

VMware Cloud Director 테 넌트 포털 가이드

수정 날짜: 2021년 4월 4일
VMware Cloud Director 10.2

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

VMware Cloud Director™ 테넌트 포털 가이드 11

1 VMware Cloud Director 테넌트 포털 시작 12

- VMware Cloud Director™ 이해 12
- VMware Cloud Director 테넌트 포털 로그인 13
- VMware Cloud Director 테넌트 포털 역할 및 권한 14
- VMware Cloud Director 테넌트 포털 사용 14
- VMware Cloud Director 글로벌 검색 사용 15
- VMware Cloud Director 빠른 검색 사용 16
- 작업 보기 17
- 진행 중인 작업 중지 18
- 이벤트 보기 18
- 사용자 기본 설정 지정 19

2 가상 시스템 작업 21

- 가상 시스템 아키텍처 22
- 가상 시스템 암호화 23
- 가상 시스템 보기 24
- 새 독립형 가상 시스템 만들기 25
- 가상 시스템의 빠른 프로비저닝 26
- 가상 시스템 콘솔 열기 27
 - 클라이언트에 VMware Remote Console 설치 27
 - 가상 시스템 원격 콘솔 열기 28
 - 웹 콘솔 열기 28
- 가상 시스템에서 전원 작업 수행 29
 - 가상 시스템의 전원 켜기 29
 - 가상 시스템의 전원 끄기 30
 - 게스트 운영 체제 종료 30
 - 가상 시스템 재설정 31
 - 가상 시스템 일시 중단 31
 - 가상 시스템의 일시 중단된 상태 삭제 32
 - 여러 VM 전원 켜기 32
 - 여러 가상 시스템 전원 끄기 32
 - 여러 가상 시스템의 일시 중단된 상태 삭제 33
 - 여러 가상 시스템 재설정 33
- 가상 시스템에 VMware Tools 설치 34

가상 시스템의 가상 하드웨어 버전 업그레이드	34
가상 시스템 속성 편집	35
가상 시스템의 일반 속성 변경	35
가상 시스템의 하드웨어 속성 변경	36
가상 시스템의 게스트 운영 체제 사용자 지정 속성 변경	39
가상 시스템의 고급 속성 변경	42
미디어 삽입	44
미디어 꺼내기	45
다른 vApp에 가상 시스템 복사	45
다른 vApp으로 가상 시스템 이동	46
가상 시스템 선호도 및 반선호도	47
선호도 및 반선호도 규칙 보기	47
선호도 규칙 만들기	48
반선호도 규칙 만들기	48
선호도 또는 반선호도 규칙 편집	49
선호도 또는 반선호도 규칙 삭제	49
가상 시스템 모니터링	50
스냅샷 작업	51
가상 시스템의 스냅샷 만들기	51
스냅샷으로 가상 시스템 되돌리기	52
가상 시스템의 스냅샷 제거	53
가상 시스템 임대 갱신	53
가상 시스템 삭제	54
자동 스케일 그룹	54
스케일 그룹 생성	55
자동 스케일링 규칙 추가	55

3 vApp 작업 57

vApp 보기	58
새 vApp 작성	58
OVF 패키지에서 vApp 만들기	60
카탈로그에서 vApp 추가	63
vApp 템플릿에서 vApp 만들기	64
vApp으로 vCenter Server에서 가상 시스템 가져오기	66
vApp에서 전원 작업 수행	66
vApp 전원 켜기	66
vApp 전원 끄기	67
vApp 재설정	67
vApp 일시 중단	68
vApp의 일시 중단된 상태 삭제	68

여러 vApp 전원 켜기	68
여러 vApp 전원 끄기	69
여러 vApp의 일시 중단된 상태 삭제	69
여러 vApp 재설정	70
여러 vApp 일시 중단	70
vApp 열기	71
vApp 속성 편집	71
vApp의 일반 속성 편집	71
vApp에서 가상 시스템의 시작 및 중지 순서 편집	72
vApp의 게스트 속성 편집	73
vApp 공유	73
vApp 네트워크 다이어그램 표시	74
vApp의 네트워크 작업	75
vApp 네트워크 보기	75
vApp 네트워크 펜싱	76
vApp에 네트워크 추가	77
vApp 네트워크에 대한 네트워크 서비스 구성	78
vApp 네트워크 삭제	84
스냅샷 작업	85
vApp의 스냅샷 만들기	85
스냅샷으로 vApp 되돌리기	86
vApp의 스냅샷 제거	86
여러 vApp의 스냅샷 생성	87
여러 vApp의 스냅샷 제거	87
여러 vApp을 스냅샷으로 되돌리기	88
vApp의 소유자 변경	88
다른 가상 데이터 센터로 vApp 이동	89
다른 가상 데이터 센터에 중지된 vApp 복사	89
전원이 켜진 vApp 복사	90
vApp에 가상 시스템 추가	91
vApp을 vApp 템플릿으로 카탈로그에 저장	92
OVF 패키지로 vApp 다운로드	93
vApp 임대 갱신	94
vApp 삭제	94
여러 vApp 삭제	95

4 Kubernetes 클러스터 작업 96

조직 VDC Kubernetes 정책 추가	97
조직 VDC Kubernetes 정책 편집	99
Tanzu Kubernetes 클러스터 만들기	99

네이티브 Kubernetes 클러스터 만들기	101
VMware Tanzu Kubernetes Grid Integrated Edition 클러스터 만들기	102
Tanzu Kubernetes 클러스터의 서비스에 대한 외부 액세스 구성	103

5 네트워크 사용 106

조직 가상 데이터 센터 네트워크 관리	109
사용 가능한 조직 VDC 네트워크 보기	110
격리된 조직 가상 데이터 센터 네트워크 추가	110
라우팅된 조직 가상 데이터 센터 네트워크 추가	112
직접 조직 가상 데이터 센터 네트워크 추가	114
가져온 NSX-T Data Center 논리적 스위치를 사용하여 조직 VDC 네트워크 추가	115
조직 가상 데이터 센터 네트워크의 일반 설정 편집	116
Edge 게이트웨이에 조직 가상 데이터 센터 네트워크 연결	116
Edge 게이트웨이에서 조직 VDC 네트워크의 연결 끊기	117
라우팅된 조직 VDC 네트워크의 인터페이스 변환	117
조직 가상 데이터 센터 네트워크에 사용되는 IP 주소 보기	118
조직 가상 데이터 센터 네트워크 IP 풀에 IP 주소 추가	118
조직 가상 데이터 센터 네트워크에서 사용되는 IP 범위 편집 또는 제거	119
조직 가상 데이터 센터 네트워크의 DNS 설정 편집	119
격리된 조직 가상 데이터 센터 네트워크의 DHCP 설정 구성	120
NSX-T Data Center에서 지원되는 라우팅된 조직 가상 데이터 센터 네트워크에 DHCP 풀 추가	121
NSX Data Center for vSphere에서 지원하는 격리된 조직 가상 데이터 센터 네트워크에 대한 기존 DHCP 풀 편집 또는 삭제	121
조직 가상 데이터 센터 네트워크 재설정	122
조직 가상 데이터 센터 네트워크 삭제	122
NSX-T Data Center를 사용하여 데이터 센터 그룹 네트워킹 관리	123
NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹 관리	124
NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에서 분산 방화벽 사용	126
NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹 네트워크 관리	130
NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹의 송신 지점 관리	135
NSX Data Center for vSphere를 사용하여 데이터 센터 그룹 네트워킹 관리	137
NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹 관리	138
NSX Data Center for vSphere에서 지원하는 데이터 센터 그룹 네트워크 관리	151
NSX Data Center for vSphere Edge 게이트웨이 서비스 관리	153
NSX Data Center for vSphere로 VMware Cloud Director 고급 네트워킹 시작	154
NSX Data Center for vSphere로 테넌트 방화벽 구성	154
NSX Data Center for vSphere Edge 게이트웨이 DHCP 관리	164
NSX Data Center for vSphere Edge 게이트웨이에서 NAT(네트워크 주소 변환) 관리	168
NSX Data Center for vSphere Edge 게이트웨이에 대한 고급 라우팅 구성	171

NSX Data Center for vSphere로 로드 밸런싱	180
NSX Data Center for vSphere Edge 게이트웨이에서 VPN을 사용하여 보안 액세스 구성	192
NSX Data Center for vSphere Edge 게이트웨이의 SSL 인증서 관리	216
NSX Data Center for vSphere Edge 게이트웨이에 대한 사용자 지정 개체 그룹화	223
NSX Data Center for vSphere Edge 게이트웨이에 대한 통계 및 로그	226
NSX Data Center for vSphere Edge 게이트웨이에 대한 SSH 명령줄 액세스 사용	227
NSX Data Center for vSphere Edge 게이트웨이에 대한 보안 태그 작업	228
NSX Data Center for vSphere Edge 게이트웨이에 대한 보안 그룹 작업	232
NSX-T Data Center Edge 게이트웨이 관리	235
NSX-T Data Center Edge 게이트웨이에 IP 집합 추가	236
NSX-T Data Center Edge 게이트웨이 방화벽 규칙 추가	236
NSX-T Edge 게이트웨이에 SNAT 또는 DNAT 규칙 추가	237
NSX-T Edge 게이트웨이에서 DNS 전달자 서비스 구성	240
사용자 지정 애플리케이션 포트 프로파일 생성	241
NSX-T Data Center Edge 게이트웨이의 IPsec 정책 기반 VPN	241
전용 외부 네트워크 서비스 구성	244
NSX Advanced 로드 밸런싱 사용	249
6 명명된 디스크 사용 및 스토리지 정책 검토	256
명명된 디스크 생성 및 사용	256
명명된 디스크 만들기	256
명명된 디스크 편집	257
가상 시스템에 명명된 디스크 연결	258
명명된 디스크 삭제	258
스토리지 정책 속성 검토	258
7 가상 데이터 센터 속성 검토 및 편집	260
가상 데이터 센터 속성 검토	260
가상 데이터 센터 메타데이터 검토	260
조직 VDC에 대한 액세스를 조직의 특정 사용자 및 그룹으로 제한	261
8 전용 vCenter Server 인스턴스, 끝점 및 프록시 사용	262
Chrome Browser Extension for VMware Cloud Director 사용	263
프록시 설정으로 브라우저 구성	263
끝점을 사용하여 구성 요소의 UI에 로그인	264
9 vApp 템플릿 작업	265
vApp 템플릿 보기	265
OVF 파일에서 vApp 템플릿 만들기	266
vApp 템플릿으로 vCenter Server에서 가상 시스템 가져오기	267

vApp 템플릿에 VM 배치 정책 및 VM 크기 조정 정책 할당	267
vApp 템플릿 다운로드	268
vApp 템플릿 삭제	269
10 미디어 파일 작업	270
미디어 파일 업로드	270
미디어 파일 삭제	271
미디어 파일 다운로드	271
11 카탈로그 작업	272
카탈로그 보기	273
카탈로그 만들기	273
카탈로그 공유	274
카탈로그 삭제	275
카탈로그의 소유자 변경	275
카탈로그에 대한 메타데이터 관리	276
카탈로그 게시	276
외부 카탈로그 구독	277
구독된 카탈로그의 위치 URL 및 암호 업데이트	277
구독된 카탈로그 동기화	278
12 조직 가상 데이터 센터 템플릿 작업	279
사용 가능한 가상 데이터 센터 템플릿 보기	279
템플릿에서 가상 데이터 센터 인스턴스화	280
13 사용자, 그룹 및 역할 관리	281
사용자 관리	281
사용자 생성	281
사용자 가져오기	283
사용자 수정	283
사용자 계정 비활성화 또는 활성화	284
사용자 삭제	284
잠긴 사용자 계정 잠금 해제	285
사용자의 리소스 할당량 관리	285
그룹 관리	286
그룹 가져오기	286
그룹 삭제	287
그룹 편집	287
그룹의 리소스 할당량 관리	288
역할 및 권한	289

미리 정의된 역할 및 역할 권한	289
미리 정의된 글로벌 테넌트 역할의 권한	291
사용자 지정 테넌트 역할 만들기	296
사용자 지정 테넌트 역할 편집	297
역할 삭제	297

14 ID 제공자 구성 298

조직에서 SAML ID 제공자를 사용하도록 설정	298
조직에 대한 LDAP 설정 편집	300
LDAP 연결 구성, 테스트 및 동기화	300

15 인증서 관리 303

신뢰할 수 있는 인증서 가져오기	303
인증서 라이브러리에 인증서 가져오기	304

16 조직 관리 305

조직 이름 및 설명 편집	305
e-메일 설정 수정	306
SMTP 설정 테스트	307
조직의 가상 시스템에 대한 도메인 설정 수정	307
다중 사이트 작업	308
다중 사이트 배포 구성 및 관리	308
임대 이해	309
조직 내의 vApp 및 vApp 템플릿 임대 정책 수정	309
조직 내의 암호 및 사용자 계정 정책 수정	310
권고 대시보드 만들기	311

17 서비스 라이브러리 작업 312

서비스 검색	312
서비스 실행	312

18 정의된 엔티티 관리 314

사용자 지정 엔티티 정의 작업	316
사용자 지정 엔티티 검색	316
사용자 지정 엔티티 정의 편집	317
사용자 지정 엔티티 정의 추가	317
사용자 지정 엔티티 인스턴스	318
사용자 지정 엔티티에 작업 연결	318
사용자 지정 엔티티 정의에서 작업 분리	319
사용자 지정 엔티티 게시	320

사용자 지정 엔티티 삭제 320

VMware Cloud Director™ 테넌트 포털 가이드

"VMware Cloud Director™ 테넌트 포털 설명서"는 VMware Cloud Director 테넌트 포털 사용 방법에 대한 정보를 제공합니다. 이 릴리스에서는 테넌트 포털을 사용하여 조직을 관리하고, 가상 시스템, vApp 및 vApp 내의 네트워크를 만들고 구성합니다. VMware Cloud Director 환경 내에서 VMware NSX® for vSphere®에 제공되는 고급 네트워킹 기능을 구성할 수도 있습니다. VMware Cloud Director 테넌트 포털을 사용하면 카탈로그, vApp 및 VDC 템플릿을 생성 및 관리하고 크로스 가상 데이터 센터 네트워크를 생성 및 관리할 수도 있습니다.

대상 사용자

이 가이드는 VMware Cloud Director 테넌트 포털의 기능을 사용하려는 모든 사용자를 대상으로 합니다. 이 정보는 테넌트 포털을 사용하여 조직을 관리하고 가상 시스템, vApp, 네트워크 등을 관리하는 **조직 관리자**를 주요 대상으로 작성되었습니다.

VMware 기술 자료 용어집

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

사용 약관

VMware는 귀하에게 귀사의 운영 프로세스를 반영하도록 이 테넌트 사용자 가이드를 수정하고 수정된 가이드를 복제하여 귀사의 고객에게 배포할 수 있는 권한을 부여합니다. 수정된 가이드에 대한 액세스 비용으로 고객에게 요금을 청구할 수 없습니다. 귀하는 이 가이드가 어떠한 종류의 보증도 없이 위에 설명된 목적으로만 무료로 제공된다는 점을 인정합니다. 따라서 귀하에게 이 가이드에 대한 액세스 권한을 제공하는 것과 관련하여 발생하는 VMware 및 VMware의 공급업체의 총 책임은 \$100를 초과하지 않습니다. 어떠한 경우에도 VMware 또는 VMware의 공급업체는 모든 책임 이론에 따라 발생하는 간접적, 부수적, 특수적 또는 결과적 손해(비즈니스 이익 손실, 비즈니스 중단 또는 비즈니스 정보 손실에 대한 손해를 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않으며, VMware 또는 그 공급업체가 그러한 손해의 가능성에 대해 조언을 받은 경우에도 마찬가지입니다. 이러한 제한은 모든 제한된 구제책이 본래 목적을 달성하지 못하더라도 적용됩니다.

VMware Cloud Director 테넌트 포털 시작

1

테넌트 포털에 로그인하면 가상 시스템 및 vApp을 만드는 것부터 고급 네트워킹 구성을 설정하고 vRealize Orchestrator 워크플로를 실행하는 것에 이르기까지 다수의 작업을 완료할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- VMware Cloud Director™ 이해
- VMware Cloud Director 테넌트 포털 로그인
- VMware Cloud Director 테넌트 포털 역할 및 권한
- VMware Cloud Director 테넌트 포털 사용
- VMware Cloud Director 글로벌 검색 사용
- VMware Cloud Director 빠른 검색 사용
- 작업 보기
- 진행 중인 작업 중지
- 이벤트 보기
- 사용자 기본 설정 지정

VMware Cloud Director™ 이해

VMware Cloud Director™에서는 조직의 구성원이 조직의 리소스와 상호 작용하여 vApp 및 가상 시스템을 만들고 관련 작업을 수행할 수 있도록 웹 기반 테넌트 포털에 대한 역할 기반 액세스 권한을 제공합니다.

조직에 액세스하려면 먼저 VMware Cloud Director **시스템 관리자**가 조직을 만들고, 조직에 리소스를 할당하고, 테넌트 포털 액세스를 위한 URL을 제공해야 합니다. 각 조직에는 구성원을 추가하고 정책 및 기본 설정을 설정하여 조직 설정을 완료하는 한 명 이상의 **조직 관리자**가 포함됩니다. 조직이 설정되면 관리자가 아닌 사용자가 로그인하여 가상 시스템 및 vApp을 만들고 사용하고 관리할 수 있습니다.

조직

조직은 사용자, 그룹 및 계산 리소스 집합에 대한 관리 단위입니다. 사용자는 **조직 관리자**가 해당 사용자를 만들거나 가져올 때 설정한 자격 증명을 입력하여 조직 수준에서 인증을 받습니다. **시스템 관리자**는 조직을 만들고 프로비저닝하고, **조직 관리자**는 조직의 사용자, 그룹 및 카탈로그를 관리합니다.

사용자 및 그룹

조직에는 임의의 수의 사용자 및 그룹이 포함될 수 있습니다. 사용자는 조직 관리자가 로컬에서 생성하거나 디렉토리 서비스에서 가져올 수 있습니다. 그룹은 디렉토리 서비스에서 가져와야 합니다. 조직 내의 권한은 사용자 및 그룹에 대한 권한 및 역할 할당을 통해 제어됩니다.

가상 데이터 센터

조직 가상 데이터 센터는 조직에 리소스를 제공합니다. 가상 데이터 센터는 가상 시스템을 저장, 배포 및 운영할 수 있는 환경을 제공합니다. 또한 가상 CD 및 DVD 미디어에 스토리지를 제공합니다. 한 조직에 여러 개의 가상 데이터 센터가 있을 수 있습니다.

조직 가상 데이터 센터 네트워크

조직 가상 데이터 센터 네트워크는 VMware Cloud Director 조직 가상 데이터 센터 안에 포함되며 조직의 모든 vApp이 사용할 수 있습니다. 조직 가상 데이터 센터 네트워크를 사용하면 조직 내의 vApp이 서로 통신할 수 있습니다. 조직 가상 데이터 센터 네트워크를 외부 네트워크에 연결하거나 격리를 통해 조직 내부용으로 사용할 수 있습니다. **시스템 관리자**만 조직 가상 데이터 센터 네트워크를 만들 수 있지만 **조직 관리자**는 제공되는 네트워크 서비스를 포함하여 조직 가상 데이터 센터 네트워크를 관리할 수 있습니다.

vApp 네트워크

vApp 네트워크는 vApp 내에 포함되어 있고 vApp 네트워크를 사용하면 vApp의 가상 시스템이 서로 통신할 수 있습니다. vApp 네트워크를 조직 가상 데이터 센터 네트워크에 연결하여 vApp이 조직 내의 다른 vApp과 통신하도록 허용할 수 있으며, 조직 가상 데이터 센터 네트워크가 외부 네트워크에 연결된 경우 조직 외부의 vApp과도 통신하도록 허용할 수 있습니다.

카탈로그

조직에서는 카탈로그를 사용하여 vApp 템플릿과 미디어 파일을 저장합니다. 카탈로그에 액세스할 수 있는 조직의 구성원은 vApp 템플릿 및 미디어 파일을 사용하여 자체 vApp을 만들 수 있습니다. **조직 관리자**는 공개 카탈로그의 항목을 조직 카탈로그에 복사할 수 있습니다.

전용 vCenter Server 인스턴스(SDDC) 및 프록시

SDDC(소프트웨어 정의 데이터 센터)는 전체 vCenter Server 환경을 캡슐화합니다. 전용 vCenter Server 인스턴스에는 기본 환경의 다양한 구성 요소에 대한 액세스를 제공하는 하나 이상의 프록시가 포함될 수 있습니다. **시스템 관리자**는 조직에 하나 이상의 전용 vCenter Server 인스턴스를 게시할 수 있습니다. 포함된 프록시를 사용하여 프록시 설정된 구성 요소의 UI 또는 API에 액세스할 수 있습니다.

VMware Cloud Director 테넌트 포털 로그인

조직에 특정된 URL을 사용하여 VMware Cloud Director 테넌트 포털에 액세스할 수 있습니다.

조직의 테넌트 포털 URL을 모르는 경우 **조직 관리자**에게 문의하십시오. 지원되는 브라우저 및 구성에 대한 내용은 "VMware Cloud Director 릴리스 정보"를 참조하십시오.

절차

- 1 웹 브라우저에서 조직의 테넌트 포털 URL로 이동합니다.

예: <https://cloud.example.com/tenant/myOrg>.

- 2 사용자 이름 및 암호를 입력하고 **로그인**을 클릭합니다.

VMware Cloud Director 테넌트 포털 역할 및 권한

VMware Cloud Director에는 미리 구성된 사용자 역할 및 권한 집합이 포함됩니다. 조직에서 기본적으로 만들어지는 역할 또는 조직 관리자가 만드는 다른 역할이 VMware Cloud Director 테넌트 포털에 액세스할 수 있습니다.

다음 조직 역할이 할당된 사용자는 테넌트 포털에 액세스할 수 있습니다. 표시되는 항목과 수행할 수 있는 작업은 특정 역할에 연결된 권한에 따라 다릅니다.

- 조직 관리자
- 카탈로그 작성자
- vApp 작성자
- vApp 사용자
- 콘솔 액세스 전용

미리 정의된 역할과 해당 권한에 대한 자세한 내용은 [미리 정의된 역할 및 역할 권한](#)을 참조하십시오.

VMware Cloud Director 테넌트 포털 사용

가상 데이터 센터가 2개 이상인 경우, VMware Cloud Director 테넌트 포털에 로그인하면 **데이터 센터** 대시보드 화면으로 이동됩니다. 가상 데이터 센터가 하나만 있는 경우, VMware Cloud Director 테넌트 포털에 로그인하면 해당 데이터 센터로 바로 이동됩니다.

데이터 센터 대시보드 화면은 지리적으로 분산된 클라우드 환경을 단일 엔티티로 테넌트에 보여 주는 VMware Cloud Director 다중 사이트 기능의 일부입니다. 다중 사이트에 대한 자세한 내용은 [다중 사이트 작업](#) 섹션을 참조하십시오.

이 대시보드는 VMware Cloud Director 가상 데이터 센터 및 사이트를 통합하여 보여주며, 단일 조직에 제한되지 않습니다. 다중 셀 및 다중 조직 환경에서는 연결된 다른 모든 조직에 대한 가상 데이터 센터도 볼 수 있습니다.

참고 테넌트 사용자는 보유한 권한에 따라 조직의 모든 구성원 사이트를 보거나 일부 사이트만 볼 수 있습니다.

조직에 대한 정보는 요약 리본의 맨 위에 표시됩니다.

조직 관리자로 로그인하면 다음 사항을 볼 수 있습니다.

- 사이트, 조직 및 가상 데이터 센터의 수

- 실행 중인 vApp 및 가상 시스템의 총 수
- CPU, 메모리 및 스토리지와 같은 사용된 하드웨어 리소스

가상 데이터 센터는 카드 보기로 표시됩니다. 각 카드에는 가상 센터가 속한 조직, vApp 수, 총 가상 시스템 수 및 실행 중인 가상 시스템 수에 관한 정보가 포함됩니다. 카드에는 데이터 센터의 사용 가능한 CPU, 메모리 및 스토리지 용량과 현재 리소스 할당 및 예약에 대한 실시간 메트릭도 표시됩니다.

맨 위 탐색에서 다른 메뉴 항목으로 이동할 수 있습니다.

메뉴 항목	설명
데이터 센터	조직의 가상 데이터 센터 , 데이터 센터 그룹 및 전용 vSphere 데이터 센터 리소스로 이동합니다.
가상 데이터 센터	조직 내의 가상 데이터 센터가 표시되는 가상 데이터 센터 화면으로 이동합니다.
전용 vSphere 데이터 센터	서비스 제공자가 조직에 게시한 전용 vSphere 데이터 센터를 표시하는 화면으로 이동합니다.
애플리케이션	조직의 가상 애플리케이션 및 가상 시스템 리소스로 이동합니다.
라이브러리	vApp 템플릿, 카탈로그, 미디어 및 기타 파일 형식에 대한 통합된 보기로 이동합니다. 이러한 템플릿 및 파일을 사용하여 가상 시스템 또는 vApp을 배포합니다.
네트워킹	조직의 네트워크, Edge 게이트웨이 및 데이터 센터 그룹으로 이동합니다.
관리	액세스 제어 , ID 제공자 구성 화면으로, 그리고 조직의 일반, 이메일, 게스트 개인 설정, 메타데이터, 다중 사이트 및 정책 설정으로 이동합니다.
모니터	작업 및 이벤트 화면으로 이동합니다. 작업 화면에는 VMware Cloud Director에서 보고한 작업이 표시됩니다. 이벤트 화면에는 VMware Cloud Director에서 보고한 이벤트가 표시됩니다.

Branding Cloud Director OpenAPI를 사용하여 VMware Cloud Director 테넌트 포털을 사용자 지정할 수 있습니다. Cloud Director OpenAPI 사용에 대한 자세한 내용은 <https://code.vmware.com>에서 "Cloud Director OpenAPI 시작하기" 문서를 참조하십시오.

VMware Cloud Director 글로벌 검색 사용

VMware Cloud Director 글로벌 검색을 사용하여 사용자 환경의 개체 이름 또는 이름의 일부로 검색을 수행할 수 있습니다. 또한 가상 시스템의 IP 주소가 정적인 경우 해당 IP 주소로 가상 시스템을 검색할 수도 있습니다.

미리 설정된 개체의 목록은 다음과 같습니다.

- 데이터 센터
- vApp 템플릿
- vApp
- 가상 시스템
- vApp 네트워크
- 카탈로그

가상 시스템이 DHCP에서 할당된 IP 주소를 사용하는 경우 검색에서 해당 IP 주소를 반환하지 않습니다. DHCP에서 할당된 IP 주소를 사용하는 가상 시스템을 검색하려는 경우에는 이름으로 검색해야 합니다.

기본적으로 로컬 사이트의 개체 내에서만 검색할 수 있습니다. 다중 사이트 환경을 사용하는 경우에는 여러 사이트 중에 선택하여 검색을 수행할 수 있습니다.

절차

- 1 VMware Cloud Director 테넌트 포털의 오른쪽 위에서 **검색** 아이콘을 클릭합니다.
- 2 (선택 사항) **고정** 아이콘을 클릭하여 검색 패널을 고정합니다.
- 3 **검색** 텍스트 상자에 일치하는 개체 이름 또는 가상 시스템의 정적 IP 주소를 검색하는 데 사용할 기호, 이름의 일부 또는 IP 주소를 입력합니다.
- 4 다중 사이트 환경을 사용하는 경우에는 검색을 수행할 사이트를 선택합니다.
- 5 **Enter** 키를 누릅니다.

결과

개체 유형별로 일치하는 상위 5개의 결과가 표시됩니다. 결과는 사전순으로 정렬됩니다.

다음에 수행할 작업

- 더 많은 결과를 보려면(있는 경우) 각 개체 유형 아래에서 **더 많이 로드**를 클릭합니다.
- 검색 결과의 특정 개체에 대한 더 많은 정보를 보려면 해당 개체를 가리킵니다.
- 특정 개체를 관리하려면, 예를 들어 개체의 설정을 보거나 수정하려면 개체를 클릭합니다. 개체에 대한 세부 정보가 왼쪽에 표시됩니다.

VMware Cloud Director 빠른 검색 사용

VMware Cloud Director 빠른 검색을 사용하여 화면, 엔티티 및 작업을 찾을 수 있습니다. 결과는 UI에서 있는 위치에 따라 다릅니다.

컨텍스트, 엔티티 선택 여부 및 특정 엔티티에 대해 사용 가능한 작업에 따라 결과가 달라집니다. 검색 결과는 섹션으로 그룹화됩니다.

- **글로벌 탐색** - 이 섹션의 결과는 특정 엔티티(예: Edge 게이트웨이, LDAP, 작업, 신뢰할 수 있는 인증서, 가상 시스템 등)와 관련이 없습니다. 이러한 결과는 UI에서 있는 위치에 관계없이 얻을 수 있습니다.
- **상황별 탐색** - 이 섹션의 결과는 UI에서 선택한 엔티티에 따라 다릅니다. 예를 들어 VM, 네트워크 다이어그램 등과 같은 vApp 특정 보기가 있습니다. vApp과 같은 엔티티를 선택하면 글로벌 및 상황별 탐색 결과와 엔티티에 적용할 수 있는 모든 작업이 검색에 표시됩니다.
- **상황별 작업** - 이 섹션의 결과는 UI에서 선택한 엔티티에 따라 다릅니다. UI에서 있는 위치와 선택한 엔티티에 따라, 빠른 검색 결과를 사용하여 엔티티와 관련된 작업을 수행할 수 있습니다. 예를 들어 가상 시스템의 세부 정보 보기에서 검색하면 선택한 VM에서 수행할 수 있는 작업, 글로벌 보기, 상황별 보기의 결과가 표시됩니다.

- 이름으로 엔티티 검색 - 엔티티 목록을 보고 있으면 목록에 있는 것과 동일한 유형의 엔티티 이름도 검색 결과에 포함될 수 있습니다. 예를 들어 VM 목록을 보고 있으면 글로벌 탐색 일치 항목 및 일치하는 VM 이름이 검색 결과에 포함됩니다. 보고 있는 목록에 엔티티가 두 페이지 이상 있으면 검색 시 전체 엔티티 목록이 확인되고 현재 페이지에 표시되지 않는 이름이 표시될 수 있습니다.

절차

- 1 **빠른 검색** 창을 엽니다.
 - 위쪽 탐색 모음에서 **도움말** 메뉴를 클릭하고 **빠른 검색**을 선택합니다.
 - 사용하는 운영 체제에 따라 **Ctrl+** 또는 **Cmd+**을 누릅니다.
- 2 검색 조건을 입력합니다.
- 3 결과를 찾아보고 옵션을 선택하거나 **Enter** 키를 눌러서 작업을 수행합니다.

위쪽 및 아래쪽 화살표 키를 사용하여 검색 결과를 탐색할 수 있습니다.

작업 보기


테넌트 포털에서 최근 작업 목록을 세부 정보 및 상태와 함께 볼 수 있습니다. 모든 작업의 목록도 볼 수 있습니다.

기본적으로 **최근 작업** 패널은 테넌트 포털 맨 아래에 표시되고 최근에 실행된 작업 목록을 포함합니다. 작업(예: 가상 시스템 만들기)을 시작하면 해당 작업이 패널에 표시됩니다. **최근 작업** 패널을 최소화하면 실행 중이거나 실패한 최근 작업 수가 표시됩니다. 이중 화살표를 클릭하면 **최근 작업** 패널을 언제든지 다시 열 수 있습니다.

작업 보기에는 모든 작업이 나열되고 작업이 실행된 시기와 완료 성공 여부가 표시됩니다. 이 보기는 환경의 문제를 해결하기 위한 첫 번째 단계입니다. 작업 보기에는 가상 시스템 또는 vApp 만들기과 같은 장기 실행 작업이 포함됩니다.

절차

- 1 위쪽 탐색 모음에서 **모니터** 및 **작업**을 클릭합니다.

모든 작업의 목록이 작업이 실행된 시간 및 작업의 상태와 함께 표시됩니다.
- 2 편집기 아이콘()을 클릭하여 작업에 대해 표시할 세부 정보를 변경합니다.
- 3 (선택 사항) 작업 세부 정보를 보려면 작업의 이름을 클릭합니다.

작업 세부 정보에는 실패한 이유, 작업이 실패한 시간 등이 포함됩니다.

세부	설명
작업	수행한 작업의 이름입니다.
작업 ID	작업의 ID입니다.
유형	작업이 수행되는 개체입니다. 예를 들어, 가상 시스템 생성한 경우 형식은 vm입니다.
조직	조직 이름입니다.

세부	설명
상태	성공, 실행 중 또는 실패와 같은 작업의 상태입니다.
이니시에이터	작업을 시작한 사용자입니다.
시작 시간	작업이 시작된 날짜 및 시간입니다.
완료 시간	작업이 성공하거나 실패한 날짜 및 시간입니다.
서비스 네임스페이스	<i>com.vmware.cloud</i> 와 같은 서비스 이름입니다.
세부 정보	작업이 실패한 이유입니다. 예를 들어 가상 시스템의 스냅샷을 만들려고 하는데 스토리지가 부족하여 작업이 실패하면 작업 세부 정보는 요청된 작업은 VDC 스토리지 할당량을 초과함: 스토리지 정책 “*”에는 8,693MB가 남아 있고 41,472MB가 요청되었습니다. 유형입니다.

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** 아이콘을 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 위쪽 탐색 모음에서 **모니터** 및 **이벤트**를 클릭합니다.
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 Task 'Modify vApp' start입니다.
이벤트 ID	작업의 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 Task 'Modify vApp' start 이벤트의 대상은 <i>vdcUpdateVapp</i> 입니다.
상태	성공 또는 실패와 같은 이벤트의 상태입니다.
서비스 네임스페이스	<i>com.vmware.cloud</i> 와 같은 서비스 이름입니다.
조직	조직의 이름입니다.
소유자	이벤트를 트리거한 사용자입니다.
발생 시간	이벤트가 발생한 날짜 및 시간입니다.

사용자 기본 설정 지정

시스템에 로그인할 때마다 적용되는 표시 내용 및 시스템 경고 기본 설정을 지정할 수 있습니다.

임대에 대해 자세히 알려면 [임대 이해](#) 항목을 참조하십시오.

절차

- 1 위쪽 탐색 모음에서 사용자 이름을 클릭하고 **사용자 기본 설정**을 선택합니다.
- 2 로그인 시 표시할 페이지를 선택합니다.
 - a **시작 페이지** 옆의 라디오 버튼을 선택하고 **편집**을 클릭합니다.
 - b 드롭다운 메뉴에서 옵션을 선택하고 **저장**을 클릭합니다.
- 3 런타임 임대 만료에 대한 e-메일 알람을 구성합니다.
 - a **배포 임대 경고 시간** 옆에 있는 라디오 버튼을 선택하고 **편집**을 클릭합니다.
 - b 초 단위로 값을 입력하고 **저장**을 클릭합니다.

4 스토리지 임대 만료에 대한 e-메일 알림을 구성합니다.

- a **스토리지 임대 경고 시간** 옆에 있는 라디오 버튼을 선택하고 **편집**을 클릭합니다.
- b 초 단위로 값을 입력하고 **저장**을 클릭합니다.

가상 시스템 작업

2

가상 시스템은 물리적 컴퓨터처럼 운영 체제와 애플리케이션을 실행하는 소프트웨어 컴퓨터입니다. 가상 시스템은 규격 및 구성 파일의 집합으로 구성되며 호스트의 물리적 리소스에 의해 지원됩니다. 모든 가상 시스템에는 물리적 하드웨어와 동일한 기능을 제공하지만 이동성이 좋고 더욱 안전하며 관리하기 쉬운 가상 디바이스가 있습니다.

물리적 시스템에서 실행할 수 있는 작업 외에도 VMware Cloud Director 가상 시스템은 가상 시스템 상태 스냅샷 만들기 및 호스트 간 가상 시스템 이동과 같은 가상 인프라 작업을 지원합니다.

VMware Cloud Director 9.5 부터는 가상 시스템에서 IPv6 연결이 지원됩니다. IPv6 네트워크에 연결된 가상 시스템에 IPv6 주소를 할당할 수 있습니다.

중요 가상 시스템 작업에 대한 모든 단계는 카드 보기에 문서화되어 있으며, 둘 이상의 가상 데이터 센터가 있다는 가정 하에 준비되었습니다. 그리드 보기에서 동일한 절차를 완료할 수도 있지만 단계가 약간 다를 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 가상 시스템 아키텍처
- 가상 시스템 암호화
- 가상 시스템 보기
- 새 독립형 가상 시스템 만들기
- 가상 시스템의 빠른 프로비저닝
- 가상 시스템 콘솔 열기
- 가상 시스템에서 전원 작업 수행
- 가상 시스템에 VMware Tools 설치
- 가상 시스템의 가상 하드웨어 버전 업그레이드
- 가상 시스템 속성 편집
- 미디어 삽입
- 미디어 꺼내기
- 다른 vApp에 가상 시스템 복사

- 다른 vApp으로 가상 시스템 이동
- 가상 시스템 선호도 및 반선호도
- 가상 시스템 모니터링
- 스냅샷 작업
- 가상 시스템 임대 갱신
- 가상 시스템 삭제
- 자동 스케일 그룹

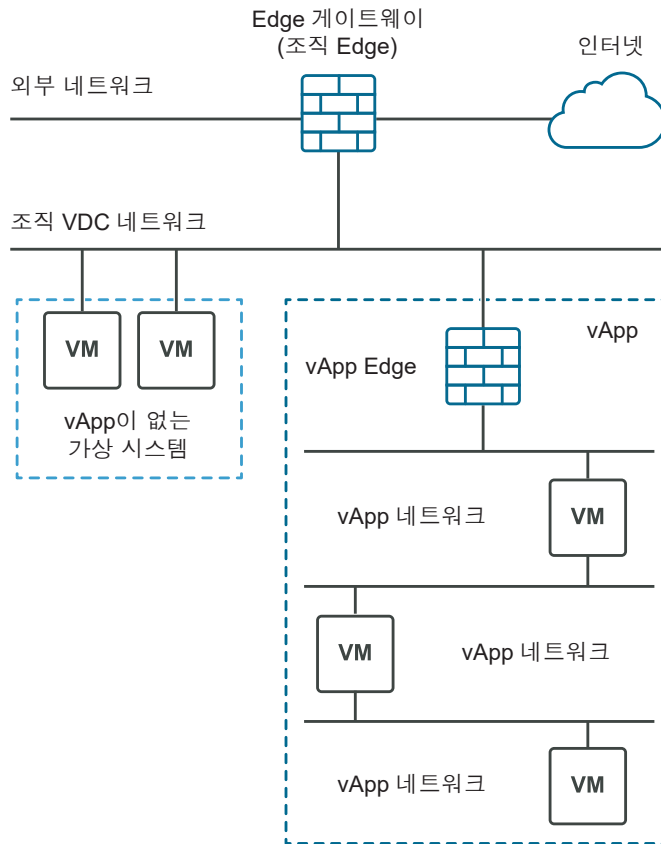
가상 시스템 아키텍처

가상 시스템은 독립형 시스템으로 존재하거나 vApp 내에 존재할 수 있습니다.

가상 시스템은 물리적 컴퓨터처럼 운영 체제와 애플리케이션을 실행하는 소프트웨어 컴퓨터입니다. 가상 시스템은 규격 및 구성 파일의 집합으로 구성되며 호스트의 물리적 리소스에 의해 지원됩니다. 모든 가상 시스템에는 물리적 하드웨어와 동일한 기능을 제공하지만 이동성이 좋고 더욱 안전하며 관리하기 쉬운 가상 디바이스가 있습니다. 가상 시스템은 독립형이거나 vApp 내에 존재할 수 있습니다. vApp은 하나 이상의 가상 시스템과 하나 이상의 네트워크로 구성되는 복합 개체입니다.

다음 그림에서는 가상 시스템을 만들 때의 여러 옵션을 보여 줍니다. 독립형 가상 시스템 또는 vApp 내에 가상 시스템을 생성할 수 있습니다. 독립형 가상 시스템은 조직 가상 데이터 센터에 직접 연결됩니다. 또는 vApp 내에 가상 시스템을 만들 수도 있습니다. vApp 안에 가상 시스템을 만들면 여러 가상 시스템과 가상 시스템에 연결된 네트워크를 그룹화할 수 있습니다. vApp을 사용하면 복잡한 애플리케이션을 작성하고 카탈로그에 저장하여 나중에 사용할 수 있습니다.

그림 2-1. 독립형 가상 시스템 또는 vApp 내의 가상 시스템



가상 시스템 암호화

VMware Cloud Director 10.1부터는 VM 암호화를 사용하여 데이터의 보안을 향상시킬 수 있습니다. VM 과 디스크를 VM 암호화 기능이 있는 스토리지 정책에 연결하여 암호화할 수 있습니다.

암호화는 가상 시스템뿐만 아니라 가상 시스템 디스크와 기타 파일도 보호합니다. API 및 UI에서 스토리지 정책에 대한 기능 및 VM과 디스크의 암호화 상태를 볼 수 있습니다. 해당하는 vCenter Server 버전에서 지원되는 암호화된 VM 및 디스크에 대해 모든 작업을 수행할 수 있습니다.

조직 VDC에 VM 암호화가 사용되도록 설정된 스토리지 정책이 있는 경우 VM 및 디스크를 암호화할 수 있습니다. "VMware Cloud Director 서비스 제공자 관리자 포털 가이드" 에서 [조직 가상 데이터 센터의 스토리지 정책에서 VM 암호화 사용](#)을 참조하십시오. VM 또는 디스크를 암호화하려면 VM 또는 디스크를 VM 암호화 사용 스토리지 정책과 연결합니다. 가상 시스템의 경우 [새 독립형 가상 시스템 만들기](#) 또는 [가상 시스템의 일반 속성 변경](#)의 내용을 참조하십시오. 명명된 디스크의 경우 [명명된 디스크 만들기](#) 또는 [명명된 디스크 편집](#)의 내용을 참조하십시오. VM 또는 디스크를 암호 해독하려면, 해당 VM 또는 디스크를 암호화를 사용하도록 설정되지 않은 스토리지 정책과 연결합니다.

VM 암호화 제한 사항

VMware Cloud Director에서는 다음과 같은 작업이 지원되지 않습니다.

- 전원이 켜진 VM 또는 해당 디스크를 암호화하거나 암호 해독.

- 암호화된 VM의 OVF를 내보내기.
- 디스크가 스냅샷의 일부인 경우 스냅샷이 있는 VM의 디스크를 암호화하고 암호 해독.
- VM의 디스크가 암호화된 정책에 있는 경우 VM을 암호 해독.
- 암호화되지 않은 VM에 암호화된 디스크를 추가.
- 암호화되지 않은 VM에서 기존 디스크를 암호화.
- 암호화된 명명된 디스크를 암호화되지 않은 VM에 추가.
- 암호화된 연결된 클론을 생성.
- 연결된 클론 VM 또는 해당 디스크를 암호화.
- 소스 VM이 암호화된 경우 vCenter Server 인스턴스 전체에서 VM을 인스턴스화, 이동 또는 복제.

참고 빠르게 프로비저닝된 조직 VDC에서 소스 또는 대상 VM이 암호화되어 있고 클론을 생성하려는 경우 VMware Cloud Director는 항상 전체 클론을 생성합니다.

VM 암호화 스토리지 기능 식별


기본적으로 **시스템 관리자** 및 **조직 관리자**는 조직 VDC 스토리지 기능과 VM 및 디스크가 암호화되었는지 여부를 확인하는 데 필요한 권한이 있습니다. **vApp 작성자**는 가상 시스템의 **세부 정보** 페이지에서 가상 시스템 및 해당 디스크의 암호화 상태를 볼 수 있습니다. 역할과 권한에 대한 자세한 내용은 **미리 정의된 역할 및 역할 권한** 항목을 참조하십시오.


