2019년 9월 19일

VMware Cloud Director 10.0

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

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

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

목차

1	vCloud Director Service Provider Admin Portal 정보	9
2	vCloud Director Service Provider Admin Portal 시작	10
	vCloud Director 관리 개요	10
	vCloud Director Service Provider Admin Portal에 로그인	13
	작업 보기	14
	진행 중인 작업 중지	14
	이벤트 보기	15
	이름 및 설명의 길이 제한	15
3	vSphere 리소스 관리	17
	vCenter Server 및 NSX 리소스 추가	18
	vCenter Server 인스턴스를 단독으로 또는 NSX Manager 인스턴스와 함께 연결	18
	vApp 검색 및 채택	21
	vCenter Server에서 NSX 라이선스 키 할당	22
	NSX-T Manager 인스턴스 등록	23
	클라우드 리소스 추가	23
	제공자 가상 데이터 센터	24
	제공자 가상 데이터 센터 생성	24
	외부 네트워크	27
	네트워크 풀	29
	vCenter Server 인스턴스 보기	33
	vCenter Server 설정 수정	34
	vCenter Server 인스턴스 사용 또는 사용 안 함	35
	vCenter Server 인스턴스 다시 연결	35
	vCenter Server 인스턴스 새로 고침	36
	vCenter Server 인스턴스의 스토리지 정책 새로 고침	36
	vCenter Server 인스턴스 등록 취소	36
	NSX Manager 설정 수정	37
	NSX-T Manager 설정 수정	37
	NSX-T Manager 인스턴스 삭제	38
	다중 사이트 배포 구성 및 관리	38
	다중 사이트 리소스 목록	40
4	제공자 가상 데이터 센터 관리	41
	제공자 가상 데이터 센터 사용 또는 사용 안 함	41

제공자 가상 데이터 센터 삭제	42
제공자 가상 데이터 센터의 일반 설정 편집	42
제공자 가상 데이터 센터 병합	43
제공자 가상 데이터 센터의 조직 가상 데이터 센터 보기	43
제공자 가상 데이터 센터의 데이터스토어 보기	44
제공자 가상 데이터 센터의 외부 네트워크 보기	45
제공자 가상 데이터 센터에서 VM 스토리지 정책 관리	45
VM 스토리지 정책을 제공자 가상 데이터 센터에 추가	45
제공자 가상 데이터 센터에서 VM 스토리지 정책 사용 또는 사용 안 함	46
제공자 가상 데이터 센터에서 VM 스토리지 정책 삭제	46
제공자 가상 데이터 센터에서 VM 스토리지 정책의 메타데이터 수정	47
제공자 가상 데이터 센터의 리소스 풀 관리	47
제공자 가상 데이터 센터에 리소스 풀 추가	47
제공자 가상 데이터 센터에서 리소스 풀 사용 또는 사용 안 함	48
제공자 가상 데이터 센터에서 리소스 풀 분리	49
제공자 가상 데이터 센터에 대한 메타데이터 수정	49

5 조직 관리 50

임대 이해	50
조직 만들기	51
조직에 대한 카탈로그 구성	51
조직에 대한 정책 구성	52
테넌트 스토리지 마이그레이션	53

6 조직 가상 데이터 센터 관리 55

할당 모델 이해	55
할당 모델의 권장 사용법	57
Flex 할당 모델	58
할당 풀 할당 모델	59
선지급 할당 모델	60
예약 풀 할당 모델	61
VM 크기 조정 및 VM 배치 정책 이해	61
VM 크기 조정 정책의 특성	65
VM 배치 정책 만들기	66
조직 VDC에 VM 배치 정책 추가	67
VM 배치 정책 삭제	68
VM 크기 조정 정책 만들기	68
조직 VDC에 VM 크기 조정 정책 추가	69
VM 크기 조정 정책 편집	70
VM 크기 조정 정책 삭제	70

조직 가상 데이터 센터 만들기	71
조직 가상 데이터 센터 사용 또는 사용 안 함	73
조직 가상 데이터 센터 삭제	74
조직 가상 데이터 센터의 이름 및 설명 수정	74
조직 가상 데이터 센터의 할당 모델 설정 수정	74
조직 가상 데이터 센터의 스토리지 설정 수정	75
조직 가상 데이터 센터의 VM 프로비저닝 설정 수정	75
VM 스토리지 정책을 조직 가상 데이터 센터에 추가	75
조직 가상 데이터 센터의 기본 스토리지 정책 변경	76
조직 가상 데이터 센터에서 스토리지 정책 제한 편집	76
조직 가상 데이터 센터에서 VM 스토리지 정책의 메타데이터 수정	77
조직 가상 데이터 센터에서 스토리지 정책 사용 또는 사용 안 함	77
조직 가상 데이터 센터에서 스토리지 정책 삭제	78
조직 가상 데이터 센터의 네트워크 설정 편집	78
크로스 가상 데이터 센터 네트워킹 구성	79
조직 가상 데이터 센터에 대한 메타데이터 수정	81
조직 가상 데이터 센터의 리소스 풀 보기	81
조직 가상 데이터 센터에서 분산 방화벽 관리	82
조직 가상 데이터 센터에서 분산 방화벽을 사용하도록 설정	82
분산 방화벽 규칙 추가	83
분산 방화벽 규칙 편집	85
사용자 지정 개체 그룹화	86
보안 그룹 작업	89
보안 태그 작업	92

7 NSX Data Center for vSphere Edge 게이트웨이 관리 97

Edge 클러스터 사용	98
NSX Data Center for vSphere Edge 게이트웨이 추가	99
NSX Data Center for vSphere Edge 게이트웨이 서비스 구성	101
NSX Data Center for vSphere Edge 게이트웨이 방화벽 관리	101
NSX Data Center for vSphere Edge 게이트웨이 DHCP 관리	105
SNAT 또는 DNAT 규칙 추가	109
고급 라우팅 구성	111
로드 밸런싱	120
VPN(Virtual Private Network)을 사용한 보안 액세스	132
SSL 인증서 관리	157
사용자 지정 개체 그룹화	164
Edge 게이트웨이의 네트워크 사용 및 IP 할당 보기	168
Edge 게이트웨이 속성 편집	168
Edge 게이트웨이에서 분산 라우팅 사용 또는 사용 안 함	168

외부 네트워크 및 Edge 게이트웨이 설정 수정	169
Edge 게이트웨이의 일반 설정 편집	169
Edge 게이트웨이의 기본 게이트웨이 편집	170
Edge 게이트웨이의 IP 설정 편집	170
Edge 게이트웨이에서 하위 할당된 IP 풀 편집	171
Edge 게이트웨이의 속도 제한 편집	171
Edge 게이트웨이 다시 배포	172
Edge 게이트웨이 삭제	172
Edge 게이트웨이에 대한 통계 및 로그	172
통계 보기	172
로그 사용	173
Edge 게이트웨이에 대한 SSH 명령줄 액세스 사용	174

8 NSX-T Data Center Edge 게이트웨이 관리 176

NSX-T Data Center Edge 게이트웨이 추가	176
NSX-T Edge 게이트웨이에 방화벽 그룹 추가	177
NSX-T Edge 게이트웨이 방화벽 규칙 추가	177
NSX-T Edge 게이트웨이에 SNAT 또는 DNAT 규칙 추가	179
NSX-T Edge 게이트웨이에서 DNS 전달자 서비스 구성	180
NSX-T Edge 게이트웨이의 IP 할당 편집	181
빠른 IP 할당	181
사용자 지정 애플리케이션 포트 프로파일 생성	182

9 전용 vCenter Server 인스턴스 및 프록시 관리 184

연결된 vCenter Server의 테넌트 액세스 사용	186
전용 vCenter Server에 대한 프록시 만들기	187
프록시 인증서 및 CRL 관리	187
전용 vCenter Server 게시	188

10 시스템 관리자 및 역할 관리 190

권한 및 역할 관리	190
미리 정의된 역할 및 역할 권한	192
시스템 관리자 권한	194
미리 정의된 글로벌 테넌트 역할의 권한	202
권한 번들 관리	207
글로벌 테넌트 역할 관리	209
제공자 역할 관리	212
제공자 사용자 및 그룹 관리	214
제공자 사용자 관리	214
제공자그룹 관리	217

11 시스템 설정 관리 219

- 일반 시스템 설정 수정 219
- 일반 시스템 설정 220
- 시스템 e-메일 설정 구성 222
- vCloud Director 라이선스 변경 222
- 카탈로그 동기화 설정 구성 223
- 차단 작업 및 알림 구성 223
 - AMQP 브로커 구성 224
 - 차단 작업 설정 구성 225
- 공개 주소 구성 225
- ID 제공자 관리 227
 - LDAP 연결 관리 227
 - SAML ID 제공자를 사용하도록 시스템 구성 230
- 플러그인 관리 232
 - 플러그인 업로드 233
 - 플러그인 사용 또는 사용 안 함 233
 - 플러그인 제거 233
 - 조직에서 플러그인 게시/게시 취소 234
- vCloud Director 포털 사용자 지정 234
- 암호 정책 구성 236
- vSphere 서비스 구성 236

12 vCloud Director 모니터링 238

- vCloud Director 및 비용 보고 238
- 제공자 가상 데이터 센터에 대한 사용 정보 보기 239

13 서비스 관리 240

- vCloud Director와 vRealize Orchestrator 통합 240
 - vCloud Director에 vRealize Orchestrator 인스턴스 등록 241
- 서비스 범주 만들기 242
- 서비스 범주 편집 242
- 서비스 가져오기 243
- 서비스 검색 243
- 서비스 실행 244
- 서비스 범주 변경 245
- 서비스 등록 취소 245
- 서비스 게시 246

14 사용자 지정 엔터티 관리 247

사용자 지정 엔티티 검색	247
사용자 지정 엔티티 정의 편집	248
사용자 지정 엔티티 정의 추가	248
사용자 지정 엔티티 인스턴스	249
사용자 지정 엔티티에 작업 연결	249
사용자 지정 엔티티에서 작업 분리	250
사용자 지정 엔티티 게시	251
사용자 지정 엔티티 삭제	251

vCloud Director Service Provider Admin Portal 정보

1

"vCloud Director Service Provider Admin Portal 가이드"에서는 Service Provider Admin Portal 사용 방법에 대한 정보를 제공합니다. service provider admin portal을 사용하여 클라우드에서 조직, 권한, 역할, 사용자 및 그룹을 관리하고 모니터링할 수 있습니다. 또한 NSX-T 지원 조직 가상 데이터 센터 네트워크를 생성하고 관리할 수도 있습니다.

대상 사용자

이 가이드는 vCloud Director Service Provider Admin Portal에 제공된 기능을 사용하려는 서비스 제공자 관리자를 대상으로 합니다.

VMware 기술 자료 용어집

VMware 기술 자료 사이트에서는 익숙하지 않은 용어를 정리한 용어집을 제공하고 있습니다. VMware 기술 설명서에 사용된 용어에 대한 정의를 보려면 <https://docs.vmware.com>을 참조하십시오.

vCloud Director Service Provider Admin Portal 시작

2

vCloud Director Service Provider Admin Portal은 서비스 제공자 관리자를 위한 전용 인터페이스입니다.

본 장은 다음 항목을 포함합니다.

- [vCloud Director 관리 개요](#)
- [vCloud Director Service Provider Admin Portal에 로그인](#)
- [작업 보기](#)
- [진행 중인 작업 중지](#)
- [이벤트 보기](#)
- [이름 및 설명의 길이 제한](#)

vCloud Director 관리 개요

VMware vCloud Director를 사용하면 가상 인프라 리소스를 가상 데이터 센터에 풀링하고 웹 기반 포털 및 프로그래밍 방식 인터페이스를 통해 완전 자동화된 카탈로그 기반 서비스로 사용자에게 공개하여 안전한 다중 테넌트 클라우드를 구축할 수 있습니다.

"vCloud Director 서비스 제공자 관리자 포털 가이드"는 시스템에 리소스를 추가하고, 조직을 만들어 프로비저닝하고, 리소스 및 조직을 관리하고, 시스템을 모니터링하는 데 관련된 정보를 제공합니다.

vSphere 및 NSX 리소스

vCloud Director는 vSphere 리소스에 의존하여 가상 시스템 실행을 위한 CPU와 메모리를 제공합니다. 또한 vSphere 데이터스토어는 가상 시스템 파일과 가상 시스템 작업에 필요한 기타 파일을 위한 스토리지를 제공합니다. vCloud Director는 vSphere 분산 스위치, vSphere 포트 그룹 및 NSX Data Center for vSphere를 사용하여 가상 시스템 네트워킹도 지원합니다.

vCloud Director에서 NSX-T Data Center의 리소스를 사용할 수도 있습니다. 클라우드에 NSX-T Manager 인스턴스를 등록하는 방법에 대한 자세한 내용은 "vCloud Director 서비스 제공자 관리자 포털 가이드" 또는 "서비스 제공자를 위한 vCloud API 프로그래밍 가이드"의 내용을 참조하십시오.

기본 vSphere 및 NSX 리소스를 사용하여 클라우드 리소스를 만들 수 있습니다.

버전 9.7부터 vCloud Director가 HTTP 프록시 서버로 작동할 수 있기 때문에 조직에서 기본 vSphere 환경에 액세스가 가능하도록 설정할 수 있습니다.

클라우드 리소스

클라우드 리소스는 기본 vSphere 리소스의 추상화입니다. vCloud Director 가상 시스템 및 vApp에 대한 계산 및 메모리 리소스를 제공합니다. vApp은 운영 세부 정보를 정의하는 매개 변수가 있는 하나 이상의 개별 가상 시스템이 포함된 가상 시스템입니다. 클라우드 리소스는 스토리지 및 네트워크 연결에 대한 액세스도 제공합니다.

클라우드 리소스에는 제공자 및 조직 가상 데이터 센터, 외부 네트워크, 조직 가상 데이터 센터 네트워크 및 네트워크 풀이 포함됩니다.

vCloud Director에 클라우드 리소스를 추가하려면 먼저 vSphere 리소스를 추가해야 합니다.

전용 vCenter Server 인스턴스 및 프록시

전용 vCenter Server 인스턴스는 전체 vCenter Server 설치를 캡슐화하는 클라우드 리소스입니다. 전용 vCenter Server 인스턴스에는 기본 vSphere 환경의 다양한 구성 요소에 대한 액세스 지점인 프록시가 하나 이상 포함되어 있습니다. 제공자는 전용 vCenter Server 인스턴스와 프록시를 생성하고 사용하도록 설정할 수 있습니다. 제공자는 전용 vCenter Server 인스턴스를 테넌트에 게시할 수 있습니다.

전용 vCenter Server 인스턴스 및 프록시를 만들고 관리하려면 Service Provider Admin Portal이나 vCloud OpenAPI를 사용하면 됩니다. <https://code.vmware.com>에서 [장 9 전용 vCenter Server 인스턴스 및 프록시 관리](#) 및 "vCloud OpenAPI 시작하기" 항목을 참조하십시오.

제공자 가상 데이터 센터

제공자 가상 데이터 센터는 단일 vCenter Server 리소스 풀의 계산 및 메모리 리소스를 해당 리소스 풀에서 사용할 수 있는 하나 이상의 데이터스토어에 포함된 스토리지 리소스와 결합합니다.

제공자 가상 데이터 센터는 vCenter Server 인스턴스와 연결된 NSX Manager 인스턴스의 네트워크 리소스 또는 클라우드에 등록된 NSX-T Manager 인스턴스의 네트워크 리소스를 사용할 수 있습니다.

지리적 위치 또는 사업부가 서로 다르거나 성능 요구 사항이 서로 다른 여러 사용자를 위해 여러 개의 제공자 가상 데이터 센터를 생성할 수 있습니다.

조직 가상 데이터 센터

조직 가상 데이터 센터는 조직에 리소스를 제공하고 제공자 가상 데이터 센터에서 분할됩니다. 조직 가상 데이터 센터는 가상 시스템을 저장, 배포 및 운영할 수 있는 환경을 제공합니다. 플로피 디스크 및 CD ROM과 같은 가상 미디어용 스토리지도 제공합니다.

한 조직에 여러 개의 조직 가상 데이터 센터가 있을 수 있습니다.

vCloud Director 네트워킹

vCloud Director는 세 가지 유형의 네트워크를 지원합니다.

- 외부 네트워크

- 조직 가상 데이터 센터 네트워크
- vApp 네트워크

일부 조직 가상 데이터 센터 네트워크와 모든 vApp 네트워크는 네트워크 폴로 지원됩니다.

외부 네트워크

외부 네트워크는 vSphere 포트 그룹을 기반으로 구별되는 논리적 네트워크입니다. 조직 가상 데이터 센터 네트워크는 외부 네트워크에 연결하여 vApp 내부의 가상 시스템에 인터넷 연결을 제공할 수 있습니다.

9.5 버전부터 vCloud Director에서 IPv6 외부 네트워크가 지원됩니다. IPv6 외부 네트워크는 IPv4 및 IPv6 서브넷 모두를 지원하고 IPv4 외부 네트워크는 IPv4 및 IPv6 서브넷 모두를 지원합니다.

기본적으로 **시스템 관리자**만 외부 네트워크를 만들고 관리할 수 있습니다.

조직 가상 데이터 센터 네트워크

조직 가상 데이터 센터 네트워크는 vCloud Director 조직 가상 데이터 센터에 속하며 조직의 모든 vApp에 사용할 수 있습니다. 조직 가상 데이터 센터 네트워크를 사용하면 조직 내의 vApp이 서로 통신할 수 있습니다. 외부 연결을 제공하기 위해 조직 가상 데이터 센터 네트워크를 외부 네트워크에 연결할 수 있습니다. 조직 내부에 격리된 조직 가상 데이터 센터 네트워크를 만들 수도 있습니다.

vCloud Director 9.5에서는 직접 조직 및 라우팅된 조직 가상 데이터 센터 네트워크에 대한 IPv6 지원이 도입되었습니다.

vCloud Director 9.5부터는 **시스템 관리자**가 NSX-T 논리적 스위치로 지원되는 격리된 가상 데이터 센터 네트워크를 생성할 수 있습니다. **조직 관리자**는 네트워크 폴로 지원되는 격리된 가상 데이터 센터 네트워크를 만들 수 있습니다.

vCloud Director 9.5에는 가상 데이터 센터 그룹에 스트레치된 네트워크를 구성하여 크로스 가상 데이터 센터 네트워크도 도입되었습니다.

기본적으로 **시스템 관리자**만 직접 및 크로스 가상 데이터 센터 네트워크를 만들 수 있습니다. **시스템 관리자**와 **조직 관리자**는 조직 가상 데이터 센터 네트워크를 관리할 수 있습니다. 단, **조직 관리자**가 수행할 수 있는 작업에는 일부 제한이 있습니다.

vApp 네트워크

vApp 네트워크는 vApp에 속하며 vApp 네트워크를 사용하면 vApp의 가상 시스템이 서로 통신할 수 있습니다. vApp이 조직의 다른 vApp과 통신할 수 있도록 설정하려면 vApp 네트워크를 조직 가상 데이터 센터 네트워크에 연결하면 됩니다. 조직 가상 데이터 센터 네트워크가 외부 네트워크에 연결되어 있으면 vApp이 다른 조직의 vApp과 통신할 수 있습니다. vApp 네트워크는 네트워크 폴로 지원됩니다.

vApp에 대한 액세스 권한이 있는 대부분의 사용자는 자체 vApp 네트워크를 만들고 관리할 수 있습니다. vApp에서 네트워크 사용에 대한 자세한 내용은 "vCloud Director 테넌트 포털 가이드"의 내용을 참조하십시오.

네트워크 풀

네트워크 풀은 조직 가상 데이터 센터에서 사용할 수 있는 구별되지 않은 네트워크의 그룹입니다. 네트워크 풀은 VLAN ID 또는 포트 그룹과 같은 vSphere 네트워크 리소스를 통해 지원됩니다. vCloud Director는 네트워크 풀을 사용하여 NAT 라우팅 및 내부 조직 가상 데이터 센터 네트워크와 모든 vApp 네트워크를 만듭니다. 풀 내 각 네트워크의 네트워크 트래픽은 계층 2에서 다른 모든 네트워크와 격리됩니다.

vCloud Director의 각 조직 가상 데이터 센터에는 하나의 네트워크 풀이 있을 수 있습니다. 여러 조직 가상 데이터 센터가 하나의 네트워크 풀을 공유할 수 있습니다. 조직 가상 데이터 센터에 대한 네트워크 풀은 조직 가상 데이터 센터의 네트워크 할당량을 충족시키기 위해 생성된 네트워크를 제공합니다.

시스템 관리자만 네트워크 풀을 만들고 관리할 수 있습니다.

조직

vCloud Director는 조직을 사용하여 다중 테넌시를 지원합니다. 조직은 사용자, 그룹 및 계산 리소스 모음의 관리 단위입니다. 사용자는 조직 관리자가 해당 사용자를 만들거나 가져올 때 설정한 자격 증명을 제공하여 조직 수준에서 인증을 받습니다. **시스템 관리자**는 조직을 만들고 프로비저닝하는 반면 **조직 관리자**는 조직 사용자, 그룹 및 카탈로그를 관리합니다. **조직 관리자** 작업은 "vCloud Director 테넌트 포털 가이드"에 설명되어 있습니다.

사용자 및 그룹

조직에는 임의의 수의 사용자 및 그룹이 포함될 수 있습니다. **조직 관리자**는 사용자를 만들 수 있고, LDAP와 같은 디렉토리 서비스에서 사용자 및 그룹을 가져올 수 있습니다. **시스템 관리자**는 각 조직에 사용할 수 있는 권한 집합을 관리합니다. **시스템 관리자**는 글로벌 테넌트 역할을 만들어 하나 이상의 조직에 게시할 수 있습니다. **조직 관리자**는 조직에 로컬 역할을 만들 수 있습니다.

카탈로그

조직에서는 카탈로그를 사용하여 vApp 템플릿과 미디어 파일을 저장합니다. 카탈로그에 액세스할 수 있는 조직의 구성원은 포함된 vApp 템플릿과 미디어 파일을 사용하여 자체 vApp을 만들 수 있습니다. **시스템 관리자**는 다른 조직에서 사용할 수 있게 조직이 카탈로그를 게시하도록 허용할 수 있습니다. 그런 다음 **조직 관리자**가 조직의 사용자에게 제공할 카탈로그 항목을 결정할 수 있습니다.

vCloud Director Service Provider Admin Portal에 로그인

웹 브라우저를 사용하여 vCloud DirectorService Provider Admin Portal에 액세스할 수 있습니다.

사전 요구 사항

vCloud Director Service Provider Admin Portal에 액세스하려면 시스템 관리자 권한이 있어야 합니다.

절차

- 1 브라우저에 vCloud Director 사이트의 Service Provider Admin Portal URL을 입력하고 Enter 키를 누릅니다.

예를 들어 **https://vcloud.example.com/provider**를 입력합니다.

- 2 시스템 관리자 사용자 이름 및 암호로 로그인합니다.


작업 보기

Service Provider Admin Portal에서 최근 작업 및 해당 상태를 볼 수 있습니다.

작업 보기에서 서비스 제공자 관리자 포털의 작업 상태를 한 눈에 볼 수 있습니다. 이 보기에는 작업이 실행된 시기와 성공 여부가 표시됩니다. 환경에 문제가 발생한 경우 문제 해결의 첫 단계로 이 도구를 사용하는 것이 좋습니다.

작업 아이콘의 파란색 및 빨간색 정보 팁에는 실행된 작업과 실패한 작업의 수가 각각 표시됩니다.

절차

- ◆ 오른쪽 위 메뉴에서 작업 아이콘()을 선택합니다.

결과

최근 작업의 목록이 작업이 실행된 시간 및 작업의 상태와 함께 표시됩니다.

진행 중인 작업 중지

필요한 모든 설정을 검토하거나 적용하기 전에 실수로 작업을 시작한 경우에는 진행 중인 작업을 중지할 수 있습니다.

최근 작업 패널은 기본적으로 테넌트 포털의 맨 아래에 표시됩니다. 작업(예: 가상 시스템 만들기)을 시작하면 해당 작업이 패널에 표시됩니다.

사전 요구 사항

최근 작업 패널이 열려 있어야 합니다.

절차

- 1 장기 실행 작업을 시작합니다.

장기 실행 작업은 가상 시스템 또는 vApp 만들기, 가상 시스템 및 vApp에서 수행되는 전원 작업 등의 작업입니다.

- 2 **최근 작업** 패널에서 **취소** 아이콘()을 클릭합니다.

- 3 **작업 취소** 대화 상자에서 **확인**을 클릭하여 작업을 취소할 것임을 확인합니다.

결과


작업이 중지됩니다.

이벤트 보기


포털에서 모든 이벤트의 목록과 세부 정보 및 상태를 볼 수 있습니다.

이벤트 보기는 포털에서 이벤트 상태를 확인하는 방법입니다. 이 보기에는 이벤트가 발생한 시기와 성공 여부가 표시됩니다. 이벤트보기에는 사용자 로그인 및 개체 생성 또는 삭제와 같은 일회성 발생이 포함됩니다.

절차

- 1 기본 메뉴()에서 **이벤트**를 선택합니다.

이벤트가 발생한 시간 및 이벤트의 상태와 함께 모든 이벤트 목록이 표시됩니다.

- 2 편집기 아이콘()을 클릭하여 이벤트에 대해 표시할 세부 정보를 변경합니다.
- 3 (선택 사항) 이벤트를 클릭하여 이벤트 세부 정보를 확인합니다.

세부	설명
이벤트	이벤트의 이름입니다. 예를 들어 가상 시스템을 포함하도록 vApp을 수정하면 전체 작업을 시작하는 이벤트는 <i>Task 'Modify vApp' start</i> 입니다.
이벤트 ID	이벤트의 ID입니다.
유형	작업이 수행되는 개체입니다. 예를 들어, 가상 시스템 생성한 경우 형식은 <i>vm</i> 입니다.
대상	이벤트의 대상 개체입니다. 예를 들어, 가상 시스템을 포함하도록 vApp을 수정하는 경우 <i>Task 'Modify vApp' start</i> 이벤트의 대상은 <i>vdcUpdateVapp</i> 입니다.
상태	성공 또는 실패와 같은 이벤트의 상태입니다.
서비스 네임스페이스	<i>com.vmware.vcloud</i> 와 같은 서비스 이름입니다.
조직	조직의 이름입니다.
소유자	이벤트를 트리거한 사용자입니다.
발생 시간	이벤트가 발생한 날짜 및 시간입니다.

이름 및 설명의 길이 제한

vCloud Director에서 값을 입력할 때 다음 지침을 따릅니다.

name 특성과 **Description** 요소 및 **ComputerName** 요소의 문자열 값에는 연결 대상 개체에 따라 길이 제한이 적용됩니다.

표 2-1. 개체 속성의 길이 제한

개체	속성	최대 길이(문자 수)
Catalog	name	128
Catalog	Description	256
EdgeGateway	name	35
Media	name	128
Media	Description	256
VApp	name	128
VApp	Description	256
VAppTemplate	name	128
VAppTemplate	Description	256
Vdc	name	128
Vdc	Description	256
Vm	name	128
Vm	ComputerName	15(Windows), 63(다른 모든 플랫폼)
Vm	Description	256

vSphere 리소스 관리

3

vCloud Director는 기본 vSphere 가상 인프라에서 리소스를 가져옵니다. vCloud Director에 vSphere 리소스를 등록한 후에 vSphere 설치 내 조직이 사용할 수 있도록 리소스를 할당할 수 있습니다.

vCloud Director는 하나 이상의 vCenter Server 환경을 사용하여 가상 데이터 센터를 지원합니다. 버전 9.7부터 vCloud Director는 vCenter Server 환경을 사용하여 하나 이상의 프록시를 포함하는 SDDC를 캡슐화할 수도 있습니다. 이러한 프록시를 테넌트가 자체 vCloud Director 계정을 사용하여 vCloud Director에서 기본 vSphere 환경에 대한 액세스 지점으로 사용하도록 설정할 수 있습니다.

vCloud Director에서 vCenter Server 인스턴스를 사용하려면 먼저 이 vCenter Server 인스턴스를 연결해야 합니다.

연결된 vCenter Server 인스턴스에 의해 지원되는 제공자 가상 데이터 센터를 생성하면, 이 vCenter Server 인스턴스는 서비스 제공자에 게시된 것으로 표시되며, 제공자 범위에 있다고도 합니다. 제공자 가상 데이터 센터 생성에 대한 자세한 내용은 [제공자 가상 데이터 센터 생성](#) 항목을 참조하십시오.

연결된 vCenter Server 인스턴스를 캡슐화하는 SDDC를 생성하면 vCenter Server는 테넌트 전용으로 설정됩니다. 이 vCenter Server 인스턴스는 테넌트에 게시된 것으로 표시되며, 테넌트 범위에 있다고도 합니다. SDDC 만들기에 대한 자세한 내용은 [장 9 전용 vCenter Server 인스턴스 및 프록시 관리](#)의 내용을 참조하십시오.

참고 기본적으로, 연결된 vCenter Server 인스턴스로는 제공자 VDC 또는 전용 vCenter Server 인스턴스 중 하나를 만들 수 있습니다. vCenter Server 인스턴스에 의해 지원되는 제공자 VDC를 생성한 경우에는 이 vCenter Server 인스턴스를 사용하여 전용 vCenter Server 인스턴스를 생성할 수 없으며, 그 반대의 경우에도 마찬가지입니다.

본 장은 다음 항목을 포함합니다.

- [vCenter Server 및 NSX 리소스 추가](#)
- [클라우드 리소스 추가](#)
- [vCenter Server 인스턴스 보기](#)
- [vCenter Server 설정 수정](#)
- [vCenter Server 인스턴스 사용 또는 사용 안 함](#)
- [vCenter Server 인스턴스 다시 연결](#)

- [vCenter Server 인스턴스 새로 고침](#)
- [vCenter Server 인스턴스의 스토리지 정책 새로 고침](#)
- [vCenter Server 인스턴스 등록 취소](#)
- [NSX Manager 설정 수정](#)
- [NSX-T Manager 설정 수정](#)
- [NSX-T Manager 인스턴스 삭제](#)
- [다중 사이트 배포 구성 및 관리](#)
- [다중 사이트 리소스 목록](#)

vCenter Server 및 NSX 리소스 추가

vCloud Director는 vSphere 리소스에 의존하여 가상 시스템 실행을 위한 CPU, 메모리 및 스토리지를 제공합니다. 또한 버전 9.7부터 vCloud Director는 테넌트와 기본 vSphere 환경 사이에서 HTTP 서버로 작동할 수 있습니다.

vCloud Director 시스템 요구 사항 및 지원되는 vCenter Server와 ESXi 버전에 대한 자세한 내용은 http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php에서 "VMware 제품 상호 운용성 매트릭스"를 참조하십시오.

vCenter Server 인스턴스를 단독으로 또는 NSX Manager 인스턴스와 함께 연결

vCenter Server 인스턴스를 연결하면 해당 리소스를 vCloud Director에서 사용할 수 있습니다. vCenter Server 인스턴스와 이에 연결된 NSX Manager 인스턴스를 함께 연결할 수 있습니다. 전용 vCenter Server 인스턴스 또는 NSX-T Manager 인스턴스와 연결된 인스턴스에 대해 vCenter Server 인스턴스만 연결할 수 있습니다.

vCloud Director는 vCenter Server 인스턴스를 연결된 해당 NSX Manager 인스턴스 또는 NSX-T Manager 인스턴스와 함께 사용할 수 있습니다.

vCloud Director가 이 vCenter Server 인스턴스와 연결된 해당 NSX Manager 인스턴스를 사용하도록 하려면 vCenter Server 및 NSX Manager 인스턴스를 함께 연결해야 합니다.

vCloud Director가 이 vCenter Server 인스턴스와 NSX-T Manager 인스턴스를 사용하도록 하려면 vCenter Server 인스턴스만 연결해야 합니다. vCenter Server 인스턴스를 단독으로 연결한 후에는 [NSX-T Manager 인스턴스 등록](#) 작업을 수행해야 합니다.

참고 vCenter Server 인스턴스만 연결했다면 나중에 연결된 해당 NSX Manager 인스턴스를 추가할 수 없습니다. vCenter Server 인스턴스를 등록 취소하고 이를 연결된 해당 NSX Manager 인스턴스와 함께 다시 연결할 수 있습니다.

vCenter Server 인스턴스를 vCloud Director 환경의 아무 사이트에도 연결할 수 있습니다.

사전 요구 사항

- vCenter 및 vSphere SSO 인증서를 확인하도록 vCloud Director를 구성한 경우 vCenter Server 인증서를 vCloud Director에 업로드했는지 확인합니다. 일반 시스템 설정에 대한 자세한 내용은 [일반 시스템 설정 수정](#) 항목을 참조하십시오.
- NSX Manager 인증서를 확인하도록 vCloud Director를 구성한 경우 NSX Manager 인증서를 vCloud Director에 업로드했는지 확인합니다. 일반 시스템 설정에 대한 자세한 내용은 [일반 시스템 설정 수정](#) 항목을 참조하십시오.

절차

1 vCenter Server 인스턴스 추가

vCenter Server 인스턴스를 추가하려면 vCenter Server 액세스 세부 정보를 입력합니다.


2 (선택 사항) 연결된 NSX Manager 인스턴스 추가

vCloud Director가 이 vCenter Server 인스턴스와 연결된 해당 NSX Manager 인스턴스를 사용하도록 하려면 NSX Manager 액세스 세부 정보를 추가해야 합니다.

vCenter Server 인스턴스 추가

vCenter Server 인스턴스를 추가하려면 vCenter Server 액세스 세부 정보를 입력합니다.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 창에서 **vCenter**를 클릭하고 **추가**를 클릭합니다.
- 3 다중 사이트 vCloud Director 배포가 있는 경우 **사이트** 드롭다운 메뉴에서 이 vCenter Server 인스턴스를 추가할 사이트를 선택하고 **다음**을 클릭합니다.
- 4 vCloud Director에서 vCenter Server 인스턴스의 이름과 설명(선택 사항)을 입력합니다.
- 5 vCenter Server 인스턴스의 URL을 입력합니다.
기본 포트를 사용하는 경우 포트 번호를 생략할 수 있습니다. 사용자 지정 포트를 사용한다면 포트 번호를 포함합니다.
예를 들어 **https://FQDN_or_IP_address:<custom_port_number>**와 같이 입력할 수 있습니다.
- 6 vCenter Server **관리자** 계정의 사용자 이름 및 암호를 입력합니다.
- 7 (선택 사항) 등록 후 vCenter Server 인스턴스를 사용하지 않도록 설정하려면 **사용** 토글을 해제합니다.

8 vCenter Server Web Client의 URL을 구성합니다.

옵션	설명
vSphere 서비스를 사용하여 URL 제공	이 옵션을 사용하려면 vCloud API를 사용하여 vSphere Lookup Service를 사용하도록 vCloud Director를 구성해야 합니다.
vSphere Web Client URL	이 옵션을 사용하려면 vSphere Web Client의 URL을 입력해야 합니다. 예를 들어 https://example.vmware.com/vsphere-client 를 입력할 수 있습니다.

- 9 제공자 VDC로 사용되지 않을 테넌트 전용 vCenter Server를 추가하려면 **테넌트 액세스 사용** 토글을 설정합니다.

- 10 다음을 클릭합니다.

- 11 (선택 사항) vCenter Server 인스턴스에 연결된 NSX Manager 인스턴스를 추가하는 것을 건너뛰고 등록을 마칩니다.

vCloud Director가 이 vCenter Server 인스턴스를 NSX-T Manager 인스턴스와 함께 사용하게 하려면 vCenter Server 인스턴스만 추가해야 합니다.

참고 나중에 연결된 NSX Manager 인스턴스를 추가할 수 없습니다. vCenter Server 인스턴스를 등록 취소하고 이를 연결된 해당 NSX Manager 인스턴스와 함께 다시 연결할 수 있습니다.

- a **NSX-V Manager 설정** 페이지에서 **설정 구성** 토글을 해제하고 **다음**을 클릭합니다.

- b **완료 준비** 페이지에서 등록 세부 정보를 검토하고 **마침**을 클릭합니다.

(선택 사항) 연결된 NSX Manager 인스턴스 추가

vCloud Director가 이 vCenter Server 인스턴스와 연결된 해당 NSX Manager 인스턴스를 사용하도록 하려면 NSX Manager 액세스 세부 정보를 추가해야 합니다.

절차

- 1 **NSX-V Manager 설정** 페이지에서 **설정 구성** 토글을 설정한 상태로 둡니다.

- 2 NSX Manager 인스턴스의 URL을 입력합니다.

기본 포트를 사용하는 경우 포트 번호를 생략할 수 있습니다. 사용자 지정 포트를 사용한다면 포트 번호를 포함합니다.

예를 들어 **https://FQDN_or_IP_address:<custom_port_number>**와 같이 입력할 수 있습니다.

- 3 **NSX 관리자** 계정의 사용자 이름 및 암호를 입력합니다.

- 4 (선택 사항) 이 vCenter Server 인스턴스에서 지원하는 가상 데이터 센터에 대해 크로스 가상 데이터 센터 네트워킹을 사용하도록 설정하려면 **크로스 VDC 네트워킹** 토글을 설정하고 네트워크 제공자 범위에 대한 이름과 제어 VM 배포 속성을 입력합니다.

제어 VM 배포 속성은 범용 라우터 같은 크로스 가상 데이터 센터 네트워킹 구성 요소를 위한 장치를 NSX Manager 인스턴스에 배포하는 데 사용됩니다.

옵션	설명
리소스 풀 경로	vCenter Server 인스턴스의 특정 리소스 풀에 대한 계층 경로(클러스터에서 시작, <i>Cluster/Resource_Pool_Parent/Target_Resource</i>)입니다. 예: TestbedCluster1/mgmt-rp . 또는 리소스 풀의 관리 개체 참조 ID를 입력할 수 있습니다. 예: resgroup-1476 .
데이터스토어 이름	장치 파일을 호스팅할 데이터스토어의 이름입니다. 예: shared-disk-1 .
관리 인터페이스	HA DLR 관리 인터페이스에 사용되는 포트 그룹 또는 vCenter Server에 있는 네트워크의 이름입니다. 예: TestbedPG1 .
네트워크 제공자 범위	데이터 센터 그룹의 네트워크 토폴로지에서 네트워크 장애 도메인에 해당합니다. 예: boston-fault1 . 크로스 가상 데이터 센터 그룹 관리에 대한 자세한 내용은 "vCloud Director 테넌트 포털 가이드"의 내용을 참조하십시오.

- 5 **완료 준비** 페이지에서 등록 세부 정보를 검토하고 **마침**을 클릭합니다.

다음에 수행할 작업

- **vCenter Server에서 NSX 라이선스 키 할당.**
- **제공자 가상 데이터 센터 생성.**

vApp 검색 및 채택

기본 구성을 사용할 경우 조직 VDC는 VDC를 지원하는 모든 vCenter Server 리소스 풀에 생성된 VM을 검색합니다. 시스템에서는 검색된 각 VM(가상 시스템)을 포함하도록 시스템 관리자 소유의 간소화된 vApp을 구성합니다. 시스템 관리자가 검색된 vApp에 대한 액세스를 부여하면 vApp을 구성 또는 재구성하거나 vApp을 채택하고 가져오기 위해 수정할 때 검색된 vApp에 포함된 VM을 참조할 수 있습니다.

검색된 vApp에는 정확히 하나의 VM이 포함되며 vCloud Director에서 만들어진 vApp에는 적용되지 않는 몇 가지 제약 조건이 적용됩니다. 이러한 vApp은 채택 여부에 관계없이 vApp을 구성 또는 재구성할 때 사용할 수 있는 VM 소스로 유용합니다.

검색된 각 vApp에는 포함된 vCenter VM의 이름에서 파생된 이름과 조직의 관리자가 지정한 접두사가 지정됩니다.

vApp을 추가적으로 검색하려는 경우, 시스템 관리자가 vCloud API를 사용하여 제공자 VDC에서 사용 가능한 지정된 리소스 풀을 채택하는 조직 VDC를 만들 수 있습니다. 이러한 채택된 리소스 풀에 포함된 vCenter VM은 검색된 vApp으로 새 VDC에 나타나며 채택 후보입니다.

참고 IDE 하드 드라이브가 있는 가상 시스템은 전원이 꺼진 상태에서에서만 검색됩니다.

vCloud Director에서 하나 이상의 vCenter VM을 검색하지 못하면 vCenter Server VM 검색을 디버깅하여 가능한 이유를 조사할 수 있습니다. 자세한 내용은 "vCloud Director 설치, 구성 및 업그레이드 가이드"의 내용을 참조하십시오.

VM 검색 사용

VM 검색은 기본적으로 사용됩니다. VM 검색을 사용 안 함으로 설정하려면 시스템 관리자가 **시스템 설정 > 일반** 탭에서 **VM 검색 사용** 확인란을 선택 취소해야 합니다. 조직 관리자는 vCloud API를 사용하여 개별 VDC 또는 조직의 모든 VDC에 대해 VM 검색을 사용 안 함으로 설정할 수 있습니다.

검색된 vApp의 VM 사용

시스템 관리자가 검색된 vApp에 대한 액세스 권한을 부여한 후에는 다른 모든 vApp 또는 vApp 템플릿에 포함된 VM을 사용할 수 있는 것과 마찬가지로 해당 vApp의 VM을 사용할 수 있습니다. 예를 들어 새 vApp을 작성할 때 VM을 지정할 수 있습니다. 검색된 vApp을 복제하거나, 채택 프로세스를 트리거하지 않고 해당 이름, 설명 또는 리스 설정을 수정할 수도 있습니다.

검색된 vApp 채택

검색된 vApp은 vApp 네트워크를 변경하거나 vApp에 VM을 추가하여 채택할 수 있습니다. 검색된 vApp을 채택한 후 시스템에서는 해당 vApp을 가져와서 vCloud Director에서 생성된 것처럼 처리합니다. 채택된 vApp이 vCloud API 요청을 사용하여 검색된 경우 이름이 **autoNature**인 요소가 포함됩니다. 검색된 vApp이 채택되거나 vCloud Director에서 만든 vApp인 경우에는 이 요소의 값이 **false**입니다. 채택된 vApp은 검색된 vApp으로 되돌릴 수 없습니다.

검색된 vApp에 포함된 VM을 삭제하거나 이동하면 시스템에서는 해당 VM이 포함된 vApp도 제거합니다. 채택된 vApp에는 이 동작이 적용되지 않습니다.

검색된 vCenter VM을 포함하도록 만들어진 vApp은 VM을 vApp으로 수동으로 가져올 때 만드는 vApp과 유사하지만 간소화된 버전이기 때문에 VDC에 배포하기 전에 몇 가지 수정 작업이 필요합니다. 예를 들어 네트워킹 및 스토리지 속성을 편집하고 조직의 필요에 맞게 기타 사항을 조정해야 할 수 있습니다.

참고 가상 시스템을 채택하면 vCenter Server에 구성되어 있는 VM 예약, 제한 및 할당률 설정이 유지되지 않습니다. 가져온 가상 시스템에는 해당 시스템이 속해 있는 조직 가상 데이터 센터의 리소스 할당 설정이 적용됩니다.

vCenter Server에서 NSX 라이선스 키 할당

vCenter Server 인스턴스를 연결된 해당 NSX Manager 인스턴스와 연결한 경우 vSphere Client를 사용하여 vCloud Director 네트워킹을 지원하는 NSX Manager 인스턴스에 대한 라이선스 키를 할당해야 합니다.

사전 요구 사항

이 작업은 시스템 관리자만 수행할 수 있습니다.

절차

1 vCenter Server 시스템에 연결된 vSphere Client에서 **홈 > 라이선싱**을 선택합니다.

- 2 보고서 보기의 경우 **자산**을 선택합니다.
- 3 NSX Manager 자산을 마우스 오른쪽 버튼으로 클릭한 후 **라이선스 키 변경**을 선택합니다.
- 4 **새 라이선스 키 할당**을 선택하고 **키 입력**을 클릭합니다.
- 5 라이선스 키를 입력하고 키의 레이블(선택 사항)을 입력한 다음 **확인**을 클릭합니다.


vCloud Director를 구입했을 때 수신한 NSX Manager 라이선스 키를 사용합니다. 여러 vCenter Server 인스턴스에서 이 라이선스 키를 사용할 수 있습니다.

- 6 **확인**을 클릭합니다.

NSX-T Manager 인스턴스 등록

NSX-T Manager 인스턴스를 vCloud Director에 등록하여 vCloud Director가 해당 네트워크 리소스를 사용하도록 할 수 있습니다. 제공자 가상 데이터 센터는 NSX Data Center for vSphere 또는 NSX-T Data Center의 네트워크 리소스를 사용할 수 있습니다.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 창에서 **NSX-T Manager**를 클릭하고 **추가**를 클릭합니다.
- 3 다중 사이트 vCloud Director 배포가 있는 경우 **사이트** 드롭다운 메뉴에서 이 NSX-T Manager 인스턴스를 추가할 사이트를 선택하고 **다음**을 클릭합니다.
- 4 vCloud Director에서 NSX-T Manager 인스턴스의 이름과 설명(선택 사항)을 입력합니다.
- 5 NSX-T Manager 인스턴스의 URL을 입력합니다.
예를 들어 **https://FQDN_or_IP_address**와 같이 입력합니다.
- 6 NSX-T Manager **관리자** 계정의 사용자 이름 및 암호를 입력합니다.
- 7 **저장**을 클릭합니다.

다음에 수행할 작업

NSX-T Data Center에서 지원하는 제공자 가상 데이터 센터 생성에 대한 자세한 내용은 <https://code.vmware.com>에서 "서비스 제공자를 위한 vCloud API 프로그래밍 가이드"의 내용을 참조하십시오.

클라우드 리소스 추가

클라우드 리소스는 기본 vSphere 리소스를 추상화한 것으로, vCloud Director 가상 시스템과 vApp에 계산 및 메모리 리소스를 제공하고 스토리지 및 네트워크 연결에 액세스할 수 있게 해 줍니다.

클라우드 리소스에는 제공자 및 조직 가상 데이터 센터, 외부 네트워크, 조직 가상 데이터 센터 네트워크 및 네트워크 풀이 포함됩니다. vCloud Director에 클라우드 리소스를 추가하려면 먼저 vSphere 리소스를 추가해야 합니다.

조직 가상 데이터 센터에 대한 자세한 내용은 [장 6 조직 가상 데이터 센터 관리](#) 항목을 참조하십시오.

조직 가상 데이터 센터 네트워크에 대한 자세한 내용은 "vCloud Director 테넌트 포털 가이드" 에서 "조직 가상 데이터 센터 네트워크 관리" 장을 참조하십시오.

vCloud Director 9.7에 전체 vCenter Server 설치를 캡슐화하는 클라우드 리소스로 SDDC 또는 전용 vCenter Server 인스턴스가 도입되었습니다. 제공자는 전용 vCenter Server를 생성하고 사용하도록 설정하여 테넌트에 게시하고, 기본 vSphere 환경의 다양한 구성 요소에 프록시를 생성하여 사용하도록 설정할 수 있습니다. 전용 vCenter Server 인스턴스와 프록시를 생성하고 테넌트에 게시하고 관리하려면, Service Provider Admin Portal 또는 vCloud OpenAPI를 사용하면 됩니다. <https://code.vmware.com> 에서 [장 9 전용 vCenter Server 인스턴스 및 프록시 관리](#) 또는 "vCloud OpenAPI 시작하기" 항목을 참조하십시오.

제공자 가상 데이터 센터

제공자 VDC(가상 데이터 센터)는 vCenter Server 리소스 풀의 계산 및 메모리 리소스를 단일 vCenter Server 인스턴스의 스토리지 정책 하나 이상의 스토리지 리소스와 결합합니다. 네트워크 리소스의 경우, 제공자 VDC는 NSX Data Center for vSphere 또는 NSX-T Data Center를 사용할 수 있습니다.

- Service Provider Admin Portal 또는 vCloud API를 사용하여 연결된 vCenter Server 인스턴스와 관련 NSX Manager 인스턴스에 의해 지원되는 제공자 VDC를 생성하고 관리할 수 있습니다.
- Service Provider Admin Portal 또는 vCloud API를 사용하여 연결된 vCenter Server 인스턴스와 NSX-T Manager 인스턴스에 의해 지원되는 제공자 VDC를 생성하고 관리할 수 있습니다.

일반 vCloud Director 시스템에는 다양한 서비스 수준 요구 사항을 충족하도록 구성된 여러 제공자 VDC가 포함되어 있습니다. 각 제공자 VDC에는 기본 리소스 풀이 있습니다. 백업 vCenter Server 인스턴스에서 기본이 아닌 리소스 풀을 추가 및 제거할 수 있습니다. 기본 리소스 풀은 제거할 수 없습니다.

제공자 가상 데이터 센터 생성

vSphere 계산, 메모리 및 스토리지 리소스를 vCloud Director에서 사용할 수 있도록 하려면 제공자 VDC(가상 데이터 센터)를 생성합니다.

조직에서 VM 배포 또는 카탈로그 생성을 시작하려면 먼저 **시스템 관리자**가 제공자 VDC 및 해당 리소스를 사용하는 조직 VDC를 만들어야 합니다. 제공자 VDC와 제공자 VDC가 지원하는 조직 VDC의 관계는 서비스 오퍼링 범위, vSphere 인프라의 용량 및 지리적 분포 및 유사한 고려 사항을 기준으로 할 수 있는 관리 의사 결정입니다. 제공자 VDC는 테넌트가 사용할 수 있는 vSphere 용량 및 서비스를 제약하기 때문에 일반적으로 **시스템 관리자**는 성능, 용량 및 기능으로 측정되는 다양한 클래스의 서비스를 제공하는 제공자 VDC를 생성합니다. 그런 다음 지원 제공자 VDC의 구성으로 정의되는 특정 클래스의 서비스를 제공하는 조직 VDC를 테넌트에게 프로비저닝할 수 있습니다.

제공자 VDC를 만들기 전에 테넌트에 제공하려는 vSphere 기능 집합을 고려하십시오. 이러한 기능 중 일부는 제공자 VDC의 기본 리소스 풀에서 구현할 수 있습니다. 다른 기능을 사용하려면 [제공자 가상 데이터 센터에 리소스 풀 추가](#)에 설명된 대로 특별히 구성된 vSphere 클러스터를 기반으로 추가 리소스 풀을 만들어서 VDC에 추가해야 할 수 있습니다.

리소스 풀을 지원하는 클러스터의 호스트에 설치된 ESXi 릴리스의 범위는 제공자 VDC에서 지원하는 조직 VDC에 배포된 VM에서 사용할 수 있는 게스트 운영 체제 및 가상 하드웨어 버전의 집합을 결정합니다.


사전 요구 사항

- Service Provider Admin Portal에 **시스템 관리자**로 로그인합니다.
- 자동화된 DRS를 사용하도록 구성된 클러스터에 사용 가능한 용량이 있는 대상 기본 리소스 풀을 생성했는지 확인합니다. 리소스 풀은 하나의 제공자 VDC에 대해서만 사용할 수 있습니다. 리소스 풀을 생성하려면 vSphere Client를 사용하면 됩니다.

vSphere HA(High Availability)를 사용하는 클러스터에 속하는 리소스 풀을 사용하려면 vSphere HA에서 슬롯 크기가 계산되는 방법을 잘 알고 있어야 합니다. 슬롯 크기 및 vSphere HA 동작 사용자 지정에 대한 자세한 내용은 "vSphere 가용성" 설명서를 참조하십시오.

- 제공자 VDC의 네트워크 리소스에 대해 NSX Data Center for vSphere를 사용하는 경우:
 - 대상 기본 리소스 풀이 포함된 vCenter Server 인스턴스가 연결되어 있고 NSX Data Center for vSphere 라이선스 키가 있는지 확인합니다.
 - NSX Manager에서 VXLAN 인프라를 설정합니다. 관련 "NSX 관리 가이드"를 참조하십시오.
이 제공자 VDC에서 기본 VXLAN 네트워크 풀 대신 사용자 지정 VXLAN 네트워크 풀을 사용하려면 해당 네트워크 풀을 지금 만듭니다. [NSX Data Center for vSphere 전송 영역에서 지원되는 네트워크 풀 만들기](#)의 내용을 참조하십시오.
- 제공자 VDC의 네트워크 리소스에 대해 NSX-T Data Center를 사용하는 경우:
 - [NSX-T Data Center Tier-0 논리적 라우터](#)로 지원되는 외부 네트워크 추가
 - [NSX-T Data Center 전송 영역에서 지원되는 네트워크 풀 만들기](#)

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭합니다.
- 3 **새로 만들기**를 클릭합니다.
- 4 다중 사이트 vCloud Director 배포가 있는 경우 **사이트** 드롭다운 메뉴에서 이 제공자 VDC 인스턴스를 추가할 사이트를 선택하고 **다음**을 클릭합니다.
- 5 제공자 VDC의 이름과 설명(선택 사항)을 입력합니다.
이러한 텍스트 상자를 사용하여 이 제공자 VDC가 지원하는 조직 VDC가 사용할 수 있는 vSphere 기능(예: **vSphere HA** 또는 **IOPS를 지원하는 스토리지 정책**)을 나타낼 수 있습니다.
- 6 (선택 사항) 생성 시 제공자 VDC를 사용하지 않도록 설정하려면 **상태** 토글을 해제합니다.
사용하지 않도록 설정된 VDC의 계산 및 스토리지 리소스는 조직 VDC 생성에 사용할 수 없습니다.
- 7 **다음**을 클릭합니다.
- 8 제공자 VDC에 리소스 풀을 제공할 vCenter Server 인스턴스를 선택하고 **다음**을 클릭합니다.
이 페이지에는 vCloud Director에 등록된 vCenter Server 인스턴스가 나열됩니다. vCenter Server 인스턴스를 클릭하면 사용 가능한 리소스 풀이 표시됩니다.

9 이 제공자 VDC에 대한 기본 리소스 풀로 사용할 리소스 풀을 선택합니다.

하나의 리소스 풀은 하나의 제공자 VDC에 사용할 수 있습니다. 제공자 VDC에 리소스 풀을 추가하면 이 리소스 풀과 해당 상위 체인을 다른 제공자 VDC에서 선택할 수 없게 됩니다.

10 제공자 VDC가 지원할 최고 가상 하드웨어 버전을 선택하고 **다음**을 클릭합니다.

시스템은 리소스 풀을 지원하는 클러스터의 모든 호스트에서 지원되는 최고 가상 하드웨어 버전을 결정하여 **지원되는 최고 하드웨어 버전** 드롭다운 메뉴에서 기본값으로 제공합니다. 이 기본값을 사용하거나 메뉴에서 더 낮은 하드웨어 버전을 선택할 수 있습니다. 사용자가 지정한 버전은 이 제공자 VDC가 지원하는 조직 VDC에서 배포된 VM이 사용할 수 있는 최고 가상 하드웨어 버전이 됩니다. 더 낮은 가상 하드웨어 버전을 선택하는 경우 일부 게스트 운영 체제는 해당 VM에서 사용하도록 지원되지 않을 수 있습니다. 선택한 하드웨어 버전을 사용하여 제공자 VDC를 생성한 후에는 버전을 업그레이드할 수만 있고 다운그레이드할 수는 없습니다.

참고 제공자 VDC에 사용 가능한 하드웨어 버전은 대상 클러스터에 있는 가장 높은 버전의 ESXi 호스트에 따라 달라집니다. 지원되는 하드웨어 버전 중 가장 높은 ESXi 호스트를 선택할 수 없는 경우, vSphere Client에서 데이터 센터의 가상 시스템 생성에 대한 기본 호환성이 **데이터 센터 설정 및 호스트 버전 사용**으로 설정되어 있는지 확인합니다. 또한 기본 호환성 설정을 클러스터에 대해 원하는 가장 높은 하드웨어 버전으로 설정할 수도 있습니다.

vCloud Director 10.0에서 지원되는 가상 시스템 하드웨어의 최고 버전은 14입니다.

11 제공자 VDC에 대해 하나 이상의 스토리지 정책을 선택하고 **다음**을 클릭합니다.

선택한 리소스 풀이 지원하는 모든 vSphere 스토리지 정책이 나열됩니다.

중요 vCloud Director는 암호화 및 Storage I/O Control 등의 호스트 기반 데이터 서비스에 대한 VM 스토리지 정책을 지원하지 않습니다.

12 이 제공자 VDC에 대한 네트워크 풀을 구성합니다.

모든 제공자 VDC에는 네트워크 풀이 있어야 합니다. 시스템에서 기본 범위를 사용하여 네트워크 풀이 생성되도록 하거나, 특정 NSX Data Center for vSphere에 기반한 사용자 지정 VXLAN 또는 NSX-T Data Center 전송 영역을 기반으로 하는 Geneve 풀을 사용할 수 있습니다.

옵션	설명
기본 VXLAN 네트워크 풀 만들기	제공자 VDC에 대한 VXLAN 풀이 시스템에서 생성됩니다.
목록에서 VXLAN 네트워크 풀 선택	목록에서 네트워크 풀을 선택하면 특정 NSX 전송 영역을 기반으로 하는 사용자 지정 VXLAN 풀을 사용할 수 있습니다.
NSX-T Manager 및 Geneve 네트워크 풀 선택	목록에서 네트워크 풀을 선택하면 NSX-T Data Center 전송 영역이 지원하는 사용자 지정 VXLAN 풀을 사용할 수 있습니다.

13 선택 항목을 검토하고 **마침**을 클릭하여 제공자 VDC를 생성합니다.

다음에 수행할 작업

제공자 VDC가 일부 조직에 필요할 수 있는 전문 기능(예: Edge 클러스터, 신호도 그룹 및 특수 구성이 포함된 호스트)을 제공할 수 있도록 보조 리소스 풀을 추가할 수 있습니다. [제공자 가상 데이터 센터에 리소스 풀 추가](#)의 내용을 참조하십시오.

외부 네트워크

vCloud Director 외부 네트워크는 시스템의 네트워크와 가상 시스템을 VPN, 회사 인트라넷 또는 공용 인터넷과 같은 시스템 외부 네트워크에 연결하는 업링크 인터페이스를 제공합니다. 외부 네트워크는 **시스템 관리자**만 생성할 수 있습니다.

시스템에 vCenter Server 인스턴스가 둘 이상 등록되어 있으면 각각 vSphere 네트워크나 Tier-0 논리적 라우터로 지원되는 외부 네트워크를 여러 개 만들 수 있습니다.

vCloud Director는 IPv4 및 IPv6 외부 네트워크를 지원합니다.

참고 외부 네트워크를 생성할 때 정의한 IP 주소 범위는 Edge 게이트웨이나 이 네트워크에 직접 연결된 가상 시스템에 할당됩니다. 따라서, IP 주소는 vCloud Director 외부에서 사용하지 않아야 합니다.

vSphere 네트워크가 지원하는 외부 네트워크

외부 네트워크는 단일 vSphere 네트워크 또는 여러 vSphere 네트워크로 지원할 수 있습니다.

- 단일 vSphere 인스턴스가 지원하는 외부 네트워크.

vSphere 네트워크에서 겹치지 않는 IP 주소 집합을 외부 네트워크의 각 소비자에게 제공하려면 **시스템 관리자**가 기본 VLAN에서 IP 범위를 수동으로 구성해야 합니다.

- 여러 vSphere 네트워크가 지원하는 외부 네트워크.

외부 네트워크는 여러 vSphere 네트워크에서 지원될 수 있습니다. 이 방법을 사용하면 vCloud Director에서 IP 주소 관리를 간소화할 수 있습니다. 외부 네트워크의 속성을 수정하여 해당 네트워크 지원을 변경할 수 있습니다.

이런 유형의 네트워크에는 몇 가지 제약 조건이 있습니다.

- 네트워크에는 시스템에 등록된 vCloud Director 인스턴스마다 최대 하나의 지원 vSphere 네트워크가 있을 수 있습니다.
- 지원 네트워크 스위치는 모두 동일한 유형(vSphere Distributed Switch 또는 표준 스위치)이어야 합니다.

Tier-0 논리적 라우터로 지원되는 외부 네트워크

외부 네트워크는 NSX-T Data Center Tier-0 논리적 라우터로 지원될 수 있습니다.

vSphere 리소스에 의해 지원되는 외부 네트워크 추가


외부 네트워크를 추가하면 vCloud Director에서 사용할 vSphere 네트워크 리소스를 등록할 수 있습니다. 외부 네트워크에 연결되는 조직 VDC 네트워크를 만들 수 있습니다.

IPv4 또는 IPv6 외부 네트워크를 추가할 수 있습니다. IPv6 외부 네트워크는 IPv4 및 IPv6 서브넷 모두를 지원하고 IPv4 외부 네트워크는 IPv4 및 IPv6 서브넷 모두를 지원합니다.

사전 요구 사항

VLAN 트렁킹 사용 여부와 관계 없이 vSphere 포트 그룹을 사용할 수 있는지 확인합니다. 정적 포트 바인딩이 있는 탄력적 포트 그룹은 최적의 성능을 보장합니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **외부 네트워크**를 클릭하고 **새로 만들기**를 클릭합니다.
- 3 **vSphere 리소스**를 선택하고 네트워크를 지원할 포트 그룹 유형을 선택하고 **다음**을 클릭합니다.
- 4 새로운 외부 네트워크의 이름과 설명(선택 사항)을 입력합니다.
- 5 외부 네트워크를 지원할 포트 그룹을 선택하고 **다음**을 클릭합니다.
- 6 하나 이상의 서브넷을 구성하고 **다음**을 클릭합니다.
 - a 서브넷을 추가하려면 **추가**를 클릭합니다.
 - b 네트워크 CIDR(Classless Inter-Domain Routing) 설정을 입력합니다.
`network_gateway_IP_address/subnet_prefix_length` 형식(예: **192.167.1.1/24**)을 사용합니다.
 - c (선택 사항) DNS 설정을 입력합니다.
 - d 하나 이상의 IP 범위 또는 IP 주소를 추가하여 정적 IP 풀을 구성합니다.
 - e **확인**을 클릭합니다.
 - f (선택 사항) 다른 서브넷을 추가하려면 이 단계를 반복합니다.
- 7 네트워크 설정을 검토하고 **마침**을 클릭합니다.

다음에 수행할 작업

외부 네트워크에 연결하는 조직 VDC 네트워크를 만들 수 있습니다.

NSX-T Data Center Tier-0 논리적 라우터로 지원되는 외부 네트워크 추가


vCloud Director에서 사용할 NSX-T Data Center 네트워크 리소스를 등록하려면 Tier-0 논리적 라우터로 지원되는 외부 네트워크를 추가합니다.

절차

- 1 Tier-0 논리적 라우터를 생성합니다.
 - NSX-T Manager에서 Tier-0 라우터를 생성합니다.
 - a NSX-T Manager 인스턴스에 관리 권한으로 로그인합니다.

- b **네트워킹**을 클릭하고 **Tier-O 게이트웨이**를 클릭하고 **Tier-O 게이트웨이 추가**를 클릭합니다.
- c Tier-O 라우터의 이름을 입력합니다.
- d 고가용성 모드를 선택합니다.

참고 기본적으로 활성-활성 모드가 사용됩니다. 활성-활성 모드에서는 모든 멤버 간에 트래픽이 로드 밸런싱됩니다. 활성-대기 모드에서는 선택된 활성 멤버에 의해 트래픽이 처리됩니다. 활성 멤버에 오류가 발생하면 새 멤버가 활성 상태가 됩니다.

- e 드롭다운 메뉴에서 이 Tier-O 논리적 라우터를 지원할 기존 NSX-T Edge 클러스터를 선택하고 **저장**을 클릭합니다.
- NSX Policy API를 사용하여 Tier-O 논리적 라우터를 생성합니다.
- 2 vCloud Director Service Provider Admin Portal에 로그인합니다.
 - 3 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - 4 왼쪽 창에서 **외부 네트워크**를 클릭하고 **새로 만들기**를 클릭합니다.
 - 5 **NSX-T 리소스(Tier-O 라우터)**를 선택하고, 네트워크를 지원할 등록된 NSX-T Manager를 선택하고 **다음**을 클릭합니다.
 - 6 새로운 외부 네트워크의 이름과 설명(선택 사항)을 입력합니다.
 - 7 외부 네트워크에 연결할 Tier-O 라우터를 선택하고 **다음**을 클릭합니다.
 - 8 하나 이상의 서브넷을 구성하고 **다음**을 클릭합니다.
 - a 서브넷을 추가하려면 **추가**를 클릭합니다.
 - b 네트워크 CIDR(Classless Inter-Domain Routing) 설정을 입력합니다.
 - c (선택 사항) DNS 설정을 입력합니다.
 - d 하나 이상의 IP 범위 또는 IP 주소를 추가하여 정적 IP 풀을 구성합니다.
 - e **확인**을 클릭합니다.
 - f (선택 사항) 또 다른 서브넷을 추가하려면 8.a~8.e 단계를 반복합니다.
 - 9 네트워크 설정을 검토하고 **마침**을 클릭합니다.

다음에 수행할 작업

Tier-O 라우터를 사용하여 외부 네트워크에 대한 업링크를 생성합니다.

네트워크 풀

네트워크 풀은 조직 VDC에서 vApp 네트워크와 특정 유형의 조직 VDC 네트워크를 만드는 데 사용할 수 있는 구별되지 않은 네트워크 그룹입니다.

네트워크 풀은 VLAN ID 또는 포트 그룹과 같은 vSphere 네트워크 리소스, NSX Data Center for vSphere 리소스 또는 NSX-T Data Center 리소스를 통해 지원됩니다.

vCloud Director는 네트워크 풀을 사용하여 NAT 라우팅 및 내부 조직 VDC 네트워크와 모든 vApp 네트워크를 만듭니다. 풀 내 각 네트워크의 네트워크 트래픽은 계층 2에서 다른 모든 네트워크와 격리됩니다.

vCloud Director의 각 조직 VDC에는 하나의 네트워크 풀이 있을 수 있습니다. 여러 조직 VDC는 네트워크 풀을 공유할 수 있습니다. 조직 VDC에 대한 네트워크 풀은 조직 VDC의 네트워크 할당량을 충족시키기 위해 생성된 네트워크를 제공합니다.

VXLAN 네트워크 풀

NSX Data Center for vSphere에서 지원하는 모든 제공자 VDC에는 VXLAN 네트워크 풀이 포함됩니다.

NSX Data Center for vSphere가 지원하는 제공자 VDC를 생성할 때, 해당 제공자 VDC를 기존 VXLAN 네트워크 풀과 연결하거나 제공자 VDC에 대한 VXLAN 네트워크 풀을 생성할 수 있습니다.

새로 생성된 VXLAN 네트워크 풀에는 포함된 제공자 VDC 이름에서 파생된 이름이 지정되어 생성 시 연결됩니다. 이 네트워크 풀은 삭제하거나 수정할 수 없습니다. 제공자 VDC 이름을 바꾸면 해당 VXLAN 네트워크 풀의 이름도 자동으로 바뀝니다.

참고 인프라 전체에서 최적의 네트워크 성능을 보장하려면 VXLAN 네트워크 풀을 하나 생성하여 모든 제공자 VDC를 생성할 때 연결합니다.

vCloud Director VXLAN 네트워크는 IETF VXLAN 표준을 기반으로 하며 다양한 이점을 제공합니다.

- 논리 네트워크가 계층 3의 경계에 걸쳐 있습니다.
- 논리 네트워크가 단일 계층 2의 여러 랙에 걸쳐 있습니다.
- 브로드캐스트를 제약합니다.
- 성능이 매우 우수합니다.
- 규모가 상당합니다(최대 1600만 개 네트워크 주소 제공).

vCloud Director 환경의 VXLAN 네트워크에 대한 자세한 내용은 "NSX 관리 가이드"를 참조하십시오.


NSX Data Center for vSphere 전송 영역에서 지원되는 네트워크 풀 만들기

vCloud Director에서 사용할 NSX Data Center for vSphere 전송 영역을 등록하려면 VXLAN 지원형 네트워크 풀을 추가합니다.

사전 요구 사항

vCloud Director에 등록된 vCenter Server에서 NSX Data Center for vSphere 전송 영역을 만듭니다. "NSX 관리 가이드"를 참조하십시오.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **네트워크 풀**을 클릭하고 **새로 만들기**를 클릭합니다.
- 3 새 네트워크 풀의 이름과 설명(선택 사항)을 입력하고 **다음**을 클릭합니다.

4 VXLAN 지원형을 선택하고 **다음**을 클릭합니다.

5 이 네트워크 풀에서 사용할 **VXLAN** 전송 영역을 지정하는 vCenter Server 인스턴스를 선택하고 **다음**을 클릭합니다.

6 새 네트워크 풀을 지원할 **NSX Data Center for vSphere** 전송 영역을 선택하고 **다음**을 클릭합니다.

참고 크로스 가상 데이터 센터 네트워킹을 위한 범용 네트워크 풀을 만들려면 **UNIVERSAL_VXLAN** 유형 전송 영역을 선택합니다.

7 네트워크 풀 설정을 검토하고 **마침**을 클릭합니다.

다음에 수행할 작업

네트워크 풀에서 지원되는 조직 VDC 네트워크를 만들거나 네트워크 풀을 조직 VDC에 연결하고 vApp 네트워크를 만듭니다.

Geneve 네트워크 풀

NSX-T Data Center가 지원하는 모든 제공자 VDC에는 **Geneve** 네트워크 풀이 포함됩니다.

Geneve는 NSX-T Data Center에서 오버레이 기능을 제공하는 네트워크 가상화 표준입니다.

NSX-T Data Center가 지원하는 제공자 VDC를 생성할 때, 해당 제공자 VDC를 기존 **Geneve** 네트워크 풀과 연결하거나 제공자 VDC에 대한 **Geneve** 네트워크 풀을 생성할 수 있습니다.

vCloud Director Geneve 네트워크는 여러 가지 이점을 제공합니다.

- 논리 네트워크가 계층 3의 경계에 걸쳐 있습니다.
- 논리 네트워크가 단일 계층 2의 여러 랙에 걸쳐 있습니다.
- 브로드캐스트를 제약합니다.
- 성능이 매우 우수합니다.
- 규모가 상당합니다(최대 1600만 개 네트워크 주소 제공).


NSX-T Data Center 전송 영역에서 지원되는 네트워크 풀 만들기

vCloud Director에서 사용할 NSX-T Data Center 전송 영역을 등록하려면 **Geneve** 지원형 네트워크 풀을 만듭니다.

사전 요구 사항

오버레이가 지원되는 NSX-T Data Center 전송 영역을 생성합니다. 전송 영역 생성 및 Geneve(Generic Network Virtualization Encapsulation) 오버레이에 대한 자세한 내용은 "NSX-T Data Center 제품 설명서"를 참조하십시오.

절차

1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.

2 왼쪽 패널에서 **네트워크 풀**을 클릭하고 **새로 만들기**를 클릭합니다.

- 3 새 네트워크 풀의 이름과 설명(선택 사항)을 입력하고 **다음**을 클릭합니다.
- 4 **Geneve 지원형**을 선택하고 **다음**을 클릭합니다.
- 5 이 네트워크 풀에 대한 전송 영역을 제공할 **NSX-T Manager** 인스턴스를 선택하고 **다음**을 클릭합니다.
- 6 **NSX-T** 전송 영역을 선택하고 **다음**을 클릭합니다.
- 7 네트워크 풀 설정을 검토하고 **마침**을 클릭합니다.

다음에 수행할 작업

네트워크 풀에서 지원되는 조직 VDC 네트워크를 만들거나 네트워크 풀을 조직 VDC에 연결하고 vApp 네트워크를 만듭니다.

VLAN ID에 의해 지원되는 네트워크 풀 만들기


vCloud Director에서 사용할 vSphere VLAN ID를 등록하려면 VLAN 지원형 네트워크 풀을 추가합니다. VLAN 지원형 네트워크 풀은 조직 VDC 네트워크를 위한 보안, 확장성 및 성능을 제공합니다.

사전 요구 사항

vSphere에서 일정 범위의 VLAN ID와 한 개의 vSphere 분산 스위치를 사용할 수 있는지 확인합니다. VLAN ID는 ESXi 서버가 연결되어 있는 물리적 스위치에서 구성된 유효한 ID여야 합니다.

경고 VLAN은 계층 2 수준에서 격리되어야 합니다. VLAN이 제대로 격리되지 않으면 네트워크에서 중단이 발생할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **네트워크 풀**을 클릭하고 **새로 만들기**를 클릭합니다.
- 3 새 네트워크 풀의 이름과 설명(선택 사항)을 입력하고 **다음**을 클릭합니다.
- 4 **VLAN 지원형**을 선택하고 **다음**을 클릭합니다.
- 5 이 네트워크 풀에서 사용할 분산 가상 스위치를 지정하는 vCenter Server 인스턴스를 선택하고 **다음**을 클릭합니다.
- 6 VLAN ID 범위를 입력하고 **다음**을 클릭합니다.
- 7 네트워크 풀에 대한 분산 스위치를 선택하고 **다음**을 클릭합니다.
- 8 네트워크 풀 설정을 검토하고 **마침**을 클릭합니다.

다음에 수행할 작업

네트워크 풀에서 지원되는 조직 VDC 네트워크를 만들거나 네트워크 풀을 조직 VDC에 연결하고 vApp 네트워크를 만듭니다.

vSphere 포트 그룹에 의해 지원되는 네트워크 풀 만들기


vSphere에서 사용할 vCloud Director 포트 그룹을 등록하려면 포트 그룹에서 지원하는 네트워크 풀을 추가합니다. 다른 유형의 네트워크 풀과 달리, 포트 그룹 지원형 네트워크 풀에는 vSphere 분산 스위치가 필요하지 않고 타사 분산 스위치와 연결된 포트 그룹을 지원할 수 있습니다.

경고 포트 그룹은 계층 2에서 다른 모든 포트 그룹과 격리해야 합니다. 포트 그룹은 물리적으로 격리하거나 VLAN 태그를 사용하여 격리해야 합니다. 포트 그룹을 제대로 격리하지 못할 경우 네트워크 중단이 발생할 수 있습니다.

사전 요구 사항

vSphere 환경에서 하나 이상의 포트 그룹을 사용할 수 있는지 확인합니다. 포트 그룹은 클러스터의 각 ESXi 호스트에서 사용할 수 있어야 하며 각 포트 그룹에서 단일 VLAN만 사용해야 합니다. VLAN 트렁킹 유무에 관계없이 포트 그룹이 지원됩니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **네트워크 풀**을 클릭하고 **새로 만들기**를 클릭합니다.
- 3 새 네트워크 풀의 이름과 설명(선택 사항)을 입력하고 **다음**을 클릭합니다.
- 4 **포트 그룹 지원형**을 선택하고 **다음**을 클릭합니다.
- 5 이 네트워크 풀에서 사용할 포트 그룹을 제공하는 vCenter Server 인스턴스를 선택하고 **다음**을 클릭합니다.
- 6 포트 그룹을 하나 이상 선택하고 **다음**을 클릭합니다.
포트 그룹마다 네트워크를 하나씩 만들 수 있습니다.
- 7 네트워크 풀 설정을 검토하고 **마침**을 클릭합니다.


다음에 수행할 작업

네트워크 풀에서 지원되는 조직 VDC 네트워크를 만들거나 네트워크 풀을 조직 VDC에 연결하고 vApp 네트워크를 만듭니다.

vCenter Server 인스턴스 보기

vCloud Director 설치의 모든 사이트에 있는 vCenter Server 인스턴스 목록을 볼 수 있습니다. vCloud Director가 각 vCenter Server 인스턴스를 사용하는 방법을 볼 수 있습니다.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **vCenter**를 클릭합니다.

결과

연결된 모든 vCenter Server 인스턴스 목록이 표시됩니다. 이 목록에는 각 vCenter Server 인스턴스에 대한 다음과 같은 정보가 포함되어 있습니다.


	설명
이름	vCloud Director에 있는 vCenter Server 인스턴스의 이름입니다.
상태	vCenter Server 상태는 정상, 주의 및 위험입니다.
상태	사용 또는 사용 안 함. vCenter Server 인스턴스 사용 또는 사용 안 함 의 내용을 참조하십시오.
연결	vCloud Director에 연결되어 있는지 여부입니다. vCenter Server 인스턴스 다시 연결 의 내용을 참조하십시오.
VC 호스트	vCenter Server 인스턴스의 FQDN입니다.
버전	vCenter Server 버전입니다.
사용량	전용 vCenter Server 인스턴스가 테넌트 액세스를 사용하도록 설정했습니다. 제공자가 여러 제공자 VDC에서 공유 vCenter Server 인스턴스의 여러 리소스 풀을 사용한 다음 해당 리소스 풀을 서로 다른 테넌트에 할당할 수 있습니다. 장 9 전용 vCenter Server 인스턴스 및 프록시 관리 의 내용을 참조하십시오.
클러스터 상태	vCenter Server 인스턴스에 있는 모든 클러스터의 상태에 대한 집계입니다. 클러스터의 상태를 집계할 때 정상과 가장 거리가 먼 클러스터의 상태가 표시됩니다.
클러스터	vCenter Server 인스턴스의 클러스터 수입니다.
VM	vCenter Server 인스턴스의 VM 수입니다.
실행 중인 VM	vCenter Server 인스턴스의 실행 중인 VM 수입니다.
CPU	활발하게 사용되는 가상 CPU의 양이며, 사용 가능한 총 vCenter Server CPU의 백분율로 표시됩니다.
메모리	활발하게 사용되는 가상 메모리의 양이며, 사용 가능한 총 vCenter Server 메모리의 백분율로 표시됩니다.
스토리지	활발하게 사용되는 가상 스토리지의 양이며, 사용 가능한 총 vCenter Server 스토리지의 백분율로 표시됩니다.

vCenter Server 설정 수정

연결된 vCenter Server 인스턴스에 대한 연결 정보가 변경되거나 vCloud Director에서 그 이름과 설명을 변경하려는 경우 해당 설정을 수정할 수 있습니다.

vCenter Server 인스턴스를 추가할 때 구성한 설정을 수정할 수 있습니다. [vCenter Server 인스턴스 추가](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 창에서 **vCenter**를 클릭하고 수정할 vCenter Server 인스턴스의 이름을 클릭합니다.
- 3 **vCenter 정보** 섹션의 오른쪽 위에서 **편집**을 클릭합니다.
- 4 vCenter Server 설정을 편집하고 **저장**을 클릭합니다.


다음에 수행할 작업

연결 정보를 수정한 경우 **vCenter Server 인스턴스 다시 연결** 작업을 수행해야 합니다.

vCenter Server 인스턴스 사용 또는 사용 안 함

vCenter Server 인스턴스에 대한 유지 보수 또는 등록 취소를 수행하기 전에 대상 vCenter Server 인스턴스를 사용하지 않도록 설정해야 합니다. 해당 리소스를 vCloud Director의 가상 데이터 센터에 제공하려면 vCenter Server 인스턴스를 사용하도록 설정해야 합니다.

절차


- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **vCenter**를 클릭합니다.
- 3 대상 vCenter Server 인스턴스의 이름 옆에 있는 라디오 버튼을 클릭하고 **사용** 또는 **사용 안 함**을 클릭합니다.
- 4 **확인**을 클릭하여 확인합니다.

vCenter Server 인스턴스 다시 연결

vCenter Server 인스턴스의 연결이 끊긴 것으로 나타나거나 연결 설정을 수정한 경우 연결 재설정을 시도할 수 있습니다.

참고 새 연결을 설정하는 동안에는 vCenter Server 인스턴스를 작업에 사용할 수 없습니다.


절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **vCenter**를 클릭합니다.
- 3 대상 vCenter Server 인스턴스의 이름 옆에 있는 라디오 버튼을 클릭하고 **다시 연결**을 클릭합니다.
- 4 **확인**을 클릭하여 확인합니다.

vCenter Server 인스턴스 새로 고침

vCloud Director 데이터베이스에서 기본 vCenter Server 리소스에 대한 정보를 업데이트하려면 vCenter Server 인스턴스를 새로 고쳐야 합니다.


절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **vCenter**를 클릭합니다.
- 3 대상 vCenter Server 인스턴스의 이름 옆에 있는 라디오 버튼을 클릭하고 **새로 고침**을 클릭합니다.
- 4 **확인**을 클릭하여 확인합니다.

vCenter Server 인스턴스의 스토리지 정책 새로 고침

vCloud Director 데이터베이스에서 기본 vSphere 환경의 VM 스토리지 정책에 대한 정보를 업데이트하려면 vCenter Server 인스턴스의 스토리지 정책을 새로 고쳐야 합니다.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **vCenter**를 클릭합니다.
- 3 대상 vCenter Server 인스턴스의 이름 옆에 있는 라디오 버튼을 클릭하고 **정책 새로 고침**을 클릭합니다.
- 4 **확인**을 클릭하여 확인합니다.


vCenter Server 인스턴스 등록 취소

vCenter Server 인스턴스의 리소스 사용을 중지하려면 vCloud Director 설치에서 이 vCenter Server 인스턴스를 제거하면 됩니다.

사전 요구 사항

- vCenter Server 인스턴스를 사용하지 않도록 설정합니다. [vCenter Server 인스턴스 사용 또는 사용 안 함](#)의 내용을 참조하십시오.
- 이 vCenter Server 인스턴스의 리소스 풀을 사용하는 모든 제공자 가상 데이터 센터를 삭제합니다. [제공자 가상 데이터 센터 삭제](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **vCenter**를 클릭합니다.
- 3 대상 vCenter Server 인스턴스의 이름 옆에 있는 라디오 버튼을 클릭하고 **등록 취소**를 클릭합니다.


4 **확인**을 클릭하여 확인합니다.

NSX Manager 설정 수정

등록된 NSX Manager 인스턴스에 대한 연결 정보가 변경되거나 vCloud Director에서 그 이름과 설명을 변경하려는 경우 해당 설정을 수정할 수 있습니다.

NSX Manager 인스턴스를 추가할 때 구성한 설정을 수정할 수 있습니다. [\(선택 사항\) 연결된 NSX Manager 인스턴스 추가](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 창에서 **vCenter**를 클릭하고 대상 NSX Manager 인스턴스에 연결된 vCenter Server 인스턴스의 이름을 클릭합니다.
- 3 **NSX-V Manager 정보** 섹션의 오른쪽 위에서 **편집**을 클릭합니다.
- 4 NSX Manager 호스트 이름 및 관리자 자격 증명을 수정하고 **저장**을 클릭합니다.
- 5 (선택 사항) 이 vCenter Server 인스턴스에서 지원하는 가상 데이터 센터에 대해 크로스 가상 데이터 센터 네트워킹을 사용하도록 설정하려면 토글을 설정한 후 네트워크 제공자 범위에 대한 이름과 제어 VM 속성을 입력합니다.

제어 VM 속성은 크로스 가상 데이터 센터 네트워킹 구성 요소(예: 범용 라우터)를 위한 NSX Manager 인스턴스에 장치를 배포하는 데 사용됩니다.


매개 변수	설명
리소스 풀 경로	vCenter Server 인스턴스의 특정 리소스 풀에 대한 계층 경로(클러스터에서 시작, <i>Cluster/Resource_Pool_Parent/Target_Resource</i>)입니다. 예: TestbedCluster1/mgmt-rp . 또는 리소스 풀의 관리 개체 참조 ID를 입력할 수 있습니다. 예: resgroup-1476 .
데이터스토어 이름	장치 파일을 호스팅할 데이터스토어의 이름입니다. 예: shared-disk-1 .
관리 인터페이스	HA DLR 관리 인터페이스에 사용되는 포트 그룹 또는 vCenter Server에 있는 네트워크의 이름입니다. 예: TestbedPG1 .
네트워크 제공자 범위	데이터 센터 그룹의 네트워크 토폴로지에서 네트워크 장애 도메인에 해당합니다. 예: boston-fault1 . 크로스 가상 데이터 센터 그룹 관리에 대한 자세한 내용은 "vCloud Director 테넌트 포털 가이드"의 내용을 참조하십시오.

NSX-T Manager 설정 수정

등록된 NSX-T Manager 인스턴스에 대한 연결 정보가 변경되거나 vCloud Director에서 그 이름과 설명을 변경하려는 경우 해당 설정을 수정할 수 있습니다.

vCenter Server 인스턴스를 추가할 때 구성한 설정을 수정할 수 있습니다. [NSX-T Manager 인스턴스 등록](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 창에서 **NSX-T Manager**를 클릭하고 수정할 NSX-T Manager 인스턴스의 이름을 클릭합니다.
- 3 **일반** 탭의 오른쪽 위에서 **편집**을 클릭합니다.
- 4 NSX-T Manager 설정을 편집하고 **저장**을 클릭합니다.


NSX-T Manager 인스턴스 삭제

NSX-T Manager 인스턴스의 리소스 사용을 중지하려면 vCloud Director 설치에서 이 vCenter Server 인스턴스를 제거하면 됩니다.

사전 요구 사항

이 NSX-T Manager 인스턴스의 리소스를 사용하는 모든 제공자 가상 데이터 센터를 삭제합니다. [제공자 가상 데이터 센터 삭제](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 창에서 **NSX-T Manager**를 클릭합니다.
- 3 제거할 NSX-T Manager 인스턴스의 이름 옆에 있는 라디오 버튼을 클릭하고 **삭제**를 클릭합니다.
- 4 **삭제**를 클릭하여 확인합니다.

다중 사이트 배포 구성 및 관리

vCloud Director 다중 사이트 기능을 사용하면 지리적으로 분산된 여러 vCloud Director 설치(서버 그룹)의 서비스 제공자 또는 테넌트가 해당 설치 및 조직을 단일 엔티티로 관리하고 모니터링할 수 있습니다.

두 개의 vCloud Director 사이트를 연결하는 경우 단일 엔티티로 사이트 관리를 사용하도록 설정합니다. 또한 해당 사이트의 조직이 서로 간에 연결을 구성하도록 설정합니다. 조직이 연결의 구성원일 때 조직 사용자는 각 구성원 조직과 해당 자산이 조직에서 사용하는 사이트에 대해 로컬인 경우에도 vCloud Director Tenant Portal을 사용하여 모든 구성원 사이트의 조직 자산에 액세스할 수 있습니다.

참고 사이트를 연결하려면 vCloud API를 사용해야 합니다. 두 사이트가 연결된 후 vCloud API 또는 vCloud Director Tenant Portal을 사용하여 해당 사이트에 위치한 조직을 연결할 수 있습니다. 자세한 내용은 "서비스 제공자를 위한 vCloud API 프로그래밍 가이드" 및 "vCloud Director 테넌트 포털 가이드" 항목을 참조하십시오.

사이트 또는 조직은 피어와 무제한 연결을 구성할 수 있지만 각 연결에는 정확히 두 개의 멤버가 포함됩니다. 각 사이트 또는 조직에는 고유한 개인 키가 있어야 합니다. 연결 구성원은 한 구성원에서 다른 구성원 간에 서명된 요청을 확인하는 데 사용되는 공용 키를 교환하여 신뢰 관계를 설정합니다.

연결의 각 사이트는 vCloud Director 서버 그룹(vCloud Director 데이터베이스를 공유하는 서버 그룹)의 범위로 정의됩니다. 연결의 각 조직은 단일 사이트를 사용합니다. 조직 관리자는 조직 사용자 및 그룹의 각 멤버 사이트의 자산에 대한 액세스를 제어합니다.

사이트 개체 및 사이트 연결

설치 또는 업그레이드 프로세스는 로컬 vCloud Director 서버 그룹을 나타내는 **Site** 개체를 생성합니다. 두 개 이상의 vCloud Director 서버 그룹으로 확장되는 인증이 있는 시스템 관리자는 이러한 서버 그룹을 vCloud Director 사이트의 연결로 구성할 수 있습니다.

조직의 연결

사이트 연결이 완료된 후 임의의 멤버 사이트의 조직 관리자가 조직 연결을 시작할 수 있습니다.

참고 System 조직을 테넌트 조직과 연결할 수 없습니다. 임의의 사이트의 System 조직은 다른 사이트의 System 조직하고만 연결할 수 있습니다.

사용자 및 그룹 ID

사이트 및 조직이 연결되려면 동일한 IDP(ID 제공자)를 사용하는 데 동의해야 합니다. 연결의 모든 조직에 대한 사용자 및 그룹 ID는 이 IDP를 통해 관리되어야 합니다.

vCloud Director 통합 IDP를 사용해야 하는 시스템 조직 이외의 모든 연결은 가장 알맞은 IDP를 자유롭게 선택할 수 있습니다.

조직 사용자 및 그룹에 대한 사이트 액세스 제어

조직 관리자는 모든 멤버 사이트에서 유효하거나 하위 집합의 멤버 사이트에서만 유효한 사용자 또는 그룹 액세스 토큰을 생성하도록 IDP를 구성할 수 있습니다. 사용자 및 그룹 ID는 모든 멤버 조직에서 동일해야 하지만 사용자 및 그룹 권한은 각 멤버 조직에서 해당 사용자와 그룹에 할당된 역할로 제한됩니다. 사용자 또는 그룹에 할당된 역할은 멤버 조직에만 로컬로 적용되며, 생성하는 모든 사용자 지정 역할도 마찬가지입니다.

로드 밸런서 요구 사항

다중 사이트 배포를 효과적으로 구현하려면 <https://vcloud.example.com>과 같은 기관 끝점에 도달하는 요청을 사이트 연결의 각 구성원에 대한 끝점(예: <https://us.vcloud.example.com> 및 <https://uk.vcloud.example.com>)으로 분산하는 로드 밸런서를 구성합니다. 또한 사이트에 둘 이상의 셀이 있는 경우 모든 셀에 수신 요청을 분산하는 로드 밸런서를 구성하여 <https://us.vcloud.example.com>에 대한 요청이 <https://cell1.us.vcloud.example.com>, <https://cell2.us.vcloud.example.com> 등에 의해 처리될 수 있도록 해야 합니다.

연결 구성원 상태

사이트 또는 조직의 연결을 만든 후 로컬 시스템은 정기적으로 각 원격 연결 구성원의 상태를 검색하고 로컬 사이트의 vCloud Director 데이터베이스에서 상태를 업데이트합니다. 구성원 상태는

SiteAssociationMember 또는 OrgAssociationMember의 Status 요소에 표시됩니다. 이 요소에는 다음 3개 값 중 하나가 포함될 수 있습니다.

ACTIVE

연결이 두 상대방에 의해 설정되었으며 원격 상대방과의 통신이 성공했습니다.

ASYMMETRIC

연결이 로컬 사이트에서 설정되었지만 원격 사이트가 아직 응답하지 않았습니다.

UNREACHABLE

연결이 두 상대방에 의해 만들어졌지만 현재 네트워크에서 원격 사이트를 연결할 수 없습니다.

구성원 상태 "하트비트" 프로세스는 vCloud Director 설치 중 시스템 조직에서 만들어진 로컬 vCloud Director 사용자 계정인 다중 사이트 시스템 사용자의 ID로 실행됩니다. 이 계정은 시스템 조직의 멤버이지만 시스템 관리자 권한이 없습니다. 사이트 연결의 원격 멤버의 상태를 검색하는 vCloud API 요청을 수행하기 위한 사용 권한을 부여하는 단일 권한인 **Multisite: System Operations**만 있습니다.

다중 사이트 리소스 목록

여러 위치에서 vCloud Director 배포로 작업하는 경우 연결된 모든 사이트의 개체에 대한 정보가 포함된 리소스 목록을 볼 수 있습니다.

버전 9.7부터, Service Provider Admin Portal에서 vSphere와 클라우드 리소스를 쉽게 탐색할 수 있도록 vCloud Director에 다중 사이트 리소스 목록이 도입되었습니다. 버전 10.0부터는 vCloud Director에서 조직을 포함하는 다중 사이트 리소스 목록이 지원됩니다.

리소스 목록은 **vSphere 리소스**와 **클라우드 리소스** 메뉴를 통해 액세스할 수 있습니다.

다른 사이트의 개체에 대한 자세한 정보에 액세스할 수 있고 로컬 사이트와 원격 사이트 모두에서 개체를 만들 수도 있습니다.

다중 사이트 vSphere 리소스 목록은 vCenter Server 인스턴스, NSX-T Manager 인스턴스, 리소스 풀, 데이터스토어, 호스트, 분산 스위치, 포트 그룹, 격리된 항목 및 스토리지 정책에 대해 지원됩니다.

다중 사이트 클라우드 리소스 목록은 조직, 조직 VDC, 조직 VDC 템플릿, 제공자 VDC, 클라우드 셀, Edge 게이트웨이, 외부 네트워크, 네트워크 풀 및 VM 크기 조정 정책에 대해 지원됩니다.

제공자 가상 데이터 센터 관리

4

제공자 가상 데이터 센터를 만든 후에 해당 속성을 수정하고, 제공자 가상 데이터 센터를 사용하지 않도록 설정하거나 삭제하고, 스토리지 정책 및 리소스 풀을 관리할 수 있습니다.

제공자 가상 데이터 센터를 만들려면 **Service Provider Admin Portal**이나 **vCloud API**를 사용해야 합니다. **Service Provider Admin Portal** 사용에 대한 자세한 내용은 [제공자 가상 데이터 센터 생성](#) 항목을 참조하십시오. **vCloud API** 사용에 대한 자세한 내용은 "서비스 제공자를 위한 vCloud API 프로그래밍 가이드"의 내용을 참조하십시오.

본 장은 다음 항목을 포함합니다.


- [제공자 가상 데이터 센터 사용 또는 사용 안 함](#)
- [제공자 가상 데이터 센터 삭제](#)
- [제공자 가상 데이터 센터의 일반 설정 편집](#)
- [제공자 가상 데이터 센터 병합](#)
- [제공자 가상 데이터 센터의 조직 가상 데이터 센터 보기](#)
- [제공자 가상 데이터 센터의 데이터스토어 보기](#)
- [제공자 가상 데이터 센터의 외부 네트워크 보기](#)
- [제공자 가상 데이터 센터에서 VM 스토리지 정책 관리](#)
- [제공자 가상 데이터 센터의 리소스 풀 관리](#)
- [제공자 가상 데이터 센터에 대한 메타데이터 수정](#)

제공자 가상 데이터 센터 사용 또는 사용 안 함

제공자 가상 데이터 센터의 리소스를 사용하는 기존의 모든 조직 가상 데이터 센터를 사용하지 않도록 설정하려면 해당하는 제공자 가상 데이터 센터를 사용하지 않도록 설정합니다. 사용하지 않도록 설정된 제공자 가상 데이터 센터의 리소스를 사용하는 조직 가상 데이터 센터는 만들 수 없습니다.

실행 중인 **vApp** 및 전원이 켜진 가상 시스템은 제공자 가상 데이터 센터가 지원하는 기존의 조직 가상 데이터 센터에서 계속 실행되지만 추가 **vApp** 또는 가상 시스템을 생성하거나 시작할 수는 없습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭합니다.
- 3 대상 제공자 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **사용** 또는 **사용 안 함**을 클릭합니다.
- 4 **확인**을 클릭하여 확인합니다.

제공자 가상 데이터 센터 삭제


vCloud Director에서 제공자 가상 데이터 센터의 리소스를 제거하기 위해 이 제공자 가상 데이터 센터를 삭제할 수 있습니다.

vSphere의 기본 리소스는 영향을 받지 않습니다.

사전 요구 사항

- 대상 제공자 가상 데이터 센터를 사용하지 않도록 설정합니다. [제공자 가상 데이터 센터 사용 또는 사용 안 함](#)의 내용을 참조하십시오.
- 이 제공자 가상 데이터 센터의 리소스를 사용하는 모든 조직 가상 데이터 센터를 삭제합니다. [조직 가상 데이터 센터 삭제](#)의 내용을 참조하십시오.


절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭합니다.
- 3 제거할 제공자 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **삭제**를 클릭합니다.
- 4 **확인**을 클릭하여 확인합니다.

제공자 가상 데이터 센터의 일반 설정 편집

제공자 가상 데이터 센터의 이름과 설명을 변경할 수 있습니다. 지원 리소스 풀에서 더 높은 가상 하드웨어 버전을 지원하는 경우에는 제공자 가상 데이터 센터에서 지원하는 최고 가상 하드웨어를 업그레이드할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 수정할 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **구성 > 일반** 탭의 오른쪽 위에서 **편집**을 클릭합니다.
- 4 (선택 사항) 제공자 가상 데이터 센터의 이름과 설명을 수정합니다.

- 5 (선택 사항) 드롭다운 메뉴에서 제공자 가상 데이터 센터에서 지원하는 최고 하드웨어 버전을 선택하고 **저장**을 클릭합니다.

선택할 수 있는 최고 버전은 제공자 가상 데이터 센터를 지원하는 리소스 풀에 있는 ESXi 호스트에 의해 결정됩니다.

참고 제공자 가상 데이터 센터에서 지원하는 하드웨어 버전으로 업그레이드만 할 수 있습니다. 하드웨어 버전을 다운그레이드할 수는 없습니다. vCloud Director 10.0에서 지원되는 가상 시스템 하드웨어의 최고 버전은 14입니다.

- 6 **저장**을 클릭합니다.


제공자 가상 데이터 센터 병합

두 제공자 가상 데이터 센터의 리소스를 결합하기 위해 이러한 제공자 가상 데이터 센터를 하나의 제공자 가상 데이터 센터로 병합할 수 있습니다.

사전 요구 사항

- 대상 제공자 가상 데이터 센터가 동일한 vCenter Server 데이터 센터에 속합니다.
- 대상 제공자 가상 데이터 센터에 탄력적인 조직 가상 데이터 센터만 포함됩니다.


절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭합니다.
- 3 확장할 제공자 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **병합**을 클릭합니다.
- 4 리소스를 병합할 제공자 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **병합**을 클릭합니다.

제공자 가상 데이터 센터의 조직 가상 데이터 센터 보기

제공자 가상 데이터 센터의 리소스를 사용하는 조직 가상 데이터 센터 목록을 볼 수 있습니다.


절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 대상 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **조직 VDC** 탭을 클릭합니다.

결과

이 제공자 가상 데이터 센터의 리소스를 소비하는 조직 가상 데이터 센터 목록이 표시됩니다. 각 조직 VDC의 상태, 실행 상태, 할당 모델, 조직, vCenter Server 인스턴스, 네트워크 수, vApp 수, 스토리지 정책 수 및 리소스 풀 수에 대한 정보가 이 목록에 포함됩니다.


다음에 수행할 작업

- vCloud Director Tenant Portal에서 대상 조직 가상 데이터 센터의 이름 옆에 있는 **팝업** 아이콘()을 클릭하면 조직 가상 데이터 센터 보기로 이동할 수 있습니다.
- 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하면 [장 6 조직 가상 데이터 센터 관리](#)에 설명된 작업과 유사한 관리 작업을 수행할 수 있습니다.

제공자 가상 데이터 센터의 데이터스토어 보기

제공자 가상 데이터 센터에 스토리지 용량을 제공하는 데이터스토어에 대한 세부 정보를 볼 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 대상 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **데이터스토어** 탭을 클릭합니다.

제공자 가상 데이터 센터의 모든 데이터스토어 목록이 표시됩니다. 이 목록에는 각 데이터스토어에 대한 다음과 같은 정보가 포함되어 있습니다.


제목	설명
이름	데이터스토어의 이름
상태	사용 또는 사용 안 함
유형	데이터스토어에 사용되는 파일 시스템 유형으로, VMFS(Virtual Machine File System) 또는 NFS(Network File System)입니다.
사용됨	로그 파일, 스냅샷, 가상 디스크를 포함하여 가상 시스템 파일로 점유되는 데이터스토어 공간입니다. 가상 시스템의 전원 이 켜지면 사용된 스토리지 공간에 로그 파일도 포함됩니다.
프로비저닝됨	가상 시스템에 보장된 데이터스토어 공간입니다. 가상 시스템에 켜진 프로비저닝이 사용되는 경우 일부 프로비저닝된 공간은 사용되고 있지 않을 수 있으며 다른 가상 시스템이 사용되지 않은 공간을 점유할 수 있습니다. 켜진 프로비저닝이 사용되는 경우 이 값은 실제 데이터스토어 용량보다 클 수 있습니다.

제목	설명
요청된 스토리지	<p>다음에 포함하여 데이터스토어의 vCloud Director 개체에만 사용되는 프로비저닝된 스토리지:</p> <ul style="list-style-type: none"> ■ vCloud Director에서 프로비저닝된 가상 시스템 ■ 카탈로그 항목(템플릿 및 미디어) ■ NSX Edge ■ 가상 시스템에 대한 사용된/사용되지 않은 메모리 스왑 요구 사항 <p>이 값에는 연결된 복제 트리의 새도 VM 또는 중간 디스크에 의해 요청되는 스토리지가 포함되지 않습니다.</p>
vCenter	데이터스토어에 연결된 vCenter Server 인스턴스입니다.

제공자 가상 데이터 센터의 외부 네트워크 보기

제공자 가상 데이터 센터에서 액세스할 수 있는 외부 네트워크 목록을 볼 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 대상 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **외부 네트워크** 탭을 클릭합니다.

결과

게이트웨이 CIDR 설정 및 IP 풀 사용에 대한 정보가 포함된 사용 가능한 외부 네트워크 목록을 볼 수 있습니다.

제공자 가상 데이터 센터에서 VM 스토리지 정책 관리

제공자 가상 데이터 센터에서 VM 스토리지 정책을 추가하고, 사용하거나 사용하지 않도록 설정하고, 제거할 수 있습니다. 제공자 가상 데이터 센터에서 VM 스토리지 정책의 메타데이터를 추가, 편집 및 삭제할 수도 있습니다.

VM 스토리지 정책을 제공자 가상 데이터 센터에 추가


VM 스토리지 정책을 제공자 가상 데이터 센터에 추가한 다음, 추가된 스토리지 정책을 지원하도록 이 제공자 가상 데이터 센터에서 지원하는 조직 가상 데이터 센터를 구성할 수 있습니다.

중요 vCloud Director는 암호화 및 Storage I/O Control 등의 호스트 기반 데이터 서비스에 대한 VM 스토리지 정책을 지원하지 않습니다.

사전 요구 사항

- vSphere 관리자가 대상 VM 스토리지 정책을 생성합니다. SPBM(스토리지 정책 기반 관리)에 대한 자세한 내용은 "vSphere 스토리지" 설명서를 참조하십시오.
- [vCenter Server 인스턴스의 스토리지 정책 새로 고침](#).

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 대상 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **스토리지 정책** 탭에서 **추가**를 클릭합니다.
- 4 추가할 하나 이상의 스토리지 정책을 선택하고 **추가**를 클릭합니다.
 *(**임의**)를 선택할 경우 데이터스토어가 제공자 가상 데이터 센터의 데이터스토어 클러스터에 추가되거나 이 클러스터에서 제거되면 vCloud Director가 해당 데이터스토어를 동적으로 추가하거나 제거합니다.


다음에 수행할 작업

스토리지 정책을 지원하도록 제공자 가상 데이터 센터에서 지원하는 조직 가상 데이터 센터를 구성합니다. [VM 스토리지 정책을 조직 가상 데이터 센터에 추가](#)의 내용을 참조하십시오.

제공자 가상 데이터 센터에서 VM 스토리지 정책 사용 또는 사용 안 함

제공자 가상 데이터 센터에서 VM 스토리지 정책을 사용하지 않도록 설정하면 해당 조직 가상 데이터 센터에서 이 VM 스토리지 정책을 더 이상 사용할 수 없습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 대상 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **스토리지 정책** 탭을 클릭합니다.
- 4 대상 VM 스토리지 정책 옆에 있는 라디오 버튼을 클릭하고 **사용** 또는 **사용 안 함**을 클릭합니다.
- 5 **확인**을 클릭하여 확인합니다.


제공자 가상 데이터 센터에서 VM 스토리지 정책 삭제

제공자 가상 데이터 센터에서 VM 스토리지 정책을 삭제할 수 있습니다.

사전 요구 사항

대상 VM 스토리지 정책을 사용하지 않도록 설정합니다. [제공자 가상 데이터 센터에서 VM 스토리지 정책 사용 또는 사용 안 함](#)의 내용을 참조하십시오.

절차


- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 대상 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **스토리지 정책** 탭을 클릭합니다.
- 4 대상 VM 스토리지 정책 옆에 있는 라디오 버튼을 클릭하고 **제거**를 클릭합니다.
- 5 **제거**를 클릭하여 확인합니다.

제공자 가상 데이터 센터에서 VM 스토리지 정책의 메타데이터 수정

제공자 가상 데이터 센터에서 스토리지 정책의 메타데이터를 추가, 편집 및 삭제할 수 있습니다.

개체 메타데이터를 사용하면 사용자 정의 *name=value* 쌍을 제공자 가상 데이터 센터의 스토리지 정책과 연결할 수 있습니다. vCloud API 쿼리 필터 식에서 개체 메타데이터를 사용할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 대상 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **스토리지 정책** 탭을 클릭합니다.
- 4 대상 VM 스토리지 정책 옆에 있는 라디오 버튼을 클릭하고 **메타데이터**를 클릭합니다.
- 5 **편집**을 클릭합니다.
- 6 (선택 사항) 키-값 쌍을 추가하려면 **추가**를 클릭하고 이름 및 값을 입력한 다음 새로운 키-값 쌍의 유형을 선택합니다.
- 7 (선택 사항) 키-값 쌍을 편집하려면 새 이름과 값을 입력하고 키-값 쌍의 새 유형을 선택합니다.
- 8 (선택 사항) 키-값 쌍을 제거하려면 해당 행의 오른쪽 끝에서 **삭제** 아이콘을 클릭합니다.
- 9 **저장**을 클릭하고 **확인**을 클릭합니다.

제공자 가상 데이터 센터의 리소스 풀 관리

제공자 가상 데이터 센터에서 보조 리소스 풀을 추가하고, 사용하거나 사용하지 않도록 설정하고, 분리할 수 있습니다. 제공자 가상 데이터 센터에서 기본 리소스 풀을 사용하지 않도록 설정하거나 분리할 수 없습니다.

제공자 가상 데이터 센터에 리소스 풀 추가

하나 이상의 보조 리소스 풀을 제공자 가상 데이터 센터에 추가하여 해당 선지급 및 할당 풀 조직 가상 데이터 센터를 확장할 수 있습니다.


계산 리소스가 여러 리소스 풀에서 지원되는 경우 더 많은 가상 시스템을 수용하도록 리소스 풀을 확장할 수 있습니다.

VLAN 업링크가 있는 NSX Edge 호스팅을 위해 최적으로 구성된 vSphere 클러스터에서 지원하는 리소스 풀을 추가할 수 있습니다. vCloud Director는 메타데이터를 사용하여 시스템에서 그러한 클러스터가 지원하는 리소스 풀에 조직 VDC Edge 게이트웨이를 배치해야 함을 나타낼 수 있습니다. 자세한 내용은 VMware 기술 자료 문서 <https://kb.vmware.com/kb/2151398>의 내용을 참조하십시오.

사전 요구 사항

vSphere 관리자가 제공자 가상 데이터 센터의 기본 리소스 풀을 지원하는 vCenter Server 인스턴스에서 대상 보조 리소스 풀을 만듭니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 대상 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **리소스 풀** 탭에서 **추가**를 클릭합니다.
- 4 추가할 하나 이상의 리소스 풀을 선택하고 **추가**를 클릭합니다.

결과

vCloud Director는 제공자 가상 데이터 센터에서 사용할 리소스 풀을 추가하여 해당 제공자 가상 데이터 센터에서 지원되는 모든 선지급 및 할당 풀 조직 가상 데이터 센터가 유연하게 됩니다.

vCloud Director는 또한 새 리소스 풀 아래에 시스템 VDC 리소스 풀을 추가합니다. 이 리소스 풀은 연결된 클론에 대한 템플릿으로 사용되는 VM 및 NSX Edge VM과 같은 시스템 리소스 생성에 사용됩니다.

중요 시스템 VDC 리소스 풀을 편집하거나 삭제하지 마십시오.


제공자 가상 데이터 센터에서 리소스 풀 사용 또는 사용 안 함

리소스 풀을 사용하지 않도록 설정하는 경우 제공자 가상 데이터 센터에서 리소스 풀의 메모리 및 계산 리소스를 더 이상 사용할 수 없습니다.

이미 진행 중인 프로세스는 사용하지 않도록 설정된 리소스 풀의 리소스를 계속 사용합니다.

참고 제공자 가상 데이터 센터의 기본 리소스 풀은 사용하지 않도록 설정할 수 없습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 대상 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **리소스 풀** 탭을 클릭합니다.
- 4 대상 리소스 풀 옆에 있는 라디오 버튼을 클릭하고 **사용** 또는 **사용 안 함**을 클릭합니다.
- 5 **확인**을 클릭하여 확인합니다.


제공자 가상 데이터 센터에서 리소스 풀 분리

제공자 가상 데이터 센터에 둘 이상의 리소스 풀이 있는 경우 제공자 가상 데이터 센터에서 보조 리소스 풀을 분리할 수 있습니다. 기본 리소스 풀은 제공자 가상 데이터 센터에서 분리할 수 없습니다.

사전 요구 사항

- 제공자 가상 데이터 센터에서 대상 리소스 풀을 사용하지 않도록 설정합니다. [제공자 가상 데이터 센터에서 리소스 풀 사용 또는 사용 안 함](#)의 내용을 참조하십시오.
- 사용하지 않도록 설정한 리소스 풀의 영향을 받는 모든 네트워크를 재배포합니다.
- 사용하지 않도록 설정한 리소스 풀의 영향을 받는 모든 Edge 게이트웨이를 재배포합니다.

절차


- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 대상 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **리소스 풀** 탭을 클릭합니다.
- 4 대상 리소스 풀 옆에 있는 라디오 버튼을 클릭하고 **분리**를 클릭합니다.
- 5 **확인**을 클릭하여 확인합니다.

제공자 가상 데이터 센터에 대한 메타데이터 수정

제공자 가상 데이터 센터에 대한 메타데이터를 추가, 편집 및 삭제할 수 있습니다.

개체 메타데이터를 사용하면 사용자 정의 *name=value* 쌍을 제공자 가상 데이터 센터와 연결할 수 있습니다. vCloud API 쿼리 필터 식에서 개체 메타데이터를 사용할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 대상 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **구성 > 메타데이터** 탭의 오른쪽 상단 모서리에서 **편집**을 클릭합니다.
- 4 (선택 사항) 키-값 쌍을 추가하려면 **추가**를 클릭하고 이름 및 값을 입력한 다음 새로운 키-값 쌍의 유형을 선택합니다.
- 5 (선택 사항) 키-값 쌍을 편집하려면 새 이름과 값을 입력하고 키-값 쌍의 새 유형을 선택합니다.
- 6 (선택 사항) 키-값 쌍을 제거하려면 해당 행의 오른쪽 끝에서 **삭제** 아이콘을 클릭합니다.
- 7 **저장**을 클릭하고 **확인**을 클릭합니다.

vCloud Director Service Provider Admin Portal을 사용하면 vCloud Director 조직을 만들고 구성하고 관리할 수 있습니다.

vCloud Director Service Provider Admin Portal을 사용하여 조직을 관리하고, 사용자가 조직에 할당된 리소스를 사용하는 방법을 결정하는 정책을 설정하고, 카탈로그의 게시 및 공유를 관리합니다.

본 장은 다음 항목을 포함합니다.

- 임대 이해
- 조직 만들기
- 조직에 대한 카탈로그 구성
- 조직에 대한 정책 구성
- 테넌트 스토리지 마이그레이션

임대 이해

조직을 만들려면 임대를 지정해야 합니다. 임대를 통해 vApp를 실행하고 vApp 및 vApp 템플릿을 저장할 수 있는 최대 시간을 지정하여 조직의 스토리지 및 계산 리소스를 일정 수준으로 제어할 수 있습니다.

런타임 임대의 목적은 비활성 vApp에서 계산 리소스를 사용하지 못하도록 하는 것입니다. 예를 들어 사용자가 vApp를 시작한 후 이를 중지하지 않고 휴가를 떠나면 vApp에서는 리소스를 계속 사용하게 됩니다.

런타임 임대는 사용자가 vApp를 시작할 때 시작되며, 런타임 임대가 만료되면 vCloud Director에서는 vApp를 중지합니다.


스토리지 임대의 목적은 사용되지 않는 vApp 및 vApp 템플릿이 스토리지 리소스를 사용하지 못하도록 하는 것입니다. vApp 스토리지 임대는 사용자가 vApp를 시작할 때 시작되며, vApp 실행에는 영향을 주지 않습니다. vApp 템플릿 스토리지 임대는 사용자가 vApp에 vApp 템플릿을 추가하거나, 작업공간에 vApp 템플릿을 추가하거나, vApp 템플릿을 다운로드, 복사 또는 이동할 때 시작됩니다.

스토리지 임대가 만료되면 vCloud Director에서는 관리자가 설정한 조직 정책에 따라 vApp 또는 vApp 템플릿을 만료된 것으로 표시하거나 삭제합니다.

조직 만들기

vCloud Director Service Provider Admin Portal에서 새 조직을 만들 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.

a 왼쪽 패널에서 **조직**을 선택합니다.

기존 조직의 목록이 그리드 보기에 표시됩니다.

- 2 새 조직을 만들려면 **+추가** 버튼을 클릭합니다.

새 **조직** 대화 상자가 열립니다.

- 3 다음 값을 입력합니다.


옵션	설명
조직 이름	조직의 테넌트 포털 액세스를 위한 URL을 구성하는 고유 식별자입니다.
조직 전체 이름	조직의 전체 이름입니다.
설명	조직에 대한 설명(선택 사항)입니다.

- 4 **만들기** 버튼을 클릭하여 만들기를 완료합니다.

조직에 대한 카탈로그 구성

조직이 해당 서비스 카탈로그를 공유하는 방법을 구성할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.

a 왼쪽 패널에서 **조직**을 선택합니다.

기존 조직의 목록이 그리드 보기에 표시됩니다.

- 2 조직을 선택하고 **구성** 탭에서 **카탈로그**를 선택합니다.

- 3 공유 및 게시 설정을 변경하려면 **편집**을 클릭합니다.

옵션	설명
공유	조직 관리자가 이 조직의 카탈로그를 이 vCloud Director 인스턴스 내의 다른 조직과 공유할 수 있습니다. 이 옵션을 선택하지 않을 경우에도 조직 내에서는 조직 관리자가 카탈로그를 공유할 수 있습니다.
외부 카탈로그에 게시 허용	조직 관리자가 카탈로그를 이 vCloud Director 인스턴스 외부의 조직에 게시할 수 있습니다.
외부 카탈로그 구 독 허용	조직 관리자가 이 vCloud Director 인스턴스 외부의 카탈로그를 구독할 수 있습니다.


조직에 대한 정책 구성

임대, 할당량 및 제한은 조직 사용자가 사용할 수 있는 스토리지 및 처리 리소스를 제한합니다. 이러한 설정을 수정하여 사용자가 조직의 리소스를 소모하거나 독점하지 못하도록 할 수 있습니다.

사전 요구 사항

[임대 이해](#)의 내용을 참조하십시오.

절차

- 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - 왼쪽 패널에서 **조직**을 선택합니다.
기존 조직의 목록이 그리드 보기에 표시됩니다.
- 조직을 선택하고 **정책** 탭을 선택합니다.
- 조직에 대한 리스, 할당량, 리소스 제한 및 암호 정책을 편집하려면 **편집**을 클릭합니다.
- 다음과 같은 설정으로 vApp 리스를 구성합니다.

옵션	설명
최대 런타임 임대	vApp이 자동으로 중지되기 전까지 실행 가능한 시간입니다.
런타임 만료 작업	만료된 실행 중인 vApp이 처리되는 방법입니다. vApp을 일시 중단하면 해당하는 모든 가상 시스템이 일시 중단되고 메모리를 디스크에 써서 가상 시스템의 현재 상태를 보존합니다. 전원 끄기 는 해당하는 모든 가상 시스템과 하위 vApp을 즉시 중지합니다.
최대 스토리지 임대	중지된 vApp이 자동으로 정리되기 전까지 사용 가능한 시간입니다.
스토리지 정리	vApp이 중지 및 정리된 후 처리되는 방법입니다.

- 다음과 같은 설정으로 vApp 템플릿 리스를 구성합니다.

옵션	설명
최대 스토리지 임대	vApp 템플릿이 자동으로 정리되기 전까지 사용 가능한 시간입니다.
스토리지 정리	만료된 vApp 템플릿이 정리된 후 처리되는 방법입니다.

- 다음과 같은 설정으로 할당량을 구성합니다.

옵션	설명
모든 VM 할당량	사용자가 이 조직에 저장할 수 있는 사용 가능한 총 VM 수입니다.
실행 중인 VM 할당량	사용자가 이 조직에서 전원을 켤 수 있는 총 VM 수입니다.

7 다음과 같은 설정으로 제한을 구성합니다.

옵션	설명
사용자당 리소스 집중 작업 수	사용자당 동시 리소스 집중 작업의 최대 수를 입력하거나 시스템 제한 상속 을 선택합니다.
사용자당 대기해야 할 리소스 집중 작업 수	사용자당 대기하는 리소스 집중 작업의 최대 수를 입력하거나 시스템 제한 상속 을 선택합니다.
조직당 리소스 집중 작업 수	조직당 동시 리소스 집중 작업의 최대 수를 입력하거나 시스템 제한 상속 을 선택합니다.
조직당 대기해야 할 리소스 집중 작업 수	조직당 대기하는 리소스 집중 작업의 최대 수를 입력하거나 시스템 제한 상속 을 선택합니다.
VM당 동시 연결 수	가상 시스템당 동시 콘솔 연결의 최대 수를 입력하거나 시스템 제한 상속 을 선택합니다.
조직당 가상 데이터 센터 수	조직당 조직 가상 데이터 센터의 최대 수를 입력하거나 시스템 할당량 상속 을 선택합니다.

8 다음과 같은 설정으로 암호 정책을 구성합니다.

옵션	설명
계정 잠금 사용	일정 횟수의 잘못된 로그인 시도 이후 사용자 계정 잠금을 사용하도록 설정합니다.
잠기기 전 잘못된 로그인 횟수	사용자 계정이 잠기기 전 잘못된 로그인 시도 횟수입니다.
계정 잠금 간격	잠긴 사용자 계정이 로그인할 수 없는 기간입니다.

테넌트 스토리지 마이그레이션

하나 이상의 조직에 있는 모든 vApp, 독립 디스크 및 카탈로그 항목을 하나 이상의 데이터스토어에서 다른 데이터스토어로 마이그레이션 할 수 있습니다.

데이터스토어 서비스를 해제하기 전에 해당 데이터스토어에 저장된 모든 항목을 새 데이터스토어로 마이그레이션해야 합니다. 스토리지 용량이 더 많거나 VMware vSAN과 같은 새로운 스토리지 기술을 사용하는 새 데이터스토어로 조직을 마이그레이션하는 것도 좋습니다.

중요 테넌트 스토리지 마이그레이션은 특히 마이그레이션할 자산이 많은 경우 장시간 실행될 수 있는 리소스 집약적인 작업입니다. 테넌트 스토리지를 마이그레이션하는 방법에 대한 자세한 내용은 <https://kb.vmware.com/kb/2151086>의 내용을 참조하십시오.

사전 요구 사항

- 대상 조직의 조직 VDC에 사용되는 스토리지 정책을 결정합니다. **VM 스토리지 정책을 조직 가상 데이터 센터에 추가**의 내용을 참조하십시오.
- 마이그레이션할 소스 데이터스토어가 포함된 각 스토리지 정책에 대해 마이그레이션할 대상 데이터스토어가 하나 이상 있는지 확인합니다. 대상 데이터스토어를 생성하거나 기존 데이터스토어를 사용할 수 있습니다. 대상 조직에 사용되는 스토리지 정책의 데이터스토어 확인에 대한 자세한 내용은 "vSphere 스토리지" 설명서를 참조하십시오.

절차

- 1 vCloud Director Service Provider Admin Portal에 **시스템 관리자**로 로그인하거나 **조직: 테넌트 스토리지 마이그레이션** 권한이 있는 역할로 로그인합니다.
- 2 **테넌트 스토리지 마이그레이션** 마법사를 시작합니다.
 - **클라우드 리소스**에서 **조직**을 선택하고 **테넌트 스토리지 마이그레이션**을 클릭합니다.
 - **vSphere 리소스**에서 **데이터스토어**를 선택하고 **테넌트 스토리지 마이그레이션**을 클릭합니다.
- 3 마이그레이션할 스토리지 항목이 포함된 하나 이상의 조직을 선택하고 **다음**을 클릭합니다.
- 4 마이그레이션할 소스 데이터스토어를 하나 이상 선택하고 **다음**을 클릭합니다.

마법사에는 시스템의 모든 데이터스토어가 나열됩니다.
- 5 하나 이상의 대상 데이터스토어를 선택하고 **다음**을 클릭합니다.
- 6 **완료 준비** 페이지를 검토하고 **마침**을 클릭하여 마이그레이션을 시작합니다.

조직 가상 데이터 센터 관리

6

조직에 리소스를 제공하려면 이 조직에 대한 조직 가상 데이터 센터를 하나 이상 생성합니다. 조직 가상 데이터 센터를 만든 후에 해당 속성을 수정하고, 조직 가상 데이터 센터를 사용하지 않도록 설정하거나 삭제하고, 할당 모델, 스토리지 및 네트워크 설정을 관리할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 할당 모델 이해
- VM 크기 조정 및 VM 배치 정책 이해
- 조직 가상 데이터 센터 만들기
- 조직 가상 데이터 센터 사용 또는 사용 안 함
- 조직 가상 데이터 센터 삭제
- 조직 가상 데이터 센터의 이름 및 설명 수정
- 조직 가상 데이터 센터의 할당 모델 설정 수정
- 조직 가상 데이터 센터의 스토리지 설정 수정
- 조직 가상 데이터 센터의 네트워크 설정 편집
- 크로스 가상 데이터 센터 네트워킹 구성
- 조직 가상 데이터 센터에 대한 메타데이터 수정
- 조직 가상 데이터 센터의 리소스 풀 보기
- 조직 가상 데이터 센터에서 분산 방화벽 관리

할당 모델 이해

할당 모델은 할당된 제공자 VDC(가상 데이터 센터) 계산 및 메모리 리소스가 조직 VDC에 커밋되는 방법과 시기를 결정합니다.

다음 표에는 조직 VDC 할당 모델에 기반한 VM(가상 시스템) 또는 리소스 풀 수준의 vSphere 리소스 배포 설정이 나와 있습니다.

	Flex 할당 모델	탄력적 할당 풀 모델	비탄력적 할당 풀 모델	선지급 모델	예약 풀 모델
탄력적	조직 VDC 구성에 기반합니다.	예	아니요	예	아니요
vCPU 속도	VM CPU 제한이 VM 크기 조정 정책에 정의되어 있지 않으면 vCPU 속도가 VDC 내의 VM CPU 제한에 영향을 줄 수 있습니다.	조직 VDC에서 실행 중인 vCPU 수에 영향을 줍니다.	해당 없음	VM CPU 제한에 영향을 줍니다.	해당 없음
리소스 풀 CPU 제한	리소스 풀의 VM 수를 기반으로 조직 VDC CPU 제한이 배분됩니다.	조직 VDC CPU 할당	조직 VDC CPU 할당	무제한	조직 VDC CPU 할당
리소스 풀 CPU 예약	리소스 풀의 vCPU 수를 기반으로 조직 VDC CPU 예약이 배분됩니다. 조직 VDC CPU 예약은 조직 VDC CPU 할당에 CPU 보장을 곱한 값과 같습니다.	전원이 켜진 VM의 합계이며, CPU 보장에 vCPU 속도를 곱하고 vCPU 수를 곱한 값과 같습니다.	조직 VDC CPU 할당 곱하기 CPU 보장	없음, 확장 가능	조직 VDC CPU 할당
리소스 풀 메모리 제한	리소스 풀의 VM 수를 기반으로 조직 VDC 메모리 제한이 배분됩니다.	무제한	조직 VDC RAM 할당	무제한	조직 VDC RAM 할당
리소스 풀 메모리 예약	리소스 풀의 VM 수를 기반으로 조직 VDC RAM 예약이 배분됩니다. 조직 VDC RAM 예약은 조직 VDC RAM 할당에 RAM 보장을 곱한 값과 같습니다.	RAM 보장에 리소스 풀에서 전원이 켜진 모든 VM의 vRAM을 곱한 합계입니다. 리소스 풀 RAM 예약은 확장이 가능합니다.	조직 VDC RAM 할당 곱하기 RAM 보장	없음, 확장 가능	조직 VDC RAM 할당
VM CPU 제한	VM의 VM 크기 조정 정책에 기반합니다.	무제한	무제한	vCPU 속도 곱하기 vCPU 수	사용자 지정
VM CPU 예약	VM의 VM 크기 조정 정책에 기반합니다.	0	0	CPU 속도 곱하기 vCPU 속도 곱하기 vCPU 수와 같습니다.	사용자 지정
VM RAM 제한	VM의 VM 크기 조정 정책에 기반합니다.	무제한	무제한	vRAM	사용자 지정
VM RAM 예약	VM의 VM 크기 조정 정책에 기반합니다.	0	vRAM 곱하기 RAM 보장 더하기 RAM 오버헤드와 같습니다.	vRAM 곱하기 RAM 보장 더하기 RAM 오버헤드와 같습니다.	사용자 지정

레거시 VDC 할당 모델을 Flex 할당 모델로 변환

탄력적 할당 풀 모델, 비탄력적 할당 풀 모델, 선지급 모델 또는 예약 풀 모델을 사용하여 VM 배치 및 VM 크기 조정 정책을 VDC에 추가합니다. VM 배치 또는 VM 크기 조정 정책이 기존 VDC 할당 모델과 호환되지 않으면, VDC를 Flex 조직 VDC로 변환하도록 결정할 수 있습니다.

VM 정책 규정 준수

때거시 VDC를 변환해도 VM 규정 비준수가 발생하지 않습니다. 관리자가 vCenter Server 인스턴스에서 직접 VM의 VM 계산 값 또는 VM 그룹 멤버 자격을 변경하는 경우에는, 할당된 VM 크기 조정 또는 VM 배치 정책을 VM이 준수하지 않을 수 있습니다. 필요한 권한이 있는 사용자가 vCloud API를 사용하여 VM 예약 및 제한 값을 변경하면 VM이 규정 비준수 상태가 될 수도 있습니다. 규정 비준수 VM이 있으면 vCloud Director Tenant Portal UI에 주의 메시지가 표시됩니다. 테넌트는 규정 비준수의 원인에 대한 자세한 정보를 볼 수 있으며 VM에 정책을 다시 적용하여 VM을 준수 상태로 다시 만들 수 있습니다.

할당 모델의 권장 사용법

각 할당 모델은 다양한 수준의 성능 제어 및 관리에 사용할 수 있습니다.

다음 표에는 각 할당 모델의 권장 사용법에 대한 정보가 나와 있습니다.

할당 모델	권장 사용
Flex 할당 모델	FLEX 할당 모델을 사용하면 워크로드 수준에서 세분화된 성능 제어를 수행할 수 있습니다. vCloud Director 시스템 관리자 는 FLEX 할당 모델을 사용하여 개별 조직 VDC의 탄력성을 관리할 수 있습니다. FLEX 할당 모델은 정책 기반 워크로드 관리를 사용합니다. FLEX 할당 모델을 사용하면 클라우드 제공자 가 조직 VDC의 메모리 오버헤드를 효과적으로 제어할 수 있고 테넌트에 엄격한 버스트 용량을 사용하도록 적용할 수 있습니다.
할당 풀 할당 모델	할당 풀 할당 모델은 테넌트가 고정된 계산 리소스 소비를 구독하여 클라우드 제공자 가 계산 리소스 용량을 예측하고 관리할 수 있는 안정적인 장기간 워크로드에 사용됩니다. 할당 풀 할당 모델은 성능 요구 사항이 다양한 워크로드에 최적입니다. 할당 풀 할당 모델을 사용하면 모든 워크로드가 vCenter Server의 리소스 풀에서 할당된 리소스를 공유합니다. 탄력성을 사용하거나 사용하지 않도록 설정하는지 여부와 관계 없이 테넌트는 제한된 양의 계산 리소스를 수신합니다. 할당 풀 할당 모델을 사용하면 클라우드 제공자 가 시스템 수준에서 탄력성을 사용하거나 사용하지 않도록 설정할 수 있고 모든 할당 풀 조직 VDC에 설정이 적용됩니다. 비탄력적 할당 풀 할당을 사용하는 경우, 조직 VDC는 VDC 리소스 풀을 미리 예약하며 테넌트는 vCPU를 오버 커밋할 수 있지만 메모리는 오버 커밋할 수 없습니다. 탄력적 풀 할당을 사용하는 경우에는, 조직 VDC가 계산 리소스를 미리 예약하지 않으며 용량은 여러 클러스터를 통해 확장할 수 있습니다. 클라우드 제공자는 물리적 계산 리소스에 대한 오버 커밋을 관리하며 테넌트는 vCPU와 메모리를 오버 커밋할 수 없습니다.
선지급	선지급 모델은 vCenter Server에서 계산 리소스를 미리 할당할 필요가 없는 경우 사용합니다. 테넌트가 VDC에 배포하는 모든 워크로드에 예약, 제한 및 할당량이 적용됩니다. 선지급 할당 모델을 사용하는 경우 조직 VDC의 모든 워크로드에는 동일한 비율의 구성된 계산 리소스가 예약됩니다. vCloud Director에 대해 모든 워크로드에 대한 모든 vCPU의 CPU 속도는 동일하며 조직 VDC 수준에서 CPU 속도를 정의할 수만 있습니다. 성능 측면에서 개별 워크로드에 대한 예약 설정을 변경할 수 없기 때문에 모든 워크로드가 동일한 기본 설정을 받습니다. 선지급 할당 모델은 동일한 조직 VDC 내에서 성능 요구 사항이 서로 다른 워크로드를 실행해야 하는 테넌트에 적합합니다. 탄력성 때문에 선지급 모델은 자동 크기 조정 애플리케이션에 속하는 일반 단기 워크로드에 적합합니다. 선지급을 사용하면 테넌트가 조직 VDC 내에서 계산 리소스 요구량의 스파이크를 일치시킬 수 있습니다.
예약 풀	예약 풀 할당 모델은 조직 VDC에서 실행 중인 워크로드의 성능을 세부적으로 제어해야 하는 경우에 사용됩니다. 클라우드 제공자 관점에서 예약 풀 할당 모델을 사용하려면 vCenter Server에서 모든 계산 리소스를 미리 할당해야 합니다. 예약 풀 할당 모델은 탄력적이지 않습니다. 예약 풀 할당 모델은 특정 테넌트 전용으로 지정된 하드웨어에서 실행되는 워크로드에 최적입니다. 이러한 경우, 테넌트 사용자는 계산 리소스에 대한 사용 및 오버 커밋을 관리할 수 있습니다.

Flex 할당 모델

vCloud Director 9.7부터 **시스템 관리자**는 Flex 할당 모델을 사용하여 조직 VDC(가상 데이터 센터)를 생성할 수 있습니다. **시스템 관리자**는 Flex 할당과 VM 크기 조정 정책을 조합하여 VDC 및 개별 VM(가상 시스템) 수준 모두에서 CPU 및 RAM 소비를 제어할 수 있습니다. Flex 할당 모델은 기존 할당 모델에서 사용할 수 있는 모든 할당 구성을 지원합니다.

vCloud Director 10.0에서는 Flex가 아닌 모든 조직 VDC를 Flex VDC로 변환할 수 있습니다.

Flex 조직 VDC를 생성할 때 **시스템 관리자**는 조직 VDC의 다음과 같은 매개 변수를 제어합니다.

매개 변수	설명
탄력성	탄력적 풀 기능을 사용하거나 사용하지 않도록 설정합니다.
VM 메모리 오버헤드 포함	이 VDC에 메모리 오버헤드를 포함하거나 제외합니다. true 로 설정하면 전원이 켜진 모든 VM의 메모리 오버헤드를 VDC의 사용 가능한 용량에서 가져오기 때문에 VDC의 전체 용량을 사용하지 못할 수 있습니다. false 로 설정하면 VDC의 할당된 용량이 아니라 제공자 VDC에서 메모리 오버헤드를 가져옵니다.
CPU 할당	이 VDC에 할당된 CPU 양(MHz 또는 GHz)입니다. CPU 할당은 VDC의 CPU 용량을 정의합니다. VDC에서 실행되는 모든 VM에 사용되는 총 CPU는 이 값을 초과할 수 없습니다.
CPU 제한	CPU 제한은 VDC의 CPU 할당량을 정의합니다. 대부분의 경우 CPU 제한은 VDC의 할당된 CPU 용량과 같습니다. VDC에 CPU를 할당하지 않아도 되는 경우(예: 선지급 모델)가 있습니다. 이 경우 CPU 할당을 0으로 설정하고 CPU 제한을 0이 아닌 값으로 설정하여, 전체 CPU 사용량에 대한 할당량을 설정해야 합니다. 이 설정을 사용하여 CPU 할당량을 무제한으로 허용할 수도 있습니다. 무제한으로 설정하면 vCenter Server에 있는 VDC의 지원 리소스 풀에 무제한 CPU가 제공됩니다.
보장된 CPU 리소스	VDC에 대해 물리적으로 예약된 CPU 할당의 백분율입니다.
vCPU 속도	VDC의 VM에 대한 기본 vCPU 속도입니다.
메모리 할당	이 VDC에 할당된 메모리 양(MB 또는 GB)입니다. 이 매개 변수는 VDC의 총 메모리 용량을 정의합니다. VDC에서 실행되는 모든 VM에 의해 구성된 총 메모리는 이 값을 초과할 수 없습니다.
보장된 메모리 리소스	VDC에 대해 물리적으로 예약된 메모리 할당의 백분율입니다.
최대 VM 수	VDC의 최대 VM 수입니다.

vCloud Director 시스템 관리자는 Flex 조직 VDC를 탄력적으로 구성하거나 비탄력적으로 구성할 수 있습니다. Flex 조직 VDC에 탄력적 풀 기능을 사용하도록 설정된 경우, 조직 VDC는 해당 제공자 VDC와 연결된 모든 리소스 풀을 포함하고 사용합니다. vCloud Director 9.7에서 비탄력적 조직 VDC를 탄력적 조직 VDC로 변환하면, 동일한 조직 VDC를 비탄력적으로 다시 변환할 수 없습니다.

Flex 할당 모델은 다른 할당 모델에 적용되는 제약 없이 조직 VM 크기 조정 정책의 기능을 지원합니다.

Flex 할당 모델에서 VM 계산 리소스 할당은 VM 크기 조정 정책에 따라 결정됩니다. 조직 VDC에 대한 VM 크기 조정 정책을 정의하지 않을 경우 계산 리소스 할당은 조직 VDC 할당 모델에 따라 결정됩니다.

Flex 할당 모델과 조직 VM 크기 조정 정책의 조합을 사용하면 단일 조직 VDC가 다른 모든 할당 모델에 공통적인 구성을 사용하는 VM을 수용할 수 있습니다. 자세한 내용은 [VM 크기 조정 및 VM 배치 정책 이해](#) 항목을 참조하십시오.

Flex 조직 VDC를 생성하려면 vCloud Director Service Provider Admin Portal 또는 vCloud API를 사용하면 됩니다. vCloud API에 대한 자세한 내용은 "서비스 제공자를 위한 vCloud API 프로그래밍 가이드" 항목을 참조하십시오.

할당 풀 할당 모델

할당 풀 할당 모델을 사용하면 제공자 VDC(가상 데이터 센터)에서 할당하는 리소스의 일정 비율이 조직 VDC에 커밋됩니다. CPU 및 메모리 모두에 대해 비율을 지정할 수 있습니다. 이러한 비율을 보장 비율 요소라고 하며, 이를 통해 리소스를 오버커밋할 수 있습니다.

시스템 관리자는 할당 풀 조직 VDC를 탄력적으로 구성하거나 비탄력적으로 구성할 수 있습니다. 탄력성은 모든 할당 풀 조직 VDC에 영향을 미치는 전역 설정입니다. [일반 시스템 설정 수정](#)의 내용을 참조하십시오.

기본적으로 할당 풀 조직 VDC는 탄력적 할당 풀을 사용하도록 설정됩니다. 가상 시스템이 여러 리소스 풀에 걸쳐 있는 할당 풀 조직 VDC가 포함된 vCloud Director 5.1에서 업그레이드된 시스템은 기본적으로 탄력적 할당 풀을 사용하도록 설정됩니다.

할당 풀 VDC에 탄력적 할당 풀 기능을 사용하도록 설정된 경우 조직 VDC는 해당 제공자 VDC와 연결된 모든 리소스 풀을 포함하고 사용합니다. 결과적으로 vCPU 주파수는 이제 할당 풀의 필수 매개 변수가 되었습니다.

CPU가 병목 현상의 요인이 되지 않으면서 조직 VDC에 가상 시스템을 충분히 배포하는 방식으로 vCPU 주파수와 보장 비율 요소를 설정해야 합니다.

가상 시스템이 생성되면 배치 엔진은 가상 시스템의 요구 사항에 가장 잘 맞는 제공자 VDC 리소스 풀에 가상 시스템을 배치합니다. 제공자 VDC 리소스 풀 아래에 이 조직 VDC에 대한 하위 리소스 풀이 생성되고 이 하위 리소스 풀 아래에 가상 시스템이 배치됩니다.

가상 시스템의 전원이 켜지면, 배치 엔진은 제공자 VDC 리소스 풀을 점검하여 가상 시스템의 전원을 여전히 켤 수 있는지 확인합니다. 그렇지 않으면, 배치 엔진이 가상 시스템을 실행하기에 충분한 리소스가 있는 제공자 VDC 리소스 풀로 가상 시스템을 이동합니다. 조직 VDC에 대한 하위 리소스 풀이 없으면 생성됩니다.

하위 리소스 풀은 새 가상 시스템을 실행하는 데 충분한 리소스로 구성됩니다. 하위 리소스 풀의 메모리 예약은 가상 시스템의 구성된 메모리 크기에 조직 VDC의 보장 비율 요소를 곱한 값만큼 증가됩니다. 하위 리소스 풀의 CPU 예약은 가상 시스템에 대해 구성된 vCPU 수, 조직 VDC 수준에 지정된 vCPU, 그리고 조직 VDC 수준에 설정된 CPU의 보장 비율 요소를 모두 곱한 값만큼 증가됩니다. 탄력적 할당 풀 기능을 사용

하도록 설정하면 하위 리소스 풀의 메모리 제한은 가상 시스템의 구성된 메모리 크기만큼 증가되고, 하위 리소스 풀의 CPU 제한은 가상 시스템에 구성된 vCPU 수에 조직 VDC 수준에 지정된 vCPU 주파수를 곱한 값만큼 증가됩니다. 가상 시스템은 해당 메모리 및 CPU 예약을 0으로 설정하도록 재구성되고, 가상 시스템 배치 엔진은 가상 시스템을 제공자 VDC 리소스 풀에 배치합니다.

탄력적 할당 풀 할당 모델을 사용하면 vCloud Director에서만 제한이 모니터링되고 관리됩니다. 탄력적 기능을 사용하지 않도록 설정하면 리소스 풀 제한이 추가적으로 설정됩니다.

할당 풀 모델의 장점은 가상 시스템이 동일한 하위 리소스 풀에 있는 유휴 가상 시스템의 리소스를 활용할 수 있다는 점입니다. 이 모델은 제공자 VDC에 추가된 새 리소스를 활용할 수 있습니다.

드문 경우이지만 전원을 켜 때 원래 리소스 풀의 리소스 부족으로 인해 가상 시스템이 생성 시 할당된 리소스 풀에서 다른 리소스 풀로 전환됩니다. 이 변경 사항에는 가상 시스템 디스크 파일을 새 리소스 풀로 이동하는 데 약간의 비용이 소요될 수 있습니다.

탄력적 할당 풀 기능을 사용하지 않도록 설정하는 경우 할당 풀 조직 VDC의 동작은 vCloud Director 1.5의 할당 풀 모델과 비슷합니다. 이 모델에서는 vCPU 주파수를 구성할 수 없습니다. 오버 커밋은 보장된 리소스 비율을 설정하여 제어합니다.

기본적으로 할당 풀 VDC의 가상 시스템은 VDC의 설정에서 예약, 제한 및 할당률 설정을 가져옵니다. CPU와 메모리 모두에 대해 사용자 지정 리소스 할당 설정을 사용하여 가상 시스템을 만들거나 재구성하려면 vCloud API를 사용할 수 있습니다. "서비스 제공자를 위한 vCloud API 프로그래밍 가이드"의 내용을 참조하십시오.

선지급 할당 모델

선지급 할당 모델을 사용하면 사용자가 조직 VDC에서 vApp을 생성할 때만 리소스가 커밋됩니다. 보장할 리소스 비율을 지정하여 리소스를 오버커밋할 수 있습니다. 제공자 VDC에 여러 리소스 풀을 추가하여 선지급 조직 VDC를 탄력적으로 만들 수 있습니다.

조직에 커밋된 리소스는 가상 시스템 수준에서 적용됩니다.

가상 시스템의 전원을 켜 때 원래 리소스 풀이 가상 시스템을 수용할 수 없으면, 배치 엔진이 리소스 풀을 점검하여 다른 리소스 풀에 가상 시스템을 할당합니다. 리소스 풀에 대해 하위 리소스 풀을 사용할 수 없는 경우, vCloud Director에서 제한이 무제한이며 속도가 0인 하위 리소스 풀이 생성됩니다. 가상 시스템의 속도는 해당 제한에 커밋된 리소스를 곱한 값으로 설정되고 가상 시스템 배치 엔진이 가상 시스템을 제공자 VDC 리소스 풀에 배치합니다.

선지급 모델의 이점은 제공자 VDC에 추가된 새 리소스를 활용할 수 있다는 점입니다.

드문 경우이지만 전원을 켜 때 원래 리소스 풀의 리소스 부족으로 인해 가상 시스템이 생성 시 할당된 리소스 풀에서 다른 리소스 풀로 전환됩니다. 이 변경 사항에는 가상 시스템 디스크 파일을 새 리소스 풀로 이동하는 데 약간의 비용이 소요될 수 있습니다.

선지급 모델에서는 리소스를 미리 예약하지 않으므로 리소스가 충분하지 않을 경우 가상 시스템의 전원이 켜지지 않을 수 있습니다. 이 모델에서 작동하는 가상 시스템은 리소스가 가상 시스템 수준에서 설정되기 때문에 동일한 하위 리소스 풀에 있는 유휴 가상 시스템의 리소스를 활용할 수 없습니다.

기본적으로 선지급 VDC에서 가상 시스템은 VDC의 설정에서 예약, 제한 및 할당률 설정을 가져옵니다. CPU와 메모리 모두에 대해 사용자 지정 리소스 할당 설정을 사용하여 가상 시스템을 만들거나 재구성하려면 vCloud API를 사용할 수 있습니다. "서비스 제공자를 위한 vCloud API 프로그래밍 가이드"의 내용을 참조하십시오.

예약 풀 할당 모델

예약 풀 할당 모델을 사용하면 할당하는 모든 리소스가 조직 VDC에 즉시 커밋됩니다. 조직의 사용자는 개별 가상 시스템에 대한 예약, 제한 및 우선 순위 설정을 지정하여 오버 커밋을 제어할 수 있습니다.

이 모델에서는 하나의 리소스 풀과 하나의 하위 리소스 풀만 사용할 수 있기 때문에 배치 엔진은 가상 시스템의 전원을 켤 때 가상 시스템의 리소스 풀을 다시 할당하지 않습니다. 가상 시스템의 속도 및 제한은 수정되지 않습니다.

예약 풀 모델을 사용하면 필요할 때마다 소스를 항상 사용할 수 있습니다. 이 모델에서는 가상 시스템 속도, 제한 및 할당률을 세밀하게 제어할 수 있기 때문에, 신중하게 계획하면 예약된 리소스 사용을 최적화할 수 있습니다. 예약 풀 VDC에서 가상 시스템 리소스 할당 설정을 구성하는 방법에 대한 자세한 내용은 "vCloud Air - Virtual Private Cloud OnDemand 사용자 설명서"의 내용을 참조하십시오.

이 모델에서 예약은 항상 기본 클러스터에서 수행됩니다. 기본 클러스터에 조직 VDC를 생성하기에 충분한 리소스가 없으면 조직 VDC 생성이 실패합니다.

이 모델의 다른 제한 사항은 모델이 유연하지 않다는 점과 조직 사용자가 가상 시스템의 할당률, 속도 및 제한을 최적의 상태로 설정하지 못해 리소스가 충분히 사용되지 않을 수 있다는 점입니다.

VM 크기 조정 및 VM 배치 정책 이해

VM 크기 조정 및 VM 배치 정책을 사용하여 특정 클러스터나 호스트에서 VM(가상 시스템) 리소스 할당과 배치를 제어할 수 있습니다.

vCloud Director 10.0에는 VM 배치 정책 및 VM 크기 조정 정책이라는 개념이 도입되었습니다.

vCloud Director **시스템 관리자**는 글로벌 수준에서 VM 크기 조정 정책을 생성 및 관리하고 개별 정책을 하나 이상의 조직 VDC에 게시할 수 있습니다. VM 배치 정책은 각 제공자 VDC에 대해 생성되고 관리됩니다. VM 배치 정책의 범위가 제공자 VDC 수준이기 때문입니다. 정책을 조직 VDC에 게시하면 조직의 사용자가 해당 정책을 사용할 수 있게 됩니다. 조직 VDC에서 가상 시스템을 생성하고 관리할 때 테넌트는 사용 가능한 정책을 가상 시스템에 할당할 수 있습니다. 조직 VDC의 테넌트와 사용자는 VM 배치 정책이나 VM 크기 조정 정책의 특정 구성을 살펴볼 수 없습니다.