가상 시스템 보기

독립형이거나 vApp의 일부인 가상 시스템을 볼 수 있습니다. 그리드 보기 또는 카드 보기로 가상 시스템을 볼 수 있습니다.

절차


- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2 다음 중 하나를 선택합니다.

- 가상 시스템을 그리드 보기에서 보려면  을 클릭합니다.

- 가상 시스템을 카드 보기에서 보려면  을 클릭합니다.

가상 시스템 목록이 그리드 보기에 표시되거나 카드 목록으로 표시됩니다.

- 3 (선택 사항) **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.

- 4 (선택 사항) 그리드 보기에서 가상 시스템 왼쪽에 있는  를 클릭하여 선택한 가상 시스템에 대해 수행할 수 있는 작업을 표시합니다.


예를 들어 가상 시스템을 종료할 수 있습니다.

- 5 가상 시스템의 게스트 운영 체제에 대한 인터페이스에 액세스하려면 카드 보기의 오른쪽 위에서 데스크톱 아이콘을 클릭합니다.
- 6 가상 시스템에 대한 세부 정보를 보고 편집하려면 **세부 정보**를 클릭합니다.

새 독립형 가상 시스템 만들기

독립형 가상 시스템을 새로 만들 수 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 **새 VM**을 클릭합니다.
- 4 가상 시스템에 대한 이름과 컴퓨터 이름을 입력합니다.

중요 컴퓨터 이름에는 영숫자와 하이픈만 포함될 수 있습니다. 컴퓨터 이름은 숫자로만 구성할 수 없으며 공백을 포함할 수 없습니다.

- 5 (선택 사항) 의미 있는 설명을 입력합니다.
- 6 가상 시스템이 생성되면 바로 가상 시스템의 전원을 켜지 선택합니다.

7 가상 시스템의 배포 방법을 선택합니다.

옵션	작업
새로 만들기	<p>사용자 지정 설정으로 새 가상 시스템을 배포합니다.</p> <ul style="list-style-type: none"> a 운영 체제 제품군과 운영 체제를 선택합니다. b (선택 사항) 부팅 이미지를 선택합니다. c (선택 사항) VM 배치 정책 및 VM 크기 조정 정책을 선택합니다. <p>VM 배치 및 VM 크기 조정 정책 드롭다운 메뉴는 서비스 제공자가 해당 정책을 조직 VDC에 게시한 경우에만 표시됩니다.</p> <ul style="list-style-type: none"> d (선택 사항) 미리 정의된 크기 조정 옵션에서 가상 시스템의 크기를 선택하거나 사용자 지정 크기 조정 옵션을 클릭하고 가상 CPU 수, 소켓당 코어 수 및 메모리 설정을 수동으로 입력합니다. <p>VM 크기를 정의하는 VM 크기 조정 정책을 선택하면 이 옵션이 표시되지 않습니다.</p> <p>미리 정의된 가상 시스템의 크기는 소, 중, 대입니다.</p> <ul style="list-style-type: none"> e 스토리지 정책 및 크기(GB)와 같은 가상 시스템의 스토리지 설정을 지정합니다. f 가상 시스템에 대한 네트워크 설정(예: 네트워크, IP 모드, IP 주소, 기본 NIC)을 지정합니다.
템플릿에서	<p>템플릿 카탈로그에서 선택한 템플릿에서 가상 시스템을 배포합니다.</p> <ul style="list-style-type: none"> a 사용 가능한 템플릿 목록에서 가상 시스템 템플릿을 선택합니다. b (선택 사항) VM 배치 정책 및 VM 크기 조정 정책을 선택합니다. <p>VM 배치 및 VM 크기 조정 정책 드롭다운 메뉴는 서비스 제공자가 해당 정책을 조직 VDC에 게시한 경우에만 표시됩니다. 선택한 템플릿에 정책이 할당된 경우에는 미리 정의된 템플릿 정책으로 제한될 수 있습니다.</p> <ul style="list-style-type: none"> c (선택 사항) 사용자 지정 스토리지 정책을 사용하도록 선택하고 사용할 사용자 지정 스토리지 정책 드롭다운 메뉴에서 사용할 스토리지 정책을 선택합니다. d 최종 사용자 라이선스 계약(있는 경우)을 읽고 수락합니다.

8 확인을 클릭하여 가상 시스템의 설정을 저장하고 생성 프로세스를 시작합니다.

카탈로그에서 가상 시스템의 카드를 볼 수 있습니다. 가상 시스템이 생성될 때까지 해당 상태는 [사용 중]으로 표시됩니다.

가상 시스템의 빠른 프로비저닝

빠른 프로비저닝을 사용하면 가상 시스템 프로비저닝 작업에 연결된 클론을 사용하여 시간을 절약할 수 있습니다.

연결된 클론은 원본과 동일한 가상 디스크를 사용하고 원본과 클론의 차이를 추적하기 위한 델타 디스크 체인이 포함된 가상 시스템의 복제본입니다. 빠른 프로비저닝을 비활성화하면 모든 프로비저닝 작업에서 전체 클론이 발생합니다.

연결된 클론은 원래 가상 시스템과 다른 vCenter Server 데이터 센터 또는 데이터스토어에 있을 수 없습니다.

VM을 신속하게 프로비저닝하면 VMware Cloud Director는 특정 vApp 템플릿과 연결된 가상 시스템의 vCenter Server 데이터 센터 및 데이터스토어에서 연결된 클론을 만들 수 있도록 새도 가상 시스템을 만듭니다.

새도 가상 시스템은 원래 가상 시스템의 복사본입니다. 새도 가상 시스템은 연결된 클론이 만들어진 데이터 센터 및 데이터스토어에 만들어집니다.

중요 네이티브 스냅샷을 사용하는 스토리지 컨테이너에서는 빠르게 프로비저닝된 VM의 인플레이스 통합이 지원되지 않습니다. VVOL 및 VAAI 지원 데이터스토어는 네이티브 스냅샷을 사용하므로 이러한 스토리지 컨테이너 중 하나에 배포된 빠르게 프로비저닝된 VM을 통합할 수 없습니다. VVOL 또는 VAAI 지원 데이터스토어에 배포된 빠르게 프로비저닝된 VM을 통합해야 하는 경우 다른 스토리지 컨테이너로 재 배치해야 합니다.

가상 시스템 콘솔 열기

가상 시스템 콘솔에 액세스하면 가상 시스템에 대한 정보를 보고, 게스트 운영 체제에 대한 작업을 수행하고, 게스트 운영 체제에 영향을 주는 작업을 수행할 수 있습니다.

사전 요구 사항

가상 시스템의 전원이 켜져 있어야 합니다.

클라이언트에 VMware Remote Console 설치

VMware Remote Console은 VMware Cloud Director를 통해 프로비저닝되고 관리되는 모든 가상 시스템에서 사용자와 게스트 간의 상호 작용을 위한 기능을 기본적으로 제공합니다. 이 섹션에서는 Windows, Apple OS X 및 Linux에 VMware Remote Console을 설치하는 데 필요한 작업을 자세히 설명합니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **vApp 사용자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

1 설치 관리자를 다운로드합니다.

- VMware Remote Console 다운로드 페이지로 이동하고 플랫폼에 대한 링크를 선택합니다.
www.vmware.com/go/download-vmrc
- VMware Cloud Director Tenant Portal의 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭합니다. 가상 시스템을 선택하고 **작업** 메뉴에서 **VMRC 다운로드**를 선택합니다.

2 플랫폼 설치를 실행합니다.

- Windows를 사용하는 경우 .msi 설치 관리자를 두 번 클릭하고 표시되는 메시지를 따릅니다.

- Linux를 사용하는 경우 **루트** 권한으로 로그인하여 .bundle 설치 관리자를 실행하고 표시되는 메시지를 따릅니다.
- Mac OS를 사용하는 경우 .dmg를 두 번 클릭하여 연 다음 VMware Remote Console 아이콘을 두 번 클릭하여 Applications 폴더에 복사합니다.

결과

설치 후 `vmrc://` 체계로 시작하는 URI(Uniform Resource Identifier)를 클릭하면 VMware Remote Console이 열립니다. VMware Workstation, Player 및 Fusion에서도 `vmrc://` URI 체계가 처리됩니다.


가상 시스템 원격 콘솔 열기

VMware Cloud Director 테넌트 포털을 통해 VMware Remote Console을 사용하여 가상 시스템 콘솔을 열 수 있습니다.

사전 요구 사항

- 로컬 시스템에 VMware Remote Console이 설치되어 있는지 확인합니다.
- 선택한 가상 시스템의 전원이 켜져 있는지 확인합니다.
- 이 작업을 수행하려면 미리 정의된 **vApp 사용자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 가상 시스템의 **작업** 메뉴에서 **VM 원격 콘솔 시작**을 선택합니다.

참고 VMware Remote Console이 설치되지 않은 경우 VMware Remote Console을 설치하거나 웹 콘솔을 사용하라는 메시지가 팝업 창에 표시됩니다.

결과

가상 시스템 콘솔은 외부 가상 원격 콘솔로 열립니다.

참고 VMware Remote Console을 사용하여 VMware Cloud Director 가상 시스템에 연결할 때에는 콘솔 상호 작용만 할 수 있습니다(Ctrl+Alt+Del 보내기). 디바이스 작업, 전원 작업 또는 설정 관리는 수행할 수 없습니다.


웹 콘솔 열기

VMware Remote Console이 로컬 시스템에 설치되지 않은 경우에도 가상 시스템의 콘솔에 연결할 수 있습니다.

사전 요구 사항

- 가상 시스템의 전원이 켜졌는지 확인합니다.
- 이 작업을 수행하려면 미리 정의된 **vApp 사용자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 가상 시스템의 **작업** 메뉴에서 **웹 콘솔 시작**을 선택합니다.

결과

가상 시스템 콘솔이 VMware HTML Console SDK를 사용하여 브라우저 탭에 열립니다.

다음에 수행할 작업

콘솔에서 마우스, 키보드 및 기타 입력 디바이스를 사용하여 콘솔 창 내부의 아무 곳이나 클릭합니다.

참고 지원되는 다국어 키보드에 대한 자세한 내용은 VMware HTML Console SDK 설명서(<https://www.vmware.com/support/developer/html-console/>)를 참조하십시오.

가상 시스템에서 전원 작업 수행

가상 시스템에서 가상 시스템 전원 켜기 또는 끄기, 가상 시스템 일시 중단 또는 재설정, 가상 시스템의 게스트 운영 체제 종료와 같은 전원 작업을 수행할 수 있습니다.

가상 시스템의 전원 켜기

가상 시스템의 전원을 켜는 것은 물리적 시스템의 전원을 켜는 것과 같습니다.


게스트 사용자 지정을 사용하도록 설정된 가상 시스템의 경우 가상 시스템에 최신 버전의 VMware Tools가 설치되어 있지 않으면 전원을 켤 수 없습니다.

사전 요구 사항

가상 시스템의 전원이 꺼져 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.

- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 시작하려는 가상 시스템의 **작업** 메뉴에서 **전원 켜기**를 선택합니다.

결과

전원이 켜진 가상 시스템은 녹색으로 전원 켜짐 상태가 표시됩니다.


가상 시스템의 전원 끄기

가상 시스템의 전원을 끄는 것은 물리적 시스템의 전원을 끄는 것과 같습니다.

사전 요구 사항

가상 시스템의 전원이 켜져 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 전원을 끄려는 가상 시스템의 **작업** 메뉴에서 **전원 끄기**를 선택합니다.

결과

전원이 꺼진 가상 시스템은 빨간색으로 전원 꺼짐 상태가 표시됩니다.


게스트 운영 체제 종료

가상 시스템의 게스트 운영 체제를 종료하는 것은 물리적 시스템의 전원을 끄는 것과 같습니다.

사전 요구 사항

가상 시스템과 게스트 운영 체제의 전원이 켜져 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 가상 시스템의 **작업** 메뉴에서 **게스트 OS 종료**를 선택합니다.

결과

게스트 운영 체제가 종료됩니다.


가상 시스템 재설정

가상 시스템을 재설정하면 상태(메모리, 캐시 등)가 지워지지만 가상 시스템은 계속 실행됩니다. 가상 시스템 재설정은 물리적 시스템의 재설정 버튼을 누르는 것과 같습니다. 가상 시스템의 전원 상태가 변경되지 않고 운영 체제의 하드 리셋이 시작됩니다.

사전 요구 사항

가상 시스템의 전원이 켜져 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 재설정하려는 가상 시스템의 **작업** 메뉴에서 **재설정**을 선택합니다.

결과

가상 시스템의 상태가 지워집니다.

가상 시스템 일시 중단


가상 시스템을 일시 중단하면 메모리가 디스크에 기록되어 현재 상태가 보존됩니다.

일시 중단 및 재개 기능을 사용하면 가상 시스템의 현재 상태를 저장한 후 나중에 동일한 상태에서 작업을 계속할 수 있습니다.

사전 요구 사항

가상 시스템의 전원이 켜져 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 일시 중단하려는 가상 시스템의 **작업** 메뉴에서 **일시 중단**을 선택합니다.

결과

가상 시스템이 일시 중단되고 상태가 보존됩니다.


가상 시스템의 일시 중단된 상태 삭제

가상 시스템이 일시 중단된 상태이고 시스템의 사용을 더 이상 재개할 필요가 없는 경우 일시 중단된 상태를 삭제할 수 있습니다. 일시 중단된 상태를 삭제하면 저장된 메모리가 제거되고 시스템이 전원이 꺼진 상태로 돌아갑니다.

사전 요구 사항

가상 시스템이 일시 중단된 상태여야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 가상 시스템의 **작업** 메뉴에서 **일시 중단된 상태 삭제**를 선택합니다.

결과

상태가 삭제되고 가상 시스템의 전원이 꺼집니다.

여러 VM 전원 켜기

동시에 여러 VM의 전원을 켤 수 있습니다.

게스트 사용자 지정을 사용하도록 설정된 가상 시스템의 경우 가상 시스템에 최신 버전의 VMware Tools가 설치되어 있지 않으면 전원을 켤 수 없습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2 **다중 선택** 옵션을 설정합니다.
- 3 전원을 켤 VM을 선택합니다.
- 4 **작업** 메뉴에서 **전원 켜기**를 선택합니다.
- 5 **확인**을 클릭하여 확인합니다.

여러 가상 시스템 전원 끄기

동시에 여러 VM의 전원을 끌 수 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.

- 2 **다중 선택** 옵션을 설정합니다.
- 3 전원을 끌 VM을 선택합니다.
- 4 **작업** 메뉴에서 **전원 끄기**를 선택합니다.
- 5 **확인**을 클릭하여 확인합니다.

여러 가상 시스템의 일시 중단된 상태 삭제

여러 VM이 일시 중단된 상태이고 더 이상 사용을 재개할 필요가 없는 경우 VM의 일시 중단된 상태를 동시에 삭제할 수 있습니다. 일시 중단된 상태를 삭제하면 저장된 메모리가 제거되고 VM이 전원이 꺼진 상태로 돌아갑니다.

사전 요구 사항

VM이 일시 중단된 상태인지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2 **다중 선택** 옵션을 설정합니다.
- 3 일시 중단된 상태를 삭제할 VM을 선택합니다.
- 4 **작업** 메뉴에서 **일시 중단된 상태 삭제**를 선택합니다.
- 5 **확인**을 클릭하여 확인합니다.

여러 가상 시스템 재설정

동시에 여러 VM을 재설정하면 상태(메모리, 캐시 등)가 지워지지만 VM은 계속 실행됩니다.

가상 시스템 재설정은 물리적 시스템의 재설정 버튼을 누르는 것과 같습니다. 가상 시스템의 전원 상태가 변경되지 않고 운영 체제의 하드 리셋이 시작됩니다.

사전 요구 사항

VM의 전원이 켜져 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2 **다중 선택** 옵션을 설정합니다.
- 3 재설정할 VM을 선택합니다.
- 4 **작업** 메뉴에서 **재설정**을 선택합니다.
- 5 **확인**을 클릭하여 확인합니다.

가상 시스템에 VMware Tools 설치


VMware Cloud Director는 VMware Tools를 사용하여 게스트 운영 체제를 사용자 지정합니다.

VMware Tools는 일반 운영 체제 드라이버를 가상 하드웨어용으로 조정된 VMware 드라이버로 교체하여 가상 시스템의 관리 및 성능을 향상시킵니다. VMware Tools는 게스트 운영 체제에 설치합니다. VMware Tools 없이도 게스트 운영 체제를 실행할 수 있기는 하지만 중요한 기능과 편리함을 놓치게 됩니다.

사전 요구 사항

- 가상 시스템의 전원이 켜졌는지 확인합니다.
- 새로 만든 가상 시스템에 게스트 운영 체제가 없는 경우 VMware Tools를 설치하려면 먼저 게스트 운영 체제를 설치해야 합니다.
- VMware Tools를 설치하기 전에 게스트 사용자 지정을 비활성화해야 합니다.
- vApp의 가상 시스템에 있는 VMware Tools 버전이 7299 이전 버전인 경우 VMware Tools를 업그레이드해야 합니다.

절차

- 1 가상 데이터 센터 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 VMware Tools를 설치할 가상 시스템의 **작업** 메뉴에서 **VMware Tools 설치**를 선택합니다.
VMware Tools가 대상 게스트 운영 체제에 설치됩니다. 설치 중에 오류가 있으면 오류 메시지가 표시됩니다. **작업** 창에서 설치 작업의 진행 상황을 볼 수도 있습니다.
- 4 가상 시스템의 웹 콘솔을 열려면 **작업** 메뉴에서 **웹 콘솔 시작**을 선택합니다.
- 5 [VMware 기술 자료 문서 1014294](#)의 지침에 따라 특정 운영 체제에 적합하게 VMware Tools를 구성합니다.

결과

VMware Tools가 게스트 운영 체제에 설치 및 구성됩니다.

가상 시스템의 가상 하드웨어 버전 업그레이드

가상 시스템의 가상 하드웨어 버전을 업그레이드할 수 있습니다. 최신 가상 하드웨어 버전이 더 많은 기능을 지원합니다.

vApp에 있는 가상 시스템의 하드웨어 버전을 다운그레이드할 수는 없습니다.

VMware Cloud Director에서 지원하는 하드웨어 버전은 지원 vSphere 리소스에 따라 결정됩니다. 지원되는 하드웨어 버전은 지원 제공자 VDC에서 지원되는 최신 가상 하드웨어 버전에 따라 다릅니다. **조직 관리자** 또는 **시스템 관리자**는 기본 하드웨어에서 지원하는 최신 버전보다 이전의 버전으로 하드웨어 버전을 설정할 수 있습니다. VMware Cloud Director 테넌트 포털은 조직 또는 제공자 VDC에 지원되는 하드웨어를 기반으로 선택할 수 있는 가상 하드웨어 버전 목록을 동적으로 설정합니다.


가상 시스템 호환성 설정에 사용할 수 있는 하드웨어 기능에 대한 정보는 "vSphere 가상 시스템 관리"를 참조하십시오.

VMware 제품 및 해당 가상 하드웨어 버전에 대한 자세한 내용은 <https://kb.vmware.com/s/article/1003746>의 내용을 참조하십시오.

사전 요구 사항

- 가상 시스템을 중지하거나 가상 시스템이 포함된 vApp을 중지합니다.
- 가상 시스템에 최신 버전의 VMware Tools가 설치되어 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 업그레이드하려는 가상 시스템의 **작업** 메뉴에서 **가상 하드웨어 버전 업그레이드**를 선택합니다.
- 4 **확인**을 클릭합니다.

결과

가상 시스템이 최신 버전으로 업그레이드됩니다.

가상 시스템 속성 편집

가상 시스템 이름 및 설명, 하드웨어 및 네트워크 설정, 게스트 OS 설정 등을 비롯한 가상 시스템의 속성을 편집할 수 있습니다.

가상 시스템의 일반 속성 변경


가상 시스템의 이름, 설명 및 기타 일반 속성을 검토하고 변경할 수 있습니다.

사전 요구 사항

운영 체제와 같은 속성을 변경하려면 시스템의 전원이 꺼져 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.

- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 편집할 가상 시스템의 카드에서 **세부 정보**를 클릭합니다.
- 4 **일반** 아래에서 편집하거나 볼 수 있는 속성의 목록은 기본적으로 확장됩니다.


옵션	작업
가상 시스템 이름	가상 시스템 이름을 편집합니다. 이 속성은 가상 시스템의 전원이 켜져 있는 동안 편집할 수 있습니다.
컴퓨터 이름	네트워크에서 가상 시스템을 식별할 수 있도록 게스트 운영 체제에 설정된 컴퓨터 및 호스트 이름을 편집합니다. 이 필드는 컴퓨터 이름에 대한 Windows 운영 체제 제한 때문에 15자로 제한됩니다. 이 속성은 가상 시스템의 전원이 켜져 있는 동안 편집할 수 있습니다.
설명	가상 시스템에 대한 설명(선택 사항)을 입력합니다. 이 속성은 가상 시스템의 전원이 켜져 있는 동안 편집할 수 있습니다.
운영 체제 제품군	드롭다운 메뉴에서 운영 체제 제품군을 선택합니다. 이 속성은 가상 시스템의 전원이 켜져 있는 동안 편집할 수 있습니다. 또한 운영 체제가 가상 시스템에 이미 있으면 이 속성을 편집할 수 없습니다.
운영 체제	드롭다운 메뉴에서 운영 체제를 선택합니다. 이 속성은 가상 시스템의 전원이 켜져 있는 동안 편집할 수 있습니다. 또한 운영 체제가 가상 시스템에 이미 있으면 이 속성을 편집할 수 없습니다.
부팅 지연	부팅 작업을 지연할 시간을 밀리초로 지정합니다. 가상 시스템의 전원을 켤 때부터 BIOS를 종료한 후 게스트 운영 체제 소프트웨어를 시작할 때까지 걸리는 시간을 줄일 수 있습니다. 부팅 지연을 더 길게 변경할 수 있습니다.
스토리지 정책	드롭다운 메뉴에서 가상 시스템이 사용할 스토리지 정책을 선택합니다. 이 속성은 가상 시스템의 전원이 켜져 있는 동안 편집할 수 있습니다.
가상 데이터 센터	이 가상 시스템이 속하는 가상 데이터 센터의 이름을 봅니다.
VMware Tools	VMware Tools가 가상 시스템에 설치되어 있는지 확인합니다.
가상 하드웨어 버전	가상 시스템의 가상 하드웨어 버전을 표시합니다.
업그레이드 대상:	업그레이드하려면 드롭다운 메뉴에서 버전을 선택합니다.
시간 동기화	가상 시스템 게스트 운영 체제와 가상 시스템 게스트 운영 체제가 실행되는 가상 데이터 센터 간의 시간 동기화를 사용하도록 설정하려면 이 확인란을 선택합니다.
BIOS 설정 입력	다음번 가상 시스템 부팅 시 BIOS나 설정 화면으로 강제로 전환할지 여부를 선택합니다. 이 속성은 가상 시스템의 전원이 켜져 있는 동안 편집할 수 있습니다.

- 5 변경을 완료했으면 **저장**을 클릭합니다.

가상 시스템의 하드웨어 속성 변경

가상 시스템의 하드웨어 속성을 검토 및 변경할 수 있습니다.

절차

- 1 가상 데이터 센터 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 편집할 가상 시스템의 카드에서 **세부 정보**를 클릭합니다.
- 4 보고 편집할 수 있는 하드웨어 속성의 목록을 확장하려면 **하드웨어**를 클릭합니다.

옵션	설명
가상 CPU 수	CPU의 수를 편집합니다. 가상 시스템에 할당할 수 있는 가상 CPU의 최대 개수는 호스트의 논리적 CPU 수 및 가상 시스템에 설치된 게스트 운영 체제 유형에 따라 달라집니다.
소켓당 코어	소켓당 코어 수를 편집합니다. 코어 수 및 소켓당 코어 수와 관련하여 가상 CPU의 할당 방법을 구성할 수 있습니다. 가상 시스템에서 필요한 CPU 코어 수를 결정한 다음 단일 코어 CPU, 듀얼 코어 CPU, 트라이 코어 CPU 등 어떤 CPU가 필요한지에 따라 각 소켓에서 원하는 코어 수를 선택합니다.
게스트 OS에 하드웨어 지원 CPU 가상화 노출	하드웨어 가상화가 필요한 애플리케이션이 가상 시스템에서 바이너리 변환 또는 반 가상화 없이 실행될 수 있도록 전체 CPU 가상화를 게스트 운영 체제에 노출할 수 있습니다.
총 메모리	가상 시스템에 대한 메모리 리소스 설정을 편집합니다. 가상 시스템의 메모리 크기는 4MB 배수이어야 합니다. 이 설정은 가상 시스템에 할당되는 ESXi 호스트 메모리의 양을 결정합니다. 가상 하드웨어 메모리 크기는 가상 시스템에서 실행되는 애플리케이션에 사용할 수 있는 메모리 양을 결정합니다. 가상 시스템은 구성된 가상 하드웨어 메모리 크기 이상의 메모리 리소스를 활용할 수 없습니다.
메모리 hot-add	메모리 hot-add를 사용하도록 설정하는 경우 가상 시스템의 전원이 켜져 있는 동안 가상 시스템에 메모리 리소스를 추가할 수 있습니다. 이 기능은 일부 게스트 운영 체제 및 가상 시스템 하드웨어 버전 7이상에서만 지원됩니다.
가상 CPU hot-add	가상 CPU hot-add를 사용하도록 설정하는 경우 가상 시스템의 전원이 켜져 있는 동안 가상 시스템에 가상 CPU를 추가할 수 있습니다. 소켓당 코어 수의 배수 단위로만 추가할 수 있습니다. 이 기능은 일부 게스트 운영 체제 및 가상 시스템 하드웨어 버전에서만 지원됩니다.
소켓 수	소켓 수를 표시합니다. 소켓 수는 사용 가능한 가상 CPU 수에 따라 결정됩니다. 가상 CPU 수를 업데이트하면 이 수가 변경됩니다.
이동식 미디어	연결된 CD/DVD, 플로피 드라이브와 같은 사용 가능한 이동식 미디어를 봅니다.

5 하드 디스크 아래에서 **추가**를 클릭하여 하드 디스크를 추가합니다.

옵션	설명
크기	하드 디스크 크기를 MB 단위로 입력합니다. 나중에 하드 디스크의 크기를 늘릴 수 있습니다. 참고 가상 시스템이 연결된 클론이 아니고 스냅샷이 없으면 기존 하드 디스크의 크기를 늘릴 수 있습니다.
정책	기본적으로 가상 시스템에 대한 스토리지 정책이 사용됩니다. 기본적으로, 가상 시스템에 연결된 모든 하드 디스크는 해당 가상 시스템에 지정된 스토리지 정책을 사용합니다. 가상 시스템을 만들거나 해당 속성을 수정할 때 이러한 디스크에 대한 이 기본값을 재정의할 수 있습니다. 각 하드 디스크의 [크기] 열에는 이 가상 시스템에 사용할 수 있는 모든 스토리지 정책이 나열된 드롭다운 메뉴가 포함되어 있습니다.
IOPS	디스크에 대한 특정 IOPS를 선택합니다. 이 옵션을 사용하여 디스크별 초당 I/O 작업 수를 제한합니다.
버스 유형	버스 유형을 선택합니다. 옵션은 Paravirtual (SCSI) , LSI Logic 병렬(SCSI) , LSI Logic SAS (SCSI) , IDE 및 SATA 입니다. 스토리지 컨트롤러 유형 및 호환성에 대한 자세한 내용은 "vSphere 가상 시스템 관리 가이드" 항목을 참조하십시오.
버스 번호	버스 번호를 입력합니다.
장치 번호	하드 디스크 드라이브의 논리 장치 번호를 입력합니다.

6 NIC 아래에서 **추가**를 클릭하여 새 NIC를 추가합니다.

NIC는 최대 10개까지 추가할 수 있습니다. 가상 시스템 하드웨어 버전에 따라 지원되는 NIC 수에 대한 자세한 내용은 <http://kb.vmware.com/s/article/2051652>를 참조하십시오. VMware Cloud Director는 가상 시스템이 실행되고 있는 동안 가상 시스템 NIC 수정을 지원합니다. 지원되는 네트워크 어댑터 유형에 대한 자세한 내용은 <http://kb.vmware.com/kb/1001805>를 참조하십시오.

옵션	설명
기본 NIC	기본 NIC를 선택한 경우 표시되는 플래그입니다. 기본 NIC를 선택합니다. 기본 NIC 설정에 따라 가상 시스템의 단일 기본 게이트웨이가 결정됩니다. 가상 시스템에서는 모든 NIC를 사용하여 NIC와 동일한 네트워크에 직접 연결된 가상 및 물리적 시스템에 연결할 수 있지만, 게이트웨이 연결이 필요한 네트워크의 시스템에 연결하는 데는 기본 NIC만 사용할 수 있습니다.
NIC	NIC의 수입니다.
연결됨	NIC를 연결하려면 확인란을 선택합니다.
네트워크	드롭다운 메뉴에서 네트워크를 선택합니다.

옵션	설명
IP 모드	<p>IP 모드를 선택합니다.</p> <p>경고 NIC를 연결할 네트워크를 선택한 경우 IP 모드를 없음으로 설정하지 마십시오.</p> <ul style="list-style-type: none"> ■ 정적 - IP 풀 네트워크 IP 풀에서 정적 IP 주소를 가져옵니다. ■ 정적 - 수동 특정 IP 주소를 수동으로 지정할 수 있습니다. 이 옵션을 선택하는 경우 IP 주소 열에 IP 주소를 입력해야 합니다. ■ DHCP DHCP 서버에서 IP 주소를 가져옵니다.
MAC 주소	드롭다운 메뉴에서 MAC 주소를 유지할지 또는 재설정할지를 선택합니다.

7 저장을 클릭합니다.

가상 시스템의 게스트 운영 체제 사용자 지정 속성 변경


VMware Cloud Director에서의 게스트 운영 체제 사용자 지정은 모든 플랫폼에 대해 선택 사항입니다. Windows 도메인에 가입해야 하는 가상 시스템의 경우에는 필수입니다.

이 메뉴에서 요청되는 정보의 일부는 Windows 플랫폼에만 적용됩니다. [게스트 OS 사용자 지정] 패널에는 가상 시스템이 Windows 도메인에 가입하는 데 필요한 정보가 포함되어 있습니다. **조직 관리자**는 해당 조직의 Windows 게스트가 가입할 수 있는 도메인에 대한 기본값을 지정할 수 있습니다. 모든 Windows 가상 시스템이 도메인에 가입해야 하는 것은 아니지만 대부분의 엔터프라이즈 설치 환경에서 도메인 구성원이 아닌 가상 시스템은 사용 가능한 많은 네트워크 리소스에 액세스할 수 없습니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **vApp 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- 게스트 사용자 지정을 사용하려면 가상 시스템에서 VMware Tools를 실행 중이어야 합니다.
- Windows 게스트 운영 체제를 사용자 지정하려면 우선 **시스템 관리자**가 VMware Cloud Director 서버 그룹에 적절한 Microsoft Sysprep 파일을 설치해야 합니다. "VMware Cloud Director 설치, 구성 및 업그레이드 가이드"를 참조하십시오.
- Linux 게스트 운영 체제를 사용자 지정하려면 게스트에 Perl이 설치되어 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.

3 편집할 가상 시스템의 카드에서 **세부 정보**를 클릭합니다.

4 **게스트 OS 사용자 지정 및 속성**을 클릭하여 게스트 운영 체제 설정 목록을 확장합니다.

옵션	설명
게스트 사용자 지정 사용	게스트 사용자 지정을 사용하도록 설정하려면 이 옵션을 선택합니다.
SID 변경	Windows 보안 ID(SID)를 변경하려면 이 옵션을 선택합니다. 이 옵션은 Windows 게스트 운영 체제를 실행하는 가상 시스템에만 적용됩니다. SID는 일부 Windows 운영 체제에서 시스템과 사용자를 고유하게 식별하기 위해 사용됩니다. 이 옵션을 선택하지 않는 경우 새 가상 시스템은 그 기반이 되는 가상 시스템 또는 템플릿과 동일한 SID를 갖게 됩니다. 컴퓨터가 도메인의 일부이고 도메인 사용자 계정만 사용된 경우에 중복 SID는 문제가 되지 않습니다. 단, 시스템이 작업 그룹에 속하거나 로컬 사용자 계정이 사용되는 경우에는 중복 SID가 파일 액세스 제어에 손상을 일으킬 수 있습니다. 자세한 내용은 Microsoft Windows 운영 체제 설명서를 참조하십시오.
로컬 관리자 암호 허용	게스트 운영 체제에서 관리자 암호를 설정하도록 허용하려면 이 옵션을 선택합니다. a 로컬 관리자의 암호를 지정합니다. 암호 지정 텍스트 상자를 비워두면 암호가 자동으로 생성됩니다. b 자동 로그인을 허용할 횟수를 지정합니다. 0 값을 입력하면 관리자 로 자동 로그인이 비활성화됩니다.
처음 로그인 시 관리자의 암호 변경 필요	관리자가 처음 로그인할 때 게스트 운영 체제의 암호를 변경하도록 요구하려면 이 옵션을 선택합니다. 보안을 위해 이 옵션을 사용하는 것이 좋습니다.
암호 자동 생성	암호 자동 생성을 허용하려면 이 옵션을 선택합니다.
도메인에 가입할 이 VM 사용	가상 시스템을 Windows 도메인에 가입시키려면 이 옵션을 선택합니다. 조직의 도메인을 사용하거나 조직의 도메인을 재정의하고 도메인 속성을 입력할 수 있습니다. a 도메인 이름을 입력합니다. b 사용자 이름과 암호를 입력합니다. c 계정 조직 구성 단위를 입력합니다.
스크립트	사용자 지정 스크립트를 사용하여 가상 시스템의 게스트 운영 체제를 수정할 수 있습니다. 가상 시스템에 사용자 지정 스크립트를 추가하면 초기 사용자 지정 및 강제 사용자 재지정 시에만 스크립트가 호출됩니다. precustomization 명령줄 매개 변수를 설정하면 게스트 사용자 지정이 시작되기 전에 스크립트가 호출됩니다. postcustomization 명령줄 매개 변수를 설정하면 게스트 사용자 지정이 완료된 후에 스크립트가 호출됩니다. ■ 스크립트 텍스트 상자 아래에 있는 [업로드] 버튼을 클릭하여 로컬 시스템의 사용자 지정 스크립트로 이동합니다. ■ 스크립트 파일 텍스트 상자에 사용자 지정 스크립트를 직접 입력합니다. 스크립트 파일 텍스트 상자에 직접 입력하는 사용자 지정 스크립트는 1500자를 초과할 수 없습니다. 자세한 내용은 VMware 기술 자료 문서 https://kb.vmware.com/kb/1026614 를 참조하십시오.

5 변경을 완료했으면 **저장**을 클릭합니다.

게스트 사용자 지정 이해

게스트 운영 체제를 사용자 지정하려면 몇 가지 설정 및 옵션에 대해 알고 있어야 합니다.

게스트 사용자 지정 사용 확인란

이 확인란은 가상 시스템 **속성** 페이지의 **게스트 OS 사용자 지정** 탭에 있습니다. 게스트 사용자 지정의 목적은 **속성** 페이지에서 선택한 옵션을 기반으로 구성하는 것입니다. 이 확인란이 선택되어 있으면 필요할 때 게스트 사용자 지정 및 사용자 재지정이 수행됩니다.

컴퓨터 이름, 네트워크 설정, 관리자 암호와 루트 암호 설정 및 만료, Windows 운영 체제의 SID 변경 등과 같은 모든 게스트 사용자 지정 기능이 작동하려면 이 프로세스가 필요합니다. **전원 켜기 및 강제 사용자 재지정**이 작동하려면 이 옵션이 선택되어 있어야 합니다.

이 확인란이 선택되어 있고 VMware Cloud Director의 가상 시스템 구성 매개 변수가 게스트 OS의 설정과 동기화되어 있지 않으면 가상 시스템 **속성** 페이지의 **프로파일** 탭에는 설정이 게스트 OS와 동기화되어 있지 않으며 가상 시스템에 게스트 사용자 지정이 필요하다는 메시지가 표시됩니다.

vApp 및 가상 시스템에 대한 게스트 사용자 지정 동작

다음 확인란은 선택 해제되어 있습니다.

- **게스트 사용자 지정 사용**
- **SID 변경**(Windows 게스트 OS의 경우)
- **암호 재설정**

사용자 지정을 수행하거나 네트워크 설정을 변경한 후 변경 내용을 게스트 OS에 반영하려는 경우에는 **게스트 사용자 지정 사용** 확인란을 선택하고 가상 시스템 **속성** 페이지의 **게스트 운영 체제 사용자 지정** 탭에서 옵션을 설정할 수 있습니다. vApp 템플릿에 있는 가상 시스템을 사용하여 vApp을 만든 다음 가상 시스템을 추가하면 vApp 템플릿이 빌드 블록 역할을 합니다. 카탈로그에 있는 가상 시스템을 새 vApp에 추가하면 가상 시스템에 대해 게스트 사용자 지정이 기본적으로 사용됩니다. 카탈로그에 있는 vApp 템플릿을 vApp으로 저장하면 **게스트 사용자 지정 사용** 확인란이 선택된 경우에만 가상 시스템에 대해 게스트 사용자 지정이 사용됩니다.

게스트 사용자 지정 설정에 대한 기본값은 다음과 같습니다.

- **게스트 사용자 지정 사용** 확인란은 카탈로그의 소스 가상 시스템과 동일합니다.
- Windows 게스트 가상 시스템의 경우 **SID 변경**은 카탈로그의 소스 가상 시스템과 동일합니다.
- 암호 재설정 설정은 카탈로그의 소스 가상 시스템과 동일합니다.

필요한 경우 vApp 시작 전에 **게스트 사용자 지정 사용** 확인란을 선택 취소할 수 있습니다.

게스트 OS 설치가 보류 중인 빈 가상 시스템을 vApp에 추가할 경우 해당 가상 시스템은 아직 사용자 지정할 준비가 되어 있지 않으므로 기본적으로 **게스트 사용자 지정 사용** 확인란이 선택 해제됩니다.

게스트 OS 및 VMware Tools를 설치한 후에 가상 시스템의 전원을 끄고 vApp를 중지한 다음 **게스트 사용자 지정 사용** 확인란을 선택하고 vApp 및 가상 시스템을 시작하여 게스트 사용자 지정을 수행할 수 있습니다.

사용자 지정된 가상 시스템에서 가상 시스템 이름 및 네트워크 설정이 업데이트된 경우 다음에 가상 시스템의 전원을 켜면 가상 시스템 사용자 재지정이 수행되어 게스트 가상 시스템과 VMware Cloud Director가 다시 동기화됩니다.

가상 시스템 전원 켜기 및 강제 사용자 재지정

가상 시스템의 전원을 켜고 가상 시스템의 사용자 재지정을 강제로 수행할 수 있습니다.


가상 시스템의 설정이 VMware Cloud Director와 동기화되어 있지 않거나 게스트 사용자 지정을 수행하려는 시도가 실패한 경우, 가상 시스템에 대한 사용자 재지정을 강제로 실행할 수 있습니다.

가상 시스템에서 실행되는 애플리케이션이 사용자 재지정을 지원하는지 확인합니다. Microsoft Sysprep을 사용하여 도메인 컨트롤러를 변경하고 SID도 변경하면 가상 시스템이 손상될 수 있습니다. 가상 시스템이 손상되는 위험을 줄이려면 사용자 재지정을 수행하기 전에 스냅샷을 생성합니다.

사전 요구 사항

- 조직 관리자여야 합니다.
- 가상 시스템의 전원이 꺼져 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 전원을 켜고 사용자 지정하려는 가상 시스템의 **전원** 메뉴에서 **전원 켜기 및 강제 사용자 재지정**을 선택합니다.

결과

가상 시스템이 사용자 재지정되고 전원이 켜집니다.

가상 시스템의 고급 속성 변경

고급 설정에서 리소스 할당 설정(할당량, 예약 및 제한)을 구성하여 가상 시스템에 제공되는 CPU, 메모리 및 스토리지 리소스의 양을 결정할 수 있습니다.

리소스 할당 설정(할당량, 예약 및 제한)을 사용하여 가상 시스템에 제공된 CPU, 메모리 및 스토리지 리소스의 양을 확인할 수 있습니다.

리소스 할당량

할당량은 가상 데이터 센터 내에서 가상 시스템의 상대적인 중요도를 지정합니다. 가상 시스템이 다른 가상 시스템에 비해 리소스 할당량이 두 배인 경우, 이들 가상 시스템이 리소스 확보를 위해 경쟁할 때 리소스 할당량이 두 배인 가상 시스템이 리소스를 두 배로 사용할 수 있습니다. 할당량은 일반적으로 [높음], [보통] 또는 [낮음]으로 지정되며, 이러한 값은 각각 4:2:1 비율의 할당량 값을 지정합니다. 사용자 지정을 선택하여 각 가상 시스템에 특정 할당량 값(비율 가중치로 표현)을 할당할 수도 있습니다. 가상 시스템에 할당량을 할당하면 해당 가상 시스템에 대해 전원이 켜진 다른 가상 시스템에 상대적인 우선 순위가 지정됩니다.

리소스 할당 예약

가상 시스템에 보장된 최소 할당량을 지정합니다. VMware Cloud Director를 사용하면 예약되지 않은 리소스가 가상 시스템의 예약을 처리할 수 있을 만큼 충분히 있는 경우에만 해당 가상 시스템의 전원을 켤 수 있습니다. 가상 데이터 센터는 리소스 부하가 심한 경우에도 이 양을 보장합니다. 예약은 구체적인 단위(메가헤르츠 또는 메가바이트)로 표현됩니다.

예를 들어 2GHz를 사용할 수 있고, 가상 시스템 1과 가상 시스템 2에 각각 1GHz의 리소스 할당 예약을 지정한다고 가정합니다. 이제 각 가상 시스템은 필요한 경우 1GHz를 보장받을 수 있습니다. 하지만 가상 시스템 1에서 500MHz만 사용 중이면 가상 시스템 2에서 1.5GHz를 사용할 수 있습니다.

예약은 기본적으로 0으로 설정됩니다. 가상 시스템에서 필요한 최소한의 CPU 또는 메모리 양을 항상 사용할 수 있도록 보장해야 하는 경우에 예약을 지정할 수 있습니다.

리소스 할당 제한

가상 시스템에 할당할 수 있는 CPU 및 메모리 리소스의 상한을 지정합니다. 가상 데이터 센터는 가상 시스템에 예약된 것보다 더 많은 리소스를 할당할 수 있지만 시스템에 사용하지 않는 리소스가 있더라도 제한을 초과하여 할당하지는 않습니다. 제한은 구체적인 단위(메가헤르츠 또는 메가바이트)로 표현됩니다.


CPU 및 메모리 리소스 제한은 기본적으로 무제한으로 설정됩니다. 메모리 제한이 무제한이면 대부분의 경우 가상 시스템이 만들어질 때 해당 가상 시스템에 대해 구성된 메모리 양이 제한으로 적용됩니다.

대부분의 경우에는 제한을 지정할 필요가 없습니다. 제한을 지정하면 유휴 리소스가 낭비될 수 있습니다. 시스템에서는 시스템 이용률이 낮고 유휴 리소스를 사용할 수 있는 경우에도 가상 시스템이 제한보다 많은 리소스를 사용하는 것을 허용하지 않습니다. 제한은 지정할만한 이유가 있을 때만 지정해야 합니다.

사전 요구 사항

- 예약 풀 가상 데이터 센터가 있어야 합니다.
- 가상 데이터 센터에서 가상 시스템을 위한 일정량의 메모리를 제공해야 합니다.
- 특정 가상 시스템에는 항상 다른 가상 시스템보다 높은 비율의 가상 데이터 센터 리소스가 할당되도록 합니다.
- 가상 시스템에 할당할 수 있는 리소스의 상한을 설정합니다.

절차

- 1 가상 데이터 센터 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 편집할 가상 시스템의 카드에서 **세부 정보**를 클릭합니다.
- 4 **고급** 및 **편집**을 클릭합니다.