VM 배치 및 크기 조정 정책을 사용하면 클라우드 제공자가 차별화된 수준의 서비스(예: CPU를 많이 사용하는 프로파일 또는 메모리 사용량이 높은 프로파일)를 정의하고 제공할 수 있습니다. 여러 VM 배치 및 VM 크기 조정 정책을 조직 VDC에 게시하면, 테넌트 사용자는 조직 VDC에서 가상 시스템을 생성하고 관리할 때 모든 사용자 지정 정책과 기본 정책 중에서 선택할 수 있습니다. 시스템 기본 정책은 모든 VDC에 대해 자동 생성됩니다. **시스템 관리자**는 VDC에서 시스템 기본 정책을 삭제하고 다른 사용자 지정 정책을 기본값으로 표시할 수 있습니다. 기본 정책은 값을 정의하지 않으며 모든 가상 시스템 구성을 허용합니다.

VM 배치 정책

VM 배치 정책은 호스트나 호스트 그룹에 가상 시스템의 배치를 정의합니다. **클라우드 제공자의 관리자**가 제공자 VDC 내에 명명된 호스트 그룹을 생성하는 메커니즘입니다. 명명된 호스트 그룹은 제공자 VDC 클러스터 내에 있는 호스트의 하위 집합이며 성능 계층 또는 라이선싱 등의 기준에 따라 선택될 수 있습니다. VM 배치 정책은 테넌트 워크로드 배치에 직접적인 영향을 주는 VM-호스트 선호도 규칙을 정의합니다. 관리자는 vCenter Server에서 VM 그룹을 사용하여 명명된 호스트 그룹을 정의하거나 노출합니다. VM 그룹은 호스트 그룹에 직접 선호도가 있으며 VM 그룹이 선호하는 호스트 그룹을 나타냅니다.

제공자 VDC 수준에서 VM 배치 정책을 정의합니다. VM 배치 정책에는 다음과 같은 특성이 포함됩니다.

- 이름(제공자 VDC에서 고유해야 함)
- 설명
- 제공자 VDC의 기본 클러스터에서 선택된 하나 이상 VM 그룹의 집합. 클러스터당 하나의 VM 그룹을 선택할 수 있습니다.

가상 시스템을 생성하는 동안 VM 배치 정책은 선택 사항이며 테넌트는 가상 시스템에 VM 배치 정책을 하나만 할당할 수 있습니다.

테넌트가 조직 VDC에 가상 시스템을 생성하고 VM 배치 정책을 선택하면 vCloud Director는 정책에서 참조되는 VM 그룹에 가상 시스템을 추가합니다. 그 결과, vCloud Director에서 적절한 호스트에 가상 시스템이 생성됩니다.

VM 배치 정책에는 각 클러스터의 VM 그룹을 0개 또는 하나 포함할 수 있습니다. 예를 들어 *oracle_license* VM 배치 정책은 *oracle_license1* 및 *oracle_license2* VM 그룹으로 구성되고 *oracle_license1* VM 그룹은 *oracle_cluster1* 클러스터에 속하고 *oracle_license2* VM 그룹은 *oracle_cluster2* 클러스터에 속할 수 있습니다.

가상 시스템에 VM 배치 정책을 할당하면 배치 엔진은 이 가상 시스템이 상주하는 클러스터의 해당 VM 그룹에 이 가상 시스템을 추가합니다. 예를 들어 *oracle_cluster1* 클러스터에 가상 시스템을 배포하기로 선택하고 이 가상 시스템에 *oracle_license* VM 배치 정책을 할당하면 배치 엔진은 가상 시스템을 *oracle_license1* VM 그룹에 추가합니다.

VM 크기 조정 정책

VM 크기 조정 정책은 조직 VDC 내에서 가상 시스템에 대한 계산 리소스 할당을 정의합니다. 계산 리소스 할당에는 CPU 및 메모리 할당, 예약, 제한 및 할당률이 포함됩니다.

VM 크기 조정을 사용하면 vCloud Director **시스템 관리자**가 가상 시스템 수준에서 계산 리소스 소비의 다음과 같은 측면을 제어할 수 있습니다.

- vCPU 수 및 vCPU 클럭 속도
- 가상 시스템에 할당된 메모리 양
- 메모리 및 CPU 예약, 제한 및 할당률
- 추가 구성.

extraConfigs API 매개 변수는 가상 시스템에서 추가 구성 값으로 적용되는 키와 값 쌍 사이의 매핑을 나타냅니다. vCloud API를 사용해야만 추가 구성으로 정책을 생성할 수 있습니다. 기존 추가 구성은 **Service Provider Admin Portal UI**에서 자세한 VM 크기 조정 정책 보기의 **추가 구성** 아래에 표시됩니다.

글로벌 수준에서 VM 크기 조정 정책을 정의합니다. VM 크기 조정 정책 특성에 대한 자세한 내용은 [VM 크기 조정 정책의 특성](#) 항목을 참조하십시오.

vCloud Director는 모든 VDC에 대한 기본 VM 크기 조정 정책을 생성합니다. 기본 VM 크기 조정 정책에는 이름과 설명만 포함되며 나머지 정책 특성은 모두 비어 있습니다.

또 하나의 VM 크기 조정 정책을 조직 VDC에 대한 기본 정책으로 정의할 수도 있습니다. 테넌트가 가상 시스템에 또 다른 특정 VM 크기 조정 정책을 할당하지 않는 한, 테넌트가 조직 VDC에서 생성하는 가상 시스템의 리소스 할당 및 소비는 기본 VM 크기 조정 정책으로 제어됩니다.

테넌트가 조직 VDC 내의 개별 가상 시스템에 할당할 수 있는 최대 계산 리소스를 제한하기 위해, 클라우드 제공자가 최대 VM 크기 조정 정책을 정의할 수 있습니다. 조직 VDC에 할당되면, 최대 VM 크기 조정 정책은 조직 VDC 내의 모든 가상 시스템에 대한 계산 리소스 구성의 상한으로 작동합니다. 가상 시스템을 생성할 때 테넌트 사용자는 최대 VM 크기 조정 정책을 사용할 수 없습니다. VM 크기 조정 정책을 최대 정책으로 정의하면 vCloud Director가 정책의 콘텐츠를 내부적으로 복사하고 복사된 콘텐츠를 최대 VM 크기 조정 정책으로 사용합니다. 따라서 조직 VDC는 처음에 사용된 VM 크기 조정 정책에 종속되지 않습니다.

VM 크기 조정 정책을 사용하여 클라우드 제공자는 조직 VDC 내의 모든 가상 시스템에 대한 계산 리소스 소비를, 예를 들어 미리 정의된 세 가지 크기(소형, 중형 및 대형)로 제한할 수 있습니다. 워크플로는 다음과 같습니다.

1 시스템 관리자가 다음 특성을 사용하여 3가지 VM 크기 조정 정책을 생성합니다.

이름	특성
소형	<ul style="list-style-type: none"> ■ 설명: 소형 VM 정책 ■ 이름: 소형 ■ 메모리: 1024 ■ vCPU 수: 1
중형	<ul style="list-style-type: none"> ■ 설명: 중형 VM 정책 ■ 이름: 중형 ■ 메모리: 2048 ■ vCPU 수: 2
대형	<ul style="list-style-type: none"> ■ 설명: 대형 VM 정책 ■ 이름: 대형 ■ 메모리: 4096 ■ vCPU 수: 4

2 새 VM 크기 조정 정책을 조직 VDC에 게시합니다.

3 필요한 경우 VM 크기 조정 정책 중 하나를 조직 VDC에 대한 기본 VM 크기 조정 정책으로 정의합니다.

클라우드 제공자가 수행할 수 있는 정책 작업은 다음과 같습니다.

- 호스트나 호스트 그룹에 가상 시스템의 배치를 정의하려면 배치 정책을 생성합니다. [VM 배치 정책 만들기](#)의 내용을 참조하십시오.
- 테넌트 워크로드에 대한 물리적 계산 리소스 할당을 제어하려면 크기 조정 정책을 생성합니다. [VM 크기 조정 정책 만들기](#)의 내용을 참조하십시오.
- 하나 이상의 조직 VDC에 VM 배치나 VM 크기 조정 정책을 게시합니다. 자세한 내용은 [조직 VDC에 VM 배치 정책 추가](#)에 나와 있습니다.
- VM 배치 또는 VM 크기 조정 정책을 기본값으로 설정합니다.
- VM 배치 정책 및 VM 크기 조정 정책을 편집합니다. vCloud Director UI에서는 정책의 이름과 설명만 편집할 수 있습니다.
- 조직 VDC에서 VM 배치 또는 VM 크기 조정 정책의 게시를 취소합니다.
- VM 배치 또는 VM 크기 조정 정책을 삭제합니다. [VM 배치 정책 삭제](#) 및 [VM 크기 조정 정책 삭제](#) 항목을 참조하십시오.

ORG_VDC_MANAGE_COMPUTE_POLICIES 권한이 있는 사용자는 VM 배치와 VM 크기 조정 정책을 생성, 업데이트 및 게시할 수 있습니다.

다음 표에는 테넌트 사용자가 수행할 수 있는 VM 크기 조정 정책 및 VM 배치 정책 작업이 나열되어 있습니다.

표 6-1. 테넌트 사용자를 위한 VM 크기 조정 정책 및 VM 배치 정책 작업

작업	설명
가상 시스템 생성 중에 가상 시스템에 정책을 할당합니다.	<p>조직 VDC에서 가상 시스템을 생성할 권한이 있는 테넌트 사용자는 vCloud Director Tenant Portal을 사용하여 가상 시스템에 VM 크기 조정 및 VM 배치 정책을 선택적으로 할당할 수 있습니다. 그러면 VM 크기 조정 정책에 정의된 매개 변수가 가상 시스템의 CPU 및 메모리 소비를 제어합니다. 가상 시스템 생성 시 테넌트가 VM 배치 또는 크기 조정 정책을 반드시 할당해야 하는 것은 아닙니다. 테넌트가 가상 시스템에 할당할 VM 크기 조정 정책을 명시적으로 선택하지 않으면 기본 VM 크기 조정 정책이 가상 시스템에 적용됩니다.</p> <p>VM 배치 정책을 생성하지 않으면 테넌트에 VM 배치 정책 옵션이 표시되지 않습니다. 크기 조정 정보가 있는 배치 정책을 테넌트가 선택하면 VM 크기 조정 정책 옵션이 테넌트에 숨겨집니다. vCloud API를 사용해야만 크기 조정 정보를 사용하여 VM 배치 정책을 생성할 수 있습니다.</p> <p>VM 크기 조정 정책이 하나만 있으면 VM 크기 조정 정책 옵션이 테넌트에게 표시되지 않습니다. 시스템 관리자가 VM 크기 조정 정책에서 vCPU 수, 소켓당 코어 및 메모리 특성을 설정한 경우, 테넌트가 정책을 선택하면 다음과 같은 값이 표시되지만 편집할 수는 없습니다.</p>
기존 가상 시스템에 정책을 할당합니다.	<p>조직 VDC에서 가상 시스템을 관리할 권한이 있는 테넌트 사용자는 vCloud Director Tenant Portal을 사용하여 기존 가상 시스템의 VM 크기 조정 및 VM 배치 정책을 할당하거나 변경할 수 있습니다. 테넌트가 VM 배치 정책을 변경하면 가상 시스템은 새 VM 배치 정책에 정의된 VM-호스트 선호도 규칙에 따라 새 호스트로 이동합니다. 테넌트가 VM 크기 조정 정책을 변경하면 새 VM 크기 조정 정책에 지정된 대로 계산 리소스를 사용하도록 가상 시스템이 재구성됩니다.</p>

VM 배치 및 VM 크기 조정 정책 작업에 대한 워크플로는 다음과 같습니다.

- 1 **시스템 관리자**가 VM 배치 정책을 하나 이상 생성합니다. [VM 배치 정책 만들기](#)의 내용을 참조하십시오.
- 2 **시스템 관리자**가 VM 크기 조정 정책을 하나 이상 생성합니다. [VM 크기 조정 정책 만들기](#)의 내용을 참조하십시오.

VM 크기 조정 정책의 이름은 단일 vCloud Director 사이트에서 고유합니다. VM 배치 정책의 이름은 정책의 제공자 VDC 범위 내에서 고유합니다.

- 3 **시스템 관리자**가 VM 배치 및 VM 크기 조정 정책을 하나 이상의 조직 VDC에 게시합니다. [조직 VDC에 VM 배치 정책 추가](#)의 내용을 참조하십시오.

VM 배치 정책을 게시하면 가상 시스템 생성 및 가상 시스템 편집 중에 조직 VDC의 테넌트 사용자가 사용할 수 있습니다.

- 4 가상 시스템을 생성하거나 업데이트할 때, 테넌트는 vCloud API 또는 vCloud Director Tenant Portal을 사용하여 VM 크기 조정 정책 및 VM 배치 정책을 가상 시스템에 할당할 수 있습니다.

VM 크기 조정 정책의 특성

VM(가상 시스템) 크기 조정 정책을 생성할 때, 사용 가능한 모든 특성의 하위 집합을 지정할 수 있습니다. 유일한 필수 특성은 VM 크기 조정 정책 이름입니다.

VM 크기 조정 정책에는 두 가지 유형의 매개 변수가 있습니다.

- 개별 VM 크기 조정 구성 - 현재 정책에 따라 VM에 대해 지정된 RAM, vCPU 수 및 소켓당 코어를 미리 구성합니다.
- 최대 리소스에 대한 제약 조건 - 현재 정책에 따라 단일 VM별 메모리 및 CPU 소비에 대한 제한을 미리 구성합니다.

다음 표에는 VM 크기 조정 정책 내에서 정의할 수 있는 모든 특성이 나열되어 있습니다.

표 6-2. VDC 계산 정책 특성

VDC 계산 정책 특성	API 매개 변수	설명
Name	name	VM 크기 조정 정책의 식별자로 사용되는 필수 매개 변수입니다.
Description	description	VM 크기 조정 정책에 대한 간단한 설명을 나타냅니다.
vCPU Speed	cpuSpeed	코어의 vCPU 속도를 MHz 또는 GHz 단위로 정의합니다.
vCPU Count	cpuCount	VM에 대해 구성된 vCPU 수를 정의합니다. VM 하드웨어 구성입니다. 테넌트가 VM 크기 조정 정책을 VM에 할당하면 이 수는 VM에 대해 구성된 vCPU 수가 됩니다.
Cores Per Socket	coresPerSocket	VM에 대한 소켓당 코어 수입니다. VM 하드웨어 구성입니다. VM 크기 조정 정책에 정의된 vCPU 수는 소켓당 코어 수로 나눌 수 있어야 합니다. vCPU 수를 소켓당 코어 수로 나눌 수 없는 경우에는 소켓당 코어 수가 유효하지 않은 상태가 됩니다.

표 6-2. VDC 계산 정책 특성 (계속)

VDC 계산 정책 특성	API 매개 변수	설명
CPU Reservation Guarantee	cpuReservation Guarantee	VM에서 예약된 CPU 리소스의 양을 정의합니다. VM에 할당된 CPU는 vCPU 수에 vCPU 속도(MHz)를 곱한 값과 같습니다. 특성 값의 범위는 0에서 1 사이입니다. CPU 예약 보장의 값이 0이면 CPU 예약이 없음을 의미합니다. 값 1이면 CPU 100% 예약을 의미합니다.
CPU Limit	cpuLimit	VM에 대한 CPU 제한을 MHz 또는 GHz 단위로 정의합니다. VDC 계산 정책에 정의되어 있지 않으면, CPU 제한은 vCPU 속도에 vCPU 수를 곱한 값과 같습니다.
CPU Shares	cpuShares	VM에 대한 CPU 할당량을 정의합니다. 할당량은 가상 데이터 센터 내에서 VM의 상대적인 중요도를 지정합니다. 다른 VM에 비해 CPU 할당량이 두 배인 VM은, 두 가상 시스템이 리소스를 놓고 경쟁하는 경우 다른 VM에 비해 CPU를 두 배로 사용할 수 있습니다. VDC 계산 정책에 정의되지 않으면 일반 할당량이 VM에 적용됩니다.
Memory	memory	VM에 대해 구성된 메모리를 MB 또는 GB 단위로 정의합니다. VM 하드웨어 구성입니다. 테넌트가 VM 크기 조정 정책을 VM에 할당하면 VM은 이 특성에 정의된 메모리 양을 받습니다.
Memory Reservation Guarantee	memoryReservation Guarantee	VM에 대해 구성된 예약 메모리 양을 정의합니다. 특성 값의 범위는 0에서 100% 사이입니다.
Memory Limit	memoryLimit	VM에 대한 메모리 제한을 MB 또는 GB 단위로 정의합니다. VM 크기 조정 정책에 정의되지 않으면, 메모리 제한은 VM에 할당된 메모리와 동일합니다.
Memory Shares	memoryShares	VM에 대한 메모리 할당량을 정의합니다. 할당량은 가상 데이터 센터 내에서 VM의 상대적인 중요도를 지정합니다. 두 VM 중 하나의 VM의 메모리 할당량이 다른 VM의 두 배인 경우, 두 가상 시스템이 리소스를 놓고 경쟁하는 경우에 비해 메모리를 두 배로 사용할 수 있습니다. VDC 계산 정책에 정의되지 않으면 일반 할당량이 VM에 적용됩니다.
Extra Configurations	extraConfigs	VM에서 추가 구성 값으로 적용되는 키와 값 쌍 사이의 매핑을 나타냅니다. vCloud API를 통해서만 추가 구성으로 정책을 생성할 수 있습니다. 기존 추가 구성은 Service Provider Admin Portal UI에서 자세한 VM 크기 조정 정책 보기의 추가 구성 아래에 표시됩니다.

VM 배치 정책 만들기


VM 배치 정책은 제공자 VDC 정책에 대한 참조가 포함된 VDC 계산 정책입니다. VM 배치 정책을 사용하여 특정 호스트, 호스트 그룹 또는 클러스터에서의 VM 배치를 정의할 수 있습니다.

사전 요구 사항

- 환경에 제공자 VDC가 하나 이상 있는지 확인합니다.
- 환경에 하나 이상의 VM 그룹이 있는지 확인합니다.

VM 그룹은 양수 또는 음수 선호도가 있는 호스트 그룹에 연결할 수 있는 VM의 모음입니다. 양수 선호도 규칙을 통해 특정 호스트에 VM 그룹이 배치되도록 할 수 있습니다. 반선호도(음수 선호도하라고도 함) 규칙은 서로 다른 호스트에 VM 그룹을 배치하여, 단일 호스트에 장애가 발생할 경우 모든 VM이 한꺼번에 실패하지 않도록 합니다. VM 그룹은 vCenter Server UI나 vCloud Director API를 통해 생성할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭합니다.
- 3 목록에서 제공자 VDC를 클릭합니다.
- 4 **VM 배치 정책** 탭을 클릭하고 **새로 만들기**를 클릭합니다.
- 5 (선택 사항) 마법사의 **VM 배치 정책이란 무엇입니까** 페이지에서 확인란을 선택하여 VM 배치 정책 정보가 표시되는 것을 중지합니다.
- 6 **다음**을 클릭합니다.
- 7 VM 배치 정책의 이름과 설명(선택 사항)을 입력합니다.
- 8 VM 그룹 또는 VM을 연결할 논리적 VM 그룹을 선택하고 **다음**을 클릭합니다.

둘 이상의 논리적 그룹을 선택할 때 테넌트가 이 정책을 VM에 적용하면, VM은 선택한 논리적 VM 그룹에 포함된 모든 VM 그룹의 멤버가 됩니다. VM은 이러한 그룹의 VM에 적용되는 모든 선호도의 조합으로 조건이 조정됩니다.

클러스터당 하나의 VM 그룹을 선택하여 인라인 논리적 VM 그룹을 생성할 수 있습니다. 이 논리적 VM 그룹에는 이름이 없으며 선택한 VM 배치 정책에만 사용할 수 있습니다.

- 9 VM 배치 정책 설정을 검토하고 **마침**을 클릭합니다.

다음에 수행할 작업

- [VM 크기 조정 정책 만들기](#).
- [조직 VDC에 VM 배치 정책 추가](#).

조직 VDC에 VM 배치 정책 추가


VM 배치 정책을 만들면 테넌트에 보이지 않습니다. VM 배치 정책을 테넌트가 사용할 수 있도록 조직 VDC에 게시할 수 있습니다.

VM 배치 정책을 조직 VDC에 게시하면 정책이 테넌트에 표시됩니다. 테넌트는 새 독립형 VM을 생성하거나 템플릿에서 VM을 생성하거나, VM을 편집하거나, vApp에 VM을 추가하거나, vApp 템플릿에서 vApp을 생성할 때 정책을 선택할 수 있습니다. 테넌트가 사용할 수 있는 VM 배치 정책은 삭제할 수 없습니다.

사전 요구 사항

- 환경에 조직 VDC가 하나 이상 있는지 확인합니다. [조직 가상 데이터 센터 만들기](#)의 내용을 참조하십시오.
- 하나 이상의 VM 배치 정책이 있는지 확인합니다. [VM 배치 정책 만들기](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 3 조직 VDC를 선택하고 **VM 배치 정책** 탭을 클릭합니다.
- 4 **추가**를 클릭합니다.
- 5 조직 VDC에 추가할 VM 배치 정책을 선택하고 **확인**을 클릭합니다.

다음에 수행할 작업

- 정책을 선택하고 **제거**를 클릭하여 정책의 게시를 취소합니다.
- VM 배치 정책을 선택하고 **기본값으로 설정**을 클릭하여 해당 정책이 VM과 vApp 생성 및 VM 편집 중에 테넌트에 대한 기본 선택 항목으로 표시되도록 합니다. 조직 VDC에 둘 이상의 VM 배치 정책이 게시된 경우 테넌트는 기본 정책이 아닌 정책을 선택할 수 있습니다.


VM 배치 정책 삭제

VM 배치 정책이 테넌트에 게시되지 않은 경우 제공자 VDC에서 삭제할 수 있습니다.

사전 요구 사항

- 환경에 하나 이상의 VM 배치 정책이 있는지 확인합니다.
- VM 배치 정책이 조직 VDC에 추가되지 않았는지 확인합니다. 테넌트가 사용할 수 있는 VM 배치 정책은 삭제할 수 없습니다.


절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭합니다.
- 3 목록에서 제공자 VDC를 클릭합니다.
- 4 **VM 배치 정책** 탭을 클릭하고 VM 배치 정책을 선택합니다.
- 5 **삭제**를 클릭합니다.

VM 크기 조정 정책 만들기

테넌트가 조직 VDC의 개별 VM에 적용할 수 있는 미리 정의된 CPU 및 메모리 사용량 제약 조건을 사용할 수 있도록 VM 크기 조정 정책을 생성할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **VM 크기 조정**을 클릭합니다.
- 3 **새로 만들기**를 클릭합니다.
- 4 VM 크기 조정 정책의 이름과 설명(선택 사항)을 입력합니다.
- 5 **다음**을 클릭합니다.
- 6 **CPU** 페이지에서 정책에 적용할 CPU 할당 설정을 선택하고 **다음**을 클릭합니다.
- 7 정책에 적용할 메모리 할당 설정을 선택하고 **다음**을 클릭합니다.
- 8 VM 크기 조정 정책 설정을 검토하고 **마침**을 클릭합니다.

다음에 수행할 작업

- VM 크기 조정 정책을 생성한 후에는 VM 크기 조정 정책 이름과 설명만 편집할 수 있습니다. [VM 크기 조정 정책 편집](#)의 내용을 참조하십시오.
- 조직 VDC에 [VM 크기 조정 정책 추가](#).
- [VM 배치 정책 만들기](#).

조직 VDC에 VM 크기 조정 정책 추가


VM 크기 조정 정책을 만들면 테넌트에 보이지 않습니다. VM 크기 조정 정책을 테넌트가 사용할 수 있도록 조직 VDC에 게시할 수 있습니다.

VM 크기 조정 정책을 조직 VDC에 게시하면 정책이 테넌트에 표시됩니다. 테넌트는 새 독립형 VM을 생성하거나 템플릿에서 VM을 생성하거나, VM을 편집하거나, vApp에 VM을 추가하거나, vApp 템플릿에서 vApp을 생성할 때 정책을 선택할 수 있습니다. 테넌트가 사용할 수 있는 VM 크기 조정 정책은 삭제할 수 없습니다.

사전 요구 사항

- 환경에 조직 VDC가 하나 이상 있는지 확인합니다. [조직 가상 데이터 센터 만들기](#)의 내용을 참조하십시오.
- 하나 이상의 VM 크기 조정 정책이 있는지 확인합니다. [VM 크기 조정 정책 만들기](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 3 조직 VDC를 선택하고 **VM 크기 조정 정책** 탭을 클릭합니다.
- 4 **추가**를 클릭합니다.

5 조직 VDC에 추가할 VM 크기 조정 정책을 선택하고 **확인**을 클릭합니다.

다음에 수행할 작업

- 정책을 선택하고 **제거**를 클릭하여 정책의 게시를 취소합니다.
- VM 크기 조정 정책을 선택하고 **기본값으로 설정**을 클릭하여 해당 정책이 VM과 vApp 생성 및 VM 편집 중에 테넌트에 대한 기본 선택 항목으로 표시되도록 합니다. 조직 VDC에 둘 이상의 VM 크기 조정 정책이 게시된 경우 테넌트는 기본 정책이 아닌 정책을 선택할 수 있습니다.


VM 크기 조정 정책 편집

VM 크기 조정 정책을 생성한 후에는 해당 정책의 이름과 설명만 편집할 수 있습니다. CPU 및 메모리 매개 변수 편집은 지원되지 않습니다.

사전 요구 사항

- 환경에 조직 VDC가 하나 이상 있는지 확인합니다. [조직 가상 데이터 센터 만들기](#)의 내용을 참조하십시오.
- 하나 이상의 VM 크기 조정 정책이 있는지 확인합니다. [VM 크기 조정 정책 만들기](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **VM 크기 조정**을 클릭합니다.
- 3 편집할 VM 크기 조정 정책의 이름을 클릭합니다.
- 4 정책의 이름과 설명을 편집하려면 **편집**을 클릭합니다.
- 5 **저장**을 클릭합니다.

다음에 수행할 작업

[조직 VDC에 VM 크기 조정 정책 추가](#)


VM 크기 조정 정책 삭제

테넌트에 게시되지 않은 VM 크기 조정 정책은 삭제할 수 있습니다.

사전 요구 사항

- 환경에 하나 이상의 VM 크기 조정 정책이 있는지 확인합니다.
- VM 크기 조정 정책이 조직 VDC에 추가되지 않았는지 확인합니다. 테넌트가 사용할 수 있는 VM 크기 조정 정책은 삭제할 수 없습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.

- 2 왼쪽 패널에서 **VM 크기 조정**을 클릭합니다.
- 3 VM 크기 조정 정책을 선택하고 **삭제**를 클릭합니다.


조직 가상 데이터 센터 만들기

조직에 리소스를 할당하려면 조직 가상 데이터 센터를 만들어야 합니다. 조직 가상 데이터 센터는 제공자 가상 데이터 센터에서 리소스를 가져옵니다. 한 조직에 다수의 조직 가상 데이터 센터가 있을 수 있습니다.

사전 요구 사항

제공자 가상 데이터 센터를 만듭니다. [제공자 가상 데이터 센터 생성](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **조직 VDC**를 클릭하고 **새로 만들기**를 클릭합니다.
- 3 새 조직 가상 데이터 센터의 이름과 설명(선택 사항)을 입력합니다.
- 4 (선택 사항) 생성 시 새 조직 가상 데이터 센터를 사용하지 않도록 설정하려면 **조직 VDC를 사용하도록 설정** 토글을 해제합니다.

사용자는 사용하지 않도록 설정된 조직 가상 데이터 센터에 vApp을 배포할 수 없습니다.

- 5 **다음**을 클릭합니다.
- 6 가상 데이터 센터를 추가할 조직의 이름 옆에 있는 라디오 버튼을 선택하고 **다음**을 클릭합니다.
- 7 조직 가상 데이터 센터에서 계산 및 스토리지 리소스를 가져올 제공자 가상 데이터 센터 이름 옆에 있는 라디오 버튼을 선택하고 **다음**을 클릭합니다.

제공자 가상 데이터 센터 목록에는 사용 가능한 리소스에 대한 정보와 함께 사이트의 사용 가능한 제공자 가상 데이터 센터가 모두 표시됩니다. 네트워크 목록에는 선택한 제공자 가상 데이터 센터에서 사용할 수 있는 네트워크에 대한 정보가 표시됩니다.

- 8 조직 가상 데이터 센터에 대한 할당 모델을 선택하고 **다음**을 클릭합니다.

옵션	설명
할당 풀	제공자 가상 데이터 센터에서 할당하는 리소스의 일정 비율이 조직 가상 데이터 센터에 커밋됩니다. CPU 및 메모리 모두에 대해 비율을 지정할 수 있습니다.
선지급	사용자가 조직 가상 데이터 센터에서 vApp을 만들 때만 리소스가 커밋됩니다.
예약 풀	할당하는 모든 리소스가 조직 가상 데이터 센터에 즉시 커밋됩니다.
Flex	VDC와 개별 가상 시스템 수준 모두에서 리소스 소비를 제어할 수 있습니다. Flex 할당 모델은 조직 VDC 계산 정책의 기능을 지원합니다. Flex 할당 모델은 다른 할당 모델에서 사용할 수 있는 모든 할당 구성을 지원합니다.

9 선택한 할당 모델에 대한 할당 설정을 구성하고 다음을 클릭합니다.

옵션	설명	할당 모델
탄력성	탄력적 풀 기능을 사용하거나 사용하지 않도록 설정합니다. 탄력적 조직 VDC는 제공자 VDC에 연결된 모든 리소스 풀을 포함하고 사용합니다.	Flex
VM 메모리 오버헤드 포함	메모리 오버헤드를 포함하거나 제외합니다.	Flex
CPU 할당	조직 가상 데이터 센터에서 실행되는 가상 시스템에 할당하려는 최대 CPU 용량입니다.	<input type="checkbox"/> 할당 풀 <input type="checkbox"/> 예약 풀 <input type="checkbox"/> Flex
CPU 리소스가 예약된 값 이상으로 증가하도록 허용	이 조직 가상 데이터 센터에 무제한 CPU 리소스를 제공하려면 이 토글을 설정합니다.	예약 풀
CPU 할당량	이 조직 가상 데이터 센터에 대한 최대 CPU 소비량입니다.	<input type="checkbox"/> 선지급 <input type="checkbox"/> Flex
보장된 CPU 리소스	조직 가상 데이터 센터에서 실행되는 가상 시스템에 보장하려는 CPU 리소스 비율입니다. 100% 미만을 보장하여 CPU 리소스의 오버 커밋을 제어할 수 있습니다. 할당 풀 할당 모델의 경우, 보장 비율은 조직 가상 데이터 센터에 대해 커밋되는 CPU 할당 비율도 결정합니다.	<input type="checkbox"/> 할당 풀 <input type="checkbox"/> 선지급 <input type="checkbox"/> Flex
vCPU 속도	vCPU 속도입니다. 조직 가상 데이터 센터에서 실행되는 가상 시스템에는 vCPU당 이 정도의 GHz가 할당됩니다.	<input type="checkbox"/> 선지급 <input type="checkbox"/> Flex
메모리 할당	조직 가상 데이터 센터에서 실행되는 가상 시스템에 할당하려는 최대 메모리 용량입니다.	<input type="checkbox"/> 할당 풀 <input type="checkbox"/> 예약 풀
메모리 할당량	조직 가상 데이터 센터에 대한 최대 메모리 소비량입니다.	<input type="checkbox"/> 선지급 <input type="checkbox"/> Flex
보장된 메모리 리소스	조직 가상 데이터 센터에서 실행되는 가상 시스템에 보장하려는 메모리 리소스의 비율입니다. 100% 미만을 보장하여 리소스를 오버커밋할 수 있습니다. 할당 풀 할당 모델의 경우, 보장 비율은 조직 가상 데이터 센터에 대해 커밋되는 메모리 할당 비율도 결정합니다.	<input type="checkbox"/> 할당 풀 <input type="checkbox"/> 선지급 <input type="checkbox"/> Flex
최대 VM 수	조직 가상 데이터 센터에 존재할 수 있는 최대 가상 시스템 수입니다.	<input type="checkbox"/> 할당 풀 <input type="checkbox"/> 선지급 <input type="checkbox"/> 예약 풀 <input type="checkbox"/> Flex

10 조직 가상 데이터 센터에 대한 스토리지 설정을 구성하고 다음을 클릭합니다.

목록에는 소스 제공자 가상 데이터 센터에서 사용하도록 설정된 스토리지 정책이 포함됩니다.

- 조직 가상 데이터 센터에 추가하려는 하나 이상의 스토리지 정책 확인란을 선택합니다.
- (선택 사항) 선택한 스토리지 정책에 할당된 스토리지 용량을 제한하려면 **할당 유형** 셀의 드롭다운 메뉴에서 **제한됨**을 선택하고 **할당된 스토리지** 셀에 최대 용량을 입력합니다.

- c (선택 사항) 기본 스토리지 정책을 변경하려면 **기본 인스턴스화 정책** 드롭다운 메뉴에서 대상 기본 스토리지 정책을 선택합니다.

vCloud Director는 스토리지 정책이 가상 시스템이나 vApp 템플릿 수준에서 지정되지 않은 모든 가상 시스템 프로비저닝 작업에 기본 스토리지 정책을 사용합니다.

- d (선택 사항) 조직 가상 데이터 센터에서 가상 시스템의 썬 프로비저닝을 사용하도록 설정하려면 **썬 프로비저닝** 토글을 설정합니다.
- e (선택 사항) 조직 가상 데이터 센터에서 가상 시스템의 빠른 프로비저닝을 사용하지 않도록 설정하려면 **빠른 프로비저닝** 토글을 해제합니다.

11 조직 가상 데이터 센터에 대한 네트워크 풀 설정을 구성하고 다음을 클릭합니다.

vCloud Director는 네트워크 풀을 사용하여 vApp 네트워크 및 내부 조직 가상 데이터 센터 네트워크를 생성합니다.

- 이 단계에서 네트워크 풀 추가를 건너뛰려면 **네트워크 풀 사용** 토글을 해제합니다.
- 네트워크 풀을 구성하려면 대상 네트워크 풀 이름 옆에 있는 라디오 버튼을 선택하고 조직 가상 데이터 센터에 대한 할당량을 입력합니다.


할당량은 이 네트워크 풀이 지원하는 조직 가상 데이터 센터의 프로비저닝된 네트워크의 최대 수입니다. 선택된 네트워크 풀에서 사용할 수 있는 네트워크의 수를 초과해서는 안 됩니다.

12 완료 준비 페이지를 검토하고 마침을 클릭합니다.

조직 가상 데이터 센터 사용 또는 사용 안 함

추가 vApp 및 가상 시스템이 조직 가상 데이터 센터의 계산 및 스토리지 리소스를 사용하지 못하게 하려면 해당하는 조직 가상 데이터 센터를 사용하지 않도록 설정하면 됩니다. 실행 중인 vApp 및 전원이 켜진 가상 시스템은 계속 실행되지만 vApp 또는 가상 시스템을 추가로 만들거나 시작할 수는 없습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 3 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 선택하고 **사용** 또는 **사용 안 함**을 클릭합니다.
- 4 **확인**을 클릭하여 확인합니다.

조직 가상 데이터 센터 삭제


조직에서 조직 가상 데이터 센터의 모든 리소스를 제거하려면 조직 가상 데이터 센터를 삭제하면 됩니다. 소스 제공자 가상 데이터 센터에서는 리소스가 영향을 받지 않은 상태로 유지됩니다.

중요 이 작업을 수행하면 조직 가상 데이터 센터 및 여기에 포함된 VM, vApp, 조직 가상 데이터 센터 네트워크 및 Edge 게이트웨이가 영구적으로 모두 제거됩니다.

사전 요구 사항

대상 조직 가상 데이터 센터에 속하는 특정 VM, vApp, vApp 템플릿 또는 미디어 파일을 유지하려면 다른 조직 가상 데이터 센터로 이동합니다.


절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 3 제거할 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 선택하고 **삭제**를 클릭합니다.
- 4 이 조직 가상 데이터 센터에 VM, vApp, 조직 가상 데이터 센터 네트워크 및 Edge 게이트웨이와 같은 리소스가 포함되어 있는 경우 제거를 확인하려면 각 리소스 유형에 대한 확인란을 선택합니다.
- 5 **삭제**를 클릭하여 확인합니다.

조직 가상 데이터 센터의 이름 및 설명 수정

vCloud Director 설치 환경이 확장됨에 따라 기존 조직 가상 데이터 센터에 더 의미 있는 이름이나 설명을 할당하려고 할 수 있습니다.

절차


- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭하고 대상 조직 가상 데이터 센터의 이름을 클릭합니다.
- 3 **일반** 탭의 오른쪽 위에서 **편집**를 클릭합니다.
- 4 새 이름과 설명을 입력하고 **저장**을 클릭합니다.

조직 가상 데이터 센터의 할당 모델 설정 수정

조직 가상 데이터 센터 할당 모델은 변경할 수 없지만 조직 가상 데이터 센터를 생성하는 동안 지정한 할당 모델에 대한 할당 설정은 변경할 수 있습니다.

조직 가상 데이터 센터를 생성하는 동안 구성한 할당 모델의 할당 설정을 수정할 수 있습니다. [단계 9](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭하고 대상 조직 가상 데이터 센터의 이름을 클릭합니다.
- 3 **할당** 탭의 오른쪽 상단 모서리에서 **편집**을 클릭합니다.
- 4 할당 모델 설정을 편집하고 **저장**을 클릭합니다.


조직 가상 데이터 센터의 스토리지 설정 수정

조직 가상 데이터 센터를 생성하는 동안 구성한 스토리지 설정을 수정할 수 있습니다.

조직 가상 데이터 센터의 VM 프로비저닝 설정 수정

조직 가상 데이터 센터를 생성할 때 구성한 가상 시스템 쉘 프로비저닝 및 빠른 프로비저닝 설정을 수정할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭하고 대상 조직 가상 데이터 센터의 이름을 클릭합니다.
- 3 **스토리지** 탭의 오른쪽 위에서 **편집**을 클릭합니다.
- 4 (선택 사항) 쉘 프로비저닝 설정을 수정합니다.
 - 조직 가상 데이터 센터에서 가상 시스템의 쉘 프로비저닝을 사용하지 않도록 설정하려면 **셸 프로비저닝** 토글을 끕니다.
 - 조직 가상 데이터 센터에서 가상 시스템의 쉘 프로비저닝을 사용하도록 설정하려면 **셸 프로비저닝** 토글을 켭니다.
- 5 (선택 사항) 빠른 프로비저닝 설정을 수정합니다.
 - 조직 가상 데이터 센터에서 가상 시스템의 빠른 프로비저닝을 사용하도록 설정하려면 **빠른 프로비저닝** 토글을 켭니다.
 - 조직 가상 데이터 센터에서 가상 시스템의 빠른 프로비저닝을 사용하지 않도록 설정하려면 **빠른 프로비저닝** 토글을 해제합니다.
- 6 **편집**을 클릭합니다.


VM 스토리지 정책을 조직 가상 데이터 센터에 추가

이전에 지원 제공자 가상 데이터 센터에 추가한 VM 스토리지 정책을 지원하도록 조직 가상 데이터 센터를 구성할 수 있습니다.

사전 요구 사항

소스 제공자 가상 데이터 센터에 대상 VM 스토리지 정책을 추가했습니다. [VM 스토리지 정책을 제공자 가상 데이터 센터에 추가](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭하고 대상 조직 가상 데이터 센터의 이름을 클릭합니다.
- 3 **스토리지** 탭을 클릭하고 **추가**를 클릭합니다.

소스 제공자 가상 데이터 센터에서 사용 가능한 추가 스토리지 정책 목록을 볼 수 있습니다.

- 4 추가할 하나 이상의 스토리지 정책의 확인란을 선택하고 **추가**를 클릭합니다.

조직 가상 데이터 센터의 기본 스토리지 정책 변경


조직 가상 데이터 센터를 생성하는 동안 구성한 기본 스토리지 정책을 변경할 수 있습니다.

vCloud Director는 스토리지 정책이 가상 시스템이나 vApp 템플릿 수준에서 지정되지 않은 모든 가상 시스템 프로비저닝 작업에 기본 스토리지 정책을 사용합니다.

사전 요구 사항

- 조직 가상 데이터 센터에 대상 기본 스토리지 정책이 추가되었습니다. [VM 스토리지 정책을 조직 가상 데이터 센터에 추가](#)의 내용을 참조하십시오.
- 대상 기본 스토리지 정책이 조직 가상 데이터 센터에서 사용하도록 설정되었습니다. [조직 가상 데이터 센터에서 스토리지 정책 사용 또는 사용 안 함](#)의 내용을 참조하십시오.

절차


- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭하고 대상 조직 가상 데이터 센터의 이름을 클릭합니다.
- 3 **스토리지** 탭을 클릭합니다.
- 4 대상 기본 스토리지 정책 이름 옆에 있는 라디오 버튼을 클릭하고 **기본값으로 설정**을 클릭합니다.
- 5 **확인**을 클릭하여 확인합니다.

조직 가상 데이터 센터에서 스토리지 정책 제한 편집

조직 가상 데이터 센터를 생성하는 동안 스토리지 정책에 대해 구성한 할당된 스토리지 용량 제한을 변경할 수 있습니다.

할당된 스토리지 용량을 무제한으로 설정하거나 조직 가상 데이터 센터의 스토리지 정책에 할당된 최대 스토리지 용량을 구성할 수 있습니다.

절차


- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭하고 대상 조직 가상 데이터 센터의 이름을 클릭합니다.
- 3 **스토리지** 탭을 클릭합니다.
- 4 대상 스토리지 정책의 이름 옆에 있는 라디오 버튼을 클릭하고 **제한 편집**을 클릭합니다.
- 5 스토리지 정책에 대한 제한 설정을 구성합니다.
 - 제한을 설정하려면 위쪽 라디오 버튼을 선택하고 조직 가상 데이터 센터의 스토리지 정책에 대한 최대 스토리지 리소스 양을 입력합니다.
 - 제한을 설정하지 않으려면 **무제한** 라디오 버튼을 선택합니다.
- 6 **편집**을 클릭합니다.

조직 가상 데이터 센터에서 VM 스토리지 정책의 메타데이터 수정

조직 가상 데이터 센터에서 스토리지 정책의 메타데이터를 추가, 편집 및 삭제할 수 있습니다.

개체 메타데이터를 사용하면 사용자 정의 *name=value* 쌍을 조직 가상 데이터 센터의 스토리지 정책과 연결할 수 있습니다. vCloud API 쿼리 필터 식에서 개체 메타데이터를 사용할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭하고 대상 조직 가상 데이터 센터의 이름을 클릭합니다.
- 3 **스토리지** 탭을 클릭합니다.
- 4 대상 스토리지 정책의 이름 옆에 있는 라디오 버튼을 클릭하고 **메타데이터**를 클릭합니다.
- 5 **편집**을 클릭합니다.
- 6 (선택 사항) 키-값 쌍을 추가하려면 **추가**를 클릭하고 이름 및 값을 입력한 다음 새로운 키-값 쌍의 유형을 선택합니다.
- 7 (선택 사항) 키-값 쌍을 편집하려면 새 이름과 값을 입력하고 키-값 쌍의 새 유형을 선택합니다.
- 8 (선택 사항) 키-값 쌍을 제거하려면 해당 행의 오른쪽 끝에서 **삭제** 아이콘을 클릭합니다.
- 9 **저장**을 클릭하고 **확인**을 클릭합니다.

조직 가상 데이터 센터에서 스토리지 정책 사용 또는 사용 안 함


추가 vApp 및 가상 시스템이 조직 가상 데이터 센터의 특정 스토리지 정책을 사용하지 못하게 하려면 조직 가상 데이터 센터에서 해당 스토리지 정책을 사용하지 않도록 설정하면 됩니다. 실행 중인 vApp 및 전원이 켜진 가상 시스템은 계속 실행되지만 이 스토리지 정책에서 vApp 또는 가상 시스템을 추가로 만들거나 시작할 수는 없습니다.

기본 스토리지 정책은 사용하지 않도록 설정할 수 없습니다.

사전 요구 사항

기본 스토리지 정책을 사용하지 않도록 설정하려면 [조직 가상 데이터 센터의 기본 스토리지 정책 변경](#)의 지침을 따르십시오.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭하고 대상 조직 가상 데이터 센터의 이름을 클릭합니다.
- 3 **스토리지** 탭을 클릭합니다.
- 4 대상 스토리지 정책의 이름 옆에 있는 라디오 버튼을 클릭하고 **사용** 또는 **사용 안 함**을 클릭합니다.
- 5 **확인**을 클릭하여 확인합니다.


조직 가상 데이터 센터에서 스토리지 정책 삭제

조직 가상 데이터 센터가 스토리지 정책을 사용하지 못하도록 하려면 조직 가상 데이터 센터에서 스토리지 정책을 제거하면 됩니다. 실행 중인 vApp 및 전원이 켜진 가상 시스템은 계속 실행되지만 이 스토리지 정책에서 vApp 또는 가상 시스템을 추가로 만들거나 시작할 수는 없습니다.

사전 요구 사항

제거하려는 스토리지 정책을 사용하지 않도록 설정합니다. [조직 가상 데이터 센터에서 스토리지 정책 사용 또는 사용 안 함](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭하고 대상 조직 가상 데이터 센터의 이름을 클릭합니다.
- 3 **스토리지** 탭을 클릭합니다.
- 4 대상 스토리지 정책의 이름 옆에 있는 라디오 버튼을 클릭하고 **제거**를 클릭합니다.
- 5 **제거**를 클릭하여 확인합니다.

조직 가상 데이터 센터의 네트워크 설정 편집

조직 가상 데이터 센터에서 새 네트워크가 프로비저닝되는 네트워크 풀을 변경할 수 있습니다. 또한 크로스 가상 데이터 센터 네트워킹에 적합하도록 조직 가상 데이터 센터를 설정할 수 있습니다.


네트워크 풀은 vApp 네트워크, 라우팅된 조직 VDC 네트워크 및 내부 조직 VDC 네트워크를 만드는 데 사용할 수 있는 구별되지 않은 네트워크의 그룹입니다. 새 네트워크에 대한 네트워크 풀을 변경할 수 있습니다. 기존 네트워크는 이전 네트워크 풀을 계속 사용합니다.

크로스 가상 데이터 센터 네트워킹을 사용하도록 설정된 조직 가상 데이터 센터를 사용하는 경우 관련 권한을 가진 조직 사용자는 데이터 센터 그룹을 만들 수 있고 이러한 그룹에서 스트레치된 계층 2 네트워크를 만들 수 있습니다.

사전 요구 사항

조직 가상 데이터 센터에 대해 크로스 VDC 네트워킹을 사용하도록 설정하려면 지원 제공자 가상 데이터 센터에서 크로스 vCenter NSX를 구성했는지 확인합니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭하고 대상 조직 가상 데이터 센터의 이름을 클릭합니다.
- 3 **네트워크 풀** 탭의 오른쪽 위에서 **편집**을 클릭합니다.
이 조직 가상 데이터 센터에서 사용되는 네트워크의 수를 볼 수 있습니다.
- 4 (선택 사항) 이 조직 가상 데이터 센터에 대한 네트워크 풀 설정을 구성합니다.
 - 이 조직 가상 데이터 센터에 대해 네트워크 풀을 사용하지 않으려는 경우 **네트워크 풀 사용** 토글을 해제합니다.
 - 이 조직 가상 데이터 센터에 대해 네트워크 풀을 구성하려는 경우 다음 단계를 따릅니다.
 - a **네트워크 풀 사용** 토글을 설정합니다.
해당 사용 상태, 사용 가능한 네트워크 및 용량에 대한 정보와 함께 사용 가능한 네트워크 풀의 목록을 볼 수 있습니다.
 - b 대상 리소스 풀의 이름 옆에 있는 라디오 버튼을 선택합니다.
 - c 조직 가상 데이터 센터에서 네트워크 풀에 대한 할당량을 구성합니다.
할당량은 프로비저닝된 최대 네트워크 수입입니다. 선택된 네트워크 풀에서 사용할 수 있는 네트워크의 수를 초과해서는 안 됩니다.
- 5 이 조직 가상 데이터 센터에 대해 크로스 가상 데이터 센터 네트워킹을 사용하도록 설정하려면 **크로스 VDC 네트워킹** 토글을 설정합니다.
- 6 **저장**을 클릭합니다.

결과

vCloud Director 테넌트 포털에서 크로스 가상 데이터 센터 네트워킹을 사용하도록 설정된 가상 데이터 센터가 데이터 센터 그룹 만들기 위한 데이터 센터 목록에 표시됩니다. 데이터 센터 그룹 만들기에 대한 자세한 내용은 "vCloud Director 테넌트 포털 가이드"의 내용을 참조하십시오.

크로스 가상 데이터 센터 네트워킹 구성

크로스 가상 데이터 센터 네트워킹 기능을 사용하면 여러 vCenter Server 인스턴스가 지원하는 가상 데이터 센터를 가진 조직이 계층 2 네트워크를 가상 데이터 센터 4개까지 스트레치할 수 있습니다. 크로스 가

상 데이터 센터 네트워킹은 크로스 vCenter NSX를 사용하며 여러 vCloud Director 사이트에 분산될 수 있습니다.

크로스 가상 데이터 센터 네트워킹에는 NSX Data Center for vSphere가 필요합니다.

크로스 가상 데이터 센터 네트워킹을 통해, 조직은 가상 데이터 센터를 4개까지 그룹화하고 각 그룹에 송신 및 스트레치된 계층 2 네트워크를 구성할 수 있습니다.

참여하는 조직 가상 데이터 센터는 서로 다른 vCloud Director 사이트에 속할 수 있습니다. [다중 사이트 배포 구성 및 관리](#)의 내용을 참조하십시오.

조직에서는 크로스 가상 데이터 센터 네트워킹을 통해 여러 가상 데이터 센터 또는 사이트에 애플리케이션을 분산시킬 수 있는 분산 시스템 아키텍처 또는 고가용성 솔루션을 구현할 수 있습니다.

시스템 관리자는 기본 크로스 vCenter NSX 환경 및 vCloud Director 서버를 구성하고 각 가상 데이터 센터에 크로스 가상 데이터 센터 네트워킹을 사용하도록 설정해야 합니다.

- 1 NSX Manager 인스턴스 중 하나를 기본 NSX Manager 인스턴스로 구성합니다. "크로스 vCenter NSX 설치 가이드"를 참조하십시오.
 - a 기본 NSX Manager 인스턴스에 NSX 클러스터를 배포합니다.
 - b 기본 NSX Manager 인스턴스에 ESXi 호스트를 준비합니다.
 - c 기본 NSX Manager 인스턴스에서 VXLAN을 구성합니다.
 - d NSX Manager 인스턴스에 기본 역할을 할당합니다.
 - e 범용 전송 영역의 세그먼트 IP에 대한 풀을 만듭니다.
 - f 범용 전송 영역을 추가합니다.
- 2 나머지 NSX Manager 인스턴스를 보조 NSX Manager로 구성합니다. "크로스 vCenter NSX 설치 가이드"를 참조하십시오.
 - a 보조 NSX Manager 인스턴스마다 ESXi 호스트를 준비합니다.
 - b 각 보조 NSX Manager 인스턴스에서 VXLAN을 구성합니다.
 - c 각 NSX Manager 인스턴스에 보조 역할을 할당합니다.
 - d ESXi 클러스터를 범용 전송 영역에 연결합니다.
- 3 각 NSX Manager 인스턴스에 대해 제어 VM 속성을 구성합니다. [NSX Manager 설정 수정](#)의 내용을 참조하십시오.
- 4 vCenter Server 인스턴스 중 하나에서 범용 유형의 전송 영역을 사용하여 VXLAN 지원 네트워크 풀을 만듭니다. [NSX Data Center for vSphere 전송 영역에서 지원되는 네트워크 풀 만들기](#)의 내용을 참조하십시오.

참고 다중 사이트 배포인 경우에는 각 vCloud Director 사이트에 VXLAN 지원 네트워크 풀을 만들어야 합니다.

- 5 각 조직 가상 데이터 센터에서 크로스 가상 데이터 센터 네트워킹을 사용하도록 설정합니다. [조직 가상 데이터 센터의 네트워크 설정 편집](#)의 내용을 참조하십시오.
- 6 조직에 다중 사이트 가상 데이터 센터가 있는 경우, vCloud Director 사이트마다 설치 ID가 다른지 확인합니다. 동일한 설치 ID로 구성된 vCloud Director 사이트가 있는 경우 "vCloud Director 설치, 구성 및 업그레이드 가이드"에서 [다중 사이트에 스트레치된 네트워크에 대한 MAC 주소 재생성](#)을 참조하십시오.


이제 **조직 관리자**가 데이터 센터 그룹, 송신 지점 및 스트레치된 네트워크를 만들고 구성할 수 있습니다. 크로스 가상 데이터 센터 네트워킹 관리에 대한 자세한 내용은 "vCloud Director 테넌트 포털 가이드"의 내용을 참조하십시오.

조직 가상 데이터 센터에 대한 메타데이터 수정

조직 가상 데이터 센터에 대한 메타데이터를 추가, 편집 및 삭제할 수 있습니다.

개체 메타데이터를 사용하면 사용자 정의 *name=value* 쌍을 조직 가상 데이터 센터와 연결할 수 있습니다. vCloud API 쿼리 필터 식에서 개체 메타데이터를 사용할 수 있습니다.


절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭하고 대상 조직 가상 데이터 센터의 이름을 클릭합니다.
- 3 **메타데이터** 탭을 클릭합니다.
- 4 **편집**을 클릭합니다.
- 5 (선택 사항) 키-값 쌍을 추가하려면 **추가**를 클릭하고 이름 및 값을 입력한 다음 새로운 키-값 쌍의 유형을 선택합니다.
- 6 (선택 사항) 키-값 쌍을 편집하려면 새 이름과 값을 입력하고 키-값 쌍의 새 유형을 선택합니다.
- 7 (선택 사항) 키-값 쌍을 제거하려면 해당 행의 오른쪽 끝에서 **삭제** 아이콘을 클릭합니다.
- 8 **저장**을 클릭하고 **확인**을 클릭합니다.

조직 가상 데이터 센터의 리소스 풀 보기

조직 가상 데이터 센터에서 사용하는 vCenter Server 리소스 풀 목록을 볼 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭하고 대상 조직 가상 데이터 센터의 이름을 클릭합니다.
- 3 **리소스 풀** 탭을 클릭합니다.

결과

조직 가상 데이터 센터에서 사용 중인 리소스 풀 및 각 리소스 풀이 속하는 vCenter Server 인스턴스가 포함된 테이블을 볼 수 있습니다.

조직 가상 데이터 센터에서 분산 방화벽 관리

조직 가상 데이터 센터에서 계층 3 및 계층 2 네트워크 보안을 제공하려면 이 조직의 가상 데이터 센터에서 분산 방화벽을 사용하도록 설정하고 규칙을 생성하면 됩니다. 분산 방화벽 규칙을 사용하면 조직 가상 데이터 센터의 가상 시스템 간에 이동하는 트래픽을 보호할 수 있습니다.

vCloud Director는 NSX Data Center for vSphere에서 지원되는 조직 가상 데이터 센터에서 분산 방화벽 서비스를 지원합니다.

분산 방화벽 규칙을 생성하려면 다양한 개체 그룹화 및 보안 그룹을 사용할 수 있습니다. [사용자 지정 개체 그룹화](#) 및 [보안 그룹 작업](#)의 내용을 참조하십시오.


Edge 게이트웨이를 드나드는 트래픽을 보호하는 방법에 대한 자세한 내용은 [NSX Data Center for vSphere Edge 게이트웨이 방화벽 관리](#) 항목을 참조하십시오.

조직 가상 데이터 센터에서 분산 방화벽을 사용하도록 설정

조직 가상 데이터 센터에서 분산 방화벽 설정을 관리하려면 먼저 조직 가상 데이터 센터에서 분산 방화벽을 사용하도록 설정해야 합니다.

vCloud Director는 NSX Data Center for vSphere에서 지원되는 조직 가상 데이터 센터에서 분산 방화벽 서비스를 지원합니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 3 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **방화벽 관리**를 클릭합니다.
- 4 **분산 방화벽 > 일반** 탭에서 **분산 방화벽 사용** 토글을 켭니다.

결과

모든 계층 3 및 계층 2 트래픽이 조직 가상 데이터 센터를 통과하도록 허용하는 기본 방화벽 규칙을 볼 수 있습니다.

- **분산 방화벽 > 일반** 탭에서 기본 허용 규칙이라는 계층 3 트래픽에 대한 기본 분산 방화벽 규칙을 볼 수 있습니다.
- **분산 방화벽 > 이더넷** 탭에서 기본 허용 규칙이라는 레이어 2 트래픽에 대한 기본 분산 방화벽 규칙을 볼 수 있습니다.

분산 방화벽 규칙 추가


먼저 조직 가상 데이터 센터의 범위에 분산 방화벽 규칙을 추가합니다. 그런 다음 규칙을 적용할 범위를 좁힐 수 있습니다. 분산 방화벽을 사용하면 각 규칙에 대해 소스 및 대상 수준에서 여러 개체를 추가할 수 있으므로 추가해야 할 총 방화벽 규칙 수가 줄어듭니다.

규칙에서 사용할 수 있는 미리 정의된 서비스 및 서비스 그룹에 대한 자세한 내용은 [방화벽 규칙에 사용할 수 있는 서비스 보기](#) 및 [방화벽 규칙에 사용할 수 있는 서비스 그룹 보기](#) 항목을 참조하십시오.


사전 요구 사항

- [조직 가상 데이터 센터에서 분산 방화벽을 사용하도록 설정](#)
- IP 집합을 규칙에서 소스 또는 대상으로 사용하려면 [방화벽 규칙 및 DHCP 릴레이 구성에 사용할 IP 집합 만들기](#)의 지침을 따르십시오.
- MAC 집합을 규칙에서 소스 또는 대상으로 사용하려면 [방화벽 규칙에 사용할 MAC 집합 만들기](#)의 지침을 따르십시오.
- 보안 그룹을 규칙에서 소스 또는 대상으로 사용하려면 [보안 그룹 만들기](#)의 지침을 따르십시오.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 3 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **방화벽 관리**를 클릭합니다.
- 4 만들려는 규칙 유형을 선택합니다. 일반 규칙 또는 이더넷 규칙을 만들 수 있습니다.

L3(계층 3) 규칙은 **일반** 탭에서 구성됩니다. L2(계층 2) 규칙은 **이더넷** 탭에서 구성됩니다.

- 5 방화벽 테이블의 기존 규칙 아래에 규칙을 추가하려면 기존 행을 클릭한 다음 **만들기**() 버튼을 클릭합니다.

새 규칙에 대한 행이 선택한 규칙 아래에 추가되고 대상, 서비스 및 **허용** 작업이 기본적으로 할당됩니다. 방화벽 테이블에 시스템이 정의한 기본 규칙(허용)만 있을 경우 새 규칙은 기본 규칙 위에 추가됩니다.

- 6 **이름** 셀을 클릭하고 이름을 입력합니다.

7 소스 셀을 클릭하고 이제 표시되는 아이콘을 사용하여 규칙에 추가할 소스를 선택합니다.

작업	설명
IP 아이콘 클릭	<p>일반 탭에서 정의하는 규칙에 적용됩니다.</p> <p>사용할 소스 값을 입력합니다. 올바른 값은 IP 주소, CIDR, IP 범위 또는 키워드 any입니다. 분산 방화벽은 IPv4 형식만 지원합니다.</p>
+ 아이콘 클릭	<p>특정 IP 주소가 아닌 개체로 소스를 지정하려면 + 아이콘을 사용합니다.</p> <ul style="list-style-type: none"> ■ 개체 선택 창을 사용하여 선택 사항과 일치하는 개체를 추가하고 유지를 클릭하여 해당 개체를 규칙에 추가합니다. ■ 규칙에서 소스를 제외하려면 개체 선택 창을 사용하여 이 규칙에 소스를 추가한 다음 제외 전환 아이콘을 선택하여 이 규칙에서 해당 소스를 제외합니다. <p>소스에서 제외 전환을 선택하면 해당 소스를 제외한 모든 소스에서 들어오는 모든 트래픽에 규칙이 적용됩니다. 제외 전환을 선택하지 않으면 개체 선택 창에서 지정한 소스에서 들어오는 트래픽에 규칙이 적용됩니다.</p>

8 대상 셀을 클릭하고 다음 작업 중 하나를 수행합니다.

작업	설명
IP 아이콘 클릭	<p>일반 탭에서 정의하는 규칙에 적용됩니다.</p> <p>사용할 대상 값을 입력합니다. 올바른 값은 IP 주소, CIDR, IP 범위 또는 키워드 any입니다. 분산 방화벽은 IPv4 형식만 지원합니다.</p>
+ 아이콘 클릭	<p>특정 IP 주소가 아닌 개체로 소스를 지정하려면 + 아이콘을 사용합니다.</p> <ul style="list-style-type: none"> ■ 개체 선택 창을 사용하여 선택 사항과 일치하는 개체를 추가하고 유지를 클릭하여 해당 개체를 규칙에 추가합니다. ■ 규칙에서 소스를 제외하려면 [개체 선택] 창을 사용하여 이 규칙에 소스를 추가한 다음 제외 전환 아이콘을 선택하여 이 규칙에서 해당 소스를 제외합니다. <p>소스에서 제외 전환을 선택하면 해당 소스를 제외한 모든 소스에서 들어오는 모든 트래픽에 규칙이 적용됩니다. 제외 전환을 선택하지 않으면 개체 선택 창에서 지정한 소스에서 들어오는 트래픽에 규칙이 적용됩니다.</p>

9 새 규칙의 서비스 셀을 클릭하고 다음 작업 중 하나를 수행합니다.

작업	설명
IP 아이콘 클릭	<p>포트-프로토콜 조합으로 서비스를 지정하려면 다음을 수행합니다.</p> <ol style="list-style-type: none"> 서비스 프로토콜을 선택합니다. 소스 및 대상 포트에 대한 포트 번호를 입력하거나 any를 지정하고 유지를 클릭합니다.
+ 아이콘 클릭	<p>미리 정의된 서비스 또는 서비스 그룹을 선택하거나 새로 정의하려면 다음을 수행합니다.</p> <ol style="list-style-type: none"> 하나 이상의 개체를 선택하고 필터에 추가합니다. 유지를 클릭합니다.

10 새 규칙의 **작업** 셀에서 규칙에 대한 작업을 구성합니다.

옵션	설명
허용	지정된 소스, 대상 및 서비스의 수신 및 발신 트래픽을 허용합니다.
거부	지정된 소스, 대상 및 서비스의 수신 및 발신 트래픽을 차단합니다.

11 새 규칙의 **방향** 셀에서 규칙을 수신 트래픽, 송신 트래픽 또는 둘 다에 적용할지를 선택합니다.**12** 일반 탭의 규칙인 경우 새 규칙의 **패킷 유형** 셀에서 **임의**, **IPv4** 또는 **IPv6**의 패킷 유형을 선택합니다.**13** **적용 대상** 셀을 선택하고 **+** 아이콘을 사용하여 이 규칙을 적용할 수 있는 개체 범위를 정의합니다.

참고 규칙의 **소스** 및 **대상** 셀에 가상 시스템이 포함되는 경우 규칙의 **적용 대상**에 해당 소스 가상 시스템 및 대상 가상 시스템을 추가해야 규칙이 올바르게 작동합니다.



14 **변경 내용 저장**을 클릭합니다.

분산 방화벽 규칙 편집

vCloud Director 환경에서 조직 가상 데이터 센터의 기존 분산 방화벽 규칙을 수정하려면 **분산 방화벽** 화면을 사용합니다.

규칙의 다양한 셀에 사용할 수 있는 설정에 대한 자세한 내용은 [분산 방화벽 규칙 추가](#) 항목을 참조하십시오.

절차

- 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **방화벽 관리**를 클릭합니다.
- 분산 방화벽 규칙을 관리하려면 다음 작업을 수행합니다.
 - 규칙을 사용하지 않도록 설정하려면 **번호** 셀의 녹색 확인 표시를 클릭합니다.
녹색 확인 표시가 빨간색의 사용 안 함 아이콘으로 변경됩니다. 사용되지 않는 규칙을 사용하려면 빨간색의 사용 안 함 아이콘을 클릭합니다.
 - 규칙 이름을 편집하려면 **이름** 셀을 두 번 클릭하고 새 이름을 입력합니다.
 - 소스, 작업 설정 등 규칙의 설정을 수정하려면 해당하는 셀을 선택하고 표시되는 컨트롤을 사용합니다.
 - 규칙을 삭제하려면 규칙을 선택하고 규칙 테이블 위에 있는 **삭제**() 버튼을 클릭합니다.
 - 규칙 테이블에서 규칙의 위치를 위 또는 아래로 이동하려면 규칙을 선택하고 규칙 테이블 위에 있는 위쪽 및 아래쪽 화살표 버튼을 클릭합니다.

5 변경 내용 저장을 클릭합니다.

사용자 지정 개체 그룹화

NSX 소프트웨어를 vCloud Director 환경에서 사용하여 특정 엔티티의 집합 및 그룹을 정의한 다음 방화벽 규칙 같은 다른 네트워크 관련 구성을 지정할 때 사용할 수 있습니다.



방화벽 규칙 및 DHCP 릴레이 구성에 사용할 IP 집합 만들기

IP 집합은 조직 가상 데이터 센터 수준에서 만들 수 있는 IP 주소 그룹입니다. 방화벽 규칙이나 DHCP 릴레이 구성에서 IP 집합을 소스 또는 대상으로 사용할 수 있습니다.

IP 집합은 **개체 그룹화** 페이지를 사용하여 생성합니다. 이 페이지를 열려면 조직 VDC의 분산 방화벽 설정 또는 조직 VDC에 속하는 Edge 게이트웨이의 서비스 설정으로 이동해야 합니다.

절차

1 개체 그룹화 페이지를 엽니다.

옵션	작업
조직 VDC의 분산 방화벽 설정	<ul style="list-style-type: none"> a 기본 메뉴()에서 클라우드 리소스를 선택합니다. b 왼쪽 창에서 조직 VDC를 클릭합니다. c 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 선택하고 방화벽 관리를 클릭합니다. d 개체 그룹화 탭을 클릭합니다.
조직 VDC에 있는 Edge 게이트웨이의 서비스 설정	<ul style="list-style-type: none"> a 기본 메뉴()에서 클라우드 리소스를 선택합니다. b 왼쪽 창에서 Edge 게이트웨이를 클릭합니다. c 대상 조직 가상 데이터 센터에 속하는 Edge 게이트웨이의 이름 옆에 있는 라디오 버튼을 선택하고 서비스를 클릭합니다. d 개체 그룹화 탭을 클릭합니다.

2 IP 집합 탭을 클릭합니다.

이미 정의된 IP 집합이 화면에 표시됩니다.

3 IP 집합을 추가하려면 **만들기**() 버튼을 클릭합니다.

4 IP 집합의 이름과 설명(선택 사항) 및 집합에 포함할 IP 주소를 입력합니다.

5 IP 집합을 저장하려면 **유지**를 클릭합니다.

결과

새 IP 집합을 방화벽 규칙 또는 DHCP 릴레이 구성의 소스 또는 대상으로 선택할 수 있습니다.



방화벽 규칙에 사용할 MAC 집합 만들기

MAC 집합은 조직 가상 데이터 센터 수준에서 생성할 수 있는 MAC 주소의 그룹입니다. 방화벽 규칙에서 MAC 집합을 소스 또는 대상으로 사용할 수 있습니다.

개체 그룹화 페이지를 사용하여 MAC 집합을 생성합니다. 이 페이지를 열려면 조직 VDC의 분산 방화벽 설정 또는 조직 VDC에 속하는 Edge 게이트웨이의 서비스 설정으로 이동해야 합니다.

절차

1 개체 그룹화 페이지를 엽니다.

옵션	작업
조직 VDC의 분산 방화벽 설정	<ul style="list-style-type: none"> a 기본 메뉴()에서 클라우드 리소스를 선택합니다. b 왼쪽 창에서 조직 VDC를 클릭합니다. c 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 선택하고 방화벽 관리를 클릭합니다. d 개체 그룹화 탭을 클릭합니다.
조직 VDC에 있는 Edge 게이트웨이의 서비스 설정	<ul style="list-style-type: none"> a 기본 메뉴()에서 클라우드 리소스를 선택합니다. b 왼쪽 창에서 Edge 게이트웨이를 클릭합니다. c 대상 조직 가상 데이터 센터에 속하는 Edge 게이트웨이의 이름 옆에 있는 라디오 버튼을 선택하고 서비스를 클릭합니다. d 개체 그룹화 탭을 클릭합니다.

2 MAC 집합 탭을 클릭합니다.

이미 정의된 MAC 집합이 화면에 표시됩니다.

3 MAC 집합을 추가하려면 만들기() 버튼을 클릭합니다.

4 집합의 이름, 설명(선택 사항) 및 집합에 포함될 MAC 주소를 입력합니다.

5 MAC 집합을 저장하려면 **유지**를 클릭합니다.

결과

새 MAC 집합을 방화벽 규칙의 소스 또는 대상으로 선택할 수 있습니다.



방화벽 규칙에 사용할 수 있는 서비스 보기

방화벽 규칙에 사용할 수 있는 서비스 목록을 볼 수 있습니다. 이 컨텍스트에서 서비스는 프로토콜-포트 조합입니다.

개체 그룹화 페이지를 사용하여 사용 가능한 서비스를 볼 수 있습니다. 이 페이지를 열려면 조직 VDC의 분산 방화벽 설정 또는 조직 VDC에 속하는 Edge 게이트웨이의 서비스 설정으로 이동해야 합니다.

절차

1 개체 그룹화 페이지를 엽니다.

옵션	작업
조직 VDC의 분산 방화벽 설정	<ol style="list-style-type: none"> 기본 메뉴()에서 클라우드 리소스를 선택합니다. 왼쪽 창에서 조직 VDC를 클릭합니다. 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 선택하고 방화벽 관리를 클릭합니다. 개체 그룹화 탭을 클릭합니다.
조직 VDC에 있는 Edge 게이트웨이의 서비스 설정	<ol style="list-style-type: none"> 기본 메뉴()에서 클라우드 리소스를 선택합니다. 왼쪽 창에서 Edge 게이트웨이를 클릭합니다. 대상 조직 가상 데이터 센터에 속하는 Edge 게이트웨이의 이름 옆에 있는 라디오 버튼을 선택하고 서비스를 클릭합니다. 개체 그룹화 탭을 클릭합니다.

2 서비스 탭을 클릭합니다.

결과

사용 가능한 서비스가 화면에 표시됩니다.



방화벽 규칙에 사용할 수 있는 서비스 그룹 보기

방화벽 규칙에 사용할 수 있는 서비스 그룹 목록을 볼 수 있습니다. 이 컨텍스트에서 서비스는 프로토콜-포트 조합이며 서비스 그룹은 서비스 또는 다른 서비스 그룹의 그룹입니다.

개체 그룹화 페이지를 사용하여 사용 가능한 서비스 그룹을 볼 수 있습니다. 이 페이지를 열려면 조직 VDC의 분산 방화벽 설정 또는 조직 VDC에 속하는 Edge 게이트웨이의 서비스 설정으로 이동해야 합니다.

절차

1 개체 그룹화 페이지를 엽니다.

옵션	작업
조직 VDC의 분산 방화벽 설정	<ol style="list-style-type: none"> 기본 메뉴()에서 클라우드 리소스를 선택합니다. 왼쪽 창에서 조직 VDC를 클릭합니다. 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 선택하고 방화벽 관리를 클릭합니다. 개체 그룹화 탭을 클릭합니다.
조직 VDC에 있는 Edge 게이트웨이의 서비스 설정	<ol style="list-style-type: none"> 기본 메뉴()에서 클라우드 리소스를 선택합니다. 왼쪽 창에서 Edge 게이트웨이를 클릭합니다. 대상 조직 가상 데이터 센터에 속하는 Edge 게이트웨이의 이름 옆에 있는 라디오 버튼을 선택하고 서비스를 클릭합니다. 개체 그룹화 탭을 클릭합니다.

2 서비스 그룹 탭을 클릭합니다.

결과

사용 가능한 서비스 그룹이 화면에 표시됩니다. [설명] 열에는 각 서비스 그룹으로 그룹화된 서비스가 표시됩니다.

보안 그룹 작업

보안 그룹은 가상 시스템, 조직 가상 데이터 센터 네트워크 또는 보안 태그 같은 자산 또는 개체 그룹화의 컬렉션입니다.