5 우선 순위 드롭다운 메뉴에서 옵션을 선택하여 CPU 설정에 대한 리소스 할당률을 설정합니다.

옵션	설명
낮음	가상 CPU당 할당률 500을 할당합니다.
보통	가상 CPU당 할당률 1000을 할당합니다.
높음	가상 CPU당 할당률 2000을 할당합니다.
사용자 지정	가상 시스템마다 할당률 값(비율 가중치를 의미함)을 입력하여 특정 할당률 값을 할당할 수 있습니다. 가상 시스템에 할당률을 할당하면 해당 가상 시스템에 대해 전원이 켜진 다른 가상 시스템에 상대적인 우선 순위가 지정됩니다.

6 CPU 설정에 대한 예약을 MHz 단위로 입력하여 지정하고 필요한 경우 CPU 설정에 대한 제한을 MHz 단위로 지정합니다.

옵션	설명
무제한	기본 CPU 리소스 옵션입니다.
최대	가상 시스템에 할당할 수 있는 CPU 리소스의 상한을 MHz 단위로 지정합니다.

7 우선 순위 드롭다운 메뉴에서 옵션을 선택하여 메모리 설정에 대한 리소스 할당률을 설정합니다.

옵션	설명
낮음	구성된 가상 시스템 메모리의 1MB당 할당률 5를 할당합니다.
보통	구성된 가상 시스템 메모리의 1MB당 할당률 10을 할당합니다.
높음	구성된 가상 시스템 메모리의 1MB당 할당률 20을 할당합니다.
사용자 지정	할당률 값을 입력하여 특정 할당률 값을 할당할 수 있습니다.

8 메모리 설정에 대한 예약을 MB 단위로 지정하고 필요한 경우 메모리 설정에 대한 제한을 MB 단위로 지정합니다.

옵션	설명
무제한	기본 메모리 리소스 옵션입니다.
최대	가상 시스템에 할당할 수 있는 메모리 예약의 상한을 지정합니다.

9 저장을 클릭합니다.


미디어 삽입

카탈로그의 CD/DVD 이미지 같은 미디어를 삽입하여 가상 시스템 게스트 운영 체제에서 사용할 수 있습니다. 이러한 미디어 파일을 사용하여 가상 시스템, 다양한 애플리케이션, 드라이버 등에 운영 체제를 설치할 수 있습니다.

사전 요구 사항

미디어 파일이 있는 카탈로그에 액세스할 수 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 미디어를 추가할 가상 시스템을 선택합니다.
- 4 **작업** 메뉴에서 **미디어 삽입**을 선택합니다.
- 5 **CD 삽입** 창에서 가상 시스템에 삽입할 미디어 파일을 선택합니다.
- 6 **삽입**을 클릭합니다.


미디어 꺼내기

가상 시스템에서 CD 또는 DVD 사용을 마친 후에는 해당 미디어 파일을 꺼낼 수 있습니다.

사전 요구 사항

미디어 파일이 가상 시스템에 삽입되어 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 미디어를 꺼낼 가상 시스템을 선택합니다.
- 4 **작업** 메뉴에서 **미디어 꺼내기**를 선택합니다.

결과

미디어 파일이 꺼내집니다.

다른 vApp에 가상 시스템 복사


가상 시스템을 다른 vApp에 복사할 수 있습니다. 가상 시스템을 복사해도 원래 가상 시스템은 소스 vApp에 유지됩니다.

가상 시스템을 복사할 때 스냅샷은 사본에 포함되지 않습니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **vApp 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- VM의 전원을 끕니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 복사하려는 가상 시스템의 **작업** 메뉴에서 **복사**를 선택합니다.
- 4 가상 시스템을 복사할 대상 vApp을 선택하고 **다음**을 클릭합니다.
- 5 가상 시스템 이름, 컴퓨터 이름, 스토리지 정책(선택 사항) 및 NIC(선택 사항)와 같은 리소스를 구성하고 **다음**을 클릭합니다.

중요 컴퓨터 이름에는 영숫자와 하이픈만 포함될 수 있습니다. 컴퓨터 이름은 숫자로만 구성할 수 없으며 공백을 사용할 수 없습니다.

- 6 **완료 준비** 페이지에서 설정을 검토하고 **완료**를 클릭합니다.

다른 vApp으로 가상 시스템 이동

가상 시스템을 다른 vApp에 이동할 수 있습니다. VM을 이동하면 VMware Cloud Director가 소스 vApp에서 원래 VM을 제거합니다.

가상 시스템을 다른 vApp으로 이동하면 스냅샷이 손실됩니다.

서로 다른 vApp 간 VM 이동에는 VMware vSphere® vMotion® 및 EVC(향상된 vMotion 호환성)를 사용합니다. 동일한 조직 내에서 동일하거나 다른 조직 VDC에 속하는 다른 vApp으로 VM을 이동할 수 있습니다. 조직 VDC는 동일하거나 서로 다른 제공자 VDC 내에 있을 수 있습니다.

다른 vApp으로 가상 시스템을 이동하는 동안 네트워크 및 스토리지 프로파일 변경과 같은 재구성을 수행할 수 있습니다.


표 2-1. 가상 시스템 이동 중 재구성 및 가상 시스템 상태

재구성	대상 vApp이 동일한 조직 VDC에 있는 경우 VM 상태	대상 vApp이 동일한 제공자 VDC 내의 다른 조직 VDC에 있는 경우 VM 상태
네트워크 변경	전원 꺼짐	해당 없음
네트워크 제거	전원 꺼짐 또는 꺼짐	해당 없음
스토리지 프로파일 변경	전원 꺼짐 또는 꺼짐	전원 꺼짐

사전 요구 사항

- **vApp 작성자** 역할이 있는지 또는 이와 동등한 권한 집합이 있는지 확인합니다.
- 기본 vSphere 리소스가 vMotion 및 EVC를 지원하는지 확인합니다. vMotion 및 EVC의 요구 사항 및 제한 사항에 대한 자세한 내용은 "vCenter Server 및 호스트 관리" 를 참조하십시오.
- VM 네트워크 또는 스토리지 프로파일을 변경하려는 경우에는 VM 전원을 꺼야 하는지 확인합니다. "VM 이동 중 재구성 및 VM 상태" 테이블을 참조하십시오.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 이동하려는 시스템의 **작업** 메뉴에서 **이동**을 선택합니다.
- 4 대상 vApp을 선택하고 **다음**을 클릭합니다.
- 5 VM 이름, 컴퓨터 이름, 스토리지 정책(선택 사항) 및 NIC(선택 사항)와 같은 리소스를 구성하고 **다음**을 클릭합니다.

중요 컴퓨터 이름에는 영숫자와 하이픈만 포함될 수 있습니다. 컴퓨터 이름은 숫자로만 구성할 수 없으며 공백을 포함할 수 없습니다.

- 6 **완료 준비** 페이지에서 설정을 검토하고 **완료**를 클릭합니다.

가상 시스템 선호도 및 반선호도

선호도 및 반선호도 규칙을 사용하면 가상 시스템 그룹을 서로 다른 ESXi 호스트 간에 분산하거나 가상 시스템 그룹을 특정 ESXi 호스트에 유지할 수 있습니다.

선호도 규칙은 가상 시스템 그룹을 하나의 특정 호스트에 배치하기 때문에 해당 가상 시스템의 사용량을 손쉽게 감사할 수 있습니다. 반선호도 규칙은 가상 시스템 그룹을 여러 호스트에 배치하여 단일 호스트에 장애가 발생하는 경우 모든 가상 시스템에서 동시에 장애가 발생하는 것을 방지합니다.


선호도 또는 반선호도 규칙이 충족되지 않으면 규칙에 추가된 가상 시스템의 전원이 켜지지 않습니다.

선호도 및 반선호도 규칙 보기

기존의 선호도 및 반선호도 규칙을 볼 수 있고 규칙에 의해 영향을 받는 가상 시스템, 규칙 사용 여부 등과 같은 해당 속성을 볼 수 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **선호도 규칙**을 선택합니다.

2 (선택 사항) **그리드 편집기** 아이콘()을 클릭하고 규칙에 대해 표시할 세부 정보를 선택합니다.

결과

기존의 선호도 및 반선호도 규칙, 가상 시스템 및 각 규칙의 사용 상태 목록이 표시됩니다.

선호도 규칙 만들기

선호도 규칙을 만들어서 특정 가상 시스템 그룹을 단일 호스트에 배치하여 해당 가상 시스템의 사용량에 대한 감사를 시행할 수 있습니다.

절차

1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **선호도 규칙**을 선택합니다.

2 **선호도 규칙** 아래에서 **새로 만들기**를 클릭합니다.

3 규칙의 이름을 입력합니다.

4 규칙을 사용하도록 설정하지 않고 규칙을 생성하려면 **사용**을 선택 해제합니다.

기본적으로 규칙을 만든 후에는 확인란이 선택되어 있고 규칙을 사용하도록 설정되어 있습니다.

5 **필수** 확인란을 선택한 상태로 둡니다.

기본적으로 각 선호도 규칙은 필수입니다. 즉, 규칙이 충족되지 않으면 규칙에 추가된 가상 시스템의 전원이 켜지지 않습니다.

6 선호도 규칙에 추가할 가상 시스템을 선택합니다.

7 **저장**을 클릭합니다.

결과

VMware Cloud Director가 선호도 규칙에 연결된 가상 시스템을 단일 호스트에 배치합니다.

반선호도 규칙 만들기

반선호도 규칙을 만들어서 특정 가상 시스템 그룹을 여러 호스트에 배치하여 단일 호스트에서 장애가 발생할 때 모든 가상 시스템에서 동시 장애가 발생하지 않도록 방지합니다.

절차

1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **선호도 규칙**을 선택합니다.

2 **반선호도 규칙** 아래에서 **새로 만들기**를 클릭합니다.

3 규칙의 이름을 입력합니다.

4 규칙을 사용하도록 설정하지 않고 규칙을 생성하려면 **사용**을 선택 해제합니다.

기본적으로 규칙을 만든 후에는 확인란이 선택되어 있고 규칙을 사용하도록 설정되어 있습니다.

5 필수 확인란을 선택한 상태로 둡니다.

기본적으로 각 반선택도 규칙은 필수입니다. 즉, 규칙이 충족되지 않으면 규칙에 추가된 가상 시스템의 전원이 켜지지 않습니다.

6 반선택도 규칙에 추가할 가상 시스템을 선택합니다.

7 저장을 클릭합니다.

결과

VMware Cloud Director가 반선택도 규칙에 연결된 가상 시스템을 여러 호스트에 배치합니다.

선택도 또는 반선택도 규칙 편집

선택도 또는 반선택도 규칙을 편집하여 규칙을 활성화 또는 비활성화하거나, 가상 시스템을 추가 또는 제거하거나, 규칙 이름이나 규칙 기본 설정을 변경할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 Organization vDC: VM-VM Affinity Edit 권한이 필요합니다. 이 권한은 미리 정의된 **카탈로그 작성자**, **vApp 작성자** 및 **조직 관리자** 역할에 포함되어 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **선택도 규칙**을 선택합니다.
- 2 편집할 규칙의 이름 옆에 있는 라디오 버튼을 클릭하고 **편집**을 클릭합니다.
- 3 규칙 속성을 편집합니다.
 - a 필요에 따라 규칙의 이름을 변경합니다.
 - b 규칙을 활성화할지 또는 비활성화할지 선택합니다.
 - c **필수** 확인란을 선택한 상태로 둡니다.
 - d 가상 시스템을 더 추가하거나 제거합니다.
- 4 **저장**을 클릭합니다.

선택도 또는 반선택도 규칙 삭제

선택도 또는 반선택도 규칙을 더 이상 사용하지 않으려면 삭제할 수 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **선택도 규칙**을 선택합니다.
- 2 삭제할 규칙의 이름 옆에 있는 라디오 버튼을 클릭하고 **삭제**를 클릭합니다.
- 3 규칙을 삭제하는 것을 확인하려면 **확인**을 클릭합니다.

결과

VMware Cloud Director에서 선호도 또는 반선호도 규칙이 삭제됩니다.

가상 시스템 모니터링


VMware Cloud Director 관리자가 가상 시스템 모니터링 기능을 사용하도록 설정한 경우에는 테넌트 포털에서 모니터링 차트를 볼 수 있습니다.

이 기능을 사용하면 지정된 가상 시스템의 시간대별(일, 주 또는 월) 상태를 파악할 수 있습니다.

사전 요구 사항

이 기능은 VMware Cloud Director 관리자가 사용하도록 설정한 경우에만 사용할 수 있습니다.

절차

- 1 가상 데이터 센터 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 모니터링할 가상 시스템을 선택하고 **세부 정보**를 클릭합니다.
- 4 **모니터링 차트**를 클릭하여 모니터링 보기를 확장합니다.
모니터링 차트가 표시됩니다.
- 5
- 6 가상 시스템 모니터링을 위한 메트릭 옵션을 선택합니다.

메트릭 드롭다운 메뉴의 목록은 **시스템 관리자**의 선택에 따라 달라집니다. 다음 옵션의 전체 또는 일부가 표시될 수 있습니다.

메트릭	설명
최근에 프로비저닝된 디스크	KB 단위로 지정됩니다. 일, 주 또는 월 보기에서 선택합니다.
평균 디스크 읽기	백분율로 지정됩니다. 일, 주 또는 월 보기에서 선택합니다.
평균 디스크 쓰기	백분율로 지정됩니다. 일, 주 또는 월 보기에서 선택합니다.
평균 CPU 사용량	백분율로 지정됩니다. 일, 주 또는 월 보기에서 선택합니다.
평균 CPU 사용량(MHz)	MHz 단위로 지정됩니다. 일, 주 또는 월 보기에서 선택합니다.

메트릭	설명
최대 CPU 사용량	백분율로 지정됩니다. 일, 주 또는 월 보기에서 선택합니다.
평균 메모리 사용량	백분율로 지정됩니다. 일, 주 또는 월 보기에서 선택합니다.
최근에 사용된 디스크	KB 단위로 지정됩니다. 일, 주 또는 월 보기에서 선택합니다.

목록에서 다른 값을 선택할 때마다 새 차트가 표시됩니다.

7 (선택 사항) 메트릭 수집에 대한 기간을 변경합니다.

8 새로 고침을 클릭합니다.

9 변경 내용을 저장하려면 **저장**을 클릭합니다.

스냅샷 작업

스냅샷은 스냅샷을 만드는 시점의 가상 시스템 상태 및 데이터를 보관합니다. 가상 시스템의 스냅샷을 생성할 때 가상 시스템은 영향을 받지 않으며, 지정된 상태의 가상 시스템 이미지만 복사 및 저장됩니다. 동일한 가상 시스템 상태로 반복해서 되돌려야 하지만 가상 시스템을 여러 개 만들지는 않으려는 경우 스냅샷을 사용하면 편리합니다.

스냅샷은 알려지지 않았거나 유해한 영향이 있을 수 있는 소프트웨어를 테스트하기 위한 단기 솔루션으로 유용합니다. 예를 들어 업데이트 패키지 설치와 같은 선형 또는 반복 프로세스나 다른 버전의 프로그램 설치와 같은 분기 프로세스 중에 스냅샷을 복원 지점으로 사용할 수 있습니다.

가상 시스템의 운영 체제를 업그레이드하는 경우 스냅샷을 사용할 수 있습니다. 예를 들어 가상 시스템을 업그레이드하기 전에 스냅샷을 만들면 업그레이드 전의 시점을 보존할 수 있습니다. 업그레이드 중에 문제가 발생하지 않으면 스냅샷을 제거하도록 선택하고 업그레이드 중에 수행된 변경 내용을 커밋할 수 있습니다. 하지만 문제가 발생하면 스냅샷으로 되돌려서 업그레이드하기 전에 저장된 가상 시스템 상태로 돌아갈 수 있습니다.

VMware Cloud Director를 사용하면 가상 시스템의 스냅샷을 하나만 사용할 수 있습니다. 가상 시스템의 새 스냅샷을 만들려고 할 때마다 이전 스냅샷이 삭제됩니다.

가상 시스템의 스냅샷 만들기

가상 시스템의 스냅샷을 만들 수 있습니다. 스냅샷을 만든 후에는 가상 시스템을 스냅샷으로 되돌리거나 스냅샷을 제거할 수 있습니다.


사전 요구 사항

가상 시스템이 명명된 디스크에 연결되어 있지 않은지 확인합니다.

참고 스냅샷에는 NIC 구성이 캡처되지 않습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.

- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.

- 3 스냅샷을 만들려는 가상 시스템의 **작업** 메뉴에서 **스냅샷 만들기**를 선택합니다.

가상 시스템의 스냅샷을 만들면 기존 스냅샷이 있는 경우 대체됩니다.

- 4 (선택 사항) 가상 시스템의 메모리에 대한 스냅샷을 만들지 여부를 선택합니다.

가상 시스템의 메모리 상태를 캡처할 경우 스냅샷에는 가상 시스템의 라이브 상태가 보관됩니다. 메모리 스냅샷은 정확한 시간에 스냅샷을 만듭니다. 예를 들어 현재 작동 중인 소프트웨어를 업그레이드하기 전에 메모리 스냅샷을 만들 수 있습니다. 메모리 스냅샷을 만들면 업그레이드가 예상대로 완료되지 않거나 소프트웨어가 원하는 대로 작동하지 않는 경우 가상 시스템을 이전 상태로 되돌릴 수 있습니다.

메모리 상태를 캡처하는 경우 가상 시스템의 파일을 중지할 필요가 없습니다. 메모리 상태를 캡처하지 않을 경우 스냅샷에는 가상 시스템의 라이브 상태가 저장되지 않으며, 사용자가 디스크를 중지하지 않는 한 디스크는 충돌 일치 상태가 됩니다.

- 5 (선택 사항) 게스트 파일 시스템을 중지할지 선택합니다.

이 작업을 수행하려면 가상 시스템에 **VMware Tools**가 설치되어 있어야 합니다. 가상 시스템을 중지하면 **VMware Tools**에서는 가상 시스템의 파일 시스템을 중지합니다. 중지 작업은 스냅샷 디스크가 게스트 파일 시스템의 일관된 상태를 나타내도록 합니다. 중지된 스냅샷은 자동 또는 정기 백업에 적절합니다. 예를 들어 가상 시스템의 작업을 알지 못하는 상황에서 복구할 최신 백업을 여러 개 확보하려면 파일을 중지하면 됩니다.

대용량 디스크가 있는 가상 시스템은 중지할 수 없습니다.

- 6 **확인**을 클릭합니다.

결과

스냅샷을 사용하면 가상 시스템을 최신 스냅샷으로 되돌릴 수 있습니다.

스냅샷으로 가상 시스템 되돌리기


가상 시스템을 스냅샷이 생성되던 시점의 상태로 되돌릴 수 있습니다.

사전 요구 사항

가상 시스템에 스냅샷이 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.

- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 스냅샷으로 되돌리려는 가상 시스템의 **작업** 메뉴에서 **스냅샷으로 되돌리기**를 선택합니다.
- 4 **확인**을 클릭합니다.

결과

가상 시스템이 저장된 스냅샷으로 되돌려집니다.

가상 시스템의 스냅샷 제거


가상 시스템의 스냅샷을 제거할 수 있습니다.

스냅샷을 제거하면 보존된 가상 시스템의 상태가 삭제되고 그 상태로 다시 돌아갈 수 없습니다. 스냅샷을 제거해도 가상 시스템의 현재 상태는 영향을 받지 않습니다.

사전 요구 사항

가상 시스템과 저장된 스냅샷이 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 스냅샷을 제거하려는 가상 시스템의 **작업** 메뉴에서 **스냅샷 제거**를 선택합니다.
- 4 **확인**을 클릭합니다.


가상 시스템 임대 갱신

임대가 곧 만료되는 경우 가상 시스템 임대를 갱신할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.

3 임대 기간이 만료되는 가상 시스템의 **작업** 메뉴에서 **임대 갱신**을 선택합니다.

결과

임대가 갱신됩니다. **임대** 필드에서 새 임대 기간을 확인할 수 있습니다.


가상 시스템 삭제

조직에서 가상 시스템을 삭제할 수 있습니다.

사전 요구 사항

가상 시스템의 전원이 꺼져 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 삭제할 가상 시스템의 **작업** 메뉴에서 **삭제**를 선택합니다.
- 4 삭제를 확인합니다.

결과

가상 시스템이 삭제됩니다.

자동 스케일 그룹

VMware Cloud Director 10.2.2부터는 현재 CPU 및 메모리 사용에 따라 애플리케이션을 자동 스케일링할 수 있습니다.

자동 스케일 솔루션의 구성에 대한 자세한 내용은 "VMware Cloud Director 설치, 구성 및 업그레이드 가이드"의 [자동 스케일 그룹](#)을 참조하십시오.

CPU 및 메모리 사용에 대해 미리 정의한 조건에 따라, 선택한 스케일 그룹의 VM 수를 VMware Cloud Director가 자동으로 스케일 업/다운할 수 있습니다. 동일한 애플리케이션을 실행하도록 구성한 서버에 대해 로드 밸런싱을 수행하려면 VMware NSX Advanced Load Balancer(Avi Networks)를 사용하면 됩니다.

시스템 관리자 및 **조직 관리자** 역할은 스케일 그룹의 VM을 완전히 제어할 수 있습니다. 다른 글로벌 테넌트 역할은 VM을 보고 VM 웹 콘솔에 액세스할 수 있지만 삭제, 편집, 전원 작업 등은 수행할 수 없습니다.

스케일 그룹을 삭제하면 VMware Cloud Director는 스케일 그룹의 기존 VM 중 어느 것도 삭제하지 않습니다.

스케일 그룹 생성

VMware Cloud Director 10.2.2부터 서비스 제공자는 스케일 그룹을 생성하는 권한을 부여할 수 있습니다. 스케일 그룹의 VM 수는 정의한 조건에 따라 자동으로 변경됩니다.

스케일 그룹은 선택한 조직 VDC(가상 데이터 센터)에서 액세스할 수 있습니다.

절차

- 1 위쪽 탐색 모음에서 **애플리케이션**을 선택하고 **스케일 그룹** 탭을 선택합니다.
- 2 **새 스케일 그룹**을 클릭합니다.
- 3 스케일 그룹을 만들 조직 VDC를 선택합니다.
- 4 새 스케일 그룹의 이름과 설명(선택 사항)을 입력합니다.
- 5 그룹을 스케일링할 최소 및 최대 VM 수를 선택하고 **다음**을 클릭합니다.
- 6 스케일 그룹의 VM용 VM 템플릿과 스토리지 정책을 선택하고 **다음**을 클릭합니다.
- 7 스케일 그룹에 대한 네트워크를 선택합니다.
 - VDC가 NSX-T Data Center로 지원될 경우 로드 밸런서를 선택합니다.
 - 로드 밸런서를 직접 관리하거나 로드 밸런서가 필요하지 않은 경우 **완전하게 설정된 네트워크가 있습니다.**를 선택합니다.
- 8 **그룹 생성 및 규칙 추가**를 클릭합니다.

결과

최소 VM 수에 도달하기 위한 스케일 그룹의 초기 확장이 VMware Cloud Director에서 시작됩니다.

다음에 수행할 작업

- **자동 스케일링 규칙 추가**
- 스케일 그룹의 세부 정보 보기에서 **모니터**를 선택하면 이 스케일 그룹과 관련된 모든 작업을 볼 수 있습니다. 예를 들어 스케일 그룹 생성 시간, 그룹에 대한 모든 확장 또는 축소 작업, 작업을 시작한 규칙 등을 볼 수 있습니다.
- 스케일 그룹을 삭제합니다. 스케일 그룹을 삭제할 때 VMware Cloud Director는 스케일 그룹의 기존 VM 중 어느 것도 삭제하지 않습니다. VM 수를 줄이려면 수동으로 삭제해야 합니다.

자동 스케일링 규칙 추가

VMware Cloud Director 10.2.2부터 서비스 제공자는 스케일 그룹을 생성하고 관리하는 권한을 부여할 수 있습니다. 스케일 그룹의 확장 또는 축소를 트리거하는 규칙을 추가할 수 있습니다.

사전 요구 사항

스케일 그룹 생성

절차

- 1 위쪽 탐색 모음에서 **애플리케이션**을 선택하고 **스케일 그룹** 탭을 선택합니다.
- 2 스케일 그룹을 선택하고 **규칙**을 선택합니다.
- 3 **규칙 추가**를 클릭합니다.
- 4 규칙의 이름을 입력합니다.
- 5 규칙이 적용될 때 스케일 그룹이 확장되어야 하는지 또는 축소되어야 하는지 선택합니다.
- 6 규칙이 적용될 때 그룹을 확장 또는 축소할 **VM** 수를 선택합니다.
- 7 그룹에서 각 자동 스케일링 후 쿨다운 시간(분)을 입력합니다.

조건을 충족해도 쿨다운 시간이 만료될 때까지 다른 스케일링을 트리거할 수 없습니다. 스케일 그룹의 규칙이 적용되면 쿨다운 시간이 재설정됩니다.

- 8 규칙을 트리거하는 조건을 추가합니다.

지속 기간은 규칙을 트리거하기 위해 조건이 유효해야 하는 시간입니다. 규칙을 트리거하려면 모든 조건이 충족되어야 합니다.

- 9 (선택 사항) 다른 조건을 추가하려면 **조건 추가**를 클릭합니다.
- 10 **추가**를 클릭합니다.

vApp 작업

3

vApp는 네트워크를 통해 통신하고 배포된 환경의 리소스와 서비스를 사용하는 하나 이상의 가상 시스템으로 구성됩니다. vApp에는 여러 개의 가상 시스템이 포함될 수 있습니다.

VMware Cloud Director 9.5부터는 vApp에서 IPv6 연결이 지원됩니다. IPv6 네트워크에 연결된 가상 시스템에 IPv6 주소를 할당할 수 있습니다.

중요 vApp 작업에 대한 모든 단계는 카드 보기에 문서화되어 있으며, 둘 이상의 가상 데이터 센터가 있다는 가정 하에 준비되었습니다. 그리드 보기에서 동일한 절차를 완료할 수도 있지만 단계가 약간 다를 수 있습니다.

본 장은 다음 항목을 포함합니다.





- vApp 보기
- 새 vApp 작성
- OVF 패키지에서 vApp 만들기
- 카탈로그에서 vApp 추가
- vApp 템플릿에서 vApp 만들기
- vApp으로 vCenter Server에서 가상 시스템 가져오기
- vApp에서 전원 작업 수행
- vApp 열기
- vApp 속성 편집
- vApp 네트워크 다이어그램 표시
- vApp의 네트워크 작업
- 스냅샷 작업
- vApp의 소유자 변경
- 다른 가상 데이터 센터로 vApp 이동
- 다른 가상 데이터 센터에 중지된 vApp 복사
- 전원이 켜진 vApp 복사

- vApp에 가상 시스템 추가
- vApp을 vApp 템플릿으로 카탈로그에 저장
- OVF 패키지로 vApp 다운로드
- vApp 임대 갱신
- vApp 삭제
- 여러 vApp 삭제

vApp 보기

그리드 보기 또는 카드 보기로 vApp을 볼 수 있습니다.

절차

- 1 가상 데이터 센터 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 vApp을 선택합니다.
- 2 vApp을 그리드 보기에서 보려면  을 클릭합니다. 카드 보기에서 보려면  을 클릭합니다. vApp 목록이 그리드에 표시되거나 카드 목록으로 표시됩니다.
- 3 (선택 사항) 확인할 세부 정보를 포함하도록 그리드 보기를 구성합니다.
 - a 그리드 보기에서 **그리드 편집기** 아이콘()을 클릭합니다.
 - b 확인하려는 세부 정보 옆에 있는 확인란을 선택하여 그리드 보기에 포함할 vApp 세부 정보를 선택합니다.
 - c 변경 내용을 저장하려면 **확인**을 클릭합니다. 선택한 세부 정보가 각 vApp의 열로 표시됩니다.
- 4 (선택 사항) 그리드 보기에서 vApp 왼쪽에 있는  를 클릭하여 선택한 vApp에 대해 수행할 수 있는 작업을 표시합니다. 예를 들어 vApp을 종료할 수 있습니다.

새 vApp 작성

vApp 템플릿을 기반으로 vApp을 생성하는 대신 카탈로그의 가상 시스템이나 새 가상 시스템, 또는 둘 모두의 조합을 사용하여 vApp을 생성하도록 결정할 수 있습니다.

vApp을 작성하려면 vApp의 이름과 설명(선택 사항)을 제공해야 합니다. 나중에 뒤로 이동하여 vApp에 가상 시스템을 추가할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **vApp 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 **새 vApp**을 선택합니다.
- 3 vApp 이름과 설명(선택 사항)을 입력합니다.
- 4 (선택 사항) 배포 시 vApp의 전원을 켜려면 **전원 켜기** 확인란을 선택합니다.

참고 vApp은 가상 시스템이 포함된 경우에만 전원을 켤 수 있습니다.

- 5 (선택 사항) 카탈로그에서 이 vApp에 추가할 가상 시스템을 검색하거나 **가상 시스템 추가**를 클릭하여 비어 있는 새 가상 시스템을 추가합니다.

카탈로그에 가상 시스템이 없는 경우에는 가상 시스템을 생성하여 vApp에 추가합니다.

- a 가상 시스템에 대한 이름과 컴퓨터 이름을 입력합니다.

중요 컴퓨터 이름에는 영숫자와 하이픈만 포함될 수 있습니다. 컴퓨터 이름은 숫자로만 구성할 수 없으며 공백을 포함할 수 없습니다.

- b (선택 사항) 의미 있는 설명을 입력합니다.

c 가상 시스템의 배포 방법을 선택합니다.

옵션	작업
새로 만들기	<p>사용자 지정 설정으로 새 가상 시스템을 배포합니다.</p> <ol style="list-style-type: none"> 1 운영 체제 제품군과 운영 체제를 선택합니다. 2 (선택 사항) 부팅 이미지를 선택합니다. 3 (선택 사항) VM 배치 정책 및 VM 크기 조정 정책을 선택합니다. <p>VM 배치 및 VM 크기 조정 정책 드롭다운 메뉴는 서비스 제공자가 해당 정책을 조직 VDC에 게시한 경우에만 표시됩니다.</p> <ol style="list-style-type: none"> 4 가상 시스템의 크기를 선택하거나 사용자 지정 크기 조정 옵션을 클릭하고 계산, 메모리 및 스토리지 설정을 수동으로 입력합니다. <p>미리 정의된 가상 시스템의 크기는 [소], [중], [대]입니다.</p> <ol style="list-style-type: none"> 5 스토리지 정책 및 크기(GB)와 같은 스토리지 옵션을 지정합니다. 6 가상 시스템에 대한 네트워크 설정(예: 네트워크, IP 모드, IP 주소, 기본 NIC)을 지정합니다.
템플릿에서	<p>템플릿 카탈로그에서 선택한 템플릿에서 가상 시스템을 배포합니다.</p> <ol style="list-style-type: none"> 1 카탈로그에서 가상 시스템 템플릿을 선택합니다. 2 (선택 사항) VM 배치 정책 및 VM 크기 조정 정책을 선택합니다. <p>VM 배치 및 VM 크기 조정 정책 드롭다운 메뉴는 서비스 제공자가 해당 정책을 조직 VDC에 게시한 경우에만 표시됩니다. 선택한 템플릿에 정책이 할당된 경우에는 미리 정의된 템플릿 정책으로 제한될 수 있습니다.</p> <ol style="list-style-type: none"> 3 (선택 사항) 사용자 지정 스토리지 정책을 사용하도록 선택하고 사용할 사용자 지정 스토리지 정책에서 정책을 선택합니다. 4 사용 가능한 최종 사용자 라이선스 계약이 있으면 검토하고 수락해야 합니다.

d vApp에 가상 시스템을 추가하려면 **확인**을 클릭합니다.

추가된 가상 시스템은 카탈로그에서 볼 수 있습니다.

6 (선택 사항) vApp 내에 추가로 생성할 각 가상 시스템에 대해 **단계 5**를 반복합니다.7 vApp 생성을 완료하려면 **만들기**를 클릭합니다.**결과**

vApp이 생성됩니다. vApp의 전원이 켜지면 vApp의 가상 시스템이 생성되고 전원도 켜집니다.

OVF 패키지에서 vApp 만들기

vApp 템플릿과 해당 카탈로그 항목을 만들지 않고도 OVF 패키지에서 직접 vApp을 만들어 배포할 수 있습니다.

VMware Cloud Director에는 OVF 배포에 대해 vCenter Server의 제한 사항과는 다른 자체 제한 사항이 있습니다. 그 결과 vCenter Server에서 성공하는 OVF 배포가 VMware Cloud Director에서는 실패할 수 있습니다.

VMware Cloud Director는 OVF 1.1을 지원하지만 OVF 1.1 스키마의 일부 섹션을 지원하지는 않습니다. 예를 들어 OVF의 DeploymentOptions 섹션은 지원되지 않습니다.

VMware Cloud Director의 OVF 배포에는 TransferService, NFS 마운트의 스푼링 영역, vCenter Server에 대한 NFC 연결, 체크섬 유효성 검사 등과 같은 많은 구성 요소가 포함됩니다. 이러한 구성 요소 중 하나라도 실패하면 OVF 업로드가 실패합니다.

매니페스트 파일과 함께 OVF 패키지를 업로드하는 경우 VMware Cloud Director는 OVF 설명자 파일과 모든 VMDK 파일의 SHA-1 해시를 manifest.mf 파일의 값으로 검증합니다. 일치하지 않는 해시가 있으면 업로드가 실패합니다. **시스템 관리자**는 CONFIG 속성을 ovf.manifest.check.disabled로 설정하여 이 검사를 비활성화할 수 있습니다.

사전 요구 사항

- 업로드할 OVF 패키지가 있고 OVF 패키지 업로드 및 vApp 배포를 위한 사용 권한이 있는지 확인합니다.
- OVF 설명자 파일의 OVF 버전이 0.9가 아닌지 확인합니다.
- VMware Cloud Director에서 지원되는 OVF 설명자 파일의 기본 최대 크기는 12MB입니다. CONFIG 속성 ovf.descriptor.size.max를 편집하여 이 값을 재정의할 수 있습니다.
- 매니페스트 파일(.mf 확장명)의 기본 최대 허용 크기가 1MB인지 확인합니다.
- OVF 패키지가 OVF XSD 스키마를 준수하는지 확인합니다.
- OVF 설명자 파일의 VirtualSystemType 요소에 하드웨어 버전이 제공된 경우 OVF를 업로드하는 VDC에서 지원되는 최고 하드웨어 버전보다 낮은지 확인합니다.
- OVF 설명자 파일에 ExtraConfig 요소가 포함된 경우 **시스템 관리자**가 extraConfigs 요소의 AllowedList에 이러한 요소를 포함했는지 확인합니다. AllowedList에 포함되지 않은 요소가 있는 경우 유효성 검사 오류가 발생하여 OVF 업로드가 실패합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 **OVF에서 vApp 추가**를 클릭합니다.
- 3 **업로드** 버튼을 클릭하여 컴퓨터에서 액세스할 수 있는 위치로 이동하고 OVF/OVA 템플릿 파일을 선택합니다.

이 위치는 로컬 하드 드라이브, 네트워크 공유 또는 CD/DVD 드라이브일 수 있습니다. 지원되는 파일 확장명은 .ova, .ovf, .vmdk, .mf, .cert 및 .strings 파일입니다. 업로드하려는 파일(예: VMDK 파일)보다 많은 파일을 참조하는 OVF 파일을 업로드하도록 선택한 경우, 모든 파일을 찾아서 선택해야 합니다.

- 4 **다음**을 클릭합니다.
- 5 배포하려는 OVF/OVA 템플릿의 세부 정보를 확인하고 **다음**을 클릭합니다.

6 vApp의 이름과 설명(선택 사항)을 입력하고 **다음**을 클릭합니다.

7 (선택 사항) vApp의 컴퓨터 이름을 영숫자만 포함되도록 변경합니다.

이 단계는 vApp의 이름에 공백 또는 특수 문자가 포함된 경우에만 필요합니다. 기본적으로 컴퓨터 이름이 가상 시스템의 이름으로 자동으로 채워집니다. 하지만 컴퓨터 이름에는 영숫자만 포함되어야 합니다.

8 **스토리지 정책** 드롭다운 메뉴에서 vApp의 각 가상 시스템에 대한 스토리지 정책을 선택하고 **다음**을 클릭합니다.

9 각 가상 시스템에 연결할 네트워크를 선택합니다.

- **네트워크** 드롭다운 메뉴에서 각 가상 시스템의 네트워크를 선택합니다.

- **고급 네트워킹 워크플로우로 전환** 확인란을 선택하고 vApp의 각 가상 시스템에 대한 기본 NIC, 네트워크 어댑터 유형, 네트워크, IP 할당 및 IP 주소 설정과 같은 네트워크 설정을 수동으로 입력할 수 있습니다.

마법사를 완료한 후 가상 시스템에 대한 추가 속성을 구성할 수 있습니다.

10 **다음**을 클릭합니다.

11 vApp에 있는 가상 시스템의 하드웨어를 사용자 지정하고 **다음**을 클릭합니다.

옵션	설명
가상 CPU 수	vApp의 각 가상 시스템에 대한 가상 CPU 수를 입력합니다. 가상 시스템에 할당할 수 있는 가상 CPU의 최대 개수는 호스트의 논리적 CPU 수 및 가상 시스템에 설치된 게스트 운영 체제 유형에 따라 달라집니다.
소켓당 코어	vApp의 각 가상 시스템에 대한 소켓당 코어 수를 입력합니다. 코어 수 및 소켓당 코어 수와 관련하여 가상 CPU의 할당 방법을 구성할 수 있습니다. 가상 시스템에서 필요한 CPU 코어 수를 결정한 다음 단일 코어 CPU, 듀얼 코어 CPU, 트라이 코어 CPU 등 어떤 CPU가 필요한지에 따라 각 소켓에서 원하는 코어 수를 선택합니다.
코어 수	vApp의 각 가상 시스템에 대한 코어 수를 봅니다. 가상 CPU 수를 업데이트하면 이 수가 변경됩니다.
총 메모리(MB)	vApp의 각 가상 시스템에 대한 메모리를 MB단위로 입력합니다. 이 설정은 가상 시스템에 할당되는 ESXi 호스트 메모리의 양을 결정합니다. 가상 하드웨어 메모리 크기는 가상 시스템에서 실행되는 애플리케이션에 사용할 수 있는 메모리 양을 결정합니다. 가상 시스템은 구성된 가상 하드웨어 메모리 크기 이상의 메모리 리소스를 활용할 수 없습니다.

12 [완료 준비] 페이지에서 설정을 검토하고 **마침**을 클릭합니다.

결과

새 vApp이 카드 보기에 표시됩니다.

카탈로그에서 vApp 추가

카탈로그에 대한 액세스 권한이 있는 경우 카탈로그의 vApp 템플릿을 사용하여 vApp을 생성할 수 있습니다.

vApp 템플릿은 vApp의 가상 시스템을 사용자 지정하는 속성과 함께 OVF 파일을 기반으로 할 수 있습니다. vApp은 이러한 속성을 상속합니다. 이러한 속성을 사용자가 구성할 수 있는 경우 해당 값을 지정할 수 있습니다.

사전 요구 사항

- 공용 카탈로그의 vApp 템플릿에 액세스하려면 **조직 관리자** 또는 **vApp 작성자** 권한이 있는지 확인합니다.
- 사용자에게 공유되는 조직 카탈로그의 vApp 템플릿에 액세스하려면 **vApp 사용자** 이상의 권한이 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 **새로 만들기**를 클릭하고 **카탈로그에서 vApp 추가**를 선택합니다.
- 3 가져올 템플릿을 선택하고 **다음**을 클릭합니다.
- 4 vApp 이름과 설명(선택 사항)을 입력합니다.
- 5 vApp에 대한 런타임 임대 및 스토리지 임대를 입력하고 **다음**을 클릭합니다.
- 6 **스토리지 정책** 드롭다운 메뉴에서 vApp의 각 가상 시스템에 대한 스토리지 정책을 선택하고 **다음**을 클릭합니다.
- 7 vApp의 가상 시스템에 대한 배치 정책 및 크기 조정 정책을 구성할 수 있는 경우 드롭다운 메뉴에서 각 가상 시스템에 대한 정책을 선택합니다.
- 8 vApp의 가상 시스템에 대한 계산 속성을 구성할 수 있는 경우 이를 사용자 지정하고 **다음**을 클릭합니다.

옵션	설명
가상 CPU	vApp의 각 가상 시스템에 대한 가상 CPU 수를 입력합니다. 가상 시스템에 할당할 수 있는 가상 CPU의 최대 개수는 호스트의 논리적 CPU 수 및 가상 시스템에 설치된 게스트 운영 체제 유형에 따라 달라집니다.
소켓당 코어	vApp의 각 가상 시스템에 대한 소켓당 코어 수를 입력합니다. 코어 수 및 소켓당 코어 수와 관련하여 가상 CPU의 할당 방법을 구성할 수 있습니다. 가상 시스템에서 필요한 CPU 코어 수를 결정한 다음 단일 코어 CPU, 듀얼 코어 CPU, 트라이 코어 CPU 등 어떤 CPU가 필요한지에 따라 각 소켓에서 원하는 코어 수를 선택합니다.

옵션	설명
코어 수	vApp의 각 가상 시스템에 대한 코어 수를 봅니다. 가상 CPU 수를 업데이트하면 이 수가 변경됩니다.
메모리	vApp의 각 가상 시스템에 대한 메모리를 MB단위로 입력합니다. 이 설정은 가상 시스템에 할당되는 ESXi 호스트 메모리의 양을 결정합니다. 가상 하드웨어 메모리 크기는 가상 시스템에서 실행되는 애플리케이션에 사용할 수 있는 메모리 양을 결정합니다. 가상 시스템은 구성된 가상 하드웨어 메모리 크기 이상의 메모리 리소스를 활용할 수 없습니다.

- 9 vApp의 가상 시스템에 대한 하드웨어 속성을 구성할 수 있는 경우 가상 시스템 하드 디스크의 크기를 사용자 지정하고 **다음**을 클릭합니다.
- 10 vApp의 가상 시스템에 대한 네트워킹 속성을 구성할 수 있는 경우 이를 사용자 지정하고 **다음**을 클릭합니다.
 - a **네트워킹 구성** 페이지에서 각 가상 시스템에서 연결할 네트워크를 선택합니다.
 - b (선택 사항) 고급 네트워킹 워크플로우로 전환하고 vApp의 가상 시스템에 대한 추가 네트워크 설정을 구성하려면 이 확인란을 선택합니다.
- 11 vApp 설정을 검토하고 **마침**을 클릭합니다.

vApp 템플릿에서 vApp 만들기

액세스할 수 있는 카탈로그에 저장된 vApp 템플릿을 기반으로 새 vApp를 만들 수 있습니다.

vApp 템플릿이 가상 시스템을 사용자 지정하기 위한 OVF 속성이 포함된 OVF 파일을 기반으로 하는 경우 이러한 속성은 vApp에 전달됩니다. 이러한 속성을 사용자가 구성할 수 있는 경우 값을 지정할 수 있습니다.

사전 요구 사항

- 조직 관리자와 vApp 작성자만 공개 카탈로그의 vApp 템플릿에 액세스할 수 있습니다.
- vApp 사용자 이상의 권한이 있으면 공유된 조직 카탈로그의 vApp 템플릿에 액세스할 수 있습니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **vApp 템플릿**을 선택합니다.
템플릿 목록이 그리드 보기에 나타납니다.
- 2 사용할 vApp 템플릿 옆에 있는 라디오 버튼을 클릭하고 **vApp 만들기**를 클릭합니다.
- 3 vApp 이름과 설명(선택 사항)을 입력합니다.
- 4 이 vApp이 자동으로 중지되기 전까지 실행 가능한 시간을 시간 또는 일 단위로 지정합니다.
- 5 중지된 vApp이 자동으로 정리되기 전에 사용 가능한 상태로 유지되는 시간을 시간 또는 일 단위로 지정합니다.
- 6 **다음**을 클릭합니다.