보안 그룹은 보안 태그, 가상 시스템 이름, 가상 시스템 게스트 OS 이름 또는 가상 시스템 게스트 호스트 이름에 기반하는 동적 구성원 조건을 사용할 수 있습니다. 예를 들어 "웹"이라는 보안 태그를 가진 모든 가상 시스템은 웹 서버를 대상으로 하는 특정 보안 그룹에 자동으로 추가됩니다. 보안 그룹을 만들면 해당 그룹에 보안 정책이 적용됩니다.


보안 그룹 만들기

사용자 정의 보안 그룹을 만들 수 있습니다.

사전 요구 사항

보안 그룹에 보안 태그를 사용하려면 [보안 태그 만들기 및 할당](#)의 지침을 따르십시오.

절차


- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 3 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **방화벽 관리**를 클릭합니다.
- 4 **개체 그룹화 > 보안 그룹** 탭을 클릭합니다.

- 5 만들기() 버튼을 클릭합니다.

- 6 보안 그룹의 이름과 설명(선택 사항)을 입력합니다.

설명에는 보안 그룹의 목록에 표시되므로 의미 있는 설명을 추가하면 보안 그룹을 쉽게 식별할 수 있습니다.

- 7 (선택 사항) 동적 구성원 집합을 추가합니다.

- a 동적 구성원 집합 아래에 있는 **추가**() 버튼을 클릭합니다.
- b 문의 조건과 일치할 때 사용할 일치 기준을 **임의** 또는 **모두** 중에서 선택합니다.
- c 일치시킬 첫 번째 개체를 입력합니다.

보안 태그, **VM 게스트 운영 체제 이름**, **VM 이름** 및 **VM 게스트 호스트 이름** 옵션을 사용할 수 있습니다.

- d 포함 항목, 다음으로 시작 또는 다음으로 끝남 같은 연산자를 선택합니다.
 - e 값을 입력합니다.
 - f (선택 사항) 다른 문을 추가하려면 **및** 또는 **또는** 부울 연산자를 사용합니다.
- 8** (선택 사항) 구성원을 포함합니다.
- a 다음 유형의 개체 찾아보기 드롭다운 메뉴에서 **가상 시스템, 조직 VDC 네트워크, IP 집합, MAC 집합** 또는 **보안 태그** 같은 개체 유형을 선택합니다.
 - b [구성원 포함] 목록에 개체를 포함하려면 왼쪽 패널에서 개체를 선택한 후 오른쪽 화살표를 클릭하여 오른쪽 패널로 이동합니다.
- 9** (선택 사항) 구성원을 제외합니다.
- a 다음 유형의 개체 찾아보기 드롭다운 메뉴에서 **가상 시스템, 조직 VDC 네트워크, IP 집합, MAC 집합** 또는 **보안 태그** 같은 개체 유형을 선택합니다.
 - b [구성원 제외] 목록에 개체를 포함하려면 왼쪽 패널에서 개체를 선택한 후 오른쪽 화살표를 클릭하여 오른쪽 패널로 이동합니다.
- 10** **유지** 를 클릭하여 변경 내용을 유지합니다.
- 작업을 완료하는 데 몇 분이 걸릴 수 있습니다.



결과





이제 방화벽 규칙 같은 규칙에서 보안 그룹을 사용할 수 있습니다.

보안 그룹 편집

사용자 정의 보안 그룹을 편집할 수 있습니다.

절차

- 1** 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - 2** 왼쪽 창에서 **조직 VDC**를 클릭합니다.
 - 3** 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **방화벽 관리**를 클릭합니다.
 - 4** **개체 그룹화 > 보안 그룹** 탭을 클릭합니다.
 - 5** 편집할 보안 그룹을 선택합니다.
- 보안 그룹 목록 아래 보안 그룹의 세부 정보가 표시됩니다.
- 6** (선택 사항) 보안 그룹의 이름과 설명을 편집합니다.
 - 7** (선택 사항) 동적 구성원 집합을 추가합니다.
- a 동적 구성원 집합 아래에 있는 **추가**() 버튼을 클릭합니다.
 - b 문의 조건과 일치할 때 사용할 일치 기준을 **임의** 또는 **모두** 중에서 선택합니다.

- c 일치시킬 첫 번째 개체를 입력합니다.
 - 보안 태그, VM 게스트 운영 체제 이름, VM 이름 및 VM 게스트 호스트 이름** 옵션을 사용할 수 있습니다.
 - d **포함 항목, 다음으로 시작** 또는 **다음으로 끝남** 같은 연산자를 선택합니다.
 - e 값을 입력합니다.
 - f (선택 사항) 다른 문을 추가하려면 **및** 또는 **또는** 부울 연산자를 사용합니다.
- 8** (선택 사항) 편집할 구성원 집합 옆에 있는 **편집**() 아이콘을 클릭하여 동적 구성원 집합을 편집합니다.
- a 필요한 변경 내용을 동적 구성원 집합에 적용합니다.
 - b **확인**을 클릭합니다.
- 9** (선택 사항) 삭제할 구성원 집합 옆에 있는 **삭제**() 아이콘을 클릭하여 동적 구성원 집합을 삭제합니다.
- 10** (선택 사항) [구성원 포함] 목록 옆에 있는 **편집**() 아이콘을 클릭하여 포함된 구성원 목록을 편집합니다.
- a **다음 유형의 개체 찾기** 드롭다운 메뉴에서 **가상 시스템, 조직 VDC 네트워크, IP 집합, MAC 집합** 또는 **보안 태그** 같은 개체 유형을 선택합니다.
 - b [구성원 포함] 목록에 개체를 포함하려면 왼쪽 패널에서 개체를 선택한 후 오른쪽 화살표를 클릭하여 오른쪽 패널로 이동합니다.
 - c [구성원 포함] 목록에서 개체를 제외하려면 오른쪽 패널에서 개체를 선택한 후 왼쪽 화살표를 클릭하여 왼쪽 패널로 이동합니다.
- 11** (선택 사항) [구성원 제외] 목록 옆에 있는 **편집**() 아이콘을 클릭하여 제외된 구성원 목록을 편집합니다.
- a **다음 유형의 개체 찾기** 드롭다운 메뉴에서 **가상 시스템, 조직 VDC 네트워크, IP 집합, MAC 집합** 또는 **보안 태그** 같은 개체 유형을 선택합니다.
 - b [구성원 제외] 목록에 개체를 포함하려면 왼쪽 패널에서 개체를 선택한 후 오른쪽 화살표를 클릭하여 오른쪽 패널로 이동합니다.
 - c [구성원 제외] 목록에서 개체를 제외하려면 오른쪽 패널에서 개체를 선택한 후 왼쪽 화살표를 클릭하여 왼쪽 패널로 이동합니다.



12 변경 내용 저장을 클릭합니다.

보안 그룹에 대한 변경 내용이 저장됩니다.

보안 그룹 삭제

사용자 정의 보안 그룹을 삭제할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 3 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **방화벽 관리**를 클릭합니다.
- 4 **개체 그룹화 > 보안 그룹** 탭을 클릭합니다.
- 5 삭제할 보안 그룹을 선택합니다.
- 6 삭제() 버튼을 클릭합니다.
- 7 **확인**을 클릭하여 삭제를 확인합니다.

결과

보안 그룹이 삭제됩니다.

보안 태그 작업

보안 태그는 가상 시스템 또는 가상 시스템 그룹에 연결할 수 있는 레이블입니다. 보안 태그는 보안 그룹과 함께 사용하도록 설계되었습니다. 보안 태그를 만든 후 보안 그룹에 연결하여 방화벽 규칙에 사용할 수 있습니다. 사용자 정의 보안 태그를 만들거나 편집하거나 할당할 수 있습니다. 특정 보안 태그가 적용된 가상 시스템 또는 보안 그룹을 볼 수도 있습니다.



보안 태그는 주로 개체를 동적으로 그룹화하여 방화벽 규칙을 간소화하는 데 사용됩니다. 예를 들어 지정된 가상 시스템에서 발생할 것으로 예상되는 작업 유형을 기준으로 여러 개의 서로 다른 보안 태그를 만들 수 있습니다. 데이터베이스 서버에 대한 보안 태그와 e-메일 서버에 대한 보안 태그를 만듭니다. 그런 다음 데이터베이스 서버 또는 e-메일 서버가 상주하는 가상 시스템에 해당하는 태그를 적용합니다. 나중에 태그를 보안 그룹에 할당하고 이에 대한 방화벽 규칙을 작성하여 가상 시스템에서 데이터베이스 서버를 실행하는지 e-메일 서버를 실행하는지에 따라 서로 다른 보안 설정을 적용할 수 있습니다. 나중에 가상 시스템의 기능을 변경하는 경우 방화벽 규칙을 편집하는 대신 보안 태그에서 가상 시스템을 제거할 수 있습니다.

보안 태그 만들기 및 할당

보안 태그를 만들고 가상 시스템 또는 가상 시스템 그룹에 할당할 수 있습니다.

보안 태그를 만들고 가상 시스템 또는 가상 시스템 그룹에 할당합니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 3 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **방화벽 관리**를 클릭합니다.
- 4 **보안 태그** 탭을 클릭합니다.
- 5 만들기() 버튼을 클릭하고 보안 태그의 이름을 입력합니다.

6 (선택 사항) 보안 태그의 설명을 입력합니다.

7 (선택 사항) 보안 태그를 가상 시스템 또는 가상 시스템 그룹에 할당합니다.

다음 유형의 개체 찾아보기 드롭다운 메뉴에 **가상 시스템**이 기본적으로 선택되어 있습니다.

a 왼쪽 패널에서 가상 시스템을 선택합니다.

b 오른쪽 화살표를 클릭하여 보안 태그를 선택한 가상 시스템에 할당합니다.

가상 시스템이 오른쪽 패널로 이동하고, 해당 가상 시스템에 보안 태그가 할당됩니다.

8 선택한 가상 시스템에 대한 태그 할당을 완료하면 **유지**를 클릭합니다.

결과

보안 태그가 만들어지고 선택한 경우 선택한 가상 시스템에 할당됩니다.

다음에 수행할 작업


보안 태그는 보안 그룹과 함께 작동하도록 설계되었습니다. 보안 그룹 만들기에 대한 자세한 내용은 [보안 그룹 만들기](#) 섹션을 참조하십시오.

보안 태그 할당 변경

보안 태그를 만든 이후 가상 시스템에 수동으로 할당할 수 있습니다. 보안 태그를 편집하여, 이미 할당된 가상 시스템에서 태그를 제거할 수도 있습니다.

보안 태그를 만든 경우 해당 보안 태그를 가상 시스템에 할당할 수 있습니다. 보안 태그를 사용하여 가상 시스템을 그룹화하고 방화벽 규칙을 작성할 수 있습니다. 예를 들어 매우 중요한 데이터를 포함하는 가상 시스템 그룹에 보안 태그를 할당할 수 있습니다.


절차

1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.

2 왼쪽 창에서 **조직 VDC**를 클릭합니다.

3 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **방화벽 관리**를 클릭합니다.

4 **보안 태그** 탭을 클릭합니다.

5 보안 태그 목록에서 편집할 보안 태그를 선택하고 **편집**() 버튼을 클릭합니다.

6 왼쪽 패널에서 가상 시스템을 선택하고 오른쪽 화살표를 클릭하여 보안 태그를 할당합니다.

오른쪽 패널의 가상 시스템에 보안 태그가 할당됩니다.

7 오른쪽 패널에서 가상 시스템을 선택하고 왼쪽 화살표를 클릭하여 태그를 제거합니다.

왼쪽 패널의 가상 시스템에는 할당된 보안 태그가 없습니다.

8 변경 내용을 모두 추가한 후 **유지**를 클릭합니다.

결과

보안 태그가 선택한 가상 시스템에 할당됩니다.

다음에 수행할 작업

보안 태그는 보안 그룹과 함께 작동하도록 설계되었습니다. 보안 그룹 만들기에 대한 자세한 내용은 [보안 그룹 만들기](#) 섹션을 참조하십시오.


적용된 보안 태그 보기

사용자 환경의 가상 시스템에 적용된 보안 태그를 볼 수 있습니다. 환경의 보안 그룹에 적용되는 보안 태그도 볼 수 있습니다.

사전 요구 사항

보안 태그가 만들어졌고 가상 시스템 또는 보안 그룹에 적용되어 있어야 합니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 3 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **방화벽 관리**를 클릭합니다.
- 4 **보안 태그** 탭에서 할당된 태그를 확인합니다.
 - a **보안 태그** 탭에서 할당 정보를 볼 보안 태그를 선택한 다음 **편집** 아이콘을 클릭합니다.
 - b **VM 할당/할당 취소** 아래에 보안 태그에 할당된 가상 시스템 목록을 볼 수 있습니다.
 - c **삭제**를 클릭합니다.
- 5 **보안 그룹** 탭에서 할당된 태그를 확인합니다.
 - a **개체 그룹화** 탭을 클릭하고 **보안 그룹**을 클릭합니다.
 - b 보안 그룹을 선택합니다.
 - c **구성원 포함** 아래의 목록에서 보안 그룹에 할당된 보안 태그를 볼 수 있습니다.

결과



기존 보안 태그와 연결된 가상 시스템 및 보안 그룹을 볼 수 있습니다. 이렇게 하면 보안 태그 및 보안 그룹에 기반한 방화벽 규칙 만들기 전략을 결정할 수 있습니다.

보안 태그 편집

사용자 정의 보안 태그를 편집할 수 있습니다.

가상 시스템의 환경 또는 기능을 변경하는 경우 방화벽 규칙이 새 시스템 구성에 적합하도록 다른 보안 태그를 사용해야 할 수 있습니다. 예를 들어 가상 시스템에 더 이상 중요 데이터를 저장하지 않는 경우 다른 보안 태그를 할당하여 중요 데이터에 적용되는 방화벽 규칙을 해당 가상 시스템에 대해 더 이상 실행하지 않을 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 3 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **방화벽 관리**를 클릭합니다.
- 4 **보안 태그** 탭을 클릭합니다.
- 5 보안 태그 목록에서 편집할 보안 태그를 선택합니다.
- 6 편집() 버튼을 클릭합니다.
- 7 보안 태그의 이름과 설명을 편집합니다.
- 8 선택한 가상 시스템에 대해 태그를 할당하거나 태그 할당을 제거합니다.
- 9 변경 내용을 저장하려면 **유지**를 클릭합니다.

다음에 수행할 작업



보안 태그를 편집하는 경우 연결된 보안 그룹 또는 방화벽 규칙을 편집해야 할 수 있습니다. 보안 그룹에 대한 자세한 내용은 [보안 그룹 작업](#) 섹션을 참조하십시오.

보안 태그 삭제

사용자 정의 보안 태그를 삭제할 수 있습니다.

가상 시스템의 기능 또는 환경이 변경된 경우 보안 태그를 삭제해야 할 수 있습니다. 예를 들어 Oracle 데이터베이스에 대한 보안 태그가 있지만 다른 데이터베이스 서버를 사용하기로 결정하는 경우 보안 태그를 제거하여 가상 시스템에서 Oracle 데이터베이스에 적용되는 방화벽 규칙이 더 이상 실행되지 않도록 할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **조직 VDC**를 클릭합니다.
- 3 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 클릭하고 **방화벽 관리**를 클릭합니다.
- 4 **보안 태그** 탭을 클릭합니다.
- 5 보안 태그 목록에서 삭제할 보안 태그를 선택합니다.
- 6 삭제() 버튼을 클릭합니다.
- 7 **확인**을 클릭하여 삭제를 확인합니다.

결과

보안 태그가 삭제됩니다.

다음에 수행할 작업

보안 태그를 삭제하는 경우 연결된 보안 그룹 또는 방화벽 규칙을 편집해야 할 수 있습니다. 보안 그룹에 대한 자세한 내용은 [보안 그룹 작업](#) 항목을 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이 관리

7

NSX Data Center for vSphere Edge 게이트웨이는 외부 네트워크와 연결할 수 있는 라우팅된 조직 가상 데이터 센터 네트워크를 제공하고 로드 밸런싱, NAT(네트워크 주소 변환), 방화벽과 같은 서비스를 제공할 수 있습니다. vCloud Director는 IPv4 및 IPv6 Edge 게이트웨이를 지원합니다.

vCloud Director 9.7부터는 계산 워크로드와 네트워킹 워크로드가 서로 다른 vSphere 리소스 풀 및 스토리지 정책을 사용하여 격리됩니다. Edge 게이트웨이는 미리 생성해야 하는 Edge 클러스터에 상주합니다. [Edge 클러스터 사용](#)의 내용을 참조하십시오.

레거시 Edge 게이트웨이를 다시 배포하여 이러한 Edge 게이트웨이를 해당 Edge 클러스터로 마이그레이션할 수 있습니다. [Edge 게이트웨이 다시 배포](#)의 내용을 참조하십시오.

중요 버전 9.7부터는 vCloud Director에서 고급 Edge 게이트웨이만 지원됩니다. 고급이 아닌 레거시 Edge 게이트웨이는 고급 게이트웨이로 변환해야 합니다. <https://kb.vmware.com/kb/66767>의 내용을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [Edge 클러스터 사용](#)
- [NSX Data Center for vSphere Edge 게이트웨이 추가](#)
- [NSX Data Center for vSphere Edge 게이트웨이 서비스 구성](#)
- [Edge 게이트웨이의 네트워크 사용 및 IP 할당 보기](#)
- [Edge 게이트웨이 속성 편집](#)
- [Edge 게이트웨이 다시 배포](#)
- [Edge 게이트웨이 삭제](#)
- [Edge 게이트웨이에 대한 통계 및 로그](#)
- [Edge 게이트웨이에 대한 SSH 명령줄 액세스 사용](#)

Edge 클러스터 사용

네트워킹 워크로드에서 계산 워크로드를 분리하기 위해 vCloud Director 9.7에 Edge 클러스터 개체가 도입되었습니다. Edge 클러스터는 조직 VDC Edge 게이트웨이에만 사용되는 스토리지 정책 및 vSphere 리소스 풀로 구성됩니다. 제공자 가상 데이터 센터는 Edge 클러스터 전용 리소스를 사용할 수 없으며 Edge 클러스터는 제공자 가상 데이터 센터 전용 리소스를 사용할 수 없습니다.

Edge 클러스터는 VLAN 확장을 줄이고 네트워크 보안 및 격리를 보장하는 전용 L2 브로드캐스트 도메인을 제공합니다. 예를 들어 Edge 클러스터에는 물리적 라우터와 피어링을 위한 추가 VLAN이 포함될 수 있습니다.

원하는 수의 Edge 클러스터를 생성할 수 있습니다. Edge 클러스터를 조직 VDC에 기본 또는 보조 Edge 클러스터로 할당할 수 있습니다.

- 조직 VDC의 기본 Edge 클러스터는 조직 VDC Edge 게이트웨이의 주 Edge 장치에 사용됩니다.
- 조직 VDC의 보조 Edge 클러스터는 Edge 게이트웨이가 HA 모드일 때 대기 Edge 장치에 사용됩니다.

서로 다른 조직 VDC는 Edge 클러스터를 공유하거나 고유한 전용 Edge 클러스터를 가질 수 있습니다.

버전 vCloud Director 9.7에서는 Edge 게이트웨이 배치를 제어하기 위해 메타데이터를 사용하는 이전 프로세스가 더 이상 사용되지 않습니다. <https://kb.vmware.com/kb/2151398>의 내용을 참조하십시오.

레거시 Edge 게이트웨이를 다시 배포하여 이러한 Edge 게이트웨이를 새로 생성된 Edge 클러스터로 마이그레이션할 수 있습니다. [Edge 게이트웨이 다시 배포](#)의 내용을 참조하십시오.

Edge 클러스터에 대한 환경 준비

- 1 vSphere에서 대상 Edge 클러스터에 대한 리소스 풀을 생성합니다.

조직 가상 데이터 센터에서 VLAN 네트워크 풀을 사용하는 경우, 조직 가상 데이터 센터의 VLAN 네트워크 풀 및 Edge 클러스터가 동일한 vSphere 분산 스위치에 상주해야 합니다.

- 2 조직 가상 데이터 센터에서 VXLAN 네트워크 풀을 사용하는 경우에는 NSX에서 VXLAN 전송 영역에 Edge 클러스터를 추가한 다음, vCloud Director에서 VXLAN 네트워크 풀을 동기화합니다.

- 3 vSphere에서 Edge 클러스터 스토리지 프로파일을 생성합니다.

Edge 클러스터 생성 및 관리

환경을 준비한 후 Edge 클러스터를 생성하고 관리하려면 vCloud OpenAPI EdgeClusters 메서드를 사용해야 합니다. <https://code.vmware.com>에서 "vCloud OpenAPI 시작하기"의 내용을 참조하십시오.

Edge 클러스터를 보려면 **Edge 클러스터 보기** 권한이 필요합니다. Edge 클러스터를 생성, 업데이트 및 삭제하려면 **Edge 클러스터 관리** 권한이 필요합니다.

Edge 클러스터를 생성할 때 이름, vSphere 리소스 풀 및 스토리지 프로파일 이름을 지정합니다.

Edge 클러스터를 생성한 후에는 해당 이름 및 설명을 수정할 수 있습니다. 포함된 Edge 게이트웨이를 삭제하거나 이동한 후에 Edge 클러스터를 삭제할 수 있습니다.

조직 VDC에 Edge 클러스터 할당

Edge 클러스터를 생성한 후에 조직 VDC 네트워크 프로파일을 업데이트하여 Edge 클러스터를 조직 VDC에 할당할 수 있습니다. Edge 클러스터를 조직 VDC에 기본 또는 보조 Edge 클러스터로 할당할 수 있습니다.

보조 Edge 클러스터를 할당하지 않으면 HA 모드의 Edge 게이트웨이의 대기 Edge 장치가 기본 Edge 클러스터에 배포되지만 기본 Edge 장치를 실행하는 호스트와 다른 호스트에 배포됩니다.

조직 VDC 네트워크 프로파일을 업데이트하고, 살펴보고, 삭제하려면 vCloud OpenAPI

VdcNetworkProfile 메시지를 사용해야 합니다. <https://code.vmware.com>에서 "vCloud OpenAPI 시작하기"의 내용을 참조하십시오.

고려 사항:

- 기본 및 보조 Edge 클러스터는 동일한 vSphere 분산 스위치에 상주해야 합니다.
- 조직 VDC에서 VXLAN 네트워크 풀을 사용하는 경우, NSX 전송 영역이 계산 및 Edge 클러스터에 걸쳐 있어야 합니다.
- 조직 VDC에서 VLAN 네트워크 풀을 사용하는 경우에는, Edge 클러스터 및 계산 클러스터가 동일한 vSphere 분산 스위치에 있어야 합니다.

조직 VDC의 기본 또는 보조 Edge 클러스터를 다시 업데이트하는 경우, 기존 Edge 게이트웨이를 새 클러스터로 이동하려면 이 Edge 게이트웨이를 다시 배포해야 합니다. [Edge 게이트웨이 다시 배포](#)의 내용을 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이 추가

NSX Data Center for vSphere Edge 게이트웨이는 외부 네트워크와 연결할 수 있는 라우팅된 조직 VDC 네트워크를 제공하고 로드 밸런싱, NAT(네트워크 주소 변환), 방화벽과 같은 서비스를 제공할 수 있습니다.

vCloud Director 9.7부터 NSX Data Center for vSphere Edge 게이트웨이는 이전에 생성하여 조직 VDC에 할당한 Edge 클러스터에 배포됩니다.


하나 이상의 외부 네트워크에 연결하는 IPv4 또는 IPv6 Edge 게이트웨이를 추가할 수 있습니다.

참고 IPv6 Edge 게이트웨이는 제한된 서비스를 지원합니다. IPv6 Edge 게이트웨이는 Edge 방화벽, 분산 방화벽 및 정적 라우팅을 지원합니다.

사전 요구 사항

- NSX Data Center for vSphere Edge 게이트웨이 배포를 위한 시스템 요구 사항에 대한 자세한 내용은 "NSX 관리 가이드"의 내용을 참조하십시오.
- 전용 Edge 클러스터에 Edge 게이트웨이를 배포하려면 조직 가상 데이터 센터에 Edge 클러스터를 생성하여 할당합니다. [Edge 클러스터 사용](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭하고 **새로 만들기**를 클릭합니다.
- 3 Edge 게이트웨이를 만들 **NSX-V** 지원형 조직 가상 데이터 센터를 선택하고 **다음**을 클릭합니다.
- 4 새 Edge 게이트웨이의 이름과 설명(선택 사항)을 입력합니다.
- 5 다음과 같은 일반 Edge 게이트웨이 설정을 설정하거나 해제한 상태로 둡니다.

일반 설정	설명
분산 라우팅	논리적 분산 라우팅을 제공하도록 Edge 게이트웨이를 구성합니다.
FIPS 모드	NSX FIPS 모드를 사용하도록 Edge 게이트웨이를 구성합니다.
고가용성	백업 Edge 게이트웨이로 자동 페일오버되도록 설정합니다.

- 6 시스템 리소스에 대한 Edge 게이트웨이 구성을 선택하고 **다음**을 클릭합니다.

구성	설명
압축	메모리와 계산 리소스를 더 적게 사용합니다.
큼	[압축] 구성보다 향상된 성능 및 용량을 제공합니다. [큼] 및 [초대형] 구성은 보안 기능이 동일합니다.
초대형	동시 세션 수가 많고 로드 밸런서를 사용하는 환경에 사용됩니다.
4배 대형	처리량이 많은 환경에 사용됩니다. 높은 연결 속도가 필요합니다.

- 7 Edge 게이트웨이를 연결할 수 있는 외부 네트워크의 서브넷을 하나 이상 선택하고 **다음**을 클릭합니다.

조직 VDC에 Edge 클러스터를 할당한 경우, 표시된 목록에는 이 Edge 클러스터에서 액세스할 수 있는 외부 네트워크가 포함됩니다.

- 8 (선택 사항) 특정 네트워크를 기본 게이트웨이로 구성합니다.
 - a 기본 게이트웨이 구성 토글을 설정합니다.
 - b 대상 외부 네트워크의 이름 옆에 있는 라디오 버튼을 클릭하고 대상 IP 주소 옆에 있는 라디오 버튼을 클릭합니다.
 - c (선택 사항) DNS 릴레이에 기본 게이트웨이 사용 토글을 설정합니다.
- 9 다음을 클릭합니다.

10 다음과 같은 고급 Edge 게이트웨이 설정을 설정하거나 해제한 상태로 두고 **다음**을 클릭합니다.

고급 설정	설명
IP 설정	Edge 게이트웨이의 각 서브넷에 대한 IP 주소를 수동으로 입력할 수 있습니다.
IP 풀 하위 할당	Edge 게이트웨이의 각 외부 네트워크의 사용 가능한 IP 풀에서 여러 정적 IP 풀을 하위 할당할 수 있습니다.
속도 제한	Edge 게이트웨이의 각 외부 네트워크에 대한 인바운드 및 아웃바운드 속도 제한을 구성할 수 있습니다.

11 (선택 사항) **단계 10 단계**에서 하나 이상의 고급 설정을 사용하도록 설정한 경우 각각의 해당 설정을 구성합니다.

고급 설정	단계
IP 설정	Edge 게이트웨이의 각 네트워크에 대해 IP 주소 셀에 IP 주소를 입력하고 다음 을 클릭합니다. 네트워크에 대한 IP 주소를 입력하지 않으면 이 네트워크에 임의의 IP 주소가 시스템에서 할당됩니다.
IP 풀 하위 할당	<ol style="list-style-type: none"> 외부 네트워크의 이름 옆에 있는 라디오 버튼을 클릭하고 편집을 클릭합니다. 이 외부 네트워크에 사용할 수 있는 IP 풀과 현재 하위 할당된 IP 풀(구성한 경우)을 볼 수 있습니다. 이 외부 네트워크에 대해 하위 할당된 IP 풀을 편집하고 저장을 클릭합니다. 사용할 수 있는 IP 풀의 범위에서 IP 주소 및 범위를 추가할 수 있습니다. 저장을 클릭합니다. 시스템에서 겹치는 IP 범위를 결합합니다. 다음을 클릭합니다. <p>참고 Edge 게이트웨이에 IP 주소를 할당하는 것은 제공자가 IP 주소의 소유권을 게이트웨이에 할당하는 프로세스입니다. vCloud Director는 할당 프로세스 중에 보조 주소로 적절한 게이트웨이 인터페이스를 자동으로 구성합니다. IP 주소가 vCloud Director 외부에서 사용되면 IP 주소 충돌이 발생할 수 있습니다.</p>
속도 제한	Edge 에지 게이트웨이의 각 외부 네트워크에 대해 사용 토글을 켜고 수신 속도 및 송신 속도 셀에 제한을 입력한 후 다음 을 클릭합니다.

12 완료 준비 페이지를 검토하고 **마침**을 클릭합니다.

NSX Data Center for vSphere Edge 게이트웨이 서비스 구성

Edge 게이트웨이에 DHCP, 방화벽, NAT(네트워크 주소 변환) 및 VPN과 같은 서비스를 구성할 수 있습니다.

NSX Data Center for vSphere Edge 게이트웨이 방화벽 관리

Edge 게이트웨이를 드나드는 트래픽을 보호하기 위해 Edge 게이트웨이에서 방화벽 규칙을 생성하고 관리할 수 있습니다.

조직 가상 데이터 센터에서 가상 시스템 간에 이동하는 트래픽을 보호하는 방법에 대한 자세한 내용은 [조직 가상 데이터 센터에서 분산 방화벽 관리](#) 항목을 참조하십시오.

분산 방화벽 화면에서 [적용 대상] 열에 고급 Edge 게이트웨이를 지정하여 만들어진 규칙은 해당하는 고급 Edge 게이트웨이의 [방화벽] 화면에 표시되지 않습니다.

Edge 게이트웨이에 대한 Edge 게이트웨이 방화벽 규칙은 **방화벽** 화면에 표시되며 다음과 같은 순서로 적용됩니다.

- 1 내부 규칙(자동 배관된 규칙). 이러한 내부 규칙은 Edge 게이트웨이 서비스를 위한 제어 트래픽의 흐름을 가능하게 합니다.
- 2 사용자 정의 규칙.
- 3 기본 규칙.

기본 규칙 설정은 어떠한 사용자 정의 방화벽 규칙과도 일치하지 않는 트래픽에 적용됩니다. 기본 규칙은 [방화벽] 화면에서 규칙의 맨 아래에 표시됩니다.

테넌트 포털에서 Edge 게이트웨이의 [방화벽 규칙] 화면에 있는 **사용** 토글을 사용하여 Edge 게이트웨이 방화벽을 사용하거나 사용하지 않도록 설정합니다.


NSX Data Center for vSphere Edge 게이트웨이 방화벽 규칙 추가

Edge 게이트웨이 **방화벽** 탭을 사용하여 해당 Edge 게이트웨이에 대한 방화벽 규칙을 추가합니다. 이러한 방화벽 규칙의 소스와 대상으로 여러 개의 NSX Edge 인터페이스와 여러 개의 IP 주소 그룹을 추가할 수 있습니다.

규칙의 소스 또는 대상에 대해 **내부**를 지정하면 포트 그룹의 모든 서브넷에 대한 트래픽은 NSX Edge Gateway에 연결됩니다. 소스를 **내부**로 선택하면 NSX Gateway에 추가 내부 인터페이스가 구성될 때 규칙이 자동으로 업데이트됩니다.

참고 동적 라우팅을 사용하도록 Edge 게이트웨이를 구성한 경우 내부 인터페이스의 Edge 게이트웨이 방화벽 규칙이 작동하지 않습니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 **방화벽 규칙** 화면이 표시되지 않으면 **방화벽** 탭을 클릭합니다.
- 3 방화벽 규칙 테이블의 기존 규칙 아래에 규칙을 추가하려면 기존 행을 클릭한 다음 **만들기** 버튼을 클릭합니다.

새 규칙에 대한 행이 선택한 규칙 아래에 추가되고 대상, 서비스 및 **허용** 작업이 기본적으로 할당됩니다. 방화벽 테이블에 시스템이 정의한 기본 규칙만 있을 경우 새 규칙은 기본 규칙 위에 추가됩니다.
- 4 **이름** 셀을 클릭하고 이름을 입력합니다.

5 소스 셀을 클릭하고 이제 표시되는 아이콘을 사용하여 규칙에 추가할 소스를 선택합니다.

옵션	설명
IP 아이콘 클릭	사용할 소스 값을 입력합니다. 올바른 값은 IP 주소, CIDR, IP 범위 또는 키워드 any 입니다. Edge 게이트웨이 방화벽은 IPv4 및 IPv6 형식을 모두 지원합니다.
+ 아이콘 클릭	<p>특정 IP 주소가 아닌 개체로 소스를 지정하려면 + 아이콘을 사용합니다.</p> <ul style="list-style-type: none"> ■ 개체 선택 창을 사용하여 선택 사항과 일치하는 개체를 추가하고 유지를 클릭하여 해당 개체를 규칙에 추가합니다. ■ 규칙에서 소스를 제외하려면 개체 선택 창을 사용하여 이 규칙에 소스를 추가한 다음 제외 전환 아이콘을 선택하여 이 규칙에서 해당 소스를 제외합니다. <p>소스에서 제외 전환을 선택하면 해당 소스를 제외한 모든 소스에서 들어오는 모든 트래픽에 규칙이 적용됩니다. 제외 전환을 선택하지 않으면 개체 선택 창에서 지정한 소스에서 들어오는 트래픽에 규칙이 적용됩니다.</p>

6 대상 셀을 클릭하고 다음 옵션 중 하나를 수행합니다.

옵션	설명
IP 아이콘 클릭	사용할 대상 값을 입력합니다. 올바른 값은 IP 주소, CIDR, IP 범위 또는 키워드 any 입니다. Edge 게이트웨이 방화벽은 IPv4 및 IPv6 형식을 모두 지원합니다.
+ 아이콘 클릭	<p>특정 IP 주소가 아닌 개체로 소스를 지정하려면 + 아이콘을 사용합니다.</p> <ul style="list-style-type: none"> ■ 개체 선택 창을 사용하여 선택 사항과 일치하는 개체를 추가하고 유지를 클릭하여 해당 개체를 규칙에 추가합니다. ■ 규칙에서 소스를 제외하려면 [개체 선택] 창을 사용하여 이 규칙에 소스를 추가한 다음 제외 전환 아이콘을 선택하여 이 규칙에서 해당 소스를 제외합니다. <p>소스에서 제외 전환을 선택하면 해당 소스를 제외한 모든 소스에서 들어오는 모든 트래픽에 규칙이 적용됩니다. 제외 전환을 선택하지 않으면 개체 선택 창에서 지정한 소스에서 들어오는 트래픽에 규칙이 적용됩니다.</p>

7 새 규칙의 서비스 셀을 클릭하고 + 아이콘을 클릭하여 서비스를 포트-프로토콜 조합으로 지정합니다.

- 서비스 프로토콜을 선택합니다.
- 소스 및 대상 포트에 대한 포트 번호를 입력하거나 **any**를 지정합니다.
- 유지**를 클릭합니다.

8 새 규칙의 작업 셀에서 규칙에 대한 작업을 구성합니다.

옵션	설명
수락	지정된 소스, 대상 및 서비스의 수신 및 발신 트래픽을 허용합니다.
거부	지정된 소스, 대상 및 서비스의 수신 및 발신 트래픽을 차단합니다.

9 변경 내용 저장을 클릭합니다.

저장 작업을 완료하는 데 몇 분이 걸릴 수 있습니다.


NSX Data Center for vSphere Edge 게이트웨이 방화벽 규칙 수정

Edge 게이트웨이에 추가된 사용자 정의 방화벽 규칙만 편집하고 삭제할 수 있습니다. 기본 규칙의 작업 설정을 변경하는 경우를 제외하고는 자동 생성된 규칙 또는 기본 규칙을 편집하거나 삭제할 수 없습니다. 사용자 정의 규칙의 우선 순위 순서를 변경할 수 있습니다.

규칙의 다양한 셀에 사용할 수 있는 설정에 대한 자세한 내용은 [NSX Data Center for vSphere Edge 게이트웨이 방화벽 규칙 추가](#) 항목을 참조하십시오.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 방화벽 탭을 클릭합니다.

3 방화벽 규칙을 관리합니다.


- 규칙을 사용하지 않도록 설정하려면 **번호** 셀의 녹색 확인 표시를 클릭합니다. 녹색 확인 표시가 빨간색의 사용 안 함 아이콘으로 변경됩니다. 사용되지 않는 규칙을 사용하려면 빨간색의 사용 안 함 아이콘을 클릭합니다.
- 규칙 이름을 편집하려면 **이름** 셀을 두 번 클릭하고 새 이름을 입력합니다.
- 소스, 작업 설정 등 규칙의 설정을 수정하려면 해당하는 셀을 선택하고 표시되는 컨트롤을 사용합니다.
- 규칙을 삭제하려면 규칙을 선택하고 규칙 테이블 위에 있는 **삭제** 버튼을 클릭합니다.
- 시스템에서 생성된 규칙을 숨기려면 **사용자 정의 규칙만 표시** 토글을 사용합니다.
- 규칙 테이블에서 규칙의 위치를 위 또는 아래로 이동하려면 규칙을 선택하고 규칙 테이블 위에 있는 위쪽 및 아래쪽 화살표 버튼을 클릭합니다.

4 변경 내용 저장을 클릭합니다.

NSX Data Center for vSphere Edge 게이트웨이에 Syslog 서버 설정 적용

하나 이상의 Edge 게이트웨이 방화벽 규칙에 대한 로깅을 사용하도록 설정한 경우, Edge 게이트웨이가 syslog 서버에 연결됩니다. syslog 서버의 초기 구성 전에 Edge 게이트웨이를 생성했거나 syslog 서버 설정을 변경한 경우에는, Edge 게이트웨이에 syslog 서버 설정을 동기화해야 합니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- 3 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **Syslog 동기화**를 클릭합니다.

4 확인을 클릭하여 확인합니다.

NSX Data Center for vSphere Edge 게이트웨이 DHCP 관리

연결된 조직 가상 데이터 센터 네트워크에 연결된 가상 시스템에 DHCP(Dynamic Host Configuration Protocol) 서비스를 제공하도록 Edge 게이트웨이를 구성합니다.

[NSX 설명서](#)에 설명된 대로 NSX Edge 게이트웨이에는 IP 주소 풀링, 일대일 정적 IP 주소 할당 및 외부 DNS 서버 구성 같은 기능이 있습니다. 정적 IP 주소 바인딩은 요청 클라이언트 가상 시스템의 관리 개체 ID 및 인터페이스 ID를 기반으로 합니다.

NSX Edge Gateway의 DHCP 서비스:

- DHCP 검색을 위해 Edge 게이트웨이의 내부 인터페이스를 수신 대기합니다.
- Edge 게이트웨이의 내부 인터페이스 IP 주소를 모든 클라이언트의 기본 게이트웨이 주소로 사용합니다.
- 컨테이너 네트워크에 대해 내부 인터페이스의 브로드캐스트 및 서브넷 마스크 값을 사용합니다.

다음의 경우 DHCP로 할당된 IP 주소가 있는 클라이언트 가상 시스템에서 DHCP 서비스를 다시 시작해야 합니다.

- DHCP 풀, 기본 게이트웨이 또는 DNS 서버를 변경하거나 삭제한 경우
- Edge 게이트웨이 인스턴스의 내부 IP 주소를 변경한 경우

참고 DHCP를 사용하는 Edge 게이트웨이의 DNS 설정이 변경된 경우 Edge 게이트웨이가 DHCP 서비스 제공을 중지할 수 있습니다. 이 상황이 발생할 경우 [DHCP 풀] 화면의 **DHCP 서비스 상태** 토글을 사용하여 해당 Edge 게이트웨이의 DHCP를 사용하지 않도록 설정한 후 다시 사용하도록 설정합니다. [DHCP IP 풀 추가](#)의 내용을 참조하십시오.

DHCP IP 풀 추가


NSX Data Center for vSphere Edge 게이트웨이의 DHCP 서비스에 필요한 IP 풀을 구성할 수 있습니다. DHCP는 조직 가상 데이터 센터 네트워크에 연결되는 가상 시스템에 대한 IP 주소 할당을 자동화합니다.

"NSX 관리" 설명서에 설명된 대로, DHCP 서비스를 사용하려면 IP 주소 풀이 필요합니다. IP 풀은 네트워크 내에 있는 순차적인 IP 주소 범위입니다. Edge 게이트웨이로 보호되고 주소가 바인딩되지 않은 가상 시스템에는 이 풀의 IP 주소가 할당됩니다. IP 풀의 범위는 서로 교차할 수 없으므로 한 IP 주소는 한 IP 풀에만 속할 수 있습니다.

참고 하나 이상의 DHCP IP 풀이 구성되어 있어야 DHCP 서비스 상태가 켜집니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 DHCP > 풀로 이동합니다.

3 DHCP 서비스를 현재 사용하도록 설정하지 않은 경우 **DHCP 서비스 상태** 토글을 켭니다.

참고 **DHCP 서비스 상태** 토글을 켜 후 변경 내용을 저장하기 전에 하나 이상의 DHCP IP 풀을 추가합니다. 화면에 DHCP IP 풀이 나열되지 않은 경우 **DHCP 서비스 상태** 토글을 켜고 변경 내용을 저장하면 토글이 꺼진 상태로 화면이 표시됩니다.

4 DHCP 풀에서 만들기() 버튼을 클릭하고, DHCP 풀에 대한 세부 정보를 지정한 다음 **유지**를 클릭합니다.

옵션	설명
IP 범위	IP 주소 범위를 입력합니다.
도메인 이름	DNS 서버의 도메인 이름입니다.
DNS 자동 구성	이 IP 풀 DNS 바인딩에 DNS 서비스 구성을 사용하려면 이 토글을 켭니다. 사용하도록 설정하면 기본 이름 서버 와 보조 이름 서버 가 자동 으로 설정됩니다.
기본 이름 서버	DNS 자동 구성 을 사용하도록 설정하지 않는 경우 기본 DNS 서버의 IP 주소를 입력합니다. 이 IP 주소는 호스트 이름과 IP 주소 간 확인에 사용됩니다.
보조 이름 서버	DNS 자동 구성 을 사용하도록 설정하지 않는 경우 보조 DNS 서버 IP 주소를 입력합니다. 이 IP 주소는 호스트 이름과 IP 주소 간 확인에 사용됩니다.
기본 게이트웨이	기본 게이트웨이 주소를 입력합니다. 기본 게이트웨이 IP 주소를 지정하지 않으면 Edge 게이트웨이 인스턴스의 내부 인터페이스가 기본 게이트웨이로 지정됩니다.
서브넷 마스크	Edge 게이트웨이 인터페이스의 서브넷 마스크를 입력합니다.
임대가 만료되지 않음	이 풀에서 할당된 IP 주소를 할당된 가상 시스템에 영구적으로 바인딩한 상태로 유지하려면 이 토글을 사용하도록 설정합니다. 이 옵션을 선택하면 임대 기간 이 무제한으로 설정됩니다.
임대 기간(초)	DHCP로 할당된 IP 주소가 클라이언트에 임대되는 기간(초)입니다. 기본 임대 기간은 하루(86400초)입니다.

참고 **임대가 만료되지 않음**을 선택하면 임대 기간을 지정할 수 없습니다.

5 변경 내용 저장을 클릭합니다.

결과

DHCP 서비스를 제공하도록 vCloud Director에서 Edge 게이트웨이가 업데이트됩니다.

DHCP 바인딩 추가


가상 시스템에서 실행 중인 서비스가 있고 IP 주소를 변경하지 않으려는 경우 가상 시스템 MAC 주소를 IP 주소에 바인딩할 수 있습니다. 바인딩하는 IP 주소는 DHCP IP 풀과 겹치지 않아야 합니다.


사전 요구 사항

바인딩을 설정할 가상 시스템의 MAC 주소를 알고 있어야 합니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 **DHCP > 바인딩** 탭에서 **만들기**() 버튼을 클릭하고 바인딩에 대한 세부 정보를 지정한 다음 **유지**를 클릭합니다.

옵션	설명
MAC 주소	IP 주소에 바인딩할 가상 시스템의 MAC 주소를 입력합니다.
호스트 이름	가상 시스템이 DHCP 임대를 요청할 때 해당 가상 시스템에 설정할 호스트 이름을 입력합니다.
IP 주소	MAC 주소에 바인딩할 IP 주소를 입력합니다.
서브넷 마스크	Edge 게이트웨이 인터페이스의 서브넷 마스크를 입력합니다.
도메인 이름	DNS 서버의 도메인 이름을 입력합니다.
DNS 자동 구성	이 DNS 바인딩에 대한 DNS 서비스 구성을 사용하려면 이 토글을 사용하도록 설정합니다. 사용하도록 설정하면 기본 이름 서버 와 보조 이름 서버 가 자동으로 설정됩니다.
기본 이름 서버	DNS 자동 구성 을 선택하지 않는 경우 기본 DNS 서버의 IP 주소를 입력합니다. 이 IP 주소는 호스트 이름과 IP 주소 간 확인에 사용됩니다.
보조 이름 서버	DNS 자동 구성 을 선택하지 않는 경우 보조 DNS 서버 IP 주소를 입력합니다. 이 IP 주소는 호스트 이름과 IP 주소 간 확인에 사용됩니다.
기본 게이트웨이	기본 게이트웨이 주소를 입력합니다. 기본 게이트웨이 IP 주소를 지정하지 않으면 Edge 게이트웨이 인스턴스의 내부 인터페이스가 기본 게이트웨이로 지정됩니다.

옵션	설명
임대가 만료되지 않음	해당 MAC 주소에 바인딩된 IP 주소를 영구적으로 유지하려면 이 토글을 사용하도록 설정합니다. 이 옵션을 선택하면 임대 기간 이 무제한으로 설정됩니다.
임대 기간(초)	DHCP로 할당된 IP 주소가 클라이언트에 임대되는 기간(초)입니다. 기본 임대 기간은 하루(86400초)입니다.
참고 임대가 만료되지 않음을 선택하면 임대 기간을 지정할 수 없습니다.	

3 변경 내용 저장을 클릭합니다.

NSX Data Center for vSphere Edge 게이트웨이에 대한 DHCP 릴레이 구성

vCloud Director 환경에서 NSX 소프트웨어를 통해 제공되는 DHCP 릴레이 기능을 사용하면 vCloud Director 환경 내에서 기존 DHCP 인프라의 IP 주소 관리에 미치는 영향 없이 기존 DHCP 인프라를 활용할 수 있습니다. DHCP 메시지가 가상 시스템에서 물리적 DHCP 인프라의 지정된 DHCP 서버로 릴레이되기 때문에 NSX 소프트웨어를 통해 제어되는 IP 주소는 나머지 DHCP 제어 환경의 IP 주소와 계속해서 동기화됩니다.

Edge 게이트웨이의 DHCP 릴레이 구성은 여러 DHCP 서버를 나열할 수 있습니다. 나열된 모든 서버로 요청이 전송됩니다. VM에서 DHCP 요청을 릴레이하는 동안 Edge 게이트웨이는 게이트웨이 IP 주소를 요청에 추가합니다. 외부 DHCP 서버는 이 게이트웨이 주소를 사용하여 일치하는 풀을 찾은 다음 요청의 IP 주소를 할당합니다. 게이트웨이 주소는 Edge 게이트웨이 인터페이스의 서브넷에 속해야 합니다.

각 Edge 게이트웨이에 다른 DHCP 서버를 지정하고 각 Edge 게이트웨이에 여러 DHCP 서버를 구성하여 다중 IP 도메인을 지원할 수 있습니다.

참고

- DHCP 릴레이는 겹치는 IP 주소 공간을 지원하지 않습니다.
- DHCP 릴레이와 DHCP 서비스를 동일한 vNIC에서 동시에 실행할 수 없습니다. vNIC에 릴레이 에이전트가 구성된 경우 해당 vNIC의 서브넷에 DHCP 풀을 구성할 수 없습니다. 자세한 내용은 "NSX 관리 가이드"를 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이에 대한 DHCP 릴레이 구성 지정

vCloud Director 환경에서 NSX 소프트웨어를 사용하면 Edge 게이트웨이에서 vCloud Director 조직 가상 데이터 센터 외부의 DHCP 서버로 DHCP 메시지를 릴레이할 수 있습니다. Edge 게이트웨이의 DHCP 릴레이 기능을 구성할 수 있습니다.

"NSX 관리" 설명서에 설명된 대로 기존 IP 집합, IP 주소 블록, 도메인 또는 이 모든 항목의 조합을 사용하여 DHCP 서버를 지정할 수 있습니다. DHCP 메시지는 지정된 모든 DHCP 서버로 릴레이됩니다.


또한 DHCP 릴레이 에이전트를 구성해야 합니다. DHCP 릴레이 에이전트는 Edge 게이트웨이의 인터페이스로, 이 인터페이스의 DHCP 요청이 외부 DHCP 서버로 릴레이됩니다.

사전 요구 사항

IP 집합을 사용하여 DHCP 서버를 지정하려는 경우 해당 IP 집합이 Edge 게이트웨이에서 사용할 수 있는 개체 그룹화로 존재하는지 확인합니다. 방화벽 규칙 및 DHCP 릴레이 구성에 사용할 IP 집합 만들기의 내용을 참조하십시오.


절차


1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 DHCP > 릴레이로 이동합니다.

3 화면의 필드를 사용하여 IP 주소, 도메인 이름 또는 IP 집합으로 DHCP 서버를 지정합니다.

기존 IP 집합 중에서 선택하려면 **추가**() 버튼을 사용하여 사용 가능한 IP 집합을 찾아볼 수 있습니다.

4 **추가**() 버튼을 클릭하고 vNIC 및 게이트웨이 IP 주소를 선택한 다음 **유지**를 클릭하여 DHCP 릴레이 에이전트를 구성하고 해당 구성을 화면의 테이블에 추가합니다.

기본적으로 게이트웨이 IP 주소는 선택한 vNIC의 기본 주소와 일치합니다. 기본값을 유지하거나 해당 vNIC에서 사용 가능한 대체 주소를 선택할 수 있습니다.

5 **변경 내용 저장**을 클릭합니다.

SNAT 또는 DNAT 규칙 추가

SNAT(소스 NAT) 규칙을 만들어 소스 IP 주소를 공개 IP 주소에서 개인 IP 주소로 또는 그 반대로 변경할 수 있습니다. DNAT(대상 NAT) 규칙을 만들어 대상 IP 주소를 공개 IP 주소에서 개인 IP 주소로 또는 그 반대로 변경할 수 있습니다.

NAT 규칙을 만들 때 다음 형식을 사용하여 원래 IP 주소와 변환된 IP 주소를 지정할 수 있습니다.


- IP 주소(예: 192.0.2.0)
- IP 주소 범위(예: 192.0.2.0-192.0.2.24)
- IP 주소/서브넷 마스크(예: 192.0.2.0/24)
- any

vCloud Director 환경의 Edge 게이트웨이에 SNAT 또는 DNAT 규칙을 구성할 때는 항상 조직 가상 데이터 센터의 관점에서 규칙을 구성해야 합니다. SNAT 규칙은 조직 가상 데이터 센터 네트워크에서 외부 네트워크 또는 다른 조직 가상 데이터 센터 네트워크로 전송되는 패킷의 소스 IP 주소를 변환합니다. DNAT 규칙은 외부 네트워크 또는 다른 조직 가상 데이터 센터 네트워크에서 들어오는 조직 가상 데이터 센터 네트워크에서 수신한 패킷의 IP 주소(필요한 경우 포트 포함)를 변환합니다.

사전 요구 사항

규칙을 추가할 NSX Data Center for vSphere Edge 게이트웨이 인터페이스에 공개 IP 주소가 추가된 상태여야 합니다. DNAT 규칙의 경우 원래(공용) IP 주소가 Edge 게이트웨이 인터페이스에 추가되어 있어야 하고 SNAT 규칙의 경우 변환된(공용) IP 주소가 인터페이스에 추가되어 있어야 합니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 **NAT**를 클릭하여 [NAT 규칙] 화면을 표시합니다.
- 3 만드는 NAT 규칙의 유형에 따라 **DNAT 규칙** 또는 **SNAT 규칙**을 클릭합니다.
- 4 대상 NAT 규칙(외부에서 내부로 들어옴)을 구성합니다.

옵션	설명
적용 대상	규칙을 적용할 인터페이스를 선택합니다.
원래 IP/범위	필요한 IP 주소를 입력합니다. 이 주소는 DNAT 규칙을 구성하는 Edge 게이트웨이의 공개 IP 주소여야 합니다. 검사 중인 패킷에서 이 IP 주소 또는 범위는 패킷의 대상 IP 주소로 나타나는 주소 또는 범위입니다. 이러한 패킷 대상 주소가 이 DNAT 규칙에 의해 변환됩니다.
프로토콜	규칙을 적용할 프로토콜을 선택합니다. 모든 프로토콜에 이 규칙을 적용하려면 임의 를 선택합니다.
원래 포트	(선택 사항) 수신 트래픽이 Edge 게이트웨이에서 가상 시스템이 연결된 내부 네트워크에 연결할 때 사용하는 포트 또는 포트 범위를 선택합니다. 프로토콜 이 ICMP 또는 임의 로 설정된 경우에는 포트 또는 포트 범위를 선택할 수 없습니다.
ICMP 유형	ICMP (디바이스 간 오류 정보 전달에 사용되는 오류 보고 및 진단 유틸리티)를 프로토콜 로 선택하는 경우 드롭다운 메뉴에서 ICMP 유형 을 선택합니다. ICMP 메시지는 유형 필드로 식별됩니다. 기본적으로 ICMP 유형은 [임의]로 설정됩니다.
변환된 IP/범위	인바운드 패킷의 대상 주소를 변환할 IP 주소 또는 IP 주소 범위를 입력합니다. 이러한 주소는 외부 네트워크의 트래픽을 수신할 수 있도록 DNAT를 구성하는 하나 이상의 가상 시스템에 대한 IP 주소입니다.
변환된 포트	(선택 사항) 인바운드 트래픽이 내부 네트워크의 가상 시스템에서 연결하는 포트 또는 포트 범위를 선택합니다. 이러한 포트는 DNAT 규칙이 가상 시스템에 대한 인바운드 패킷에 대해 변환하는 포트입니다.
설명	(선택 사항) 이 규칙의 작업을 식별하는 데 도움이 되는 설명을 입력합니다.
사용	이 규칙을 사용하도록 설정하려면 토글을 켭니다.
로그 사용	이 규칙에 의해 수행된 주소 변환을 기록하려면 토글을 켭니다.

5 소스 NAT 규칙(내부에서 외부로 나감)을 구성합니다.

옵션	설명
적용 대상	규칙을 적용할 인터페이스를 선택합니다.
원래 소스 IP/범위	이 규칙에 적용할 원래 IP 주소 또는 IP 주소 범위를 입력합니다. 이러한 주소는 외부 네트워크로 트래픽을 전송할 수 있도록 SNAT 규칙을 구성하는 하나 이상의 가상 시스템에 대한 IP 주소입니다.
변환된 소스 IP/범위	필요한 IP 주소를 입력합니다. 이 주소는 항상 SNAT 규칙을 구성하는 게이트웨이의 공개 IP 주소입니다. 외부 네트워크로 트래픽을 전송할 때 아웃바운드 패킷의 소스 주소(가상 시스템)를 변환할 IP 주소를 지정합니다.
설명	(선택 사항) 이 규칙의 작업을 식별하는 데 도움이 되는 설명을 입력합니다.
사용	이 규칙을 사용하도록 설정하려면 토글을 켭니다.
로깅 사용	이 규칙에 의해 수행된 주소 변환을 기록하려면 토글을 켭니다.

6 **유지**를 클릭하여 화면에 표시된 테이블에 규칙을 추가합니다.

7 추가 규칙을 구성하려면 단계를 반복합니다.

8 **변경 내용 저장**을 클릭하여 시스템에 규칙을 저장합니다.

다음에 수행할 작업

방금 구성한 SNAT 또는 DNAT 규칙에 대해 해당하는 Edge 게이트웨이 방화벽 규칙을 추가합니다. [NSX Data Center for vSphere Edge 게이트웨이 방화벽 규칙 추가](#)의 내용을 참조하십시오.

고급 라우팅 구성

NSX Data Center for vSphere Edge 게이트웨이에 대해 NSX 소프트웨어에서 제공하는 정적 및 동적 라우팅 기능을 구성할 수 있습니다.

동적 라우팅을 사용하도록 설정하려면 BGP(Border Gateway Protocol) 또는 OSPF(Open Shortest Path First) 프로토콜을 사용하여 고급 Edge 게이트웨이를 구성합니다.

NSX의 라우팅 기능에 대한 자세한 내용은 "NSX 관리" 설명서에서 "라우팅"을 참조하십시오.


각 고급 Edge 게이트웨이에 대한 정적 및 동적 라우팅을 지정할 수 있습니다. 동적 라우팅 기능은 계층 2 브로드캐스트 도메인 간에 필요한 전달 정보를 제공하므로 계층 2 브로드캐스트 도메인을 줄이고 네트워크 효율성 및 확장성을 높일 수 있습니다. NSX는 이러한 인텔리전스를 동-서 라우팅 워크로드의 위치로 확장합니다. 이 기능은 추가 비용 또는 시간을 들여 홉을 확장할 필요 없이 더 많은 가상 시스템이 직접 통신할 수 있도록 합니다.

NSX Data Center for vSphere Edge 게이트웨이의 기본 라우팅 구성 지정

Edge 게이트웨이의 정적 라우팅 및 동적 라우팅에 대한 기본 설정을 지정할 수 있습니다.

참고 구성된 라우팅 설정을 모두 제거하려면 **라우팅 구성** 화면의 맨 아래에서 **글로벌 구성 지우기**를 사용합니다. 이 작업을 수행하면 현재 하위 화면에 지정된 모든 라우팅 설정(기본 라우팅 설정, 정적 경로, OSPF, BGP 및 라우트 재분산)이 삭제됩니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 **라우팅 > 라우팅 구성**으로 이동합니다.
- 3 이 Edge 게이트웨이에 대해 ECMP(Equal Cost Multipath) 라우팅을 사용하도록 설정하려면 **ECMP** 토글을 켭니다.

"NSX 관리" 설명서에 나와 있는 대로 ECMP는 최적의 여러 경로를 통해 다음 홉 패킷이 단일 대상으로 전달될 수 있도록 하는 라우팅 전략입니다. NSX는 이러한 최적의 경로를 구성된 정적 경로를 사용하여 정적으로 결정하거나 OSPF 또는 BGP 같은 동적 라우팅 프로토콜의 메트릭 계산 결과를 바탕으로 결정합니다. 정적 경로에 대한 여러 경로를 지정하려면 [정적 경로] 화면에서 여러 개의 다음 홉을 지정합니다.

ECMP 및 NSX에 대한 자세한 내용은 "NSX 문제 해결 가이드"의 라우팅 항목을 참조하십시오.
- 4 기본 라우팅 게이트웨이의 설정을 지정합니다.
 - a **적용 대상** 드롭다운 목록을 사용하여 대상 네트워크로 향하는 그 다음 홉에 연결할 수 있는 인터페이스를 선택합니다.

선택한 인터페이스에 대한 세부 정보를 보려면 파란색 정보 아이콘을 클릭합니다.
 - b 게이트웨이 IP 주소를 입력합니다.
 - c MTU를 입력합니다.
 - d (선택 사항) 설명(선택 사항)을 입력합니다.
 - e **변경 내용 저장**을 클릭합니다.

5 기본 동적 라우팅 설정을 지정합니다.

참고 환경에 IPsec VPN이 구성되어 있는 경우 동적 라우팅을 사용하지 마십시오.

a 라우터 ID를 선택합니다.

목록에서 라우터 ID를 선택하거나 **+** 아이콘을 사용하여 새로 입력할 수 있습니다. 이 라우터 ID는 Edge 게이트웨이에서 동적 라우팅을 위한 커널에 경로를 푸시하는 첫 번째 업링크 IP 주소입니다.

b 로깅 사용 토글을 켜고 로그 수준을 선택하여 로깅을 구성합니다.

c 확인을 클릭합니다.

6 변경 내용 저장을 클릭합니다.

다음에 수행할 작업

정적 경로를 추가합니다. [정적 경로 추가](#)의 내용을 참조하십시오.

라우트 재분산을 구성합니다. [라우트 재분산 구성](#)의 내용을 참조하십시오.

동적 라우팅을 구성합니다. 다음 항목을 참조하십시오.

■ BGP 구성

■ OSPF 구성

정적 경로 추가

대상 서브넷 또는 호스트에 대한 정적 경로를 추가할 수 있습니다.

기본 라우팅 구성에서 ECMP를 사용하도록 설정한 경우 정적 경로에 여러 개의 다음 홉을 지정할 수 있습니다. ECMP 사용 설정을 위한 단계는 [NSX Data Center for vSphere Edge 게이트웨이의 기본 라우팅 구성 지정](#) 섹션을 참조하십시오.

사전 요구 사항

NSX 설명서에 설명된 대로 정적 경로의 다음 홉 IP 주소가 NSX Data Center for vSphere Edge 게이트웨이의 인터페이스 중 하나와 연결된 서브넷에 있어야 합니다. 그렇지 않으면 해당 정적 경로의 구성이 실패합니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.

b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.

c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 라우팅 > 정적 경로로 이동합니다.

3 만들기() 버튼을 클릭합니다.

4 정적 경로에 대한 다음 옵션을 구성합니다.

옵션	설명
네트워크	네트워크를 CIDR 표기법으로 입력합니다.
다음 홉	다음 홉의 IP 주소를 입력합니다. 다음 홉 IP 주소는 Edge 게이트웨이 인터페이스 중 하나와 연결된 서브넷에 있어야 합니다. ECMP를 사용하도록 설정한 경우 여러 개의 다음 홉을 입력할 수 있습니다.
MTU	데이터 패킷의 최대 전송 값을 편집합니다. MTU 값은 선택한 Edge 게이트웨이 인터페이스에 설정된 MTU보다 높을 수 없습니다. Edge 게이트웨이 인터페이스에 기본적으로 설정된 MTU는 [라우팅 구성] 화면에서 볼 수 있습니다.
인터페이스	필요한 경우 정적 경로를 추가할 Edge 게이트웨이 인터페이스를 선택합니다. 기본적으로 그 다음 홉 주소와 일치하는 인터페이스가 선택됩니다.
설명	필요한 경우 정적 경로에 대한 설명을 입력합니다.

5 변경 내용 저장을 클릭합니다.

다음에 수행할 작업

정적 경로에 대한 NAT 규칙을 구성합니다. [SNAT 또는 DNAT 규칙 추가](#)의 내용을 참조하십시오.

트래픽이 정적 경로를 이동할 수 있도록 하는 방화벽 규칙을 추가합니다. [NSX Data Center for vSphere Edge 게이트웨이 방화벽 규칙 추가](#)의 내용을 참조하십시오.

OSPF 구성

NSX Data Center for vSphere Edge 게이트웨이의 동적 라우팅 기능을 위해 OSPF(Open Shortest Path First) 라우팅 프로토콜을 구성할 수 있습니다. vCloud Director 환경에서는 주로 vCloud Director의 Edge 게이트웨이 간에 라우팅 정보를 교환하기 위해 Edge 게이트웨이에 OSPF를 적용합니다.


NSX Edge Gateway는 IP 패킷을 단일 라우팅 도메인 내에서만 라우팅하는 내부 게이트웨이 프로토콜인 OSPF를 지원합니다. "NSX 관리 가이드"에 설명된 대로 NSX Edge Gateway에 OSPF를 구성하면 Edge 게이트웨이가 경로를 학습하고 알릴 수 있습니다. Edge 게이트웨이는 OSPF를 사용하여 사용 가능한 Edge 게이트웨이에서 링크 상태 정보를 수집하고 네트워크의 토폴로지 맵을 만듭니다. 토폴로지는 인터넷 계층에 제공되는 라우팅 테이블을 결정하며 인터넷 계층은 IP 패킷에 있는 대상 IP 주소를 기반으로 라우팅 관련 결정을 내립니다.

결과적으로 OSPF 라우팅 정책은 동일 비용 경로 간의 트래픽 로드 밸런싱을 동적으로 처리합니다. OSPF 네트워크는 트래픽 흐름을 최적화하고 라우팅 테이블의 크기를 제한하기 위해 라우팅 영역으로 분할됩니다. 영역은 영역 ID가 동일한 OSPF 네트워크, 라우터 및 링크의 논리적 컬렉션입니다. 영역은 영역 ID로 식별됩니다.

사전 요구 사항


라우터 ID를 구성해야 합니다. [NSX Data Center for vSphere Edge 게이트웨이의 기본 라우팅 구성 지정](#).

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 라우팅 > OSPF로 이동합니다.
- 3 현재 OSPF를 사용하도록 설정하지 않은 경우 **OSPF 사용** 토글을 사용하여 설정합니다.
- 4 조직의 필요에 따라 OSPF 설정을 구성합니다.

옵션	설명
정상적인 다시 시작 사용	OSPF 서비스를 다시 시작할 때 패킷 전달이 중단 없이 계속되도록 지정합니다.
기본 시작 사용	Edge 게이트웨이가 OSPF 피어에 대한 기본 게이트웨이임을 알릴 수 있도록 합니다.


- 5 (선택 사항) **변경 내용 저장**을 클릭하거나 영역 정의 및 인터페이스 매핑 구성을 계속할 수 있습니다.

- 6 **추가**() 버튼을 클릭하고 대화 상자에 매핑 세부 정보를 지정한 후 **유지**를 클릭하여 OSPF 영역 정의를 추가합니다.

참고 기본적으로 영역 ID 51의 영역은 NSSA(Not-So-Stubby Area)로 구성되며 OSPF 화면의 영역 정의 테이블에 자동으로 표시됩니다. NSSA 영역을 수정하거나 삭제할 수 있습니다.

옵션	설명
영역 ID	IP 주소 또는 십진수 숫자 형식으로 영역 ID를 입력합니다.
영역 유형	<p>일반 또는 NSSA를 선택합니다.</p> <p>NSSA는 AS 외부 LSA(Link-State Advertisement)가 NSSA로 플러딩되지 않도록 합니다. NSSA는 외부 대상에 대한 기본 라우팅을 사용합니다. 따라서 NSSA는 OSPF 라우팅 도메인의 Edge에 배치되어야 합니다. NSSA는 외부 경로를 OSPF 라우팅 도메인으로 가져올 수 있으며, 이는 OSPF 라우팅 도메인의 일부가 아닌 작은 라우팅 도메인에 전송 서비스를 제공한다는 의미입니다.</p>
영역 인증	<p>영역 수준에서 수행할 OSPF 인증 유형을 선택합니다.</p> <p>영역 내의 모든 Edge 게이트웨이에는 동일한 인증 및 해당하는 암호가 구성되어야 합니다. MD5 인증이 작동하려면 수신기와 송신기의 MD5 키가 동일해야 합니다. 다음을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 없음 인증이 필요하지 않습니다. ■ 암호 이 항목을 선택하면 영역 인증 값 필드에서 지정하는 암호가 전송 패킷에 포함됩니다. ■ MD5 이 항목을 선택하면 인증에 MD5(Message Digest type 5) 암호화가 사용됩니다. 전송 패킷에 MD5 체크섬이 포함됩니다. 영역 인증 값 필드에 MD5 키를 입력합니다.

- 7 **변경 내용 저장**을 클릭하여 인터페이스 매핑을 추가할 때 새로 구성된 영역 정의를 선택할 수 있도록 합니다.

- 8 **추가**() 버튼을 클릭하고 대화 상자에 매핑 세부 정보를 지정한 후 **유지**를 클릭하여 인터페이스 매핑을 추가합니다.

이러한 매핑은 Edge 게이트웨이 인터페이스를 영역에 매핑합니다.

- a 대화 상자에서 영역 정의에 매핑할 인터페이스를 선택합니다.

인터페이스는 두 Edge 게이트웨이가 연결되는 외부 네트워크를 지정합니다.

- b 선택된 인터페이스에 매핑할 영역의 영역 ID를 선택합니다.

- c (선택 사항) OSPF 설정을 기본값에서 변경하여 이 인터페이스 매핑에 적절하게 사용자 지정합니다.

새 매핑을 구성하는 경우 이러한 설정의 기본값이 표시됩니다. 대부분의 경우 기본 설정을 유지하는 것이 좋습니다. 설정을 변경하는 경우 OSPF 피어에서 동일한 설정을 사용하도록 하십시오.

옵션	설명
Hello 간격	인터페이스에서 전송되는 Hello 패킷 간의 간격(초)입니다.
비활성 간격	인접 라우터의 비활성화가 선언되기 전에 인접 라우터로부터 최소 한 개의 Hello 패킷이 수신되어야 하는 간격(초)입니다.
우선순위	인터페이스의 우선 순위입니다. 우선 순위가 가장 높은 인터페이스는 지정된 Edge 게이트웨이 라우터입니다.
비용	해당 인터페이스를 통과하여 패킷을 보내는 데 필요한 오버헤드입니다. 인터페이스 비용은 해당 인터페이스의 대역폭과 반비례합니다. 대역폭이 클수록 비용이 적어집니다.

- d **유지**를 클릭합니다.

9 OSPF 화면에서 **변경 내용 저장**을 클릭합니다.

다음에 수행할 작업

라우팅 정보를 교환할 다른 Edge 게이트웨이에 OSPF를 구성합니다.

OSPF가 설정된 Edge 게이트웨이 간의 트래픽을 허용하는 방화벽 규칙을 추가합니다. [NSX Data Center for vSphere Edge 게이트웨이 방화벽 규칙 추가](#)의 내용을 참조하십시오.


라우트 재분산 및 방화벽 구성이 올바른 경로의 알림을 허용하는지 확인하십시오. [라우트 재분산 구성](#)의 내용을 참조하십시오.

BGP 구성


NSX Data Center for vSphere Edge 게이트웨이의 동적 라우팅 기능을 위해 BGP(Border Gateway Protocol)를 구성할 수 있습니다.

"NSX 관리 가이드"에 설명된 대로 BGP는 여러 독립 시스템 간의 네트워크 연결을 지정하는 IP 네트워크 또는 접두사 테이블을 사용하여 라우팅과 관련된 중요한 결정을 내립니다. 네트워킹 필드에서 BGP Speaker는 BGP를 실행하는 네트워킹 디바이스를 나타냅니다. 두 BGP Speaker는 라우팅 정보가 교환되기 전에 연결을 설정합니다. BGP 인접 라우터는 이러한 연결을 설정한 BGP Speaker를 나타냅니다. 두 디바이스는 연결을 설정한 후 경로를 교환하고 테이블을 동기화합니다. 각 디바이스는 연결 유지 메시지를 보내 이 연결 관계를 유지합니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 **라우팅 > BGP**로 이동합니다.
- 3 현재 BGP를 사용하도록 설정하지 않은 경우 **BGP 사용** 토글을 사용하여 설정합니다.
- 4 조직의 필요에 따라 BGP 설정을 구성합니다.

옵션	설명
정상적인 다시 시작 사용	BGP 서비스를 다시 시작할 때 패킷 전달이 중단 없이 계속되도록 지정합니다.
기본 시작 사용	Edge 게이트웨이가 BGP 인접 라우터에 대한 기본 게이트웨이임을 알릴 수 있도록 합니다.
로컬 AS	필수. 프로토콜의 로컬 AS(독립 시스템) 기능에 사용할 AS ID 번호를 지정합니다. 지정하는 값은 1에서 65534 사이의 전역적으로 고유한 번호여야 합니다. 로컬 AS는 BGP의 기능입니다. 구성하는 Edge 게이트웨이에 로컬 AS 번호가 할당됩니다. Edge 게이트웨이는 Edge 게이트웨이가 다른 독립 시스템의 BGP 인접 라우터와 피어 관계인 경우 이 ID를 알립니다. 동적 라우팅 알고리즘은 경로가 이동하는 독립 시스템의 경로를 하나의 메트릭으로 사용하여 대상까지 이동하는 최적의 경로를 선택합니다.

- 5 **변경 내용 저장**을 클릭하거나 BGP 라우팅 인접 라우터에 설정을 구성할 수 있습니다.
- 6 **추가**() 버튼을 클릭하고 대화 상자에 인접 라우팅 세부 정보를 지정한 후 **유지**를 클릭하여 BGP 인접 구성을 추가합니다.

옵션	설명
IP 주소	이 Edge 게이트웨이에 대한 BGP 인접 라우터의 IP 주소를 입력합니다.
원격 AS	이 BGP 인접 라우터가 속하는 독립 시스템에 대한 1~65534의 전역적으로 고유한 번호를 입력합니다. 이 원격 AS 번호는 시스템의 BGP 인접 라우터 테이블에서 BGP 인접 라우터 항목에 사용됩니다.
무게	인접 라우터 연결에 대한 기본 가중치입니다. 조직의 필요에 따라 조정합니다.
연결 유지 시간	소프트웨어가 연결 유지 메시지를 피어에 전송하는 빈도입니다. 기본 빈도는 60초입니다. 조직의 필요에 맞게 조정합니다.

옵션	설명
연결 억제 시간	<p>소프트웨어가 연결 유지 메시지를 수신하지 못하게 된 후부터 피어가 비활성화됨을 선언할 때까지의 간격입니다. 이 간격은 연결 유지 간격의 세 배여야 합니다. 기본 간격은 180초입니다. 조직의 필요에 맞게 조정합니다.</p> <p>두 BGP 인접 라우터 간의 피어 관계가 설정되면 Edge 게이트웨이가 연결 억제 타이머를 시작합니다. 인접 라우터에서 연결 유지 메시지가 수신될 때마다 연결 억제 타이머가 0으로 재설정됩니다. Edge 게이트웨이가 세 번 연속 연결 유지 메시지를 수신하지 못해 연결 억제 타이머가 연결 유지 간격의 세 배 값에 도달하면 Edge 게이트웨이는 인접 라우터가 중단된 것으로 간주하고 이 인접 라우터의 경로를 삭제합니다.</p>
암호	<p>이 BGP 인접 라우터에 인증이 필요한 경우 인증 암호를 입력합니다.</p> <p>인접 라우터 간의 연결에 전송된 각 세그먼트가 확인됩니다. 두 BGP 인접 라우터에 동일한 암호를 사용하여 MD5 인증을 구성해야 합니다. 그렇지 않으면 인접 라우터 간의 연결이 설정되지 않습니다.</p>
BGP 필터	<p>이 BGP 인접 라우터의 접두사 목록을 사용하여 경로 필터링을 지정하려면 이 테이블을 사용합니다.</p> <p>경고 필터의 마지막에 block all 규칙이 적용됩니다.</p> <p>+ 아이콘을 클릭하고 옵션을 구성하여 테이블에 필터를 추가합니다. 유지를 클릭하여 각 필터를 저장합니다.</p> <ul style="list-style-type: none"> ■ 방향을 선택하여 인접 라우터로 가는 트래픽을 필터링할지 인접 라우터에서 오는 트래픽을 필터링할지를 표시합니다. ■ 작업을 선택하여 트래픽을 허용할지 거부할지를 표시합니다. ■ 인접 라우터의 송/수신에서 필터링할 네트워크를 입력합니다. ANY를 입력하거나 네트워크를 CIDR 형식으로 입력합니다. ■ IP 접두사 목록에서 le 및 ge 키워드를 사용하려면 IP 접두사 GE 및 IP 접두사 LE를 입력합니다.

7 변경 내용 저장을 클릭하여 시스템에 구성을 저장합니다.

다음에 수행할 작업

라우팅 정보를 교환할 다른 Edge 게이트웨이에 BGP를 구성합니다.


BGP가 구성된 Edge 게이트웨이의 트래픽 송/수신을 허용하는 방화벽 규칙을 추가합니다. 자세한 내용은 [NSX Data Center for vSphere Edge 게이트웨이 방화벽 규칙 추가](#) 섹션을 참조하십시오.

라우트 재분산 구성

기본적으로 라우터는 동일한 프로토콜을 실행하는 다른 라우터와만 경로를 공유합니다. 다중 프로토콜 환경을 구성한 경우 교차 프로토콜 경로 공유를 사용하도록 라우트 재분산을 구성해야 합니다. NSX Data Center for vSphere Edge 게이트웨이에 대한 라우트 재분산을 구성할 수 있습니다.

절차


1 Edge 게이트웨이 서비스를 엽니다.

- 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 라우팅 > 라우트 재분산으로 이동합니다.

3 프로토콜 토글을 사용하여 라우트 재분산을 사용할 프로토콜을 켭니다.

4 IP 접두사를 화면의 테이블에 추가합니다.

- 추가() 버튼을 클릭합니다.
- 네트워크의 이름 및 IP 주소를 CIDR 형식으로 입력합니다.
- 유지**를 클릭합니다.

5 추가() 버튼을 클릭하고 대화 상자에 조건을 지정한 후 **유지**를 클릭하여 각 IP 접두사에 대해 재분산 조건을 지정합니다.

테이블의 항목은 순차적으로 처리됩니다. 위쪽 및 아래쪽 화살표를 사용하여 순서를 조정합니다.

옵션	설명
접두사 이름	이 조건을 적용할 특정 IP 접두사를 선택하거나 임의 를 선택하여 모든 네트워크 라우터에 조건을 적용합니다.
학습자 프로토콜	이 재분산 조건에서 다른 프로토콜을 통해 경로를 학습할 프로토콜을 선택합니다.
다음에서 학습 허용:	학습자 프로토콜 목록에서 선택한 프로토콜이 학습할 수 있는 경로가 있는 네트워크 유형을 선택합니다.
작업	선택한 네트워크 유형의 재분산을 허용할지, 아니면 거부할지를 선택합니다.

6 변경 내용 저장을 클릭합니다.

로드 밸런싱

로드 밸런서는 들어오는 서비스 요청을 사용자에게 투명한 로드 분산 방식으로 여러 서버에 분산합니다. 로드 밸런싱은 리소스 사용을 최적화하고, 처리량을 극대화하며, 응답 시간을 최소화하고, 오버로드를 방지하는 데 도움이 됩니다.

NSX 로드 밸런서는 두 개의 로드 밸런싱 엔진을 지원합니다. 계층 4 로드 밸런서는 패킷 기반으로 빠른 경로 처리를 제공합니다. 계층 7 로드 밸런서는 소켓 기반이며, 고급 트래픽 관리 전략과 백엔드 서비스를 위한 DDOS 완화를 지원합니다.

Edge 게이트웨이는 외부 네트워크에서 수신되는 트래픽을 로드 밸런싱하기 때문에 NSX Data Center for vSphere Edge 게이트웨이에 대한 로드 밸런싱은 외부 인터페이스에 구성됩니다. 로드 밸런싱을 위한 가상 서버를 구성할 때 조직 VDC에 있는 사용 가능한 IP 주소 중 하나를 지정합니다.

로드 밸런싱 전략 및 개념

패킷 기반 로드 밸런싱 전략은 TCP 및 UDP 계층에서 구현됩니다. 패킷 기반 로드 밸런싱은 연결을 중지하거나 전체 요청을 버퍼링하지 않습니다. 대신 패킷을 조작한 후, 선택한 서버로 직접 전송합니다. TCP 및 UDP 세션은 단일 세션에 대한 패킷이 동일한 서버에 직접 연결되도록 로드 밸런서에 유지됩니다. 글로벌 구성과 관련 가상 서버 구성 모두에서 [가속화 사용]을 선택하여 패킷 기반 로드 밸런싱을 사용하도록 설정할 수 있습니다.

소켓 기반 로드 밸런싱 전략은 소켓 인터페이스 위에 구현됩니다. 단일 요청에 대해 두 개의 연결, 즉 클라이언트 연결과 서버 연결이 설정됩니다. 서버 연결은 서버 선택 후에 설정됩니다. HTTP 소켓 기반 구현의 경우 선택적 L7 조작을 사용하여 선택된 서버에 전송하기 전에 전체 요청이 수신됩니다. HTTPS 소켓 기반 구현의 경우 클라이언트 연결 또는 서버 연결에서 인증 정보가 교환됩니다. 소켓 기반 로드 밸런싱은 TCP, HTTP 및 HTTPS 가상 서버의 기본 모드입니다.

NSX 로드 밸런서의 주요 개념은 가상 서버, 서버 풀, 서버 풀 멤버 및 서비스 모니터입니다.

가상 서버

IP, 포트, 프로토콜 및 TCP 또는 UDP와 같은 애플리케이션 프로파일의 고유 조합으로 나타내는 애플리케이션 서비스의 추상적 개념입니다.

서버 풀

백엔드 서버 그룹입니다.

서버 풀 멤버

백엔드 서버를 풀의 멤버로 나타냅니다.

서비스 모니터

백엔드 서버의 상태에 대한 검색 방법을 정의합니다.

애플리케이션 프로파일

특정 애플리케이션에 대한 TCP, UDP, 지속성 및 인증서 구성을 나타냅니다.

설정 개요

먼저 로드 밸런서에 대한 글로벌 옵션을 설정합니다. 이제 백엔드 서버 멤버로 구성된 서버 풀을 생성하고 서비스 모니터와 풀을 연결하여 백엔드 서버를 효과적으로 관리하고 공유할 수 있습니다.

그런 다음 애플리케이션 프로파일을 생성하여 클라이언트 SSL, 서버 SSL, X-Forwarded-For 또는 지속성과 같은 로드 밸런서의 공통 애플리케이션 동작을 정의합니다. 지속성은 유사한 특성을 가진 후속 요청을 전송합니다. 예를 들어 로드 밸런싱 알고리즘을 실행하지 않고 소스 IP 또는 쿠키를 동일한 풀 멤버로 디스패치해야 합니다. 애플리케이션 프로파일은 가상 서버에서 재사용할 수 있습니다.

그런 다음 선택적 애플리케이션 규칙을 생성하여 서로 다른 요청이 서로 다른 풀에 의해 처리될 수 있도록 특정 URL 또는 호스트 이름 일치와 같은 트래픽 조작에 대해 애플리케이션별 설정을 구성합니다. 다음으로, 애플리케이션과 관련된 서비스 모니터를 생성하거나 요구에 부합하는 경우 기존 서비스 모니터를 사용할 수 있습니다.

필요한 경우 L7 가상 서버의 고급 기능을 지원하는 애플리케이션 규칙을 생성할 수 있습니다. 애플리케이션 규칙의 일부 사용 사례로는 콘텐츠 전환, 헤더 조작, 보안 규칙, DOS 보호 등이 있습니다.

마지막으로 서버 풀, 애플리케이션 프로파일 및 잠재적 애플리케이션 규칙을 함께 연결하는 가상 서버를 생성합니다.


가상 서버가 요청을 수신하면 로드 밸런싱 알고리즘이 풀 멤버 구성과 런타임 상태를 고려합니다. 이후 알고리즘은 트래픽을 분산하기 위해 하나 이상의 멤버로 이루어진 적절한 풀을 계산합니다. 풀 멤버 구성에는 가중치, 최대 연결, 조건 상태와 같은 설정이 포함됩니다. 런타임 상태에는 현재 연결, 응답 시간, 상태 점검 상태 정보가 포함됩니다. 계산 방법은 라운드 로빈, 가중치가 적용된 라운드 로빈, 최소 연결, 소스 IP 해시, 가중치가 적용된 최소 연결, URL, URI 또는 HTTP 헤더일 수 있습니다.

각 풀은 연결된 서비스 모니터에 의해 모니터링됩니다. 로드 밸런서가 풀 멤버의 문제를 발견하면 해당 멤버를 [다운] 상태로 표시합니다. 서버 풀에서 풀 멤버를 선택하면 [가동] 서버만 선택됩니다. 서버 풀을 서비스 모니터로 구성하지 않은 경우 모든 풀 멤버가 [가동]으로 간주됩니다.

로드 밸런서 서비스 구성

글로벌 로드 밸런서 구성 매개 변수에는 전체 지원, 일부 계층 4 또는 계층 7 엔진 및 기록할 이벤트 유형의 규격이 포함됩니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 **로드 밸런서 > 글로벌 구성**으로 이동합니다.
- 3 사용하도록 설정할 옵션을 선택합니다.

옵션	작업
상태	<p>토글 아이콘을 클릭하여 로드 밸런서를 사용하도록 설정합니다.</p> <p>로드 밸런서가 L7 엔진보다 빠른 L4 엔진을 사용하도록 구성하려면 가속화 사용을 설정합니다. L4 TCP VIP가 Edge 게이트웨이 방화벽보다 먼저 처리되므로 방화벽 허용 규칙이 필요하지 않습니다.</p> <p>참고 HTTP 및 HTTPS에 대한 L7 VIP는 방화벽 다음에 처리되므로 가속화를 사용하도록 설정하지 않은 경우 이러한 프로토콜에 대한 L7 VIP 액세스를 허용하려면 Edge 게이트웨이 방화벽 규칙이 있어야 합니다. 가속화를 사용하도록 설정하고 서버 풀이 비투명 모드인 경우 SNAT 규칙이 추가되므로 Edge 게이트웨이에서 방화벽을 사용하도록 설정되어 있는지 확인해야 합니다.</p>
로깅 사용	Edge 게이트웨이 로드 밸런서가 트래픽 로그를 수집할 수 있도록 로깅을 사용하도록 설정합니다.
로그 수준	로그에 수집될 이벤트의 심각도 선택합니다.

4 변경 내용 저장을 클릭합니다.

저장 작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

다음에 수행할 작업

로드 밸런서에 대한 애플리케이션 프로파일을 구성합니다. [애플리케이션 프로파일 만들기](#)의 내용을 참조하십시오.

애플리케이션 프로파일 만들기


애플리케이션 프로파일은 특정 유형의 네트워크 트래픽에 대한 로드 밸런서의 동작을 정의합니다. 프로파일을 구성한 후 가상 서버에 연결합니다. 그러면 가상 서버가 프로파일에 지정된 값에 따라 트래픽을 처리합니다. 프로파일을 사용하면 네트워크 트래픽 관리를 효과적으로 제어하고 트래픽 관리 작업을 더 쉽고 효율적으로 수행할 수 있습니다.

HTTPS 트래픽에 프로파일을 만드는 경우 다음 HTTPS 트래픽 패턴을 사용할 수 있습니다.

- 클라이언트 -> HTTPS -> LB(SSL 종료) -> HTTP -> 서버
- 클라이언트 -> HTTPS -> LB(SSL 종료) -> HTTPS -> 서버
- 클라이언트 -> HTTPS -> LB(SSL 패스스루) -> HTTPS -> 서버
- 클라이언트 -> HTTP -> LB -> HTTP -> 서버

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 로드 밸런서 > 애플리케이션 프로파일로 이동합니다.

3 만들기() 버튼을 클릭합니다.

4 프로파일의 이름을 입력합니다.

5 애플리케이션 프로파일을 구성합니다.

옵션	설명
유형	서버에 요청을 보낼 때 사용할 프로토콜 유형을 선택합니다. 필수 매개 변수 목록은 선택한 프로토콜에 따라 다릅니다. 선택한 프로토콜에 해당되지 않는 매개 변수는 입력할 수 없습니다. 다른 모든 매개 변수는 필수입니다.
SSL 패스스루 사용	가상 서버에 SSL 인증을 패스스루하려면 클릭합니다. 그렇지 않으면 SSL 인증이 대상 주소에서 수행됩니다.
HTTP 리디렉션 URL	(HTTP 및 HTTPS) 대상 주소에 도착하는 트래픽을 리디렉션할 URL을 입력합니다.

옵션	설명
지속성	<p>프로파일에 대한 지속성 메커니즘을 지정합니다.</p> <p>지속성은 세션 데이터(예: 클라이언트 요청에 서비스를 제공한 특정 풀 구성원)를 추적하고 저장합니다. 따라서 클라이언트 요청이 세션 수명 전체 또는 후속 세션에서 동일한 풀 구성원에 전달될 수 있습니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> ■ 소스 IP <p>소스 IP 지속성은 소스 IP 주소를 기반으로 세션을 추적합니다. 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 할당합니다.</p> ■ MSRDP <p>(TCP만 해당) MSRDP(Microsoft 원격 데스크톱 프로토콜) 지속성은 Microsoft RDP(원격 데스크톱 프로토콜) 서비스를 실행하는 서버와 Windows 클라이언트 간에 영구 세션을 유지합니다. MSRDP 지속성 사용에 권장되는 시나리오는 Windows Server 게스트 운영 체제를 실행하는 구성원으로 구성되는 로드 밸런싱 풀을 만드는 것입니다. 이 풀의 모든 구성원은 Windows 클러스터에 속하고 Windows 세션 디렉터리에 참여합니다.</p> ■ SSL 세션 ID <p>SSL 세션 ID 지속성은 SSL 패스워드를 사용하도록 설정할 때 사용할 수 있습니다. SSL 세션 ID 지속성은 동일한 클라이언트로부터의 반복 연결이 동일한 서버로 전송되도록 합니다. 세션 ID 지속성을 사용하면 SSL 세션 재개를 사용하여 클라이언트와 서버 모두에 대한 처리 시간을 절약할 수 있습니다.</p>
쿠키 이름	<p>(HTTP 및 HTTPS) 지속성 메커니즘으로 쿠키를 지정한 경우 쿠키 이름을 입력합니다. 쿠키 지속성은 클라이언트가 사이트에 처음으로 액세스할 때 쿠키를 사용하여 세션을 고유하게 식별합니다. 로드 밸런서는 이 쿠키를 참조로 세션의 후속 요청을 연결하여 모두 동일한 가상 서버로 이동할 수 있도록 합니다.</p>
모드	<p>쿠키를 삽입할 때 사용할 모드를 선택합니다. 다음 모드가 지원됩니다.</p> <ul style="list-style-type: none"> ■ 삽입 <p>Edge 게이트웨이가 쿠키를 전송합니다. 서버가 하나 이상의 쿠키를 전송하면 클라이언트에 쿠키 하나가 추가로 수신됩니다(서버 쿠키와 Edge 게이트웨이 쿠키). 서버가 쿠키를 전송하지 않으면 클라이언트에 Edge 게이트웨이 쿠키만 수신됩니다.</p> ■ 접두사 <p>클라이언트가 둘 이상의 쿠키를 지원하지 않는 경우 이 옵션을 선택합니다.</p> <p>참고 모든 브라우저는 다중 쿠키를 수락합니다. 그러나 단일 쿠키만 지원하는 독점적 클라이언트 기반의 독점적 애플리케이션의 경우는 다릅니다. 웹 서버는 평소대로 쿠키를 전송합니다. Edge 게이트웨이는 쿠키 정보를 서버 쿠키 값에 접두사로 주입합니다. 이 추가 쿠키 정보는 Edge 게이트웨이가 쿠키 정보를 서버로 보낼 때 제거됩니다.</p> ■ 애플리케이션 세션 이 옵션을 선택하면 서버가 쿠키를 보내지 않습니다. 대신 사용자 세션 정보를 URL로 보냅니다. 예를 들어 <code>http://example.com/admin/UpdateUserServlet;jsessionid=0I24B9ASD7BSSD</code> URL로 전송합니다. 여기서 <code>jsessionid</code>가 사용자 세션 정보이며 지속성을 위해 사용됩니다. 애플리케이션 세션 지속성 테이블은 문제 해결용으로 확인할 수 없습니다.

옵션	설명
(초) 후에 만료됨	지속성을 유효한 상태로 유지할 시간(초)을 입력합니다. 1~86400 범위의 양수여야 합니다. 참고 TCP 소스 IP 지속성을 사용하는 L7 로드 밸런싱의 경우 새 TCP 연결이 일정 기간 동안 생성되지 않으면 기존 연결이 유지되는 경우에도 지속성 항목이 시간 초과됩니다.
X-Forwarded-For HTTP 헤더 삽입	(HTTP 및 HTTPS) X-Forwarded-For HTTP 헤더 삽입을 선택하면 로드 밸런서를 통해 웹 서버에 연결하는 클라이언트의 원래 IP 주소가 식별됩니다. 참고 SSL 패스스루를 사용하도록 설정한 경우에는 이 헤더를 사용할 수 없습니다.
풀 쪽 SSL 사용	(HTTPS만 해당) [풀 인증서] 탭에서 풀 쪽 SSL 사용을 선택하여 서버 측 로드 밸런서 인증에 사용할 인증서, CA 또는 CRL을 정의합니다.

- 6 (HTTPS만 해당) 애플리케이션 프로파일에 사용할 인증서를 구성합니다. 필요한 인증서가 없는 경우 **인증서** 탭에서 인증서를 만들 수 있습니다.

옵션	설명
가상 서버 인증서	HTTPS 트래픽 암호 해독에 사용할 인증서, CA 또는 CRL을 선택합니다.
풀 인증서	서버 측 로드 밸런서의 인증에 사용할 인증서, CA 또는 CRL을 정의합니다. 참고 이 탭을 사용하려면 풀 쪽 SSL 사용을 선택합니다.
암호	SSL/TLS 핸드셰이크 중에 협상되는 암호 알고리즘(또는 암호 그룹)을 선택합니다.
클라이언트 인증	클라이언트 인증을 무시할지, 아니면 필수로 설정할지를 지정합니다. 참고 필수로 설정하면 요청 또는 핸드셰이크가 취소된 후 클라이언트가 인증서를 제공해야 합니다.

- 7 **유지** 를 클릭하여 변경 내용을 유지합니다.

작업을 완료하는 데 몇 분이 걸릴 수 있습니다.



다음에 수행할 작업

로드 밸런서에 대한 서비스 모니터를 추가하여 다양한 유형의 네트워크 트래픽에 대한 상태 점검을 정의합니다. [서비스 모니터 만들기](#)의 내용을 참조하십시오.

서비스 모니터 만들기

특정 유형의 네트워크 트래픽에 대한 상태 점검 매개 변수를 정의하는 서비스 모니터를 만듭니다. 서비스 모니터를 풀에 연결하면 풀 구성원이 서비스 모니터 매개 변수에 따라 모니터링됩니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 **로드 밸런서 > 서비스 모니터링**으로 이동합니다.
- 3 만들기() 버튼을 클릭합니다.
- 4 서비스 모니터의 이름을 입력합니다.
- 5 (선택 사항) 서비스 모니터에 대한 다음 옵션을 구성합니다.

옵션	설명
간격	지정된 방법 을 사용하여 서버를 모니터링할 간격을 입력합니다.
시간 초과	서버의 응답을 수신해야 하는 최대 시간을 초 단위로 입력합니다.
최대 재시도 횟수	서버가 다운된 것으로 선언하기 전에 지정된 모니터링 방법 이 연속으로 실패해야 하는 횟수를 입력합니다.
유형	상태 점검 요청을 서버로 보낼 때 사용할 방법(HTTP, HTTPS, TCP, ICMP 또는 UDP)을 선택합니다. 선택한 유형에 따라 새 서비스 모니터 대화 상자의 나머지 옵션이 사용되거나 사용되지 않습니다.
예상	(HTTP 및 HTTPS) 모니터가 HTTP 또는 HTTPS 응답의 상태 줄에서 일치할 것으로 예상하는 문자열을 입력합니다(예: HTTP/1.1).
방법	(HTTP 및 HTTPS) 서버 상태를 감지할 때 사용할 방법을 선택합니다.
URL	(HTTP 및 HTTPS) 서버 상태 요청에 사용할 URL을 입력합니다. 참고 POST 방법을 선택하는 경우 보내기 에 대한 값을 지정해야 합니다.
보내기	(HTTP, HTTPS, UDP) 보낼 데이터를 입력합니다.
받기	(HTTP, HTTPS 및 UDP) 응답 콘텐츠에서 일치 여부를 확인할 문자열을 입력합니다. 참고 예상 이 일치하지 않으면 모니터가 받기 콘텐츠의 일치를 시도하지 않습니다.
확장	(모두) 고급 모니터 매개 변수를 키=값 쌍으로 입력합니다. 예를 들어 warning=10은 서버가 10초 내에 응답하지 않을 경우 상태를 warning으로 설정합니다. 모든 확장 항목은 캐리지 리턴 문자로 구분해야 합니다. 예는 다음과 같습니다. <pre><extension>delay=2 critical=3 escape</extension></pre>

6 유지 를 클릭하여 변경 내용을 유지합니다.

작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

예제: 각 프로토콜에 대해 지원되는 확장

표 7-1. HTTP/HTTPS 프로토콜에 대한 확장

모니터 확장	설명
no-body	문서 본문을 기다리지 않고 HTTP/HTTPS 헤더까지만 읽습니다. 참고 HTTP GET 또는 HTTP POST는 계속 전송되고 HEAD 방법은 전송되지 않습니다.
max-age=SECONDS	문서가 SECONDS 이상 경과한 경우 경고합니다. 분의 경우 10m, 시간의 경우 10h 또는 일의 경우 10d의 형식으로 숫자를 입력할 수 있습니다.
content-type=STRING	POST 호출에 Content-Type 헤더 미디어 유형을 지정합니다.
linespan	정규식을 새 행으로 연장할 수 있습니다(-r 또는 -R에 선행해야 함).
regex=STRING 또는 ereg=STRING	정규식 STRING의 페이지를 검색합니다.
eregi=STRING	대/소문자를 구분하지 않는 정규식 STRING의 페이지를 검색합니다.
invert-regex	찾은 경우 CRITICAL을 반환하고 찾을 수 없는 경우 OK를 반환합니다.
proxy-authorization=AUTH_PAIR	기본 인증을 사용하는 프록시 서버의 username:password를 지정합니다.
useragent=STRING	HTTP 헤더의 문자열을 User Agent로 전송합니다.
header=STRING	HTTP 헤더의 다른 모든 태그를 전송합니다. 추가 헤더가 있는 경우 여러 번 사용합니다.
onredirect=ok warning critical follow sticky stickyport	리디렉션된 페이지를 처리하는 방법을 나타냅니다. sticky 는 follow 와 유사하지만 지정된 IP 주소에 고정됩니다. stickyport 는 포트가 동일하게 유지되도록 합니다.
pagesize=INTEGER:INTEGER	필요한 최소 및 최대 페이지 크기(바이트)를 지정합니다.
warning=DOUBLE	경고 상태를 야기하는 응답 시간(초)을 지정합니다.
critical=DOUBLE	위험 상태를 야기하는 응답 시간(초)을 지정합니다.

표 7-2. HTTPS 프로토콜 전용 확장

모니터 확장	설명
sni	SSL/TLS 호스트 이름 확장 지원(SNI)을 사용하도록 설정합니다.
certificate=INTEGER	인증서의 최소 유효 기간을 지정합니다. 포트 기본값은 443입니다. 이 옵션을 사용하는 경우 URL이 검사되지 않습니다.
authorization=AUTH_PAIR	기본 인증을 사용하는 사이트의 username:password를 지정합니다.

표 7-3. TCP 프로토콜에 대한 확장

모니터 확장	설명
escape	send 또는 quit 문자열에 \n, \r, \t 또는 \ 문자를 사용할 수 있습니다. send 또는 quit 옵션의 앞에 사용해야 합니다. 기본적으로 send에는 아무 문자도 추가되지 않으며 quit의 끝에는 \r\n 문자가 추가됩니다.
모든	서버 응답에 있어야 하는 모든 예상 문자열을 지정합니다. 기본적으로 any가 사용됩니다.
quit=STRING	서버로 문자열을 보내 연결을 완전히 닫습니다.
refuse=ok warn crit	ok, warn 또는 crit 상태를 사용하여 TCP 거부를 수락합니다. 기본적으로 crit 상태가 사용됩니다.
mismatch=ok warn crit	ok, warn 또는 crit 상태를 사용하여 예상되는 문자열 불일치를 수락합니다. 기본적으로 warn 상태가 사용됩니다.
jail	TCP 소켓의 출력을 숨깁니다.
maxbytes=INTEGER	지정된 바이트 수보다 많은 바이트가 수신되는 경우 연결을 닫습니다.
delay=INTEGER	문자열을 보내고 지정된 시간(초) 동안 대기한 후 응답을 폴링합니다.
certificate=INTEGER[,INTEGER]	인증서의 최소 유효 기간을 지정합니다. 첫 번째 값은 경고에 대한 #days이고 두 번째 값은 위험입니다(지정되지 않은 경우 0).
ssl	연결에 SSL을 사용합니다.
warning=DOUBLE	경고 상태를 야기하는 응답 시간(초)을 지정합니다.
critical=DOUBLE	위험 상태를 야기하는 응답 시간(초)을 지정합니다.



다음에 수행할 작업

로드 밸런서에 대한 서버 풀을 추가합니다. [로드 밸런싱을 위한 서버 풀 추가](#)의 내용을 참조하십시오.


로드 밸런싱을 위한 서버 풀 추가

서버 풀을 추가하여 백엔드 서버를 유연하고 효율적으로 관리 및 공유할 수 있습니다. 로드 밸런서 분산 방법은 풀이 관리하며 상태 점검 매개 변수에 대한 서비스 모니터가 풀에 연결되어 있습니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 **로드 밸런서 > 풀**로 이동합니다.
- 3 만들기() 버튼을 클릭합니다.
- 4 로드 밸런서 풀의 이름과 설명(선택 항목)을 입력합니다.
- 5 **알고리즘** 드롭다운 메뉴에서 서비스의 밸런싱 방법을 선택합니다.

옵션	설명
ROUND-ROBIN	각 서버에 할당된 가중치 순서대로 서버가 사용됩니다. 이는 서버의 처리 시간이 균등하게 분산된 상태를 유지하는 가장 유연하고 공정한 알고리즘입니다.
IP-HASH	각 패킷에 대해 소스 및 대상 IP 주소의 해시를 기반으로 서버를 선택합니다.
LEASTCONN	서버에 이미 열려 있는 연결 수를 기반으로 하여 클라이언트 요청을 여러 서버로 분산합니다. 새 연결은 열린 연결 수가 가장 적은 서버로 전송됩니다.
URI	URI의 왼쪽 부분(물음표 앞부분)을 해시한 후 실행 중인 서버의 총 가중치로 나눕니다. 이 결과에 따라 요청을 수신할 서버가 지정됩니다. 이 옵션을 사용하면 서버가 중단되지 않는 한 URI가 항상 동일한 서버로 연결됩니다.
HTTPHEADER	각 HTTP 요청에서 HTTP 헤더 이름을 조회합니다. 괄호 안의 헤더 이름은 ACL 'hdr()' 함수와 마찬가지로 대/소문자를 구분하지 않습니다. 헤더가 없거나 값이 포함되지 않은 경우 라운드 로빈 알고리즘이 적용됩니다. HTTPHEADER 알고리즘 매개 변수에는 headerName=<name> 옵션이 하나 있습니다. 예를 들어 host를 HTTPHEADER 알고리즘 매개 변수로 사용할 수 있습니다.
URL	각 HTTP GET 요청의 쿼리 문자열에서 인수에 지정된 URL 매개 변수를 조회합니다. 매개 변수 다음에 등호(=)와 값이 오는 경우 이 값을 해시하고 실행 중인 서버의 총 가중치로 나눕니다. 이 결과에 따라 요청을 수신할 서버가 지정됩니다. 이 프로세스는 요청의 사용자 식별자를 추적하고 서버가 중단되지 않는 한 동일한 사용자 ID가 항상 동일한 서버로 전송되도록 합니다. 값 또는 매개 변수가 없는 경우 라운드 로빈 알고리즘이 적용됩니다. URL 알고리즘 매개 변수에는 urlParam=<url> 옵션이 하나 있습니다.

- 6 풀에 구성원을 추가합니다.
 - a 추가() 버튼을 클릭합니다.
 - b 풀 구성원의 이름을 입력합니다.
 - c 풀 구성원의 IP 주소를 입력합니다.
 - d 구성원이 로드 밸런서의 트래픽을 수신할 포트를 입력합니다.

- e 구성원이 상태 모니터 요청을 수신할 모니터 포트를 입력합니다.
- f **가중치** 텍스트 상자에 이 구성원이 처리할 트래픽의 비율을 입력합니다. 1~256 범위의 정수여야 합니다.
- g (선택 사항) **최대 연결** 텍스트 상자에 구성원이 처리할 수 있는 최대 동시 연결 수를 입력합니다.
수신 요청의 수가 최대 연결 수를 초과하면 요청이 대기열로 이동하고 로드 밸런서가 연결이 해제 될 때까지 대기합니다.
- h (선택 사항) **최소 연결** 텍스트 상자에 구성원이 항상 수락해야 하는 최소 동시 연결 수를 입력합니다.
- i **유지**를 클릭하여 새 구성원을 풀에 추가합니다.
작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

7 (선택 사항) 클라이언트 IP 주소를 백엔드 서버에 표시하려면 투명을 선택합니다.

투명을 선택하지 않으면(기본값) 백엔드 서버에 트래픽 소스의 IP 주소가 로드 밸런서의 내부 IP 주소로 표시됩니다.

투명을 선택하면 소스 IP 주소가 클라이언트의 실제 IP 주소로 표시되며 Edge 게이트웨이를 기본 게이트웨이로 설정하여 반환 패킷이 Edge 게이트웨이를 통해 전송되도록 해야 합니다.

8 유지를 클릭하여 변경 내용을 유지합니다.

작업을 완료하는 데 몇 분이 걸릴 수 있습니다.



다음에 수행할 작업

로드 밸런서에 대한 가상 서버를 추가합니다. 가상 서버는 공개 IP 주소를 사용하며 모든 수신 클라이언트 요청을 처리합니다. [가상 서버 추가](#)의 내용을 참조하십시오.

애플리케이션 규칙 추가

애플리케이션 규칙을 작성하여 IP 애플리케이션 트래픽을 직접 조작하고 관리할 수 있습니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 **로드 밸런서 > 애플리케이션 규칙**으로 이동합니다.
- 3 **추가**() 버튼을 클릭합니다.
- 4 애플리케이션 규칙의 이름을 입력합니다.

5 애플리케이션 규칙의 스크립트를 입력합니다.

애플리케이션 규칙 구문에 대한 자세한 내용은 <http://cbonte.github.io/haproxy-dconv/configuration-1.5.html>을 참조하십시오.

6 유지 를 클릭하여 변경 내용을 유지합니다.

작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

다음에 수행할 작업

로드 밸런서에 대해 추가된 가상 서버에 새 애플리케이션 규칙을 연결합니다. [가상 서버 추가](#)의 내용을 참조하십시오.


가상 서버 추가

NSX Data Center for vSphere Edge 게이트웨이 내부 또는 업링크 인터페이스를 가상 서버로 추가합니다. 가상 서버는 공개 IP 주소를 사용하며 모든 수신 클라이언트 요청을 처리합니다.

기본적으로 로드 밸런서는 각 클라이언트 요청 후 서버 TCP 연결을 닫습니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 로드 밸런서 > 가상 서버로 이동합니다.

3 추가() 버튼을 클릭합니다.

4 일반 탭에서 가상 서버에 대한 다음 옵션을 구성합니다.

옵션	설명
가상 서버 사용	가상 서버를 사용하도록 설정하려면 클릭합니다.
가속화 사용	가속화를 사용하도록 설정하려면 클릭합니다.
애플리케이션 프로파일	가상 서버와 연결할 애플리케이션 프로파일을 선택합니다.
이름	가상 서버의 이름을 입력합니다.
설명	가상 서버에 대한 설명(선택 사항)을 입력합니다.
IP 주소	로드 밸런서가 수신 대기하는 IP 주소를 입력하거나 찾아서 선택합니다.
프로토콜	가상 서버가 수락하는 프로토콜을 선택합니다. 선택한 애플리케이션 프로파일 에 사용되는 동일한 프로토콜을 선택해야 합니다.
포트	로드 밸런서가 수신하는 포트 번호를 입력합니다.
기본 풀	로드 밸런서가 사용할 서버 풀을 선택합니다.

옵션	설명
연결 제한	(선택 사항) 가상 서버가 처리할 수 있는 최대 동시 연결 수를 입력합니다.
연결 속도 제한(CPS)	(선택 사항) 초당 수신되는 새 연결 요청의 최대 수를 입력합니다.

- 5 (선택 사항) 애플리케이션 규칙을 가상 서버에 연결하려면 **고급** 탭을 클릭하고 다음 단계를 완료합니다.

- a **추가**() 버튼을 클릭합니다.

로드 밸런서에 대해 만들어진 애플리케이션 규칙이 표시됩니다. 필요한 경우 로드 밸런서에 대한 애플리케이션 규칙을 추가합니다. [애플리케이션 규칙 추가](#)의 내용을 참조하십시오.

- 6 **유지**를 클릭하여 변경 내용을 유지합니다.

작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

다음에 수행할 작업

새 가상 서버(대상 IP 주소)로의 트래픽을 허용하는 Edge 게이트웨이 방화벽 규칙을 만듭니다. [NSX Data Center for vSphere Edge 게이트웨이 방화벽 규칙 추가](#) 항목을 참조하십시오.

VPN(Virtual Private Network)을 사용한 보안 액세스

NSX Data Center for vSphere Edge 게이트웨이에 대해 NSX 소프트웨어에서 제공하는 VPN 기능을 구성할 수 있습니다. SSL VPN-Plus 터널, IPsec VPN 터널 또는 L2 VPN 터널을 사용하여 조직 가상 데이터 센터에 대한 VPN 연결을 구성할 수 있습니다.

"NSX 관리 가이드"에 설명된 대로 NSX Edge Gateway는 다음 VPN 서비스를 지원합니다.

- SSL VPN-Plus. 원격 사용자가 비공개 기업 애플리케이션에 액세스할 수 있도록 합니다.
- IPsec VPN. NSX가 있는 원격 사이트 또는 타사 하드웨어 라우터나 VPN 게이트웨이가 있는 원격 사이트와 NSX Edge Gateway 사이의 사이트 간 연결을 제공합니다.
- L2 VPN. 가상 시스템이 지리적 경계 전체에서 동일한 IP 주소로 네트워크에 연결을 유지할 수 있도록 함으로써 조직 가상 데이터 센터를 확장할 수 있도록 합니다.

vCloud Director 환경에서 다음과 같은 VPN 터널을 만들 수 있습니다.

- 동일한 조직의 조직 가상 데이터 센터 네트워크 간 VPN 터널
- 서로 다른 조직의 조직 가상 데이터 센터 네트워크 간 VPN 터널
- 조직 가상 데이터 센터 네트워크와 외부 네트워크 간 VPN 터널

참고 vCloud Director는 동일한 두 Edge 게이트웨이 간의 다중 VPN 터널을 지원하지 않습니다. 두 Edge 게이트웨이 간에 기존 터널이 있고 이 터널에 다른 서브넷을 추가하려는 경우 기존 VPN 터널을 삭제한 후 새 서브넷을 포함하는 새 터널을 만듭니다.

Edge 게이트웨이에 대한 VPN 터널을 구성한 후 VPN 클라이언트를 사용하여 원격 위치에서 해당 Edge 게이트웨이를 통해 지원되는 조직 가상 데이터 센터에 연결할 수 있습니다.

SSL VPN-Plus 구성

vCloud Director 환경의 NSX Data Center for vSphere Edge 게이트웨이를 위한 SSL VPN-Plus 서비스는 원격 사용자가 Edge 게이트웨이로 지원되는 조직 가상 데이터 센터의 개인 네트워크 및 애플리케이션에 안전하게 연결할 수 있도록 합니다. Edge 게이트웨이에서 다양한 SSL VPN-Plus 서비스를 구성할 수 있습니다.

vCloud Director 환경에서 Edge 게이트웨이 SSL VPN-Plus 기능은 네트워크 액세스 모드를 지원합니다. 원격 사용자는 SSL 클라이언트를 설치하여 보안 연결을 설정하고 Edge 게이트웨이 뒤에서 네트워크 및 애플리케이션에 액세스해야 합니다. Edge 게이트웨이 SSL VPN-Plus 구성 중에 운영 체제의 설치 패키지를 추가하고 특정 매개 변수를 구성합니다. 자세한 내용은 [SSL VPN-Plus Client 설치 패키지 추가](#)를 참조하십시오.

Edge 게이트웨이에 SSL VPN-Plus를 구성하는 프로세스는 여러 단계를 수행하여 완료됩니다.

사전 요구 사항

SSL VPN-Plus에 필요한 모든 SSL 인증서가 **인증서** 화면에 추가되었는지 확인합니다. [SSL 인증서 관리](#)의 내용을 참조하십시오.

참고 Edge 게이트웨이에서 포트 443은 HTTPS의 기본 포트입니다. SSL VPN 기능을 사용하려면 외부 네트워크에서 Edge 게이트웨이 HTTPS 포트에 액세스할 수 있어야 합니다. SSL VPN 클라이언트가 작동하려면 클라이언트 시스템이 **SSL VPN-Plus** 탭에 있는 [서버 설정] 화면에서 구성된 Edge 게이트웨이 IP 주소 및 포트에 연결할 수 있어야 합니다. [SSL VPN 서버 설정 구성](#)의 내용을 참조하십시오.

절차

1 [SSL-VPN Plus](#) 화면으로 이동

[SSL-VPN Plus] 화면으로 이동하여 NSX Data Center for vSphere Edge 게이트웨이에 대한 SSL-VPN Plus 서비스 구성을 시작할 수 있습니다.

2 [SSL VPN](#) 서버 설정 구성

이러한 서버 설정은 서비스가 수신하는 IP 주소 및 포트, 서비스의 암호 목록 및 서비스 인증서와 같은 SSL VPN 서버를 구성합니다. NSX Data Center for vSphere Edge 게이트웨이에 연결할 때 원격 사용자는 이 서버 설정에서 설정한 것과 동일한 IP 주소와 포트를 지정합니다.

3 [NSX Data Center for vSphere Edge](#) 게이트웨이에서 [SSL VPN-Plus](#)와 함께 사용할 IP 풀 생성

SSL VPN-Plus 탭에서 **IP 풀** 화면을 사용하여 구성하는 정적 IP 풀의 가상 IP 주소가 원격 사용자에게 할당됩니다.

4 NSX Data Center for vSphere Edge 게이트웨이에서 SSL VPN-Plus와 함께 사용할 개인 네트워크 추가

SSL VPN-Plus 탭에서 [개인 네트워크] 화면을 사용하여 개인 네트워크를 구성합니다. 개인 네트워크는 원격 사용자가 VPN 클라이언트와 SSL VPN 터널을 사용하여 연결할 때 VPN 클라이언트가 액세스해야 하는 네트워크입니다. 사용되도록 설정된 개인 네트워크는 VPN 클라이언트의 라우팅 테이블에 설치됩니다.

5 NSX Data Center for vSphere Edge 게이트웨이에서 SSL VPN-Plus에 대한 인증 서비스 구성

SSL VPN-Plus 탭에서 **인증** 화면을 사용하여 Edge 게이트웨이의 SSL VPN 서비스에 대한 로컬 인증 서버를 설정하고 필요한 경우 클라이언트 인증서 인증을 사용하도록 설정합니다. 이 인증 서버는 연결하는 사용자를 인증하는 데 사용됩니다. 이 로컬 인증 서버에서 구성된 모든 사용자가 인증됩니다.

6 로컬 SSL VPN-Plus 인증 서버에 SSL VPN-Plus 사용자 추가

SSL VPN-Plus 탭에서 **사용자** 화면을 사용하여 원격 사용자에 대한 계정을 NSX Data Center for vSphere Edge 게이트웨이의 SSL VPN 서비스에 대한 로컬 인증 서버에 추가합니다.

7 SSL VPN-Plus Client 설치 패키지 추가

SSL VPN-Plus 탭에서 [설치 패키지] 화면을 사용하여 원격 사용자를 위한 SSL VPN-Plus Client의 명명된 설치 패키지를 생성합니다.

8 SSL VPN-Plus Client 구성 편집

SSL VPN-Plus 탭에서 **클라이언트 구성** 화면을 사용하여 원격 사용자가 SSL VPN에 로그인할 때 SSL VPN 클라이언트 터널이 응답하는 방식을 사용자 지정합니다.

9 NSX Data Center for vSphere Edge 게이트웨이에 대한 일반 SSL VPN-Plus 설정 사용자 지정


기본적으로 시스템은 vCloud Director 환경의 Edge 게이트웨이에 대한 일부 SSL VPN-Plus 설정을 설정합니다. 이러한 설정은 vCloud Director 테넌트 포털의 **SSL VPN-Plus** 탭에 있는 **일반 설정** 화면에서 사용자 지정할 수 있습니다.

SSL-VPN Plus 화면으로 이동

[SSL-VPN Plus] 화면으로 이동하여 NSX Data Center for vSphere Edge 게이트웨이에 대한 SSL-VPN Plus 서비스 구성을 시작할 수 있습니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 SSL VPN-Plus 탭을 클릭합니다.

다음에 수행할 작업

일반 화면에서 기본 SSL VPN-Plus 설정을 구성합니다. [NSX Data Center for vSphere Edge 게이트웨이에 대한 일반 SSL VPN-Plus 설정 사용자 지정](#)의 내용을 참조하십시오.

SSL VPN 서버 설정 구성

이러한 서버 설정은 서비스가 수신하는 IP 주소 및 포트, 서비스의 암호 목록 및 서비스 인증서와 같은 SSL VPN 서버를 구성합니다. NSX Data Center for vSphere Edge 게이트웨이에 연결할 때 원격 사용자는 이 서버 설정에서 설정한 것과 동일한 IP 주소와 포트를 지정합니다.

Edge 게이트웨이가 해당 외부 인터페이스에서 여러 개의 오버레이 IP 주소 네트워크로 구성되어 있는 경우 SSL VPN 서버에 대해 선택하는 IP 주소는 Edge 게이트웨이의 기본 외부 인터페이스와 다를 수 있습니다.

SSL VPN 서버 설정을 구성하는 동안 SSL VPN 터널에 사용할 암호화 알고리즘을 선택해야 합니다. 하나 이상의 암호를 선택할 수 있습니다. 선택 항목의 보안 수준에 따라 신중하게 암호를 선택해야 합니다.

기본적으로 시스템에서는 각 Edge 게이트웨이에 대해 SSL VPN 터널의 기본 서버 ID 인증서로 생성되는 자체 서명된 기본 인증서를 사용합니다. 이 기본 인증서 대신 **인증서** 화면에서 시스템에 추가한 디지털 인증서를 사용하도록 선택할 수 있습니다.

사전 요구 사항

- [SSL VPN-Plus 구성](#)에 설명된 사전 요구 사항을 충족했는지 확인합니다.
- 기본 인증서가 아닌 다른 서비스 인증서를 사용하는 경우 필수 인증서를 시스템으로 가져옵니다. [Edge 게이트웨이에 서비스 인증서 추가](#)의 내용을 참조하십시오.
- [SSL-VPN Plus 화면으로 이동](#).

절차

- 1 **SSL VPN-Plus** 화면에서 **서버 설정**을 클릭합니다.
- 2 **사용**을 클릭합니다.
- 3 드롭다운 메뉴에서 IP 주소를 선택합니다.
- 4 (선택 사항) TCP 포트 번호를 입력합니다.

이 TCP 포트 번호는 SSL 클라이언트 설치 패키지에서 사용됩니다. 기본적으로 시스템에서는 포트 443을 사용합니다. 이것은 HTTPS/SSL 트래픽에 대한 기본 포트입니다. 포트 번호는 필수이지만 통신을 위해 원하는 TCP 포트를 설정할 수 있습니다.

참고 SSL VPN 클라이언트를 사용하려면 여기서 구성된 IP 주소와 포트를 원격 사용자의 클라이언트 시스템에서 연결할 수 있어야 합니다. 기본 포트 번호를 변경하는 경우 대상 사용자의 시스템에서 IP 주소 및 포트 조합에 연결할 수 있는지 확인하십시오.

- 5 암호 목록에서 암호화 방법을 선택합니다.

6 서비스 Syslog 로깅 정책을 구성합니다.

로깅은 기본적으로 사용되도록 설정되어 있습니다. 로깅할 메시지의 수준을 변경하거나 로깅을 사용하지 않도록 설정할 수 있습니다.

7 (선택 사항) 시스템에서 생성한 자체 서명된 기본 인증서 대신 서비스 인증서를 사용하려면 **서버 인증서 변경**을 클릭하고 인증서를 선택한 후 **확인**을 클릭합니다.**8** **변경 내용 저장**을 클릭합니다.

다음에 수행할 작업

참고 설정한 Edge 게이트웨이 IP 주소 및 TCP 포트 번호에 원격 사용자가 연결할 수 있어야 합니다. 이 절차에서 구성된 SSL VPN-Plus IP 주소 및 포트에 대한 액세스를 허용하는 Edge 게이트웨이 방화벽 규칙을 추가합니다. [NSX Data Center for vSphere Edge 게이트웨이 방화벽 규칙 추가](#)의 내용을 참조하십시오.

원격 사용자가 SSL VPN-Plus를 사용하여 연결할 때 IP 주소가 원격 사용자에게 할당되도록 IP 풀을 추가합니다. [NSX Data Center for vSphere Edge 게이트웨이에서 SSL VPN-Plus와 함께 사용할 IP 풀 생성](#)의 내용을 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이에서 SSL VPN-Plus와 함께 사용할 IP 풀 생성

SSL VPN-Plus 탭에서 **IP 풀** 화면을 사용하여 구성하는 정적 IP 풀의 가상 IP 주소가 원격 사용자에게 할당됩니다.

이 화면에 추가되는 각 IP 풀은 Edge 게이트웨이에서 구성된 IP 주소 서브넷을 생성합니다. 이러한 IP 풀에서 사용되는 IP 주소 범위는 Edge 게이트웨이에서 구성된 기타 모든 네트워크와 달라야 합니다.

참고 SSL VPN은 IP 풀이 화면 테이블에 나타나는 순서를 기반으로 IP 풀에서 IP 주소를 원격 사용자에게 할당합니다. 화면 테이블에 IP 풀을 추가한 후에는 위쪽 및 아래쪽 화살표를 사용하여 테이블에서 해당 위치를 조정할 수 있습니다.

사전 요구 사항

- [SSL-VPN Plus 화면으로 이동](#).
- [SSL VPN 서버 설정 구성](#).

절차

1 **SSL VPN-Plus** 탭에서 **IP 풀**을 클릭합니다.**2** 만들기() 버튼을 클릭합니다.

3 IP 풀 설정을 구성합니다.

옵션	작업
IP 범위	이 IP 풀의 IP 주소 범위를 입력합니다(예: 127.0.0.1-127.0.0.9). 이러한 IP 주소는 VPN 클라이언트가 인증하고 SSL VPN 터널에 연결할 때 VPN 클라이언트에 할당됩니다.
넷마스크	IP 풀의 넷마스크를 입력합니다(예: 255.255.255.0).
게이트웨이	Edge 게이트웨이가 이 IP 풀의 게이트웨이 주소로 만들고 할당하도록 지정할 IP 주소를 입력합니다. IP 풀이 만들어지면 Edge 게이트웨이 가상 시스템에 가상 어댑터가 만들어지고 이 IP 주소가 해당 가상 인터페이스에서 구성됩니다. 이 IP 주소는 IP 범위 필드의 범위 내에도 있지 않은 서브넷 내의 임의의 IP일 수 있습니다.
설명	(선택 사항) 이 IP 풀에 대한 설명을 입력합니다.
상태	이 IP 풀을 사용하도록 설정할지 선택합니다.
기본 DNS	(선택 사항) 이러한 가상 IP 주소에 대한 이름 확인에 사용될 기본 DNS 서버의 이름을 입력합니다.
보조 DNS	(선택 사항) 사용할 보조 DNS 서버의 이름을 입력합니다.
DNS 접미사	(선택 사항) 도메인 기반 호스트 이름 확인을 위해 클라이언트 시스템이 호스팅되는 도메인의 DNS 접미사를 입력합니다.
WINS 서버	(선택 사항) 조직의 요구에 맞게 WINS 서버 주소를 입력합니다.

4 유지를 클릭합니다.

결과

IP 풀 구성이 화면 테이블에 추가됩니다.

다음에 수행할 작업

SSL VPN-Plus를 사용하여 연결하는 원격 사용자가 액세스할 수 있는 개인 네트워크를 추가합니다. [NSX Data Center for vSphere Edge 게이트웨이](#)에서 **SSL VPN-Plus**와 함께 사용할 개인 네트워크 추가의 내용을 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이에서 **SSL VPN-Plus**와 함께 사용할 개인 네트워크 추가 **SSL VPN-Plus** 탭에서 [개인 네트워크] 화면을 사용하여 개인 네트워크를 구성합니다. 개인 네트워크는 원격 사용자가 VPN 클라이언트와 SSL VPN 터널을 사용하여 연결할 때 VPN 클라이언트가 액세스해야 하는 네트워크입니다. 사용되도록 설정된 개인 네트워크는 VPN 클라이언트의 라우팅 테이블에 설치됩니다.


개인 네트워크는 VPN 클라이언트에 대해 트래픽을 암호화하거나 암호화에서 제외하려는 Edge 게이트웨이로 보호되는 연결 가능한 모든 IP 네트워크의 목록입니다. SSL VPN 터널을 통해 액세스해야 하는 각 개인 네트워크는 개별 항목으로 추가되어야 합니다. 라우트 요약 기술을 사용하여 항목의 수를 제한할 수 있습니다.

- 원격 사용자는 SSL VPN-Plus를 사용하여 IP 풀이 화면 테이블에 나타나는 순서(위에서 아래로)를 기반으로 개인 네트워크에 액세스할 수 있습니다. 화면 테이블에 개인 네트워크를 추가한 후에는 위쪽 및 아래쪽 화살표를 사용하여 테이블에서 해당 위치를 조정할 수 있습니다.
- 개인 네트워크에 대해 TCP 최적화를 사용하도록 선택하면 활성 모드의 FTP와 같은 일부 애플리케이션이 해당 서버넷 내에서 작동하지 않을 수 있습니다. 활성 모드에서 구성된 FTP 서버를 추가하려면 해당 FTP 서버에 대해 또 다른 개인 네트워크를 추가하고 해당 개인 네트워크에 대해 TCP 최적화를 사용하지 않도록 설정해야 합니다. 또한 해당 FTP 서버에 대해 개인 네트워크가 사용되도록 설정되고 TCP 최적화된 개인 네트워크 위의 화면 테이블에 나타나야 합니다.

사전 요구 사항

- [SSL-VPN Plus 화면으로 이동](#).
- [NSX Data Center for vSphere Edge 게이트웨이에서 SSL VPN-Plus와 함께 사용할 IP 풀 생성](#).

절차

- 1 **SSL VPN-Plus** 탭에서 **개인 네트워크**를 클릭합니다.
- 2 **추가**() 버튼을 클릭합니다.
- 3 개인 네트워크 설정을 구성합니다.

옵션	작업
네트워크	CIDR 형식으로 개인 네트워크 IP 주소를 입력합니다(예: 192.169.1.0/24).
설명	(선택 사항) 네트워크에 대한 설명을 입력합니다.
트래픽 보내기	VPN 클라이언트가 개인 네트워크 및 인터넷 트래픽을 보내는 방법을 지정합니다. <ul style="list-style-type: none"> ■ 터널을 통해 VPN 클라이언트가 SSL VPN-Plus 사용 Edge 게이트웨이를 통해 개인 네트워크 및 인터넷 트래픽을 보냅니다. ■ 터널 우회 VPN 클라이언트가 Edge 게이트웨이를 우회하고 트래픽을 개인 서버에 직접 보냅니다.

옵션	작업
TCP 최적화 사용	<p>(선택 사항) 인터넷 속도를 최적화하려면 트래픽을 보내는 방법으로 터널을 통해 선택한 경우에 TCP 최적화 사용도 선택해야 합니다.</p> <p>이 옵션을 선택하면 VPN 터널 내 TCP 패킷의 성능은 향상되지만 UDP 트래픽의 성능은 향상되지 않습니다.</p> <p>기존 전체 액세스 SSL VPN 터널은 인터넷을 통해 암호화를 위한 두 번째 TCP/IP 스택에 TCP/IP 데이터를 전송합니다. 이 일반적인 방법은 두 개의 개별 TCP 스트림에서 애플리케이션 계층 데이터를 캡슐화합니다. 인터넷 환경이 최적화된 조건에서도 일어날 수 있는 패킷 손실이 발생할 경우 TCP-over-TCP 멜트다운이라는 성능 저하 현상이 일어납니다. TCP-over-TCP 멜트다운에서는 두 개의 TCP 장비가 IP 데이터의 동일한 단일 패킷을 수정하기 때문에 네트워크 처리량이 저하되고 연결 시간 초과가 발생합니다. TCP 최적화 사용을 선택하면 이 TCP-over-TCP 문제가 발생할 위험이 사라집니다.</p> <hr/> <p>참고 TCP 최적화를 사용하는 경우</p> <ul style="list-style-type: none"> ■ 인터넷 트래픽을 최적화할 대상 포트 번호를 입력해야 합니다. ■ SSL VPN 서버는 VPN 클라이언트를 대신하여 TCP 연결을 엽니다. SSL VPN 서버가 TCP 연결을 열면 자동으로 생성된 첫 번째 Edge 방화벽 규칙이 적용되어 Edge 게이트웨이에서 열린 모든 연결이 통과됩니다. 최적화되지 않은 트래픽은 일반 Edge 방화벽 규칙에 의해 평가됩니다. 기본 생성된 TCP 규칙은 모든 연결을 허용합니다. <hr/>
포트	<p>터널을 통해를 선택한 경우, 원격 사용자가 내부 서버에 액세스할 수 있도록 열어 둔 포트 번호의 범위를 입력합니다(예: FTP 트래픽의 경우 20–21, HTTP 트래픽의 경우 80–81).</p> <p>사용자에게 무제한 액세스를 제공하려면 이 필드를 비워 둡니다.</p> <hr/>
상태	<p>개인 네트워크를 사용하거나 사용하지 않도록 설정합니다.</p> <hr/>

4 **유지**를 클릭합니다.

5 **변경 내용 저장**을 클릭하여 시스템에 구성을 저장합니다.

다음에 수행할 작업

인증 서버를 추가합니다. [NSX Data Center for vSphere Edge 게이트웨이에서 SSL VPN-Plus에 대한 인증 서비스 구성](#)의 내용을 참조하십시오.

중요 이 화면에 추가한 개인 네트워크에 대한 네트워크 트래픽을 허용하려면 해당하는 방화벽 규칙을 추가합니다. [NSX Data Center for vSphere Edge 게이트웨이 방화벽 규칙 추가](#)의 내용을 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이에서 SSL VPN-Plus에 대한 인증 서비스 구성

SSL VPN-Plus 탭에서 **인증** 화면을 사용하여 Edge 게이트웨이의 SSL VPN 서비스에 대한 로컬 인증 서버를 설정하고 필요한 경우 클라이언트 인증서 인증을 사용하도록 설정합니다. 이 인증 서버는 연결하는 사용자를 인증하는 데 사용됩니다. 이 로컬 인증 서버에서 구성된 모든 사용자가 인증됩니다.

하나의 로컬 SSL VPN-Plus 인증 서버만 Edge 게이트웨이에서 구성할 수 있습니다. **+ 로컬**을 클릭하고 추가 인증 서버를 지정하면 구성을 저장하려고 할 때 오류 메시지가 표시됩니다.

SSL VPN에서 인증할 수 있는 최대 시간은 3분입니다. 이 최대값은 기본적으로 3분인 비인증 시간 초과에 의해 결정된 것으로 구성할 수 없습니다. 따라서 체인 권한 부여에 여러 인증 서버가 있고 사용자 인증에 3분 넘게 걸리는 경우 사용자는 인증되지 않습니다.

사전 요구 사항

- [SSL-VPN Plus](#) 화면으로 이동.
- [NSX Data Center for vSphere Edge](#) 게이트웨이에서 [SSL VPN-Plus](#)와 함께 사용할 개인 네트워크 추가.
- 클라이언트 인증서 인증을 사용하도록 설정하려면 CA 인증서가 Edge 게이트웨이에 추가되었는지 확인합니다. [SSL 인증서 신뢰 확인](#)을 위해 [Edge 게이트웨이에 CA 인증서 추가](#)의 내용을 참조하십시오.

절차

- 1 **SSL VPN-Plus** 탭을 클릭하고 **인증**을 클릭합니다.
- 2 **로컬**을 클릭합니다.

3 인증 서버 설정을 구성합니다.

- a (선택 사항) 암호 정책을 사용하도록 설정하고 구성합니다.

옵션	설명
암호 정책 사용	여기에서 구성하는 암호 정책 설정을 적용합니다.
암호 길이	암호 길이에 허용되는 최소 문자 수와 최대 문자 수를 입력합니다.
최소 영문자 수	(선택 사항) 암호에 필요한 영문자의 최소 수를 입력합니다.
최소 숫자 수	(선택 사항) 암호에 필요한 숫자의 최소 수를 입력합니다.
최소 특수 문자 수	(선택 사항) 앰퍼샌드(&), 해시태그(#), 퍼센트 기호(%) 등 암호에 필요한 특수 문자의 최소 수를 입력합니다.
암호에 사용자 ID가 포함되지 않아야 함	(선택 사항) 암호에 사용자 ID가 포함되지 않아야 한다는 조건을 사용하도록 설정합니다.
암호 만료 기간:	(선택 사항) 사용자가 변경하기 전까지 암호를 사용할 수 있는 최대 일수를 입력합니다.
만료 알림 기간:	(선택 사항) 암호 만료 기간: 값에 도달하기 전 암호가 곧 만료된다는 알림을 사용자에게 전달할 일수를 입력합니다.

- b (선택 사항) 계정 잠금 정책을 사용하도록 설정하고 구성합니다.

옵션	설명
계정 잠금 정책 사용	여기에서 구성하는 계정 잠금 정책 설정을 적용합니다.
재시도 횟수	사용자가 계정에 액세스를 시도할 수 있는 횟수를 입력합니다.
재시도 기간	특정 시간 내에 로그인 시도에 실패할 경우 사용자의 계정이 잠금에 되는 해당 시간(분)을 입력합니다. 예를 들어 재시도 횟수 를 5로 지정하고 재시도 기간 을 1분으로 지정하는 경우 1분 내에 5회 시도하여 로그인하지 못하면 사용자의 계정이 잠깁니다.
잠금 기간	사용자 계정을 잠금 상태로 유지하는 기간을 입력합니다. 이 시간이 경과하면 계정이 자동으로 잠금 해제됩니다.

- c 상태 섹션에서 이 인증 서버를 사용하도록 설정합니다.

- d (선택 사항) 보조 인증을 구성합니다.

옵션	설명
이 서버를 보조 인증에 사용	(선택 사항) 서버를 보조 인증에 사용할지 지정합니다.
인증이 실패하면 세션 종료	(선택 사항) 인증이 실패한 경우 VPN 세션을 종료할지 지정합니다.

- e **유지**를 클릭합니다.

- 4 (선택 사항) 클라이언트 인증서 인증을 사용하도록 설정하려면 **인증서 변경**을 클릭한 후 사용 전환 옵션을 설정하고, 사용할 CA 인증서를 선택한 다음 **확인**을 클릭합니다.

다음에 수행할 작업

로컬 사용자를 로컬 인증 서버에 추가하여 해당 사용자가 SSL VPN-Plus에 연결할 수 있도록 합니다. [로컬 SSL VPN-Plus 인증 서버에 SSL VPN-Plus 사용자 추가](#)의 내용을 참조하십시오.

SSL 클라이언트가 포함된 설치 패키지를 생성하여 원격 사용자가 로컬 시스템에 이를 설치할 수 있도록 합니다. [SSL VPN-Plus Client 설치 패키지 추가](#)의 내용을 참조하십시오.

로컬 SSL VPN-Plus 인증 서버에 SSL VPN-Plus 사용자 추가

SSL VPN-Plus 탭에서 **사용자** 화면을 사용하여 원격 사용자에 대한 계정을 NSX Data Center for vSphere Edge 게이트웨이의 SSL VPN 서비스에 대한 로컬 인증 서버에 추가합니다.

참고 로컬 인증 서버가 아직 구성되지 않은 경우 **사용자** 화면에서 사용자를 추가하면 기본값이 적용된 로컬 인증 서버가 자동으로 추가됩니다. 그런 다음 **인증** 화면에서 편집 버튼을 사용하여 기본값을 보고 편집할 수 있습니다. **인증** 화면 사용에 대한 자세한 내용은 [NSX Data Center for vSphere Edge 게이트웨이에서 SSL VPN-Plus에 대한 인증 서비스 구성](#)의 내용을 참조하십시오.

사전 요구 사항

[SSL-VPN Plus 화면으로 이동](#).

절차

1 **SSL VPN-Plus** 탭에서 **사용자**를 클릭합니다.

2 만들기() 버튼을 클릭합니다.

3 사용자에게 대해 다음 옵션을 구성합니다.

옵션	설명
사용자 ID	사용자 ID를 입력합니다.
암호	사용자 암호를 입력합니다.
암호 다시 입력	암호를 다시 입력합니다.
이름	(선택 사항) 사용자의 이름을 입력합니다.
성	(선택 사항) 사용자의 성을 입력합니다.
설명	(선택 사항) 사용자에게 대한 설명을 입력합니다.
사용	사용자를 사용하도록 설정할지 여부를 지정합니다.
암호가 만료되지 않음	(선택 사항) 이 사용자에게 대해 항상 동일한 암호를 유지할지 지정합니다.
암호 변경 허용	(선택 사항) 사용자가 암호를 변경할 수 있도록 할지 지정합니다.
다음 로그인 시 암호 변경	(선택 사항) 이 사용자가 다음번 로그인 시 때 암호를 변경하도록 할지 지정합니다.

4 **유지**를 클릭합니다.

5 다른 사용자를 추가하려면 단계를 반복합니다.

다음에 수행할 작업

로컬 사용자를 로컬 인증 서버에 추가하여 해당 사용자가 **SSL VPN-Plus**에 연결할 수 있도록 합니다. [로컬 SSL VPN-Plus 인증 서버에 SSL VPN-Plus 사용자 추가](#)의 내용을 참조하십시오.

SSL 클라이언트가 포함된 설치 패키지를 생성하여 원격 사용자가 로컬 시스템에 이를 설치할 수 있도록 합니다. [SSL VPN-Plus Client 설치 패키지 추가](#)의 내용을 참조하십시오.

SSL VPN-Plus Client 설치 패키지 추가

SSL VPN-Plus 탭에서 [설치 패키지] 화면을 사용하여 원격 사용자를 위한 **SSL VPN-Plus Client**의 명명된 설치 패키지를 생성합니다.


SSL VPN-Plus Client 설치 패키지를 **NSX Data Center for vSphere Edge** 게이트웨이에 추가할 수 있습니다. 새로운 사용자가 처음 **VPN** 연결을 사용하기 위해 로그인하면 이 패키지를 다운로드하여 설치하라는 메시지가 표시됩니다. 추가된 경우 **Edge** 게이트웨이 공용 인터페이스의 **FQDN**에서 이러한 클라이언트 설치 패키지를 다운로드할 수 있습니다.


Windows, Linux 및 Mac 운영 체제에서 실행되는 설치 패키지를 생성할 수 있습니다. **SSL VPN** 클라이언트별로 서로 다른 설치 매개 변수가 필요한 경우 각 구성에 대한 설치 패키지를 생성합니다.

사전 요구 사항

[SSL-VPN Plus 화면으로 이동](#)

절차

- 1 테넌트 포털의 **SSL VPN-Plus** 탭에서 **설치 패키지**를 클릭합니다.
- 2 **추가**() 버튼을 클릭합니다.
- 3 설치 패키지 설정을 구성합니다.

옵션	설명
프로파일 이름	이 설치 패키지의 프로파일 이름을 입력합니다. 이 이름은 원격 사용자에게 표시되어 Edge 게이트웨이에 대한 이 SSL VPN 연결을 식별합니다.
게이트웨이	Edge 게이트웨이 공용 인터페이스의 IP 주소 또는 FQDN 을 입력합니다. 입력하는 IP 주소 또는 FQDN 은 SSL VPN 클라이언트에 바인딩됩니다. 클라이언트가 원격 사용자의 로컬 시스템에 설치되어 있는 경우 이 IP 주소 또는 FQDN 이 해당 SSL VPN 클라이언트에 표시됩니다. Edge 게이트웨이 업링크 인터페이스를 이 SSL VPN 클라이언트에 추가로 바인딩하려면 추가 () 버튼을 클릭하여 행을 추가하고 해당 인터페이스 IP 주소 또는 FQDN 과 포트를 입력합니다.
포트	(선택 사항) 표시된 기본 포트 값을 수정하려면 값을 두 번 클릭하고 새 값을 입력합니다.

옵션	설명
Windows	설치 패키지를 만들 운영 체제를 선택합니다.
Linux	
Mac	
설명	(선택 사항) 사용자에게 대한 설명을 입력합니다.
사용	이 패키지를 사용하도록 설정할지 지정합니다.

4 Windows용 설치 매개 변수를 선택합니다.

옵션	설명
로그온 시 클라이언트 시작	원격 사용자가 로컬 시스템에 로그인할 때 SSL VPN 클라이언트를 시작합니다.
암호 기억 허용	클라이언트가 사용자 암호를 기억하도록 설정합니다.
자동 모드 설치 사용	원격 사용자에게 설치 명령을 숨깁니다.
SSL 클라이언트 네트워크 어댑터 숨기기	SSL VPN 클라이언트 설치 패키지와 함께 원격 사용자의 컴퓨터에 설치된 VMware SSL VPN-Plus 어댑터를 숨깁니다.
클라이언트 시스템 트레이 아이콘 숨기기	VPN 연결이 활성 상태인지 여부를 표시하는 SSL VPN 트레이 아이콘을 숨깁니다.
바탕 화면 아이콘 만들기	SSL 클라이언트를 호출하는 아이콘을 사용자의 바탕 화면에 만듭니다.
자동 모드 작업 사용	설치가 완료되었음을 나타내는 창을 숨깁니다.
서버 보안 인증서 검증	SSL VPN 클라이언트가 보안 연결을 설정하기 전에 SSL VPN 서버 인증서를 검증합니다.

5 유지를 클릭합니다.

다음에 수행할 작업

클라이언트 구성을 편집합니다. [SSL VPN-Plus Client 구성 편집](#)의 내용을 참조하십시오.

SSL VPN-Plus Client 구성 편집

SSL VPN-Plus 탭에서 **클라이언트 구성** 화면을 사용하여 원격 사용자가 SSL VPN에 로그인할 때 SSL VPN 클라이언트 터널이 응답하는 방식을 사용자 지정합니다.

사전 요구 사항

[SSL-VPN Plus 화면으로 이동](#)

절차

1 SSL VPN-Plus 탭에서 **클라이언트 구성**을 클릭합니다.

2 터널링 모드를 선택합니다.

- 분할 터널 모드에서는 VPN 트래픽만 Edge 게이트웨이를 통과합니다.
- 전체 터널 모드에서는 Edge 게이트웨이가 원격 사용자의 기본 게이트웨이가 되며 VPN, 로컬, 인터넷 등의 모든 트래픽이 Edge 게이트웨이를 통과합니다.

- 3 전체 터널 모드를 선택하는 경우 원격 사용자의 클라이언트가 사용하는 기본 게이트웨이의 IP 주소를 입력하고 필요하면 로컬 서브넷 트래픽이 VPN 터널을 통과하지 못하도록 제외할지 선택합니다.
- 4 (선택 사항) 자동 다시 연결을 사용하지 않도록 설정합니다.

자동 다시 연결 사용은 기본적으로 사용되도록 설정되어 있습니다. 자동 다시 연결을 사용하도록 설정하면 SSL VPN 클라이언트는 사용자 연결이 끊어졌을 때 사용자를 자동으로 다시 연결합니다.

- 5 (선택 사항) 필요한 경우 클라이언트 업그레이드를 사용할 수 있을 때 클라이언트가 이를 원격 사용자에게 알리는 기능을 사용하도록 설정합니다.

이 옵션은 기본적으로 사용되지 않도록 설정되어 있습니다. 이 옵션을 사용하도록 설정한 경우 원격 사용자는 업그레이드 설치를 선택할 수 있습니다.

6 변경 내용 저장을 클릭합니다.

NSX Data Center for vSphere Edge 게이트웨이에 대한 일반 SSL VPN-Plus 설정 사용자 지정

기본적으로 시스템은 vCloud Director 환경의 Edge 게이트웨이에 대한 일부 SSL VPN-Plus 설정을 설정합니다. 이러한 설정은 vCloud Director 테넌트 포털의 **SSL VPN-Plus** 탭에 있는 **일반 설정** 화면에서 사용자 지정할 수 있습니다.

사전 요구 사항

[SSL-VPN Plus 화면으로 이동](#).

절차

- 1 **SSL VPN-Plus** 탭에서 **일반 설정**을 클릭합니다.
- 2 조직의 필요에 맞게 일반 설정을 편집합니다.

옵션	설명
동일한 사용자 이름을 사용한 다중 로그인 방지	설정하면 원격 사용자가 동일한 사용자 이름으로 활성 로그인 세션을 하나만 가질 수 있도록 제한됩니다.
압축	설정하면 TCP 기반의 지능형 데이터 압축이 사용되도록 설정되고 데이터 전송 속도가 향상됩니다.
로깅 사용	설정하면 SSL VPN 게이트웨이를 통과하는 트래픽의 로그가 유지됩니다. 로깅은 기본적으로 사용되도록 설정되어 있습니다.
가상 키보드 강제 적용	설정하면 원격 사용자가 로그인 정보를 입력할 때 가상(화면) 키보드만 사용해야 합니다.
가상 키보드의 키 임의 배치	설정하면 가상 키보드에서 임의의 지정된 키 레이아웃을 사용합니다.
세션 유희 시간 제한	세션 유희 시간 초과를 분 단위로 입력합니다. 지정된 기간 동안 사용자 세션에 활동이 없으면 사용자 세션 연결이 끊깁니다. 시스템 기본값은 10분입니다.
사용자 알림	원격 사용자가 로그인할 때 표시할 메시지를 입력합니다.
공용 URL 액세스 사용	설정하면 원격 사용자 액세스가 명시적으로 구성되지 않은 사이트에 원격 사용자가 액세스할 수 있습니다.