7 vApp을 만들려는 가상 데이터 센터를 선택합니다.

8 스토리지 정책을 선택합니다.

9 다음을 클릭합니다.

10 VMware Cloud Director 10.2.2 이상인 경우 VM 배치 및 크기 조정 정책을 구성합니다.

버전 10.2.2부터 배치 정책은 글로벌 정책이고 여러 제공자 VDC에 게시할 수 있으며 vApp 템플릿에는 크기 조정 및 배치 정책 정보가 모두 포함됩니다.

11 각 가상 시스템에 연결할 네트워크를 선택합니다.

- **네트워크** 드롭다운 메뉴에서 각 가상 시스템의 네트워크를 선택합니다.

- **고급 네트워킹 워크플로우로 전환** 확인란을 선택하고 vApp의 각 가상 시스템에 대한 기본 NIC, 네트워크 어댑터 유형, 네트워크, IP 할당 및 IP 주소 설정과 같은 네트워크 설정을 수동으로 입력할 수 있습니다.

마법사를 완료한 후 가상 시스템에 대한 추가 속성을 구성할 수 있습니다.

12 다음을 클릭합니다.

13 vApp에 있는 가상 시스템의 하드웨어를 사용자 지정하고 다음을 클릭합니다.

옵션	설명
가상 CPU 수	vApp의 각 가상 시스템에 대한 가상 CPU 수를 입력합니다. 가상 시스템에 할당할 수 있는 가상 CPU의 최대 개수는 호스트의 논리적 CPU 수 및 가상 시스템에 설치된 게스트 운영 체제 유형에 따라 달라집니다.
소켓당 코어	vApp의 각 가상 시스템에 대한 소켓당 코어 수를 입력합니다. 코어 수 및 소켓당 코어 수와 관련하여 가상 CPU의 할당 방법을 구성할 수 있습니다. 가상 시스템에서 필요한 CPU 코어 수를 결정한 다음 단일 코어 CPU, 듀얼 코어 CPU, 트라이 코어 CPU 등 어떤 CPU가 필요한지에 따라 각 소켓에서 원하는 코어 수를 선택합니다.
코어 수	vApp의 각 가상 시스템에 대한 코어 수를 봅니다. 가상 CPU 수를 업데이트하면 이 수가 변경됩니다.
총 메모리(MB)	vApp의 각 가상 시스템에 대한 메모리를 MB단위로 입력합니다. 이 설정은 가상 시스템에 할당되는 ESXi 호스트 메모리의 양을 결정합니다. 가상 하드웨어 메모리 크기는 가상 시스템에서 실행되는 애플리케이션에 사용할 수 있는 메모리 양을 결정합니다. 가상 시스템은 구성된 가상 하드웨어 메모리 크기 이상의 메모리 리소스를 활용할 수 없습니다.
하드 디스크 속성	가상 시스템 하드 디스크의 크기를 MB 단위로 입력합니다.

14 [완료 준비] 페이지에서 설정을 검토하고 마침을 클릭합니다.

결과

새 vApp이 카드 보기에 표시됩니다.

vApp으로 vCenter Server에서 가상 시스템 가져오기

시스템 관리자 권한이 있는 경우 vCenter Server VM을 vApp으로 VMware Cloud Director에 가져올 수 있습니다.

가상 시스템을 가져오면 vCenter Server에 구성되어 있는 가상 시스템 예약, 제한 및 공유 설정이 유지되지 않습니다. 가져온 가상 시스템에는 해당 시스템이 속해 있는 조직 가상 데이터 센터의 리소스 할당 설정이 적용됩니다.

사전 요구 사항

vCenter Server에서 가상 시스템을 보고 가져오려면 **시스템 관리자** 권한이 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 **새로 만들기**를 클릭하고 **vCenter에서 가져오기**를 선택합니다.
- 3 드롭다운 메뉴에서 가상 시스템을 가져올 vCenter Server 인스턴스를 선택합니다.
- 4 가져올 가상 시스템을 선택합니다.
- 5 vApp 이름과 설명(선택 사항)을 입력합니다.
- 6 드롭다운 메뉴에서 vApp을 저장 및 실행할 가상 데이터 센터를 선택합니다.
- 7 (선택 사항) 드롭다운 메뉴에서 vApp에 대한 스토리지 정책을 선택합니다.
- 8 (선택 사항) 소스 가상 시스템을 삭제하려면 **가상 시스템 이동** 옵션을 설정합니다.
- 9 **가져오기**를 클릭합니다.

vApp에서 전원 작업 수행

vApp 전원 켜기 또는 끄기, vApp 일시 중단 또는 재설정과 같은 vApp의 전원 작업을 수행할 수 있습니다.


vApp 전원 켜기

vApp의 전원을 켜면 vApp에서 아직 전원이 켜져 있지 않은 모든 가상 시스템의 전원이 켜집니다.

사전 요구 사항

vApp 작성자 이상의 권한이 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.

3 전원을 켜려는 vApp의 **작업** 메뉴에서 **전원 켜기**를 선택합니다.

결과

vApp의 전원이 켜집니다.


vApp 전원 끄기

vApp의 전원을 끄면 vApp에 있는 모든 가상 시스템의 전원이 꺼집니다. 카탈로그에 vApp 추가, 복사 또는 다른 VDC로 이동과 같은 특정 작업을 수행하려면 먼저 vApp의 전원을 꺼야 합니다.

사전 요구 사항

vApp가 시작되어 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 중지하려는 vApp의 **작업** 메뉴에서 **전원 끄기**를 선택합니다.
- 4 **확인**을 클릭합니다.

결과

vApp 자체를 포함하여 vApp에 있는 모든 가상 시스템의 전원이 꺼집니다.


vApp 재설정

vApp을 재설정 하면 상태(메모리, 캐시 등)가 지워지지만 vApp은 계속 실행됩니다.

사전 요구 사항

vApp이 시작되고 그 안에 포함된 가상 시스템의 전원이 켜져 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 재설정하려는 vApp의 **작업** 메뉴에서 **재설정**을 선택합니다.

결과

상태가 지워지고 vApp은 계속 실행됩니다.


vApp 일시 중단

vApp을 일시 중단하면 메모리가 디스크에 기록되어 현재 상태가 보존됩니다.

사전 요구 사항

vApp가 실행 중이어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 일시 중단하려는 vApp의 **작업** 메뉴에서 **일시 중단**을 선택합니다.

결과

vApp이 일시 중단되고 해당 상태가 보존됩니다.


vApp의 일시 중단된 상태 삭제

vApp이 일시 중단된 상태이고 vApp의 사용을 더 이상 재개할 필요가 없는 경우 일시 중단된 상태를 삭제할 수 있습니다. 일시 중단된 상태를 삭제하면 저장된 메모리가 제거되고 vApp이 전원이 꺼진 상태로 돌아갑니다.

사전 요구 사항

vApp이 일시 중단된 상태에 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 일시 중단된 vApp의 **작업** 메뉴에서 **일시 중단된 상태 삭제**를 선택합니다.

결과

상태가 삭제되고 vApp의 전원이 꺼집니다.

여러 vApp 전원 켜기

동시에 여러 vApp의 전원을 켤 수 있습니다. 이 작업을 수행하면 vApp에서 아직 전원이 켜져 있지 않은 모든 VM의 전원이 켜집니다.

사전 요구 사항

vApp 작성자 이상의 권한이 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 **다중 선택** 옵션을 설정합니다.
- 3 전원을 켜 **vApp**을 선택합니다.
- 4 **작업** 메뉴에서 **전원 켜기**를 선택합니다.
- 5 **확인**을 클릭하여 확인합니다.

여러 vApp 전원 끄기

동시에 여러 vApp의 전원을 끌 수 있습니다. 이 작업은 vApp에 있는 모든 가상 시스템의 전원을 끕니다. 카탈로그에 vApp 추가, 복사 또는 다른 가상 데이터 센터로 이동과 같은 특정 작업을 수행하려면 먼저 vApp의 전원을 꺼야 합니다.

사전 요구 사항

- vApp이 시작되었는지 확인합니다.
- **vApp 작성자** 이상의 권한이 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 **다중 선택** 옵션을 설정합니다.
- 3 전원을 끌 **vApp**을 선택합니다.
- 4 **작업** 메뉴에서 **전원 끄기**를 선택합니다.
- 5 **확인**을 클릭하여 확인합니다.

여러 vApp의 일시 중단된 상태 삭제

여러 vApp이 일시 중단된 상태이고 더 이상 사용을 재개할 필요가 없는 경우 vApp의 일시 중단된 상태를 동시에 삭제할 수 있습니다. 일시 중단된 상태를 삭제하면 저장된 메모리가 제거되고 vApp이 전원이 꺼진 상태로 돌아갑니다.

사전 요구 사항

- vApp이 일시 중단된 상태인지 확인합니다.
- **vApp 작성자** 이상의 권한이 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.

- 2 **다중 선택** 옵션을 설정합니다.
- 3 전원을 끌 일시 중단된 vApp을 선택합니다.
- 4 **작업** 메뉴에서 **일시 중단된 상태 삭제**를 선택합니다.

결과

vApp의 전원이 꺼집니다.

여러 vApp 재설정

동시에 여러 vApp을 재설정하면 메모리, 캐시를 포함한 해당 상태가 지워지지만 vApp은 계속 실행됩니다.

사전 요구 사항

- vApp이 시작되었는지 그리고 그 안에 포함된 가상 시스템의 전원이 켜져 있는지 확인합니다.
- **vApp 작성자** 이상의 권한이 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 **다중 선택** 옵션을 설정합니다.
- 3 재설정할 vApp을 선택합니다.
- 4 **작업** 메뉴에서 **재설정**을 선택하고 **확인**을 클릭하여 확인합니다.

결과

각 vApp의 상태가 지워지고 vApp은 계속 실행됩니다.

여러 vApp 일시 중단

동시에 여러 vApp을 일시 중단하면 메모리가 디스크에 기록되어 현재 상태가 보존됩니다.

사전 요구 사항

vApp이 실행되고 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 **다중 선택** 옵션을 설정합니다.
- 3 일시 중단할 vApp을 선택합니다.
- 4 일시 중단하려는 vApp의 **작업** 메뉴에서 **일시 중단**을 선택하고 **확인**을 클릭하여 확인합니다.

결과


vApp이 일시 중단되고 해당 상태가 보존됩니다.

vApp 열기

vApp을 열어서 vApp에 포함된 가상 시스템과 네트워크를 볼 수 있습니다. 가상 시스템과 네트워크의 연결 방식을 보여주는 다이어그램도 볼 수 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.

- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.

카드 보기에서 이름, 전원 상태, 임대 정보, 생성 날짜, 소유자, vApp과 연결된 가상 시스템 수, 총 CPU 수, 총 스토리지 및 메모리, 연결된 네트워크와 같은 각 vApp에 대한 일반 정보를 볼 수 있습니다.

- 3 선택한 vApp의 상세 설정을 보려면 vApp 카드에서 **세부 정보**를 클릭합니다.

vApp 속성 편집

vApp 이름 및 설명, 임대 설정, vApp에서 가상 시스템을 시작하는 순서, 공유 설정 및 네트워크 설정을 비롯한 기존 vApp의 속성을 편집할 수 있습니다.

vApp의 일반 속성 편집


vApp의 이름, 설명 및 기타 일반 속성을 검토하고 변경할 수 있습니다.

사전 요구 사항

vApp가 전원이 꺼져 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.

- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.

- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭하여 vApp 속성을 보고 편집합니다.

- 4 필요에 따라 속성을 검토 및 변경하고 **저장**을 클릭합니다.

옵션	작업
이름	vApp의 새 이름을 입력합니다.
설명	vApp의 설명(선택 사항)을 입력합니다.

옵션	작업
가상 데이터 센터	vApp이 속한 데이터 센터의 이름입니다.
스냅샷	스냅샷이 있는 경우 스냅샷 세부 정보가 표시됩니다.
임대	<p>임대를 갱신하려면 갱신을 선택합니다.</p> <p>a 런타임 임대를 시간 또는 일 수로 예약합니다.</p> <p>vApp이 자동으로 중지되기 전까지 실행 가능한 시간을 정의합니다.</p> <p>b 스토리지 임대를 시간 또는 일 수로 예약합니다.</p> <p>vApp이 자동으로 삭제되기 전에 사용 가능한 상태로 유지되는 시간을 정의합니다.</p>

결과

일반 설정이 저장됩니다.

vApp에서 가상 시스템의 시작 및 중지 순서 편집


vApp 내에서 가상 시스템의 시작 및 중지 순서를 구성할 수 있습니다. 특정 순서로 시작하고 중지해야 하는 가상 시스템에 응용 프로그램이 설치된 경우 시작 및 중지 순서를 구성합니다.

이러한 설정은 가상 시스템을 특정 순서로 시작하고 중지해야 하는 경우 유용합니다. 예를 들어 데이터베이스 서버가 상주하는 가상 시스템, 애플리케이션 서버가 상주하는 가상 시스템 및 웹 서버가 상주하는 가상 시스템이 있습니다. 관련된 기능이 올바르게 작동하려면 데이터베이스 서버를 먼저 시작하고 애플리케이션 서버를 두 번째로 시작하고 웹 서버를 마지막으로 시작해야 합니다.

사전 요구 사항

vApp가 전원이 꺼져 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭합니다.
- 4 **시작 및 중지 순서** 탭을 클릭하고 **편집**을 클릭합니다.
- 5 각 가상 시스템에 대한 시작 및 중지 순서 속성을 편집하고 **확인**을 클릭합니다.

옵션	작업
시작 순서	가상 시스템을 시작할 순서를 입력합니다. 순서의 각 시스템에 대한 값을 입력해야 합니다.
시작 동작	<p>시작 동작을 선택합니다.</p> <p>시작 동작은 가상 시스템이 포함된 vApp을 시작할 때 가상 시스템에서 수행되는 작업을 결정합니다. 기본적으로 이 옵션은 전원 켜기로 설정되어 있습니다.</p>

옵션	작업
시작 대기	시작 대기 시간을 입력합니다. 시작 대기 시간은 VMware Cloud Director가 순서의 다음 시스템을 시작하기 전에 대기할 시간(초)입니다.
중지 동작	중지 동작을 선택합니다. 중지 동작은 가상 시스템이 포함된 vApp을 중지할 때 가상 시스템에서 수행하는 작업입니다. 전원 끄기 를 선택하면 안정성을 보장하는 종료 동작 없이 VM 전원이 꺼집니다. 이는 소켓에서 플러그를 뽑는 것과 같습니다. VMware Tools를 설치하지 않은 경우 이 동작을 선택합니다. 설치한 경우 안정적인 종료를 위해 종료 를 선택합니다.
중지 대기	중지 대기 시간을 입력합니다. 중지 대기 시간은 VMware Cloud Director가 순서의 다음 가상 시스템을 종료하기 전에 대기할 시간(초)입니다.

vApp의 게스트 속성 편집


vApp에 사용자가 구성할 수 있는 OVF 속성이 포함되어 있는 경우 이러한 속성을 검토하고 수정할 수 있습니다.

vApp의 가상 시스템에 동일한 이름의 사용자가 구성할 수 있는 속성 값이 포함되어 있는 경우 가상 시스템 값이 우선합니다.

사전 요구 사항

vApp이 중지되었는지 그리고 해당 게스트 속성을 사용자가 구성할 수 있는지 확인합니다.

절차


- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **가상 시스템**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 목록을 표시하고 필요에 따라 **정렬 기준** 드롭다운 메뉴에서 가상 시스템 목록을 정렬합니다.
- 3 편집할 가상 시스템의 카드에서 **세부 정보**를 클릭합니다.
- 4 **게스트 속성**을 클릭하고 **편집**을 클릭합니다.
- 5 vApp에 대한 게스트 속성을 수정하고 **확인**을 클릭합니다.

vApp 공유

vApp을 조직 내의 다른 그룹이나 사용자와 공유할 수 있습니다. 설정한 액세스 제어에 따라 공유 vApp에서 수행할 수 있는 작업이 결정됩니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.

- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭하고 아래로 스크롤하여 vApp의 공유 속성으로 이동합니다.
- 4 vApp을 공유하려는 사용자를 선택하고 **저장**을 클릭합니다.

옵션	작업
조직 내 모든 사람과 공유	<p>조직의 모든 사용자와 공유하고 액세스 수준을 선택하려면 이 옵션을 선택합니다.</p> <ul style="list-style-type: none"> ■ 모든 권한을 부여하려면 모든 권한을 선택합니다. <p>조직의 모든 사용자는 vApp을 열고, 시작하고, vApp 템플릿으로 저장할 수 있으며 템플릿을 카탈로그에 추가하고, vApp의 소유자를 변경하고, 카탈로그에 복사하고, 속성을 수정할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 읽기 전용 액세스 권한을 부여하려면 읽기 전용을 선택합니다.
특정 사용자 및 그룹과 공유	<p>지정한 사용자와만 공유하려면 이 옵션을 선택합니다.</p> <ol style="list-style-type: none"> a 액세스 권한이 없는 사용자 및 그룹 패널에서 이름을 선택하고 액세스 권한이 있는 사용자 및 그룹 패널로 해당 이름을 이동합니다. b 지정한 사용자 및 그룹의 액세스 수준을 선택합니다. <ul style="list-style-type: none"> ■ 모든 권한을 부여하려면 모든 권한을 선택합니다. <p>모든 권한을 가진 사용자는 vApp을 열고, 시작하고, vApp 템플릿으로 저장할 수 있으며 템플릿을 카탈로그에 추가하고, vApp의 소유자를 변경하고, 카탈로그에 복사하고, 속성을 수정할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 읽기 전용 액세스 권한을 부여하려면 읽기 전용을 선택합니다.

결과

vApp가 지정한 사용자 또는 그룹과 공유됩니다.


vApp 네트워크 다이어그램 표시

vApp 네트워크 다이어그램에서는 vApp의 가상 시스템 및 네트워크를 그래픽으로 볼 수 있습니다.

사전 요구 사항

vApp 네트워크 다이어그램을 보려면 vApp에 40개 미만의 가상 시스템이 포함되어 있어야 합니다. vApp에 포함된 가상 시스템의 수가 40개 이상인 경우 다이어그램을 사용할 수 없습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 vApp을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭합니다.

4 네트워크 다이어그램 탭을 클릭합니다.

vApp의 가상 시스템과 네트워크가 어떻게 연결되어 있는지 보여 주는 다이어그램이 표시됩니다. 별표 기호는 기본 NIC를 나타냅니다. NIC가 연결되어 있으면 녹색으로 나타나고 NIC가 연결되어 있지 않으면 흰색으로 나타납니다.

5 (선택 사항) 연결된 가상 시스템과 네트워크를 강조 표시하려면 네트워크 또는 가상 시스템을 클릭합니다.

연결된 개체와 개체 간의 연결이 강조 표시됩니다.

다음에 수행할 작업

이 페이지에서 가상 시스템 또는 네트워크를 추가할 수 있습니다.

vApp의 네트워크 작업

vApp의 가상 시스템은 vApp 네트워크(격리되거나 라우팅된) 및 조직 가상 데이터 센터 네트워크(직접 또는 펜싱된)에 연결할 수 있습니다. vApp에 여러 유형의 네트워크를 추가하여 여러 가지 네트워킹 시나리오를 처리할 수 있습니다.

vApp의 가상 시스템은 vApp에서 사용할 수 있는 네트워크에 연결할 수 있습니다. 가상 시스템을 다른 네트워크에 연결하려면 먼저 해당 네트워크를 vApp에 추가해야 합니다.

vApp은 vApp 네트워크와 조직 가상 데이터 센터 네트워크를 포함할 수 있습니다. vApp 네트워크는 격리되거나 라우팅될 수 있습니다. 격리된 vApp 네트워크는 vApp 내에 포함됩니다. vApp 네트워크를 조직 가상 데이터 센터 네트워크로 라우팅하여 vApp 외부의 가상 시스템에 연결을 제공할 수도 있습니다. 라우팅된 vApp 네트워크에 대해 방화벽 및 정적 라우팅과 같은 네트워크 서비스를 구성할 수 있습니다.

참고 NSX Data Center for vSphere에서 지원하는 조직 VDC는 라우팅된 vApp 네트워크, 격리된 vApp 네트워크 및 직접 vApp 네트워크를 지원합니다.

NSX-T Data Center에서 지원하는 조직 VDC는 격리된 vApp 네트워크 및 직접 vApp 네트워크를 지원합니다.

vApp을 조직 가상 데이터 센터 네트워크에 직접 연결할 수 있습니다. 동일한 조직 가상 데이터 센터 네트워크에 연결된 동일한 가상 시스템이 포함된 vApp이 여러 개 있는 경우 vApp을 동시에 시작하려면 vApp을 펜싱할 수 있습니다. vApp을 펜싱하면 MAC 및 IP 주소를 격리하여 충돌 없이 가상 시스템의 전원을 켤 수 있습니다.

vApp에 추가하는 네트워크는 vApp을 생성한 조직 가상 데이터 센터와 연결된 네트워크 풀을 사용합니다.


vApp 네트워크 보기

vApp의 네트워크에 액세스하고 볼 수 있습니다.

사전 요구 사항

절차


- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.

- 2  을 클릭하여 카드 보기에서 **vApp**을 확인합니다.

- 3 선택한 **vApp**의 카드에서 **세부 정보**를 클릭합니다.

- 4 **네트워크** 탭을 클릭합니다.

네트워크 목록이 있으면 표시됩니다. 각 네트워크에 대해 이름, 게이트웨이, 넷마스크, 연결, 유지된 IP 및 NAT 리소스와 같은 정보를 볼 수 있습니다.

- 5 (선택 사항) 표시할 열을 편집하려면 **그리드 편집기** 아이콘()을 클릭하고 표시하거나 숨길 각 열의 확인란을 선택하거나 선택 취소합니다.

vApp 네트워크 펜싱

서로 다른 **vApp**에 포함되어 있는 동일한 가상 시스템의 전원을 켜면 충돌이 발생할 수 있습니다. 서로 다른 **vApp**에 있는 동일한 가상 시스템의 전원을 충돌 없이 켜려면 **vApp**을 펜싱해야 합니다.


vApp을 펜싱하면 가상 시스템의 **MAC** 주소와 **IP** 주소가 격리되고 조직 **VDC** 네트워크의 연결 유형이 직접에서 펜싱됨으로 변경됩니다. 펜싱된 네트워크에서는 방화벽이 자동으로 사용되도록 설정 및 구성되어 송신 트래픽만 허용됩니다. **vApp**을 펜싱하는 경우 펜싱된 네트워크의 **NAT** 및 방화벽 규칙도 구성할 수 있습니다.

사전 요구 사항

- 직접 **vApp** 네트워크만 펜싱할 수 있습니다. **vApp**에서 둘 이상의 네트워크를 사용 중이고 다른 네트워크가 예를 들어 라우팅된 네트워크인 경우 직접 네트워크만 펜싱됩니다.
- **vApp**에서 직접 네트워크를 사용하는 가상 시스템을 중지하여 직접 **vApp** 네트워크가 현재 사용되지 않도록 해야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.

- 2  을 클릭하여 카드 보기에서 **vApp**을 확인합니다.

- 3 선택한 **vApp**의 카드에서 **세부 정보**를 클릭합니다.

- 4 **네트워크** 탭을 클릭합니다.

- 5 **vApp**이 펜싱되지 않으면 **편집** 버튼을 클릭합니다.

- 6 **vApp 펜싱** 옵션을 설정하고 **확인**을 클릭합니다.

결과

가상 시스템의 IP 주소와 MAC 주소가 격리됩니다. 서로 다른 vApp에 있는 동일한 가상 시스템의 전원을 충돌 없이 켤 수 있습니다.

vApp에 네트워크 추가

vApp에 네트워크를 추가하여 해당 네트워크를 vApp의 가상 시스템에서 사용할 수 있도록 할 수 있습니다. vApp에 vApp 네트워크 또는 조직 가상 데이터 센터 네트워크를 추가할 수 있습니다.


연결은 직접 연결이거나 펜싱된 연결일 수 있습니다. 펜싱을 사용하면 가상 시스템의 MAC 및 IP 주소를 격리함으로써 서로 다른 vApp에 있는 동일한 가상 시스템의 전원을 충돌 없이 켤 수 있습니다.

펜싱을 사용하도록 설정되고 vApp의 전원이 켜지면, 격리된 네트워크가 조직 가상 데이터 센터 네트워크 풀에서 생성됩니다. Edge 게이트웨이가 생성되어 격리된 네트워크와 조직 가상 데이터 센터 네트워크에 연결됩니다. 가상 시스템으로 들어오고 가상 시스템에서 나가는 트래픽은 NAT 및 프록시 AR을 사용하여 IP 주소를 변환하는 Edge 게이트웨이를 통과합니다. 이를 통해 라우터가 동일한 IP 공간을 사용하여 두 네트워크 간에 트래픽을 전달할 수 있습니다.

사전 요구 사항

조직 가상 데이터 센터 네트워크를 추가하려면 관리자가 그러한 네트워크를 생성해두어야 합니다.

절차

- 1 가상 데이터 센터 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 vApp을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 선택된 vApp의 카드에서 작업을 클릭하고 네트워크 추가를 선택합니다.
- 4 추가할 네트워크 유형을 선택합니다.

옵션	작업
조직 VDC 네트워크	사용 가능한 네트워크의 목록에서 조직 가상 데이터 센터 네트워크를 선택합니다.
vApp 네트워크	<ul style="list-style-type: none"> a 네트워크 이름과 설명(선택 사항)을 입력합니다. b 네트워크 게이트웨이 CIDR를 입력합니다. c (선택 사항) 기본 및 보조 DNS와 DNS 접미사를 입력합니다. d (선택 사항) 게스트 VLAN을 허용할지 선택합니다. e (선택 사항) IP범위 등의 정적 IP 풀 설정을 입력합니다. f (선택 사항) 조직 가상 데이터 센터 네트워크에 연결하려면 조직 VDC 네트워크에 연결 옵션을 설정하고 목록에서 네트워크를 선택합니다.

- 5 추가를 클릭합니다.

결과

네트워크가 vApp에 추가됩니다.

다음에 수행할 작업

vApp의 가상 시스템을 네트워크에 연결합니다.

vApp 네트워크에 대한 네트워크 서비스 구성

일부 vApp 네트워크를 만들기 위한 DHCP, 방화벽, NAT(네트워크 주소 변환), VPN, 정적 라우팅 등의 네트워크 서비스를 구성할 수 있습니다.

사용할 수 있는 네트워크 서비스는 vApp 네트워크의 유형에 따라 달라집니다.

표 3-1. 네트워크 유형별 사용 가능한 네트워크 서비스

vApp 네트워크 유형	DHCP	방화벽	NAT	정적 라우팅
직접				
라우팅됨	X	X	X	X
격리됨	X			


참고 NSX Data Center for vSphere에서 지원하는 조직 VDC는 라우팅된 vApp 네트워크, 격리된 vApp 네트워크 및 직접 vApp 네트워크를 지원합니다.

NSX-T Data Center에서 지원하는 조직 VDC는 격리된 vApp 네트워크 및 직접 vApp 네트워크를 지원합니다.

일반 네트워크 세부 정보 보기 및 편집

네트워크 이름 및 설명 같은 일반 vApp 네트워크 세부 정보를 보고 편집할 수 있습니다.


절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭합니다.
- 4 **네트워크** 탭에서 네트워크를 클릭하여 네트워크 세부 정보를 봅니다.
- 5 **일반** 탭에서 네트워크 정보를 검토합니다.
- 6 **편집**을 클릭합니다.
- 7 vApp 네트워크 이름 및 설명을 편집합니다.
- 8 **저장**을 클릭합니다.

vApp 네트워크의 정적 IP 풀 설정 편집

정적 IP 주소 풀에서 정적 IP 주소를 가져와 vApp의 가상 시스템에 제공하도록 vApp 네트워크를 구성할 수 있습니다.


절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭합니다.
- 4 **네트워크** 탭에서 네트워크를 클릭하여 네트워크 세부 정보를 봅니다.
- 5 **IP 관리** 탭에서 **정적 풀**을 클릭합니다.
- 6 **편집**을 클릭합니다.
- 7 IP 범위를 입력하고 **추가**를 클릭합니다.
- 8 **저장**을 클릭합니다.

vApp 네트워크의 DNS 설정 편집

vApp 네트워크를 만든 후에는 언제든지 DNS 설정을 보고 편집할 수 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭합니다.
- 4 **네트워크** 탭에서 네트워크를 클릭하여 네트워크 세부 정보를 봅니다.
- 5 **IP 관리** 탭에서 **DNS**를 클릭합니다.
DNS 설정이 표시됩니다.
- 6 **편집**을 클릭합니다.
- 7 기본 및 보조 DNS와 DNS 접미사를 편집합니다.
- 8 **저장**을 클릭합니다.

vApp 네트워크의 DHCP 구성

일부 vApp 네트워크에서 vApp의 가상 시스템에 DHCP 서비스를 제공하도록 구성할 수 있습니다.

vApp 네트워크에 대해 DHCP를 사용하도록 설정하는 경우 vApp에 있는 가상 시스템의 NIC를 해당 네트워크에 연결하고, DHCP를 해당 NIC의 IP 모드로 선택합니다. 가상 시스템의 전원을 켜면 VMware Cloud Director가 가상 시스템에 DHCP IP 주소를 할당합니다.

사전 요구 사항

- vApp 네트워크가 라우팅되었는지 또는 격리되었는지 확인합니다.

- NSX Data Center for vSphere에서 지원되는 조직 가상 데이터 센터에 vApp이 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.

- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.

- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭합니다.

- 4 **네트워크** 탭에서 네트워크를 클릭하여 네트워크 세부 정보를 봅니다.

- 5 **IP 관리** 탭에서 **DHCP**를 클릭합니다.

DHCP 상태가 표시됩니다.

- 6 **편집**을 클릭합니다.

- 7 **사용**을 클릭합니다.

- 8 **IP 풀** 텍스트 상자에 IP 주소 범위를 입력합니다.

VMware Cloud Director는 이러한 주소를 사용하여 DHCP 요청을 충족합니다. DHCP IP 주소 범위는 vApp 네트워크의 정적 IP 풀과 겹칠 수 없습니다.

- 9 기본 및 최대 임대 기간을 초 단위로 설정합니다.


- 10 **저장**을 클릭합니다.

vApp 네트워크에 대한 IP 할당 표시

vApp의 네트워크에 대한 IP 할당을 검토할 수 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.

- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.

- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭합니다.

- 4 **네트워크** 탭에서 네트워크를 클릭하여 네트워크 세부 정보를 봅니다.

- 5 **IP 관리** 탭에서 **IP 할당**을 클릭합니다.

할당된 IP 주소가 표시됩니다.

vApp 네트워크에 대해 정적 라우팅 구성


정적 라우팅 서비스를 제공하도록 특정 vApp 네트워크를 구성하여 서로 다른 vApp 네트워크의 가상 시스템이 통신하도록 허용할 수 있습니다.

생성한 모든 정적 경로는 자동으로 활성화됩니다.

사전 요구 사항

라우팅되는 vApp 네트워크가 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭합니다.
- 4 **네트워크** 탭에서 네트워크를 클릭하여 네트워크 세부 정보를 봅니다.
- 5 **라우팅** 탭에서 **편집**을 클릭합니다.

네트워크에 대해 정적 라우팅을 활성화하거나 비활성화할 수 있습니다.

vApp 네트워크에 대해 정적 라우팅 추가

동일한 조직 가상 데이터 센터 네트워크에 라우팅된 두 vApp 네트워크 사이에 정적 경로를 추가할 수 있습니다. 정적 경로는 네트워크 사이의 트래픽을 가능하게 합니다.


펜싱된 vApp에 또는 겹치는 네트워크 간에는 정적 경로를 추가할 수 없습니다. vApp 네트워크에 정적 경로를 추가한 후에는 해당 정적 경로에서 트래픽을 허용하도록 네트워크 방화벽 규칙을 구성합니다. 정적 경로가 있는 vApp의 경우, 할당된 IP 주소를 vApp 또는 관련 네트워크가 삭제될 때까지 사용하도록 선택합니다.

정적 경로는 해당 경로가 포함된 vApp가 실행 중인 경우에만 작동합니다. vApp에 정적 경로가 포함되어 있는 경우 vApp의 상위 네트워크를 변경하거나, vApp를 삭제하거나, vApp 네트워크를 삭제하면 정적 경로가 작동하지 않으며 정적 경로를 수동으로 제거해야 합니다.

사전 요구 사항

- 두 vApp 네트워크가 동일한 조직 가상 데이터 센터 네트워크에 라우팅되어 있어야 합니다.
- vApp 네트워크가 한 번 이상 시작되었던 vApp에 있어야 합니다.
- 두 vApp 네트워크 모두에서 정적 라우팅을 사용하도록 설정되어 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭합니다.
- 4 **네트워크** 탭에서 네트워크를 클릭하여 네트워크 세부 정보를 봅니다.

5 라우팅 탭의 [정적 라우팅] 에서 **추가**를 클릭합니다.

할당된 IP 주소가 표시됩니다.

6 정적 경로의 이름을 입력합니다.**7** CIDR 형식으로 네트워크 주소를 입력합니다.

네트워크 주소는 정적 경로를 추가할 대상 vApp 네트워크의 주소입니다.

8 다음 홉 IP 주소를 입력합니다.

다음 홉 IP 주소는 해당 vApp 네트워크 라우터의 외부 IP 주소입니다.

9 저장을 클릭합니다.**10** 두 번째 vApp 네트워크에 대해 동일한 절차를 반복합니다.**예제: 정적 라우팅 예**

vApp 네트워크 1과 vApp 네트워크 2는 모두 공유 조직 네트워크로 라우팅됩니다. vApp 네트워크 간의 트래픽이 허용되도록 각 vApp 네트워크에 정적 경로를 만들 수 있습니다. vApp 네트워크에 대한 정보를 사용하여 정적 경로를 만들 수 있습니다.

표 3-2. 네트워크 정보

네트워크 이름	네트워크 규격	라우터 외부 IP 주소
vApp 네트워크 1	192.168.1.0/24	192.168.0.100
vApp 네트워크 2	192.168.2.0/24	192.168.0.101
공유 조직 네트워크	192.168.0.0/24	NA

vApp 네트워크 1에서 vApp 네트워크 2에 대한 정적 경로를 만들고, vApp 네트워크 2에서 vApp 네트워크 1에 대한 정적 경로를 만듭니다.

표 3-3. 정적 라우팅 설정

vApp 네트워크	경로 이름	네트워크	다음 홉 IP 주소
vApp 네트워크 1	tovapp2	192.168.2.0/24	192.168.0.101
vApp 네트워크 2	tovapp1	192.168.1.0/24	192.168.0.100

vApp 네트워크에 포트 전달 규칙 추가

NAT 매핑 규칙을 추가하여 특정 vApp 네트워크에서 포트 전달을 제공하도록 구성할 수 있습니다.

포트 전달은 vApp 네트워크의 가상 시스템에서 실행되는 서비스에 대한 외부 액세스를 제공합니다.

포트 전달을 구성하면 VMware Cloud Director는 외부 포트를 인바운드 트래픽 전용 가상 시스템에서 실행되는 서비스에 매핑합니다.


포트 전달 규칙을 vApp 네트워크에 추가하면 NAT 매핑 규칙 목록의 맨 아래에 나타납니다. 포트 전달 규칙의 적용 순서를 설정하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

사전 요구 사항

- vApp 네트워크가 라우팅되고 있는지 확인합니다.
- vApp 네트워크의 방화벽이 활성화되어 있는지 확인합니다. 방화벽을 비활성화하면 NAT 매핑 규칙이 더 이상 vApp 네트워크에 적용되지 않습니다.

절차

1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.

2  을 클릭하여 카드 보기에서 vApp을 확인합니다.

3 선택한 vApp의 카드에서 **세부 정보**를 클릭합니다.

4 **네트워크** 탭에서 네트워크를 클릭하여 네트워크 세부 정보를 봅니다.

5 **서비스**를 클릭하고 **편집**을 클릭합니다.

6 NAT를 사용하도록 설정하려면 **NAT** 옵션을 설정합니다.

7 **NAT 유형** 드롭다운 메뉴에서 **포트 전달**을 선택하고 **추가**를 클릭합니다.

8 (선택 사항) IP 가장을 사용하도록 설정하려면 확인란을 선택합니다.

9 포트 전달 규칙을 구성합니다.

- a 외부 포트를 선택합니다.
- b 전달 대상 포트를 선택합니다.
- c 가상 시스템 인터페이스를 선택합니다.
- d 전달할 트래픽 유형에 대한 프로토콜을 선택합니다.

10 **저장**을 클릭합니다.

다음에 수행할 작업

필요한 경우 **위로 이동** 또는 **아래로 이동** 버튼을 사용하여 포트 전달 규칙을 재정렬합니다.

vApp 네트워크에 IP 변환 규칙 추가

NAT 매핑 규칙을 추가하여 특정 vApp 네트워크에서 IP 변환을 제공하도록 구성할 수 있습니다.


네트워크에 대한 IP 변환 규칙을 만들면 vCloud Director에서는 네트워크의 포트 그룹과 연결된 Edge 게이트웨이에 DNAT 및 SNAT 규칙을 추가합니다. DNAT 규칙은 외부 IP 주소를 인바운드 트래픽에 대한 내부 IP 주소로 변환합니다. SNAT 규칙은 내부 IP 주소를 아웃바운드 트래픽에 대한 외부 IP 주소로 변환합니다.

사전 요구 사항

- vApp 네트워크가 라우팅되고 있는지 확인합니다.

- vApp 네트워크의 방화벽이 활성화되어 있는지 확인합니다. 방화벽을 비활성화하면 NAT 매핑 규칙이 더 이상 vApp 네트워크에 적용되지 않습니다.

절차

- 1 가상 데이터 센터 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 vApp을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭합니다.
- 4 **네트워크** 탭에서 네트워크를 클릭하여 네트워크 세부 정보를 봅니다.
- 5 서비스를 클릭하고 **편집**을 클릭합니다.
- 6 NAT를 사용하도록 설정하려면 NAT 옵션을 설정합니다.
- 7 **NAT 유형** 드롭다운 메뉴에서 **IP 변환**을 선택하고 **추가**를 클릭합니다.
- 8 가상 시스템 인터페이스를 선택하고 **보존**을 클릭합니다.
- 9 매핑 모드를 선택합니다.
- 10 수동 매핑 모드를 선택한 경우 외부 IP 주소를 입력합니다.
- 11 **저장**을 클릭합니다.

다음에 수행할 작업

필요한 경우 **위로 이동** 또는 **아래로 이동** 버튼을 사용하여 IP 변환 규칙을 재정렬합니다.


vApp 네트워크 삭제

vApp의 네트워크가 더 이상 필요하지 않는 경우 네트워크를 삭제할 수 있습니다.

사전 요구 사항

vApp가 중지되어 있고 vApp의 가상 시스템이 네트워크에 연결되어 있지 않아야 합니다.

절차

- 1 가상 데이터 센터 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 vApp을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 선택한 vApp의 카드에서 **세부 정보**를 클릭합니다.
- 4 **네트워크** 탭에서 삭제할 네트워크를 선택하고 **삭제**를 클릭한 후 삭제를 확인합니다.

스냅샷 작업

스냅샷을 만들면 vApp에 포함된 가상 시스템의 상태와 데이터가 특정 시점에서 보존됩니다. 스냅샷은 장기간 사용하거나 vApp의 백업을 대신할 용도로 설계되지 않았습니다.

vApp의 가상 시스템을 업그레이드하는 경우 스냅샷을 사용할 수 있습니다. 예를 들어 가상 시스템을 업그레이드하기 전에 스냅샷을 만들어 업그레이드 전의 시점을 보존합니다. 이렇게 하려면 업그레이드 전에 스냅샷을 저장한 다음 업그레이드를 수행합니다. 업그레이드 중에 문제가 발생하지 않으면 스냅샷을 제거하도록 선택하고 업그레이드 중에 수행된 변경 내용을 커밋할 수 있습니다. 그러나 문제가 발생한 경우 스냅샷을 되돌려 업그레이드 전에 저장된 vApp 상태로 돌아갈 수 있습니다.

vApp의 스냅샷 만들기


vApp의 스냅샷을 만들면 vApp의 모든 가상 시스템에 대한 스냅샷이 만들어집니다. 스냅샷을 만든 후에는 vApp의 모든 가상 시스템을 스냅샷으로 되돌리거나 스냅샷이 필요하지 않은 경우에는 제거할 수 있습니다.

vApp 스냅샷에는 몇 가지 제한 사항이 있습니다.

- vApp 스냅샷에는 NIC 구성이 캡처되지 않습니다.
- vApp의 가상 시스템이 명명된 디스크에 연결되어 있으면 vApp 스냅샷을 만들 수 없습니다.

절차

- 1 가상 데이터 센터 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 vApp을 선택합니다.

- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.

- 3 스냅샷을 만들려는 vApp의 **작업** 메뉴에서 **스냅샷 만들기**를 선택합니다.

vApp의 스냅샷을 만들면 기존 스냅샷이 있는 경우 대체됩니다.

- 4 (선택 사항) vApp의 메모리에 대한 스냅샷을 만들지 여부를 선택합니다.

vApp 메모리 상태를 캡처할 경우 스냅샷에는 vApp과 vApp에 있는 가상 시스템의 라이브 상태가 보관됩니다. 메모리 스냅샷은 정확한 시간에 스냅샷을 만듭니다. 예를 들어 현재 작동 중인 소프트웨어를 업그레이드하기 전에 메모리 스냅샷을 만들 수 있습니다. 메모리 스냅샷을 만들면 업그레이드가 예상대로 완료되지 않거나 소프트웨어가 원하는 대로 작동하지 않는 경우 가상 시스템을 이전 상태로 되돌릴 수 있습니다.

메모리 상태를 캡처하는 경우 vApp의 파일을 중지할 필요가 없습니다. 메모리 상태를 캡처하지 않을 경우 스냅샷에는 vApp의 라이브 상태가 저장되지 않으며, 사용자가 디스크를 중지하지 않는 한 디스크는 충돌 일치 상태가 됩니다.

5 (선택 사항) 게스트 파일 시스템을 중지할지 선택합니다.

이 작업을 수행하려면 vApp의 가상 시스템에 VMware Tools가 설치되어 있어야 합니다. 가상 시스템을 중지하면 VMware Tools에서는 가상 시스템의 파일 시스템을 중지합니다. 중지 작업은 스냅샷 디스크가 게스트 파일 시스템의 일관된 상태를 나타내도록 합니다. 중지된 스냅샷은 자동 또는 정기 백업에 적절합니다. 예를 들어 가상 시스템의 작업을 알지 못하는 상황에서 복구할 최신 백업을 여러 개 확보하려면 파일을 중지하면 됩니다.

대용량 디스크가 있는 vApp은 중지할 수 없습니다.

6 확인을 클릭합니다.

결과

vApp의 스냅샷이 만들어집니다.

다음에 수행할 작업

vApp의 모든 가상 시스템을 최신 스냅샷으로 되돌릴 수 있습니다.


스냅샷으로 vApp 되돌리기

vApp의 모든 가상 시스템을 vApp 스냅샷을 만들던 시점의 상태로 되돌릴 수 있습니다.

사전 요구 사항

vApp에 기존 스냅샷이 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 되돌리려는 vApp의 **작업** 메뉴에서 **스냅샷으로 되돌리기**를 선택합니다.
- 4 **확인**을 클릭합니다.

결과

vApp의 모든 가상 시스템이 스냅샷 상태로 되돌려집니다.

vApp의 스냅샷 제거


vApp의 스냅샷을 제거할 수 있습니다.

vApp 스냅샷을 제거하면 vApp 스냅샷의 가상 시스템 상태가 삭제되며 해당 상태로 다시 돌아갈 수 없습니다. 스냅샷을 제거해도 vApp의 현재 상태는 영향을 받지 않습니다.