옵션	설명
강제 시간 초과 사용	설정하면 강제 시간 초과 필드에 지정하는 시간이 경과했을 때 원격 사용자 연결이 끊깁니다.
강제 시간 초과	시간 초과 기간(분)을 입력합니다. 이 필드는 강제 시간 초과 사용 전환 옵션을 설정했을 때 표시됩니다.

3 변경 내용 저장을 클릭합니다.

IPsec VPN 구성

vCloud Director 환경에서 NSX Data Center for vSphere Edge 게이트웨이는 조직 가상 데이터 센터 네트워크 간 VPN 터널 또는 조직 가상 데이터 센터 네트워크와 외부 IP 주소 간 VPN 터널의 보안을 위한 사이트 간 IPsec(인터넷 프로토콜 보안)을 지원합니다. Edge 게이트웨이에서 IPsec VPN 서비스를 구성할 수 있습니다.

원격 네트워크에서 조직 가상 데이터 센터로의 IPsec VPN 연결을 설정하는 것이 가장 일반적인 시나리오입니다. NSX 소프트웨어는 인증서 인증, 미리 공유한 키 모드, 자체 및 원격 VPN 라우터 간의 IP 유니캐스트 트래픽 지원을 비롯한 Edge 게이트웨이 IPsec VPN 기능을 제공합니다. 또한 IPsec 터널을 통해 Edge 게이트웨이 뒤의 내부 네트워크에 연결하도록 다수의 서브넷을 구성할 수 있습니다. IPsec 터널을 통해 내부 네트워크에 연결하도록 여러 서브넷을 구성하는 경우 이러한 서브넷과 Edge 게이트웨이 뒤 내부 네트워크의 주소 범위가 겹치지 않아야 합니다.

참고 IPsec 터널에서 로컬 및 원격 피어의 IP 주소가 겹치면 로컬로 연결된 경로 및 자동 배관된 경로의 존재 유무에 따라 터널을 통과하여 전달되는 트래픽의 일관성이 유지되지 않을 수 있습니다.

다음 IPsec VPN 알고리즘이 지원됩니다.

- AES(AES128-CBC)
- AES256(AES256-CBC)
- Triple-DES(3DES192-CBC)
- AES-GCM(AES128-GCM)
- DH-2(Diffie-Hellman 그룹 2)
- DH-5(Diffie-Hellman 그룹 5)
- DH-14(Diffie-Hellman 그룹 14)

참고 동적 라우팅 프로토콜은 IPsec VPN에서 지원되지 않습니다. 조직 가상 데이터 센터의 Edge 게이트웨이와 물리적 사이트의 실제 게이트웨이 VPN 사이에 IPsec VPN 터널을 구성하면 해당 연결에 대한 동적 라우팅을 구성할 수 없습니다. 해당 원격 사이트의 IP 주소는 Edge 게이트웨이 업링크의 동적 라우팅을 통해 알 수 없습니다.

"NSX 관리 가이드"의 "IPSec VPN 개요" 항목에 설명된 대로 Edge 게이트웨이에서 지원되는 최대 터널 수는 구성된 크기(소형, 대형, 초대형, 4배 대형)에 따라 결정됩니다.

Edge 게이트웨이 구성의 크기를 보려면 Edge 게이트웨이로 이동하여 Edge 게이트웨이 이름을 클릭합니다.

Edge 게이트웨이에 IPsec VPN을 구성하는 프로세스는 여러 단계를 수행하여 완료됩니다.

참고 터널 끝점 간에 방화벽이 있는 경우 IPsec VPN 서비스를 구성한 후 다음 IP 프로토콜 및 UDP 포트를 허용하도록 방화벽 규칙을 업데이트해야 합니다.

- IP 프로토콜 ID 50(ESP)
- IP 프로토콜 ID 51(AH)
- UDP 포트 500(IKE)
- UDP 포트 4500

절차

1 [IPsec VPN] 화면으로 이동

IPsec VPN 화면에서 NSX Data Center for vSphere Edge 게이트웨이에 대한 IPsec VPN 서비스 구성을 시작할 수 있습니다.

2 NSX Data Center for vSphere Edge 게이트웨이에 대한 IPsec VPN 사이트 연결 구성

vCloud Director 테넌트 포털의 **IPsec VPN 사이트** 화면에서 조직 가상 데이터 센터와 Edge 게이트웨이 IPsec VPN 기능을 사용하는 다른 사이트 간에 IPsec VPN 연결을 만드는 데 필요한 설정을 구성합니다.

3 NSX Data Center for vSphere Edge 게이트웨이에서 IPsec VPN 서비스 사용

하나 이상의 IPsec VPN 연결이 구성된 경우 Edge 게이트웨이에서 IPsec VPN 서비스를 사용하도록 설정할 수 있습니다.

4 글로벌 IPsec VPN 설정 지정


글로벌 구성 화면을 사용하여 Edge 게이트웨이 수준에서 IPsec VPN 인증 설정을 구성합니다. 이 화면에서 미리 공유한 글로벌 키를 설정하고 인증서 인증을 사용하도록 설정할 수 있습니다.

[IPsec VPN] 화면으로 이동

IPsec VPN 화면에서 NSX Data Center for vSphere Edge 게이트웨이에 대한 IPsec VPN 서비스 구성을 시작할 수 있습니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 VPN > IPsec VPN으로 이동합니다.

다음에 수행할 작업

IPsec VPN 사이트 화면을 사용하여 IPsec VPN 연결을 구성합니다. Edge 게이트웨이에서 IPsec VPN 서비스를 사용하도록 설정하려면 하나 이상의 연결이 구성되어 있어야 합니다. [NSX Data Center for vSphere Edge 게이트웨이에 대한 IPsec VPN 사이트 연결 구성](#)의 내용을 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이에 대한 IPsec VPN 사이트 연결 구성

vCloud Director 테넌트 포털의 **IPsec VPN 사이트** 화면에서 조직 가상 데이터 센터와 Edge 게이트웨이 IPsec VPN 기능을 사용하는 다른 사이트 간에 IPsec VPN 연결을 만드는 데 필요한 설정을 구성합니다.

사이트 간 IPsec VPN 연결을 구성하는 경우 현재 위치의 관점에서 연결을 구성합니다. 연결을 설정하려면 vCloud Director 환경의 컨텍스트에서 개념을 이해해야 VPN 연결을 올바르게 구성할 수 있습니다.

- 로컬 및 피어 서브넷은 VPN이 연결하는 네트워크를 지정합니다. IPsec VPN 사이트에 대한 구성에서 이러한 서브넷을 지정하는 경우에는 특정 IP 주소가 아닌 네트워크 범위를 입력합니다.
192.168.99.0/24 같은 CIDR 형식을 사용합니다.
- 피어 ID는 VPN 연결을 종료하는 원격 디바이스를 고유하게 식별하는 식별자이며 일반적으로 해당 디바이스의 공개 IP 주소입니다. 인증서 인증을 사용하는 피어의 경우 이 ID는 피어 인증서에 설정된 고유 이름이어야 합니다. PSK 피어의 경우 이 ID는 임의의 문자열일 수 있습니다. NSX 모범 사례는 원격 디바이스의 공개 IP 주소 또는 FQDN을 피어 ID로 사용하는 것입니다. 피어 IP 주소가 다른 조직 가상 데이터 센터 네트워크의 주소인 경우 피어의 기본 IP 주소를 입력합니다. 피어에 NAT가 구성된 경우 피어의 개인 IP 주소를 입력합니다.
- 피어 끝점은 연결하는 원격 디바이스의 공개 IP 주소를 지정합니다. 인터넷에서 피어의 게이트웨이에 직접 액세스할 수 없고 다른 디바이스를 통해 연결되는 경우 피어 끝점이 피어 ID와 다른 주소일 수 있습니다. 피어에 NAT가 구성된 경우 디바이스가 NAT에 사용하는 공개 IP 주소를 입력합니다.
- 로컬 ID는 조직 가상 데이터 센터의 Edge 게이트웨이에 대한 공개 IP 주소를 지정합니다. Edge 게이트웨이 방화벽과 함께 IP 주소 또는 호스트 이름을 입력할 수 있습니다.
- 로컬 끝점은 Edge 게이트웨이가 전송 시 사용하는 조직 가상 데이터 센터의 네트워크를 지정합니다. 일반적으로 Edge 게이트웨이의 외부 네트워크는 로컬 끝점입니다.

사전 요구 사항

- [\[IPsec VPN\] 화면으로 이동](#).
- [IPsec VPN 구성](#).
- 글로벌 인증서를 인증 방법으로 사용하려는 경우 **글로벌 구성** 화면에서 인증서 인증이 사용되도록 설정되었는지 확인합니다. [글로벌 IPsec VPN 설정 지정](#)의 내용을 참조하십시오.

절차

1 **IPsec VPN** 탭에서 **IPsec VPN 사이트**를 클릭합니다.

2 **추가**() 버튼을 클릭합니다.

3 IPsec VPN 연결 설정을 구성합니다.

옵션	작업
사용	두 개의 VPN 끝점 사이에 이 연결을 사용합니다.
PFS(Perfect Forward Secrecy) 사용	<p>사용자가 시작하는 모든 IPsec VPN 세션에 대해 시스템이 고유 공용 키를 생성하도록 하려면 이 옵션을 사용합니다.</p> <p>PFS를 사용하면 시스템이 Edge 게이트웨이 개인 키와 각 세션 키 사이의 링크를 만들지 않습니다.</p> <p>세션 키가 손상될 경우 해당 키로 보호되는 특정 세션에서 교환되는 데이터를 제외한 다른 데이터는 영향을 받지 않습니다. 서버의 개인 키가 손상되면 아카이브된 세션 또는 이후 세션을 암호 해독하는 데 사용할 수 없습니다.</p> <p>PFS를 사용하는 경우 이 Edge 게이트웨이에 대한 IPsec VPN 연결에 약간의 처리 오버헤드가 발생합니다.</p> <p>중요 고유 세션 키를 사용하여 추가 세션 키를 파생할 수 없습니다. 또한 PFS가 작동하려면 IPsec VPN 터널의 양쪽에서 PFS를 지원해야 합니다.</p>
이름	(선택 사항) 연결의 이름을 입력합니다.
로컬 ID	<p>Edge 게이트웨이 인스턴스의 외부 IP 주소(Edge 게이트웨이의 공개 IP 주소)를 입력합니다.</p> <p>이 IP 주소는 원격 사이트의 IPsec VPN 구성에서 피어 ID로 사용됩니다.</p>
로컬 끝점	<p>이 연결의 로컬 끝점인 네트워크를 입력합니다.</p> <p>로컬 끝점은 Edge 게이트웨이가 전송 시 사용하는 조직 가상 데이터 센터의 네트워크를 지정합니다. 일반적으로 외부 네트워크가 로컬 끝점입니다.</p> <p>미리 공유한 키를 사용하는 IP-to-IP 터널을 추가하는 경우에는 로컬 ID와 로컬 끝점 IP가 같을 수 있습니다.</p>
로컬 서브넷	<p>사이트 간에 공유하는 네트워크를 입력하고, 서브넷을 여러 개 입력하려면 쉼표를 구분 기호로 사용합니다.</p> <p>IP 주소를 CIDR 형식으로 입력하여 네트워크 범위(특정 IP 주소 아님)를 입력합니다 (예: 192.168.99.0/24).</p>
피어 ID	<p>피어 사이트를 고유하게 식별할 피어 ID를 입력합니다.</p> <p>피어 ID는 VPN 연결을 종료하는 원격 디바이스를 고유하게 식별하는 식별자이며 일반적으로 해당 디바이스의 공개 IP 주소입니다.</p> <p>인증서 인증을 사용하는 피어의 경우 ID는 피어 인증서의 고유 이름이어야 합니다. PSK 피어의 경우 이 ID는 임의의 문자열일 수 있습니다. NSX 모범 사례는 원격 디바이스의 IP 주소 또는 FQDN을 피어 ID로 사용하는 것입니다.</p> <p>피어 IP 주소가 다른 조직 가상 데이터 센터 네트워크의 주소인 경우 피어의 기본 IP 주소를 입력합니다. 피어에 NAT가 구성된 경우 피어의 개인 IP 주소를 입력합니다.</p>
피어 끝점	<p>피어 사이트의 IP 주소 또는 FQDN을 입력합니다. 이는 연결하는 원격 디바이스의 공용 주소입니다.</p> <p>참고 피어에 NAT가 구성된 경우 디바이스가 NAT에 사용하는 공개 IP 주소를 입력합니다.</p>
피어 서브넷	<p>VPN이 연결하는 원격 네트워크를 입력하고, 서브넷을 여러 개 입력하려면 쉼표를 구분 기호로 사용합니다.</p> <p>IP 주소를 CIDR 형식으로 입력하여 네트워크 범위(특정 IP 주소 아님)를 입력합니다 (예: 192.168.99.0/24).</p>

옵션	작업
암호화 알고리즘	<p>드롭다운 메뉴에서 암호화 알고리즘 유형을 선택합니다.</p> <p>참고 원격 사이트 VPN 디바이스에 구성된 암호화 유형과 일치하는 암호화 유형을 선택해야 합니다.</p>
인증	<p>인증을 선택합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> ■ PSK <p>PSK(미리 공유한 키)는 Edge 게이트웨이와 피어 사이트 간에 공유되는 비밀 키를 인증에 사용하도록 지정합니다.</p> ■ 인증서 <p>인증서 인증은 글로벌 수준에서 정의된 인증서를 인증에 사용하도록 지정합니다. 이 옵션은 IPsec VPN 탭의 글로벌 구성 화면에서 글로벌 인증서를 구성한 경우에만 사용할 수 있습니다.</p>
공유 키 변경	<p>(선택 사항) 기존 연결의 설정을 업데이트하는 경우 이 옵션을 사용하도록 설정하여 미리 공유한 키 필드를 사용할 수 있도록 한 후 공유 키를 업데이트할 수 있습니다.</p>
미리 공유한 키	<p>인증 유형으로 PSK를 선택한 경우, 최대 길이가 128바이트인 영숫자 암호 문자열을 입력합니다.</p> <p>참고 공유 키는 원격 사이트 VPN 디바이스에 구성된 키와 일치해야 합니다. 모범 사례는 익명 사이트가 VPN 서비스에 연결할 때 공유 키를 구성하는 것입니다.</p>
공유 키 표시	<p>(선택 사항) 공유 키를 화면에 표시하려면 이 옵션을 사용하도록 설정합니다.</p>
Diffie-Hellman 그룹	<p>피어 사이트와 이 Edge 게이트웨이가 비보안 통신 채널을 통해 공유 암호를 설정하는 것을 허용하는 암호화 체계를 선택합니다.</p> <p>참고 Diffie-Hellman 그룹은 원격 사이트 VPN 디바이스에 구성된 Diffie-Hellman 그룹과 일치해야 합니다.</p>
확장	<p>(선택 사항) 다음 옵션 중 하나를 입력합니다.</p> <ul style="list-style-type: none"> ■ <code>securelocaltrafficbyip=IPAddress</code> - Edge 게이트웨이 로컬 트래픽을 IPsec VPN 터널을 통해 리디렉션합니다. <p>기본값입니다.</p> <ul style="list-style-type: none"> ■ <code>passthroughSubnets=PeerSubnetIPAddress</code> - 서브넷을 겹칠 수 있습니다.

4 **유지**를 클릭합니다.

5 **변경 내용 저장**을 클릭합니다.

저장 작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

다음에 수행할 작업

원격 사이트에 대한 연결을 구성합니다. 연결의 양쪽(조직 가상 데이터 센터와 피어 사이트)에서 IPsec VPN 연결을 구성해야 합니다.

이 Edge 게이트웨이에서 IPsec VPN 서비스를 사용하도록 설정합니다. IPsec VPN 연결을 하나 이상 구성한 경우 서비스를 사용하도록 설정할 수 있습니다. [NSX Data Center for vSphere Edge 게이트웨이에서 IPsec VPN 서비스 사용](#)의 내용을 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이에서 IPsec VPN 서비스 사용

하나 이상의 IPsec VPN 연결이 구성된 경우 Edge 게이트웨이에서 IPsec VPN 서비스를 사용하도록 설정할 수 있습니다.

사전 요구 사항

- [\[IPsec VPN\] 화면으로 이동.](#)
- 하나 이상의 IPsec VPN 연결이 이 Edge 게이트웨이에 대해 구성되었는지 확인합니다. [NSX Data Center for vSphere Edge 게이트웨이에 대한 IPsec VPN 사이트 연결 구성](#)에 설명된 단계를 참조하십시오.

절차

- 1 **IPsec VPN** 탭에서 **활성화 상태**를 클릭합니다.
- 2 IPsec VPN 서비스를 사용하도록 설정하려면 **IPsec VPN 서비스 상태**를 클릭합니다.
- 3 **변경 내용 저장**을 클릭합니다.

결과

Edge 게이트웨이의 IPsec VPN 서비스가 활성화됩니다.

글로벌 IPsec VPN 설정 지정


글로벌 구성 화면을 사용하여 Edge 게이트웨이 수준에서 IPsec VPN 인증 설정을 구성합니다. 이 화면에서 미리 공유한 글로벌 키를 설정하고 인증서 인증을 사용하도록 설정할 수 있습니다.

미리 공유한 글로벌 키는 피어 끝점이 **any**로 설정된 사이트에 사용됩니다.

사전 요구 사항

- 인증서 인증을 사용하도록 설정하려면 **인증서** 화면에 하나 이상의 서비스 인증서와 해당하는 CA 서명된 인증서가 있는지 확인합니다. 자체 서명된 인증서는 IPsec VPN에 사용할 수 없습니다. [Edge 게이트웨이에 서비스 인증서 추가](#)의 내용을 참조하십시오.
- [\[IPsec VPN\] 화면으로 이동.](#)

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 **IPsec VPN** 탭에서 **글로벌 구성**을 클릭합니다.

3 (선택 사항) 미리 공유한 글로벌 키를 설정합니다.

- a **공유 키 변경** 옵션을 사용하도록 설정합니다.
- b 미리 공유한 키를 입력합니다.

글로벌 PSK(미리 공유한 키)는 피어 끝점이 **any**로 설정된 모든 사이트에서 공유됩니다. 글로벌 PSK가 이미 설정된 경우 PSK를 빈 값으로 변경하고 저장해도 기존 설정에 영향을 주지 않습니다.

- c (선택 사항) 필요한 경우 **공유 키 표시**를 사용하도록 설정하여 미리 공유한 키를 표시합니다.
- d **변경 내용 저장**을 클릭합니다.

4 인증서 인증을 구성합니다.

- a **인증서 인증 사용**을 켭니다.
- b 해당하는 서비스 인증서, CA 인증서 및 CRL을 선택합니다.
- c **변경 내용 저장**을 클릭합니다.

다음에 수행할 작업

필요한 경우 Edge 게이트웨이의 IPsec VPN 서비스에 대한 로깅을 사용하도록 설정할 수 있습니다. [Edge 게이트웨이에 대한 통계 및 로그](#)의 내용을 참조하십시오.

L2 VPN 구성

vCloud Director 환경에서 NSX Data Center for vSphere Edge 게이트웨이는 L2 VPN을 지원합니다. L2 VPN을 사용하면 가상 시스템이 지리적 경계를 넘어 동일한 IP 주소를 유지하면서 네트워크 연결을 유지하도록 하여 조직 가상 데이터 센터를 확장할 수 있습니다. Edge 게이트웨이에서 L2 VPN 서비스를 구성할 수 있습니다.

NSX Data Center for vSphere는 Edge 게이트웨이의 L2 VPN 기능을 제공합니다. L2 VPN을 사용하면 두 사이트 간에 터널을 구성할 수 있습니다. 가상 시스템은 이러한 사이트를 이동하는 동안에도 동일한 서브넷에 유지되므로 L2 VPN을 사용하여 네트워크를 스트레치하여 조직 가상 데이터 센터를 확장할 수 있습니다. 한 사이트의 Edge 게이트웨이에서 다른 사이트의 가상 시스템에 모든 서비스를 제공할 수 있습니다.

L2 VPN 터널을 만들려면 L2 VPN 서버와 L2 VPN 클라이언트를 구성합니다. "NSX 관리 가이드"에 설명된 대로 L2 VPN 서버는 대상 Edge 게이트웨이이며 L2 VPN 클라이언트는 소스 Edge 게이트웨이입니다. 각 Edge 게이트웨이에 L2 VPN 설정을 구성한 후 서버와 클라이언트에서 L2 VPN 서비스를 사용하도록 설정해야 합니다.

참고 하위 인터페이스로 만들어지고 라우팅된 조직 가상 데이터 센터 네트워크가 Edge 게이트웨이에 있어야 합니다.

절차

1 [L2 VPN] 화면으로 이동

NSX Data Center for vSphere Edge 게이트웨이에 대한 L2 VPN 서비스 구성을 시작하려면 **L2 VPN** 화면으로 이동해야 합니다.

2 NSX Data Center for vSphere Edge 게이트웨이를 L2 VPN 서버로 구성

L2 VPN 서버는 L2 VPN 클라이언트가 연결할 대상 NSX Edge입니다.

3 NSX Data Center for vSphere Edge 게이트웨이를 L2 VPN 클라이언트로 구성

L2 VPN 클라이언트는 대상 NSX Edge인 L2 VPN 서버와 통신을 시작하는 소스 NSX Edge입니다.

4 NSX Data Center for vSphere Edge 게이트웨이에서 L2 VPN 서비스 사용


필수 L2 VPN 설정이 구성된 경우 Edge 게이트웨이에서 L2 VPN 서비스를 사용하도록 설정할 수 있습니다.

[L2 VPN] 화면으로 이동

NSX Data Center for vSphere Edge 게이트웨이에 대한 L2 VPN 서비스 구성을 시작하려면 **L2 VPN** 화면으로 이동해야 합니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 VPN > L2 VPN으로 이동합니다.

다음에 수행할 작업

L2 VPN 서버를 구성합니다. **NSX Data Center for vSphere Edge 게이트웨이를 L2 VPN 서버로 구성**의 내용을 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이를 L2 VPN 서버로 구성

L2 VPN 서버는 L2 VPN 클라이언트가 연결할 대상 NSX Edge입니다.

"NSX 관리 가이드"에 설명된 대로 이 L2 VPN 서버에 여러 개의 피어 사이트를 연결할 수 있습니다.

참고 사이트 구성 설정을 변경하면 Edge 게이트웨이가 기존의 모든 연결을 끊고 다시 연결합니다.

사전 요구 사항

- Edge 게이트웨이에 Edge 게이트웨이의 하위 인터페이스로 구성되고 라우팅된 조직 가상 데이터 센터 네트워크가 있는지 확인합니다.
- [\[L2 VPN\] 화면으로 이동](#).
- 서비스 인증서를 L2 VPN 연결에 바인딩하려면 Edge 게이트웨이에 서버 인증서가 업로드되어 있는지 확인합니다. [Edge 게이트웨이에 서비스 인증서 추가](#)의 내용을 참조하십시오.
- L2 VPN 서비스를 사용하도록 설정하려면 서버의 수신기 IP, 수신기 포트, 암호화 알고리즘 및 하나 이상의 피어 사이트가 구성되어 있어야 합니다.

절차

- 1 **L2 VPN** 탭에서 L2 VPN 모드에 대해 **서버**를 선택합니다.
- 2 **서버 글로벌** 탭에서 L2 VPN 서버의 글로벌 구성 세부 정보를 구성합니다.

옵션	작업
수신기 IP	Edge 게이트웨이 외부 인터페이스의 기본 또는 보조 IP 주소를 선택합니다.
수신기 포트	조직의 필요에 맞게 표시된 값을 편집합니다. L2 VPN 서비스의 기본 포트는 443입니다.
암호화 알고리즘	서버와 클라이언트 간 통신에 사용할 암호화 알고리즘을 선택합니다.
서비스 인증서 세부 정보	서버 인증서 변경 을 클릭하여 L2 VPN 서버에 바인딩할 인증서를 선택합니다. 서버 인증서 변경 창에서 서버 인증서 확인 을 설정하고 목록에서 서버 인증서를 선택한 후 확인 을 클릭합니다.

- 3 피어 사이트를 구성하려면 **서버 사이트** 탭을 클릭합니다.

- 4 **추가**() 버튼을 클릭합니다.

- 5 L2 VPN 피어 사이트에 대한 설정을 구성합니다.

옵션	작업
사용	이 피어 사이트를 사용하도록 설정합니다.
이름	피어 사이트의 고유한 이름을 입력합니다.
설명	(선택 사항) 설명을 입력합니다.
사용자 ID	피어 사이트를 인증할 때 사용할 사용자 이름과 암호를 입력합니다.
암호	피어 사이트의 사용자 자격 증명은 클라이언트 측 자격 증명과 동일해야 합니다.
암호 확인	

옵션	작업
스트레치된 인터페이스	클라이언트와 함께 스트레치될 하위 인터페이스를 하나 이상 선택합니다. Edge 게이트웨이의 하위 인터페이스로 구성된 조직 가상 데이터 센터 네트워크를 하위 인터페이스로 선택할 수 있습니다.
송신 최적화 게이트웨이 주소	(선택 사항) 가상 시스템의 기본 게이트웨이가 두 사이트에서 동일한 경우 L2 VPN 터널을 통해 로컬로 라우팅하거나 차단할 트래픽의 하위 인터페이스에 대한 게이트웨이 IP 주소를 입력합니다.

6 **유지**를 클릭합니다.

7 **변경 내용 저장**을 클릭합니다.

저장 작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

다음에 수행할 작업

이 Edge 게이트웨이에서 L2 VPN 서비스를 사용하도록 설정합니다. [NSX Data Center for vSphere Edge 게이트웨이에서 L2 VPN 서비스 사용](#)의 내용을 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이를 L2 VPN 클라이언트로 구성

L2 VPN 클라이언트는 대상 NSX Edge인 L2 VPN 서버와 통신을 시작하는 소스 NSX Edge입니다.

사전 요구 사항

- [\[L2 VPN\] 화면으로 이동](#).
- 이 L2 VPN 클라이언트가 서버 인증서를 사용하는 L2 VPN 서버에 연결 중인 경우 이 L2 VPN 클라이언트에 대한 서버 인증서 검증을 사용하도록 설정하기 위해 해당 CA 인증서가 Edge 게이트웨이에 업로드되었는지 확인합니다. [SSL 인증서 신뢰 확인을 위해 Edge 게이트웨이에 CA 인증서 추가](#)의 내용을 참조하십시오.

절차

1 **L2 VPN** 탭에서 L2 VPN 모드에 대해 **클라이언트**를 선택합니다.

2 **클라이언트 글로벌** 탭에서 L2 VPN 클라이언트의 글로벌 구성 세부 정보를 구성합니다.

옵션	설명
서버 주소	이 클라이언트가 연결될 L2 VPN 서버의 IP 주소를 입력합니다.
서버 포트	클라이언트가 연결해야 하는 L2 VPN 서버 포트를 입력합니다. 기본 포트는 443입니다.
암호화 알고리즘	서버와 통신하기 위한 암호화 알고리즘을 선택합니다.
스트레치된 인터페이스	서버로 스트레치될 하위 인터페이스를 선택합니다. Edge 게이트웨이의 하위 인터페이스로 구성된 조직 가상 데이터 센터 네트워크를 하위 인터페이스로 선택할 수 있습니다.

옵션	설명
송신 최적화 게이트웨이 주소	(선택 사항) 가상 시스템의 기본 게이트웨이가 두 사이트에서 동일한 경우 하위 인터페이스의 게이트웨이 IP 주소 또는 트래픽이 터널을 통해 이동해서는 안 되는 IP 주소를 입력합니다.
사용자 세부 정보	서버 인증을 위한 사용자 ID와 암호를 입력합니다.

3 변경 내용 저장

저장 작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

4 (선택 사항) 고급 옵션을 구성하려면 클라이언트 고급 탭을 클릭합니다.

5 이 L2 VPN 클라이언트 Edge가 인터넷에 직접 액세스할 수 없고 프록시 서버를 사용하여 L2 VPN 서버 Edge에 연결해야 하는 경우 프록시 설정을 지정합니다.

옵션	설명
보안 프록시 사용	보안 프록시를 사용하도록 설정하려면 선택합니다.
주소	프록시 서버 IP 주소를 입력합니다.
포트	프록시 서버 포트를 입력합니다.
사용자 이름 암호	프록시 서버 인증 자격 증명을 입력합니다.

6 서버 인증서 검증을 사용하도록 설정하려면 CA 인증서 변경을 클릭하고 적절한 CA 인증서를 선택합니다.

7 변경 내용 저장

저장 작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

다음에 수행할 작업

이 Edge 게이트웨이에서 L2 VPN 서비스를 사용하도록 설정합니다. [NSX Data Center for vSphere Edge 게이트웨이에서 L2 VPN 서비스 사용](#)의 내용을 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이에서 L2 VPN 서비스 사용

필수 L2 VPN 설정이 구성된 경우 Edge 게이트웨이에서 L2 VPN 서비스를 사용하도록 설정할 수 있습니다.

참고 이 Edge 게이트웨이에 HA가 이미 구성되어 있는 경우 Edge 게이트웨이에 둘 이상의 내부 인터페이스가 구성되어 있는지 확인합니다. 단일 인터페이스만 존재하고 이 인터페이스가 HA 기능에 의해 이미 사용된 경우 동일한 내부 인터페이스의 L2 VPN 구성이 실패합니다.

사전 요구 사항

- 이 Edge 게이트웨이가 대상 NSX Edge인 L2 VPN 서버인 경우, 필수 L2 VPN 서버 설정 및 하나 이상의 L2 VPN 피어 사이트가 구성되어 있는지 확인합니다. [NSX Data Center for vSphere Edge 게이트웨이를 L2 VPN 서버로 구성](#)에 설명된 단계를 참조하십시오.

- 이 Edge 게이트웨이가 소스 NSX Edge인 L2 VPN 클라이언트인 경우, L2 VPN 클라이언트 설정이 구성되어 있는지 확인합니다. [NSX Data Center for vSphere Edge 게이트웨이를 L2 VPN 클라이언트로 구성](#)에 설명된 단계를 참조하십시오.
- [\[L2 VPN\] 화면으로 이동](#).

절차

- 1 **L2 VPN** 탭에서 **사용** 전환을 클릭합니다.
- 2 **변경 내용 저장**을 클릭합니다.

결과

Edge 게이트웨이의 L2 VPN 서비스가 활성화됩니다.

다음에 수행할 작업

인터넷에 연결된 방화벽 쪽에서 NAT 또는 방화벽 규칙을 생성하여 L2 VPN 서버가 L2 VPN 클라이언트에 연결되도록 합니다.

NSX Data Center for vSphere Edge 게이트웨이에서 L2 VPN 서비스 구성 제거

Edge 게이트웨이의 기존 L2 VPN 서비스 구성을 제거할 수 있습니다. 이 작업을 수행하면 Edge 게이트웨이에서 L2 VPN 서비스가 사용되지 않도록 설정됩니다.

사전 요구 사항

[\[L2 VPN\] 화면으로 이동](#)

절차

- 1 L2 VPN 화면 맨 아래로 스크롤하여 **구성 삭제**를 클릭합니다.
- 2 **확인**을 클릭하여 삭제를 확인합니다.

결과

L2 VPN 서비스가 사용되지 않도록 설정되고 구성 세부 정보가 Edge 게이트웨이에서 제거됩니다.

SSL 인증서 관리

NSX 소프트웨어는 vCloud Director 환경에서 Edge 게이트웨이에 구성된 SSL VPN-Plus 및 IPsec VPN 터널과 함께 SSL(Secure Sockets Layer) 인증서를 사용할 수 있는 기능을 제공합니다.

vCloud Director 환경의 Edge 게이트웨이는 자체 서명된 인증서, CA(인증 기관) 서명 인증서 및 CA 생성/서명 인증서를 지원합니다. CSR(인증서 서명 요청)을 생성하고, 인증서를 가져오고, 가져온 인증서를 관리하고, CRL(인증서 해지 목록)을 만들 수 있습니다.

조직 가상 데이터 센터에서 인증서 사용

vCloud Director 조직 가상 데이터 센터의 다음 네트워킹 영역에 대한 인증서를 관리할 수 있습니다.

- 조직 가상 데이터 센터 네트워크와 원격 네트워크 간의 IPsec VPN 터널

- 개인 네트워크의 원격 사용자와 조직 가상 데이터 센터의 웹 리소스 간의 SSL VPN-Plus 연결
- 두 NSX Edge 게이트웨이 간의 L2 VPN 터널
- 조직 가상 데이터 센터의 로드 밸런싱을 위해 구성된 가상 서버 및 풀 서버

클라이언트 인증서 사용 방법

CAI 명령 또는 REST 호출을 통해 클라이언트 인증서를 생성할 수 있습니다. 그런 다음 이 인증서를 원격 사용자에게 배포하면 원격 사용자가 웹 브라우저에 이 인증서를 설치할 수 있습니다.

클라이언트 인증서를 구현하는 경우의 가장 큰 장점은 각 원격 사용자의 참조 클라이언트 인증서를 저장한 다음 원격 사용자가 제시하는 클라이언트 인증서와 비교 확인할 수 있다는 것입니다. 특정 사용자의 향후 연결을 차단하려면 클라이언트 인증서의 보안 서버 목록에서 참조 인증서를 삭제하면 됩니다. 인증서를 삭제하면 해당 사용자의 연결이 거부됩니다.


Edge 게이트웨이에 대한 인증서 서명 요청 생성

CA에서 서명된 인증서를 주문하거나 자체 서명된 인증서를 생성하려면 우선 Edge 게이트웨이에 대한 CSR(인증서 서명 요청)을 생성해야 합니다.

CSR은 SSL 인증서가 필요한 NSX Edge 게이트웨이에서 생성해야 하는 인코딩된 파일입니다. CSR을 사용하면 회사에서 회사 이름과 도메인 이름을 식별하는 정보와 함께 공용 키를 전송하는 방식을 표준화할 수 있습니다.

Edge 게이트웨이에서 유지되어야 하는 일치하는 개인 키 파일로 CSR을 생성합니다. CSR에는 일치하는 공용 키와 조직 이름, 위치, 도메인 이름과 같은 기타 정보가 포함되어 있습니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 **인증서** 탭을 클릭합니다.
- 3 **인증서** 탭에서 **CSR**을 클릭합니다.
- 4 CSR에 대한 다음 옵션을 구성합니다.

옵션	설명
일반 이름	인증서를 사용할 조직의 FQDN(정규화된 도메인 이름)을 입력합니다(예: <code>www.example.com</code>). 일반 이름에 <code>http://</code> 또는 <code>https://</code> 접두사를 포함하지 마십시오.
조직 구성 단위	이 필드는 이 인증서가 연결된 vCloud Director 조직 내의 사업부를 서로 구분하는 데 사용됩니다. 예를 들어 엔지니어링 또는 영업을 사용합니다.

옵션	설명
조직 이름	법적으로 등록되어 있는 회사 이름을 입력합니다. 나열된 조직은 인증서 요청에 있는 도메인 이름의 법적 등록자여야 합니다.
구/군/시	회사가 법적으로 등록되어 있는 시 또는 지역을 입력합니다.
시/도 이름	회사가 법적으로 등록되어 있는 시/도의 약어가 아닌 전체 이름을 입력합니다.
국가 코드	회사가 법적으로 등록되어 있는 국가 이름을 입력합니다.
개인 키 알고리즘	인증서의 키 유형(RSA 또는 DSA)을 입력합니다. 일반적으로 RSA가 사용됩니다. 키 유형은 호스트 간 통신을 위한 암호화 알고리즘을 정의합니다. 참고 SSL VPN-Plus는 RSA 인증서만 지원합니다.
키 크기	키 크기를 비트 단위로 입력합니다. 최소 크기는 2048비트입니다.
설명	(선택 사항) 인증서에 대한 설명을 입력합니다.

5 유지를 클릭합니다.

시스템에서 CSR을 생성하고 'CSR' 유형의 새 항목을 화면 목록에 추가합니다.

결과

화면 목록에서 CSR 유형의 항목을 선택하면 CSR 세부 정보가 화면에 표시됩니다. CSR의 표시된 PEM 형식 데이터를 복사하고 이를 CA(인증 기관)에 제출하여 CA 서명된 인증서를 가져올 수 있습니다.

다음에 수행할 작업

CSR을 사용하여 서비스 인증서를 생성하는 방법에는 다음과 같은 두 가지 옵션이 있습니다.

- CSR을 CA에 전송하여 CA 서명된 인증서를 가져옵니다. CA에서 서명된 인증서를 전송하면 서명된 인증서를 시스템으로 가져옵니다. [Edge 게이트웨이에 대해 생성된 CSR에 해당하는 CA 서명된 인증서 가져오기](#)의 내용을 참조하십시오.
- CSR을 사용하여 자체 서명된 인증서를 생성합니다. [자체 서명된 서비스 인증서 구성](#)의 내용을 참조하십시오.

Edge 게이트웨이에 대해 생성된 CSR에 해당하는 CA 서명된 인증서 가져오기


CSR(인증서 서명 요청)을 생성하고 이 CSR을 기반으로 CA 서명된 인증서를 가져온 후에는 Edge 게이트웨이에서 사용할 수 있도록 CA 서명된 인증서를 가져올 수 있습니다.

사전 요구 사항

CSR에 해당하는 CA 서명된 인증서를 가져왔는지 확인합니다. CA 서명된 인증서의 개인 키가 선택된 CSR의 개인 키와 일치하지 않는 경우 가져오기 프로세스가 실패합니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 인증서 탭을 클릭합니다.

3 화면 테이블에서 CA 서명된 인증서를 가져오려는 관련 CSR을 선택합니다.

4 서명된 인증서를 가져옵니다.

- a **CSR에 대해 생성된 서명된 인증서**를 클릭합니다.
- b CA 서명된 인증서의 PEM 데이터를 제공합니다.
 - 데이터가 사용자가 이동할 수 있는 시스템의 PEM 파일에 있는 경우 **업로드** 버튼을 클릭하여 해당 파일을 찾아 선택합니다.
 - PEM 데이터를 복사하여 붙여 넣을 수 있는 경우 데이터를 **서명된 인증서(PEM 형식)** 필드에 붙여 넣습니다.

-----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 행을 포함합니다.
- c (선택 사항) 설명을 입력할 수 있습니다.
- d **유지**를 클릭합니다.

참고 CA 서명된 인증서의 개인 키가 [인증서] 화면에서 선택한 CSR의 개인 키와 일치하지 않는 경우 가져오기 프로세스가 실패합니다.

결과

유형이 '서비스 인증서'인 CA 서명된 인증서가 화면 목록에 나타납니다.

다음에 수행할 작업

필요한 대로 CA 서명된 인증서를 SSL VPN-Plus 또는 IPsec VPN 터널에 연결합니다. [SSL VPN 서버 설정 구성](#) 및 [글로벌 IPsec VPN 설정 지정](#)의 내용을 참조하십시오.

자체 서명된 서비스 인증서 구성

VPN 관련 기능에서 사용하기 위해 자체 서명된 서비스 인증서를 Edge 게이트웨이와 함께 구성할 수 있습니다. 자체 서명된 인증서를 생성, 설치 및 관리할 수 있습니다.


[인증서] 화면에서 서비스 인증서를 사용할 수 있는 경우 Edge 게이트웨이의 VPN 관련 설정을 구성할 때 이 서비스 인증서를 지정할 수 있습니다. VPN은 지정된 서비스 인증서를 VPN에 액세스하는 클라이언트에 제공합니다.

사전 요구 사항

Edge 게이트웨이의 **인증서** 화면에서 하나 이상의 CSR을 사용할 수 있는지 확인합니다. [Edge 게이트웨이에 대한 인증서 서명 요청 생성](#)의 내용을 참조하십시오.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 인증서 탭을 클릭합니다.

3 이 자체 서명된 인증서에 대해 사용하려는 CSR을 목록에서 선택하고 **자체 서명 CSR**을 클릭합니다.

4 자체 서명된 인증서의 유효 기간(일)을 입력합니다.

5 **유지**를 클릭합니다.

시스템에서 자체 서명된 인증서를 생성하고 '서비스 인증서' 유형의 새 항목을 화면 목록에 추가합니다.

결과

Edge 게이트웨이에서 자체 서명된 인증서를 사용할 수 있습니다. 화면 목록에서 '서비스 인증서' 유형의 항목을 선택할 때 해당 세부 정보가 화면에 표시됩니다.

SSL 인증서 신뢰 확인을 위해 Edge 게이트웨이에 CA 인증서 추가

Edge 게이트웨이에 CA 인증서를 추가하면 인증을 위해 Edge 게이트웨이에 제공되는 SSL 인증서(일반적으로 Edge 게이트웨이에 대한 VPN 연결에 사용되는 클라이언트 인증서)의 신뢰를 확인할 수 있습니다.

일반적으로 회사 또는 조직의 루트 인증서를 CA 인증서로 추가합니다. 일반적으로 SSL VPN에서 인증서를 사용하여 VPN 클라이언트를 인증하는 데 사용할 수 있습니다. 클라이언트 인증서를 VPN 클라이언트에 배포할 수 있으며, VPN 클라이언트가 연결되면 해당 클라이언트 인증서가 CA 인증서에 대해 검증됩니다.

참고 CA 인증서를 추가할 때 일반적으로 관련 CRL(인증서 해지 목록)을 구성합니다. CRL은 해지된 인증서를 제시하는 클라이언트로부터 보호합니다. [Edge 게이트웨이에 인증서 해지 목록 추가](#)의 내용을 참조하십시오.

사전 요구 사항

PEM 형식의 CA 인증서 데이터가 있는지 확인합니다. 사용자 인터페이스에서, CA 인증서의 PEM 데이터를 붙여 넣거나 데이터가 들어 있고 로컬 시스템의 네트워크에서 사용할 수 있는 파일을 찾아 선택할 수 있습니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴(≡)에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 인증서 탭을 클릭합니다.

3 CA 인증서를 클릭합니다.

4 CA 인증서 데이터를 제공합니다.

- 데이터가 사용자가 이동할 수 있는 시스템의 PEM 파일에 있는 경우 **업로드** 버튼을 클릭하여 해당 파일을 찾아 선택합니다.
- PEM 데이터를 복사하여 붙여 넣을 수 있는 경우 데이터를 **CA 인증서(PEM 형식)** 필드에 붙여 넣습니다.

-----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 행을 포함합니다.

5 (선택 사항) 설명을 입력할 수 있습니다.

6 **유지**를 클릭합니다.

결과

유형이 'CA 인증서'인 CA 인증서가 화면 목록에 나타납니다. 이제 Edge 게이트웨이의 VPN 관련 설정을 구성할 때 이 CA 인증서를 지정할 수 있습니다.

Edge 게이트웨이에 인증서 해지 목록 추가

CRL(인증서 해지 목록)은 발급 CA(인증 기관)에서 발표한 해지된 디지털 인증서의 목록으로, 이러한 해지된 인증서를 제시하는 사용자를 신뢰하지 않도록 시스템을 업데이트할 수 있습니다. Edge 게이트웨이에 CRL을 추가할 수 있습니다.


"NSX 관리 가이드"에 설명된 대로, CRL에는 다음과 같은 항목이 포함되어 있습니다.

- 해지된 인증서와 해지 이유
- 인증서가 발급된 날짜
- 인증서를 발급한 단체
- 제안된 다음 릴리스 날짜

잠재적 사용자가 서버에 액세스하려고 하면 서버가 해당 특정 사용자의 CRL 항목을 기준으로 액세스를 허용하거나 거부합니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 인증서 탭을 클릭합니다.

3 CRL을 클릭합니다.

4 CRL 데이터를 제공합니다.

- 데이터가 사용자가 이동할 수 있는 시스템의 PEM 파일에 있는 경우 **업로드** 버튼을 클릭하여 해당 파일을 찾아 선택합니다.
- PEM 데이터를 복사하여 붙여 넣을 수 있는 경우 데이터를 **CRL(PEM 형식)** 필드에 붙여 넣습니다.
-----BEGIN X509 CRL----- 및 -----END X509 CRL----- 행을 포함합니다.

5 (선택 사항) 설명을 입력할 수 있습니다.

6 유지를 클릭합니다.

결과

CRL이 화면 목록에 나타납니다.

Edge 게이트웨이에 서비스 인증서 추가


Edge 게이트웨이에 서비스 인증서를 추가하면 이 인증서를 Edge 게이트웨이의 VPN 관련 설정에서 사용할 수 있습니다. **인증서** 화면에 서비스 인증서를 추가할 수 있습니다.

사전 요구 사항

서비스 인증서가 있는지 그리고 그 개인 키가 PEM 형식인지 확인합니다. 사용자 인터페이스에서, PEM 데이터에 붙여 넣거나 PEM 데이터가 들어 있고 로컬 시스템의 네트워크에서 사용할 수 있는 파일로 이동할 수 있습니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 인증서 탭을 클릭합니다.

3 서비스 인증서를 클릭합니다.

4 서비스 인증서의 PEM 형식 데이터를 입력합니다.

- 데이터가 사용자가 이동할 수 있는 시스템의 PEM 파일에 있는 경우 **업로드** 버튼을 클릭하여 해당 파일을 찾아 선택합니다.
- PEM 데이터를 복사하여 붙여 넣을 수 있는 경우 데이터를 **서비스 인증서(PEM 형식)** 필드에 붙여 넣습니다.

-----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 행을 포함합니다.

5 인증서 개인 키의 PEM 형식 데이터를 입력합니다.

- 데이터가 사용자가 이동할 수 있는 시스템의 PEM 파일에 있는 경우 **업로드** 버튼을 클릭하여 해당 파일을 찾아 선택합니다.
- PEM 데이터를 복사하여 붙여 넣을 수 있는 경우 데이터를 **개인 키(PEM 형식)** 필드에 붙여 넣습니다.

-----BEGIN RSA PRIVATE KEY----- 및 -----END RSA PRIVATE KEY----- 행을 포함합니다.

6 개인 키 암호를 입력하고 확인합니다.**7** (선택 사항) 설명을 입력할 수 있습니다.**8** **유지**를 클릭합니다.**결과**

유형이 '서비스 인증서'인 인증서가 화면 목록에 나타납니다. 이제 Edge 게이트웨이의 VPN 관련 설정을 구성할 때 이 서비스 인증서를 선택할 수 있습니다.

사용자 지정 개체 그룹화

NSX 소프트웨어를 vCloud Director 환경에서 사용하여 특정 엔티티의 집합 및 그룹을 정의한 다음 방화벽 규칙 같은 다른 네트워크 관련 구성을 지정할 때 사용할 수 있습니다.

방화벽 규칙 및 DHCP 릴레이 구성에 사용할 IP 집합 만들기

IP 집합은 조직 가상 데이터 센터 수준에서 만들 수 있는 IP 주소 그룹입니다. 방화벽 규칙이나 DHCP 릴레이 구성에서 IP 집합을 소스 또는 대상으로 사용할 수 있습니다.

IP 집합은 **개체 그룹화** 페이지를 사용하여 생성합니다. 이 페이지를 열려면 조직 VDC의 분산 방화벽 설정 또는 조직 VDC에 속하는 Edge 게이트웨이의 서비스 설정으로 이동해야 합니다.

절차

1 개체 그룹화 페이지를 엽니다.

옵션	작업
조직 VDC의 분산 방화벽 설정	<ul style="list-style-type: none"> a 기본 메뉴()에서 클라우드 리소스를 선택합니다. b 왼쪽 창에서 조직 VDC를 클릭합니다. c 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 선택하고 방화벽 관리를 클릭합니다. d 개체 그룹화 탭을 클릭합니다.
조직 VDC에 있는 Edge 게이트웨이의 서비스 설정	<ul style="list-style-type: none"> a 기본 메뉴()에서 클라우드 리소스를 선택합니다. b 왼쪽 창에서 Edge 게이트웨이를 클릭합니다. c 대상 조직 가상 데이터 센터에 속하는 Edge 게이트웨이의 이름 옆에 있는 라디오 버튼을 선택하고 서비스를 클릭합니다. d 개체 그룹화 탭을 클릭합니다.

2 IP 집합 탭을 클릭합니다.

이미 정의된 IP 집합이 화면에 표시됩니다.

3 IP 집합을 추가하려면 **만들기**() 버튼을 클릭합니다.

4 IP 집합의 이름과 설명(선택 사항) 및 집합에 포함할 IP 주소를 입력합니다.

5 IP 집합을 저장하려면 **유지**를 클릭합니다.

결과

새 IP 집합을 방화벽 규칙 또는 DHCP 릴레이 구성의 소스 또는 대상으로 선택할 수 있습니다.

방화벽 규칙에 사용할 MAC 집합 만들기

MAC 집합은 조직 가상 데이터 센터 수준에서 생성할 수 있는 MAC 주소의 그룹입니다. 방화벽 규칙에서 MAC 집합을 소스 또는 대상으로 사용할 수 있습니다.

개체 그룹화 페이지를 사용하여 MAC 집합을 생성합니다. 이 페이지를 열려면 조직 VDC의 분산 방화벽 설정 또는 조직 VDC에 속하는 Edge 게이트웨이의 서비스 설정으로 이동해야 합니다.

절차

1 개체 그룹화 페이지를 엽니다.

옵션	작업
조직 VDC의 분산 방화벽 설정	<ul style="list-style-type: none"> a 기본 메뉴()에서 클라우드 리소스를 선택합니다. b 왼쪽 창에서 조직 VDC를 클릭합니다. c 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 선택하고 방화벽 관리를 클릭합니다. d 개체 그룹화 탭을 클릭합니다.
조직 VDC에 있는 Edge 게이트웨이의 서비스 설정	<ul style="list-style-type: none"> a 기본 메뉴()에서 클라우드 리소스를 선택합니다. b 왼쪽 창에서 Edge 게이트웨이를 클릭합니다. c 대상 조직 가상 데이터 센터에 속하는 Edge 게이트웨이의 이름 옆에 있는 라디오 버튼을 선택하고 서비스를 클릭합니다. d 개체 그룹화 탭을 클릭합니다.

2 MAC 집합 탭을 클릭합니다.

이미 정의된 MAC 집합이 화면에 표시됩니다.

3 MAC 집합을 추가하려면 **만들기**() 버튼을 클릭합니다.

4 집합의 이름, 설명(선택 사항) 및 집합에 포함될 MAC 주소를 입력합니다.

5 MAC 집합을 저장하려면 **유지**를 클릭합니다.

결과

새 MAC 집합을 방화벽 규칙의 소스 또는 대상으로 선택할 수 있습니다.



방화벽 규칙에 사용할 수 있는 서비스 보기

방화벽 규칙에 사용할 수 있는 서비스 목록을 볼 수 있습니다. 이 컨텍스트에서 서비스는 프로토콜-포트 조합입니다.

개체 그룹화 페이지를 사용하여 사용 가능한 서비스를 볼 수 있습니다. 이 페이지를 열려면 조직 VDC의 분산 방화벽 설정 또는 조직 VDC에 속하는 Edge 게이트웨이의 서비스 설정으로 이동해야 합니다.

절차

1 개체 그룹화 페이지를 엽니다.

옵션	작업
조직 VDC의 분산 방화벽 설정	<ul style="list-style-type: none"> a 기본 메뉴()에서 클라우드 리소스를 선택합니다. b 왼쪽 창에서 조직 VDC를 클릭합니다. c 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 선택하고 방화벽 관리를 클릭합니다. d 개체 그룹화 탭을 클릭합니다.
조직 VDC에 있는 Edge 게이트웨이의 서비스 설정	<ul style="list-style-type: none"> a 기본 메뉴()에서 클라우드 리소스를 선택합니다. b 왼쪽 창에서 Edge 게이트웨이를 클릭합니다. c 대상 조직 가상 데이터 센터에 속하는 Edge 게이트웨이의 이름 옆에 있는 라디오 버튼을 선택하고 서비스를 클릭합니다. d 개체 그룹화 탭을 클릭합니다.

2 서비스 탭을 클릭합니다.

결과

사용 가능한 서비스가 화면에 표시됩니다.


방화벽 규칙에 사용할 수 있는 서비스 그룹 보기

방화벽 규칙에 사용할 수 있는 서비스 그룹 목록을 볼 수 있습니다. 이 컨텍스트에서 서비스는 프로토콜-포트 조합이며 서비스 그룹은 서비스 또는 다른 서비스 그룹의 그룹입니다.

개체 그룹화 페이지를 사용하여 사용 가능한 서비스 그룹을 볼 수 있습니다. 이 페이지를 열려면 조직 VDC의 분산 방화벽 설정 또는 조직 VDC에 속하는 Edge 게이트웨이의 서비스 설정으로 이동해야 합니다.

절차

1 개체 그룹화 페이지를 엽니다.

옵션	작업
조직 VDC의 분산 방화벽 설정	<ul style="list-style-type: none"> a 기본 메뉴()에서 클라우드 리소스를 선택합니다. b 왼쪽 창에서 조직 VDC를 클릭합니다. c 대상 조직 가상 데이터 센터의 이름 옆에 있는 라디오 버튼을 선택하고 방화벽 관리를 클릭합니다. d 개체 그룹화 탭을 클릭합니다.
조직 VDC에 있는 Edge 게이트웨이의 서비스 설정	<ul style="list-style-type: none"> a 기본 메뉴()에서 클라우드 리소스를 선택합니다. b 왼쪽 창에서 Edge 게이트웨이를 클릭합니다. c 대상 조직 가상 데이터 센터에 속하는 Edge 게이트웨이의 이름 옆에 있는 라디오 버튼을 선택하고 서비스를 클릭합니다. d 개체 그룹화 탭을 클릭합니다.

2 서비스 그룹 탭을 클릭합니다.


결과

사용 가능한 서비스 그룹이 화면에 표시됩니다. [설명] 열에는 각 서비스 그룹으로 그룹화된 서비스가 표시됩니다.

Edge 게이트웨이의 네트워크 사용 및 IP 할당 보기

IP 풀 사용 및 서브넷에 대한 정보를 포함하여 Edge 게이트웨이의 네트워크를 볼 수 있습니다. 각 네트워크에 할당된 IP 주소도 볼 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭하고 대상 Edge 게이트웨이의 이름을 클릭합니다.
- 3 외부 네트워크 및 해당 IP 풀 사용과 서브넷에 대한 정보를 보려면 **외부 네트워크 > 네트워크 및 서브넷** 탭을 클릭합니다.
- 4 외부 네트워크 및 해당 IP 주소와 범주에 대한 정보를 보려면 **외부 네트워크 > IP 할당** 탭을 클릭합니다.

Edge 게이트웨이 속성 편집


Edge 게이트웨이에서 분산 라우팅 사용 또는 사용 안 함

Edge 게이트웨이에서 vCloud Director 분산 라우팅을 사용하도록 설정한 후에 조직 관리자는 Edge 게이트웨이에 연결된 분산 인터페이스를 사용하여 라우팅된 조직 가상 데이터 센터 네트워크를 여러 개 생성할 수 있습니다. 이러한 네트워크의 트래픽은 VM 간 통신에 최적화됩니다.

사전 요구 사항

백업 NSX Manager 인스턴스가 NSX Controller 클러스터로 구성되어 있습니다. "NSX 관리 가이드"의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- 3 대상 Edge 게이트웨이의 이름 옆에 있는 라디오 버튼을 선택하고 **분산 라우팅 사용** 또는 **분산 라우팅 사용 안 함**을 클릭합니다.
- 4 **확인**을 클릭하여 확인합니다.


외부 네트워크 및 Edge 게이트웨이 설정 수정

외부 네트워크와 Edge 게이트웨이 설정을 수정하려면 **Edge 게이트웨이 편집** 마법사를 사용합니다. 여기에는 Edge 게이트웨이를 생성하는 데 사용한 마법사와 동일한 페이지가 포함되어 있습니다.

Edge 게이트웨이를 추가할 때 구성한 설정을 수정할 수 있습니다. [NSX Data Center for vSphere Edge 게이트웨이 추가](#)의 내용을 참조하십시오.

분산 라우팅 설정을 수정하려면 [Edge 게이트웨이에서 분산 라우팅 사용 또는 사용 안 함](#)의 내용을 참조하십시오.


절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- 3 수정할 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **편집**을 클릭합니다.
- 4 Edge 게이트웨이 설정을 수정하려면 **다음**을 클릭하고 **Edge 게이트웨이 편집** 마법사 페이지로 이동하여 **완료 준비** 페이지에서 **마침**을 클릭합니다.

Edge 게이트웨이의 일반 설정 편집

Edge 게이트웨이의 이름과 설명을 수정하고 FIPS 모드와 고가용성 상태를 사용하거나 사용하지 않도록 설정하고 Edge 게이트웨이 크기 구성을 변경할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭하고 대상 Edge 게이트웨이의 이름을 클릭합니다.
- 3 **일반** 탭의 오른쪽 상단 모서리에서 **편집**을 클릭합니다.
- 4 (선택 사항) Edge 게이트웨이의 이름과 설명을 편집합니다.
- 5 (선택 사항) 각각의 일반 Edge 게이트웨이 설정을 켜거나 끕니다.

일반 설정	설명
FIPS 모드	NSX FIPS 모드를 사용하도록 Edge 게이트웨이를 구성합니다.
고가용성	백업 Edge 게이트웨이로 자동 페일오버되도록 설정합니다.

- 6 (선택 사항) 시스템 리소스에 대한 Edge 게이트웨이 구성을 변경합니다.

구성	설명
압축	메모리와 계산 리소스를 더 적게 사용합니다.
큼	[압축] 구성보다 향상된 성능 및 용량을 제공합니다. [큼] 및 [초대형] 구성은 보안 기능이 동일합니다.


구성	설명
초대형	동시 세션 수가 많고 로드 밸런서를 사용하는 환경에 사용됩니다.
4배 대형	처리량이 많은 환경에 사용됩니다. 높은 연결 속도가 필요합니다.

7 **저장**을 클릭하여 변경을 확인합니다.

Edge 게이트웨이의 기본 게이트웨이 편집

Edge 게이트웨이가 기본 게이트웨이로 사용하는 네트워크를 변경할 수 있습니다.


절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭하고 대상 Edge 게이트웨이의 이름을 클릭합니다.
- 3 **외부 네트워크 > 기본 게이트웨이** 탭의 오른쪽 상단에서 **편집**을 클릭합니다.
- 4 (선택 사항) 특정 네트워크를 기본 게이트웨이로 구성합니다.
 - a **기본 게이트웨이 구성** 토글을 설정합니다.
 - b 대상 외부 네트워크의 이름 옆에 있는 라디오 버튼을 선택하고 대상 IP 주소 옆에 있는 라디오 버튼을 선택합니다.
 - c (선택 사항) **DNS 릴레이에 기본 게이트웨이 사용** 토글을 설정합니다.
- 5 **저장**을 클릭하여 변경을 확인합니다.

Edge 게이트웨이의 IP 설정 편집

Edge 게이트웨이의 외부 네트워크에 대한 IP 설정을 수정할 수 있습니다.

절차


- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭하고 대상 Edge 게이트웨이의 이름을 클릭합니다.
- 3 **외부 네트워크 > IP 설정** 탭에서 **편집**을 클릭합니다.
- 4 Edge 게이트웨이의 각 네트워크에 대해 **IP 주소** 셀에 IP 주소를 입력하거나 셀을 비워둡니다.
네트워크에 대한 IP 주소를 입력하지 않으면 이 네트워크에 임의의 IP 주소가 시스템에서 할당됩니다.
- 5 **저장**을 클릭하여 변경을 확인합니다.

Edge 게이트웨이에서 하위 할당된 IP 풀 편집

Edge 게이트웨이의 외부 네트워크의 사용 가능한 IP 풀에서 여러 정적 IP 풀을 하위 할당할 수 있습니다.

참고 하위 할당을 통해 Edge 게이트웨이에 IP 주소를 할당하는 것은 제공자가 IP 주소의 소유권을 게이트웨이에 할당하는 프로세스입니다. vCloud Director는 하위 할당 프로세스 중에 보조 주소로 적절한 게이트웨이 인터페이스를 자동으로 구성하기 때문에, vCloud Director 외부에서 사용되는 IP 주소가 있으면 IP 주소 충돌이 발생할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭하고 대상 Edge 게이트웨이의 이름을 클릭합니다.
- 3 **외부 네트워크 > 하위 할당된 IP 풀** 탭을 클릭합니다.
이 Edge 게이트웨이의 각 외부 네트워크에 대해 현재 하위 할당된 IP 풀을 볼 수 있습니다.
- 4 외부 네트워크의 이름 옆에 있는 라디오 버튼을 클릭하고 **편집**을 클릭합니다.
이 외부 네트워크에 사용할 수 있는 IP 풀과 현재 하위 할당된 IP 풀(구성한 경우)을 볼 수 있습니다.
- 5 이 외부 네트워크에 대해 하위 할당된 IP 풀을 편집하고 **저장**을 클릭합니다.
사용할 수 있는 IP 풀의 범위에서 IP 주소 및 범위를 추가, 수정 및 제거할 수 있습니다.

결과


시스템에서 겹치는 IP 범위를 결합합니다.

Edge 게이트웨이의 속도 제한 편집

Edge 게이트웨이의 각 외부 네트워크에 대한 인바운드 및 아웃바운드 속도 제한을 구성할 수 있습니다.

속도 제한은 정적 바인딩이 적용된 분산 포트 그룹에서 지원하는 외부 네트워크에만 적용됩니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭하고 대상 Edge 게이트웨이의 이름을 클릭합니다.
- 3 **외부 네트워크 > 속도 제한** 탭의 오른쪽 위에서 **편집**을 클릭합니다.
이 Edge 게이트웨이의 각 외부 네트워크에 대한 현재 속도 제한을 볼 수 있습니다.
- 4 속도 제한을 편집하고 **저장**을 클릭합니다.
Edge 게이트웨이의 각 외부 네트워크에 대해 속도 제한을 사용 또는 사용하지 않도록 설정하고 수신 및 송신 비율을 변경할 수 있습니다.


Edge 게이트웨이 다시 배포

Edge 게이트웨이 장치를 삭제하고 최신 구성을 사용하여 새로 배포할 수 있습니다.

Edge 서비스가 예상대로 작동하지 않으면 Edge 게이트웨이 장치를 다시 배포할 수 있습니다.

Edge 게이트웨이를 다시 배포하면 vCloud Director가 삭제하고 최신 구성을 사용하여 다시 생성합니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- 3 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **다시 배포**를 클릭합니다.
- 4 **확인**을 클릭하여 확인합니다.

결과

Edge 게이트웨이 가상 시스템이 새 가상 시스템으로 바뀌고 모든 서비스가 복원됩니다.


Edge 게이트웨이 삭제

조직 가상 데이터 센터에서 Edge 게이트웨이를 제거할 수 있습니다.

사전 요구 사항

대상 Edge 게이트웨이를 사용하는 조직 가상 데이터 센터 네트워크를 모두 삭제합니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- 3 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **삭제**를 클릭합니다.
- 4 **삭제**를 클릭하여 확인합니다.

Edge 게이트웨이에 대한 통계 및 로그


Edge 게이트웨이에 대한 통계 및 로그를 볼 수 있습니다.

통계 보기

Edge 게이트웨이 서비스 화면에서 통계를 볼 수 있습니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 통계 탭을 클릭합니다.

3 보려는 통계 유형에 따라 탭을 탐색합니다.

옵션	설명
연결	[연결] 화면은 운영 가시성을 제공합니다. 이 화면에는 선택한 Edge 게이트웨이의 인터페이스를 통과하는 트래픽에 대한 그래프 외에도, 방화벽 및 로드 밸런서 서비스에 대한 연결 통계가 표시됩니다. 통계를 볼 기간을 선택합니다.
IPsec VPN	[IPsec VPN] 화면에는 IPsec VPN 상태와 통계 및 각 터널의 상태와 통계가 표시됩니다.
L2 VPN	[L2 VPN] 화면에는 L2 VPN 상태 및 통계가 표시됩니다.

로깅 사용


Edge 게이트웨이에 대한 로깅을 사용하도록 설정할 수 있습니다. 로그 데이터를 수집할 기능에 대한 로깅을 사용하도록 설정하는 것 외에도 구성을 완료하려면 수집된 로그 데이터를 수신할 Syslog 서버가 있어야 합니다. [Edge 설정] 화면에서 Syslog 서버를 구성할 때 해당 Syslog 서버에서 기록된 데이터에 액세스할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 Edge 설정 탭에서 Syslog 서버 편집 버튼을 클릭합니다.

로깅을 사용하도록 설정된 서비스에 대한 Edge 게이트웨이의 네트워킹 관련 로그에 대해 Syslog 서버를 사용자 지정할 수 있습니다.

vCloud Director 시스템 관리자가 vCloud Director 환경에 대해 Syslog 서버를 이미 구성한 경우, 이 Syslog 서버가 시스템에서 기본적으로 사용되며 해당 IP 주소가 **Edge 설정** 화면에 표시됩니다.


3 기능별로 로깅을 사용하도록 설정합니다.

- **NAT** 탭에서 **DNAT 규칙** 버튼을 클릭하고 **로깅 사용** 토글을 켭니다.
주소 변환을 기록합니다.
- **NAT** 탭에서 **SNAT 규칙** 버튼을 클릭하고 **로깅 사용** 토글을 켭니다.
주소 변환을 기록합니다.
- **라우팅** 탭에서 **라우팅 구성**을 클릭하고 [동적 라우팅 구성] 아래에서 **로깅 사용** 토글을 켭니다.
동적 라우팅 활동을 기록합니다. **로그 수준** 드롭다운 메뉴에서 기록할 메시지 상태 수준의 하한을 선택할 수 있습니다.
- **로드 밸런서** 탭에서 **글로벌 구성**을 클릭하고 **로깅 사용** 토글을 켭니다.
로드 밸런서의 트래픽 흐름을 기록합니다. **로그 수준** 드롭다운 메뉴에서 기록할 메시지 상태 수준의 하한을 선택할 수 있습니다.
- **VPN** 탭에서 **IPSec VPN > 로깅 설정**으로 이동하여 **로깅 사용** 토글을 켭니다.
로컬 서브넷과 피어 서브넷 사이의 트래픽 흐름을 기록합니다. **로그 수준** 드롭다운 메뉴에서 기록할 메시지 상태 수준의 하한을 선택할 수 있습니다.
- **SSL VPN-Plus** 탭에서 **일반 설정**을 클릭하고 **로깅 사용** 토글을 켭니다.
SSL VPN 게이트웨이를 통과하는 트래픽의 로그를 유지합니다.
- **SSL VPN-Plus** 탭에서 **서버 설정**을 클릭하고 **로깅 사용** 토글을 켭니다.
SSL VPN 서버에서 발생하는 Syslog 활동을 기록합니다. **로그 수준** 드롭다운 메뉴에서 기록할 메시지 상태 수준의 하한을 선택할 수 있습니다.

Edge 게이트웨이에 대한 SSH 명령줄 액세스 사용

Edge 게이트웨이에 대한 SSH 명령줄 액세스를 사용하도록 설정할 수 있습니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 **Edge 설정** 탭을 클릭합니다.

3 SSH 설정을 구성합니다.

옵션	설명
사용자 이름	이 Edge 게이트웨이에 대한 SSH 액세스 자격 증명을 입력합니다.
암호	기본적으로 SSH 사용자 이름은 admin 입니다.
암호 다시 입력	
암호 만료	암호의 만료 기간(일)을 입력합니다.
로그인 배너	Edge 게이트웨이에 대한 SSH 연결을 시작하는 사용자에게 표시할 텍스트를 입력합니다.

4 사용 토글을 켭니다.

다음에 수행할 작업

이 Edge 게이트웨이에 대한 SSH 액세스를 허용하도록 NAT 또는 방화벽 규칙을 적절히 구성합니다.

NSX-T Data Center Edge 게이트웨이 관리

8

NSX-T Data Center Edge 게이트웨이는 IP 관리 속성 및 외부 네트워크에 연결할 수 있는 라우팅된 조직 VDC 네트워크를 제공합니다. 방화벽, NAT(네트워크 주소 변환), DNS 전달 및 DHCP와 같은 서비스도 제공할 수 있으며, 이러한 서비스는 기본적으로 사용하도록 설정됩니다.

본 장은 다음 항목을 포함합니다.

- NSX-T Data Center Edge 게이트웨이 추가
- NSX-T Edge 게이트웨이에 방화벽 그룹 추가
- NSX-T Edge 게이트웨이 방화벽 규칙 추가
- NSX-T Edge 게이트웨이에 SNAT 또는 DNAT 규칙 추가
- NSX-T Edge 게이트웨이에서 DNS 전달자 서비스 구성
- NSX-T Edge 게이트웨이의 IP 할당 편집
- 빠른 IP 할당
- 사용자 지정 애플리케이션 포트 프로파일 생성


NSX-T Data Center Edge 게이트웨이 추가

NSX-T Data Center Edge 게이트웨이는 외부 네트워크와 연결할 수 있는 라우팅된 조직 VDC 네트워크를 제공하고 로드 밸런싱, NAT(네트워크 주소 변환), 방화벽과 같은 서비스를 제공할 수 있습니다.

사전 요구 사항

NSX-T Data Center Edge 게이트웨이 배포를 위한 시스템 요구 사항에 대한 자세한 내용은 "NSX-T 관리 가이드"의 내용을 참조하십시오.

절차


- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- 3 **새로 만들기**를 클릭합니다.
- 4 Edge 게이트웨이를 만들 NSX-T 지원형 조직 VDC를 선택하고 **다음**을 클릭합니다.

- 5 새 Edge 게이트웨이의 이름과 설명(선택 사항)을 입력하고 **다음**을 클릭합니다.
- 6 새 Edge 게이트웨이를 연결할 외부 네트워크를 선택하고 **다음**을 클릭합니다.
- 7 (선택 사항) Edge 게이트웨이에 할당된 IP 주소 또는 IP 주소 범위를 편집하고 **다음**을 클릭합니다.
- 8 **완료 준비** 페이지를 검토하고 **마침**을 클릭합니다.

NSX-T Edge 게이트웨이에 방화벽 그룹 추가

방화벽 규칙을 생성하여 NSX-T Edge 게이트웨이에 추가하려면 먼저 방화벽 그룹을 생성해야 합니다. 방화벽 그룹은 방화벽 규칙이 적용되는 개체 그룹입니다. 여러 개체를 방화벽 그룹으로 결합하면, 생성되는 총 방화벽 규칙 수를 줄이는 데 도움이 됩니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 NSX-T Edge 게이트웨이를 클릭하고 **보안**을 클릭합니다.
- 3 **그룹** 탭을 클릭하고 **새로 만들기**를 클릭합니다.
- 4 방화벽 그룹의 이름과 설명(선택 사항)을 입력합니다.
- 5 그룹에 포함된 가상 시스템의 IP 주소 또는 IP 주소 범위를 입력하고 **추가**를 클릭합니다.
- 6 방화벽 그룹을 저장하려면 **저장**을 클릭합니다.

결과

방화벽 그룹을 생성하여 NSX-T Edge 게이트웨이에 추가했습니다.


다음에 수행할 작업

[NSX-T Edge 게이트웨이 방화벽 규칙 추가](#)

NSX-T Edge 게이트웨이 방화벽 규칙 추가

NSX-T Edge 게이트웨이의 수신 및 송신 네트워크 트래픽을 제어하려면 방화벽 규칙을 생성합니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 Edge 게이트웨이를 클릭하고 **서비스**를 클릭합니다.
- 3 **방화벽** 화면이 표시되지 않으면 **방화벽** 탭을 클릭합니다.
- 4 **규칙 편집**을 클릭합니다.
- 5 방화벽 규칙을 선택하고 **위에 추가** 버튼을 클릭합니다.
새 규칙에 대한 행이 선택한 규칙 위에 추가됩니다.
- 6 방화벽 규칙을 구성합니다.

옵션	설명
이름	규칙의 이름을 입력합니다.
상태	생성 시 규칙을 사용하도록 설정하려면 상태 토글을 설정합니다.
애플리케이션	(선택 사항) 규칙이 적용되는 특정 포트 프로파일을 선택하려면 애플리케이션 토글을 설정하고 저장 을 클릭합니다.
소스	<p>옵션을 선택하고 유지를 클릭합니다.</p> <ul style="list-style-type: none"> ■ 임의의 소스 주소에서 발생한 트래픽을 허용하거나 거부하려면 모든 소스 토글을 설정합니다. ■ 특정 방화벽 그룹에서 발생한 트래픽을 허용하거나 거부하려면 목록에서 해당 방화벽 그룹을 선택합니다.
대상	<p>옵션을 선택하고 유지를 클릭합니다.</p> <ul style="list-style-type: none"> ■ 임의의 대상 주소로 보내는 트래픽을 허용하거나 거부하려면 모든 대상 토글을 설정합니다. ■ 특정 방화벽 그룹에서 발생한 트래픽을 허용하거나 거부하려면 목록에서 해당 방화벽 그룹을 선택합니다.
작업	<p>작업 드롭다운 메뉴에서 옵션을 선택합니다.</p> <ul style="list-style-type: none"> ■ 지정된 소스, 대상 및 서비스의 송신 또는 수신 트래픽을 허용하려면 수락을 선택합니다. ■ 지정된 소스, 대상 및 서비스의 송신 또는 수신 트래픽을 차단하려면 거부를 선택합니다.
IP 프로토콜	규칙을 IPv4 또는 IPv6 중 어느 트래픽에 적용할지 선택합니다.
방향	규칙을 적용할 트래픽 방향을 선택합니다.
로깅 사용	이 규칙에 의해 수행된 주소 변환을 기록하려면 로깅 사용 토글을 설정합니다.