사전 요구 사항

vApp의 스냅샷을 만들었습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 스냅샷을 제거하려는 vApp의 **작업** 메뉴에서 **스냅샷 제거**를 선택합니다.
- 4 **확인**을 클릭합니다.

결과

스냅샷이 제거됩니다.

여러 vApp의 스냅샷 생성

여러 vApp의 스냅샷을 생성하면 vApp의 모든 가상 시스템에 대한 스냅샷이 생성됩니다. 스냅샷을 생성한 후에는 vApp의 모든 가상 시스템을 스냅샷으로 되돌리거나 스냅샷이 필요하지 않은 경우에는 스냅샷을 제거할 수 있습니다.

vApp 스냅샷에는 몇 가지 제한 사항이 있습니다.

- vApp 스냅샷에는 NIC 구성이 캡처되지 않습니다.
- vApp의 가상 시스템이 명명된 디스크에 연결되어 있으면 vApp 스냅샷을 생성할 수 없습니다.
- 여러 vApp의 스냅샷을 생성하면 vApp의 메모리 스냅샷이 생성되지 않고 vApp의 게스트 파일 시스템이 중지되지 않습니다. vApp의 메모리 스냅샷을 생성하거나 게스트 파일 시스템을 중지하려는 경우 각 vApp에 대해 개별 스냅샷을 생성해야 합니다. **vApp의 스냅샷 만들기**의 내용을 참조하십시오.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 **다중 선택** 옵션을 설정합니다.
- 3 스냅샷을 생성할 vApp을 선택합니다.
- 4 **작업** 메뉴에서 **스냅샷 만들기**를 선택하고 **확인**을 클릭하여 확인합니다.

다음에 수행할 작업

- vApp의 모든 가상 시스템을 최신 스냅샷으로 되돌릴 수 있습니다. **여러 vApp을 스냅샷으로 되돌리기**의 내용을 참조하십시오.
- vApp의 스냅샷을 제거할 수 있습니다. **여러 vApp의 스냅샷 제거**의 내용을 참조하십시오.

여러 vApp의 스냅샷 제거

여러 vApp의 스냅샷이 필요하지 않은 경우 이를 동시에 제거할 수 있습니다.

vApp 스냅샷을 제거하면 vApp 스냅샷의 가상 시스템 상태가 삭제되며 해당 상태로 다시 돌아갈 수 없습니다. 스냅샷을 제거해도 vApp의 현재 상태는 영향을 받지 않습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 **다중 선택** 옵션을 설정합니다.
- 3 제거할 스냅샷이 있는 vApp을 선택합니다.
- 4 **작업** 메뉴에서 **스냅샷 제거**를 선택합니다.

여러 vApp을 스냅샷으로 되돌리기

여러 vApp의 모든 가상 시스템을 vApp 스냅샷을 생성했던 시점의 상태로 되돌릴 수 있습니다.

사전 요구 사항

되돌리려는 vApp에 기존 스냅샷이 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 **다중 선택** 옵션을 설정합니다.
- 3 최신의 스냅샷으로 되돌리려는 vApp을 선택합니다.
- 4 **작업** 메뉴에서 **스냅샷으로 되돌리기**를 선택합니다.
- 5 **확인**을 클릭하여 확인합니다.


vApp의 소유자 변경

예를 들어 vApp 소유자가 퇴사하거나 회사 내에서 역할이 변경되면 vApp의 소유자를 변경할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 소유자를 변경하려는 vApp의 **작업** 메뉴에서 **소유자 변경**을 선택합니다.

4 목록에서 사용자를 선택합니다.

5 **확인**을 클릭합니다.

결과

vApp의 소유자가 변경되었습니다.


다른 가상 데이터 센터로 vApp 이동

vApp을 다른 가상 데이터 센터로 이동할 경우 해당 vApp은 소스 가상 데이터 센터에서 제거됩니다.

사전 요구 사항

- **vApp 작성자** 이상의 권한이 있어야 합니다.
- vApp의 전원이 꺼져 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 이동하려는 vApp의 **작업** 메뉴에서 **이동**을 선택합니다.
- 4 vApp을 이동할 대상 가상 데이터 센터를 선택하고 **확인**을 클릭합니다.
- 5 (선택 사항) 스토리지 정책을 선택합니다.
- 6 **확인**을 클릭합니다.

결과

vApp이 소스 데이터 센터에서 제거되고 대상 데이터 센터로 이동됩니다.

다른 가상 데이터 센터에 중지된 vApp 복사


vApp을 다른 가상 데이터 센터에 복사해도 원래 vApp은 소스 가상 데이터 센터에 유지됩니다.

사전 요구 사항

- **vApp 작성자** 이상의 권한이 있어야 합니다.
- vApp의 전원이 꺼져 있습니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.

- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 복사하려는 vApp의 **작업** 메뉴에서 **복사**를 선택합니다.
- 4 이름과 설명을 입력합니다.
- 5 vApp의 복사본을 만들려는 가상 데이터 센터를 선택합니다.
- 6 (선택 사항) 스토리지 정책을 선택합니다.
- 7 **확인**을 클릭합니다.

결과

vApp이 제공한 이름과 설명이 적용되어 지정된 가상 데이터 센터에 복사됩니다.

전원이 켜진 vApp 복사


기존 vApp을 기반으로 vApp을 만들려면 vApp을 복사하고 복사본을 필요에 맞게 변경하면 됩니다. vApp을 복사하기 전에 vApp의 가상 시스템 전원을 끄지 않아도 됩니다. 실행 중인 가상 시스템의 메모리 상태는 복사된 vApp에 보존됩니다.

사전 요구 사항

다음과 같은 조건을 충족하는지 확인합니다.

- **vApp 사용자** 이상의 권한이 있어야 합니다.
- 조직 가상 데이터 센터는 vCenter Server 5.5 이상에서 백업됩니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 복사하려는 vApp의 **작업** 메뉴에서 **복사**를 선택합니다.
- 4 이름과 설명을 입력합니다.
- 5 vApp의 복사본을 만들려는 가상 데이터 센터를 선택합니다.
- 6 (선택 사항) 스토리지 정책을 선택합니다.
- 7 **확인**을 클릭합니다.

결과

vApp의 복사본이 만들어지고 vApp 복사본이 일시 중단된 상태가 됩니다. 복사된 vApp이 네트워크 펜싱에 대해 사용되도록 설정됩니다.

다음에 수행할 작업

새 vApp의 네트워크 속성을 수정하거나 vApp의 전원을 켭니다.


vApp에 가상 시스템 추가

vApp에 가상 시스템을 추가할 수 있습니다.

사전 요구 사항

공개 카탈로그의 가상 시스템에 액세스하려면 **조직 관리자** 또는 **vApp 작성자**여야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 3 가상 시스템을 추가할 vApp의 **작업** 메뉴에서 **VM 추가**를 선택합니다.
vApp에 연결된 가상 시스템 목록이 **VM 추가** 창에 표시됩니다.
- 4 새 가상 시스템을 만들고 이를 자동으로 vApp에 연결하려면 **가상 시스템 추가**를 클릭합니다.
- 5 가상 시스템에 대한 이름과 컴퓨터 이름을 입력합니다.

중요 컴퓨터 이름에는 영숫자와 하이픈만 포함될 수 있습니다. 컴퓨터 이름은 숫자로만 구성할 수 없으며 공백을 포함할 수 없습니다.

- 6 (선택 사항) 의미 있는 설명을 입력합니다.
- 7 가상 시스템이 생성되면 바로 가상 시스템의 전원을 켜지 선택합니다.

8 가상 시스템의 배포 방법을 선택합니다.

옵션	작업
새로 만들기	<p>사용자 지정 설정으로 새 가상 시스템을 배포합니다.</p> <ul style="list-style-type: none"> a 운영 체제 제품군과 운영 체제를 선택합니다. b (선택 사항) 부팅 이미지를 선택합니다. c 계산 정책을 선택합니다. d 가상 시스템의 크기를 선택하거나 사용자 지정 크기 조정 옵션을 클릭하고 계산, 메모리 및 스토리지 설정을 수동으로 입력합니다. <p>미리 정의된 크기 조정 옵션은 [소], [중], [대]입니다.</p> <ul style="list-style-type: none"> e 스토리지 정책 및 크기(GB)와 같은 가상 시스템의 스토리지 설정을 지정합니다. f 가상 시스템에 대한 네트워크 설정(예: 네트워크, IP 모드, IP 주소, 기본 NIC)을 지정합니다.
템플릿에서	<p>템플릿 카탈로그에서 선택한 템플릿에서 가상 시스템을 배포합니다.</p> <ul style="list-style-type: none"> a 카탈로그에서 가상 시스템 템플릿을 선택합니다. b (선택 사항) 사용자 지정 스토리지 정책을 사용하도록 선택하고 사용할 사용자 지정 스토리지 정책에서 정책을 선택합니다. c 사용 가능한 최종 사용자 라이선스 계약이 있다면 계약 내용을 검토한 후 수락합니다.

9 확인을 클릭하여 가상 시스템을 생성합니다.

10 추가를 클릭하여 가상 시스템을 vApp에 추가합니다.

vApp을 vApp 템플릿으로 카탈로그에 저장


vApp을 카탈로그에 추가하여 특정 vApp을 vApp 템플릿으로 변환할 수 있습니다.

VMware Cloud Director 10.2.2부터는 vApp을 카탈로그에 추가하면 vApp 템플릿에는 소스 vApp의 배치 및 크기 조정 정책이 수정 불가능 태그로 포함됩니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **vApp 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- 조직에 사용 가능한 공간이 있는 가상 데이터 센터와 카탈로그가 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2  을 클릭하여 카드 보기에서 vApp을 확인합니다.

- 3 카탈로그에 추가할 vApp의 **작업** 메뉴에서 **카탈로그에 추가**를 선택합니다.

참고 vApp에 실행 중인 가상 시스템이 있는 경우에도 vApp을 카탈로그에 추가할 수 있습니다. 그러나 실행 중인 vApp을 선택하면 vApp이 vApp 템플릿으로 카탈로그에 추가되고 모든 가상 시스템이 일시 중단된 상태가 됩니다.

- 4 **카탈로그** 드롭다운 메뉴에서 대상 카탈로그를 선택합니다.
- 5 vApp 템플릿의 이름과 설명(선택 사항)을 입력합니다.
- 6 (선택 사항) 기존의 vApp 템플릿을 새 카탈로그 항목으로 덮어쓰려면 **카탈로그 항목 덮어쓰기**를 선택하고 덮어쓸 카탈로그 항목을 선택합니다.

예를 들어 새 vApp 버전을 카탈로그에 업로드할 때 이전 버전을 덮어쓸 수 있습니다.

- 7 템플릿 사용 방법을 지정합니다.

이 설정은 vApp 템플릿을 기반으로 vApp을 만들 때 적용됩니다. 이 템플릿에서 개별 가상 시스템을 사용하여 vApp을 구축하는 경우에는 설정이 무시됩니다.

옵션	설명
동일한 복사본 만들기	vApp 템플릿으로 vApp을 만들 때 vApp의 동일한 복사본을 만들려면 선택합니다.
VM 설정 사용자 지정	vApp 템플릿으로 vApp을 만들 때 가상 시스템 설정의 사용자 지정을 사용하도록 설정하려면 선택합니다.

- 8 vApp 템플릿 생성을 완료하려면 **확인**을 클릭합니다.

결과

vApp 템플릿이 지정된 카탈로그에 나타납니다.


OVF 패키지로 vApp 다운로드

vApp을 OVF 패키지 또는 OVA(동일한 OVF 파일 패키지의 단일 파일 배포)로 다운로드할 수 있습니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **vApp 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- vApp가 전원이 꺼져 있고 배포 취소되어 있는지 확인합니다.

절차

- 가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
-  을 클릭하여 카드 보기에서 vApp을 확인합니다.
- 다운로드할 vApp의 **작업** 메뉴에서 **다운로드**를 선택합니다.

- 4 vApp을 다운로드할 형식을 선택합니다.
- 5 (선택 사항) vApp에 상주하는 가상 시스템의 UUID 및 MAC 주소를 다운로드되는 OVF 패키지에 포함하려면 **ID 정보 보존**을 선택합니다.

이 옵션은 패키지 이동을 제한하므로 필요한 경우에만 사용해야 합니다.

- 6 **확인**을 클릭하여 선택 사항을 확인하고 다운로드를 시작합니다.

결과

기본적으로 패키지는 브라우저의 Downloads 폴더에 다운로드됩니다.

vApp 임대 갱신

vApp 리스가 만료되었거나 만료 예정인 경우 갱신할 수 있습니다.

사전 요구 사항

미리 정의된 역할 **vApp 사용자** 또는 이와 동등한 권한 집합이 할당되어 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 갱신할 vApp을 선택합니다.
- 3 **작업** 메뉴에서 **임대 갱신**을 선택합니다.
- 4 vApp의 런타임 임대를 갱신합니다.
 - a **런타임 임대** 확인란을 선택합니다.
 - b 드롭다운 메뉴에서 런타임 임대에 대한 값을 선택합니다.
 시간 또는 일 단위로 값을 선택하거나 임대를 **만료 안 함**으로 설정할 수 있습니다. **시스템 관리자**는 선택할 수 있는 최대 길이를 제한할 수 있습니다.
- 5 vApp의 스토리지 임대를 갱신합니다.
 - a **스토리지 임대** 확인란을 선택합니다.
 - b 드롭다운 메뉴에서 스토리지 임대에 대한 값을 선택합니다.
 시간 또는 일 단위로 값을 선택하거나 임대를 **만료 안 함**으로 설정할 수 있습니다. **시스템 관리자**는 선택할 수 있는 최대 길이를 제한할 수 있습니다.

vApp 삭제

조직에서 vApp를 삭제하여 제거할 수 있습니다.

사전 요구 사항

vApp가 중지되어 있어야 합니다.

vApp 작성자 이상의 권한이 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 삭제할 vApp을 선택합니다.
- 3 **작업** 메뉴에서 **삭제**를 선택합니다.
- 4 **확인**을 클릭합니다.

결과

vApp이 삭제됩니다.

여러 vApp 삭제

조직에서 여러 vApp을 제거하기 위해 동시에 삭제할 수 있습니다.

사전 요구 사항

- vApp이 중지되었는지 확인합니다.
- **vApp 작성자** 이상의 권한이 있는지 확인합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **vApp**을 선택합니다.
- 2 **다중 선택** 옵션을 설정합니다.
- 3 삭제할 vApp을 선택합니다.
- 4 **작업** 메뉴에서 **삭제**를 선택합니다.
- 5 **삭제**를 클릭하여 확인합니다.

Kubernetes 클러스터 작업

4

기존 조직 VDC 정책에서 다양한 노드 크기의 Kubernetes 클러스터를 생성할 수 있습니다.

Kubernetes Container Clusters는 VMware Cloud Director용 Container Service Extension 플러그인입니다. VMware Cloud Director Tenant Portal에서 Kubernetes Container Clusters 플러그인을 사용하여 네이티브 및 TKGI(VMware Tanzu Kubernetes Grid Integrated Edition) 클러스터가 있는 클러스터를 배포할 수 있습니다. Kubernetes Container Clusters 플러그인 없이 Tanzu Kubernetes 클러스터를 만들 수 있습니다.

vSphere 클러스터에서 사용하도록 설정할 경우 VMware vSphere® with VMware Tanzu™는 전용 리소스 풀에서 업스트림 Kubernetes 클러스터를 생성하는 기능을 제공합니다. 자세한 내용은 vSphere 설명서에서 "vSphere with Kubernetes 구성 및 관리" 가이드를 참조하십시오.

서비스 제공자가 제공자 VDC Kubernetes 정책을 생성하고 이 정책을 조직 VDC에 게시하면 조직 VDC Kubernetes 정책이 생성됩니다. Kubernetes Container Clusters 플러그인을 사용하여 조직 VDC Kubernetes 정책 중 하나를 적용하여 Tanzu Kubernetes 클러스터를 생성할 수 있습니다.

Kubernetes 런타임 옵션

- Tanzu Kubernetes 클러스터 - vSphere Kubernetes 런타임 옵션을 사용하여 vSphere with VMware Tanzu 관리형 Tanzu Kubernetes 클러스터를 생성할 수 있습니다. 이 옵션은 더 많은 기능을 제공하지만 비용이 더 높을 수 있습니다. 자세한 내용은 vSphere 설명서에서 "vSphere with Kubernetes 구성 및 관리" 가이드를 참조하십시오.
- 네이티브 클러스터 - Kubernetes Container Clusters 플러그인은 네이티브 Kubernetes 런타임으로 클러스터를 관리합니다. 이러한 클러스터는 단일 제어부 노드를 사용하며 고가용성 기능이 적고, 제공되는 영구 볼륨 선택 항목이 적으며 네트워킹 자동화를 제공하지 않습니다. 하지만 저렴한 비용으로 제공될 수 있습니다.
- TKGI 클러스터 - VMware Tanzu Kubernetes Grid Integrated Edition은 멀티 클라우드 기업과 서비스 제공자를 위한 Kubernetes를 운용하기 위해 특별히 구축된 컨테이너 솔루션입니다. 여기에 포함된 기능에는 Kubernetes 클러스터를 위한 고가용성, 자동 크기 조정, 상태 확인은 물론 자동 복구 및 롤링 업그레이드 등이 있습니다. TKGI 클러스터에 대한 자세한 내용은 "VMware Tanzu Kubernetes Grid Integrated Edition" 설명서를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [조직 VDC Kubernetes 정책 추가](#)

- 조직 VDC Kubernetes 정책 편집
- Tanzu Kubernetes 클러스터 만들기
- 네이티브 Kubernetes 클러스터 만들기
- VMware Tanzu Kubernetes Grid Integrated Edition 클러스터 만들기
- Tanzu Kubernetes 클러스터의 서비스에 대한 외부 액세스 구성

조직 VDC Kubernetes 정책 추가

시스템 관리자 권한이 있으면 제공자 VDC Kubernetes 정책을 사용하여 조직 VDC Kubernetes 정책을 추가할 수 있습니다. 조직 VDC Kubernetes 정책을 사용하여 Tanzu Kubernetes 클러스터를 생성할 수 있습니다.

조직 VDC에 제공자 VDC Kubernetes 정책을 추가하거나 게시할 때 조직 VDC 정책을 생성하여 테넌트에서 제공자 VDC Kubernetes 정책을 사용할 수 있도록 합니다. 테넌트는 사용 가능한 조직 VDC Kubernetes 정책을 사용하여 Tanzu Kubernetes 클러스터를 생성하는 동안 Kubernetes 용량을 활용할 수 있습니다. Kubernetes 정책은 배치, 인프라 품질 및 영구 볼륨 스토리지 클래스를 캡슐화합니다. Kubernetes 정책은 계산 제한이 서로 다를 수 있습니다.

단일 조직 VDC에 여러 조직 VDC Kubernetes 정책을 추가할 수 있습니다. 단일 제공자 VDC Kubernetes 정책을 사용하여 여러 조직 VDC Kubernetes 정책을 생성할 수 있습니다. 조직 VDC Kubernetes 정책을 서비스 품질의 지표로 사용할 수 있습니다. 예를 들어 보장된 시스템 클래스와 빠른 스토리지 클래스를 선택할 수 있는 Gold Kubernetes 정책 또는 사용 시도 시스템 클래스와 느린 스토리지 클래스를 선택할 수 있는 Silver Kubernetes 정책을 게시할 수 있습니다.

사전 요구 사항

- **시스템 관리자** 역할 또는 이와 동등한 권한 집합이 포함된 역할이 있는지 확인합니다. 다른 모든 역할은 조직 VDC Kubernetes 정책을 볼 수만 있습니다.
- 환경에 감독자 클러스터에 의해 지원되는 제공자 VDC가 하나 이상 있는지 확인합니다. 감독자 클러스터에서 지원되는 제공자 VDC는 Service Provider Admin Portal의 **제공자 VDC** 탭에 Kubernetes 아이콘으로 표시됩니다. vSphere with VMware Tanzu의 VMware Cloud Director에 대한 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"에서 [VMware Cloud Director에서 vSphere with Kubernetes 사용](#)을 참조하십시오.
- Flex 조직 VDC에 로그인했는지 확인합니다.
- Tanzu Kubernetes 클러스터에 대한 가상 시스템 클래스 유형을 숙지합니다. vSphere 설명서에서 "vSphere with Kubernetes 구성 및 관리" 가이드를 참조하십시오.

절차

- 1 위쪽 탐색 모음에서 **데이터 센터**를 클릭한 다음, **가상 데이터 센터**를 클릭합니다.
- 2 조직 가상 데이터 센터를 선택합니다.

- 3 왼쪽 패널의 **설정**에서 **Kubernetes 정책**을 선택하고 **추가**를 클릭합니다.

조직 VDC에 게시 마법사가 나타납니다.

- 4 조직 VDC Kubernetes 정책에 대한 테넌트 확인 가능 이름과 설명을 입력하고 **다음**을 클릭합니다.

- 5 사용할 제공자 VDC Kubernetes 정책을 선택하고 **다음**을 클릭합니다.

- 6 이 정책에 따라 생성된 Tanzu Kubernetes 클러스터에 대한 CPU 및 메모리 제한을 선택합니다.

최대 제한은 조직 VDC의 CPU 및 메모리 할당에 따라 다릅니다. 정책을 추가하면 선택한 제한이 테넌트에 대한 최대값으로 작동합니다.

- 7 이 정책에 생성된 Tanzu Kubernetes 클러스터 노드에 대해 CPU와 메모리를 예약할지 여부를 선택하고 **다음**을 클릭합니다.

각 클래스 유형에는 보장됨 및 사용 시도라는 두 가지 버전이 있습니다. 보장된 클래스 버전은 구성된 리소스를 완전히 예약하는 반면 사용 시도 버전에서는 리소스가 오버 커밋될 수 있습니다. 선택 사항에 따라 마법사의 다음 페이지에서 보장된 또는 사용 시도 버전의 VM 클래스 유형 중에 선택할 수 있습니다.

- 전체 CPU 및 메모리 예약을 위해서는 보장된 버전의 VM 클래스 유형에 대해 **예**를 선택합니다.
- CPU 및 메모리 예약이 없는 사용 시도 버전의 VM 클래스 유형에 대해서는 **아니요**를 선택합니다.

- 8 마법사의 **시스템 클래스** 페이지에서 이 정책에 사용할 수 있는 VM 클래스 유형을 하나 이상 선택합니다.

선택한 시스템 클래스는 조직 VDC에 정책을 추가할 때 테넌트가 사용할 수 있는 유일한 클래스 유형입니다.

- 9 하나 이상의 스토리지 정책을 선택합니다.

- 10 선택 사항을 검토하고 **게시**를 클릭합니다.

결과

게시된 정책에 대한 정보가 Kubernetes 정책 목록에 표시됩니다. 게시된 정책은 정책의 지정된 리소스 제한을 사용하여 감독자 클러스터에 감독자 네임스페이스를 생성합니다.

테넌트는 Kubernetes 정책을 사용하여 Tanzu Kubernetes 클러스터를 생성할 수 있습니다. VMware Cloud Director는 이 Kubernetes 정책에 따라 생성된 각 Tanzu Kubernetes 클러스터를 동일한 감독자 네임스페이스에 배치합니다. 정책 리소스 제한은 감독자 네임스페이스에 대한 리소스 제한이 됩니다. 감독자 네임스페이스의 모든 테넌트 생성 Tanzu Kubernetes 클러스터는 이러한 제한 내에서 리소스를 두고 경합합니다.

다음에 수행할 작업

- 조직 VDC Kubernetes 정책을 삭제합니다.
- Service Provider Admin Portal을 사용하여 조직 리소스 할당량을 관리할 수 있습니다. "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"에서 [조직의 리소스 소비에 대한 할당량 관리](#)를 참조하십시오.

- 그룹의 리소스 할당량 관리 또는 사용자의 리소스 할당량 관리

조직 VDC Kubernetes 정책 편집

시스템 관리자 권한이 있으면 조직 VDC Kubernetes 정책을 수정하여 설명과 CPU 및 메모리 제한을 변경할 수 있습니다.

사전 요구 사항

시스템 관리자 역할 또는 이와 동등한 권한 집합이 포함된 역할이 있는지 확인합니다. 다른 모든 역할은 조직 VDC Kubernetes 정책을 볼 수만 있습니다.

절차

- 1 위쪽 탐색 모음에서 **데이터 센터**를 클릭한 다음, **가상 데이터 센터**를 클릭합니다.
- 2 조직 가상 데이터 센터를 선택합니다.
- 3 왼쪽 패널의 **설정** 아래에서 **Kubernetes 정책**을 선택합니다.
- 4 편집할 조직 VDC Kubernetes 정책을 선택하고 **편집**을 클릭합니다.

VDC Kubernetes 정책 편집 마법사가 나타납니다.

- 5 조직 VDC Kubernetes 정책의 설명을 편집하고 **다음**을 클릭합니다.

정책의 이름은 정책을 게시하는 동안 생성된 감독자 네임스페이스에 연결되며 변경할 수 없습니다.

- 6 조직 VDC Kubernetes 정책에 대한 CPU 및 메모리 제한을 편집하고 **다음**을 클릭합니다.

CPU 및 메모리 예약은 편집할 수 없습니다.

- 7 새 정책 세부 정보를 검토하고 **저장**을 클릭합니다.

다음에 수행할 작업

- 조직 VDC Kubernetes 정책을 삭제합니다.
- Service Provider Admin Portal을 사용하여 조직 리소스 할당량을 변경할 수 있습니다. "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"에서 [조직의 리소스 소비에 대한 할당량 관리](#)를 참조하십시오.
- 그룹 및 사용자 할당량을 변경합니다. [그룹의 리소스 할당량 관리](#) 또는 [사용자의 리소스 할당량 관리](#) 항목을 참조하십시오.

Tanzu Kubernetes 클러스터 만들기

Kubernetes Container Clusters 플러그인을 사용하여 Tanzu Kubernetes 클러스터를 만들 수 있습니다.

클러스터 만들기를 위한 다른 Kubernetes 런타임 옵션에 대한 자세한 내용은 [장 4 Kubernetes 클러스터 작업](#) 항목을 참조하십시오.

Container Service Extension CLI를 사용하여 Kubernetes 클러스터를 관리할 수도 있습니다. [Container Service Extension](#) 설명서를 참조하십시오.

VMware Cloud Director는 PodSecurityPolicy 승인 컨트롤러가 사용되도록 설정된 Tanzu Kubernetes 클러스터를 프로비저닝합니다. 워크로드를 배포하려면 포드 보안 정책을 만들어야 합니다. Kubernetes에서 포드 보안 정책의 사용을 구현하는 방법에 대한 자세한 내용은 "vSphere with Kubernetes 구성 및 관리" 가이드에서 "Tanzu Kubernetes 클러스터에서 포드 보안 정책 사용" 항목을 참조하십시오.

사전 요구 사항

- 서비스 제공자가 Kubernetes Container Clusters 플러그인을 조직에 게시했는지 확인합니다. 위쪽 탐색 모음의 **자세히 > Kubernetes Container Clusters**에서 플러그인을 찾을 수 있습니다.
- 조직 VDC에 조직 VDC Kubernetes 정책이 하나 이상 있는지 확인합니다. 조직 VDC Kubernetes 정책을 추가하려면 **조직 VDC Kubernetes 정책** 추가 항목을 참조하십시오.
- 서비스 제공자가 **vmware:tkgcluster Entitlement** 권한 번들을 조직에 게시했고 Tanzu Kubernetes 클러스터를 만들고 수정할 수 있는 **편집: Tanzu Kubernetes 게스트 클러스터** 권한을 부여했는지 확인합니다. 클러스터를 삭제할 수 있으려면 **모든 권한: Tanzu Kubernetes 게스트 클러스터** 권한이 있어야 합니다.
- 서비스 제공자가 액세스 수준에 대한 정보를 사용하여 ACL(Access Control List) 항목을 만들었는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **추가 > Kubernetes Container Clusters**를 선택합니다.
- 2 (선택 사항) TKGI 클러스터 생성을 위해 조직 VDC를 사용하도록 설정한 경우 **Kubernetes Container Clusters** 페이지에서 **vSphere with Tanzu 및 네이티브** 탭을 선택합니다.
- 3 **새로 만들기**를 클릭합니다.
- 4 **vSphere with Tanzu** 런타임 옵션을 선택하고 **다음**을 클릭합니다.
- 5 새 Kubernetes 클러스터의 이름을 입력하고 **다음**을 클릭합니다.
- 6 Tanzu Kubernetes 클러스터를 배포할 조직 VDC를 선택하고 **다음**을 클릭합니다.
- 7 조직 VDC Kubernetes 정책 및 Kubernetes 버전을 선택하고 **다음**을 클릭합니다.

VMware Cloud Director는 조직 VDC 또는 Kubernetes 정책에 연결되지 않은 기본 Kubernetes 버전 집합을 표시합니다. 이러한 버전은 글로벌 설정입니다. 사용 가능한 버전 목록을 변경하려면 셀 관리 도구를 사용하여 `./cell-management-tool manage-config --name wcp.supported.kubernetes.versions -v version_numbers` 명령을 쉘프로 구분된 버전 번호와 함께 실행합니다.

- 8 새 클러스터의 제어부 및 작업자 노드 수를 선택합니다.
- 9 제어부 및 작업자 노드에 대한 시스템 클래스를 선택하고 **다음**을 클릭합니다.
- 10 제어부 및 작업자 노드에 대한 Kubernetes 정책 스토리지 클래스를 선택하고 **다음**을 클릭합니다.

- 11 (선택 사항) VMware Cloud Director 10.2.2 이상의 경우 Kubernetes 서비스에 대한 IP 주소 범위와 Kubernetes 포트에 대한 범위를 지정하고 **다음**을 클릭합니다.

CIDR(Classless Inter-Domain Routing)은 IP 라우팅 및 IP 주소 할당 방법입니다.

옵션	설명
Pods CIDR	Kubernetes 포트에 사용할 IP 주소 범위를 지정합니다. 기본 값은 192.168.0.0/16입니다. 포트 서브넷 크기는 /24보다 크거나 같아야 합니다. 이 값은 감독자 클러스터 설정과 겹치지 않아야 합니다. 하나의 IP 범위를 입력할 수 있습니다.
Services CIDR	Kubernetes 서비스에 사용할 IP 주소 범위를 지정합니다. 기본 값은 10.96.0.0/12입니다. 이 값은 감독자 클러스터 설정과 겹치지 않아야 합니다. 하나의 IP 범위를 입력할 수 있습니다.

- 12 클러스터 설정을 검토하고 **마침**을 클릭합니다.

다음에 수행할 작업

- 작업자 노드 수를 변경하려면 Kubernetes 클러스터의 크기를 조정합니다.
- kubeconfig 파일을 다운로드합니다. kubectl 명령줄 도구는 kubeconfig 파일을 사용하여 클러스터, 사용자, 네임스페이스 및 인증 메커니즘에 대한 정보를 얻습니다.
- Kubernetes 클러스터를 삭제합니다.

네이티브 Kubernetes 클러스터 만들기

Kubernetes Container Clusters 플러그인을 사용하여 Container Service Extension 3.0 관리 Kubernetes 클러스터를 만들 수 있습니다.

클러스터 만들기를 위한 다른 Kubernetes 런타임 옵션에 대한 자세한 내용은 [장 4 Kubernetes 클러스터 작업](#) 항목을 참조하십시오.

Container Service Extension CLI를 사용하여 Kubernetes 클러스터를 관리할 수도 있습니다. [Container Service Extension](#) 설명서를 참조하십시오.

사전 요구 사항

- 서비스 제공자가 Kubernetes Container Clusters 플러그인을 조직에 게시했는지 확인합니다. Kubernetes Container Clusters는 VMware Cloud Director용 Container Service Extension 플러그인입니다. 위쪽 탐색 모음의 **자세히 > Kubernetes Container Clusters**에서 플러그인을 찾을 수 있습니다.
- 서비스 제공자가 Container Service Extension 3.0 서버 설정을 완료했고 Container Service Extension 네이티브 배치 정책을 조직 VDC에 게시했는지 확인합니다.
- 서비스 제공자가 **cse:nativeCluster Entitlement** 권한 번들을 조직에 게시했고 네이티브 Kubernetes 클러스터를 만들고 수정할 수 있는 **편집: CSE:NATIVECLUSTER** 권한을 부여했는지 확인합니다. 클러스터를 삭제할 수 있으려면 **모든 권한: CSE:NATIVECLUSTER** 권한이 있어야 합니다.

- 서비스 제공자가 액세스 수준에 대한 정보를 사용하여 ACL(Access Control List) 항목을 만들었는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **추가 > Kubernetes Container Clusters**를 선택합니다.
- 2 (선택 사항) TKGI 클러스터 생성을 위해 조직 VDC를 사용하도록 설정한 경우 **Kubernetes Container Clusters** 페이지에서 **vSphere with Tanzu** 및 **네이티브** 탭을 선택합니다.
- 3 **새로 만들기**를 클릭합니다.
- 4 **네이티브** Kubernetes 런타임 옵션을 선택합니다.
- 5 이름을 입력하고 목록에서 Kubernetes 템플릿을 선택합니다.
- 6 (선택 사항) 새 Kubernetes 클러스터 및 SSH 공용 키에 대한 설명을 입력합니다.
- 7 **다음**을 클릭합니다.
- 8 네이티브 클러스터를 배포할 조직 VDC를 선택하고 **다음**을 클릭합니다.
- 9 제어부 및 작업자 노드 수를 선택하고 필요한 경우 노드에 대한 크기 조정 정책을 선택합니다.
- 10 **다음**을 클릭합니다.
- 11 NFS 소프트웨어를 사용하여 추가 VM을 배포하려는 경우 **NFS 사용** 옵션을 사용하도록 전환합니다.
- 12 (선택 사항) 제어부 및 작업자 노드에 대한 스토리지 정책을 선택합니다.
- 13 **다음**을 클릭합니다.
- 14 Kubernetes 클러스터에 대한 네트워크를 선택하고 **다음**을 클릭합니다.
- 15 클러스터 설정을 검토하고 **마침**을 클릭합니다.

다음에 수행할 작업

- 작업자 노드 수를 변경하려면 Kubernetes 클러스터의 크기를 조정합니다.
- kubeconfig 파일을 다운로드합니다. kubectl 명령줄 도구는 kubeconfig 파일을 사용하여 클러스터, 사용자, 네임스페이스 및 인증 메커니즘에 대한 정보를 얻습니다.
- Kubernetes 클러스터를 삭제합니다.

VMware Tanzu Kubernetes Grid Integrated Edition 클러스터 만들기

Container Service Extension을 사용하여 VMware Tanzu Kubernetes Grid Integrated Edition(TKGI) 클러스터를 만들 수 있습니다.

클러스터 만들기를 위한 다른 Kubernetes 런타임 옵션에 대한 자세한 내용은 [장 4 Kubernetes 클러스터 작업](#) 항목을 참조하십시오.

Container Service Extension CLI를 사용하여 Kubernetes 클러스터를 관리할 수도 있습니다. [Container Service Extension](#) 설명서를 참조하십시오.

사전 요구 사항

- 서비스 제공자가 Kubernetes Container Clusters 플러그인을 조직에 게시했는지 확인합니다.
Kubernetes Container Clusters는 VMware Cloud Director용 Container Service Extension 플러그인입니다. 위쪽 탐색 모음의 **자세히 > Kubernetes Container Clusters**에서 플러그인을 찾을 수 있습니다.
- 서비스 제공자가 Container Service Extension 3.0 서버 설정을 완료했고 Container Service Extension TKGI 사용 설정 메타데이터를 조직 VDC에 게시했는지 확인합니다.
- **{cse}:PKS DEPLOY RIGHT** 권한이 있는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **추가 > Kubernetes Container Clusters**를 선택합니다.
- 2 **Kubernetes Container Clusters** 페이지에서 **TKGI** 탭을 선택하고 **새로 만들기**를 클릭합니다.
새 TKGI 클러스터 만들기 마법사가 열립니다.
- 3 TKGI 클러스터를 배포할 조직 VDC를 선택하고 **다음**을 클릭합니다.
VMware Cloud Director는 CSE 서버에서 정보를 요청하기 때문에 목록을 로드하는 데 시간이 오래 걸릴 수 있습니다.
- 4 새 TKGI 클러스터의 이름을 입력하고 작업자 노드 수를 선택합니다.
TKGI 클러스터에는 하나 이상의 작업자 노드가 있어야 합니다.
- 5 **다음**을 클릭합니다.
- 6 클러스터 설정을 검토하고 **마침**을 클릭합니다.
- 7 (선택 사항) 새 TKGI 클러스터를 클러스터 목록에 표시하려면 페이지 오른쪽에서 **새로 고침** 버튼을 클릭합니다.

다음에 수행할 작업

- 작업자 노드 수를 변경하려면 Kubernetes 클러스터의 크기를 조정합니다.
- kubeconfig 파일을 다운로드합니다. kubectl 명령줄 도구는 kubeconfig 파일을 사용하여 클러스터, 사용자, 네임스페이스 및 인증 메커니즘에 대한 정보를 얻습니다.
- Kubernetes 클러스터를 삭제합니다.

Tanzu Kubernetes 클러스터의 서비스에 대한 외부 액세스 구성

VMware Cloud Director 10.2.2부터 Tanzu Kubernetes 클러스터는 기본적으로 클러스터가 생성된 동일한 조직 가상 데이터 센터 내에 있는 네트워크의 IP 서브넷에서만 연결할 수 있습니다. 필요한 경우 Tanzu Kubernetes 클러스터에서 특정 서비스에 대한 외부 액세스를 수동으로 구성할 수 있습니다.

VDC Kubernetes 정책이 조직 VDC에 게시되면 VDC 내의 인증된 소스에서 클러스터에 액세스할 수 있도록 클러스터 Edge 게이트웨이에 방화벽 정책이 자동으로 프로비저닝됩니다. 또한 조직 VDC 내의 워크로드가 클러스터 Edge 게이트웨이에 연결될 수 있도록 조직 VDC 내의 NSX-T Data Center Edge 게이트웨이에 시스템 SNAT 규칙이 자동으로 추가됩니다.

참고 조직 가상 데이터 센터가 NSX-T Data Center 그룹의 일부이면 데이터 센터 그룹의 다른 VDC가 클러스터 Edge 게이트웨이에 연결할 수 없습니다.

클러스터 Edge 게이트웨이에 프로비저닝된 방화벽 정책과 NSX-T Data Center Edge 게이트웨이의 SNAT 규칙은 **시스템 관리자**가 VDC에서 Kubernetes 정책을 삭제하지 않는 한 모두 제거될 수 없습니다.

필요한 경우 외부 네트워크에서 Tanzu Kubernetes 클러스터의 특정 서비스에 대한 액세스를 수동으로 구성할 수 있습니다. 이렇게 하려면 외부 위치에서 들어오는 트래픽이 클러스터 Edge 게이트웨이로 전달되도록 NSX-T Data Center Edge 게이트웨이에서 DNAT 규칙을 생성해야 합니다.

사전 요구 사항

- 클라우드 인프라가 vSphere 7.0 업데이트 1C, 7.0 업데이트 2 이상으로 지원되는지 확인합니다. **시스템 관리자**에게 문의하십시오.
- **조직 관리자** 권한이 있는지 확인합니다.
- **시스템 관리자**가 Tanzu Kubernetes 클러스터가 있는 조직 가상 데이터 센터 내에 NSX-T Data Center Edge 게이트웨이를 생성했는지 확인합니다.
- 서비스에 사용할 공용 IP 주소가 DNAT 규칙을 추가하려는 Edge 게이트웨이 인터페이스에 할당되었는지 확인합니다.
- kubectl 명령줄 도구의 `get services my-service` 명령을 사용하여 노출하려는 서비스의 외부 IP를 검색합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 Edge 게이트웨이를 클릭하고 **서비스**에서 **NAT**를 클릭합니다.
- 3 규칙을 추가하려면 **새로 만들기**를 클릭합니다.
- 4 외부 네트워크에 연결하려는 서비스에 대한 DNAT 규칙을 구성합니다.

옵션	설명
이름	규칙의 의미 있는 이름을 입력합니다.
설명	(선택 사항) 규칙에 대한 설명을 입력합니다.
상태	생성 시 규칙을 사용하도록 설정하려면 상태 토글을 설정합니다.
인터페이스 유형	드롭다운 메뉴에서 DNAT를 선택합니다.
외부 IP	서비스의 공용 IP 주소를 입력합니다. 입력하는 IP 주소는 NSX-T Data Center Edge 게이트웨이의 하위 할당된 IP 범위에 속해야 합니다.

옵션	설명
애플리케이션	상자를 비워 둡니다.
내부 IP	Kubernetes 수신 풀에서 할당된 서비스 IP 주소를 입력합니다.
내부 포트	(선택 사항) 인바운드 트래픽이 전달되는 포트 번호를 입력합니다.
로깅	(선택 사항) 이 규칙에 의해 수행된 주소 변환을 기록하려면 로깅 옵션을 토글하여 켭니다.

5 저장

다음에 수행할 작업

외부 네트워크에서 Kubernetes 서비스로 게시된 다른 애플리케이션에 대한 액세스를 제공하려면 각각에 대해 추가적인 DNAT 규칙을 구성해야 합니다.

네트워크 사용

5

다목적 클라우드 환경에서 매우 유연하고 안전한 네트워크 인프라를 제공하기 위해 VMware Cloud Director는 4가지 범주의 네트워크로 계층화된 네트워킹 아키텍처를 사용합니다. 네트워크 범주는 외부 네트워크, 조직 VDC(가상 데이터 센터) 네트워크, 데이터 센터 그룹 네트워크 및 vApp 네트워크입니다. 대부분의 VMware Cloud Director 네트워크 유형에는 Edge 게이트웨이, 네트워크 풀과 같은 추가적인 인프라 개체가 필요합니다.

외부 네트워크

외부 네트워크는 VMware Cloud Director 환경의 네트워크와 가상 시스템을 VPN, 회사 인트라넷 또는 공용 인터넷과 같은 네트워크 외부로 연결하는 업링크 인터페이스를 제공합니다.

외부 네트워크는 단일 vSphere 네트워크, 다중 vSphere 네트워크 또는 NSX-T Data Center Tier-0 논리적 라우터에서 지원됩니다.

외부 네트워크는 **시스템 관리자**만 만들 수 있습니다. 외부 네트워크에 대한 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"에서 참조하십시오.

네트워크 풀

네트워크 풀이란 요청 시에 vApp 네트워크 및 특정 유형의 조직 VDC 네트워크를 생성하는 데 사용할 수 있는 격리된 계층 2 네트워크 세그먼트의 집합입니다.

네트워크 풀은 조직 VDC 네트워크 및 vApp 네트워크보다 먼저 만들어야 합니다. 네트워크 풀이 없는 경우 조직에서 사용할 수 있는 네트워크 옵션은 외부 네트워크에 대한 직접 연결이 유일합니다.

네트워크 풀은 **시스템 관리자**만 만들 수 있습니다.

네트워크 풀에 대한 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"에서 참조하십시오.

조직 VDC 네트워크

조직 VDC(가상 데이터 센터 네트워크)를 사용하면 vApp이 서로 통신하거나 조직 밖의 외부 네트워크와 통신할 수 있습니다.

조직 VDC 네트워크와 외부 네트워크의 연결에 따라 조직 VDC 네트워크에는 여러 가지 유형이 있습니다.

조직 VDC 네트워크는 외부 네트워크에 대한 직접 연결이나 라우팅된 연결을 제공하거나, 외부 네트워크 및 기타 조직 VDC 네트워크와 격리될 수 있습니다. 라우팅된 연결을 사용하려면 조직 VDC에서 Edge 게이트웨이와 네트워크 풀이 필요합니다.

시스템 관리자 또는 **조직 관리자**는 조직 VDC 네트워크를 생성하여 조직에 할당합니다.

새로 생성된 조직 VDC에는 사용 가능한 네트워크가 없습니다. **시스템 관리자**가 필수 네트워크 인프라를 만들면 **조직 관리자**가 대부분의 조직 VDC 네트워크 유형을 생성하고 관리할 수 있습니다.

NSX Data Center for vSphere에서 지원하는 데이터 센터 그룹 네트워크

데이터 센터 그룹에 걸쳐 있는 NSX Data Center for vSphere에서 지원하는 네트워크입니다. 데이터 센터 그룹은 단일 사이트 또는 다중 사이트 VMware Cloud Director 배포에서 1~16개의 조직 VDC로 구성될 수 있습니다.

NSX-T Data Center에서 지원하는 데이터 센터 그룹 네트워크

데이터 센터 그룹 네트워크는 하나 이상의 VDC 간에 공유되고 vApp에서 연결할 수 있는 조직 VDC 네트워크의 한 유형입니다.

시스템 관리자 또는 **조직 관리자**는 데이터 센터 그룹 네트워크를 생성하고 단일 VDC 그룹으로 범위를 지정합니다.

VMware Cloud Director는 NSX-T Data Center에서 지원하는 격리된, 가져온, 라우팅된, 직접 데이터 센터 그룹 네트워크를 지원합니다.

vApp 네트워크

vApp 네트워크를 사용하면 가상 시스템이 서로 통신하거나 조직 VDC 네트워크에 연결하여 다른 vApp의 가상 시스템과 통신할 수 있습니다.

vApp 네트워크는 vApp 내에 포함됩니다. vApp 네트워크는 다른 네트워크에서 격리되거나 조직 VDC 네트워크에 연결될 수 있습니다.

모든 vApp에는 vApp 네트워크가 포함되어 있습니다. 이 네트워크는 vApp이 배포될 때 만들어지고 vApp이 배포 취소될 때 삭제됩니다.

조직 관리자는 vApp 네트워크를 설정하고 제어합니다.

vApp의 네트워크 유형

vApp의 가상 시스템은 격리되거나 직접 연결되거나 라우팅될 수 있는 vApp 네트워크에 연결하거나 조직 VDC 네트워크에 연결할 수 있습니다.

참고 NSX Data Center for vSphere에서 지원하는 조직 VDC는 라우팅된 vApp 네트워크, 격리된 vApp 네트워크 및 직접 vApp 네트워크를 지원합니다.

NSX-T Data Center에서 지원하는 조직 VDC는 격리된 vApp 네트워크 및 직접 vApp 네트워크를 지원합니다.

vApp에 여러 유형의 네트워크를 추가하여 여러 가지 네트워킹 시나리오를 처리할 수 있습니다.

vApp의 가상 시스템은 vApp에서 사용할 수 있는 네트워크에 연결할 수 있습니다. 가상 시스템을 다른 네트워크에 연결하려면 먼저 이 네트워크를 vApp에 추가해야 합니다.

vApp은 vApp 네트워크와 조직 VDC 네트워크를 포함할 수 있습니다. 격리된 vApp 네트워크는 vApp 내에 포함됩니다.

vApp 네트워크를 조직 VDC 네트워크로 라우팅하여 vApp 외부의 가상 시스템에 연결을 제공할 수도 있습니다. 라우팅된 vApp 네트워크에 대해 방화벽 및 정적 라우팅과 같은 네트워크 서비스를 구성할 수 있습니다.

vApp을 조직 VDC 네트워크에 직접 연결할 수 있습니다.

동일한 조직 VDC 네트워크에 연결된 동일한 가상 시스템이 포함된 vApp이 여러 개 있는 경우 vApp을 동시에 시작하려면 vApp을 펜싱할 수 있습니다. vApp을 펜싱하면 MAC 및 IP 주소를 격리하여 충돌 없이 가상 시스템의 전원을 켤 수 있습니다.

자세한 내용은 [vApp의 네트워크 작업](#)을 참조하십시오.

Edge 게이트웨이

Edge 게이트웨이는 외부 네트워크와 연결할 수 있는 라우팅된 조직 VDC 네트워크를 제공하고 로드 밸런싱, 네트워크 주소 변환, 방화벽과 같은 서비스를 제공할 수 있습니다. VMware Cloud Director는 IPv4 및 IPv6 Edge 게이트웨이를 지원합니다.

Edge 게이트웨이를 사용하려면 NSX Data Center for vSphere 또는 NSX-T Data Center가 필요합니다.

본 장은 다음 항목을 포함합니다.

- 조직 가상 데이터 센터 네트워크 관리
- NSX-T Data Center를 사용하여 데이터 센터 그룹 네트워킹 관리
- NSX Data Center for vSphere를 사용하여 데이터 센터 그룹 네트워킹 관리
- NSX Data Center for vSphere Edge 게이트웨이 서비스 관리
- NSX-T Data Center Edge 게이트웨이 관리

조직 가상 데이터 센터 네트워크 관리

시스템 관리자 또는 **조직 관리자**는 조직 VDC 네트워크를 생성하여 조직 VDC 또는 조직 VDC 그룹에 할당합니다. **조직 관리자**는 네트워크에 대한 정보 보기, 네트워크 서비스 구성 등의 작업을 수행할 수 있습니다.

NSX Data Center for vSphere에서 지원되는 직접, 라우팅된, 격리된 또는 데이터 센터 그룹 조직 VDC 네트워크를 사용할 수 있습니다.

NSX-T Data Center에서 지원되는 라우팅된, 격리된, 가져온, 직접 조직 VDC 네트워크를 사용할 수 있습니다. NSX-T Data Center에서 지원되는 라우팅된, 격리된, 가져온 데이터 센터 그룹 네트워크를 사용할 수도 있습니다.

표 5-1. 조직 VDC 네트워크 유형

데이터 센터 유형 네트워크	설명
직접	<p>시스템 관리자가 프로비저닝하고 vSphere 리소스에 의해 지원되는 외부 네트워크 중 하나에 직접 연결되는 조직 VDC 네트워크입니다.</p> <p>직접 네트워크는 NSX Data Center for vSphere에서 지원되는 조직 VDC에 대해 지원되며, VMware Cloud Director 10.2.2부터는 NSX-T Data Center에서 지원되는 조직 VDC에 대해 지원됩니다.</p> <p>직접 네트워크는 여러 조직 VDC에서 액세스할 수 있습니다.</p> <p>서로 다른 조직 VDC에 속하는 가상 시스템이 이 네트워크에 연결하고 트래픽을 볼 수 있습니다.</p> <p>직접 네트워크는 조직 VDC 외부의 가상 시스템에 대한 직접 레이어 2 연결을 제공합니다. 이 조직 VDC 외부의 가상 시스템은 조직 VDC의 가상 시스템에 직접 연결할 수 있습니다.</p> <p>참고 직접 조직 VDC 네트워크는 서비스 관리자만 추가할 수 있습니다.</p> <p>IPv4 또는 IPv6일 수 있습니다.</p>
격리된(내부)	<p>격리된 네트워크는 동일한 조직 VDC에서만 액세스할 수 있습니다. 이 조직 VDC의 가상 시스템만 내부 조직 VDC 네트워크에 연결하고 트래픽을 확인할 수 있습니다.</p> <p>격리된 네트워크는 NSX-T Data Center에서 지원하는 조직 VDC 및 조직 VDC NSX Data Center for vSphere에 대해 지원됩니다.</p> <p>격리된 조직 VDC 네트워크는 여러 가상 시스템 및 vApp이 연결할 수 있는 격리된 개인 네트워크를 조직 VDC에 제공합니다. 이 네트워크는 조직 VDC 외부의 가상 시스템에 연결을 제공하지 않습니다. 조직 VDC 외부의 시스템은 조직 VDC 내에 있는 시스템에 연결할 수 없습니다.</p>
라우팅된	<p>라우팅된 네트워크는 동일한 조직 VDC에서만 액세스할 수 있습니다. 이 조직 VDC 내에 있는 가상 시스템만 이 네트워크에 연결할 수 있습니다.</p> <p>이 네트워크는 외부 네트워크에 대한 제어된 액세스도 제공합니다. 시스템 관리자나 조직 관리자는 외부 네트워크에서 특정 가상 시스템에 액세스할 수 있도록 NAT(네트워크 주소 변환), 방화벽 및 VPN 설정을 구성할 수 있습니다.</p> <p>IPv4 또는 IPv6일 수 있습니다.</p>
가져온 NSX-T Data Center 논리적 스위치	<p>가져온 NSX-T Data Center 네트워크는 NSX-T Data Center에서 만들어지고 기존 NSX-T Data Center 논리적 스위치를 사용하는 논리적 세그먼트입니다. 특정 조직에 조직 VDC 네트워크로 가져옵니다.</p> <p>참고 시스템 관리자만 NSX-T Data Center 네트워크를 가져올 수 있습니다.</p>

표 5-1. 조직 VDC 네트워크 유형 (계속)

데이터 센터 유형 네트워크	설명
NSX Data Center for vSphere에서 지원하는 데이터 센터 그룹 네트워크	이 네트워크는 데이터 센터 그룹에 걸쳐 있는 데이터 센터 그룹 네트워크의 일부입니다. 데이터 센터 그룹은 단일 사이트 또는 다중 사이트 VMware Cloud Director 배포에서 1~16개의 조직 VDC로 구성될 수 있습니다. 이 네트워크에 연결된 가상 시스템은 스트레치된 기본 네트워크에 연결됩니다.
NSX-T Data Center에서 지원하는 데이터 센터 그룹 네트워크	데이터 센터 그룹 네트워크는 하나 이상의 VDC 간에 공유되고 vApp에서 연결할 수 있는, NSX-T Data Center에서 지원하는 조직 VDC 네트워크의 한 유형입니다. 데이터 센터 그룹 네트워크는 격리하거나, 가져오거나, 라우팅할 수 있으며 NSX-T Data Center가 필요합니다.

조직 VDC 네트워크를 관리하는 모든 단계는 환경에 둘 이상의 VDC가 있다고 가정하고 문서화되었습니다.

사용 가능한 조직 VDC 네트워크 보기

사용 가능한 조직 가상 데이터 센터 네트워크를 볼 수 있습니다.

사전 요구 사항

조직 관리자, 시스템 관리자인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.

절차

- ◆ 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.

결과

네트워크 탭에는 다양한 조건으로 필터링할 수 있는 사용 가능한 네트워크 목록이 표시됩니다.

다음에 수행할 작업

조직 VDC 네트워크를 추가할 수 있습니다. 기존 조직 VDC 네트워크를 편집하거나, 범위를 늘리거나, 삭제하거나, 재설정할 수도 있습니다.

격리된 조직 가상 데이터 센터 네트워크 추가

이 조직에서만 액세스할 수 있는 격리된 조직 VDC 네트워크를 추가할 수 있습니다. 이 네트워크는 이 조직 외부의 가상 시스템에 연결을 제공하지 않습니다. 이 조직 외부의 가상 시스템은 조직의 가상 시스템에 연결할 수 없습니다.

조직의 요구 사항에 맞게 격리된 조직 VDC 네트워크와 라우팅된 조직 VDC 네트워크를 혼합하여 추가할 수 있습니다. 예를 들어 Edge 게이트웨이와 연결되어 있고 인터넷에 연결된 별도의 네트워크를 보유하면서 중요한 정보가 포함된 네트워크를 격리할 수 있습니다.

네트워크 풀로 지원되는 격리된 VDC 네트워크를 만들 수 있습니다. 서비스 제공자는 NSX-T 논리적 스위치로 지원되는 격리된 VDC 네트워크를 만들 수도 있습니다.

사용자는 격리된 IPv4 조직 VDC 네트워크만 만들 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 **네트워크** 탭에서 **새로 만들기**를 클릭합니다.
- 3 **범위** 페이지에서 **조직 가상 데이터 센터**를 선택하고 네트워크를 생성할 VDC를 선택한 후 **다음**을 클릭합니다.
- 4 **네트워크 유형 선택** 페이지에서 **격리됨**을 선택하고 **다음**을 클릭합니다.
- 5 네트워크의 의미 있는 이름을 입력합니다.
- 6 네트워크에 대한 CIDR(Classless Inter-Domain Routing) 설정을 입력합니다.

network_gateway_IP_address/subnet_prefix_length 형식(예: **192.167.1.1/24**)을 사용합니다.

- 7 조직 VDC 네트워크에 대한 설명을 입력합니다.
- 8 (선택 사항) 네트워크를 생성한 VDC가 NSX Data Center for vSphere에서 지원되는 경우 **공유됨** 옵션 토글을 설정하여 조직 VDC 네트워크를 동일한 조직 내의 다른 조직 VDC에서 사용할 수 있도록 합니다.

예를 들어 예약 또는 할당 풀이 할당 모델로 설정된 조직 VDC 내에 애플리케이션이 있는 경우 이 옵션을 사용할 수 있습니다. 이 경우 더 많은 가상 시스템을 실행할 공간이 충분하지 않을 수 있습니다. 선지급을 사용하여 보조 조직 VDC를 만들면 해당 네트워크에서 임시로 추가 가상 시스템을 실행할 수 있습니다.

참고 조직 VDC는 동일한 제공자 VDC로 지원되어야 합니다.

- 9 **다음**을 클릭합니다.
- 10 (선택 사항) 정적 IP 주소가 필요한 가상 시스템에 할당할 하나 이상의 IP 주소를 예약하려면 네트워크에 대한 **정적 IP 풀**을 구성합니다.
 - a IP 주소 또는 IP 주소 범위를 입력하고 **추가**를 클릭합니다.
여러 정적 IP 주소 또는 범위를 추가하려면 이 단계를 반복합니다.
 - b (선택 사항) IP 주소 및 범위를 수정하거나 제거하려면 **수정** 또는 **제거**를 클릭합니다.
- 11 **다음**을 클릭합니다.

12 (선택 사항) DNS 설정을 구성합니다.

옵션	작업
기본 DNS	기본 DNS 서버의 IP 주소를 입력합니다.
보조 DNS	보조 DNS 서버의 IP 주소를 입력합니다.
DNS 접미사	DNS 접미사를 입력합니다. DNS 접미사는 호스트 이름이 포함되지 않은 DNS 이름입니다.

13 다음을 클릭합니다.

14 완료 준비 페이지에서 설정을 검토하고 마침을 클릭합니다.

라우팅된 조직 가상 데이터 센터 네트워크 추가

외부 네트워크에 대한 액세스를 제어하려면 라우팅된 조직 VDC 네트워크를 추가하면 됩니다. **시스템 관리자**와 **조직 관리자**는 외부 네트워크에서 특정 가상 시스템에 액세스할 수 있도록 NAT(네트워크 주소 변환), 방화벽 및 VPN 설정을 구성할 수 있습니다.

조직의 요구 사항에 맞게 라우팅된 조직 VDC 네트워크와 격리된 조직 VDC 네트워크를 혼합하여 추가할 수 있습니다. 예를 들어 중요한 정보가 포함된 격리된 네트워크를 유지하면서 Edge 게이트웨이와 연결되어 있고 인터넷에 연결된 네트워크를 추가할 수 있습니다.

IPv4 또는 IPv6 라우팅된 조직 VDC 네트워크를 추가할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 **네트워크** 탭에서 **새로 만들기**를 클릭합니다.
- 3 **범위** 페이지에서 **조직 가상 데이터 센터**를 선택하고 네트워크를 생성할 VDC를 선택한 후 **다음**을 클릭합니다.
- 4 **네트워크 유형 선택** 페이지에서 **라우팅됨**을 선택하고 **다음**을 클릭합니다.
- 5 네트워크의 의미 있는 이름을 입력합니다.
- 6 네트워크에 대한 CIDR(Classless Inter-Domain Routing) 설정을 입력합니다.
network_gateway_IP_address/subnet_prefix_length 형식(예: **192.167.1.1/24**)을 사용합니다.
- 7 조직 VDC 네트워크에 대한 설명을 입력합니다.

- 8 (선택 사항) 네트워크를 생성한 VDC가 NSX Data Center for vSphere에서 지원되는 경우 **공유됨** 옵션 토글을 설정하여 조직 VDC 네트워크를 동일한 조직 내의 다른 조직 VDC에서 사용할 수 있도록 합니다.

예를 들어 예약 또는 할당 풀이 할당 모델로 설정된 조직 VDC 내에 애플리케이션이 있는 경우 이 옵션을 사용할 수 있습니다. 이 경우 더 많은 가상 시스템을 실행할 공간이 충분하지 않을 수 있습니다. 선지급을 사용하여 보조 조직 VDC를 만들면 해당 네트워크에서 임시로 추가 가상 시스템을 실행할 수 있습니다.

참고 조직 VDC는 동일한 네트워크 풀을 공유해야 합니다.

- 9 다음을 클릭합니다.

- 10 **Edge 연결** 페이지에서 조직 VDC 네트워크와 연결할 Edge 게이트웨이를 선택합니다.

조직 VDC에 둘 이상의 Edge 게이트웨이가 포함되어 있는 경우 이 네트워크에서 연결할 하나의 Edge 게이트웨이를 선택해야 합니다. 라우팅된 다른 네트워크를 지원하려면 Edge 게이트웨이의 [사용 가능한 네트워크 수] 열에 1 이상의 값이 표시되어야 합니다.

- 11 **인터페이스 유형** 드롭다운 메뉴에서 인터페이스 유형을 선택합니다.

옵션	설명
내부	Edge 게이트웨이의 내부 인터페이스 중 하나에 연결합니다. 허용되는 최대 네트워크 수는 9입니다.
분산	이 Edge 게이트웨이에 연결된 논리적 분산 라우터에서 네트워크를 만듭니다. 허용되는 최대 네트워크 수는 400입니다.
하위 인터페이스	조직 VDC 네트워크를 확장합니다. VMware Cloud Director는 L2 VPN을 통해 확장하는 데 사용할 네트워크를 식별합니다. VMware Cloud Director는 NSX 네트워크 가상화를 통해 이 네트워크에 사용할 트렁크 인터페이스 유형을 만듭니다. 허용되는 최대 네트워크 수는 200입니다.

- 12 (선택 사항) 이 네트워크에서 게스트 VLAN의 태그 지정을 사용하도록 설정하려면 **게스트 VLAN 허용** 옵션을 설정합니다.

- 13 다음을 클릭합니다.

- 14 (선택 사항) 정적 IP 주소가 필요한 가상 시스템에 할당할 하나 이상의 IP 주소를 예약하려면 네트워크에 대한 **정적 IP 풀**을 구성합니다.

- a IP 주소 또는 IP 주소 범위를 입력하고 **추가**를 클릭합니다.

여러 정적 IP 주소 또는 범위를 추가하려면 이 단계를 반복합니다.

- b (선택 사항) IP 주소 및 범위를 수정하거나 제거하려면 **수정** 또는 **제거**를 클릭합니다.

- 15 다음을 클릭합니다.

16 (선택 사항) DNS 설정을 구성합니다.

옵션	작업
기본 DNS	기본 DNS 서버의 IP 주소를 입력합니다.
보조 DNS	보조 DNS 서버의 IP 주소를 입력합니다.
DNS 접미사	DNS 접미사를 입력합니다. DNS 접미사는 호스트 이름이 포함되지 않은 DNS 이름입니다.

17 다음을 클릭합니다.

18 완료 준비 페이지에서 설정을 검토하고 마침을 클릭합니다.

직접 조직 가상 데이터 센터 네트워크 추가

시스템 관리자는 직접 연결을 설정하여 직접 경로를 통해 외부 네트워크에 연결할 수 있습니다.

VMware Cloud Director 10.2.2부터는 NSX-T Data Center 및 NSX Data Center for vSphere가 지원하는 조직 VDCS에서 직접 네트워크 생성이 지원됩니다.

조직 관리자로 VMware Cloud Director 테넌트 포털에 로그인한 후 직접 조직 가상 데이터 센터 네트워크를 만들려고 시도하면 권한이 부족하다는 경고 메시지가 표시됩니다.

사전 요구 사항

시스템 관리자 권한이 있는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 **네트워크** 탭에서 **새로 만들기**를 클릭합니다.
- 3 범위 페이지에서 **조직 가상 데이터 센터**를 선택하고 네트워크를 생성할 VDC를 선택한 후 다음을 클릭합니다.
- 4 **네트워크 유형** 페이지에서 **직접**을 선택한 후 다음을 클릭합니다.
- 5 네트워크의 의미 있는 이름을 입력합니다.
- 6 조직 VDC 네트워크에 대한 설명을 입력합니다.
- 7 (선택 사항) 조직 VDC 네트워크를 동일한 조직 내의 다른 조직 VDC가 사용할 수 있게 하려면 **공유됨** 옵션을 설정합니다.
- 8 **외부 네트워크 연결** 페이지에서 새 조직 가상 데이터 센터 네트워크를 직접 연결할 외부 네트워크를 선택하고 다음을 클릭합니다.
- 9 완료 준비 페이지에서 설정을 검토하고 마침을 클릭합니다.

가져온 NSX-T Data Center 논리적 스위치를 사용하여 조직 VDC 네트워크 추가

시스템 관리자는 연결된 NSX-T Manager 인스턴스에서 논리적 스위치를 가져와서 조직 VDC 네트워크를 만들 수 있습니다.

사전 요구 사항

- **시스템 관리자** 권한이 있는지 확인합니다.
- 대상 조직 가상 데이터 센터를 지원하는 제공자 가상 데이터 센터가 NSX-T Manager 인스턴스와 연결되어 있는지 확인합니다.
- 다른 조직 가상 데이터 센터 네트워크에서 사용 중이 아닌 NSX-T 논리적 스위치를 하나 이상 만들어야 합니다.

NSX-T 논리적 스위치 생성 및 구성에 대한 자세한 내용은 "NSX-T Data Center 관리 가이드"의 내용을 참조하십시오.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 **네트워크** 탭에서 **새로 만들기**를 클릭합니다.
- 3 **범위** 페이지에서 **조직 가상 데이터 센터**를 선택하고 네트워크를 생성할 VDC를 선택한 후 **다음**을 클릭합니다.
- 4 **네트워크 유형** 페이지에서 **가져옴**을 선택한 다음 **NSX-T 논리적 스위치**를 선택하고 **다음**을 클릭합니다.
- 5 사용 가능한 NSX-T 논리적 스위치 목록에서 대상 스위치를 선택하고 **다음**을 클릭합니다.
- 6 네트워크의 의미 있는 이름을 입력합니다.
- 7 네트워크에 대한 CIDR(Classless Inter-Domain Routing) 설정을 입력합니다.

network_gateway_IP_address/subnet_prefix_length 형식(예: **192.167.1.1/24**)을 사용합니다.

스위치에 서브넷이 구성되어 있으면 이 정보가 미리 채워집니다.

- 8 조직 VDC 네트워크에 대한 설명을 입력합니다.
- 9 **다음**을 클릭합니다.
- 10 (선택 사항) DNS 설정 및 정적 IP 풀을 구성합니다.
여러 개의 IP 주소 및 IP 범위를 추가할 수 있습니다.
- 11 **다음**을 클릭합니다.
- 12 **완료 준비** 페이지에서 설정을 검토하고 **마침**을 클릭합니다.

조직 가상 데이터 센터 네트워크의 일반 설정 편집

조직 VDC 네트워크의 속성을 수정할 수 있습니다.

사전 요구 사항

조직 관리자, 시스템 관리자인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 **네트워크** 탭에서 편집할 조직 VDC 네트워크의 이름을 클릭합니다.
- 3 **일반** 탭에서 **편집**을 클릭합니다.
 - a 네트워크의 이름과 설명을 편집합니다.
 - b 네트워크를 생성한 VDC가 NSX Data Center for vSphere에서 지원되는 경우 **공유됨** 옵션 토글을 설정하거나 해제하여 조직 VDC 네트워크를 동일한 조직 내의 다른 조직 VDC에서 사용할 수 있도록 합니다.
- 4 **저장**을 클릭합니다.

Edge 게이트웨이에 조직 가상 데이터 센터 네트워크 연결

조직 VDC 네트워크를 생성한 후 해당 네트워크를 Edge 게이트웨이에 연결할 수 있습니다.

버전 10.1부터 VMware Cloud Director는 NSX Data Center for vSphere 또는 NSX-T Data Center가 지원하는 조직 VDC 네트워크에 대한 Edge 게이트웨이로의 연결을 지원합니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 또는 **시스템 관리자** 역할 또는 조직에 게시된 **조직 VDC 네트워크: 속성 편집** 및 **VDC 그룹: 보기** 권한을 포함하는 역할 중 하나가 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 Edge 게이트웨이에 연결할 조직 VDC 네트워크의 이름을 클릭합니다.
- 3 **일반** 탭에서 **편집**을 클릭합니다.
- 4 **연결**을 클릭합니다.
- 5 Edge 게이트웨이에 네트워크를 연결합니다.
 - a **Edge 게이트웨이에 연결** 옵션을 설정합니다.
 - b 사용 가능한 Edge 게이트웨이의 목록에서 연결할 Edge 게이트웨이를 선택합니다.
 - c 인터페이스 유형을 선택합니다.
 - d 게스트 VLAN을 허용하려면 **게스트 VLAN 허용** 옵션을 설정합니다.

6 저장을 클릭합니다.

결과

조직 VDC 네트워크가 Edge 게이트웨이에 연결되고 [격리됨]에서 [라우팅됨]으로 변환됩니다.

Edge 게이트웨이에서 조직 VDC 네트워크의 연결 끊기

Edge 게이트웨이에서 조직 VDC 네트워크의 연결을 끊어서 라우팅됨에서 격리됨으로 변환할 수 있습니다.

버전 10.1부터 Edge 게이트웨이와 연결하거나 연결을 끊는 것은 NSX Data Center for vSphere 또는 NSX-T Data Center에서 지원되는 조직 VDC 네트워크에 대해 지원됩니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 또는 **시스템 관리자** 역할 또는 **조직 VDC 네트워크: 속성 편집** 권한이 포함된 역할 중 하나가 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 연결을 끊을 조직 VDC 네트워크의 이름을 클릭합니다.
- 3 **일반** 탭에서 **편집**을 클릭합니다.
- 4 **연결**을 클릭합니다.
- 5 Edge 게이트웨이에서 네트워크의 연결을 끊으려면 **Edge 게이트웨이에 연결** 옵션의 토글을 끕니다.
- 6 **저장**을 클릭합니다.

결과

Edge 게이트웨이에서 조직 VDC 네트워크의 연결을 끊었습니다. 조직 VDC 네트워크가 라우팅됨에서 격리됨으로 변환됩니다.

라우팅된 조직 VDC 네트워크의 인터페이스 변환

예를 들어 네트워크 속성을 편집하여 네트워크 인터페이스를 내부에서 하위 인터페이스 또는 분산 라우팅으로 변경할 수 있습니다.

참고 크로스 VDC 네트워크는 변환할 수 없습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.

- 2 편집할 조직 VDC 네트워크의 이름을 클릭합니다.
- 3 일반 탭에서 **편집**을 클릭합니다.
- 4 **연결**을 클릭합니다.
- 5 **인터페이스 유형** 드롭다운 메뉴에서 인터페이스 유형을 선택합니다.

옵션	설명
내부	Edge 게이트웨이의 내부 인터페이스 중 하나에 연결합니다. 허용되는 최대 네트워크 수는 9입니다.
분산	이 Edge 게이트웨이에 연결된 논리적 분산 라우터에서 네트워크를 만듭니다. 허용되는 최대 네트워크 수는 400입니다.
하위 인터페이스	조직 VDC 네트워크를 확장합니다. VMware Cloud Director는 L2 VPN을 통해 확장하는 데 사용할 네트워크를 식별합니다. VMware Cloud Director는 NSX 네트워크 가상화를 통해 이 네트워크에 사용할 트렁크 인터페이스 유형을 만듭니다. 허용되는 최대 네트워크 수는 200입니다.

- 6 **저장**을 클릭합니다.

조직 가상 데이터 센터 네트워크에 사용되는 IP 주소 보기

조직 가상 데이터 센터 네트워크 IP 풀에서 현재 사용 중인 IP 주소의 목록을 볼 수 있습니다.

사전 요구 사항

- **조직 관리자, 시스템 관리자**인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.
- 네트워크가 격리된 또는 라우팅된 조직 가상 데이터 센터 네트워크인지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 사용되는 IP 주소를 볼 네트워크의 이름을 클릭합니다.
- 3 **IP 관리** 섹션에서 **IP 사용량**을 클릭하여 현재 사용 중인 IP 주소를 확인합니다.

조직 가상 데이터 센터 네트워크 IP 풀에 IP 주소 추가

조직 가상 데이터 센터 네트워크의 IP 주소가 부족할 경우 해당 IP 풀에 주소를 더 추가할 수 있습니다.

직접 연결이 있는 외부 조직 가상 데이터 센터 네트워크에는 IP 주소를 추가할 수 없습니다.

사전 요구 사항

- **조직 관리자, 시스템 관리자**인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.
- 네트워크가 격리된 또는 라우팅된 조직 가상 데이터 센터 네트워크인지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.

- 2 편집할 네트워크의 이름을 클릭합니다.
- 3 **IP 관리** 섹션에서 **정적 IP 풀** 탭을 클릭합니다.
- 4 오른쪽에서 **편집** 버튼을 클릭합니다.

네트워크 편집 창에 게이트웨이 CIDR 및 IP 주소 범위가 표시됩니다(있는 경우).

- 5 **정적 IP 풀** 텍스트 상자에 IP 주소 또는 IP 주소 범위를 입력하고 **추가**를 클릭합니다.

참고 크로스 VDC 네트워크의 경우, 여기에 입력하는 IP 주소는 동일한 스트레치된 네트워크의 다른 조직 VDC 네트워크에 할당된 IP 주소와 겹치지 않아야 합니다.

- 6 **저장**을 클릭합니다.

결과

IP 주소 또는 IP 주소 범위가 네트워크 IP 풀에 추가됩니다.

조직 가상 데이터 센터 네트워크에서 사용되는 IP 범위 편집 또는 제거

조직 가상 데이터 센터 네트워크에 더 이상 필요하지 않은 IP 주소가 포함되어 있는 경우 해당 주소를 편집하거나 IP 풀에서 삭제할 수 있습니다.

사전 요구 사항

- **조직 관리자, 시스템 관리자**인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.
- 네트워크가 격리된 또는 라우팅된 조직 가상 데이터 센터 네트워크인지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 편집할 네트워크의 이름을 클릭합니다.
- 3 **IP 관리** 섹션에서 **정적 IP 풀**을 클릭합니다.
- 4 오른쪽에서 **편집** 버튼을 클릭합니다.
 - IP 범위를 수정하려면 범위를 선택하고 필요한 대로 내용을 편집한 후 **수정**을 클릭합니다.
 - IP 범위를 제거하려면 범위를 선택하고 **제거**를 클릭합니다.
- 5 **저장**을 클릭합니다.

조직 가상 데이터 센터 네트워크의 DNS 설정 편집

조직 가상 데이터 센터 네트워크의 DNS 설정을 편집할 수 있습니다.

사전 요구 사항

- **조직 관리자, 시스템 관리자**인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.
- 네트워크가 격리된 또는 라우팅된 조직 가상 데이터 센터 네트워크인지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 편집할 네트워크의 이름을 클릭합니다.
- 3 **IP 관리** 섹션에서 **DNS**를 클릭합니다.
- 4 오른쪽에서 **편집** 버튼을 클릭합니다.
- 5 기본 DNS, 보조 DNS 및 DNS 접미사 정보를 필요한 대로 편집합니다.
- 6 **저장**을 클릭합니다.

격리된 조직 가상 데이터 센터 네트워크의 DHCP 설정 구성

NSX Data Center for vSphere가 지원하는 격리된 조직 VDC 네트워크의 DHCP 설정을 편집할 수 있습니다. 조직 VDC 네트워크의 DHCP 서비스는 DHCP에서 주소를 요청하도록 구성된 VM NIC에 해당 주소 풀의 IP 주소를 제공합니다. 이 서비스는 가상 시스템의 전원이 켜지면 주소를 제공합니다.

버전 10.2부터 VMware Cloud Director는 IPv4 및 IPv6 모두에 대해 DHCP 설정을 지원합니다. VMware Cloud Director API를 사용하여 IPv6 설정을 구성할 수 있습니다.

사전 요구 사항

- **조직 관리자, 시스템 관리자**인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.
- 네트워크가 격리된 조직 가상 데이터 센터 네트워크인지 확인합니다.
- NSX Data Center for vSphere에서 네트워크가 지원되는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 편집할 네트워크의 이름을 클릭합니다.
- 3 **IP 관리** 섹션에서 **DHCP**를 클릭합니다.
- 4 DHCP를 사용하도록 설정하려면 **DHCP 풀 서비스**의 오른쪽에서 **편집**을 클릭합니다.
- 5 **DHCP 풀 서비스** 옵션을 설정하고 **저장**을 클릭합니다.
DHCP 클라이언트가 요청한 주소를 DHCP 풀에서 가져옵니다.
- 6 네트워크에 대한 DHCP 풀을 만듭니다.
 - a **새로 만들기**를 클릭합니다.
 - b 풀에 대한 IP 주소 범위를 입력합니다.

지정하는 IP 주소 범위는 조직 가상 데이터 센터에 대한 정적 IP 주소 풀과 겹칠 수 없습니다.

- c DHCP 주소에 대한 기본 임대 기간을 초 단위로 지정합니다.

기본값은 3,600초입니다.

- d DHCP 주소에 대한 최대 임대 기간을 초 단위로 지정합니다.

이것은 DHCP 할당 IP 주소가 가상 시스템에 임대되는 최대 시간입니다. 기본값은 7,200초입니다.

7 저장을 클릭합니다.

NSX-T Data Center에서 지원되는 라우팅된 조직 가상 데이터 센터 네트워크에 DHCP 풀 추가

NSX-T Data Center에서 지원되는 라우팅된 조직 VDC 네트워크에 DHCP 풀을 추가할 수 있습니다.

참고 NSX-T Data Center가 지원하는 조직 VDC 네트워크에서는 DHCP 풀 삭제 또는 업데이트가 지원되지 않습니다.

사전 요구 사항

- 이러한 작업을 수행하려면 미리 정의된 **조직 관리자** 또는 **시스템 관리자** 역할이나 이와 동등한 권한 집합이 포함된 역할이 필요합니다.
- 네트워크가 라우팅된 조직 가상 데이터 센터 네트워크인지 확인합니다.
- NSX-T Data Center에서 네트워크가 지원되는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 편집할 네트워크의 이름을 클릭합니다.
- 3 **IP 관리** 섹션에서 DHCP를 클릭합니다.
- 4 DHCP 풀을 추가하려면 **새로 만들기**를 클릭합니다.
- 5 풀에 대한 IPv4 주소 범위를 입력합니다.
- 6 **저장**을 클릭합니다.

NSX Data Center for vSphere에서 지원하는 격리된 조직 가상 데이터 센터 네트워크에 대한 기존 DHCP 풀 편집 또는 삭제

격리된 조직 가상 데이터 센터 네트워크 내에서 특정 DHCP 풀이 더 이상 필요하지 않은 경우 NSX Data Center for vSphere에서 지원하는 풀을 삭제하거나 편집할 수 있습니다.

사전 요구 사항

- **조직 관리자**, **시스템 관리자**인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.
- 네트워크가 격리된 조직 가상 데이터 센터 네트워크인지 확인합니다.

- 조직 가상 데이터 센터 네트워크가 NSX Data Center for vSphere에서 지원되는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 편집할 네트워크의 이름을 클릭합니다.
- 3 **IP 관리** 섹션을 클릭하고 **DHCP**를 클릭합니다.
- 4 기존 DHCP 풀을 편집 또는 삭제합니다.

옵션	작업
DHCP 풀을 편집합니다.	<ol style="list-style-type: none"> 1 편집할 DHCP 풀을 선택합니다. 2 편집 버튼을 클릭합니다. 3 풀에 대한 IP 주소 범위를 업데이트합니다. 4 DHCP 주소에 대한 기본 임대 기간을 초 단위로 편집합니다. 5 DHCP 주소에 대한 최대 임대 기간을 초 단위로 편집합니다. 6 저장을 클릭합니다.
DHCP 풀을 삭제합니다.	<ol style="list-style-type: none"> 1 삭제할 DHCP 풀을 선택합니다. 2 삭제 버튼을 클릭합니다.

조직 가상 데이터 센터 네트워크 재설정

조직 가상 데이터 센터 네트워크와 연결된 DHCP 설정, 방화벽 설정 등의 네트워크 서비스가 제대로 작동하지 않을 경우 네트워크를 재설정할 수 있습니다.

조직 가상 데이터 센터 네트워크를 재설정할 때 DHCP 서비스 게이트웨이가 강제로 재배포되도록 합니다. 이 작업을 수행하면 네트워크가 재설정되는 동안 DHCP 서비스가 일시적으로 중단되고 네트워크 서비스를 사용할 수 없습니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- 네트워크가 가상 시스템, vApp 또는 다른 네트워크에 연결되어 있지 않습니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 조직 VDC 네트워크를 선택합니다.
- 3 **재설정**을 클릭하고 재설정 작업을 확인합니다.

조직 가상 데이터 센터 네트워크 삭제

조직 가상 데이터 센터 네트워크가 더 이상 필요하지 않은 경우 해당 네트워크를 삭제할 수 있습니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- 네트워크가 가상 시스템, vApp 또는 다른 네트워크에 연결되어 있지 않습니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 대상 네트워크의 이름 옆에 있는 라디오 버튼을 클릭하고 **삭제**를 클릭합니다.
- 3 **확인**을 클릭하여 확인합니다.

NSX-T Data Center를 사용하여 데이터 센터 그룹 네트워킹 관리

버전 10.2부터 VMware Cloud Director는 NSX-T Data Center에서 지원하는 데이터 센터 그룹 네트워킹을 지원합니다.

여러 조직 VDC에서 네트워크를 생성하려면 먼저 VDC를 그룹화한 다음, 공유되는 그룹 네트워크를 만듭니다.

NSX-T Data Center에서 지원하는 데이터 센터 그룹 네트워크는 데이터 센터 그룹 전체에 적용되는 수준 2 네트워크 공유, 단일 활성 송신 지점 구성 및 DFW(분산 방화벽) 규칙을 제공합니다.

데이터 센터 그룹

데이터 센터 그룹은 중앙 집중식 네트워킹 관리, 송신 지점 구성 및 그룹 내의 모든 네트워크 간의 동-서 트래픽을 제공하는 크로스 VDC 라우터 역할을 합니다. 데이터 센터 그룹은 활성 송신 지점을 공유하도록 구성된 1~16개의 VDC를 포함할 수 있습니다.

가용성 영역

가용성 영역은 네트워크에서 사용할 수 있는 계산 클러스터 또는 계산 장애 도메인을 나타냅니다. 기본적으로 가용성 영역은 제공자 VDC입니다.

중요 **시스템 관리자**는 vCenter Server 인스턴스 및 필요한 경우 vCenter Server 인스턴스에서 지원되는 제공자 VDC에 대해 **계산 제공자 범위**를 설정하여 NSX-T Data Center를 사용하는 그룹 네트워킹에 대한 가용성 영역을 구성해야 합니다. 기본적으로 제공자 VDC의 계산 제공자 범위는 이 VDC를 지원하는 vCenter Server 인스턴스에서 복사됩니다. **시스템 관리자**는 단일 vCenter Server 인스턴스에서 지원되는 서로 다른 제공자 VDC에 대해 계산 제공자 범위를 구분할 수 있습니다. 예를 들어 범위가 **Germany**인 vCenter Server 인스턴스와 범위가 **Munich**인 제공자 VDC가 있을 수 있습니다.

시스템 관리자는 가용성 영역을 네트워크 제공자 범위로 재구성할 수도 있으며, 이는 일반적으로 연결된 NSX-T Manager가 있는 기본 vCenter Server 인스턴스를 나타냅니다.

송신 지점

데이터 센터 그룹을 외부 네트워크에 연결하기 위해 구성하는 기존 NSX-T Data Center Edge 게이트웨이입니다.

데이터 센터 그룹 네트워크

데이터 센터 그룹 내의 모든 VDC에서 공유되는 레이어 2 네트워크입니다.

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹 관리

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹을 생성한 후, 그룹에 데이터 센터를 추가하고, 제거하고, 그룹 설정을 편집할 수 있습니다.

데이터 센터 그룹에는 가상 데이터 센터를 16개까지 포함할 수 있습니다.

데이터 센터 그룹에서 제거하는 VDC에는 데이터 센터 그룹에 참여하는 네트워크에 연결된 워크로드가 없어야 합니다.

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹 만들기

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에는 1~16개의 VDC를 그룹화할 수 있습니다.

사전 요구 사항

조직 관리자, 시스템 관리자인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
- 2 **새로 만들기**를 클릭합니다.
- 3 **VDC 시작** 페이지에서 그룹을 시작할 NSX-T Data Center에서 지원하는 VDC를 선택합니다.
- 4 새 데이터 센터 그룹의 이름과 설명(선택 사항)을 입력합니다.
- 5 **참여 중인 VDC** 페이지에서 새 데이터 센터 그룹에 대한 추가 데이터 센터를 선택하고 **다음**을 클릭합니다.
- 6 데이터 센터 그룹 세부 정보를 검토하고 **마침**을 클릭합니다.

결과

새로 생성된 그룹이 데이터 센터 그룹 목록에 나타납니다.

다음에 수행할 작업

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에 걸친 네트워크를 생성합니다.

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹의 일반 설정 보기 및 편집

조직에서 NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹을 살펴보고 편집할 수 있습니다.

사전 요구 사항

조직 관리자이거나 동등한 권한 집합을 가진 역할이 있는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
- 3 **일반 설정** 창에서 **편집**을 클릭합니다.
- 4 데이터 센터 그룹의 이름과 설명(선택 사항)을 편집하고 **저장**을 클릭하여 확인합니다.

데이터 센터 그룹에서 참여 중인 VDC 관리

VDC 그룹의 일부가 되고 서로 통신할 VDC를 선택할 수 있습니다.

사전 요구 사항

조직 관리자이거나 동등한 권한 집합을 가진 역할이 있는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
- 3 **참여 중인 VDC**를 클릭한 다음 **관리**를 클릭합니다.
- 4 그룹에 포함할 VDC를 선택하고 **저장**을 클릭하여 확인합니다.

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹 동기화

데이터 센터 그룹에 참여하는 모든 VDC가 계속 존재하며 제대로 구성되어 있는지 확인하려면 데이터 센터 그룹을 동기화하면 됩니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
- 3 **동기화**를 클릭하고 확인합니다.

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에서 분산 방화벽 사용

버전 10.2부터 VMware Cloud Director는 NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에 대한 분산 방화벽 서비스를 지원합니다.

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에 분산 방화벽을 사용하도록 설정하면 데이터 센터 그룹에 적용되는 단일 기본 보안 정책을 생성합니다.

조직 관리자는 데이터 센터 그룹의 기본 보안 정책과 연결된 추가 분산 방화벽 규칙을 생성하고 수정할 수 있습니다.

분산 방화벽 서비스는 기본적으로 사용하도록 설정되어 있지 않습니다. 분산 방화벽을 사용하도록 설정한 후에는 분산 방화벽 규칙 생성이 용이하도록 IP 집합 및 보안 그룹을 생성할 수 있습니다.

참고 생성하는 분산 방화벽 규칙은 데이터 센터 그룹 네트워크에 연결된 워크로드에만 적용됩니다.

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에 대한 분산 방화벽 활성화

분산 방화벽을 사용하면 단일 데이터 센터 그룹 전체에 수준 3 방화벽 규칙 집합을 적용할 수 있습니다.

분산 방화벽은 기본적으로 사용되도록 설정되어 있지 않습니다. 이 기능을 사용하도록 설정할 때 단일 기본 보안 정책을 생성합니다.

사전 요구 사항

시스템 관리자 권한이 있는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
- 3 **분산 방화벽** 섹션에서 **활성화**를 클릭하고 분산 방화벽을 활성화할 것임을 확인합니다.

다음에 수행할 작업

분산 방화벽 규칙을 생성합니다.