- 7 **저장**을 클릭합니다.
- 8 추가 규칙을 구성하려면 위의 단계를 반복합니다.

결과

방화벽 규칙이 생성되면 **Edge** 게이트웨이 방화벽 규칙 목록에 나타납니다. 필요에 따라 규칙을 위로 이동하거나 아래로 이동하거나 편집하거나 삭제할 수 있습니다.

NSX-T Edge 게이트웨이에 SNAT 또는 DNAT 규칙 추가


소스 IP 주소를 개인에서 공용 IP 주소로 변경하려면 **SNAT**(소스 NAT) 규칙을 생성합니다. 대상 IP 주소를 공용에서 개인 IP 주소로 변경하려면 **DNAT**(대상 NAT) 규칙을 생성합니다.

vCloud Director 환경의 **Edge** 게이트웨이에 **SNAT** 또는 **DNAT** 규칙을 구성할 때는 항상 조직 **VDC**의 관점에서 규칙을 구성해야 합니다. **SNAT** 규칙은 조직 **VDC** 네트워크에서 외부 네트워크 또는 다른 조직 **VDC** 네트워크로 전송되는 패킷의 소스 IP 주소를 변환합니다. **DNAT** 규칙은 외부 네트워크 또는 다른 조직 **VDC** 네트워크에서 조직 **VDC** 네트워크로 들어오는 패킷의 IP 주소(필요한 경우 포트 포함)를 변환합니다.

사전 요구 사항

규칙을 추가할 **Edge** 게이트웨이 인터페이스에 공개 IP 주소가 추가된 상태여야 합니다.

절차

- 1 **Edge** 게이트웨이 서비스를 엽니다.
 - a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - c 대상 **Edge** 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- 2 **Edge** 게이트웨이를 클릭하고 **NAT**를 클릭합니다.
- 3 규칙을 추가하려면 **추가**를 클릭합니다.
- 4 소스 NAT 규칙(내부에서 외부로 나감)을 구성합니다.

옵션	설명
이름	규칙의 이름을 입력합니다.
상태	생성 시 규칙을 사용하도록 설정하려면 상태 토글을 설정합니다.
인터페이스 유형	규칙을 적용할 인터페이스를 선택합니다.
외부 IP	SNAT 규칙을 구성하는 Edge 게이트웨이의 공개 IP 주소를 입력합니다.
내부 IP	외부 네트워크로 트래픽을 보낼 수 있도록 SNAT 를 구성하려는 가상 시스템의 IP 주소나 IP 주소 범위를 입력합니다.
로깅 사용	이 규칙에 의해 수행된 주소 변환을 기록하려면 로깅 사용 토글을 설정합니다.

5 대상 NAT 규칙(외부에서 내부로 이동)을 구성합니다.

옵션	설명
이름	규칙의 이름을 입력합니다.
상태	생성 시 규칙을 사용하도록 설정하려면 상태 토글을 설정합니다.
인터페이스 유형	규칙을 적용할 인터페이스를 선택합니다.
외부 IP	DNAT 규칙을 구성하는 Edge 게이트웨이의 공개 IP 주소를 입력합니다. 입력하는 IP 주소는 Edge 게이트웨이의 하위 할당된 IP 범위에 속해야 합니다.
애플리케이션	(선택 사항) 규칙을 적용할 특정 애플리케이션 포트 프로파일을 선택합니다. 애플리케이션 포트 프로파일에는 수신 트래픽이 Edge 게이트웨이에서 내부 네트워크에 연결하는 데 사용하는 포트와 프로토콜이 포함됩니다.
내부 IP	외부 네트워크의 트래픽을 수신할 수 있도록 DNAT를 구성하려는 가상 시스템의 IP 주소나 IP 주소 범위를 입력합니다.
내부 포트	(선택 사항) DNAT 규칙이 가상 시스템으로 인바운드된 패킷을 변환하는 포트 또는 포트 범위를 선택합니다.
로깅 사용	이 규칙에 의해 수행된 주소 변환을 기록하려면 로깅 사용 토글을 설정합니다.

6 저장을 클릭합니다.


7 추가 규칙을 구성하려면 위의 단계를 반복합니다.

NSX-T Edge 게이트웨이에서 DNS 전달자 서비스 구성

DNS 쿼리를 외부 DNS 서버에 전달하려면 DNS 전달자를 구성합니다.

DNS 전달자 서비스 구성의 일부로 조건부 전달자 영역을 추가할 수도 있습니다. 조건부 전달자 영역은 FQDN DNS 영역이 최대 5개 포함된 목록으로 구성됩니다. DNS 쿼리가 이 목록의 도메인 이름과 일치하면 해당 전달자 영역의 서버로 쿼리가 전달됩니다.

절차

- Edge 게이트웨이 서비스를 엽니다.
 - 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
 - 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
 - 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.
- Edge 게이트웨이를 클릭하고 **서비스**를 클릭합니다.
- DNS**를 클릭하고 **DNS 전달자** 섹션에서 **편집**을 클릭합니다.
- DNS 전달자 서비스를 사용하도록 설정하려면 **상태** 토글을 설정합니다.
- 기본 DNS 영역의 이름과 설명(선택 사항)을 입력합니다.
- 하나 이상의 업스트림 서버 IP 주소를 쉼표로 구분하여 입력합니다.

7 **저장**을 클릭합니다.

8 (선택 사항) 조건부 전달자 영역을 추가합니다.


- a **조건부 전달자 영역** 섹션에서 **추가**를 클릭합니다.
- b 전달자 영역의 이름을 입력합니다.
- c 하나 이상의 업스트림 서버 IP 주소를 쉼표로 구분하여 입력합니다.
- d 하나 이상의 도메인 이름을 쉼표로 구분하여 입력하고 **저장**을 클릭합니다.

NSX-T Edge 게이트웨이의 IP 할당 편집

외부 네트워크의 여러 IP 주소를 Edge 게이트웨이에 할당할 수 있습니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 Edge 게이트웨이를 클릭하고 **IP 할당**을 클릭합니다.

IP 관리 그리드에서 Edge 게이트웨이에 할당된 IP 주소와 현재 Edge 게이트웨이에서 현재 사용 중인 IP 주소를 볼 수 있습니다.

3 **할당된 IP** 섹션에서 **IP 관리**를 클릭합니다.

IP 관리 그리드에서 Edge 게이트웨이에서 사용할 수 있는 각 외부 네트워크의 IP 사용량을 볼 수 있습니다.

4 IP 범위를 입력하고 **추가**를 클릭합니다.

5 **저장**을 클릭합니다.

결과

IP 주소가 Edge 게이트웨이에 할당됩니다.

다음에 수행할 작업


Edge 게이트웨이에 할당된 IP 주소를 보거나 필요에 따라 IP 주소를 더 추가하거나 제거합니다.

빠른 IP 할당

빠른 IP 할당을 사용하면 특정 IP 주소나 IP 주소 범위를 입력하지 않고도, 외부 네트워크 서브넷의 IP 주소를 Edge 게이트웨이에 할당할 수 있습니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

2 Edge 게이트웨이를 클릭하고 **IP 할당**을 클릭합니다.

IP 관리 그리드에서 Edge 게이트웨이에 할당된 IP 주소와 현재 Edge 게이트웨이에서 현재 사용 중인 IP 주소를 볼 수 있습니다.

3 할당된 IP 섹션에서 **빠른 IP 할당**을 클릭합니다.

4 드롭다운 메뉴에서 IP 주소를 할당할 서브넷을 선택합니다.

여러 서브넷을 사용할 수 있는 경우 **임의**를 선택하면 하나 이상의 서브넷에서 IP 주소가 할당됩니다.

5 Edge 게이트웨이에 할당할 IP 주소 수를 입력하고 **저장**을 클릭합니다.

이 숫자는 선택한 서브넷에서 사용 가능한 IP 주소 수보다 작아야 합니다.

결과

IP 주소가 Edge 게이트웨이에 할당됩니다.

다음에 수행할 작업

Edge 게이트웨이에 할당된 IP 주소를 보거나 필요에 따라 IP 주소를 더 추가하거나 제거합니다.

사용자 지정 애플리케이션 포트 프로파일 생성


방화벽 및 NAT 규칙을 생성하기 위해 미리 구성된 애플리케이션 포트 프로파일 및 사용자 지정 애플리케이션 포트 프로파일을 사용할 수 있습니다.

애플리케이션 포트 프로파일에는 Edge 게이트웨이의 방화벽 및 NAT 서비스에 사용되는 프로토콜과 포트 또는 포트 그룹의 조합이 포함됩니다. NSX-T Data Center에 대해 미리 구성된 기본 포트 프로파일 외에도 사용자 지정 애플리케이션 포트 프로파일을 생성할 수 있습니다.

Edge 게이트웨이에서 사용자 지정 애플리케이션 포트 프로파일을 생성하면 동일한 조직 VDC에 있는 다른 모든 NSX-T Data Center Edge 게이트웨이에 표시됩니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- a 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- b 왼쪽 창에서 **Edge 게이트웨이**를 클릭합니다.
- c 대상 Edge 게이트웨이 이름 옆에 있는 라디오 버튼을 클릭하고 **서비스**를 클릭합니다.

- 2 Edge 게이트웨이를 클릭하고 **보안** 탭을 클릭합니다.
- 3 **애플리케이션 포트 프로파일**을 클릭합니다.
- 4 **사용자 지정 애플리케이션** 섹션에서 **새로 만들기**를 클릭합니다.
- 5 애플리케이션 포트 프로파일의 이름과 설명(선택 사항)을 입력합니다.
- 6 드롭다운 메뉴에서 프로토콜을 선택합니다.
- 7 포트 또는 포트 범위를 쉽표로 구분하여 입력하고 **저장**을 클릭합니다.

다음에 수행할 작업

애플리케이션 포트 프로파일을 사용하여 방화벽 및 NAT 규칙을 생성합니다. [NSX-T Edge 게이트웨이 방화벽 규칙 추가](#) 및 [NSX-T Edge 게이트웨이에 SNAT 또는 DNAT 규칙 추가](#) 항목을 참조하십시오.

전용 vCenter Server 인스턴스 및 프록시 관리

9

vCloud Director는 테넌트와 기본 vSphere 환경 사이에서 HTTP 프록시 서버로 작동할 수 있습니다. 전용 vCenter Server 인스턴스를 사용하면 vCloud Director를 vSphere 환경에 대한 CPOM(중앙 관리 지점)으로 사용할 수 있습니다.

vCenter Server 인스턴스를 vCloud Director에 추가할 때 인스턴스의 용도를 지정할 수 있습니다.

전용 vCenter Server

연결된 vCenter Server 인스턴스의 인프라가 SDDC(소프트웨어 정의 데이터 센터)로 캡슐화되고 단일 테넌트에만 전용으로 사용됩니다. 해당 인스턴스에 대한 테넌트 액세스를 사용하도록 설정하여 전용 vCenter Server 인스턴스를 생성합니다. 테넌트 액세스를 사용하도록 설정한 후에 전용 vCenter Server 인스턴스를 테넌트에 게시할 수 있습니다.

공유된 vCenter Server

제공자가 여러 제공자 VDC에서 vCenter Server 인스턴스의 여러 리소스 풀을 사용한 다음 해당 리소스 풀을 서로 다른 테넌트에 할당할 수 있습니다. 공유 vCenter Server 인스턴스는 테넌트에 게시할 수 없습니다.

없음

vCenter Server 인스턴스에는 특정 용도가 없습니다.

전용 vCenter Server 인스턴스를 사용하면 vCloud Director를 모든 vSphere 환경에 대한 중앙 관리 지점으로 사용할 수 있습니다.

- 해당하는 전용 vCenter Server를 해당 조직에만 게시하여 vCenter Server 인스턴스의 리소스를 단일 테넌트 전용으로 지정할 수 있습니다. 테넌트는 이 리소스를 다른 테넌트와 공유하지 않습니다. 테넌트는 VPN 없이 UI 또는 API 프록시를 사용하여 전용 vCenter Server 인스턴스에 액세스할 수 있습니다.
- vCloud Director를 경량 디렉토리로 사용하여 모든 vCenter Server 인스턴스를 등록할 수 있습니다.
- vCloud Director를 모든 vCenter Server 인스턴스에 대한 API 끝점으로 사용할 수 있습니다.

대상 vCenter Server 인스턴스를 vCloud Director에 연결하는 동안이나 연결한 후에 테넌트 액세스를 사용하도록 설정하고 vCenter Server 인스턴스를 전용으로 표시할 수 있습니다. [vCenter Server 인스턴스를 단독으로 또는 NSX Manager 인스턴스와 함께 연결](#) 항목을 참조하십시오.

연결된 vCenter Server 인스턴스를 사용하여 공유 vCenter Server 또는 전용 vCenter Server를 만들 수 있습니다. 공유 vCenter Server 인스턴스를 만들면 이 vCenter Server 인스턴스를 사용하여 전용 vCenter Server를 만들 수 없고, 그 반대의 경우에도 마찬가지입니다.

테넌트가 기본 vSphere 환경에 액세스하는 데 사용할 수 있는 프록시를 만들 수 있습니다. 사용자는 자신의 vCloud Director 계정을 사용하여 프록시를 통해 구성 요소의 UI 또는 API에 로그인할 수 있습니다.

vCloud Director의 전용 vCenter Server 인스턴스는 vCenter Server에 공개적으로 액세스할 수 있어야 하는 요구 사항을 제거합니다. 액세스를 제어하기 위해 vCloud Director에서 SDDC에 대한 테넌트 액세스를 사용하거나 사용하지 않도록 설정할 수 있습니다.

프록시는 SDDC의 구성 요소(예: vCenter Server 인스턴스, ESXi 호스트 또는 NSX Manager 인스턴스)에 대한 액세스 지점입니다. 프록시를 사용하거나 사용하지 않도록 설정하면 해당 프록시를 통해 테넌트 액세스를 허용하고 중지할 수 있습니다.

전용 vCenter Server 인스턴스 및 프록시 생성 및 관리

전용 vCenter Server 인스턴스 및 프록시를 만들고 관리하려면 서비스 제공자 관리 포털이나 vCloud OpenAPI를 사용하면 됩니다. vCloud OpenAPI는 <https://code.vmware.com>에서 "vCloud OpenAPI 시작하기" 항목을 참조하십시오.

중요 vCloud Director에는 전용 vCenter Server 인스턴스마다 직접 네트워크 연결이 필요합니다. vCenter Server 인스턴스가 외부 Platform Services Controller를 사용하는 경우, vCloud Director에는 Platform Services Controller에 대한 직접 네트워크 연결도 필요합니다.

프록시 설정된 전용 vCenter Server에서 VMware OVF Tool을 사용하려면 vCloud Director에 각 ESXi 호스트에 대한 직접 연결이 필요합니다.

1 전용 vCenter Server 인스턴스를 생성합니다.

vCloud Director 환경에 vCenter Server 인스턴스를 추가하는 경우 **vCenter Server 추가** 마법사에서 테넌트 액세스를 사용하도록 설정하여 전용 vCenter Server 인스턴스를 생성할 수 있습니다. vCenter Server 인스턴스를 연결하는 동안 이에 대한 프록시를 생성할 수도 있습니다. **vCenter Server 인스턴스 추가**의 내용을 참조하십시오. vCloud Director에 이미 추가되었지만 지정된 용도가 없는 vCenter Server 인스턴스에 대해 테넌트 액세스를 사용하도록 설정할 수 있습니다. **연결된 vCenter Server의 테넌트 액세스 사용**의 내용을 참조하십시오. 테넌트 액세스를 사용하도록 설정하면 vCenter Server 인스턴스가 테넌트에 게시될 수 있습니다.

2 프록시를 추가합니다.

vCenter Server 인스턴스를 vCloud Director에 연결할 때 또는 나중에 프록시를 생성할 수 있습니다. vCenter Server 인스턴스가 외부 Platform Services Controller를 사용하는 경우 vCloud Director는 Platform Services Controller에 대한 프록시도 생성합니다. 상위 및 하위 프록시를 사용하면 테넌트에서 특정 프록시를 숨기거나 상위 프록시를 통해 하위 프록시 그룹을 사용하거나 사용하지 않도록 설정할 수 있습니다. vCloud Director에 vCenter Server 인스턴스를 추가한 후 프록시를 생성하는 방법에 대한 자세한 내용은 **전용 vCenter Server에 대한 프록시 만들기** 항목을 참조하십시오.

vSphere 리소스 아래 **프록시** 탭에서 프록시를 편집하고, 사용하거나 사용하지 않도록 설정하고, 삭제할 수 있습니다. vCenter Server 인스턴스에 둘 이상의 프록시가 있는 경우 기본 프록시를 선택할 수 있습니다.

참고 전용 vCenter Server 인스턴스에 프록시를 추가할 때 인증서와 지문을 업로드해야 프록시 설정된 구성 요소가 자체 서명된 인증서를 사용하는 경우 테넌트가 인증서와 지문을 검색할 수 있습니다.

인증서와 CRL(인증서 해지 목록)을 살펴보고 관리하려면 [프록시 인증서 및 CRL 관리](#) 항목을 참조하십시오.

- 3 생성된 프록시의 인증서와 지문을 가져오고 인증서와 지문이 존재하며 올바른지 확인합니다. [프록시 인증서 및 CRL 관리](#)의 내용을 참조하십시오.

- 4 전용 vCenter Server 인스턴스를 하나 이상의 조직에 게시합니다.

전용 vCenter Server 인스턴스를 테넌트에 게시하여 vCloud Director Tenant Portal에 표시할 수 있습니다. 대부분의 경우 하나의 vCenter Server 인스턴스는 하나의 테넌트에만 게시되어야 합니다. [전용 vCenter Server 게시](#)의 내용을 참조하십시오.

- 5 테넌트가 vCloud Director Tenant Portal에서 전용 vCenter Server 인스턴스 및 프록시에 액세스할 수 있도록 설정하려면 해당 조직에 **CPOM 확장** 플러그인을 게시해야 합니다. [조직에서 플러그인 게시/게시 취소](#)의 내용을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [연결된 vCenter Server의 테넌트 액세스 사용](#)
- [전용 vCenter Server에 대한 프록시 만들기](#)
- [프록시 인증서 및 CRL 관리](#)
- [전용 vCenter Server 게시](#)

연결된 vCenter Server의 테넌트 액세스 사용


vCloud Director에 이미 추가되었지만 지정된 용도가 없는 vCenter Server 인스턴스에 대해 테넌트 액세스를 사용하도록 설정할 수 있습니다. 테넌트 액세스를 사용하도록 설정하면 전용 vCenter Server 인스턴스가 생성되어 테넌트에 게시할 수 있습니다.

연결된 vCenter Server 인스턴스를 사용하여 공유 vCenter Server 또는 전용 vCenter Server를 만들 수 있습니다. 공유 vCenter Server 인스턴스를 만들어서 전용 vCenter Server로 사용하려면, 먼저 vCenter Server 인스턴스의 리소스를 사용하고 있는 제공자 VDC(가상 데이터 센터)를 모두 삭제해야 합니다. 공유 vCenter Server 인스턴스에 연결된 제공자 VDC를 모두 삭제하면 해당 상태가 [없음]으로 변경됩니다.

사전 요구 사항

환경에 전용 또는 공유되지 않은 연결된 vCenter Server가 하나 이상 있는지 확인합니다.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **vCenter**를 클릭합니다.
- 3 **사용량** 열에서 지정된 용도가 없는 vCenter Server를 선택합니다.
- 4 **테넌트 액세스 사용**을 클릭합니다.

다음에 수행할 작업

[전용 vCenter Server 게시](#)의 내용을 참조하십시오.


전용 vCenter Server에 대한 프록시 만들기

테넌트가 기본 vSphere 환경에 액세스하는 데 사용할 수 있는 프록시를 만들 수 있습니다. vCloud Director에서 전용 vCenter Server 인스턴스에 대한 프록시를 생성할 수 있습니다.

사전 요구 사항

- vCloud Director 환경에서 테넌트 액세스를 사용하도록 설정된 vCenter Server 인스턴스가 하나 이상 있는지 확인합니다. [장 9 전용 vCenter Server 인스턴스 및 프록시 관리](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **vCenter**를 클릭합니다.
- 3 전용 vCenter Server 인스턴스를 선택합니다.
- 4 자세한 vCenter Server 정보가 포함된 페이지에서 **프록시** 탭을 클릭하고 **새로 만들기**를 클릭합니다.
- 5 새 프록시의 이름, 대상 호스트 및 UI URL을 입력합니다.
대상 호스트는 vCloud Director를 프록시로 사용할 구성 요소의 호스트 이름 또는 IP 주소입니다. 새 프록시의 UI URL은 테넌트가 프록시를 열 때 vCloud Director UI가 알려주는 URL입니다.
- 6 테넌트에 프록시가 보이도록 하려면 **테넌트에 표시** 옵션의 토글을 켭니다.
- 7 (선택 사항) **상위 프록시 선택**을 클릭하고 목록에서 프록시를 선택합니다.
- 8 **저장**을 클릭합니다.

다음에 수행할 작업

[프록시 인증서 및 CRL 관리](#).


프록시 인증서 및 CRL 관리

프록시 인증서와 CRL(인증서 해지 목록)을 살펴보고 다운로드하고 업로드할 수 있습니다.

사전 요구 사항

- vCloud Director 환경에서 테넌트 액세스를 사용하도록 설정된 vCenter Server 인스턴스가 하나 이상 있는지 확인합니다. [장 9 전용 vCenter Server 인스턴스 및 프록시 관리](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **프록시**를 클릭하고 프록시를 선택합니다.
- 3 **인증서 관리**를 클릭합니다.
- 4 인증서와 CRL을 업로드하거나 다운로드합니다.
- 5 **저장**을 클릭합니다.

전용 vCenter Server 게시


전용 vCenter Server를 테넌트에 게시하고 vCloud Director Tenant Portal을 통해 볼 수 있습니다. 기본적으로 하나의 vCenter Server는 하나의 테넌트에만 게시해야 합니다.

기본적으로 SDDC는 해당하는 전용 vCenter Server 인스턴스를 조직에만 게시하여 단일 테넌트에 전용으로 사용하는 vCenter Server 인스턴스입니다. 테넌트는 전용 vCenter Server 인스턴스 리소스를 다른 테넌트와 공유하지 않습니다. 전용 vCenter Server 인스턴스를 여러 테넌트에 게시하면 테넌트 경계를 위반합니다. 하지만 테넌트가 다수의 전용 vCenter Server 인스턴스에 액세스할 수 있어야 하는 경우가 있습니다. 이러한 경우에는 전용 vCenter Server 인스턴스를 여러 테넌트에 게시할 수 있습니다.

사전 요구 사항

- vCloud Director 환경에서 테넌트 액세스를 사용하도록 설정된 vCenter Server 인스턴스가 하나 이상 있는지 확인합니다. [장 9 전용 vCenter Server 인스턴스 및 프록시 관리](#)의 내용을 참조하십시오.

절차

- 1 기본 메뉴()에서 **vSphere 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **vCenter**를 클릭합니다.
- 3 테넌트 액세스를 사용하도록 설정된 vCenter Server를 선택합니다.

테넌트 액세스를 사용하도록 설정된 vCenter Server 인스턴스의 **사용량** 열에는 전용 값이 있습니다.

- 4 **테넌트 관리**를 클릭합니다.
- 5 vCenter Server 인스턴스를 게시할 테넌트를 하나 이상 선택합니다.
목록에서 테넌트의 선택을 취소하면 vCenter Server의 게시가 취소됩니다.
- 6 **저장**을 클릭합니다.

다음에 수행할 작업

사용자가 vCloud Director Tenant Portal에서 전용 vCenter Server 인스턴스 및 프록시에 액세스할 수 있도록 설정하려면 해당 조직에 **CPOM 확장** 플러그인을 게시해야 합니다. [조직에서 플러그인 게시/게시 취소](#)의 내용을 참조하십시오.

시스템 관리자 및 역할 관리

10

vCloud Director 서비스 제공자 관리자 포털을 사용하면 시스템 관리자를 vCloud Director에 개별적으로 추가하거나 LDAP 그룹의 일부로 추가할 수 있습니다. 조직 내에서 사용자가 갖는 권한을 결정하는 역할을 추가하고 수정할 수도 있습니다.

참고 vCloud Director 9.5부터는 서비스 제공자가 vCloud Director 서비스 제공자 관리자 포털을 사용하거나 vCloud OpenAPI를 사용하여 제공자 역할을 만들고 제공자 사용자와 그룹을 관리할 수 있습니다. 제공자 역할, 사용자 및 그룹 관리에 대한 자세한 내용은 "vCloud Director 서비스 제공자 관리자 포털 가이드"의 내용을 참조하십시오. vCloud OpenAPI 설명서를 보려면 https://vCloud_Director_IP_address_or_host_name/docs를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- 권한 및 역할 관리
- 제공자 사용자 및 그룹 관리

권한 및 역할 관리

권한은 vCloud Director에서 액세스 제어의 기본 단위입니다. 역할은 역할 이름과 권한 집합을 연결합니다. 각 조직은 서로 다른 권한과 역할을 가질 수 있습니다.

vCloud Director는 역할 및 역할에 연결된 권한을 사용하여, 사용자 또는 그룹에 작업을 수행할 수 있는 권한이 있는지 결정합니다. vCloud Director 가이드에 설명되어 있는 절차 대부분에는 사전 요구 사항에 특정 역할이 나와 있습니다. 이러한 전제 조건은 이름이 지정된 역할이 수정되지 않은 미리 정의된 역할이거나, 동등한 권한 집합을 가진 역할이라고 가정합니다.

vCloud Director 9.5에는 각 조직에서 사용 가능한 권한 및 역할을 관리하는 데 시스템 관리자가 사용할 수 있는 권한 번들과 글로벌 테넌트 역할이 도입되었습니다.

vCloud Director를 설치하면 시스템에서 사용할 수 있는 모든 권한이 포함된 시스템 권한 번들만이 시스템에 포함되어 있습니다. 시스템 권한 번들은 어떤 조직에도 게시되지 않습니다. 시스템에는 모든 조직에 게시되는 기본 제공 글로벌 테넌트 역할도 포함됩니다. 미리 정의된 역할에 대한 자세한 내용은 [미리 정의된 역할 및 역할 권한](#) 항목을 참조하십시오.

9.1 또는 이전 버전에서 vCloud Director를 업그레이드하면 시스템 권한 번들 외에 기존의 각 조직에 사용되는 레거시 권한 번들이 시스템에 포함됩니다. 각 레거시 권한 번들은 업그레이드 시 연결되었던 조직에서 사용할 수 있는 권한이 포함되며, 해당 조직에만 게시됩니다.

참고 기존 조직에 대한 권한 번들 모델을 사용하기 시작하려면 해당하는 레거시 권한 번들을 삭제해야 합니다.

vCloud Director 9.1 또는 이전 버전에서 업그레이드한 경우, 기존 역할 템플릿은 모든 조직에 글로벌 테넌트 역할로 게시되고, 역할 템플릿에서 연결 해제된 기존 역할은 해당하는 조직에서 테넌트별 역할로 사용할 수 있습니다.

권한 용어

권한

각 권한은 vCloud Director의 특정 개체 유형에 대한 보기 또는 관리 액세스를 제공합니다. 권한은 어떤 개체에 연결되는지에 따라 vApp, 카탈로그, 조직 등 서로 다른 범주에 속합니다. 제공자 조직에는 시스템에서 사용할 수 있는 모든 권한이 포함됩니다. 시스템 관리자는 각 조직에서 사용할 수 있는 권한을 정의합니다. vCloud Director에 포함되는 권한은 만들거나 수정할 수 없습니다.

권한 번들

시스템 관리자는 각 조직에서 사용할 수 있는 권한을 권한 번들을 사용하여 관리할 수 있습니다. 권한 번들은 시스템 관리자가 하나 이상의 조직에 게시할 수 있는 권한 집합입니다. 시스템 관리자는 서비스 계층, 별도로 비용을 부과할 수 있는 기능 또는 기타 임의의 권한 그룹에 해당하는 권한 번들을 만들고 게시할 수 있습니다. 권한 번들은 시스템 관리자만 보고 관리할 수 있습니다. 조직 하나에 여러 개의 번들을 게시할 수 있습니다.

조직 권한

조직 권한은 조직에서 사용할 수 있는 전체 권한 집합입니다. 조직 권한은 여러 개의 권한 번들로 구성될 수 있지만 조직 관리자 및 사용자에게는 테넌트별 역할을 만들고 수정하는 데 사용할 수 있는 모든 권한이 하나의 집합으로 표시됩니다.

역할 용어

역할

역할은 하나 이상의 사용자 및 그룹에 할당할 수 있는 권한 집합입니다. 사용자 또는 그룹을 만들거나 가져오는 경우에는 해당 사용자나 그룹에 역할을 할당해야 합니다.

제공자 역할

제공자 역할은 제공자 조직에서만 사용할 수 있는 역할 집합입니다. 제공자 역할은 제공자 사용자에게만 할당할 수 있습니다. 시스템 관리자는 사용자 지정 제공자 역할을 만들 수 있습니다.

테넌트 역할

테넌트 역할은 조직에서 사용할 수 있는 역할 집합입니다.

시스템 관리자는 글로벌 테넌트 역할을 만들고 편집하여 하나 이상의 조직에 게시할 수 있습니다. 글로벌 테넌트 역할은 해당 역할이 게시된 조직의 테넌트 사용자에게 할당할 수 있습니다. 조직 관리자는 글로벌 테넌트 역할을 편집할 수 없습니다.

참고 테넌트 사용자는 자신이 속한 조직에 게시된 역할에 포함되어 있는 권한만 사용할 수 있습니다.

테넌트별 역할

조직 관리자는 자신의 조직에만 해당하는 로컬 테넌트별 역할을 만들고 편집할 수 있습니다. 테넌트별 역할은 해당하는 조직 내의 테넌트 사용자에게만 할당할 수 있습니다. 테넌트별 역할은 조직 권한의 하위 집합만 포함할 수 있습니다.

테넌트별 역할 관리에 대한 자세한 내용은 "vCloud Director 테넌트 포털 가이드"의 내용을 참조하십시오.

미리 정의된 역할 및 역할 권한

미리 정의된 각 vCloud Director 역할에는 일반적인 워크플로에 들어 있는 작업을 수행하는 데 필요한 기본 권한 집합이 포함되어 있습니다. 기본적으로 미리 정의된 모든 글로벌 테넌트 역할은 시스템의 모든 조직에 게시됩니다.

미리 정의된 제공자 역할

기본적으로 제공자 조직에만 로컬인 제공자 역할은 **시스템 관리자** 및 **다중 사이트 시스템** 역할입니다. **시스템 관리자**는 추가 사용자 지정 제공자 역할을 만들 수 있습니다.

시스템 관리자

시스템 관리자 역할은 제공자 조직에만 있습니다. **시스템 관리자** 역할에는 시스템의 모든 권한이 포함되어 있습니다. **시스템 관리자** 역할에만 사용 가능한 권한 목록은 [시스템 관리자 권한](#)의 내용을 참조하십시오. **시스템 관리자** 자격 증명은 설치 및 구성 중에 설정됩니다. **시스템 관리자**는 제공자 조직에 추가 시스템 관리자 및 사용자 계정을 만들 수 있습니다.

다중 사이트 시스템

다중 사이트 배포에 대해 하트비트 프로세스를 실행하는 데 사용됩니다. 이 역할에는 유일한 권한 **다중 사이트: 시스템 작업**만 있으며, 이 권한은 사이트 연결의 원격 구성원 상태를 검색하는 vCloud API 요청을 수행하기 위한 사용 권한을 부여합니다.

미리 정의된 글로벌 테넌트 역할

미리 정의된 글로벌 테넌트 역할 및 이 역할에 포함된 권한은 기본적으로 모든 조직에 게시됩니다. **시스템 관리자**는 개별 조직에서 권한 및 글로벌 테넌트 역할을 게시 취소할 수 있습니다. **시스템 관리자**는 미리 정의된 글로벌 테넌트 역할을 편집하거나 삭제할 수 있습니다. **시스템 관리자**는 추가 글로벌 테넌트 역할을 만들고 게시할 수 있습니다.

조직 관리자

조직을 만든 후에는 **시스템 관리자**가 조직 내의 원하는 사용자에게 **조직 관리자** 역할을 할당할 수 있습니다. 미리 정의된 **조직 관리자** 역할이 있는 사용자는 조직 내의 사용자와 그룹을 관리하고, 미리 정의된 **조직 관리자** 역할을 비롯한 역할을 사용자와 그룹에 할당할 수 있습니다. **조직 관리자**가 만들거나 수정한 역할은 다른 조직에 표시되지 않습니다.

카탈로그 작성자

미리 정의된 **카탈로그 작성자** 역할과 연결된 권한이 있는 사용자는 카탈로그를 만들고 게시할 수 있습니다.

vApp 작성자

미리 정의된 **vApp 작성자** 역할과 연결된 권한이 있는 사용자는 카탈로그를 사용하고 vApp을 만들 수 있습니다.

vApp 사용자

미리 정의된 **vApp 사용자** 역할과 연결된 권한이 있는 사용자는 기존 vApp을 사용할 수 있습니다.

콘솔 액세스 전용

미리 정의된 **콘솔 액세스 전용** 역할과 연결된 권한이 있는 사용자는 가상 시스템 상태와 속성을 보고 게스트 OS를 사용할 수 있습니다.

ID 제공자로 지연

미리 정의된 **ID 제공자로 지연** 역할과 연결된 권한은 사용자의 OAuth 또는 SAML ID 제공자로부터 수신한 정보에 기반하여 결정됩니다. **ID 제공자로 지연** 역할에 사용자나 그룹을 할당할 때 자격이 되면 ID 제공자가 제공한 역할 또는 그룹 이름이 조직에 정의된 역할 또는 그룹 이름과 대/소문자를 구분하여 정확히 일치해야 합니다.


- 사용자가 OAuth ID 제공자에 의해 정의된 경우, 사용자의 OAuth 토큰의 **roles** 어레이에 명명된 역할이 사용자에게 할당됩니다.
- 사용자가 SAML ID 제공자에 의해 정의된 경우에는 SAML 특성에 명명된 역할이 사용자에게 할당됩니다. 이 이름은 조직의 **OrgFederationSettings**에 있는 **SamlAttributeMapping** 요소에 있는 **RoleAttributeName** 요소에 나타납니다.

ID 제공자로 지연 역할이 사용자에게 할당되었으나 조직에 일치하는 역할 또는 그룹 이름이 없는 경우 사용자가 조직에 로그인할 수 있지만 권한은 없습니다. ID 제공자가 사용자를 **시스템 관리자**와 같은 시스템 수준 역할에 연결한 경우 사용자는 조직에 로그인할 수 있지만 아무 권한도 없습니다. 이런 사용자에게 수동으로 역할을 할당해야 합니다.

ID 제공자로 지연 역할을 제외하고 미리 정의된 각각의 역할에는 기본 권한 집합이 포함되어 있습니다. 미리 정의된 역할에 포함된 권한은 **시스템 관리자**만 수정할 수 있습니다. **시스템 관리자**가 미리 정의된 역할을 수정하면 수정 사항은 시스템에서 해당 역할의 모든 인스턴스에 전파됩니다.

미리 정의된 글로벌 테넌트 역할의 권한

시스템 관리자는 Service Provider Admin Portal을 사용하여 역할에 포함되어 있는 권한 목록을 볼 수 있습니다.

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **역할**을 선택합니다.
- 3 보려는 역할의 이름을 클릭합니다.

조직 관리자는 Service Provider Admin Portal 또는 vCloud OpenAPI를 사용하여 역할에 포함된 권한을 보거나 조직의 로컬 역할을 만들 수 있습니다.

다양한 권한이 미리 정의된 다수의 글로벌 역할에 공통적입니다. 이러한 권한은 기본적으로 모든 새 조직에 부여되며 **조직 관리자**가 생성한 다른 역할에 사용할 수 있습니다. 미리 정의된 테넌트 역할의 권한 목록은 [미리 정의된 글로벌 테넌트 역할의 권한](#)의 내용을 참조하십시오.

시스템 관리자 권한

시스템 관리자 역할은 제공자 조직에만 있습니다. 기본적으로 **시스템 관리자** 역할에는 모든 vCloud Director 권한이 있습니다.

시스템 관리자 역할에는 모든 vCloud Director 권한이 있습니다. 이 목록은 **시스템 관리자**만 사용할 수 있는 권한으로 구성됩니다. **시스템 관리자** 역할에 [미리 정의된 글로벌 테넌트 역할의 권한](#)도 있습니다.

표 10-1. 시스템 관리자만 사용할 수 있는 권한

이 릴리스의 새로운 기능	권한 이름
	액세스 제어 목록: 관리
	액세스 제어 목록: 보기
	추가 서비스: 워크플로 실행
	추가 서비스: 실행 중인 워크플로 보기
	추가 서비스: 워크플로 보기
	리소스 풀 채택: 보기
	대체 관리자 엔티티: 보기
	AMQP 설정: 관리
	AMQP 설정: 보기
✓	API 탐색기: 보기
	카탈로그: vSphere에서 미디어 가져오기
	카탈로그: 새도 VM 보기
	카탈로그: VCSP 게시 구독 캐시

표 10-1. 시스템 관리자만 사용할 수 있는 권한 (계속)

이 릴리스의 새로운 기능	권한 이름
	셀 구성: 보기
	클라우드 터널 서버: 관리
	클라우드 터널 서버: 보기
	컨텐츠 라이브러리 시스템 설정: 관리
	컨텐츠 라이브러리 시스템 설정: 보기
	사용자 지정 엔티티: 사용자 지정 엔티티 정의 생성
	사용자 지정 엔티티: 사용자 지정 엔티티 정의 삭제
	사용자 지정 엔티티: 사용자 지정 엔티티 정의 편집
	사용자 지정 엔티티: 사용자 지정 엔티티 정의 보기
	데이터스토어: 삭제
	데이터스토어: 편집
	데이터스토어: 사용 또는 사용 안 함
	데이터스토어: vSphere에서 열기
	데이터스토어: 보기
	직접 조직 vDC 네트워크: 관리
	분산 가상 스위치: vSphere에서 열기
	Edge 클러스터: 관리
	Edge 클러스터: 보기
	확장 서비스 API 정의: 관리
	확장 서비스 API 정의: 보기
	확장 서비스: 보기
	확장: 보기
	외부 서비스: 관리
	외부 서비스: 보기
	일반: 오류 세부 정보 보기
	글로벌 역할: 편집
	글로벌 역할: 보기
	호스트: 사용 또는 사용 안 함

표 10-1. 시스템 관리자만 사용할 수 있는 권한 (계속)

이 릴리스의 새로운 기능	권한 이름
	호스트: 관리
	호스트: vSphere에서 열기
	호스트: 준비 또는 준비 취소
	호스트: 복구
	호스트: 업그레이드
	호스트: 보기
	Kerberos 설정: 관리
	Kerberos 설정: 보기
	LDAP 설정: 관리
	LDAP 설정: 보기
	라이선스 보고서: 보기
	지역화 리소스: 관리
	다중 사이트: 시스템 작업
	네트워크 풀: 만들기 또는 삭제
	네트워크 풀: 편집
	네트워크 풀: vSphere에서 열기
	네트워크 풀: 복구
	네트워크 풀: 보기
	NSX-T: 편집
	NSX-T: 보기
	개체 확장: 관리
	개체 확장: 보기
	조직 네트워크: 만들기 또는 삭제
	조직 네트워크: vSphere에서 열기
	조직 vDC 계산 정책: 관리 보기
	조직 vDC 계산 정책: 관리
	조직 vDC 분산 방화벽: 사용/사용 안 함
	조직 vDC 게이트웨이: BGP 라우팅 구성

표 10-1. 시스템 관리자만 사용할 수 있는 권한 (계속)

이 릴리스의 새로운 기능	권한 이름
	조직 vDC 게이트웨이: L2 VPN 구성
	조직 vDC 게이트웨이: OSPF 라우팅 구성
	조직 vDC 게이트웨이: 원격 액세스 구성
	조직 vDC 게이트웨이: SSL VPN 구성
	조직 vDC 게이트웨이: 시스템 로깅 구성
	조직 vDC 게이트웨이: 만들기
	조직 vDC 게이트웨이: 삭제
	조직 vDC 게이트웨이: 분산 라우팅
	조직 vDC 게이트웨이: 가져오기
	조직 vDC 게이트웨이: 폼 팩터 수정
	조직 vDC 게이트웨이: 업데이트
	조직 vDC 게이트웨이: 속성 업데이트
	조직 vDC 게이트웨이: 업그레이드
	조직 vDC 게이트웨이: BGP 라우팅 보기
	조직 vDC 게이트웨이: L2 VPN 보기
	조직 vDC 게이트웨이: OSPF 라우팅 보기
	조직 vDC 게이트웨이: 원격 액세스 보기
	조직 vDC 게이트웨이: SSL VPN 보기
	조직 vDC 네트워크: 가져오기
	조직 vDC 리소스 풀: vSphere에서 열기
	조직 vDC 리소스 풀: 보기
	조직 vDC 스토리지 정책: 편집
	조직 vDC 스토리지 정책: 사용 또는 사용 안 함
	조직 vDC 스토리지 정책: vSphere에서 열기
	조직 vDC 스토리지 정책: 제거
	조직 vDC: 만들기
	조직 vDC: 삭제
	조직 vDC: 사용 또는 사용 안 함

표 10-1. 시스템 관리자만 사용할 수 있는 권한 (계속)

이 릴리스의 새로운 기능	권한 이름
	조직 vDC: 확장된 편집
	조직 vDC: 확장된 보기
	조직: 활성화 또는 비활성화
	조직: 만들기 또는 삭제
	조직: 제한 편집
	조직: 이름 편집
	조직: 테넌트 스토리지 마이그레이션
	조직: 관리자 쿼리 수행
	조직: 테넌트로 제공자 LDAP 사용
	포트 그룹: vSphere에서 열기
	기본 설정: 기본 설정 정의 관리
	제공자 네트워크: 만들기 또는 삭제
	제공자 네트워크: 편집
	제공자 네트워크: vSphere에서 열기
	제공자 네트워크: 보기
	제공자 vDC 계산 정책: 관리
	제공자 vDC 계산 정책: 보기
	제공자 vDC 리소스 풀: VM 마이그레이션
	제공자 vDC 리소스 풀: vSphere에서 열기
	제공자 vDC 리소스 풀: 보기
	제공자 vDC 스토리지 정책: 편집
	제공자 vDC 스토리지 정책: 사용 또는 사용 안 함
	제공자 vDC 스토리지 정책: vSphere에서 열기
	제공자 vDC 스토리지 정책: 제거
	제공자 vDC 스토리지 정책: 보기
	제공자 vDC: 리소스 풀 추가
	제공자 vDC: 만들기 또는 삭제
	제공자 vDC: 리소스 풀 삭제

표 10-1. 시스템 관리자만 사용할 수 있는 권한 (계속)

이 릴리스의 새로운 기능	권한 이름
	제공자 vDC: 편집
	제공자 vDC: 사용 또는 사용 안 함
	제공자 vDC: 리소스 풀 사용 또는 사용 안 함
	제공자 vDC: vSphere VXLAN 사용
	제공자 vDC: 병합
	제공자 vDC: 보기
	VM 다시 로드: 관리
	리소스 클래스 작업: 관리
	리소스 클래스 작업: 보기
	리소스 풀: 열기
	리소스 풀: vSphere에서 열기
	리소스 풀: 보기
	권한: 관리
	권한: 보기
	권한 번들: 편집
	권한 번들: 보기
	SDDC: 관리
	SDDC: 프록시 관리
	SDDC: 보기
	선택기 확장: 관리
	선택기 확장: 보기
	서비스 애플리케이션: 관리
	서비스 애플리케이션: 보기
	서비스 인증: 관리
	서비스 구성: 관리
	서비스 구성: 보기
	서비스 라이브러리: 서비스 라이브러리 만들기
	서비스 라이브러리: 서비스 라이브러리에서 서비스 삭제

표 10-1. 시스템 관리자만 사용할 수 있는 권한 (계속)

이 릴리스의 새로운 기능	권한 이름
	서비스 라이브러리: 서비스 메타데이터 편집
	서비스 라이브러리: 서비스의 콘텐츠 편집
	서비스 링크: 관리
	서비스 링크: 보기
	서비스 리소스 유형: 관리
	서비스 리소스 유형: 보기
	서비스 리소스: 관리
	서비스 리소스: 보기
	공유 조직 vDC 네트워크: 관리
	사이트: 편집
	사이트: 보기
	격리된 항목: 관리
	격리된 항목: 보기
	시스템 작업: 시스템 작업 실행
	시스템 조직: 관리
	시스템 조직: 보기
	시스템 설정: 관리
	시스템 설정: 보기
	작업: 재개, 중단 또는 실패
	작업: 업데이트
	작업: 작업 보기
✓	토큰: 관리
✓	토큰: 모두 관리
	UI 플러그인: 정의, 업로드, 수정, 삭제, 연결 또는 연결 해제
	UI 포털 브랜딩: 관리
	vApp 템플릿: 스토리지 임대 만료 강제 적용
	vApp 템플릿: 가져오기
	vApp 템플릿: vSphere에서 열기

표 10-1. 시스템 관리자만 사용할 수 있는 권한 (계속)

이 릴리스의 새로운 기능	권한 이름
	vApp: 모든 추가 구성 허용
	vApp: 이더넷 병합 추가 구성 허용
	vApp: 지연 시간 추가 구성 허용
	vApp: 일치하는 추가 구성 허용
	vApp: NUMA 노드 선호도 추가 구성 허용
	vApp: 모든 VDC 유형에서 VM CPU 및 메모리 예약 설정 편집
	vApp: 유지 보수 모드 시작/종료
	vApp: 런타임 임대 만료 강제 적용
	vApp: 스토리지 임대 만료 강제 적용
	vApp: 가져오기 옵션
	vApp: 유지 보수 관리
	vApp: vSphere에서 열기
	vApp: 새로 VM 보기
	vApp: VM 규정 준수 검사
	vApp: VM 마이그레이션, 강제 배포 해제, 재배포, 통합
	VCD 확장: 등록, 등록 취소, 새로 고침, 연결 또는 연결 해제
	VCD 확장: 보기
	vCenter: 연결 또는 분리
	vCenter: 사용 또는 사용 안 함
	vCenter: vSphere에서 열기
	vCenter: 새로 고침
	vCenter: 보기
	vDC 그룹: 구성
	vDC 그룹: 보기
	VDC 템플릿: ACL 관리
	VDC 템플릿: 확장된 보기
	VDC 템플릿: 관리
	VMC: SDDC 등록

표 10-1. 시스템 관리자만 사용할 수 있는 권한 (계속)

이 릴리스의 새로운 기능	권한 이름
	vRealize Orchestrator: 테넌트에 대한 워크플로 게시 및 게시 취소
	vRealize Orchestrator: vRealize Orchestrator 서버 등록 및 등록 취소
	vRealize Orchestrator: 등록된 vRealize Orchestrator 서버 보기
	vSphere 서버: 관리
	vSphere 서버: 프록시 관리
	vSphere 서버: 보기

미리 정의된 글로벌 테넌트 역할의 권한

다양한 권한이 미리 정의된 다수의 글로벌 역할에 공통적입니다. 이러한 권한은 기본적으로 모든 새 조직에 부여되며 **조직 관리자**가 생성한 다른 역할에 사용할 수 있습니다.

vCloud Director의 글로벌 테넌트 역할에 포함된 권한

이 릴리스의 새로운 기능	권한 이름	조직 관리자	카탈로그 작성자	vApp 작성자	vApp 사용자	콘솔 액세스 전용
	모든 조직 VDC 액세스	✓				
	카탈로그: 내 클라우드의 vApp 추가	✓	✓	✓		
	카탈로그: 소유자 변경	✓				
	카탈로그: CLSP 게시 구독	✓	✓			
	카탈로그: 카탈로그 만들기/삭제	✓	✓			
	카탈로그: 속성 편집	✓	✓			
	카탈로그: 게시	✓	✓			
	카탈로그: 공유	✓	✓			
	카탈로그: ACL 보기	✓	✓			
	카탈로그: 개인 및 공유 카탈로그 보기	✓	✓	✓		
	카탈로그: 게시된 카탈로그 보기	✓				
	사용자 지정 엔티티: 조직의 모든 사용자 지정 엔티티 인스턴스 보기	✓				

이 릴리스의 새로운 기능	권한 이름	조직 관리자	카탈로그 작성자	vApp 작성자	vApp 사용자	콘솔 액세스 전용
	사용자 지정 엔티티: 사용자 지정 엔티티 인스턴스 보기	✓				
	디스크: 소유자 변경	✓	✓			
	디스크: 만들기	✓	✓	✓		
	디스크: 삭제	✓	✓	✓		
	디스크: 속성 편집	✓	✓	✓		
	디스크: 속성 보기	✓	✓	✓	✓	
	일반: 관리자 제어	✓				
	일반: 관리자 보기	✓				
	일반: 알림 보내기	✓				
	그룹/사용자: 보기	✓				
	하이브리드 클라우드 작업: 제어 티켓 획득	✓				
	하이브리드 클라우드 작업: 클라우드 역터널 티켓 획득	✓				
	하이브리드 클라우드 작업: To-the-Cloud 터널 티켓 확보	✓				
	하이브리드 클라우드 작업: 클라우드 역터널 만들기	✓				
	하이브리드 클라우드 작업: To-the-Cloud 터널 만들기	✓				
	하이브리드 클라우드 작업: 클라우드 역터널 삭제	✓				
	하이브리드 클라우드 작업: To-the-Cloud 터널 삭제	✓				
	하이브리드 클라우드 작업: 클라우드 역터널 끝점 태그 업데이트	✓				
	하이브리드 클라우드 작업: 클라우드 역터널 보기	✓				
	하이브리드 클라우드 작업: To-the-Cloud 터널 보기	✓				
	조직 네트워크: 속성 편집	✓				
	조직 네트워크: 보기	✓				
	조직 vDC 계산 정책: 보기	✓	✓	✓	✓	

이 릴리스의 새로운 기능	권한 이름	조직 관리자	카탈로그 작성자	vApp 작성자	vApp 사용자	콘솔 액세스 전용
	조직 vDC 분산 방화벽: 규칙 구성	✓				
	조직 vDC 분산 방화벽: 규칙 보기	✓				
	조직 vDC 게이트웨이: DHCP 구성	✓				
✓	조직 vDC 게이트웨이: DNS 구성	✓				
✓	조직 vDC 게이트웨이: ECMP 라우팅 구성	✓				
	조직 vDC 게이트웨이: 방화벽 구성	✓				
	조직 vDC 게이트웨이: IPSec VPN 구성	✓				
	조직 vDC 게이트웨이: 로드 밸런서 구성	✓				
	조직 vDC 게이트웨이: NAT 구성	✓				
	조직 vDC 게이트웨이: 정적 라우팅 구성	✓				
	조직 vDC 게이트웨이: Syslog 구성	✓				
	조직 vDC 게이트웨이: 고급 네트워킹으로 변환	✓				
	조직 vDC 게이트웨이: 보기	✓				
	조직 vDC 게이트웨이: DHCP 보기	✓				
✓	조직 vDC 게이트웨이: DNS 보기	✓				
	조직 vDC 게이트웨이: 방화벽 보기	✓				
	조직 vDC 게이트웨이: IPSec VPN 보기	✓				
	조직 vDC 게이트웨이: 로드 밸런서 보기	✓				
	조직 vDC 게이트웨이: NAT 보기	✓				
	조직 vDC 게이트웨이: 정적 라우팅 보기	✓				

이 릴리스의 새로운 기능	권한 이름	조직 관리자	카탈로그 작성자	vApp 작성자	vApp 사용자	콘솔 액세스 전용
	조직 vDC 네트워크: 속성 편집	✓				
	조직 vDC 네트워크: 속성 보기	✓		✓		
	조직 vDC 스토리지 프로파일: 기본값 설정	✓				
	조직 vDC: 편집	✓				
	조직 vDC: ACL 편집	✓				
	조직 vDC: 방화벽 관리	✓				
	조직 vDC: 보기	✓	✓			
	조직 vDC: ACL 보기	✓				
	조직 vDC: 메트릭 보기	✓				
	조직 vDC: VM-VM 선호도 편집	✓	✓	✓		
	조직: 연결 설정 편집	✓				
	조직: 페더레이션 설정 편집	✓				
	조직: LDAP 설정 편집	✓				
	조직: 임대 정책 편집	✓				
	조직: OAuth 설정 편집	✓				
	조직: 암호 정책 편집	✓				
	조직: 속성 편집	✓				
	조직: 할당량 정책 편집	✓				
	조직: SMTP 설정 편집	✓				
	조직: VDC ACL 편집 중 IdP에서 사용자/그룹 가져오기	✓				
	조직: 보기	✓	✓	✓		
	조직: 메트릭 보기	✓				
	역할: 만들기, 편집, 삭제 또는 복사	✓				
	서비스 라이브러리: 서비스 라이브러리 보기	✓				
	UI 플러그인: 보기	✓	✓	✓	✓	
	vApp 템플릿/미디어: 복사	✓	✓	✓		

이 릴리스의 새로운 기능	권한 이름	조직 관리자	카탈로그 작성자	vApp 작성자	vApp 사용자	콘솔 액세스 전용
	vApp 템플릿/미디어: 만들기/업로드	✓	✓			
	vApp 템플릿/미디어: 편집	✓	✓	✓		
	vApp 템플릿/미디어: 보기	✓	✓	✓	✓	
	vApp 템플릿: 소유자 변경	✓	✓			
	vApp 템플릿: 체크 아웃	✓	✓	✓	✓	
	vApp 템플릿: 다운로드	✓	✓			
	vApp : 소유자 변경	✓				
	vApp : 복사	✓	✓	✓	✓	
	vApp : 만들기/재구성	✓	✓	✓		
	vApp : 삭제	✓	✓	✓	✓	
	vApp : 다운로드	✓	✓	✓		
	vApp : 속성 편집	✓	✓	✓	✓	
	vApp : VM 계산 정책 편집	✓	✓	✓		
	vApp : VM CPU 편집	✓	✓	✓		
	vApp : VM 하드 디스크 편집	✓	✓	✓		
	vApp : VM 메모리 편집	✓	✓	✓		
	vApp : VM 네트워크 편집	✓	✓	✓	✓	
	vApp : VM 속성 편집	✓	✓	✓	✓	
	vApp : VM 암호 설정 관리	✓	✓	✓	✓	✓
	vApp : 전원 작업	✓	✓	✓	✓	
	vApp : 공유	✓	✓	✓	✓	
	vApp : 스냅샷 작업	✓	✓	✓	✓	
	vApp : 업로드	✓	✓	✓		
	vApp : 콘솔 사용	✓	✓	✓	✓	✓
	vApp : ACL 보기	✓	✓	✓	✓	
	vApp : VM 메트릭 보기	✓		✓	✓	
	vApp : VM 부팅 옵션	✓	✓	✓		
	vApp : vCenter에 대한 VM 메타데이터	✓	✓	✓		

이 릴리스의 새로운 기능	권한 이름	조직 관리자	카탈로그 작성자	vApp 작성자	vApp 사용자	콘솔 액세스 전용
	VDC 템플릿: 인스턴스화	✓				
	VDC 템플릿: 보기	✓				


권한 번들 관리

시스템 관리자는 권한 번들을 만들어 클라우드에 있는 하나 이상의 조직에 게시할 수 있습니다. 기존 권한 번들을 편집하고 삭제할 수 있습니다. 클라우드에 있는 조직에서 권한 번들을 게시 취소할 수 있습니다.

권한 번들 만들기

권한 집합을 권한 번들로 그룹화하여 시스템에 있는 하나 이상의 조직에 게시할 수 있습니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **테넌트 액세스 제어** 아래에서 **권한 번들**을 클릭합니다.
- 3 **추가**를 클릭합니다.
- 4 새 권한 번들의 이름과 설명(선택 사항)을 입력합니다.
- 5 이 번들에 연결할 권한을 선택합니다.

권한은 연결된 해당 개체에 대한 보기 또는 관리 액세스를 위한 범주 및 하위 범주로 그룹화됩니다.

하위 범주별 보기 또는 관리 권한 또는 글로벌 보기 또는 관리 권한을 개별적으로 선택할 수 있습니다.

범주	설명
액세스 제어	조직, 권한, 역할 및 사용자를 보고 관리하는 권한이 포함됩니다.
관리	일반 설정 및 다중 사이트 설정을 보고 관리하는 권한이 포함됩니다.
계산	조직 및 제공자 VDC, vApp, 조직 VDC 템플릿 및 VM 모니터링을 보고 관리하는 권한이 포함됩니다.
확장	vCloud Director 플러그인과 확장을 보고 관리하는 권한이 포함됩니다.
인프라	vSphere 리소스를 보고 관리하는 권한이 포함됩니다.
라이브러리	카탈로그 및 카탈로그 항목을 보고 관리하는 권한이 포함됩니다.
네트워킹	네트워크 리소스를 보고 관리하는 권한이 포함됩니다.

- 6 **저장**을 클릭합니다.

다음에 수행할 작업


새로 만든 권한 번들은 시스템에 있는 하나 이상의 조직에 게시할 수 있습니다. [권한 번들 게시 또는 게시 취소](#)의 내용을 참조하십시오.

권한 번들 게시 또는 게시 취소

권한 번들은 시스템에 있는 하나 이상의 조직에 게시할 수 있습니다. 조직에 권한 번들을 게시하면 이 번들에 포함된 권한이 조직 권한 집합의 일부가 됩니다.

조직 권한은 여러 개의 권한 번들로 구성될 수 있지만 조직 관리자 및 사용자에게는 역할을 만들고 수정하는 데 사용할 수 있는 모든 권한이 하나의 집합으로 표시됩니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **테넌트 액세스 제어** 아래에서 **권한 번들**을 클릭합니다.
- 3 대상 번들 옆에 있는 라디오 버튼을 선택하고 **게시**를 클릭합니다.
- 4 번들을 게시하려면 다음을 수행합니다.
 - a **테넌트에 게시**를 선택합니다.
 - b 역할을 게시할 대상 조직을 선택합니다.
 - 시스템에 있는 기존 조직 및 새로 만든 조직 모두에 번들을 게시하려면 **모든 테넌트에 게시**를 선택합니다.
 - 시스템에 있는 특정 조직에 번들을 게시하려면 조직을 개별적으로 선택합니다.
- 5 번들을 게시 취소하려면 다음을 수행합니다.
 - 시스템에 있는 모든 조직에서 번들을 게시 취소하려면 **테넌트에 게시**를 선택 취소합니다.
 - 시스템에 있는 특정 조직에서 번들을 게시 취소하려면 **모든 테넌트에 게시**를 선택 취소한 후 조직을 개별적으로 선택 취소합니다.
- 6 **저장**을 클릭합니다.

결과


게시된 번들에 포함된 권한은 선택된 조직에서 사용할 수 있으며 해당 조직 내의 역할에 사용할 수 있습니다.

게시 취소된 번들에 포함된 권한은 선택된 조직에서 제거되며 해당 조직 내의 역할에 사용할 수 없습니다.

권한 번들 보기 및 편집

권한 번들에 포함된 권한을 볼 수 있습니다. 번들의 이름, 설명 및 권한을 수정할 수 있습니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.

2 왼쪽 패널의 **테넌트 액세스 제어** 아래에서 **권한 번들**을 클릭합니다.

3 대상 번들의 이름을 클릭합니다.

권한 범주를 확장하여 번들에 연결된 권한을 볼 수 있습니다.

4 번들을 편집하고 **유지**를 클릭합니다.


결과

번들의 권한을 수정하면 이 권한 번들이 게시된 모든 조직에 새 권한 집합이 적용됩니다.

권한 번들 삭제

조직에서 더 이상 사용하지 않는 권한 번들을 제거할 수 있습니다.

절차

1 기본 메뉴()에서 **관리**를 선택합니다.

2 왼쪽 패널의 **테넌트 액세스 제어** 아래에서 **권한 번들**을 클릭합니다.

3 대상 번들 옆에 있는 라디오 버튼을 선택하고 **삭제**를 클릭합니다.

4 **확인**을 클릭하여 확인합니다.

글로벌 테넌트 역할 관리

시스템 관리자는 글로벌 테넌트 역할을 만들어 클라우드에 있는 하나 이상의 조직에 게시할 수 있습니다. 기존의 글로벌 테넌트 역할을 편집하고 삭제할 수 있습니다. 클라우드에 있는 개별 조직에서 글로벌 테넌트 역할을 게시 취소할 수 있습니다.

초기 vCloud Director 설치 및 설정 후에는 모든 조직에 게시되는 미리 정의된 글로벌 테넌트 역할 집합이 시스템에 포함됩니다. [미리 정의된 역할 및 역할 권한](#)의 내용을 참조하십시오.


글로벌 테넌트 역할 만들기

시스템의 조직 하나 이상에 게시할 수 있는 글로벌 테넌트 역할을 만들 수 있습니다.

초기 vCloud Director 설치 및 설정 후에는 모든 조직에 게시되는 미리 정의된 글로벌 테넌트 역할이 시스템에 포함됩니다. 미리 정의된 역할에 대한 자세한 내용은 [미리 정의된 역할 및 역할 권한](#) 항목을 참조하십시오.

시스템에 사용자 지정 글로벌 역할을 추가할 수 있습니다.

절차

1 기본 메뉴()에서 **관리**를 선택합니다.

2 왼쪽 패널의 **테넌트 액세스 제어** 아래에서 **글로벌 역할**을 클릭합니다.

3 **추가**를 클릭합니다.

4 새 역할의 이름과 설명(선택 사항)을 입력합니다.

5 이 역할에 연결할 권한을 선택합니다.

권한은 연결된 해당 개체에 대한 보기 또는 관리 액세스를 위한 범주 및 하위 범주로 그룹화됩니다.

하위 범주별 보기 또는 관리 권한 또는 글로벌 보기 또는 관리 권한을 개별적으로 선택할 수 있습니다.

범주	설명
액세스 제어	조직, 권한, 역할 및 사용자를 보고 관리하는 권한이 포함됩니다.
관리	일반 설정 및 다중 사이트 설정을 보고 관리하는 권한이 포함됩니다.
계산	조직 및 제공자 VDC, vApp, 조직 VDC 템플릿 및 VM 모니터링을 보고 관리하는 권한이 포함됩니다.
확장	vCloud Director 플러그인과 확장을 보고 관리하는 권한이 포함됩니다.
인프라	vSphere 리소스를 보고 관리하는 권한이 포함됩니다.
라이브러리	카탈로그 및 카탈로그 항목을 보고 관리하는 권한이 포함됩니다.
네트워킹	네트워크 리소스를 보고 관리하는 권한이 포함됩니다.

6 유지를 클릭합니다.

결과

생성 시 새 글로벌 테넌트 권한은 vCloud Director 제공자 조직에서만 사용할 수 있습니다.

다음에 수행할 작업

새로 만든 역할은 시스템에 있는 하나 이상의 조직에 게시할 수 있습니다. [글로벌 테넌트 역할 게시 또는 게시 취소](#)의 내용을 참조하십시오.


글로벌 테넌트 역할 게시 또는 게시 취소

글로벌 테넌트 역할은 시스템에 있는 하나 이상의 조직에 게시할 수 있습니다. 조직에 역할을 게시하면 이 역할은 해당 조직 테넌트 역할 집합의 일부가 됩니다.

사전 요구 사항

조직에서 글로벌 테넌트 역할을 게시 취소하려는 경우에는 조직 내에 이 역할이 할당된 사용자가 없는지 확인해야 합니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **테넌트 액세스 제어** 아래에서 **글로벌 역할**을 클릭합니다.
- 3 대상 역할 옆에 있는 라디오 버튼을 선택하고 **게시**를 클릭합니다.

4 역할을 게시하려면 다음을 수행합니다.

a **테넌트에 게시**를 선택합니다.

b 역할을 게시할 대상 조직을 선택합니다.

- 시스템에 있는 기존 조직 및 새로 만든 조직 모두에 역할을 게시하려면 **모든 테넌트에 게시**를 선택합니다.
- 시스템에 있는 특정 조직에 역할을 게시하려면 조직을 개별적으로 선택합니다.

5 역할을 게시 취소하려면 다음을 수행합니다.

- 시스템에 있는 모든 조직에서 역할을 게시 취소하려면 **테넌트에 게시**를 선택 취소합니다.
- 시스템에 있는 특정 조직에서 역할을 게시 취소하려면 **모든 테넌트에 게시**를 선택 취소한 후 조직을 개별적으로 선택 취소합니다.

6 **저장**을 클릭합니다.**결과**


게시된 역할은 선택된 조직에서 사용할 수 있으며 해당 조직 내의 사용자에게 할당할 수 있습니다. 조직 관리자는 자신의 조직에 게시된 글로벌 테넌트 역할을 편집할 수 없습니다.

게시 취소된 역할은 선택된 조직에서 제거되며, 해당 조직 내의 사용자에게 할당할 수 없습니다.

글로벌 테넌트 역할 보기 및 편집

글로벌 테넌트 역할에 포함된 권한을 볼 수 있습니다. 글로벌 테넌트 역할의 이름, 설명 및 권한을 수정할 수 있습니다.

절차

- 1** 기본 메뉴()에서 **관리**를 선택합니다.
- 2** 왼쪽 패널의 **테넌트 액세스 제어** 아래에서 **글로벌 역할**을 클릭합니다.
- 3** 대상 역할의 이름을 클릭합니다.
권한 범주를 확장하여 역할에 연결된 권한을 볼 수 있습니다.
- 4** 역할의 이름, 설명 또는 권한을 수정하려면 **편집**을 클릭합니다.
- 5** 역할을 편집하고 **유지**를 클릭합니다.

결과

역할의 권한을 수정하면 모든 조직에서 이 역할이 할당된 사용자에게 새 권한 집합이 적용됩니다.


글로벌 테넌트 역할 삭제

조직에서 더 이상 사용하지 않는 글로벌 테넌트 역할을 제거할 수 있습니다.

사전 요구 사항

삭제할 글로벌 테넌트 역할이 모든 조직의 어느 사용자에게도 할당되어 있지 않아야 합니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **테넌트 액세스 제어** 아래에서 **글로벌 역할**을 클릭합니다.
- 3 대상 역할 옆에 있는 라디오 버튼을 선택하고 **삭제**를 클릭합니다.
- 4 **확인**을 클릭하여 확인합니다.

제공자 역할 관리

vCloud Director 제공자 조직에 역할을 만들고 관리할 수 있습니다.

테넌트 역할 관리에 대한 자세한 내용은 "vCloud Director 테넌트 포털 가이드"의 내용을 참조하십시오.


제공자 역할 만들기

vCloud Director 제공자 조직에 역할을 만들 수 있습니다.

초기 vCloud Director 설치 및 설정 후에는 제공자 조직의 로컬 역할 및 모든 조직의 글로벌 역할로 사용되는 미리 정의된 역할이 시스템에 포함됩니다. 미리 정의된 역할에 대한 자세한 내용은 [미리 정의된 역할 및 역할 권한](#) 항목을 참조하십시오.

제공자 조직에 사용자 지정 제공자 역할을 추가할 수 있습니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **역할**을 클릭합니다.
- 3 **새로 만들기**를 클릭합니다.
- 4 새 역할의 이름과 설명(선택 사항)을 입력합니다.
- 5 이 역할에 연결할 권한을 선택합니다.

권한은 연결된 해당 개체에 대한 보기 또는 관리 액세스를 위한 범주 및 하위 범주로 그룹화됩니다.

하위 범주별 보기 또는 관리 권한 또는 글로벌 보기 또는 관리 권한을 개별적으로 선택할 수 있습니다.

범주	설명
액세스 제어	조직, 권한, 역할 및 사용자를 보고 관리하는 권한이 포함됩니다.
관리	일반 설정 및 다중 사이트 설정을 보고 관리하는 권한이 포함됩니다.
계산	조직 및 제공자 VDC, vApp, 조직 VDC 템플릿 및 VM 모니터링을 보고 관리하는 권한이 포함됩니다.

범주	설명
확장	vCloud Director 플러그인과 확장을 보고 관리하는 권한이 포함됩니다.
인프라	vSphere 리소스를 보고 관리하는 권한이 포함됩니다.
라이브러리	카탈로그 및 카탈로그 항목을 보고 관리하는 권한이 포함됩니다.
네트워킹	네트워크 리소스를 보고 관리하는 권한이 포함됩니다.

6 저장을 클릭합니다.


결과

새로 만든 역할은 제공자 조직의 사용자에게 할당할 수 있습니다.

제공자 역할 보기 또는 편집

vCloud Director 제공자 조직의 로컬 역할에 포함된 권한을 볼 수 있습니다. 역할의 이름, 설명 및 권한을 수정할 수 있습니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **역할**을 클릭합니다.
- 3 대상 역할의 이름을 클릭합니다.
권한 범주를 확장하여 역할에 연결된 권한을 볼 수 있습니다.
- 4 역할의 이름, 설명 또는 권한을 수정하려면 **편집**을 클릭합니다.
- 5 역할을 편집하고 **저장**을 클릭합니다.

결과

역할의 권한을 수정하면 이 역할이 할당된 사용자에게 새 권한 집합이 적용됩니다.


제공자 역할 삭제

vCloud Director 제공자 조직에서 더 이상 사용하지 않는 역할을 제거할 수 있습니다.

사전 요구 사항

삭제할 역할이 사용자에게 할당되어 있지 않아야 합니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **역할**을 클릭합니다.

3 대상 역할 옆에 있는 라디오 버튼을 선택하고 **삭제**를 클릭합니다.

4 **확인**을 클릭하여 확인합니다.

제공자 사용자 및 그룹 관리

vCloud Director 제공자 조직에 사용자 및 그룹을 추가하고 가져올 수 있습니다.

조직 사용자 및 그룹 관리에 대한 자세한 내용은 "vCloud Director 테넌트 포털 가이드"의 내용을 참조하십시오.

제공자 사용자 관리

Service Provider Admin Portal을 사용하여 제공자 조직에 속한 사용자를 관리할 수 있습니다.


조직의 테넌트 사용자 관리에 대한 자세한 내용은 "vCloud Director 테넌트 포털 가이드"의 내용을 참조하십시오.

제공자 사용자 만들기

vCloud Director 제공자 조직에 사용자를 만들 수 있습니다.

vCloud Director 설치 및 설정 중에는 **시스템 관리자** 계정을 만듭니다. 초기 설정 이후에는 제공자 조직에 추가적인 관리자와 사용자를 만들 수 있습니다.

절차

- 1** 기본 메뉴()에서 **관리**를 선택합니다.
- 2** 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **사용자**를 클릭합니다.
- 3** **새로 만들기**를 클릭합니다.
- 4** 새 사용자의 사용자 이름과 암호를 입력합니다.
암호는 6자 이상이어야 합니다.
- 5** 생성 시 사용자를 사용하도록 설정할지 여부를 선택합니다.
- 6** **사용 가능한 역할** 드롭다운 메뉴에서 사용자의 역할을 선택합니다.
사용 가능한 역할 목록은 글로벌 역할 및 사용자 시스템 조직의 로컬 역할로 구성됩니다.
- 7** (선택 사항) 사용자의 연락처 정보를 입력합니다.
전체 이름, e-메일 주소, 전화 번호 및 메신저 ID를 입력할 수 있습니다.
- 8** (선택 사항) 사용자의 할당량을 설정합니다.
 - a** 사용자 소유의 가상 시스템에 제한을 설정하거나, **무제한**을 선택할 수 있습니다.
 - b** 사용자 소유의 실행 중인 가상 시스템에 제한을 설정하거나, **무제한**을 선택할 수 있습니다.


제공자 사용자 가져오기

이전에 구성된 LDAP 또는 SAML ID 제공자에서 vCloud Director 제공자 조직으로 사용자를 가져올 수 있습니다.

사전 요구 사항

시스템 LDAP 연결 구성 또는 SAML ID 제공자를 사용하도록 시스템 구성 작업을 수행합니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **사용자**를 클릭합니다.
- 3 **사용자 가져오기**를 클릭합니다.
- 4 소스 드롭다운 메뉴에서 ID 제공자 유형을 선택합니다.

LDAP 또는 SAML일 수 있습니다.