데이터 센터 그룹에 IP 집합 추가

분산 방화벽 규칙을 생성하여 데이터 센터 그룹에 추가하려면 먼저 IP 집합을 생성해야 합니다. IP 집합은 분산 방화벽 규칙이 적용되는 IP 주소 및 네트워크 그룹입니다. 여러 개체를 IP 집합으로 결합하면, 생성할 분산 방화벽 규칙의 총 수를 줄이는 데 도움이 됩니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
- 3 보안에서 **IP 집합**을 클릭합니다.
- 4 **새로 만들기**를 클릭합니다.
- 5 새 IP 집합의 의미 있는 이름과 설명(선택 사항)을 입력합니다.
- 6 IPv4 주소, IPv6 주소 또는 주소 범위를 CIDR 형식으로 입력하고 **추가**를 클릭합니다.
- 7 기존 IP 주소 또는 범위를 수정하려면 **수정**을 클릭하고 값을 편집합니다.
- 8 **저장**을 클릭하여 확인합니다.

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에 보안 그룹 생성

데이터 센터 그룹에 대한 분산 방화벽 규칙을 생성하기 전에, 데이터 센터 그룹 네트워크를 규칙이 적용되는 보안 그룹으로 그룹화할 수 있습니다.

보안 그룹은 분산 방화벽 규칙이 적용되는 데이터 센터 그룹 네트워크 그룹입니다. 네트워크를 그룹화하면 생성할 분산 방화벽 규칙의 총 수를 줄일 수 있습니다.

사전 요구 사항

NSX-T Data Center에서 지원하는 데이터 센터 그룹 네트워크가 하나 이상 있는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
- 3 보안에서 **보안 그룹**을 클릭하고 **새로 만들기**를 클릭합니다.
- 4 보안 그룹의 이름과 설명(선택 사항)을 입력하고 **저장**을 클릭합니다.
새 보안 그룹이 목록에 나타납니다.
- 5 새로 생성된 보안 그룹을 선택하고 **구성원 관리**를 클릭합니다.
- 6 보안 그룹에 추가할 데이터 센터 그룹 네트워크를 선택합니다.
- 7 **저장**을 클릭합니다.

다음에 수행할 작업

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에 분산 방화벽 규칙 추가

데이터 센터 그룹에 애플리케이션 포트 프로파일 추가

분산 방화벽 규칙을 생성하려면 미리 구성된 애플리케이션 포트 프로파일 및 사용자 지정 애플리케이션 포트 프로파일을 사용하면 됩니다.

애플리케이션 포트 프로파일에는 방화벽 서비스에 사용되는 프로토콜과 포트 또는 포트 그룹의 조합이 포함됩니다. 미리 구성된 기본 포트 프로파일 외에도 사용자 지정 애플리케이션 포트 프로파일을 생성할 수 있습니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
- 3 보안에서 **애플리케이션 포트 프로파일**을 클릭합니다.
- 4 **사용자 지정 애플리케이션** 창에서 **새로 만들기**를 클릭합니다.
- 5 애플리케이션 포트 프로파일의 이름과 설명(선택 사항)을 입력합니다.
- 6 **프로토콜** 드롭다운 메뉴에서 프로토콜을 선택합니다.
- 7 포트 또는 포트 범위를 쉼표로 구분하여 입력하고 **저장**을 클릭합니다.
- 8 포트 프로파일을 추가로 구성하려면 단계를 반복합니다.

다음에 수행할 작업

애플리케이션 포트 프로파일을 사용하여 분산 방화벽 규칙을 생성합니다.

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에 분산 방화벽 규칙 추가

생성하는 분산 방화벽 규칙은 데이터 센터 그룹 네트워크에 연결된 워크로드에만 적용됩니다.

사전 요구 사항

데이터 센터 그룹에 대한 분산 방화벽 서비스를 사용하도록 설정했는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
- 3 왼쪽에서 **분산 방화벽** 탭을 클릭합니다.
- 4 **규칙 편집**을 클릭합니다.
- 5 방화벽 규칙을 추가하려면 **맨 위에 새로 만들기**를 클릭합니다.

6 규칙을 구성합니다.

옵션	설명
이름	규칙의 이름을 입력합니다.
상태	생성 시 규칙을 사용하도록 설정하려면 상태 옵션을 토글하여 켭니다.
애플리케이션	(선택 사항) 규칙이 적용되는 특정 포트 프로파일을 선택하려면 애플리케이션 토글을 설정하고 저장 을 클릭합니다.
컨텍스트	(선택 사항) 규칙에 대한 NSX-T Data Center 컨텍스트 프로파일을 선택합니다.
소스	소스 트래픽을 선택하고 유지 를 클릭합니다. <ul style="list-style-type: none"> ■ 임의의 소스 주소에서 발생한 트래픽을 허용하거나 거부하려면 모든 소스 토글을 설정합니다. ■ 특정 IP 집합 또는 보안 그룹에서 발생한 트래픽을 허용하거나 거부하려면 목록에서 IP 집합 및 보안 그룹을 선택합니다.
대상	대상 트래픽을 선택하고 유지 를 클릭합니다. <ul style="list-style-type: none"> ■ 임의의 대상 주소로 보내는 트래픽을 허용하거나 거부하려면 모든 대상 토글을 설정합니다. ■ 특정 IP 집합 또는 보안 그룹으로 보내는 트래픽을 허용하거나 거부하려면 목록에서 IP 집합 및 보안 그룹을 선택합니다.
작업	작업 드롭다운 메뉴에서 특정 소스와 주고 받는 트래픽을 허용할지, 아니면 거부할지를 선택합니다. <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.
로깅 사용	이 규칙에 의해 수행된 주소 변환을 기록하려면 로깅 사용 토글을 설정합니다.

7 저장을 클릭합니다.

8 추가 규칙을 구성하려면 단계를 반복합니다.

결과

방화벽 규칙을 생성하면 분산 방화벽 규칙 목록에 나타납니다. 필요에 따라 규칙을 위 또는 아래로 이동하거나 규칙을 편집 또는 삭제할 수 있습니다.

기본 분산 방화벽 정책 비활성화

분산 방화벽 서비스를 비활성화하려면 먼저 기본 분산 방화벽 정책을 비활성화해야 합니다.

기본 정책을 비활성화하면 분산 방화벽 규칙을 편집할 수는 있지만 규칙이 더 이상 적용되지 않습니다.

절차

1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.

데이터 센터 그룹 목록이 나타납니다.

- 2 대상 데이터 센터 그룹을 클릭합니다.
- 3 왼쪽에서 **분산 방화벽** 탭을 클릭합니다.
- 4 분산 방화벽 규칙 목록 위의 **기본 정책** 카드에서 **사용 안 함**을 클릭하고 작업을 확인합니다.

결과

기본 정책이 비활성화됩니다. 나머지 분산 방화벽 규칙은 편집할 수 있지만 적용되지는 않습니다.

분산 방화벽 서비스 비활성화

분산 방화벽 서비스를 사용하지 않으려면 비활성화할 수 있습니다.

데이터 센터 그룹에 대한 분산 방화벽 서비스를 비활성화하면 이 그룹에 대한 보안 규칙 구성이 영구적으로 삭제되고 복구할 수 없습니다.

사전 요구 사항

기본 분산 방화벽 정책 비활성화

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
- 3 **일반**을 클릭합니다.
- 4 오른쪽에 있는 **분산 방화벽** 창에서 **비활성화**를 클릭하고 작업을 확인합니다.

결과

분산 방화벽 서비스가 비활성화되고 보안 규칙 구성이 삭제됩니다.

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹 네트워크 관리

데이터 센터 그룹을 만들고 구성한 후에는 참여 중인 VDC에 걸쳐 있는 데이터 센터 그룹 네트워크를 만들고 관리할 수 있습니다.

NSX-T Data Center에서 지원하는 라우팅, 격리 및 가져온 조직 데이터 센터 그룹 네트워크를 사용할 수 있습니다.

데이터 센터 그룹 네트워크는 단일 데이터 센터 그룹으로만 범위를 지정할 수 있습니다.

조직 VDC에서 데이터 센터 그룹으로 기존 네트워크의 범위를 늘릴 수 있습니다.

모든 유형의 네트워크를 데이터 센터 그룹에 추가할 수 있습니다.

중요 네트워크가 격리된 경우에도 데이터 센터 그룹에 참여하는 네트워크의 IP 주소는 겹치지 않아야 합니다.

표 5-2. 데이터 센터 그룹 네트워크 유형

데이터 센터 그룹 네트워크 유형	설명
격리됨	격리된 데이터 센터 그룹 네트워크에는 동일한 데이터 센터 그룹의 VDC에서만 액세스할 수 있습니다. 이 조직 VDC의 가상 시스템만 격리된 데이터 센터 그룹 네트워크에 연결하고 트래픽을 확인할 수 있습니다.
라우팅됨	라우팅된 데이터 센터 그룹 네트워크는 데이터 센터 그룹의 일부인 NSX-T Data Center Edge 게이트웨이를 통해 외부 네트워크에 대한 제어된 액세스를 제공합니다.
가져옴	가져온 데이터 센터 그룹 네트워크는 기존의 NSX-T Data Center 논리적 스위치를 사용합니다. 시스템 관리자만 네트워크를 가져올 수 있습니다.

NSX-T Data Center에서 지원되는 격리된 데이터 센터 그룹 네트워크 생성

데이터 센터 그룹의 VM에만 액세스할 수 있는 격리된 데이터 센터 그룹 네트워크를 추가할 수 있습니다. 이 네트워크 외부에 있는 VM은 동일한 데이터 센터 그룹의 다른 네트워크에 연결되어 있는지 여부에 관계 없이 연결되지 않습니다.

사전 요구 사항

- 조직 관리자 권한이 있는지 확인합니다.
- NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹을 생성했는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 **네트워크** 탭에서 **새로 만들기**를 클릭합니다.
- 3 **범위** 페이지에서 **데이터 센터 그룹**을 선택하고 네트워크를 생성할 NSX-T Data Center 네트워크 제공자가 포함된 그룹을 선택합니다.
- 4 **네트워크 유형** 페이지에서 **격리됨**을 선택한 후 **다음**을 클릭합니다.
- 5 네트워크의 의미 있는 이름을 입력합니다.
- 6 네트워크에 대한 CIDR(Classless Inter-Domain Routing) 설정을 입력합니다.
network_gateway_IP_address/subnet_prefix_length 형식(예: **192.167.1.1/24**)을 사용합니다.
- 7 조직 VDC 네트워크에 대한 설명을 입력합니다.
- 8 **다음**을 클릭합니다.
- 9 (선택 사항) 정적 IP 주소가 필요한 가상 시스템에 할당할 하나 이상의 IP 주소를 예약하려면 네트워크에 대한 **정적 IP 풀**을 구성합니다.
 - a IP 주소 또는 IP 주소 범위를 입력하고 **추가**를 클릭합니다.
여러 정적 IP 주소 또는 범위를 추가하려면 이 단계를 반복합니다.
 - b (선택 사항) IP 주소 및 범위를 수정하거나 제거하려면 **수정** 또는 **제거**를 클릭합니다.

10 (선택 사항) DNS 설정을 구성합니다.

옵션	작업
기본 DNS	기본 DNS 서버의 IP 주소를 입력합니다.
보조 DNS	보조 DNS 서버의 IP 주소를 입력합니다.
DNS 접미사	DNS 접미사를 입력합니다. DNS 접미사는 호스트 이름이 포함되지 않은 DNS 이름입니다.

11 완료 준비 페이지에서 설정을 검토하고 **마침**을 클릭합니다.

NSX-T Data Center에서 지원되는 라우팅된 데이터 센터 그룹 네트워크 생성

외부 네트워크에 대한 액세스를 제어하려면 라우팅된 데이터 센터 그룹 네트워크를 추가하면 됩니다.

사전 요구 사항

- **조직 관리자**이거나 동등한 권한 집합을 가진 역할이 있는지 확인합니다.
- NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹을 생성했는지 확인합니다.
- 기존 NSX-T Data Center Edge 게이트웨이의 범위를 라우팅된 네트워크를 생성하려는 데이터 센터 그룹으로 지정했는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 **네트워크** 탭에서 **새로 만들기**를 클릭합니다.
- 3 **범위** 페이지에서 **데이터 센터 그룹**을 선택하고 네트워크를 생성할 NSX-T Data Center 네트워크 제공자가 포함된 그룹을 선택합니다.
- 4 **네트워크 유형** 페이지에서 **라우팅됨**을 선택한 후 **다음**을 클릭합니다.
데이터 센터 그룹으로 범위가 지정된 사용 가능한 Edge 게이트웨이가 하나만 있으면 네트워크에 자동으로 할당됩니다.
- 5 데이터 센터 그룹에 사용할 수 있는 NSX-T Data Center가 둘 이상 있으면 목록에서 Edge 게이트웨이를 선택하고 **다음**을 클릭합니다.
- 6 네트워크의 의미 있는 이름을 입력합니다.
- 7 네트워크에 대한 CIDR(Classless Inter-Domain Routing) 설정을 입력합니다.
network_gateway_IP_address/subnet_prefix_length 형식(예: **192.167.1.1/24**)을 사용합니다.
- 8 조직 VDC 네트워크에 대한 설명을 입력합니다.
- 9 **다음**을 클릭합니다.

10 (선택 사항) 정적 IP 주소가 필요한 가상 시스템에 할당할 하나 이상의 IP 주소를 예약하려면 네트워크에 대한 **정적 IP 풀**을 구성합니다.

a IP 주소 또는 IP 주소 범위를 입력하고 **추가**를 클릭합니다.

여러 정적 IP 주소 또는 범위를 추가하려면 이 단계를 반복합니다.

b (선택 사항) IP 주소 및 범위를 수정하거나 제거하려면 **수정** 또는 **제거**를 클릭합니다.

11 (선택 사항) DNS 설정을 구성합니다.

옵션	작업
기본 DNS	기본 DNS 서버의 IP 주소를 입력합니다.
보조 DNS	보조 DNS 서버의 IP 주소를 입력합니다.
DNS 접미사	DNS 접미사를 입력합니다. DNS 접미사는 호스트 이름이 포함되지 않은 DNS 이름입니다.

12 완료 준비 페이지에서 설정을 검토하고 **마침**을 클릭합니다.

가져온 NSX-T 논리적 스위치를 사용하여 데이터 센터 그룹 네트워크 생성

시스템 관리자는 연결된 NSX-T Manager 인스턴스에서 세그먼트를 가져와서 조직 VDC 네트워크를 만들 수 있습니다.

사전 요구 사항

- **시스템 관리자** 권한이 있는지 확인합니다.
- NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹을 생성했는지 확인합니다.
- 대상 가상 데이터 센터 그룹을 지원하는 제공자 가상 데이터 센터가 NSX-T Manager 인스턴스와 연결되어 있는지 확인합니다.
- 다른 네트워크에 사용되지 않는 NSX-T 논리적 스위치를 하나 이상 생성했는지 확인합니다. NSX-T 논리적 스위치 생성 및 구성에 대한 자세한 내용은 "NSX-T Data Center 관리 가이드"의 내용을 참조하십시오.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 **네트워크** 탭에서 **새로 만들기**를 클릭합니다.
- 3 **범위** 페이지에서 **데이터 센터 그룹**을 선택하고 네트워크를 생성할 NSX-T Data Center 네트워크 제공자가 포함된 그룹을 선택합니다.
- 4 **네트워크 유형** 페이지에서 **가져옴**을 선택한 후 **다음**을 클릭합니다.
- 5 사용 가능한 NSX-T 논리적 스위치 목록에서 대상 스위치를 선택하고 **다음**을 클릭합니다.
- 6 네트워크의 의미 있는 이름을 입력합니다.

- 7 네트워크에 대한 CIDR(Classless Inter-Domain Routing) 설정을 입력합니다.

network_gateway_IP_address/subnet_prefix_length 형식(예: **192.167.1.1/24**)을 사용합니다.

- 8 조직 VDC 네트워크에 대한 설명을 입력합니다.

- 9 다음을 클릭합니다.

- 10 (선택 사항) 정적 IP 주소가 필요한 가상 시스템에 할당할 하나 이상의 IP 주소를 예약하려면 네트워크에 대한 **정적 IP 풀**을 구성합니다.

- a IP 주소 또는 IP 주소 범위를 입력하고 **추가**를 클릭합니다.

여러 정적 IP 주소 또는 범위를 추가하려면 이 단계를 반복합니다.

- b (선택 사항) IP 주소 및 범위를 수정하거나 제거하려면 **수정** 또는 **제거**를 클릭합니다.

- 11 (선택 사항) DNS 설정을 구성합니다.

옵션	작업
기본 DNS	기본 DNS 서버의 IP 주소를 입력합니다.
보조 DNS	보조 DNS 서버의 IP 주소를 입력합니다.
DNS 접미사	DNS 접미사를 입력합니다. DNS 접미사는 호스트 이름이 포함되지 않은 DNS 이름입니다.

- 12 **완료 준비** 페이지에서 설정을 검토하고 **마침**을 클릭합니다.

NSX-T Data Center에서 지원되는 조직 VDC 네트워크의 범위 늘리기

조직 VDC 네트워크의 범위를 데이터 센터 그룹 네트워크로 늘리면 데이터 센터 그룹에 참여하는 모든 데이터 센터의 워크로드를 연결할 수 있습니다.

사전 요구 사항

- **조직 관리자**이거나 동등한 권한 집합을 가진 역할이 있는지 확인합니다.
- NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹을 생성했는지 확인합니다.
- NSX-T Data Center에서 지원되는 조직 VDC 네트워크를 생성했는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 범위를 늘릴 조직 VDC 네트워크 옆에 있는 라디오 버튼을 클릭하고 **범위 늘리기**를 클릭합니다.
- 3 데이터 센터 그룹 목록에서 데이터 센터 그룹을 선택하고 **확인**을 클릭하여 확인합니다.

결과

네트워크 범위가 데이터 센터 그룹 네트워크로 늘어납니다. 네트워크 목록에, 선택한 데이터 센터 그룹으로 범위가 지정된 것으로 표시됩니다.

NSX-T Data Center에서 지원되는 데이터 센터 그룹 네트워크의 범위 줄이기

NSX-T Data Center에서 지원되는 데이터 센터 그룹 네트워크의 범위를 조직 VDC 네트워크로 줄일 수 있습니다.

데이터 센터 그룹 네트워크의 범위를 단일 조직 VDC 네트워크로 줄이면 조직 VDC에만 속하는 워크로드에 대한 네트워크 연결을 제공합니다.

사전 요구 사항

- **조직 관리자**이거나 동등한 권한 집합을 가진 역할이 있는지 확인합니다.
- VDC 네트워크를 생성하고 해당 범위를 NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹으로 지정했는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 범위를 줄일 데이터 센터 그룹 네트워크 옆에 있는 라디오 버튼을 클릭하고 **범위 줄이기**를 클릭합니다.
- 3 그룹 네트워크의 구성원인 VDC 목록에서 네트워크 범위를 지정할 VDC를 선택하고 **확인**을 클릭합니다.

결과

네트워크 범위가 단일 조직 VDC 네트워크로 줄어듭니다.

NSX-T Data Center 네트워크 제공자 유형을 사용하는 데이터 센터 그룹의 송신 지점 관리

데이터 센터 그룹 네트워크로 들어오거나 나가는 트래픽을 외부 네트워크로 라우팅하려는 경우 NSX-T Data Center Edge 게이트웨이를 데이터 센터 그룹의 송신 지점으로 구성할 수 있습니다.

Edge 게이트웨이가 데이터 센터 그룹의 송신 지점이 되도록 구성하면 해당 범위가 데이터 센터 그룹으로 늘어납니다. Edge 게이트웨이는 그룹에 참여하는 모든 데이터 센터에서 공유됩니다. Edge 게이트웨이에 연결된 모든 라우팅된 네트워크는 데이터 센터 그룹에 연결되고 여기로 범위가 지정됩니다.

모든 Edge 게이트웨이 서비스는 Edge 게이트웨이 기능의 일부를 유지합니다. 자세한 내용은 [NSX-T Data Center Edge 게이트웨이 관리](#) 항목을 참조하십시오.

VDC가 데이터 센터 그룹의 구성원이고 대상 범위에 속하지 않는 라우팅된 네트워크에 연결된 워크로드가 없는 경우 데이터 센터 그룹에서 Edge 게이트웨이를 제거하고 단일 VDC로 범위를 지정할 수 있습니다.

Edge 게이트웨이를 격리된 데이터 센터 그룹 네트워크에 추가하고 라우팅된 데이터 센터 네트워크로 변환할 수 있습니다. 또한 데이터 센터 그룹 네트워크에서 Edge 게이트웨이에 대한 연결을 제거하여 라우팅된 네트워크를 격리된 데이터 센터 그룹 네트워크로 변환할 수도 있습니다.

데이터 센터 그룹에 NSX-T Data Center Edge 게이트웨이 추가

NSX-T Data Center Edge 게이트웨이가 데이터 센터 그룹의 송신 지점이 되도록 구성하려면 Edge 게이트웨이의 범위를 늘립니다. 그러면 게이트웨이는 그룹에 참여하는 모든 데이터 센터에서 공유됩니다.

Edge 게이트웨이의 범위를 데이터 센터 그룹으로 지정하면 Edge 게이트웨이에 연결된 모든 라우팅된 네트워크가 데이터 센터 그룹에 연결되고 여기로 범위가 지정됩니다.

Edge 게이트웨이에 연결하는 새로운 모든 라우팅된 네트워크는 데이터 센터 그룹에 속합니다.

VDC로 범위가 지정된 Edge 게이트웨이에 연결된 라우팅된 네트워크는 Edge의 범위를 데이터 센터 그룹으로 늘린 경우에만 데이터 센터 그룹에 참여할 수 있습니다.

사전 요구 사항

기존 NSX-T Data Center Edge 게이트웨이를 데이터 센터 그룹에 참여하는 VDC 중 하나와 연결했는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
- 3 **Edge 게이트웨이**를 클릭한 다음 **Edge 추가**를 클릭합니다.
- 4 사용 가능한 Edge 게이트웨이 중 하나를 선택하고 **저장**을 클릭합니다.

결과

Edge 게이트웨이 범위가 데이터 센터 그룹으로 늘어납니다. 범위 변경은 기존의 기본 서비스 또는 네트워크에는 영향을 주지 않습니다.

특정 VDC로 NSX-T Data Center Edge 게이트웨이의 범위 줄이기

범위가 지정된 데이터 센터 그룹에서 Edge 게이트웨이를 제거하여 NSX-T Data Center Edge 게이트웨이의 범위를 특정 VDC로 줄일 수 있습니다.

Edge 게이트웨이의 범위를 특정 VDC로 줄이면 Edge 게이트웨이에서 사용 중인 모든 보안 그룹 개체가 그대로 유지됩니다. 분산 방화벽에 의해 독점적으로 사용되는 보안 그룹은 VDC 그룹의 일부로 유지됩니다.

사전 요구 사항

- 범위를 줄이기 위해 Edge 게이트웨이의 범위로 설정할 대상 VDC가 데이터 센터 그룹의 구성원인지 확인합니다.
- 대상 Edge 게이트웨이 범위에 속하지 않은 라우팅된 네트워크에 연결된 워크로드가 없는지 확인합니다.
- Edge 게이트웨이와 분산 방화벽 둘 다에서 사용 중인 데이터 센터 그룹에 보안 그룹 또는 IP 집합이 없는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
- 3 **Edge 게이트웨이**를 클릭한 다음 **Edge 제거**를 클릭합니다.
- 4 범위를 줄이기 위해 Edge 게이트웨이 범위로 설정할 VDC를 선택하고 **저장**을 클릭합니다.

NSX Data Center for vSphere를 사용하여 데이터 센터 그룹 네트워킹 관리

여러 조직 가상 데이터 센터 간에 네트워크를 만들려면 먼저 가상 데이터 센터를 그룹화한 다음 데이터 센터 그룹으로 범위가 지정된 VDC 네트워크를 만듭니다.

VMware Cloud Director는 단일 네트워크 장애 도메인에 대한 활성 송신 지점 및 대기 송신 지점을 모두 사용하여 NSX Data Center for vSphere에서 지원하는 조직 가상 데이터 센터에 대한 데이터 센터 그룹 네트워킹을 지원합니다.

NSX Data Center for vSphere에서 지원하는 데이터 센터 그룹에는 공통 송신 지점을 구성하거나 각 네트워크 장애 도메인 또는 로컬 그룹에 하나의 송신 지점을 구성할 수 있습니다.

데이터 센터 그룹

데이터 센터 그룹은 중앙 집중식 네트워킹 관리, 여러 가상 데이터 센터의 여러 송신 지점에 대한 구성, 그룹 내의 모든 네트워크 간의 동-서 트래픽을 제공하는 가상 데이터 센터 그룹 라우터 역할을 합니다. 데이터 센터 그룹은 여러 송신 지점을 공유하도록 구성된 1~16개의 가상 데이터 센터를 포함할 수 있습니다. 데이터 센터 그룹은 다음의 송신 지점 구성 중 하나를 사용할 수 있습니다.

표 5-3. NSX Data Center for vSphere에서 지원하는 데이터 센터 그룹에 대한 송신 지점 구성 유형

송신 지점 구성 유형	설명
일반 송신 지점 구성	<p>하나의 능동 송신 지점과 하나의 대기 송신 지점이 있는 데이터 센터 그룹을 구성할 수 있습니다. 이 두 송신 지점은 데이터 센터 그룹의 네트워크 장애 도메인 전체의 참여 중인 가상 데이터 센터가 공통으로 사용합니다.</p> <p>이 구성을 사용하는 데이터 센터 그룹에는 최대 4개의 네트워크 장애 도메인에 속한 데이터 센터가 포함될 수 있습니다.</p>
장애 도메인당 송신 지점이 있는 구성	<p>데이터 센터 그룹의 각 네트워크 장애 도메인에 대해 하나의 능동 송신 지점과 하나의 대기 송신 지점이 있는 데이터 센터 그룹을 구성할 수 있습니다.</p> <p>이 구성을 사용하는 데이터 센터 그룹에는 최대 4개의 네트워크 장애 도메인에 속한 데이터 센터가 포함될 수 있습니다.</p>
로컬 그룹 구성	<p>로컬 데이터 센터 그룹의 조직 가상 데이터 센터는 단일 vCenter Server 인스턴스에서 지원합니다. 단일 네트워크 장애 도메인에 대해 하나의 능동 송신 지점과 하나의 대기 송신 지점이 있는 로컬 데이터 센터 그룹을 구성할 수 있습니다.</p>

조직에서는 여러 개의 데이터 센터 그룹을 가질 수 있습니다. 조직 가상 데이터 센터는 여러 데이터 센터 그룹에 참여할 수 있습니다.

참여하는 조직 가상 데이터 센터는 서로 다른 VMware Cloud Director 사이트에 속할 수 있습니다. **다중 사이트 배포 구성 및 관리**의 내용을 참조하십시오.

네트워크 장애 도메인

네트워크 제공자 범위로, 일반적으로 기본 vCenter Server 인스턴스 및 연결된 NSX Manager를 나타냅니다.

송신 지점

데이터 센터 그룹 또는 네트워크 장애 도메인을 인터넷에 연결하는 Edge 게이트웨이입니다. Edge 게이트웨이는 데이터 센터 그룹의 가상 데이터 센터에 속해 있어야 합니다. 송신 지점을 나타내는 Edge 게이트웨이 및 가상 데이터 센터 그룹 또는 네트워크 장애 도메인의 범용 라우터에 BGP 경로가 구성됩니다. Edge 게이트웨이의 기존 경로는 영향을 받지 않습니다.

스트레치된 네트워크

데이터 센터 그룹 내의 모든 가상 데이터 센터에 스트레치되는 레이어 2 네트워크입니다. IPv4만 가능합니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹 관리

NSX Data Center for vSphere가 지원하는 데이터 센터 그룹을 만든 후 데이터 센터 그룹의 네트워크 토폴로지를 편집할 수 있습니다. 그룹에서 가상 데이터 센터를 추가 및 제거할 수 있습니다. 송신 지점을 스왑, 교체 및 제거할 수 있습니다. 여러 동기화 작업을 수행하여 구성 실패 문제를 해결할 수 있습니다.

일반 송신 구성을 장애 도메인당 송신 구성으로 변환하거나 그 반대로 변환할 수 없습니다.

일반 송신 구성을 사용하는 NSX Data Center for vSphere가 지원하는 데이터 센터 그룹 만들기 및 구성

일반 송신 구성을 사용하는 NSX Data Center for vSphere가 지원하는 가상 데이터 센터 그룹을 만들고 구성할 수 있습니다. 이 경우 활성 송신 지점 및 대기 송신 지점 역할을 하는 Edge 게이트웨이 쌍을 참여하는 모든 가상 데이터 센터에 설정합니다.

사전 요구 사항

- 이 작업에는 **시스템 관리자** 역할 또는 조직에 **vDC 그룹: vDC 그룹 구성** 권한이 게시된 역할이 필요합니다.
- **시스템 관리자**는 대상 가상 데이터 센터에서 크로스 가상 데이터 센터 네트워킹을 사용하도록 설정해야 합니다.

절차

- 1 일반 송신 구성을 사용하는 NSX Data Center for vSphere가 지원하는 데이터 센터 그룹 만들기
일반 송신 구성을 사용하는 데이터 센터 그룹에는 1-16개의 가상 데이터 센터를 그룹화할 수 있습니다.
- 2 NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에 활성 송신 지점 추가
데이터 센터 그룹을 인터넷에 연결하려면 해당 네트워크 토폴로지에 활성 송신 지점을 추가해야 합니다.
- 3 NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에 대기 송신 지점 추가
일반 송신 지점 구성을 사용하는 가상 데이터 센터 그룹에는 Fault Tolerance 시나리오의 대기 송신 지점 역할을 하는 보조 송신 지점을 추가할 수 있습니다.

일반 송신 구성을 사용하는 NSX Data Center for vSphere가 지원하는 데이터 센터 그룹 만들기

일반 송신 구성을 사용하는 데이터 센터 그룹에는 1-16개의 가상 데이터 센터를 그룹화할 수 있습니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 **새로 만들기**를 클릭합니다.
- 3 **VDC 시작** 페이지에서 VDC 그룹을 시작할 VDC를 선택합니다.
- 4 새 데이터 센터 그룹의 이름과 설명(선택 사항)을 입력합니다.
- 5 **일반 송신 지점**을 선택하고 **다음**을 클릭합니다.

- 6 참여 중인 VDC** 페이지에서 새 데이터 센터 그룹에 대한 추가 데이터 센터를 선택하고 **다음**을 클릭합니다.

데이터 센터 페이지에는 **시스템 관리자**가 크로스 가상 데이터 센터 네트워킹에 대해 사용하도록 설정한 VDC 목록이 포함되어 있습니다.

- 7** 데이터 센터 그룹 세부 정보를 검토하고 **마침**을 클릭합니다.

결과

새로 생성된 가상 데이터 센터 그룹이 **데이터 센터 그룹** 보기에 나열됩니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에 활성 송신 지점 추가

데이터 센터 그룹을 인터넷에 연결하려면 해당 네트워크 토폴로지에 활성 송신 지점을 추가해야 합니다.

사전 요구 사항

시스템 관리자가 데이터 센터 그룹에 참여 중인 가상 데이터 센터 중 하나에 Edge 게이트웨이를 하나 이상 만들었어야 합니다.

절차

- 1** 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.

데이터 센터 그룹 목록이 나타납니다.

- 2** 대상 데이터 센터 그룹을 클릭합니다.

이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.

- 3** **송신 지점 추가**를 클릭합니다.

활성 송신 지점 추가 페이지가 열리고, 참여 중인 가상 데이터 센터에 속한 Edge 게이트웨이의 목록이 표시됩니다.

- 4** 이 데이터 센터 그룹의 활성 송신 지점 역할을 할 Edge 게이트웨이를 선택하고 **추가**를 클릭합니다.

결과

송신 지점을 나타내는 Edge 게이트웨이 및 가상 데이터 센터 그룹의 범용 라우터에 BGP 경로가 구성됩니다. Edge 게이트웨이의 기존 경로는 영향을 받지 않습니다.

새로 추가한 송신 지점이 네트워크 토폴로지 다이어그램에 업데이트됩니다. 참여 중인 가상 데이터 센터가 인터넷에 보내는 트래픽은 파란색 실선으로 표시됩니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에 대기 송신 지점 추가

일반 송신 지점 구성을 사용하는 가상 데이터 센터 그룹에는 Fault Tolerance 시나리오의 대기 송신 지점 역할을 하는 보조 송신 지점을 추가할 수 있습니다.

사전 요구 사항

활성 송신 지점 역할을 하는 Edge 게이트웨이와는 별도로, 그룹에 참여 중인 가상 데이터 센터 중 하나에 Edge 게이트웨이가 하나 이상 있어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.

데이터 센터 그룹 목록이 나타납니다.

- 2 대상 데이터 센터 그룹을 클릭합니다.

이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.

- 3 **대기 송신 지점 추가**를 클릭합니다.

대기 송신 지점 추가 페이지가 열리고, 참여 중인 가상 데이터 센터에 속한 Edge 게이트웨이 중 현재 사용 중이 아닌 Edge 게이트웨이의 목록이 표시됩니다. 이 가상 데이터 센터 그룹의 능동 송신 지점에서 사용 중인 Edge 게이트웨이는 표시되지 않습니다.

- 4 이 데이터 센터 그룹의 대기 송신 지점 역할을 할 Edge 게이트웨이를 선택하고 **추가**를 클릭합니다.

결과

송신 지점을 나타내는 Edge 게이트웨이 및 네트워크 장애 도메인의 범용 라우터에 BGP 경로가 구성됩니다. 구성은 Edge 게이트웨이의 기존 경로에 영향을 주지 않습니다.

새로 추가한 송신 지점이 네트워크 토폴로지 다이어그램에 업데이트됩니다. Fault Tolerance 시나리오에 서 참여 중인 가상 데이터 센터가 인터넷에 보내는 트래픽은 파란색 점선으로 표시됩니다.

장애 도메인 송신 구성을 사용하는 NSX Data Center for vSphere가 지원하는 데이터 센터 그룹 만들기 및 구성

장애 도메인 송신 구성을 사용하는 NSX Data Center for vSphere가 지원하는 가상 데이터 센터 그룹을 만들고 구성할 수 있습니다. 이 경우 활성 송신 지점 역할을 하는 Edge 게이트웨이를 그룹의 각 네트워크 장애 도메인에 구성합니다. 장애 도메인 송신 구성을 사용하는 데이터 센터 그룹에는 대기 송신을 생성할 수 없습니다.

사전 요구 사항

이 작업에는 **시스템 관리자** 역할 또는 조직에 **vDC 그룹: vDC 그룹 구성** 권한이 게시된 역할이 필요합니다.

절차

- 1 장애 도메인 송신 구성을 사용하는 NSX Data Center for vSphere가 지원하는 데이터 센터 그룹 만들기

장애 도메인 송신 구성을 사용하는 NSX Data Center for vSphere가 지원하는 데이터 센터 그룹에는 1-16개의 가상 데이터 센터를 그룹화할 수 있습니다.

2 장애 도메인에 송신 지점 추가

NSX Data Center for vSphere가 지원하는 데이터 센터 그룹의 네트워크 장애 도메인에서 가상 데이터 센터를 인터넷에 연결하려면 네트워크 장애 도메인에 송신 지점을 추가해야 합니다. 데이터 센터 그룹에 있는 각 네트워크 장애 도메인에 송신 지점을 추가할 수 있습니다. 장애 도메인 송신 구성이 설정된 데이터 센터 그룹에는 대기 송신 지점이 지원되지 않습니다.

장애 도메인 송신 구성을 사용하는 NSX Data Center for vSphere가 지원하는 데이터 센터 그룹 만들기

장애 도메인 송신 구성을 사용하는 NSX Data Center for vSphere가 지원하는 데이터 센터 그룹에는 1-16 개의 가상 데이터 센터를 그룹화할 수 있습니다.

사전 요구 사항

시스템 관리자가 크로스 가상 데이터 센터 네트워킹을 사용하도록 대상 가상 데이터 센터를 설정했습니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 **새로 만들기**를 클릭합니다.
- 3 새 데이터 센터 그룹의 이름과 설명(선택 사항)을 입력합니다.
- 4 **장애 도메인당 송신 지점**을 선택하고 **다음**을 클릭합니다.
- 5 **참여 중인 VDC** 페이지에서 새 데이터 센터 그룹에 대한 추가 데이터 센터를 선택하고 **다음**을 클릭합니다.
데이터 센터 페이지에는 **시스템 관리자**가 크로스 가상 데이터 센터 네트워킹에 대해 사용하도록 설정한 VDC 목록이 포함되어 있습니다.
- 6 데이터 센터 그룹 세부 정보를 검토하고 **마침**을 클릭합니다.

결과

새로 생성된 가상 데이터 센터 그룹이 **데이터 센터 그룹** 보기에 나열됩니다.

장애 도메인에 송신 지점 추가

NSX Data Center for vSphere가 지원하는 데이터 센터 그룹의 네트워크 장애 도메인에서 가상 데이터 센터를 인터넷에 연결하려면 네트워크 장애 도메인에 송신 지점을 추가해야 합니다. 데이터 센터 그룹에 있는 각 네트워크 장애 도메인에 송신 지점을 추가할 수 있습니다. 장애 도메인 송신 구성이 설정된 데이터 센터 그룹에는 대기 송신 지점이 지원되지 않습니다.

사전 요구 사항

이 데이터 센터 그룹에서 송신 지점으로 사용 중인 **Edge** 게이트웨이와는 별도로, 참여 중인 가상 데이터 센터 중 하나에 현재 사용되지 않는 **Edge** 게이트웨이가 하나 이상 있어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.
- 3 네트워크 토폴로지 다이어그램에서 대상 네트워크 장애 도메인을 클릭합니다.
네트워크 장애 도메인은 실선으로 표시되며, 다이어그램 하단에 해당 이름이 나와 있습니다.
선택한 장애 도메인이 파란색으로 표시됩니다.
- 4 **송신 지점 추가**를 클릭합니다.
활성 송신 지점 추가 페이지가 열리고, 참여 중인 가상 데이터 센터에 속한 Edge 게이트웨이의 목록이 표시됩니다.
- 5 이 장애 도메인의 송신 지점 역할을 할 Edge 게이트웨이를 선택하고 **추가**를 클릭합니다.

결과

송신 지점을 나타내는 Edge 게이트웨이 및 네트워크 장애 도메인의 범용 라우터에 BGP 경로가 구성됩니다. Edge 게이트웨이의 기존 경로는 영향을 받지 않습니다.

새로 추가한 송신 지점이 네트워크 토폴로지 다이어그램에 업데이트됩니다. 네트워크 장애 도메인의 가상 데이터 센터가 인터넷에 보내는 트래픽은 파란색 실선으로 표시됩니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 로컬 가상 데이터 센터 그룹 생성 및 구성

버전 10.1부터 VMware Cloud Director는 단일 네트워크 장애 도메인에 대해 활성 및 대기 송신 지점이 모두 있는 NSX Data Center for vSphere가 지원하는 데이터 센터 그룹을 지원합니다.

로컬 그룹의 조직 가상 데이터 센터는 단일 vCenter Server 인스턴스에서 지원합니다.

로컬 데이터 센터 그룹에서 Edge 게이트웨이 쌍(능동 송신 지점 및 대기 송신 지점)을 설정하여 동일한 네트워크 장애 도메인 내에서 고가용성 및 재해 복구 시나리오를 지원할 수 있습니다.

사전 요구 사항

이 작업에는 **시스템 관리자** 역할 또는 조직에 **vDC 그룹: vDC 그룹 구성** 권한이 게시된 역할이 필요합니다.

절차

- 1 **NSX Data Center for vSphere** 네트워크 제공자 유형을 사용하는 로컬 데이터 센터 그룹 만들기
장애 도메인 송신 구성을 사용하는 NSX Data Center for vSphere가 지원하는 데이터 센터 그룹에는 1-16개의 VDC(가상 데이터 센터)를 그룹화할 수 있습니다.

2 NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 로컬 데이터 센터 그룹에 대한 활성 송신 지점 추가

NSX Data Center for vSphere가 지원하는 로컬 데이터 센터 그룹의 데이터 센터를 인터넷에 연결하려면 해당 네트워크 장애 도메인에 활성 송신 지점을 추가해야 합니다.

3 NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 로컬 데이터 센터 그룹에 대한 대기 송신 지점 추가

로컬 데이터 센터 그룹 구성에서 Fault Tolerance 시나리오의 대기 송신 지점 역할을 하는 보조 송신 지점을 추가할 수 있습니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 로컬 데이터 센터 그룹 만들기

장애 도메인 송신 구성을 사용하는 NSX Data Center for vSphere가 지원하는 데이터 센터 그룹에는 1-16 개의 VDC(가상 데이터 센터)를 그룹화할 수 있습니다.

사전 요구 사항

시스템 관리자가 크로스 가상 데이터 센터 네트워킹을 사용하도록 대상 가상 데이터 센터를 설정했습니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 **새로 만들기**를 클릭합니다.
- 3 **VDC 시작** 페이지에서 VDC 그룹을 시작할 VDC를 선택합니다.
- 4 새 데이터 센터 그룹의 이름과 설명(선택 사항)을 입력합니다.
- 5 단일 네트워크 장애 도메인의 가상 데이터 센터만 포함하는 그룹을 만들려면 **로컬 그룹 만들기** 옵션을 전환합니다.
- 6 **다음**을 클릭합니다.
- 7 **참여 중인 VDC** 페이지에서 새 데이터 센터 그룹에 대한 추가 데이터 센터를 선택하고 **다음**을 클릭합니다.
데이터 센터 페이지에는 **시스템 관리자**가 크로스 가상 데이터 센터 네트워킹에 대해 사용하도록 설정한 VDC 목록이 포함되어 있습니다.
- 8 데이터 센터 그룹 세부 정보를 검토하고 **마침**을 클릭합니다.

결과

새로 생성된 가상 데이터 센터 그룹이 **데이터 센터 그룹** 보기에 나타납니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 로컬 데이터 센터 그룹에 대한 활성 송신 지점 추가

NSX Data Center for vSphere가 지원하는 로컬 데이터 센터 그룹의 데이터 센터를 인터넷에 연결하려면 해당 네트워크 장애 도메인에 활성 송신 지점을 추가해야 합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.

데이터 센터 그룹 목록이 나타납니다.

- 2 대상 데이터 센터 그룹을 클릭합니다.

이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.

- 3 **송신 지점 추가**를 클릭합니다.

- 4 참여 중인 가상 데이터 센터에 속한 **Edge** 게이트웨이 목록에서 데이터 센터 그룹에 대한 능동 송신 지점 역할을 할 **Edge** 게이트웨이를 선택하고 **추가**를 클릭합니다.

결과

송신 지점을 나타내는 **Edge** 게이트웨이 및 네트워크 장애 도메인의 범용 라우터에 **BGP** 경로가 구성됩니다. 구성은 **Edge** 게이트웨이의 기존 경로에 영향을 주지 않습니다.

새로 추가된 활성 송신 지점이 네트워크 토폴로지의 다이어그램에 나타납니다. 파란색 연속 선은 네트워크 장애 도메인의 가상 데이터 센터에서 인터넷으로 향하는 트래픽을 나타냅니다.

다음에 수행할 작업

송신 지점 **Fault Tolerance**를 허용하려면 로컬 데이터 센터 그룹에 대해 대기 송신 지점을 추가합니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 로컬 데이터 센터 그룹에 대한 대기 송신 지점 추가

로컬 데이터 센터 그룹 구성에서 **Fault Tolerance** 시나리오의 대기 송신 지점 역할을 하는 보조 송신 지점을 추가할 수 있습니다.

사전 요구 사항

활성 송신 지점 역할을 하는 **Edge** 게이트웨이와는 별도로, 로컬 데이터 센터 그룹에 참여 중인 가상 데이터 센터 중 하나에 **Edge** 게이트웨이가 하나 이상 있어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.

데이터 센터 그룹 목록이 나타납니다.

- 2 대상 데이터 센터 그룹을 클릭합니다.

이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.

3 대기 송신 지점 추가를 클릭합니다.