ID 제공자를 하나만 구성한 경우에는 이 옵션이 하드 코딩됩니다.

- 5 사용자를 지정합니다.

옵션	설명
LDAP	<ol style="list-style-type: none"> a 사용자의 전체 또는 일부 이름을 입력하고 검색을 클릭합니다. b 가져올 사용자를 검색 결과에서 선택합니다. c 역할 할당 드롭다운 메뉴에서 가져온 사용자를 위한 역할을 선택합니다.
SAML	<ol style="list-style-type: none"> a 가져올 사용자의 사용자 이름을 SAML ID 제공자가 지원하는 이름 식별자 형식으로 입력합니다. 각 사용자 이름을 새 줄에 입력합니다. b 역할 할당 드롭다운 메뉴에서 가져온 사용자를 위한 역할을 선택합니다.

- 6 **저장**을 클릭합니다.


결과

가져온 사용자를 사용자 목록에서 볼 수 있습니다.

제공자 사용자 편집

제공자 조직에 속한 사용자의 암호, 역할, 연락처 정보 및 할당량을 변경할 수 있습니다. 사용자 이름은 변경할 수 없습니다.

절차


- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **사용자**를 클릭합니다.
- 3 대상 사용자의 이름 옆에 있는 라디오 버튼을 클릭하고 **편집**을 클릭합니다.

- 4 사용자 세부 정보를 편집하고 **저장**을 클릭합니다.

제공자 사용자 사용 안 함 또는 사용

사용자를 사용하지 않도록 설정하면 해당 사용자가 vCloud Director에 로그인할 수 없습니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **사용자**를 클릭합니다.
- 3 대상 사용자의 이름 옆에 있는 라디오 버튼을 클릭하고 **사용 안 함** 또는 **사용**을 클릭합니다.
- 4 사용자를 사용하지 않도록 설정하는 경우, **확인**을 클릭하여 확인합니다.


제공자 사용자 삭제

사용자 계정을 삭제하여 vCloud Director 제공자 조직에서 사용자를 제거할 수 있습니다.

사전 요구 사항

삭제할 사용자를 사용하지 않도록 설정합니다. [제공자 사용자 사용 안 함 또는 사용](#)의 내용을 참조하십시오.

절차


- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **사용자**를 클릭합니다.
- 3 대상 사용자의 이름 옆에 있는 라디오 버튼을 클릭하고 **삭제**를 클릭합니다.
- 4 **확인**을 클릭하여 확인합니다.

제공자 사용자 잠금 해제

암호 정책 시스템 설정에서 계정 잠금을 사용하도록 설정한 경우, 사용자의 로그인이 지정된 횟수만큼 실패하면 해당 계정이 잠길 수 있습니다. 계정 잠금 간격이 설정되어 있더라도 잠금이 만료될 때까지 기다리지 않고 사용자 계정을 잠금 해제할 수 있습니다.

계정 잠금 정책 구성에 대한 자세한 내용은 [암호 정책 구성](#) 항목을 참조하십시오.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **사용자**를 클릭합니다.
- 3 대상 사용자의 이름 옆에 있는 라디오 버튼을 클릭하고 **잠금 해제**를 클릭합니다.

제공자그룹 관리

Service Provider Admin Portal을 사용하여 제공자 조직에서 그룹 가져오기, 편집 및 삭제를 수행할 수 있습니다.

조직의 그룹 관리에 대한 자세한 내용은 "vCloud Director 테넌트 포털 가이드"의 내용을 참조하십시오.


제공자 그룹 가져오기

이전에 구성된 LDAP 또는 SAML ID 제공자에서 vCloud Director 제공자 조직으로 그룹을 가져올 수 있습니다.

사전 요구 사항

시스템 LDAP 연결 구성 또는 SAML ID 제공자를 사용하도록 시스템 구성 작업을 수행합니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **그룹**을 클릭합니다.
- 3 **그룹 가져오기**를 클릭합니다.
- 4 **소스** 드롭다운 메뉴에서 ID 제공자 유형을 선택합니다.

LDAP 또는 **SAML**일 수 있습니다.

ID 제공자를 하나만 구성한 경우에는 이 옵션이 하드 코딩됩니다.

- 5 사용자를 지정합니다.


옵션	설명
LDAP	a 그룹의 전체 또는 일부 이름을 입력하고 검색 을 클릭합니다.
	b 가져올 그룹을 검색 결과에서 선택합니다.
	c 역할 할당 드롭다운 메뉴에서 가져온 그룹에 있는 사용자의 역할을 선택합니다.
SAML	a 가져올 그룹의 이름을 SAML ID 제공자가 지원하는 이름 식별자 형식으로 입력합니다.
	각 그룹 이름을 새 줄에 입력합니다.
	b 역할 할당 드롭다운 메뉴에서 가져온 그룹에 있는 사용자의 역할을 선택합니다.

- 6 **저장**을 클릭합니다.

제공자 그룹 편집

이전에 vCloud Director 제공자 조직에 가져온 그룹에 대해 설명을 편집하거나 구성원의 역할을 변경할 수 있습니다.

절차


- 1 기본 메뉴()에서 **관리**를 선택합니다.

- 2 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **그룹**을 클릭합니다.
- 3 대상 그룹의 이름 옆에 있는 라디오 버튼을 클릭하고 **편집**을 클릭합니다.
- 4 그룹 세부 정보를 편집하고 **저장**을 클릭합니다.

제공자 그룹 삭제

vCloud Director 제공자 조직에서 그룹을 제거할 수 있습니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **제공자 액세스 제어** 아래에서 **그룹**을 클릭합니다.
- 3 대상 그룹의 이름 옆에 있는 라디오 버튼을 클릭하고 **삭제**를 클릭합니다.
- 4 **확인**을 클릭하여 확인합니다.

vCloud Director 시스템 관리자는 LDAP, e-메일 알림, 라이선싱 및 일반 시스템 기본 설정과 관련된 시스템 전반의 설정을 제어할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 일반 시스템 설정 수정
- 일반 시스템 설정
- 시스템 e-메일 설정 구성
- vCloud Director 라이선스 변경
- 카탈로그 동기화 설정 구성
- 차단 작업 및 알림 구성
- 공개 주소 구성
- ID 제공자 관리
- 플러그인 관리
- vCloud Director 포털 사용자 지정
- 암호 정책 구성
- vSphere 서비스 구성


일반 시스템 설정 수정

vCloud Director에는 활동 로그, 네트워킹, 세션 시간 초과, 인증서, 조직 제한, 작업 제한 등과 관련된 일반 시스템 설정이 포함됩니다. 기본 설정은 많은 환경에 적합하지만 필요에 맞게 설정을 수정할 수 있습니다.

수정할 수 있는 속성 목록은 [일반 시스템 설정](#) 항목을 참조하십시오.

참고 vCloud Director 장치의 날짜, 시간 또는 표준 시간대 변경에 대한 자세한 내용은 <https://kb.vmware.com/kb/59674> 문서를 참조하십시오.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **설정** 아래에서 **일반**을 클릭합니다.
- 3 수정할 섹션에 대해 **편집**을 클릭하고 속성을 편집한 다음 **저장**을 클릭합니다.

일반 시스템 설정

vCloud Director에는 필요에 맞게 수정할 수 있는 일반 시스템 설정이 포함되어 있습니다.

표 11-1. 일반 시스템 설정

이름	범주	설명
Activity log history to keep	활동 로그	로그 기록을 삭제하기 전에 보관할 기간(일)입니다. 0 을 입력하면 로그가 삭제되지 않습니다.
Activity log history shown	활동 로그	표시할 로그 기록 기간(일)입니다. 모든 활동을 표시하려면 0 을 입력합니다.
Display debug information	활동 로그	vCloud Director 작업 로그에 디버거 정보를 표시하려면 이 설정을 사용하도록 설정합니다.
IP address release timeout	네트워킹	릴리스된 IP 주소가 다시 할당 가능한 상태로 되기까지 보류할 시간(초)입니다. 이 기본 설정은 오래된 항목이 클라이언트 ARP 테이블에서 만료될 수 있도록 2시간(7200초)으로 지정됩니다.
Allow Overlapping External Networks	네트워킹	동일한 네트워크 세그먼트에서 실행되는 외부 네트워크를 추가하려면 이 확인란을 선택합니다. 이 설정은 비 VLAN 기반 방법을 사용하여 외부 네트워크를 격리하는 경우에만 사용하도록 설정합니다.
Allow FIPS mode	네트워킹	Edge 게이트웨이에서 FIPS 모드의 지원을 허용합니다. NSX 6.3 이상이 필요합니다. "VMware NSX for vSphere" 설명서의 FIPS 모드 를 참조하십시오.
Default syslog server settings for networks	네트워킹	네트워크에서 사용할 Syslog 서버 최대 2개에 대한 IP 주소를 입력합니다. 이 설정은 클라우드 셀에서 사용하는 Syslog 서버에는 적용되지 않습니다.
Provider Locale	지역화	로그 항목, e-메일 경고 등을 포함한 제공자 활동의 로케일을 선택합니다.
Idle session timeout	시간 초과	사용자 상호 작용이 없어도 vCloud Director 애플리케이션이 활성 상태로 유지되는 시간입니다.
Maximum session timeout	시간 초과	vCloud Director 애플리케이션이 활성 상태로 유지되는 최대 시간입니다.
Host refresh frequency	시간 초과	vCloud Director가 ESXi 호스트에 액세스할 수 있는지 여부를 확인하는 빈도입니다.
Host hung timeout	시간 초과	호스트를 응답 없음으로 표시하기 전에 기다릴 시간을 선택합니다.

표 11-1. 일반 시스템 설정 (계속)

이름	범주	설명
Transfer session timeout	시간 초과	일시 중지되거나 취소된 미디어 업로드 또는 vApp 템플릿 업로드 등의 업로드 작업을 실패로 처리하기 전에 기다릴 시간입니다. 이 제한 시간은 진행 중인 업로드 작업에는 영향을 주지 않습니다.
Enable upload quarantine with a timeout of __ seconds	시간 초과	업로드된 파일을 격리하려면 이 확인란을 선택하고 시간을 나타내는 시간 초과 값을 입력합니다.
Verify vCenter and vSphere SSO certificates	인증서	vCloud Director가 신뢰할 수 있는 vCenter Server와만 통신하도록 허용하려면 이 확인란을 선택합니다. 찾아보기 를 클릭하여 JCEKS 키 저장소를 찾고 키 저장소 암호를 입력합니다.
Verify NSX Manager certificates	인증서	vCloud Director가 NSX Manager의 신뢰할 수 있는 인스턴스와만 통신하도록 허용하려면 이 확인란을 선택합니다. 찾아보기 를 클릭하여 JCEKS 키 저장소를 찾고 키 저장소 암호를 입력합니다.
Edit Organization Limits	조직 VDC 제한	조직당 조직 가상 데이터 센터의 최대 수를 입력하거나 무제한 을 선택합니다.
Number of resource intensive operations running per user	작업 제한	사용자당 리소스 사용이 많은 동시 작업의 최대 수를 입력하거나 무제한 을 선택합니다.
Number of resource intensive operations to be queued per user (in addition to running)	작업 제한	사용자당 대기열에 있는 리소스 사용이 많은 작업의 최대 수를 입력하거나 무제한 을 선택합니다.
Number of resource intensive operations running per organization	작업 제한	조직당 리소스 사용이 많은 동시 작업의 최대 수를 입력하거나 무제한 을 선택합니다.
Number of resource intensive operations to be queued per organization	작업 제한	조직당 대기열에 있는 리소스 사용이 많은 작업의 최대 수를 입력하거나 무제한 을 선택합니다.
Provide default vApp names	기타	새 vApp의 기본 이름을 제공하도록 vCloud Director를 구성하려면 이 확인란을 선택합니다.
Make Allocation pool Org VDCs elastic	기타	탄력적 할당 풀을 사용하도록 설정하여 모든 할당 풀 조직 가상 데이터 센터를 탄력적으로 만들려면 이 확인란을 선택합니다. 이 옵션을 선택 해제하기 전에 각 조직 가상 데이터 센터의 모든 가상 시스템이 단일 클러스터로 마이그레이션되었는지 확인합니다.
VM discovery enabled	기타	기본적으로 각 조직 VDC는 해당 VDC를 지원하는 모든 리소스 풀에 만들어진 vCenter VM을 자동으로 검색합니다. 시스템의 모든 VDC에 대해 이 설정을 비활성화하려면 선택을 취소합니다.


시스템 e-메일 설정 구성

SMTP 서버 설정 및 vCloud Director 알림 설정 구성을 포함하여 시스템 e-메일 설정을 편집할 수 있습니다.

vCloud Director에는 사용자 알림 및 시스템 경고 e-메일을 시스템 사용자에게 보내기 위한 SMTP 서버가 필요합니다.

vCloud Director는 보고해야 할 중요한 정보가 있을 때 시스템 경고 e-메일을 보냅니다. 예를 들어 vCloud Director는 데이터스토어의 공간이 부족하면 경고를 보냅니다. 모든 시스템 관리자에게 또는 지정된 e-메일 주소 목록으로 e-메일 경고를 보내도록 vCloud Director를 구성할 수 있습니다.

절차


- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 창의 **설정**에서 **e-메일**을 선택하고 **편집**을 클릭합니다.
- 3 SMTP 메일 서버의 DNS 호스트 이름이나 IP 주소를 입력합니다.
- 4 SMTP 서버 포트 번호를 입력합니다.
- 5 (선택 사항) SMTP 서버에 사용자 이름이 필요한 경우 **인증 필요** 옵션을 설정하고 SMTP 계정의 사용자 이름과 암호를 입력합니다.
- 6 **알림 설정** 탭을 선택합니다.
- 7 vCloud Director e-메일의 보낸 사람으로 표시할 e-메일 주소를 입력합니다.
vCloud Director에서는 보낸 사람의 e-메일 주소를 사용하여 런타임 및 스토리지 임대 만료 경고를 보냅니다.
- 8 (선택 사항) 제목 접두사 텍스트를 입력합니다.
- 9 알림의 수신자를 선택합니다.
기본적으로 조직 관리자만 SMTP 알림을 받습니다.
- 10 **저장**을 클릭합니다.
- 11 (선택 사항) SMTP 설정을 테스트합니다.
 - a **테스트**를 클릭합니다.
 - b **인증 필요** 옵션을 사용하도록 설정한 경우 SMTP 서버 암호를 입력합니다.
 - c 대상 e-메일 주소를 입력하고 **테스트**를 클릭합니다.

vCloud Director 라이선스 변경

vCloud Director를 실행하려면 일련 번호로 지정된 유효한 라이선스가 필요합니다. 초기 vCloud Director 구성 중에 입력한 라이선싱 정보를 수정할 수 있습니다.

vCloud Director 제품 일련 번호는 vCenter Server 라이선스 키와 동일하지 않습니다. VMware License Portal에서 vCloud Director 일련 번호를 가져올 수 있습니다.


절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 창에서 **라이선스**를 선택하고 **편집**을 클릭합니다.
- 3 새 일련 번호를 입력하고 **저장**을 클릭합니다.

카탈로그 동기화 설정 구성

카탈로그 구독의 새로 고침 빈도를 포함하여 모든 조직 및 카탈로그에 대한 카탈로그 동기화 설정을 편집할 수 있습니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 창의 **설정**에서 **카탈로그**를 선택합니다.
- 3 **편집**을 클릭합니다.
- 4 카탈로그 동기화를 사용하도록 설정합니다.
- 5 동기화 시작 및 중지 시간을 설정합니다.
- 6 동기화 간격을 설정합니다.

동기화 간격은 카탈로그 구독의 새로 고침 빈도입니다.

- 7 **저장**을 클릭합니다.

다음에 수행할 작업

카탈로그 동기화 임계치 조절 구성에 대한 자세한 내용은 "vCloud Director 설치, 구성 및 업그레이드 가이드"의 내용을 참조하십시오.

차단 작업 및 알림 구성

차단 작업 및 알림을 사용하여 특정 이벤트에 의해 트리거된 AMQP 메시지를 보내도록 vCloud Director를 구성할 수 있습니다.


이 메시지 중 일부는 단순히 이벤트가 발생했음을 알립니다. 다른 메시지는 지정된 AMQP 끝점에 정보를 게시하여 요청된 작업이 차단되었고 해당 끝점에 바인딩된 클라이언트 애플리케이션의 작업을 대기하고 있음을 알립니다. 이러한 메시지를 차단 작업이라고 합니다.

시스템 관리자는 AMQP 클라이언트의 프로그래밍 방식 작업의 적용을 받는 시스템 전체 차단 작업 집합을 구성할 수 있습니다.

AMQP 브로커 구성

vCloud Director가 특정 이벤트에 의해 트리거된 AMQP 메시지를 보내도록 하려면 AMQP 브로커를 구성해야 합니다. AMQP 메시지를 사용하여 기본 사용자 요청의 처리를 자동화할 수 있습니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 **설정**에서 **확장성**을 선택합니다.
AMQP 브로커 탭이 열립니다.
- 3 **AMQP 브로커** 섹션의 **편집** 버튼을 클릭합니다.
- 4 AMQP 호스트의 DNS 호스트 이름이나 IP 주소를 입력합니다.
RabbitMQ 서버 호스트의 정규화된 도메인 이름(예: *amqp.example.com*)
- 5 AMQP 포트를 입력합니다.
브로커가 메시지를 수신하는 기본 포트는 5672입니다.
- 6 exchange를 입력합니다.
- 7 vHost를 입력합니다.
기본값은 /입니다.
- 8 접두사를 입력합니다.
- 9 (선택 사항) SSL을 사용하려면 **SSL 사용** 토글을 설정하고 인증서 옵션 중 하나를 선택합니다.

기본적으로 vCloud Director AMQP 서비스는 암호화되지 않은 메시지를 보냅니다. SSL을 사용하여 이러한 메시지를 암호화하도록 AMQP 서비스를 구성할 수 있습니다. VMware Cloud Director 셸에 있는 Java Runtime Environment의 기본 JCEKS 신뢰 저장소를 사용하여 브로커 인증서를 확인하도록 서비스를 구성할 수도 있습니다(일반적으로 `$VCLLOUD_HOME/jre/lib/security/cacerts`에 위치).

옵션	설명
모든 인증서 수락	인증서 소유자 필드의 CN 레코드는 AMQP 브로커 호스트 이름과 일치해야 합니다. 브로커 호스트 이름이 일치하지 않는 인증서를 사용하려면 모든 인증서 수락 토글을 설정합니다.
SSL 인증서	SSL 인증서를 업로드합니다.
SSL 키 저장소(JCEKS)	SSL 키 저장소를 업로드하고 키 저장소 암호를 입력합니다.


- 10 사용자 이름과 암호를 입력하여 AMQP 호스트에 연결합니다.
- 11 **저장**을 클릭합니다.
- 12 (선택 사항) 설정을 테스트하려면 **AMQP 브로커** 섹션에서 **테스트** 버튼을 클릭하고 암호를 입력합니다.

- 13** (선택 사항) AMQP 브로커에 감사 이벤트를 게시하려면 **비차단 AMQP 알림** 섹션에서 **편집** 버튼을 클릭하고 **알림 사용** 토글을 설정합니다.

차단 작업 설정 구성

특정 작업을 차단 작업으로 구성할 수 있습니다. 이러한 작업은 **시스템 관리자**가 작업할 때까지 또는 미리 구성된 타이머가 만료될 때까지 일시 중단됩니다. 차단 작업에 대한 시간 초과 설정 및 기본 동작을 지정할 수 있습니다. 설정은 설치의 모든 조직에 적용됩니다.

절차

- 1** 기본 메뉴()에서 **관리**를 선택합니다.
- 2** **설정**에서 **확장성**을 선택합니다.
- 3** **차단 작업** 탭을 선택합니다.
- 4** 기본 확장 시간 초과와 기본 시간 초과 동작을 편집하려면 **일반** 섹션에서 **편집** 버튼을 클릭합니다.
 - a** **기본 차단 작업 시간 초과**를 편집합니다.
 - b** **기본 시간 초과 동작**을 편집합니다.
기본 시간 초과 동작은 **기본 차단 작업 시간 초과**가 만료된 후의 동작입니다.
 - c** **저장**을 클릭합니다.
- 5** 차단 작업으로 간주되는 작업의 목록을 편집하려면 **작업** 섹션에서 **편집** 버튼을 클릭합니다.
 - a** 차단 작업 목록에서 작업을 선택하거나 선택 취소합니다.
 - b** **저장**을 클릭합니다.

공개 주소 구성

로드 밸런서 또는 프록시 요구 사항을 충족하기 위해 vCloud Director 웹 포털, vCloud Director API 및 콘솔 프록시에 대한 기본 끝점 웹 주소를 변경할 수 있습니다.

공개 주소는 vCloud Director의 클라이언트에게 노출되는 웹 주소입니다. 이러한 주소의 기본값은 설치 중에 지정됩니다. 필요한 경우 주소를 업데이트할 수 있습니다.

vCloud Director가 단일 셀로 구성된 경우, 설치 관리자는 일반적으로 **API** 및 **Web** 클라이언트에 충분한 액세스를 제공하는 공용 끝점을 생성합니다. 셀이 여러 개 포함된 설치 및 배포에서는 대개 셀과 클라이언트 사이에 로드 밸런서를 배치합니다. 클라이언트는 로드 밸런서의 주소로 시스템에 액세스합니다. 로드 밸런서는 사용 가능한 셀에 클라이언트 요청을 분산시킵니다. 프록시를 포함하거나 DMZ에 셀을 배치하는 다른 네트워크 구성에는 사용자 지정된 끝점도 필요합니다. 끝점 URL 세부 정보는 네트워크 구성에 따라 다릅니다.


vCloud Director Tenant Portal 및 vCloud Director 웹 콘솔의 끝점에는 가능하면 서명된 SSL 인증서가 필요합니다. vCloud Director를 설치 또는 배포할 때 이러한 인증서의 경로를 지정해야 합니다. 설치 또는 배포 후에 이러한 끝점을 사용자 지정할 경우 **hostname** 및 **subject alternative name**과 같은 끝점 세부 정보와 일치하는 새 인증서를 설치해야 할 수 있습니다.

vCloud Director 장치의 경우, 장치가 콘솔 프록시 서비스에 사용자 지정 포트 8443가 포함된 단일 IP 주소를 사용하기 때문에 vCloud Director 공용 콘솔 프록시 주소를 구성해야 합니다. [단계 6](#)의 내용을 참조하십시오.

사전 요구 사항

시스템 관리자로 로그인했는지 확인합니다. **시스템 관리자**만 공용 끝점을 사용자 지정할 수 있습니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **설정** 아래에서 **공개 주소**를 클릭합니다.
- 3 공용 끝점을 사용자 지정하려면 **편집**을 클릭합니다.
- 4 vCloud Director URL을 사용자 지정하려면 **웹 포털** 끝점을 편집합니다.
 - a HTTP(비보안) 연결을 위한 사용자 지정 vCloud Director 공용 URL을 입력합니다.
 - b HTTPS(보안) 연결을 위한 사용자 지정 vCloud Director 공용 URL을 입력하고 **업로드**를 클릭하여 해당 끝점의 신뢰 체인을 설정하는 인증서를 업로드합니다.

인증서 체인은 서비스 끝점에서 사용되는 인증서와 일치해야 하며, 이것은 별칭이 **consoleproxy**인 각 vCloud Director 셀 키 저장소에 업로드된 인증서입니다. 로드 밸런서에서 콘솔 프록시 연결의 SSL 종료는 지원되지 않습니다. 인증서 체인에는 끝점 인증서, 중간 인증서 및 개인 키 없는 PEM 형식의 루트 인증서가 포함되어야 합니다.

- 5** (선택 사항) Cloud Director REST API와 OpenAPI URL을 사용자 지정하려면 **웹 포털 설정 사용** 토글을 해제합니다.

- a** 사용자 지정 HTTP 기본 URL을 입력합니다.

예를 들어 HTTP 기본 URL을 **http://vcloud.example.com**으로 설정하면 **http://vcloud.example.com/api**에서 vCloud Director API에 액세스하고 **http://vcloud.example.com/cloudapi**에서 vCloud Director OpenAPI에 액세스할 수 있습니다.

- b** 사용자 지정 HTTPS REST API 기본 URL을 입력하고 **업로드**를 클릭하여 해당 끝점의 신뢰 체인을 설정하는 인증서를 업로드합니다.

예를 들어 HTTPS REST API 기본 URL을 **https://vcloud.example.com**으로 설정하면 **https://vcloud.example.com/api**에서 vCloud Director API에 액세스하고 **https://vcloud.example.com/cloudapi**에서 vCloud Director OpenAPI에 액세스할 수 있습니다.

인증서 체인은 서비스 끝점에 사용되는 인증서와 일치해야 하며, 별칭이 **http**인 각 vCloud Director 셀 키 저장소에 업로드된 인증서이거나 SSL 종료에 사용되는 경우 로드 밸런서 VIP 인증서입니다. 인증서 체인에는 끝점 인증서, 중간 인증서 및 개인 키 없는 PEM 형식의 루트 인증서가 포함되어야 합니다.

- 6** 사용자 지정 vCloud Director 공용 콘솔 프록시 주소를 입력합니다.

- vCloud Director 장치 공용 콘솔 프록시 주소를 사용자 지정합니다.

이 주소는 vCloud Director 장치 **eth0** NIC의 FQDN(정규화된 도메인 이름)으로, 콘솔 프록시 서비스를 위한 사용자 지정 포트 **8443**이 포함된 FQDN 또는 IP 주소로 지정됩니다.

- Linux의 vCloud Director 공용 콘솔 프록시 주소를 사용자 지정합니다.

이 주소는 포트 번호가 있는 로드 밸런서 또는 vCloud Director 서버의 FQDN(정규화된 도메인 이름)입니다. 기본 포트는 **443**입니다.

예를 들어 FQDN이 **vcloud.example.com**인 vCloud Director 장치 인스턴스의 경우 **vcloud.example.com:8443**을 입력합니다.

vCloud Director는 VM에서 원격 콘솔 창을 열 때 콘솔 프록시 주소를 사용합니다.

- 7** **저장**을 클릭합니다.

ID 제공자 관리

클라우드를 외부 ID 제공자와 통합하여 사용자와 그룹을 조직에 가져올 수 있습니다. 시스템 또는 조직 수준에서 LDAP 서버 연결을 구성할 수 있습니다. 조직 수준에서 SAML 통합을 구성할 수 있습니다.


LDAP 연결 관리

시스템 관리자는 LDAP 서버를 사용자 및 그룹의 소스로 사용하도록 vCloud Director 시스템 조직과 시스템 내의 다른 모든 조직을 구성할 수 있습니다. 조직에서는 시스템 LDAP 연결 또는 개인 LDAP 연결을 사용할 수 있습니다.

시스템 LDAP 연결 구성

시스템 수준에서 LDAP 연결을 구성하여 vCloud Director 및 해당 조직에 사용자 및 그룹에 대한 공유 액세스를 제공할 수 있습니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **ID 제공자** 아래에서 **LDAP**를 클릭합니다.

현재 LDAP 설정이 표시됩니다.



다음에 수행할 작업

[LDAP 연결 구성, 테스트 및 동기화](#).

조직 LDAP 연결 구성

시스템 LDAP 연결을 사용자 및 그룹의 공유 소스로 사용하도록 조직을 구성할 수 있습니다. 개별 LDAP 연결을 사용자 및 그룹의 개인 소스로 사용하도록 조직을 구성할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **조직**을 클릭합니다.
- 3 대상 조직의 이름을 클릭합니다.
조직의 vCloud Director 테넌트 포털로 리디렉션됩니다.
- 4 기본 메뉴()에서 **관리**를 선택합니다.
- 5 왼쪽 패널의 **ID 제공자** 아래에서 **LDAP**를 클릭합니다.
현재 LDAP 설정이 표시됩니다.
- 6 **LDAP 옵션** 탭에서 **편집**을 클릭합니다.
- 7 이 조직의 사용자 및 그룹 LDAP 소스를 구성하고 **저장**을 클릭합니다.

옵션	설명
LDAP 사용 안 함	조직에서 LDAP 서버를 조직 사용자 및 그룹의 소스로 사용하지 않습니다.
VCD 시스템 LDAP 서비스	조직에서 이전에 구성된 vCloud Director 시스템 LDAP 연결을 사용합니다. 시스템 LDAP 연결 구성 의 내용을 참조하십시오.
사용자 지정 LDAP 서비스	조직에서 개인 LDAP 서버를 조직 사용자 및 그룹의 소스로 사용합니다. 사용자 지정 LDAP 탭을 클릭하고 LDAP 연결 구성, 테스트 및 동기화 의 작업을 수행합니다.

LDAP 연결 구성, 테스트 및 동기화


시스템 또는 조직 LDAP 연결을 구성하려면 LDAP 서버 세부 정보를 구성합니다. 연결을 테스트하여 올바른 설정을 입력했는지, 사용자 및 그룹 특성이 올바르게 매핑되었는지 확인할 수 있습니다. LDAP 연결에 성공하면 언제든지 vCloud Director를 LDAP 서버와 동기화할 수 있습니다.

사전 요구 사항

LDAPS 서버에 연결하려는 경우, Java 8 Update 181의 향상된 LDAP 지원을 위해 제대로 구성된 인증서가 있는지 확인합니다. 자세한 내용은 <https://www.java.com>에서 "Java 8 릴리스 변경 내용"을 참조하십시오.

절차

1 연결 탭에 LDAP 연결을 위한 필수 정보를 입력합니다.

필요한 정보	설명
서버	LDAP 서버의 호스트 이름이나 IP 주소입니다.
포트	LDAP 서버가 수신 대기하는 포트 번호입니다. LDAP의 경우 기본 포트 번호는 389입니다. LDAPS의 경우 기본 포트 번호는 636입니다.
기본 고유 이름	기본 DN(고유 이름)은 vCloud Director가 연결할 LDAP 디렉토리 내의 위치입니다. 루트에 연결하려면 도메인 구성 요소만 입력합니다(예: DC=example,DC=com). 트리의 노드에 연결하려면 해당 노드의 고유 이름을 입력합니다(예: OU=ServiceDirector,DC=example,DC=com). 노드에 연결하면 vCloud Director가 사용할 수 있는 디렉토리의 범위가 제한됩니다.
연결 유형	LDAP 서버의 유형입니다. Active Directory 또는 OpenLDAP 일 수 있습니다.
SSL 사용	서버가 LDAPS인 경우에 이 확인란을 선택합니다.
모든 인증서 수락	서버가 LDAPS인 경우 이 확인란을 선택하거나 LDAP SSL 인증서를 업로드합니다.
사용자 지정 Truststore	서버가 LDAPS인 경우 업로드 아이콘()을 클릭하고 LDAP SSL 인증서를 가져오거나, 모든 인증서 수락 을 선택합니다.
인증 방법	단순한 인증의 경우에는 LDAP 서버에 사용자의 DN과 암호를 보냅니다. LDAP를 사용하는 경우에는 LDAP 암호가 네트워크를 통해 일반 텍스트로 전송됩니다. Kerberos를 사용하려면 vCloud API를 사용하여 LDAP 연결을 구성해야 합니다.

필요한 정보	설명
사용자 이름	LDAP 서버에 연결하기 위한 전체 LDAP DN 사용자 이름입니다. LDAP 서버에 익명 읽기 지원을 사용하도록 설정되어 있으면 이러한 텍스트 상자를 비워둘 수 있습니다.
암호	LDAP 서버에 연결하기 위한 암호입니다. LDAP 서버에 익명 읽기 지원을 사용하도록 설정되어 있으면 이러한 텍스트 상자를 비워둘 수 있습니다.

- 2 사용자 특성** 탭을 클릭하고 사용자 특성의 기본값을 검토합니다. LDAP 디렉토리에서 다른 스키마를 사용하는 경우, 값을 수정합니다.
- 3 그룹 특성** 탭을 클릭하고 그룹 특성의 기본값을 검토합니다. LDAP 디렉토리에서 다른 스키마를 사용하는 경우, 값을 수정합니다.
- 4 저장**을 클릭합니다.
- LDAP 연결 설정 및 LDAP 특성 매핑을 테스트하려면 다음을 수행합니다.
 - 테스트**를 클릭합니다.
 - 구성한 LDAP 서버 사용자 암호를 입력하고 **테스트**를 클릭합니다.
연결에 성공하면 녹색 확인 표시가 표시됩니다.
검색된 사용자 및 그룹 특성 값이 테이블에 표시됩니다. LDAP 특성에 성공적으로 매핑된 값에는 녹색 확인 표시가 표시됩니다. LDAP 특성에 매핑되지 않은 값은 비어 있고, 빨간색 느낌표가 표시됩니다.
 - 종료하려면 **취소**를 클릭합니다.
- vCloud Director를 구성된 LDAP 서버와 동기화하려면 **동기화**를 클릭합니다.
vCloud Director는 일반 시스템 설정에 설정된 동기화 간격에 따라 사용자 및 그룹 정보를 LDAP 서버와 정기적으로 동기화합니다.
동기화가 완료될 때까지 몇 분 정도 기다립니다.

결과

새로 구성된 LDAP 서버에서 사용자 및 그룹을 가져올 수 있습니다.

SAML ID 제공자를 사용하도록 시스템 구성

SAML ID 제공자의 사용자 및 그룹을 시스템 조직에 가져오려면 이 SAML ID 제공자를 사용하여 시스템 조직을 구성해야 합니다. 가져온 사용자는 SAML ID 제공자에 설정된 자격 증명을 사용하여 시스템 조직에 로그인할 수 있습니다.

SAML ID 제공자를 사용하여 vCloud Director를 구성하려면 SAML 서비스 제공자 및 ID 제공자 메타데이터를 교환하여 상호 신뢰를 설정해야 합니다.

가져온 사용자가 로그인을 시도하면 시스템에서는 **SAML 토큰**(사용할 수 있는 경우)에서 다음 특성을 추출하여, 사용자에게 대한 해당 정보를 해석하는 데 사용합니다.

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"`(구성 가능한 특성)

그룹 정보는 사용자를 직접 가져오지 않았지만 가져온 그룹의 구성원 자격으로 사용자의 로그인이 예상되는 경우에 사용됩니다. 사용자는 여러 그룹에 속해 있을 수 있으므로 세션 중에 여러 개의 역할을 가질 수 있습니다.


가져온 사용자 또는 그룹에 ID 제공자로 지연 역할이 할당된 경우, 역할은 토큰의 역할 특성에서 수집된 정보를 기반으로 할당됩니다. 다른 특성을 사용할 경우, **API**를 사용하여 이 특성 이름을 구성할 수 있으며 역할 특성만 구성 가능합니다. ID 제공자로 지연 역할을 사용하지만 추출된 역할 정보가 없는 경우, 사용자는 로그인할 수 있지만 활동을 수행할 수 있는 권한이 없습니다.

사전 요구 사항

- SAML 2.0을 준수하는 ID 제공자에 액세스할 수 있는지 확인합니다.
- 다음 메타데이터가 포함된 XML 파일을 SAML ID 제공자로부터 가져옵니다.
 - Single Sign-On 서비스의 위치
 - 단일 로그아웃 서비스의 위치
 - 서비스의 X.509 인증서 위치

SAML ID 제공자의 메타데이터를 구성하고 확보하는 방법에 대한 자세한 내용은 SAML 제공자에게 문의하여 설명서를 참조하십시오.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 [ID 제공자] 아래에서 **SAML**을 클릭하고 **편집**을 클릭합니다.
현재 SAML 설정이 표시됩니다.

3 서비스 제공자 탭에서 vCloud Director SAML 서비스 제공자 메타데이터를 다운로드합니다.

- a 시스템 조직의 엔티티 ID를 입력합니다.

엔티티 ID는 ID 제공자에서 시스템 조직을 고유하게 식별합니다.

- b 인증서 만료 날짜를 확인하고, 곧 만료 예정인 경우 **재생성**을 클릭하여 인증서를 재생성합니다.

인증서는 SAML 메타데이터에 포함되어 있으며 암호화 및 서명에 모두 사용됩니다. 조직과 SAML IDP 간에 신뢰가 설정된 방식에 따라 이들 중 하나 또는 둘 모두 필요할 수 있습니다.


- c **메타데이터** 링크를 클릭합니다.

이 링크는 `https://VCD_host_name/cloud/org/System/saml/metadata/alias/vcd`와 유사합니다.

브라우저에서 SAML 서비스 제공자 메타데이터를 다운로드합니다. XML 파일 형식의 이 메타데이터는 ID 제공자에게 제공해야 합니다.

4 ID 제공자 탭에서 앞서 ID 제공자로부터 받은 SAML 메타데이터를 업로드합니다.

- a **SAML ID 제공자 사용**을 선택합니다.

- b **찾아보기** 아이콘()을 클릭하고 파일을 업로드하거나, 파일의 내용을 복사하여 **메타데이터 XML** 텍스트 상자에 붙여넣습니다.

5 저장을 클릭합니다.

결과

플러그인 관리

vCloud Director 플러그인은 Service Provider Admin Portal과 vCloud Director Tenant Portal의 기능을 확장합니다. Service Provider Admin Portal에서 플러그인을 업로드하고, 사용하지 않도록 설정하고, 삭제할 수 있습니다. 서비스 제공자 및 개별 조직에 플러그인을 게시할 수 있습니다.

일부 플러그인은 vCloud Director의 일부로 설치됩니다.

CPOM 확장

vCloud Director Tenant Portal을 사용하여 전용 vCenter Server 인스턴스와 프록시를 보고 관리할 수 있는 기능을 제공합니다.

포털 사용자 지정

vCloud Director Service Provider Admin Portal과 vCloud Director Tenant Portal을 사용자 지정하는 기능을 제공합니다.

vCloud Availability

VMware vCloud® Availability™ 플러그인을 사용하면 vCloud Director 사용자 인터페이스에서 직접 vCloud Availability Portal에 액세스할 수 있습니다. 자세한 내용은 [vCloud Availability 설명서](#)를 참조하십시오.


플러그인 업로드

클라우드의 서비스 제공자 및 조직에서 사용하도록 vCloud Director Service Provider Admin Portal에 추가 플러그인을 업로드할 수 있습니다.

사전 요구 사항

플러그인 설치 파일을 다운로드합니다.

절차

- 1 기본 메뉴()에서 **포털 사용자 지정**을 선택합니다.
- 2 **업로드**를 클릭합니다.
- 3 **플러그인 파일 선택**을 클릭하고 대상 설치 파일로 이동하여 **열기**를 클릭합니다.
- 4 **다음**을 클릭합니다.
- 5 이 플러그인에 대한 범위를 선택합니다.


옵션	설명
서비스 제공자	vCloud Director Service Provider Admin Portal에서 플러그인 기능을 사용할 수 있게 됩니다.
테넌트	선택한 조직의 vCloud Director Service Provider Admin Portal에서 플러그인 기능을 사용할 수 있게 됩니다.

- 6 플러그인 범위를 테넌트로 지정하는 경우 이 플러그인을 게시하려는 조직을 선택합니다.
- 7 **검토 및 마침** 페이지를 검토하고 **마침**을 클릭합니다.

플러그인 사용 또는 사용 안 함

모든 조직이 특정 플러그인을 사용하지 못하게 하려면, 해당 플러그인을 사용하지 않도록 설정하면 됩니다.


절차

- 1 기본 메뉴()에서 **포털 사용자 지정**을 선택합니다.
- 2 대상 플러그인의 이름 옆에 있는 확인란을 선택하고 **사용** 또는 **사용 안 함**을 클릭합니다.

플러그인 제거

vCloud Director Service Provider Admin Portal에서 하나 이상의 플러그인을 제거할 수 있습니다.

절차


- 1 기본 메뉴()에서 **포털 사용자 지정**을 선택합니다.
- 2 제거하려는 플러그인 이름 옆에 있는 확인란을 선택하고 **삭제**를 클릭합니다.
- 3 **저장**을 클릭하여 확인합니다.

조직에서 플러그인 게시/게시 취소

플러그인이 제공하는 기능을 사용할 수 있는 조직 집합을 수정할 수 있습니다.

여러 플러그인에 대한 조직 집합을 수정할 수 있습니다.

절차

- 1 기본 메뉴()에서 **포털 사용자 지정**을 선택합니다.
- 2 대상 플러그인의 이름 옆에 있는 확인란을 선택하고 **게시**를 클릭합니다.
- 3 이 플러그인에 대한 범위를 선택합니다.

옵션	설명
서비스 제공자	vCloud Director Service Provider Admin Portal에서 플러그인 기능을 사용할 수 있게 됩니다.
테넌트	선택한 조직의 vCloud Director Service Provider Admin Portal에서 플러그인 기능을 사용할 수 있게 됩니다.

- 4 플러그인 범위를 테넌트로 지정하는 경우 이 플러그인을 게시하려는 조직을 선택합니다.
- 5 **저장**을 클릭합니다.

vCloud Director 포털 사용자 지정

회사 브랜딩 표준을 충족하고 완전히 사용자 지정 가능한 클라우드 환경을 만들기 위해 각 조직의 vCloud Director Service Provider Admin Portal 및 vCloud Director Tenant Portal에 대한 로고와 테마를 설정할 수 있습니다. vCloud Director 포털의 오른쪽 상단 메뉴 두 개에 대한 사용자 지정 링크를 수정하고 추가할 수도 있습니다.

참고 브랜딩 특성과 링크를 사용자 지정하려면 **branding vCloud OpenAPI** 메서드를 사용해야 합니다. <https://code.vmware.com>에서 "vCloud OpenAPI 시작하기"의 내용을 참조하십시오.

포털 브랜딩

설치 과정에서 vCloud Director에 두 가지 테마가 포함됩니다(기본값 및 어두움). 사용자 지정 테마를 만들고, 관리하고 적용할 수 있습니다. 포털 이름, 로고 및 브라우저 아이콘을 변경할 수도 있습니다. 또한 브라우저 제목에는 직접 설정한 포털 이름이 적용됩니다.

시스템 수준에서 브랜딩 특성을 설정하여 vCloud Director Service Provider Admin Portal을 사용자 지정할 수 있습니다. 특정 테넌트에 대해 브랜딩 특성을 구성하지 않는 한 각 조직의 vCloud Director Tenant Portal에 시스템 브랜딩 특성이 적용됩니다.

특정 테넌트의 경우 원하는 포털 이름, 배경색, 로고, 아이콘, 테마 및 사용자 지정 링크의 조합을 선택해서 재정의할 수 있습니다. 값을 설정하는 않으면 해당하는 시스템 기본값이 사용됩니다.

참고 기본적으로 개별 테넌트 브랜딩은 로그인한 세션의 외부에 표시되지 않습니다. 개별 테넌트 브랜딩은 로그인 및 로그아웃 페이지에 표시되지 않으므로 테넌트는 다른 테넌트의 존재를 검색할 수 없습니다. 셸 관리 도구를 사용하여 로그인한 세션의 외부에서 브랜딩을 사용하도록 설정할 수 있습니다.

```
manage-config -n backend.branding.requireAuthForBranding -v false
```

셸 관리 도구를 사용하는 방법에 대한 자세한 내용은 "vCloud Director 설치, 구성 및 업그레이드 가이드" 항목을 참조하십시오.

사용자 지정 링크

사용자 지정 링크는 포털 브랜딩의 구성 요소입니다. 사용자 지정 링크에는 두 가지 유형이 있습니다.

- **override** 메뉴 항목은 **도움말**, **정보** 및 **VMRC 다운로드** 메뉴 항목에 대한 기존 링크를 대체합니다. 기본적으로 **VMRC 다운로드**는 사용자를 <https://my.vmware.com>으로 리디렉션하여 VMRC를 다운로드하며, 이 경우 사용자에게 등록된 계정이 있어야 다운로드할 수 있습니다. 이 링크를 재정의하여 VMRC 설치 관리자를 자체 서버에 재배포할 수 있습니다.
- **link** 메뉴 항목은 포털의 오른쪽 상단 모서리에 있는 **로그아웃** 메뉴 항목에 추가하는 새로운 링크입니다. 새로운 사용자 지정 링크는 **API 호출**에 지정된 순서대로 나타납니다.

section 및 **separator** 메뉴 항목을 사용하여 이러한 사용자 지정 링크를 구성할 수 있습니다. **section** 메뉴 항목은 메뉴에 머리글을 추가하고, **separator** 메뉴 항목은 메뉴에 줄을 추가합니다.

사용자 지정 링크는 쿼리 매개 변수의 형태로 다른 애플리케이션에 식별 정보를 전달하는 데 사용할 수 있는 사용자 지정 변수를 지원합니다.

vCloud Director는 사용자 지정 링크의 url 값에 대해 다음과 같은 사용자 지정 변수를 지원합니다.

표 11-2. 사용자 지정 링크에 대한 사용자 지정 변수

변수	설명
<code>\${TENANT_NAME}</code>	조직 이름
<code>\${TENANT_ID}</code>	조직 ID
<code>\${SESSION_TOKEN}</code>	x-vcloud-authorization 토큰

예를 들면 다음과 같습니다.

```
url: https://host:port/tenant/${TENANT_NAME}/vdc
```

myorg라는 조직의 경우 vCloud Director Tenant Portal은 위의 URL에서 아래 URL로 변환됩니다.


```
url: https://host:port/tenant/myorg/vdcs
```

암호 정책 구성

사용자가 로그인을 시도하여 특정 횟수만큼 실패하는 경우 vCloud Director에 로그인하지 못하게 하려면, 계정 잠금을 사용하도록 설정하면 됩니다.

시스템 계정 잠금 정책을 변경하면 모든 새 조직에 적용됩니다. 계정 잠금 정책을 변경하기 전에 생성된 조직은 조직 수준에서 변경해야 합니다.

절차


- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **설정** 아래에서 **암호 정책**을 클릭합니다.
- 3 **편집**을 클릭합니다.
- 4 계정 잠금을 사용하도록 설정하려면 **계정 잠금** 토글을 설정합니다.
- 5 계정을 잠그기 전에 허용된 로그인 실패 횟수를 선택합니다.
- 6 잠금 간격을 선택합니다.
- 7 **시스템 관리자** 계정 잠금을 사용하도록 설정하려면 **시스템 관리자 계정을 잠글 수 있음** 토글을 설정합니다.
- 8 **저장**을 클릭합니다.

vSphere 서비스 구성

vCenter Single Sign-On을 사용하도록 vCloud Director를 구성하고 설정하여 vSphere ID 제공자가 시스템 관리자를 인증하도록 할 수 있습니다.

vCenter Lookup Service는 vSphere 인프라에 대한 토폴로지 정보를 포함하므로 vSphere 구성 요소가 이 서비스를 통해 서로 안전하게 연결할 수 있습니다.

절차

- 1 기본 메뉴()에서 **관리**를 선택합니다.
- 2 왼쪽 창의 **설정**에서 **vSphere 서비스**를 선택합니다.
- 3 vSphere 서비스를 구성합니다.
 - vCenter Lookup Service에 vCloud Director를 등록하려면 **등록**을 클릭합니다.
 - vCenter Lookup Service에서 vCloud Director 등록을 취소하려면 **등록 취소**를 클릭합니다.
- 4 vCenter Lookup Service URL을 입력합니다(예: https://hostname:7444/lookupservice/sdk).

- 5 관리 권한이 있는 vCenter Single Sign-On 사용자(예: `administrator@your_domain_name` 사용자)의 사용자 이름과 암호를 입력합니다.

결과

vCenter Lookup Service에 vCloud Director를 등록한 경우 **시스템 관리자**는 vCenter Single Sign-On 자격 증명을 사용하여 vCloud Director에 로그인해야 합니다.

vCloud Director 모니터링

12

시스템 관리자는 완료된 작업과 진행 중인 작업을 모니터링하고 제공자 가상 데이터 센터, 조직 가상 데이터 센터 및 데이터스토어 수준에서 리소스 사용량 정보를 확인할 수 있습니다.

버전 9.1부터는 vCloud Director에서 VMware vCenter Chargeback Manager가 지원되지 않습니다. [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [vCloud Director 및 비용 보고](#)
- [제공자 가상 데이터 센터에 대한 사용 정보 보기](#)

vCloud Director 및 비용 보고

vCloud Director용 VMware vRealize Operations Tenant App을 사용하여 vCloud Director에 대한 비용 보고 시스템을 구성할 수 있습니다.

VMware vRealize Operations Tenant App에는 서비스 제공자가 고객에게 차지백 서비스를 제공할 수 있는 측정 기능이 있습니다.

또한 VMware vRealize Operations Tenant App은 테넌트 관리자에게 환경 및 청구 데이터에 대한 가시성을 제공하는 테넌트용 애플리케이션이기도 합니다.

vCloud Director와 VMware vRealize Operations Tenant App 간 호환성에 대한 자세한 내용은 "VMware 제품 상호 운용성 매트릭스" (http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php)를 참조하십시오.


VMware vRealize Operations Tenant App은 <https://marketplace.vmware.com/vsx/solutions/management-pack-for-vcloud-director>에서 다운로드할 수 있습니다.

VMware vRealize Operations Tenant App을 사용하는 방법에 대한 자세한 내용은 "vRealize Operations Tenant App for vCloud Director를 서비스 제공자로 사용" 및 "vRealize Operations Tenant App for vCloud Director를 테넌트로 사용" 항목을 참조하십시오.

제공자 가상 데이터 센터에 대한 사용 정보 보기

제공자 가상 데이터 센터는 계산, 메모리 및 스토리지 리소스를 해당 조직 가상 데이터 센터에 제공합니다. 제공자 가상 데이터 센터 리소스의 사용을 모니터링하여 리소스를 더 추가할지 결정할 수 있습니다.

절차

- 1 기본 메뉴()에서 **클라우드 리소스**를 선택합니다.
- 2 왼쪽 패널에서 **제공자 VDC**를 클릭하고 대상 제공자 가상 데이터 센터의 이름을 클릭합니다.
- 3 **구성 > 메트릭** 탭을 클릭합니다.
- 4 각 매개 변수에 대한 자세한 내용을 보려면 각 정보 아이콘을 클릭합니다.

vCloud Director Service Provider Admin Portal의 콘텐츠 라이브러리 보기는 vRealize Orchestrator와의 통합을 위한 인터페이스를 제공합니다. vRealize Orchestrator 워크플로는 서비스 제공자 관리자가 테넌트 또는 다른 서비스 제공자에게 게시할 수 있는 서비스의 카탈로그로 사용할 수 있으며 이러한 방식으로 제공하는 기능 및 관리 기능의 집합을 확장합니다.

본 장은 다음 항목을 포함합니다.

- [vCloud Director와 vRealize Orchestrator 통합](#)
- [서비스 범주 만들기](#)
- [서비스 범주 편집](#)
- [서비스 가져오기](#)
- [서비스 검색](#)
- [서비스 실행](#)
- [서비스 범주 변경](#)
- [서비스 등록 취소](#)
- [서비스 게시](#)

vCloud Director와 vRealize Orchestrator 통합

vCloud Director Service Provider Admin Portal을 통해 vRealize Orchestrator를 vCloud Director와 통합합니다.

vRealize Orchestrator를 vCloud Director와 통합하면 서비스 제공자 관리자가 타사 플러그인의 워크플로 오케스트레이션 및 활용을 통해 복잡한 자동화 작업을 개발하도록 허용함으로써 vCloud Director의 기본 기능이 확장됩니다.

vCloud Director Service Provider Admin Portal을 통해 서비스 제공자 관리자는 등록된 vRealize Orchestrator 서버 인스턴스에서 워크플로를 보고 가져오고 실행할 수 있습니다.

vCloud Director Service Provider Admin Portal에서 vRealize Orchestrator 워크플로를 서비스 제공자 또는 테넌트에 게시하여 사용자 지정 서비스와 기본 제공 서비스의 빠른 액세스 제어 및 실행이 가능하도록 할 수 있습니다.

vRealize Orchestrator에는 특정 문제점을 해결하고 일반적인 관리 작업을 수행하도록 설계된 사전 구축 작업이 포함된 광범위한 워크플로 라이브러리가 있습니다. [VMware Solution Exchange](#)에서 타사 플러그인도 사용할 수 있습니다.



vCloud Director에 vRealize Orchestrator 인스턴스 등록


vCloud Director에서 vRealize Orchestrator를 통해 작업의 자동화 및 워크플로의 오케스트레이션을 활용하려면 vCloud Director Service Provider Admin Portal에서 vRealize Orchestrator 인스턴스를 등록합니다.

사전 요구 사항

- vRealize Orchestrator 서버 인스턴스를 배포 및 구성합니다. 자세한 내용은 vRealize Orchestrator 설명서의 "VMware vRealize Orchestrator 설치 및 구성"을 참조하십시오.
- vSphere를 인증 제공자로 사용하도록 vRealize Orchestrator를 구성합니다.
- vRealize Orchestrator가 인증에 사용하는 vCenter Single-Sign On과 동일한 Platform Services Controller의 조희 서비스에 vCloud Director가 등록되어 있는지 확인합니다.

절차

- 1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.
 - a 왼쪽 패널에서 **서비스 관리**를 선택합니다.
등록된 vRealize Orchestrator 서버의 목록이 표시됩니다.
- 2 새 vRealize Orchestrator 서버를 등록하려면  버튼을 클릭합니다.
vRealize Orchestrator 등록 대화 상자가 표시됩니다.
- 3 다음 값을 입력합니다.

옵션	설명
이름	등록된 vRealize Orchestrator 인스턴스의 이름입니다.
설명	등록된 vRealize Orchestrator 서버 인스턴스의 설명입니다.
호스트 이름	vRealize Orchestrator 서버의 정규화된 도메인 이름 및 서버 포트입니다. 기본 HTTPS 포트 값은 8281입니다. 참고 vCloud Director는 vRealize Orchestrator의 API 인스턴스에 연결됩니다.
사용자 이름	vRealize Orchestrator 관리자 그룹의 구성원인 사용자 계정입니다.
암호	vRealize Orchestrator 관리자 계정의 암호입니다.
Trust Anchor	PEM 형식의 vRealize Orchestrator 서버 SSL 인증서입니다. 업로드 아이콘()을 클릭하여 .pem 파일을 찾아 선택합니다.

4 확인을 클릭하여 등록을 완료합니다.

vRealize Orchestrator 서버가 vCloud Director에 등록됩니다.

서비스 범주 만들기

서비스 범주의 서비스를 구성할 수 있습니다.

절차

1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.

a 왼쪽 패널에서 **서비스 관리**를 선택합니다.

b **서비스 범주** 탭으로 이동합니다.

기존 서버 범주의 목록이 표시됩니다.

2 새 서비스 범주를 만들려면 버튼을 클릭합니다.

새 **서비스 범주** 대화 상자가 표시됩니다.

3 다음 값을 입력합니다.

옵션	설명
이름	서비스 범주의 이름입니다.
아이콘	서비스 범주에 대해 표시할 아이콘을 가져옵니다.
설명	서비스 범주에 대한 간략한 설명입니다.

서비스 범주 편집

기존 서비스 범주를 편집할 수 있습니다.

절차

1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.

a 왼쪽 패널에서 **서비스 관리**를 선택합니다.

b **서비스 범주** 탭으로 이동합니다.

기존 서버 범주의 목록이 표시됩니다.

2 선택된 서비스 범주의 왼쪽에 있는 목록 표시줄()을 사용하고 **편집**을 클릭합니다.

3 다음 값을 편집합니다.

옵션	설명
이름	서비스 범주의 이름입니다.
아이콘	서비스 범주에 대해 표시할 아이콘을 가져옵니다.
설명	서비스 범주에 대한 간략한 설명입니다.

서비스 가져오기

vCloud Director에 등록된 vRealize Orchestrator 인스턴스의 워크플로 라이브러리에서 서비스를 가져올 수 있습니다.

사전 요구 사항

- vRealize Orchestrator 인스턴스를 등록합니다. [vCloud Director에 vRealize Orchestrator 인스턴스 등록](#)의 내용을 참조하십시오.
- 서비스 범주를 만듭니다. [서비스 범주 만들기](#)의 내용을 참조하십시오.

절차

1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.

a 왼쪽 패널에서 **서비스 라이브러리**를 선택합니다.

사용 가능한 서비스가 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되어 페이지당 12개 항목으로 표시됩니다. 각 카드는 항목이 vRealize Orchestrator 워크플로임을 나타내고 워크플로를 가져오는 서비스 범주에 해당하는 태그 및 서비스의 이름을 표시합니다.

2 새 서비스를 가져오려면 **가져오기** 버튼을 클릭합니다.

3 **가져오기** 마법사의 단계를 따릅니다.

옵션	설명
대상 라이브러리로 가져오기	서비스를 가져올 서비스 범주를 선택합니다.
소스 선택	워크플로를 가져올 vRealize Orchestrator 인스턴스를 선택합니다.
워크플로 선택	계층 트리 보기를 확장하여 가져올 워크플로를 하나 이상 선택합니다.
검토	세부 정보를 검토하고 완료 를 클릭하여 가져오기를 완료합니다.

가져온 워크플로가 **서비스 라이브러리** 카드 보기에 표시됩니다.

서비스 검색

이름을 기준으로 또는 서비스가 속한 서비스 범주를 기준으로 서비스를 검색할 수 있습니다.

절차

1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.

a 왼쪽 패널에서 **서비스 라이브러리**를 선택합니다.

사용 가능한 서비스가 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되어 페이지당 12개 항목으로 표시됩니다. 각 카드는 항목이 vRealize Orchestrator 워크플로임을 나타내고 워크플로를 가져오는 서비스 범주에 해당하는 태그 및 서비스의 이름을 표시합니다.

2 페이지의 상단에 있는 **검색** 텍스트 상자에 찾으려는 서비스 범주 또는 서비스 이름의 단어 또는 문자를 입력합니다.


a 서비스 이름에서 검색할지 또는 범주에서 검색할지 선택합니다.

검색 결과가 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되어 페이지당 12개 항목으로 표시됩니다.

서비스 실행

vRealize Orchestrator 워크플로를 가져온 서비스로 실행할 수 있습니다.

절차

1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.

a 왼쪽 패널에서 **서비스 라이브러리**를 선택합니다.

사용 가능한 서비스가 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되어 페이지당 12개 항목으로 표시됩니다. 각 카드는 항목이 vRealize Orchestrator 워크플로임을 나타내고 워크플로를 가져오는 서비스 범주에 해당하는 태그 및 서비스의 이름을 표시합니다.

2 서비스를 실행하려면 선택된 서비스의 카드에서 **실행**을 클릭합니다.

서비스 실행 마법사가 표시됩니다.

3 서비스의 필수 입력 매개 변수를 입력하고 **마침**을 클릭합니다.

결과

최근 작업 보기에서 실행의 상태를 모니터링할 수 있습니다. 자세한 내용은 [작업 보기](#) 항목을 참조하십시오.

참고 vRealize Orchestrator 워크플로를 vCloud Director 서비스로 시작하는 경우 vCloud Director가 몇 개의 사용자 지정 매개 변수를 워크플로 실행 컨텍스트에 추가합니다.

사용자 지정 속성	설명
_vcd_orgName	서비스를 실행하는 사용자가 속한 조직의 이름입니다.
_vcd_orgId	서비스를 실행하는 사용자가 속한 조직의 ID입니다.
_vcd_username	서비스를 실행하는 사용자의 이름입니다.
_vcd_isAdmin	서비스를 실행하는 사용자가 관리자 인 경우 True 값이 있습니다.
_vdc_isAdmin	더 이상 사용되지 않습니다. 서비스를 실행하는 사용자가 관리자 인 경우 True 값이 있습니다.
_vdc_username	더 이상 사용되지 않습니다. 서비스를 실행하는 사용자의 이름입니다.
_vcd_sessionToken	vCloud Director에 대한 인증 성공 후 수신한 인증 토큰
_vcd_apiEndpoint	vCloud Director REST API 끝점

서비스 범주 변경

서비스가 속한 범주를 변경할 수 있습니다.

절차

1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.

a 왼쪽 패널에서 **서비스 라이브러리**를 선택합니다.

사용 가능한 서비스가 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되어 페이지당 12개 항목으로 표시됩니다. 각 카드는 항목이 vRealize Orchestrator 워크플로임을 나타내고 워크플로를 가져오는 서비스 범주에 해당하는 태그 및 서비스의 이름을 표시합니다.

2 선택된 서비스의 카드에서 **관리 > 범주 변경**을 선택합니다.


범주 변경 대화 상자가 열립니다.

3 서비스를 배치할 범주를 선택하고 **저장**을 클릭합니다.

서비스 등록 취소

서비스를 등록 취소하여 서비스 제공자와 테넌트의 서비스에 대한 액세스를 제거할 수 있습니다.

절차

- 1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.
 - a 왼쪽 패널에서 **서비스 라이브러리**를 선택합니다.


사용 가능한 서비스가 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되어 페이지당 12개 항목으로 표시됩니다. 각 카드는 항목이 vRealize Orchestrator 워크플로임을 나타내고 워크플로를 가져오는 서비스 범주에 해당하는 태그 및 서비스의 이름을 표시합니다.
- 2 선택된 서비스의 카드에서 **관리 > 워크플로 등록 취소**를 선택합니다.

워크플로 등록 취소 대화 상자가 열립니다.
- 3 서비스 라이브러리에서 서비스를 제거하려면 **삭제**를 클릭합니다.

서비스 게시

서비스를 게시하여 서비스에 대한 서비스 제공자 및 테넌트 액세스를 제어할 수 있습니다.

절차

- 1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.
 - a 왼쪽 패널에서 **서비스 라이브러리**를 선택합니다.

사용 가능한 서비스가 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되어 페이지당 12개 항목으로 표시됩니다. 각 카드는 항목이 vRealize Orchestrator 워크플로임을 나타내고 워크플로를 가져오는 서비스 범주에 해당하는 태그 및 서비스의 이름을 표시합니다.
- 2 선택된 서비스의 카드에서 **관리 > 워크플로 게시**를 선택합니다.

워크플로 게시 대화 상자가 표시됩니다
- 3 서비스 제공자에 게시하려면 **서비스 제공자에 게시**를 선택하고 **저장**을 클릭합니다.
- 4 특정 테넌트 조직에 게시하려면 **테넌트에 게시** 버튼을 선택합니다
 - a 사용 가능한 테넌트 조직이 포함된 목록이 표시됩니다. 워크플로를 게시할 테넌트 조직을 선택하고 **저장**을 클릭합니다.
- 5 모든 테넌트 조직에 게시하려면 **모든 테넌트에 게시**를 선택하고 **저장**을 클릭합니다.

vCloud Director의 사용자 지정 엔티티 정의는 vRealize Orchestrator 개체 유형에 바인딩된 개체 유형입니다. 서비스 제공자가 사용자 지정 엔티티 정의를 다른 서비스 제공자 또는 하나 이상의 테넌트에 게시하는 경우 vCloud Director 사용자는 해당 요구 사항에 따라 이러한 유형을 소유하고 관리하고 변경할 수 있습니다. 서비스 제공자 사용자 및 조직 사용자는 서비스를 실행하여 사용자 지정 엔티티를 인스턴스화하고 개체의 인스턴스에 작업을 적용할 수 있습니다.


본 장은 다음 항목을 포함합니다.

- 사용자 지정 엔티티 검색
- 사용자 지정 엔티티 정의 편집
- 사용자 지정 엔티티 정의 추가
- 사용자 지정 엔티티 인스턴스
- 사용자 지정 엔티티에 작업 연결
- 사용자 지정 엔티티에서 작업 분리
- 사용자 지정 엔티티 게시
- 사용자 지정 엔티티 삭제

사용자 지정 엔티티 검색

이름을 기준으로 사용자 지정 엔티티를 검색할 수 있습니다.

절차

- 1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.
 - a 왼쪽 패널에서 **사용자 지정 엔티티 정의**를 선택합니다.

사용자 지정 엔티티 목록이 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되며 페이지당 12개 항목이 표시됩니다. 각 카드는 사용자 지정 엔티티의 이름, 엔티티가 매핑된 vRealize Orchestrator 유형, 엔티티의 유형 및 설명(사용 가능한 경우)을 표시합니다.


- 2 페이지의 상단에 있는 **검색** 텍스트 상자에 찾으려는 엔티티 이름의 단어 또는 문자를 입력합니다.

검색 결과가 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되어 페이지당 12개 항목으로 표시됩니다.

사용자 지정 엔티티 정의 편집

사용자 지정 엔티티의 이름 및 설명을 수정할 수 있습니다. 엔티티가 바인딩된 vRealize Orchestrator 개체 유형 또는 엔티티의 유형을 변경할 수 없습니다. 이는 사용자 지정 엔티티의 기본 속성입니다. 기본 속성을 수정하려는 경우 사용자 지정 엔티티 정의를 삭제한 후 다시 만들어야 합니다.

절차

- 1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.

a 왼쪽 패널에서 **사용자 지정 엔티티 정의**를 선택합니다.

사용자 지정 엔티티 목록이 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되며 페이지당 12개 항목이 표시됩니다. 각 카드는 사용자 지정 엔티티의 이름, 엔티티가 매핑된 vRealize Orchestrator 유형, 엔티티의 유형 및 설명(사용 가능한 경우)을 표시합니다.

- 2 선택된 사용자 지정 엔티티의 카드에서 **작업 > 편집**을 선택합니다.

새 대화 상자가 열립니다.


- 3 사용자 지정 엔티티 정의의 이름 또는 설명을 수정합니다.

- 4 **확인**을 클릭하고 변경을 확인합니다.

사용자 지정 엔티티 정의 추가


사용자 지정 엔티티를 만들고 기존 vRealize Orchestrator 개체 유형에 매핑할 수 있습니다.

절차

- 1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.


a 왼쪽 패널에서 **사용자 지정 엔티티 정의**를 선택합니다.

사용자 지정 엔티티 목록이 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되며 페이지당 12개 항목이 표시됩니다. 각 카드는 사용자 지정 엔티티의 이름, 엔티티가 매핑된 vRealize Orchestrator 유형, 엔티티의 유형 및 설명(사용 가능한 경우)을 표시합니다.

- 2  아이콘을 클릭하여 새 사용자 지정 엔티티를 추가합니다.

새 대화 상자가 열립니다.

3 사용자 지정 엔티티 정의 마법사의 단계를 따릅니다.

단계	
이름 및 설명	새 엔티티의 이름과 설명(선택 사항)을 입력합니다. 엔티티 유형의 이름(예: <code>sshHost</code>)을 입력합니다.
vRO	드롭다운 메뉴에서 사용자 지정 엔티티 정의를 매핑하는 데 사용할 vRealize Orchestrator를 선택합니다. 참고 2개 이상의 vRealize Orchestrator 서버가 있는 경우 각 서버에 대해 별도로 사용자 지정 엔티티 정의를 만들어야 합니다.
유형	목록 보기 아이콘()을 클릭하여 플러그인별로 그룹화된 사용 가능한 vRealize Orchestrator 개체 유형을 검색합니다. 예를 들어 SSH > 호스트 입니다. 유형의 이름을 아는 경우 직접 텍스트 상자에 입력할 수 있습니다. 예: <code>SSH:Host</code> .
검토	지정한 세부 정보를 검토하고 완료 를 클릭하여 만들기를 완료합니다.



결과

새 사용자 지정 엔티티 정의가 카드 보기에 표시됩니다.

사용자 지정 엔티티 인스턴스

vCloud Director에서 사용자 지정 엔티티 정의로 이미 정의된 개체 유형이 되는 입력 매개 변수로 vRealize Orchestrator 워크플로를 실행하면 출력 매개 변수가 사용자 지정 엔티티의 인스턴스로 표시됩니다.

절차

- 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.
 - 왼쪽 패널에서 **사용자 지정 엔티티 정의**를 선택합니다.
사용자 지정 엔티티 목록이 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되며 페이지당 12개 항목이 표시됩니다. 각 카드는 사용자 지정 엔티티의 이름, 엔티티가 매핑된 vRealize Orchestrator 유형, 엔티티의 유형 및 설명(사용 가능한 경우)을 표시합니다.
- 선택된 사용자 지정 엔티티의 카드에서 **인스턴스**를 클릭합니다.
사용 가능한 인스턴스가 그리드 보기에 표시됩니다.
- 각 엔티티의 왼쪽에 있는 목록 표시줄()을 클릭하여 연결된 워크플로를 표시합니다.
워크플로를 클릭하면 엔티티 인스턴스를 입력 매개 변수로 가져오는 워크플로 실행이 시작됩니다.

사용자 지정 엔티티에 작업 연결

사용자 지정 엔티티 정의에 작업을 연결하여 특정 사용자 지정 엔티티의 인스턴스에서 vRealize Orchestrator 워크플로 집합을 실행할 수 있습니다.

절차

1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.

a 왼쪽 패널에서 **사용자 지정 엔티티 정의**를 선택합니다.

사용자 지정 엔티티 목록이 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되며 페이지당 12개 항목이 표시됩니다. 각 카드는 사용자 지정 엔티티의 이름, 엔티티가 매핑된 vRealize Orchestrator 유형, 엔티티의 유형 및 설명(사용 가능한 경우)을 표시합니다.

2 선택된 사용자 지정 엔티티의 카드에서 **작업 > 작업 연결**을 선택합니다.

새 대화 상자가 열립니다.

3 **VRO 워크플로에 사용자 지정 엔티티 연결** 마법사의 단계를 따릅니다.

단계	세부 정보
VRO 워크플로 선택	나열된 워크플로 중 하나를 선택합니다. 이는 서비스 라이브러리 페이지에서 사용 가능한 워크플로입니다.
워크플로 입력 매개 변수 선택	목록에서 사용 가능한 입력 매개 변수를 선택합니다. vRealize Orchestrator 워크플로의 유형을 사용자 지정 엔티티 정의의 유형과 연결합니다.
연결 검토	지정한 세부 정보를 검토하고 완료 를 클릭하여 연결을 완료합니다.


예

예를 들어 **SSH:Host** 유형의 사용자 지정 엔티티가 있는 경우 사용자 지정 엔티티의 유형과 일치하는 **sshHost** 입력 매개 변수를 선택하여 **Add a Root Folder to SSH Host** 워크플로와 연결할 수 있습니다.

사용자 지정 엔티티에서 작업 분리

연결된 작업 목록에서 vRealize Orchestrator 워크플로를 제거할 수 있습니다.

절차

1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.

a 왼쪽 패널에서 **사용자 지정 엔티티 정의**를 선택합니다.

사용자 지정 엔티티 목록이 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되며 페이지당 12개 항목이 표시됩니다. 각 카드는 사용자 지정 엔티티의 이름, 엔티티가 매핑된 vRealize Orchestrator 유형, 엔티티의 유형 및 설명(사용 가능한 경우)을 표시합니다.

2 선택된 사용자 지정 엔티티의 카드에서 **작업 > 작업 분리**를 선택합니다.

새 대화 상자가 열립니다.

3 제거할 워크플로를 선택하고 **작업 분리**를 클릭합니다.

vRealize Orchestrator 워크플로가 더 이상 사용자 지정 엔티티와 연결되어 있지 않습니다.

사용자 지정 엔티티 게시

사용자 지정 엔티티를 게시해야 다른 테넌트 또는 서비스 제공자의 사용자가 사용자 지정 엔티티 인스턴스를 입력 매개 변수로 사용하여 워크플로를 실행할 수 있습니다.

절차

- 1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.

- a 왼쪽 패널에서 **사용자 지정 엔티티 정의**를 선택합니다.

사용자 지정 엔티티 목록이 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되며 페이지당 12개 항목이 표시됩니다. 각 카드는 사용자 지정 엔티티의 이름, 엔티티가 매핑된 vRealize Orchestrator 유형, 엔티티의 유형 및 설명(사용 가능한 경우)을 표시합니다.

- 2 선택된 사용자 지정 엔티티의 카드에서 **작업 > 게시**를 선택합니다.

새 대화 상자가 열립니다.

- 3 사용자 지정 엔티티 정의를 서비스 제공자, 모든 테넌트 또는 선택된 테넌트에만 게시할지 선택합니다.


- 4 **저장**을 클릭하고 변경을 확인합니다.

선택된 상대방이 사용자 지정 엔티티 정의를 사용할 수 있습니다.

사용자 지정 엔티티 삭제

사용자 지정 엔티티가 더 이상 사용되지 않거나, 잘못 구성되었거나, vRealize Orchestrator 유형을 다른 사용자 지정 엔티티로 매핑하려는 경우 사용자 지정 엔티티 정의를 삭제할 수 있습니다.

절차

- 1 기본 메뉴()에서 **컨텐츠 라이브러리**를 선택합니다.

- a 왼쪽 패널에서 **사용자 지정 엔티티 정의**를 선택합니다.

사용자 지정 엔티티 목록이 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되며 페이지당 12개 항목이 표시됩니다. 각 카드는 사용자 지정 엔티티의 이름, 엔티티가 매핑된 vRealize Orchestrator 유형, 엔티티의 유형 및 설명(사용 가능한 경우)을 표시합니다.

- 2 선택된 사용자 지정 엔티티의 카드에서 **작업 > 삭제**를 선택합니다.

- 3 삭제를 확인합니다.

사용자 지정 엔티티가 카드 보기에서 제거됩니다.