대기 송신 지점 추가 페이지가 열리고, 참여 중인 가상 데이터 센터에 속한 Edge 게이트웨이 중 현재 사용 중이 아닌 Edge 게이트웨이의 목록이 표시됩니다. 이 가상 데이터 센터 그룹의 능동 송신 지점에서 사용 중인 Edge 게이트웨이는 흐리게 나타납니다.

4 이 데이터 센터 그룹의 대기 송신 지점 역할을 할 Edge 게이트웨이를 선택하고 **추가**를 클릭합니다.

결과

송신 지점을 나타내는 Edge 게이트웨이 및 네트워크 장애 도메인의 범용 라우터에 BGP 경로가 구성됩니다. 구성은 Edge 게이트웨이의 기존 경로에 영향을 주지 않습니다.

새로 추가된 송신 지점이 네트워크 토폴로지 다이어그램에 나타납니다. 파란색 파선은 Fault Tolerance 시나리오에서 참여 중인 가상 데이터 센터에서 인터넷으로 향하는 트래픽을 나타냅니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹 보기

조직의 데이터 센터 그룹 및 이 그룹의 현재 구성에 대한 세부 정보를 볼 수 있습니다.

사전 요구 사항

이 작업에는 **시스템 관리자** 역할 또는 조직에 **vDC 그룹: vDC 그룹 보기** 권한이 게시된 역할이 필요합니다.

절차

1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.

데이터 센터 그룹 목록이 나타납니다.

2 대상 데이터 센터 그룹을 클릭합니다.

이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에 가상 데이터 센터 추가

기존 네트워크를 새 가상 데이터 센터로 스트레칭한 경우, 데이터 센터 그룹에 가상 데이터 센터를 추가할 수 있습니다.

사전 요구 사항

- 이 작업에는 **시스템 관리자** 역할 또는 조직에 **vDC 그룹: vDC 그룹 구성** 권한이 게시된 역할이 필요합니다.
- 데이터 센터 그룹의 가상 데이터 센터 수가 4개 미만이어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.

데이터 센터 그룹 목록이 나타납니다.

- 2 대상 데이터 센터 그룹을 클릭합니다.

이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.

- 3 **데이터 센터 추가**를 클릭합니다.

- 4 **데이터 센터** 페이지에서 데이터 센터 그룹에 추가할 데이터 센터를 선택하고 **마침**을 클릭합니다.

데이터 센터 페이지에는 시스템 관리자가 크로스 가상 데이터 센터 네트워킹에 사용할 수 있게 설정한 가상 데이터 센터 목록이 있습니다.

참고 데이터 센터 그룹에는 가상 데이터 센터를 4개까지 포함할 수 있습니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에서 가상 데이터 센터 제거

가상 데이터 센터에서 기존 네트워크를 스트레치 취소하여 데이터 센터 그룹에서 해당 가상 데이터 센터를 제거할 수 있습니다.

사전 요구 사항

- 이 작업에는 **시스템 관리자** 역할 또는 조직에 **vDC 그룹: vDC 그룹 구성** 권한이 게시된 역할이 필요합니다.
- 데이터 센터 그룹에 3개 이상의 가상 데이터 센터가 포함되어야 합니다.
- 제거하려는 가상 데이터 센터는 데이터 센터 그룹에 송신 지점을 제공하지 않아야 합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.

데이터 센터 그룹 목록이 나타납니다.

- 2 대상 데이터 센터 그룹을 클릭합니다.

이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.

- 3 대상 가상 데이터 센터 카드의 오른쪽 위에서 점 세 개를 클릭한 후 **제거**를 클릭합니다.

- 4 **제거**를 클릭하여 확인합니다.

결과

가상 데이터 센터가 데이터 센터 그룹의 네트워크 토폴로지 다이어그램에서 제거됩니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹 동기화

데이터 센터 그룹 네트워크 구성을 다시 적용하고 참여 중인 모든 가상 데이터 센터가 활성 상태를 유지하도록 하려면 데이터 센터 그룹을 동기화하면 됩니다.

참고 데이터 센터 그룹 동기화 프로세스 중에는 범용 라우터가 NSX에서 동기화되기 때문에 데이터 센터 그룹을 몇 초 동안 사용할 수 없습니다.

사전 요구 사항

이 작업에는 **시스템 관리자** 역할 또는 조직에 **vDC 그룹: vDC 그룹 구성** 권한이 게시된 역할이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.

데이터 센터 그룹 목록이 나타납니다.

- 2 대상 데이터 센터 그룹을 클릭합니다.

이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.

- 3 **데이터 센터 그룹 동기화**를 클릭합니다.

- 4 **확인**을 클릭하여 확인합니다.

NSX Data Center for vSphere 네트워크 제공자 유형 및 일반 송신 구성을 사용하는 데이터 센터 그룹의 송신 지점 스왑

일반 송신 구성을 사용하여 데이터 센터 그룹에 활성 송신 지점과 대기 송신 지점을 구성한 후 송신 지점의 역할을 스왑할 수 있습니다. 활성 송신 지점을 대기 송신 지점으로 만들거나 그 반대로 바꿀 수 있습니다.

사전 요구 사항

이 작업에는 **시스템 관리자** 역할 또는 조직에 **vDC 그룹: vDC 그룹 구성** 권한이 게시된 역할이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.

데이터 센터 그룹 목록이 나타납니다.

- 2 대상 데이터 센터 그룹을 클릭합니다.

이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.

3 **송신 지점 스왑**을 클릭합니다.

4 **확인**을 클릭하여 확인합니다.

결과

새 트래픽 경로가 네트워크 토폴로지 다이어그램에 업데이트됩니다. 이제 인터넷 트래픽이 새 활성 송신 지점에 리디렉션됩니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹의 송신 지점에 대한 Edge 게이트웨이 바꾸기

데이터 센터 그룹에서 활성 또는 대기 송신 지점을 나타내는 Edge 게이트웨이를 바꿀 수 있습니다.

사전 요구 사항

- 이 작업에는 **시스템 관리자** 역할 또는 조직에 **vDC 그룹: vDC 그룹 구성** 권한이 게시된 역할이 필요합니다.
- 새 Edge 게이트웨이는 데이터 센터 그룹에서 다른 송신 지점에 사용 중이 아니어야 합니다.

절차

1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.

데이터 센터 그룹 목록이 나타납니다.

2 대상 데이터 센터 그룹을 클릭합니다.

이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.

3 네트워크 장애 도메인 구성에서 송신 지점을 바꾸는 경우, 네트워크 토폴로지 다이어그램에서 대상 송신 지점의 네트워크 장애 도메인을 선택합니다.

네트워크 장애 도메인은 실선으로 표시되며, 다이어그램 하단에 도메인 이름이 표시됩니다.

선택한 네트워크 장애 도메인은 파란색으로 표시됩니다.

4 대상 송신 지점 카드의 오른쪽 위에서 점 세 개를 클릭한 후 **바꾸기**를 클릭합니다.

송신 지점 바꾸기 페이지가 열리고, 참여 중인 가상 데이터 센터에 속한 Edge 게이트웨이의 목록이 표시됩니다.

5 새 Edge 게이트웨이를 선택하고 **바꾸기**를 클릭합니다.

결과

BGP 경로가 이전 Edge 게이트웨이에서 제거되고, 송신 지점을 나타내는 새 Edge 게이트웨이 및 가상 데이터 센터 그룹의 범용 라우터에 구성됩니다.

네트워크 토폴로지 다이어그램이 새 Edge 게이트웨이의 이름으로 업데이트됩니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹에서 송신 지점 제거

데이터 센터 그룹 또는 네트워크 장애 도메인의 인터넷 연결을 끊으려면 해당 송신 지점을 제거하면 됩니다.

사전 요구 사항

- 이 작업에는 **시스템 관리자** 역할 또는 조직에 **vDC 그룹: vDC 그룹 구성** 권한이 게시된 역할이 필요합니다.
- 대기 송신 지점과 쌍으로 구성된 활성 송신 지점을 제거하려는 경우에는 송신 지점을 스왑하거나 대기 송신 지점을 제거해야 합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.
- 3 네트워크 장애 도메인 구성에서 송신 지점을 제거하는 경우, 네트워크 토폴로지 다이어그램에서 대상 송신 지점의 네트워크 장애 도메인을 선택합니다.
네트워크 장애 도메인은 실선으로 표시되며, 다이어그램 하단에 도메인 이름이 표시됩니다.
선택한 네트워크 장애 도메인은 파란색으로 표시됩니다.
- 4 대상 송신 지점 카드의 오른쪽 위에서 점 세 개를 클릭한 후 **삭제**를 클릭합니다.
- 5 **확인**을 클릭하여 확인합니다.

결과

다른 범용 라우터에서 사용 중이 아닌 경우, 송신 지점을 나타내는 Edge 게이트웨이에서 BGP 경로가 제거됩니다.

송신 지점이 네트워크 토폴로지 다이어그램에서 제거됩니다.

NSX Data Center for vSphere 네트워크 제공자 유형을 사용하는 데이터 센터 그룹의 경로 및 송신 지점 동기화

경로를 동기화하여 데이터 센터 그룹이나 네트워크 장애 도메인 및 연결된 송신 지점에 동적 라우팅 구성을 다시 적용할 수 있습니다. 송신 지점을 동기화하면 송신 지점이 데이터 센터 그룹에 제대로 연결되도록 할 수 있습니다.

사전 요구 사항

- 이 작업에는 **시스템 관리자** 역할 또는 조직에 **vDC 그룹: vDC 그룹 구성** 권한이 게시된 역할이 필요합니다.
- 대상 데이터 센터 그룹 또는 네트워크 장애 도메인에 대해 송신 지점이 구성되어 있습니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭한 다음, **데이터 센터 그룹** 탭을 클릭합니다.
데이터 센터 그룹 목록이 나타납니다.
- 2 대상 데이터 센터 그룹을 클릭합니다.
이 데이터 센터 그룹에 대한 **네트워크 토폴로지** 보기가 열립니다. 현재 네트워크 토폴로지의 다이어그램이 참여 중인 VDC와 해당 네트워크 장애 도메인, 송신 지점(구성된 경우) 및 트래픽 경로를 표시합니다.
- 3 데이터 센터 그룹 내의 네트워크 도메인 그룹을 동기화하는 경우, 네트워크 토폴로지 다이어그램에서 대상 네트워크 장애 도메인을 선택합니다.
네트워크 장애 도메인은 실선으로 표시되며, 다이어그램 하단에 도메인 이름이 표시됩니다.
선택한 네트워크 장애 도메인은 파란색으로 표시됩니다.
- 4 그룹 또는 네트워크 장애 도메인 및 연결된 송신 지점에 동적 라우팅 구성을 다시 적용하려면 **경로 동기화**를 클릭한 후 **확인**을 클릭합니다.
- 5 송신 지점을 해당 데이터 센터 그룹과 동기화하려면 대상 송신 지점 카드의 오른쪽 위에서 점 세 개를 클릭하고 **동기화**를 클릭한 후 **확인**을 클릭합니다.

NSX Data Center for vSphere에서 지원하는 데이터 센터 그룹 네트워크 관리

데이터 센터 그룹을 만들고 구성한 후에는 참여 중인 가상 데이터 센터에 걸쳐 있는 VDC 그룹 레이어 2 네트워크를 만들고 관리할 수 있습니다.

NSX Data Center for vSphere에서 지원하는 VDC 그룹 네트워크 추가

데이터 센터 그룹에 참여하는 모든 가상 데이터 센터에서 VDC 그룹 네트워크를 만들 수 있습니다.

NSX Data Center for vSphere에서 지원하는 IPv4 데이터 센터 그룹 네트워크만 추가할 수 있습니다.

사전 요구 사항

이 작업에는 미리 정의된 **조직 관리자** 역할 또는 **조직 VDC 네트워크: 속성 편집** 권한이 있는 역할이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 **네트워크** 탭에서 **새로 만들기**를 클릭합니다.

- 3 범위 페이지에서 **데이터 센터 그룹**을 선택하고 네트워크를 생성할 NSX Data Center for vSphere에서 지원하는 데이터 센터 그룹을 선택한 후 **다음**을 클릭합니다.
- 4 네트워크의 의미 있는 이름을 입력합니다.
- 5 네트워크에 대한 CIDR(Classless Inter-Domain Routing) 설정을 입력합니다.
network_gateway_IP_address/subnet_prefix_length 형식(예: **192.167.1.1/24**)을 사용합니다.
- 6 조직 VDC 네트워크에 대한 설명을 입력합니다.
- 7 **다음**을 클릭합니다.
- 8 설정을 검토하고 **마침**을 클릭합니다.

결과

조직의 네트워크 목록에서 새로 만든 데이터 센터 그룹 네트워크를 볼 수 있습니다.

해당 네트워크 유형은 크로스 VDC로 나열됩니다.

참여 중인 각 가상 데이터 센터에 대해 크로스 VDC 라우팅 유형의 조직 가상 데이터 센터 네트워크가 만들어집니다. 참여 중인 가상 데이터 센터의 카드를 클릭한 다음 **네트워크**를 클릭하여 참여 중인 가상 데이터 센터의 VDC 그룹 네트워크를 볼 수 있습니다. 가상 시스템 또는 vApp이 이와 같은 조직 가상 데이터 센터 네트워크에 연결할 경우, 해당 가상 시스템 또는 vApp은 VDC 그룹 네트워크에 연결됩니다.

다음에 수행할 작업

크로스 VDC 조직 가상 데이터 센터 네트워크 각각에 정적 IP 주소와 IP 풀을 할당할 수 있습니다. [조직 가상 데이터 센터 네트워크 IP 풀에 IP 주소 추가](#)의 내용을 참조하십시오.

VDC 그룹 네트워크에 연결된 가상 시스템의 DNS 및 DHCP 구성은 VMware Cloud Director OpenAPI를 사용할 수 있습니다. VMware Cloud Director OpenAPI 설명서를 검토하려면 https://Cloud_Director_IP_address_or_host_name/docs를 참조하십시오. 코드 샘플을 보고 VMware Cloud Director OpenAPI 호출을 테스트하려면 https://Cloud_Director_IP_address_or_host_name/api-explorer?scope=organization_name을 참조하십시오.

NSX Data Center for vSphere에서 지원하는 데이터 센터 그룹 네트워크 보기 또는 편집

NSX Data Center for vSphere에서 지원하는 데이터 센터 그룹 네트워크의 이름, 설명 및 CIDR 설정을 볼 수 있습니다. NSX Data Center for vSphere에서 지원하는 데이터 센터 그룹 네트워크의 이름과 설명만 편집할 수 있습니다.

가상 데이터 센터 수준에서 데이터 센터 그룹 네트워크의 정적 IP 풀 할당 편집에 대한 자세한 내용은 [조직 가상 데이터 센터 네트워크 IP 풀에 IP 주소 추가](#) 항목을 참조하십시오.

사전 요구 사항

미리 정의된 **조직 관리자** 역할 또는 **조직 VDC 네트워크: 속성 보기** 및 **조직 VDC 네트워크: 속성 편집** 권한이 포함된 역할이 할당되었는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 대상 네트워크를 클릭하여 세부 정보를 확인합니다.
- 3 네트워크의 이름과 설명을 편집하려면 **편집**을 클릭합니다.
- 4 네트워크 세부 정보를 편집하고 **저장**을 클릭합니다.

NSX Data Center for vSphere에서 지원하는 데이터 센터 그룹 네트워크 동기화

참여하는 모든 가상 데이터 센터가 NSX Data Center for vSphere에서 지원하는 데이터 센터 그룹 네트워크에 액세스할 수 있도록 하려면 데이터 센터 그룹 네트워크를 동기화하면 됩니다.

사전 요구 사항

이 작업에는 미리 정의된 **조직 관리자** 역할 또는 **조직 VDC 네트워크: 속성 편집** 권한이 있는 역할이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭합니다.
- 2 네트워크 탭에서 대상 네트워크의 이름 옆에 있는 라디오 버튼을 선택하고 **동기화**를 클릭합니다.
- 3 **확인**을 클릭하여 확인합니다.

NSX Data Center for vSphere Edge 게이트웨이 서비스 관리

VMware Cloud Director는 NSX Data Center for vSphere 네트워크 가상화 소프트웨어를 기반으로 클라우드 환경에서 향상된 보안 제어, 라우팅 및 네트워크 확장 기능을 제공하는 고급 네트워킹 기능을 제공합니다.

이러한 네트워킹 기능을 사용하여 조직 가상 데이터 센터의 보안을 탁월한 수준으로 유지하고 네트워크를 격리할 수 있습니다. 이러한 기능은 다음과 같은 이점을 제공합니다.

- 동적 라우팅. NSX Data Center for vSphere 기능은 VMware Cloud Director 환경에서 BGP(Border Gateway Protocol) 및 OSPF(Open Shortest Path First) 같은 라우팅 프로토콜을 지원하여 시스템 간의 네트워크 통합을 간소화하고 이중화되고 연속적인 방식으로 클라우드 호스팅 애플리케이션을 배포할 수 있도록 합니다.
- 세분화된 네트워크 보안 및 격리. NSX Data Center for vSphere 기능은 VMware Cloud Director 환경에서 개체 기반 규칙 정의를 사용하여 상태 저장 네트워크 트래픽 격리를 수행할 수 있도록 합니다. 따라서 다수의 가상 네트워크가 필요하지 않습니다. 이 제로 트러스트 보안 모델은 애플리케이션 또는

가상 시스템이 손상된 경우 침입자가 전체 네트워크에 액세스하는 것을 방지합니다. 동일한 네트워크 보안 정책을 사용하여 VMware Cloud Director 환경의 모든 물리적 위치에 있는 애플리케이션을 보호하고 제로 트러스트 보안 모델을 확장하여 애플리케이션이 배포된 모든 이동식 디바이스를 보호할 수 있으므로 네트워크 구성이 간소화됩니다.

- **NSX Data Center for vSphere**가 제공하는 추가 기능으로는 지점 및 사이트 간(IPsec VPN)과 사용자(SSL VPN-Plus) 연결에 대한 향상된 VPN 지원, HTTPS의 향상된 로드 밸런싱 및 개선된 네트워크 확장성이 있습니다.

Edge 게이트웨이 방화벽과 분산 방화벽의 두 가지 방화벽을 구성할 수 있습니다. 이러한 방화벽 간의 차이점에 대한 자세한 내용은 [NSX Data Center for vSphere로 테넌트 방화벽 구성](#) 섹션을 참조하십시오.

이러한 고급 네트워킹 기능은 VMware Cloud Director 테넌트 포털이나 VMware Cloud Director Service Provider Admin Portal을 사용하여 액세스할 수 있습니다. 먼저 Edge 게이트웨이를 고급 Edge 게이트웨이로 변환해야 합니다. [NSX Data Center for vSphere Edge 게이트웨이](#)를 고급 Edge 게이트웨이로 변환의 내용을 참조하십시오.

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

NSX Data Center for vSphere로 VMware Cloud Director 고급 네트워킹 시작

VMware Cloud Director 고급 네트워킹을 사용하여 VMware Cloud Director 시스템의 조직에 대한 관리 작업을 수행할 수 있습니다. 분산 방화벽을 비롯하여 NSX Data Center for vSphere의 고급 네트워킹 기능을 관리할 수 있습니다. 이러한 기능은 VMware Cloud Director 시스템 관리자를 통해 조직에 제공됩니다.

NSX Data Center for vSphere에 제공되는 고급 네트워킹의 일반적인 사용자는 다음과 같습니다.

- **VMware Cloud Director 시스템 관리자.** 테넌트 포털을 사용하여 조직의 분산 방화벽을 비롯한 고급 네트워킹 기능을 구성할 수 있습니다.
- **조직 관리자.** 테넌트 포털을 사용하여 **시스템 관리자**가 조직에서 사용할 수 있게 설정한 분산 방화벽 및 기타 고급 네트워킹 기능을 관리합니다.

NSX Data Center for vSphere로 테넌트 방화벽 구성

테넌트 포털을 사용하여 VMware Cloud Director 조직 가상 데이터 센터의 NSX Data Center for vSphere가 제공하는 방화벽 기능을 구성할 수 있습니다. 분산 방화벽을 위한 방화벽 규칙을 생성하여 조직 가상 데이터 센터의 가상 시스템 간에 보안을 제공하고 Edge 게이트웨이 방화벽에 적용할 방화벽 규칙을 생성하여 조직 가상 데이터 센터의 가상 시스템을 외부 네트워크 트래픽으로부터 보호할 수 있습니다.

참고 테넌트 포털은 Edge 게이트웨이 방화벽과 분산 방화벽을 모두 구성할 수 있는 기능을 제공합니다.

NSX Data Center for vSphere 논리적 방화벽 기술은 서로 다른 배포 사용 사례를 해결할 수 있는 두 가지 구성 요소로 이루어져 있습니다. Edge 게이트웨이 방화벽은 북-남 트래픽 적용에 중점을 두고 분산 방화벽은 동-서 액세스 제어에 중점을 둡니다.

Edge 게이트웨이 방화벽과 분산 방화벽 간 주요 차이점

Edge 게이트웨이 방화벽은 북-남 트래픽을 모니터링하여 사이트 간 IPSec, SSL VPN 기능은 물론 방화벽, NAT(네트워크 주소 변환)를 포함하는 경계 보안 기능을 제공합니다.

분산 방화벽은 각 가상 시스템과 애플리케이션을 계층 2(L2) 수준으로 격리하고 보호하는 기능을 제공합니다. 분산 방화벽을 구성하면 외부 또는 내부 네트워크 보안 손상을 효과적으로 격리하여 동일한 네트워크 세그먼트의 가상 시스템 간 동-서 트래픽을 격리할 수 있습니다. 보안 정책이 중앙에서 관리, 상속 및 중첩 가능하므로 네트워킹 및 보안 관리자는 정책을 효과적으로 관리할 수 있습니다. 또한 일단 보안 정책을 배포하면 가상 시스템 또는 애플리케이션이 다른 가상 데이터 센터로 이동할 때 정의된 보안 정책을 여기에 적용할 수 있습니다.

방화벽 규칙 정보

관련 제품 설명서에 설명된 대로, 중앙 집중화된 수준에서 정의된 방화벽 규칙을 NSX Data Center for vSphere에서는 사전 규칙이라고 합니다. 또한 개별 Edge 게이트웨이 수준에서도 규칙을 추가할 수 있는데 이러한 규칙을 로컬 규칙이라고 합니다.

각 트래픽 세션은 방화벽 테이블 맨 위에 있는 규칙을 확인한 후 테이블의 후속 규칙을 확인합니다. 테이블에서 트래픽 매개 변수와 일치하는 첫 번째 규칙이 적용됩니다. 규칙은 다음과 같은 순서로 표시됩니다.

- 1 사용자 정의 사전 규칙. 최상위 우선 순위를 가지며 가상 NIC 수준별 우선 순위에 따라 위에서 아래로 적용됩니다.
- 2 Auto-plumbed 규칙(제어 트래픽이 Edge 게이트웨이 서비스로 흐르도록 하는 규칙).
- 3 Edge 게이트웨이 수준에서 정의되는 로컬 규칙.
- 4 기본 분산 방화벽 규칙

NSX Data Center for vSphere 소프트웨어가 방화벽 규칙을 적용하는 방법에 대한 자세한 내용은 NSX Data Center for vSphere 설명서에서 "방화벽 규칙의 순서 변경"을 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이 방화벽

Edge 게이트웨이 방화벽은 IP/VLAN 구성체 기반 DMZ 구축, 다중 테넌트 가상 데이터 센터에서 테넌트 간의 분리, NAT(네트워크 주소 변환), 파트너(익스트라넷) VPN, 사용자 기반 SSL VPN과 같은 주요 경계 보안 요구 사항을 충족시키는 데 도움을 줍니다.

VMware Cloud Director 환경에서 Edge 게이트웨이 방화벽 기능은 NSX Data Center for vSphere에 의해 제공됩니다. NSX Data Center for vSphere에서 이 방화벽 기능을 Edge 방화벽이라고도 합니다.

Edge 게이트웨이 방화벽은 북-남 트래픽을 모니터링하여 사이트 간 IPSec, SSL VPN 기능은 물론 방화벽, NAT(네트워크 주소 변환)를 포함하는 경계 보안 기능을 제공합니다.

NSX Data Center for vSphere의 Edge 게이트웨이 방화벽이 제공하는 기능에 대한 자세한 내용은 NSX Data Center for vSphere 설명서를 참조하십시오.

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 [테넌트 포털을 사용하여 NSX Data Center for vSphere 분산 방화벽 규칙 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 활성화 또는 비활성화합니다.

NSX Data Center for vSphere Edge 게이트웨이를 고급 Edge 게이트웨이로 변환

테넌트 포털에서 NSX Data Center for vSphere Edge 게이트웨이 작업을 수행하려면 고급 Edge 게이트웨이로 변환해야 합니다. 고급 Edge 게이트웨이로 변환한 후에는 이러한 고급 Edge 게이트웨이에 대해 NSX Data Center for vSphere가 제공하는 정적 및 동적 라우팅 기능을 테넌트 포털을 사용하여 구성할 수 있습니다.

사전 요구 사항

기존 Edge 게이트웨이가 있어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 편집할 Edge 게이트웨이를 선택합니다.
- 3 **고급으로 변환**을 클릭합니다.

결과

Edge 게이트웨이가 고급 Edge 게이트웨이로 변환됩니다.

다음에 수행할 작업

고급 Edge 게이트웨이로 변환한 후 게이트웨이를 선택하고 **서비스**를 클릭하여 설정을 구성할 수 있습니다.

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

- Edge 게이트웨이 서비스를 엽니다.
 - 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 방화벽 규칙** 화면이 표시되지 않으면 **방화벽** 탭을 클릭합니다.
- 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.
- 이름** 셀을 클릭하고 이름을 입력합니다.
- 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	특정 IP 주소가 아닌 개체로 소스를 지정하려면 + 아이콘을 사용합니다. <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. 소스에서 제외 전환을 선택하면 해당 소스를 제외한 모든 소스에서 들어오는 모든 트래픽에 규칙이 적용됩니다. 제외 전환을 선택하지 않으면 개체 선택 창에서 지정된 소스에서 들어오는 트래픽에 규칙이 적용됩니다.

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

- Edge 게이트웨이 서비스를 엽니다.
 - 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 방화벽** 탭을 클릭합니다.

3 방화벽 규칙을 관리합니다.

- 규칙을 비활성화하려면 **번호** 셀의 녹색 확인 표시를 클릭합니다. 녹색 확인 표시가 빨간색의 비활성화됨 아이콘으로 변경됩니다. 규칙이 비활성화되어 있고 규칙을 활성화하려면 빨간색 비활성화됨 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 분산 방화벽

분산 방화벽을 사용하면 가상 시스템 이름과 특성을 기반으로 가상 시스템과 같은 조직 가상 데이터 센터 엔티티를 세분화할 수 있습니다.

VMware Cloud Director는 NSX Data Center for vSphere에서 지원되는 조직 가상 데이터 센터에서 분산 방화벽 서비스를 지원합니다. NSX Data Center for vSphere 설명서에 설명된 대로, 이 분산 방화벽은 가상 워크로드와 네트워크에 대한 가시성 및 제어 기능을 제공하는 방화벽으로, 하이퍼바이저 커널이 내장되어 있습니다. 가상 시스템 이름과 같은 개체, IP 주소 또는 IP 집합 주소와 같은 네트워크 구성체를 기반으로 액세스 제어 정책을 생성할 수 있습니다. 방화벽 규칙은 각 가상 시스템의 vNIC 수준에서 적용되므로 가상 시스템이 vSphere vMotion에 의해 새 ESXi 호스트로 이동하더라도 일관된 액세스 제어를 제공합니다. 이 분산 방화벽은 회선에 가까운 속도 처리 시 동-서 트래픽을 검사할 수 있는 미세-세분화 보안 모델을 지원합니다.

NSX Data Center for vSphere 설명서에 설명된 대로, 계층 2(L2) 패킷의 경우 분산 방화벽은 성능 향상을 위해 캐시를 생성합니다. 계층 3(L3) 패킷은 다음 순서로 처리됩니다.

- 1 모든 패킷은 기존 상태에 대해 검사됩니다.
 - 2 상태 일치 항목이 있으면 패킷이 처리됩니다.
 - 3 상태 일치 항목이 없으면 일치 항목을 찾을 때까지 규칙을 통해 패킷이 처리됩니다.
- TCP 패킷의 경우 SYN 플래그가 있는 패킷에 대해서만 상태가 설정됩니다. 하지만 프로토콜(서비스 ANY)을 지정하지 않는 규칙은 임의의 플래그 조합을 사용하여 TCP 패킷을 일치시킬 수 있습니다.
 - UDP 패킷의 경우 패킷에서 5-튜플 세부 정보가 추출됩니다. 상태 테이블에 상태가 없는 경우 추출된 5-튜플 세부 정보를 사용하여 새 상태가 생성됩니다. 이후 수신된 패킷은 방금 생성된 상태에 대해 일치됩니다.
 - ICMP 패킷의 경우 ICMP 유형, 코드 및 패킷 방향을 사용하여 상태를 생성합니다.

분산 방화벽은 ID 기반 규칙을 생성할 때에도 유용할 수 있습니다. 관리자는 엔터프라이즈 AD(Active Directory)에 정의된 대로 사용자의 그룹 멤버 자격을 기반으로 액세스 제어를 적용할 수 있습니다. ID 기반 방화벽 규칙을 사용할 수 있는 경우에 대한 몇 가지 사용 사례는 다음과 같습니다.

- 사용자 인증에 AD가 사용되는 환경에서 사용자가 랩톱 또는 모바일 디바이스를 사용하여 가상 애플리케이션에 액세스
- Microsoft Windows 기반 가상 시스템 환경에서 사용자가 VDI 인프라를 사용하여 가상 애플리케이션에 액세스

분산 방화벽이 제공하는 기능에 대한 자세한 내용은 NSX Data Center for vSphere 설명서를 참조하십시오.

NSX Data Center for vSphere가 지원하는 조직 가상 데이터 센터에서 분산 방화벽 사용

테넌트 포털을 사용하여 조직 가상 데이터 센터에서 NSX Data Center for vSphere가 제공하는 분산 방화벽 기능을 사용하려면 해당 조직 가상 데이터 센터에 대해 분산 방화벽을 사용하도록 설정해야 합니다.

VMware Cloud Director 시스템 관리자 또는 **org_vdc_distributed_firewall_enable** 권한이 있는 사용자는 조직 가상 데이터 센터에서 분산 방화벽을 사용하도록 설정할 수 있습니다.

테넌트 포털의 [분산 방화벽] 화면에서 조직 가상 데이터 센터의 분산 방화벽을 사용하도록 설정합니다.

사전 요구 사항

조직 가상 데이터 센터가 속하는 조직에 다음 권한이 할당되어 있는지 확인합니다.

- 조직 vDC 분산 방화벽: 사용/사용 안 함
- 조직 vDC 분산 방화벽: 규칙 구성
- 조직 vDC 분산 방화벽: 규칙 보기

VMware Cloud Director **시스템 관리자**는 조직에 권한을 할당합니다. [조직 vDC 분산 방화벽: 사용/사용 안 함] 권한은 테넌트 포털에서 사용자 인터페이스를 사용하여 분산 방화벽을 활성화하는 데 필요합니다. [조직 vDC 분산 방화벽: 규칙 보기] 권한은 테넌트 포털에서 방화벽 규칙을 보는 데 필요하며 [조직 vDC 분산 방화벽: 규칙 구성] 권한은 테넌트 포털을 사용하여 방화벽 규칙을 구성하는 데 필요합니다.

[조직 vDC 분산 방화벽: 사용/사용 안 함]이라는 권한을 부여하는 역할이 할당되어 있는지 확인합니다. 이 권한은 VMware Cloud Director 시스템의 미리 정의된 역할 중에 시스템 관리자 역할에만 기본적으로 부여됩니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 **네트워킹** 아래에서 **보안**을 선택합니다.
- 2 분산 방화벽 규칙을 구성할 조직 가상 데이터 센터를 선택합니다.
- 3 **서비스 구성**을 클릭합니다.
- 4 **분산 방화벽** 탭에서 분산 방화벽을 사용하도록 설정합니다.

다음에 수행할 작업

기본 분산 방화벽 규칙에 대한 설명은 [테넌트 포털을 사용하여 NSX Data Center for vSphere 분산 방화벽 규칙 관리](#) 섹션을 참조하십시오.

테넌트 포털을 사용하여 NSX Data Center for vSphere 분산 방화벽 규칙 관리

NSX Data Center for vSphere 설명서에 설명된 대로, 기본 방화벽 설정은 사용자 정의 방화벽 규칙과 일치하지 않는 트래픽에 적용됩니다. VMware Cloud Director Tenant Portal에서, 기본 분산 방화벽 규칙은 [기본 허용 규칙]이라는 레이블이 지정되어 있습니다.

VMware Cloud Director Tenant Portal을 사용하여 분산 방화벽 설정을 관리할 수 있으려면 조직 가상 데이터 센터에서 분산 방화벽 기능을 사용하도록 설정해야 합니다.

기본 분산 방화벽 규칙은 모든 계층 3 및 계층 2 트래픽이 조직의 가상 데이터 센터를 통과하는 것을 허용하도록 구성되어 있습니다. 이 설정은 사용자 인터페이스의 [작업] 열에 설정된 [허용]으로 표시됩니다. 기본 규칙은 항상 규칙 테이블의 맨 아래에 위치합니다.

중요 기본 분산 방화벽 규칙은 삭제하거나 수정할 수 없습니다.

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

- [NSX Data Center for vSphere](#)가 지원하는 조직 가상 데이터 센터에서 분산 방화벽 사용
- IP 집합을 규칙에서 소스 또는 대상으로 사용하려면 방화벽 규칙 및 DHCP 릴레이 구성에 사용할 IP 집합 만들기의 지침을 따르십시오.
- MAC 집합을 규칙에서 소스 또는 대상으로 사용하려면 방화벽 규칙에 사용할 MAC 집합 만들기의 지침을 따르십시오.
- 보안 그룹을 규칙에서 소스 또는 대상으로 사용하려면 보안 그룹 만들기의 지침을 따르십시오.

절차

- 1 가상 데이터 센터 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 **네트워킹** 아래에서 **보안**을 선택합니다.
- 2 방화벽 규칙을 수정할 보안 서비스 VDC 네트워크를 선택하고 **서비스 구성**을 클릭합니다.
[보안 서비스] 화면이 표시됩니다.
- 3 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.

- 4 방화벽 테이블의 기존 규칙 아래 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.

- 5 **이름** 셀을 클릭하고 이름을 입력합니다.
- 6 **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>

- 7 **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>

8 새 규칙의 **서비스** 셀을 클릭하고 다음 작업 중 하나를 수행합니다.

작업	설명
IP 아이콘 클릭	포트-프로토콜 조합으로 서비스를 지정하려면 다음을 수행합니다. a 서비스 프로토콜을 선택합니다. b 소스 및 대상 포트에 대한 포트 번호를 입력하거나 any 를 지정하고 유지 를 클릭합니다.
+ 아이콘 클릭	미리 정의된 서비스 또는 서비스 그룹을 선택하거나 새로 정의하려면 다음을 수행합니다. a 하나 이상의 개체를 선택하고 필터에 추가합니다. b 유지 를 클릭합니다.

9 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.

10 새 규칙의 **방향** 셀에서 규칙을 수신 트래픽, 송신 트래픽 또는 둘 다에 적용할지를 선택합니다.

11 일반 탭의 규칙인 경우 새 규칙의 **패킷 유형** 셀에서 **임의**, **IPV4** 또는 **IPV6**의 패킷 유형을 선택합니다.

12 **적용 대상** 셀을 선택하고 **+** 아이콘을 사용하여 이 규칙을 적용할 수 있는 개체 범위를 정의합니다.

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.

중요 IP 주소 그룹(IP 집합), MAC 주소 그룹(MAC 집합) 및 IP 집합이나 MAC 집합이 포함된 보안 그룹은 올바른 입력 매개 변수가 아닙니다.

13 **변경 내용 저장**을 클릭합니다.

분산 방화벽 규칙 편집

VMware Cloud 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

1 가상 데이터 센터 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 **네트워킹** 아래에서 **보안**을 선택합니다.

2 방화벽 규칙을 수정할 보안 서비스 VDC 네트워크를 선택하고 **서비스 구성**을 클릭합니다.

[보안 서비스] 화면이 표시됩니다.

3 분산 방화벽 규칙을 관리하려면 다음 작업을 수행합니다.

- 규칙을 비활성화하려면 **번호** 셀의 녹색 확인 표시를 클릭합니다.
녹색 확인 표시가 빨간색의 비활성화된 아이콘으로 변경됩니다. 규칙이 비활성화되어 있고 규칙을 활성화하려면 빨간색 비활성화된 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.

4 **변경 내용 저장**을 클릭합니다.

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 설명서에 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 DHCP가 활성화된 Edge 게이트웨이의 DNS 설정이 변경되면 Edge 게이트웨이가 DHCP 서비스 제공을 중지할 수 있습니다. 이 상황이 발생할 경우 [DHCP 풀] 화면의 **DHCP 서비스 상태** 토글을 사용하여 해당 Edge 게이트웨이의 DHCP를 비활성화했다가 다시 활성화합니다. **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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 2 **DHCP > 풀**로 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.

옵션	설명
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 않음을 선택하면 임대 기간을 지정할 수 없습니다.	

5 변경 내용 저장을 클릭합니다.

결과

DHCP 서비스를 제공하도록 VMware Cloud 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

- Edge 게이트웨이 서비스를 엽니다.
 - 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 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.

옵션	설명
보조 이름 서버	DNS 자동 구성을 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.
임대가 만료되지 않음	해당 MAC 주소에 바인딩된 IP 주소를 영구적으로 유지하려면 이 토글을 사용하도록 설정합니다. 이 옵션을 선택하면 임대 기간이 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

VMware Cloud Director 환경에서 NSX 소프트웨어를 통해 제공되는 DHCP 릴레이 기능을 사용하면 VMware Cloud 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

VMware Cloud Director 환경에서 NSX 소프트웨어를 사용하면 Edge 게이트웨이에서 VMware Cloud 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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 2 **DHCP > 릴레이**로 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.

NSX Data Center for vSphere Edge 게이트웨이에서 NAT(네트워크 주소 변환) 관리

VMware Cloud Director 환경에서 NSX Data Center for vSphere 소프트웨어를 사용하면 Edge 게이트웨이에서 NAT(네트워크 주소 변환) 서비스를 제공할 수 있습니다. 이 기술을 사용하면 조직에서 사용해야 하는 공개 IP 주소의 수를 줄일 수 있기 때문에 경제적 이점과 보안 이점을 누릴 수 있습니다.

Edge 게이트웨이 NAT 서비스는 개인 네트워크의 가상 시스템 또는 가상 시스템 그룹에 공개 주소를 할당하는 기능을 제공합니다. Edge 게이트웨이가 조직 가상 데이터 센터의 개인 주소 지정 가상 시스템에서 실행 중인 서비스에 대해 액세스를 제공하도록 하려면 Edge 게이트웨이에서 NAT 규칙을 구성해야 합니다. 가장 일반적인 경우, 조직 가상 데이터 센터 네트워크의 주소가 외부 네트워크에 노출되지 않도록 NAT 서비스를 VMware Cloud Director 환경의 Edge 게이트웨이에 있는 업링크 인터페이스에 연결합니다.

NAT 서비스 구성은 SNAT(소스 NAT) 규칙과 DNAT(대상 NAT) 규칙으로 구분됩니다. VMware Cloud Director 환경의 Edge 게이트웨이에 SNAT 또는 DNAT 규칙을 구성할 때는 항상 조직 가상 데이터 센터의 관점에서 규칙을 구성해야 합니다. 특히, 이것은 다음과 같은 방식으로 규칙을 구성해야 함을 의미합니다.

- **SNAT:** 트래픽이 조직 가상 데이터 센터의 내부 네트워크에 있는 가상 시스템(소스)에서 인터넷을 통해 외부 네트워크(대상)로 이동합니다. SNAT 규칙은 조직 가상 데이터 센터 네트워크에서 외부 네트워크나 다른 조직 가상 데이터 센터 네트워크로 전송되는 송신 패킷 소스 IP 주소를 변환합니다.
- **DNAT:** 트래픽이 인터넷(소스)에서 조직 가상 데이터 센터 내부의 가상 시스템(대상)으로 이동합니다. 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.

NAT 규칙을 구성하여 조직 가상 데이터 센터 내부에 개인 IP 주소 공간을 생성할 수 있습니다. 이 구성을 통해 하나의 조직 가상 데이터 센터에서 다른 데이터 센터로 개인 IP 주소 공간을 포팅할 수 있습니다.

NAT 규칙을 구성하면 다른 조직의 가상 데이터 센터에서 사용되었던 동일한 개인 IP 주소를 사용자 조직 가상 데이터 센터의 가상 시스템에도 사용할 수 있습니다.

VMware Cloud Director 환경의 NAT 규칙 기능은 다음을 지원합니다.

- 개인 IP 주소 공간 내에 서브넷 생성
- Edge 게이트웨이에 대해 여러 개의 개인 IP 주소 공간 생성
- 여러 Edge 게이트웨이 인터페이스에서 여러 NAT 규칙 구성

중요 Edge 게이트웨이 네트워크의 가상 시스템에 액세스할 수 있으려면 Edge 게이트웨이에서 방화벽 및 NAT 규칙을 모두 구성해야 합니다. 기본적으로 Edge 게이트웨이는 Edge 게이트웨이 네트워크의 가상 시스템에서 들어오고 나가는 모든 네트워크 트래픽을 거부하도록 구성된 방화벽 규칙으로 배포됩니다. 또한 NAT는 Edge 게이트웨이에서 기본적으로 비활성화되므로 Edge 게이트웨이에서 NAT를 구성하는 경우가 아니면 Edge 게이트웨이가 수신 트래픽과 송신 트래픽의 IP 주소를 변환할 수 없습니다. 방화벽 규칙을 추가하여 해당 트래픽을 허용하지 않으면 NAT 규칙을 구성한 후 네트워크에서 가상 시스템에 대해 ping을 시도했을 때 ping이 실패합니다.

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

VMware Cloud 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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **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 입력하거나 목록에서 할당된 IP 주소를 선택합니다. 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.

옵션	설명
소스 IP 주소	규칙을 특정 도메인의 트래픽에 대해서만 적용하려는 경우 이 도메인에 대한 IP 주소 또는 IP 주소 범위를 CIDR 형식으로 입력합니다. 이 텍스트 상자를 비워 두는 경우 DNAT 규칙이 로컬 서브넷의 모든 IP 주소에 적용됩니다.
소스 포트	(선택 사항) 소스에 대한 포트 번호를 입력합니다.
설명	(선택 사항) DNAT 규칙에 대한 의미 있는 설명을 입력합니다.
사용	이 규칙을 활성화하려면 토글을 설정합니다.
로깅 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 입력하거나 목록에서 할당된 IP 주소를 선택합니다. 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.
대상 IP 주소	(선택 사항) 규칙을 특정 도메인으로 전송되는 트래픽에 대해서만 적용하려는 경우 이 도메인에 대한 IP 주소 또는 IP 주소 범위를 CIDR 형식으로 입력합니다. 이 텍스트 상자를 비워 두는 경우 SNAT 규칙이 로컬 서브넷 외부의 모든 대상에 적용됩니다.
대상 포트	(선택 사항) 대상에 대한 포트 번호를 입력합니다.
설명	(선택 사항) SNAT 규칙에 대한 의미 있는 설명을 입력합니다.
사용	이 규칙을 활성화하려면 토글을 설정합니다.
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.

NSX Data Center for vSphere Edge 게이트웨이에 대한 고급 라우팅 구성

NSX Data Center for vSphere Edge 게이트웨이에서 정적 및 동적 라우팅을 구성할 수 있습니다.

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

NSX Data Center for vSphere가 제공하는 라우팅 기능에 대한 자세한 내용은 NSX Data Center for vSphere 설명서를 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. NSX Data Center for vSphere는 이러한 인텔리전스를 동-서 라우팅 워크로드의 위치로 확장합니다. 이 기능은 추가 비용 또는 시간을 들여 홑을 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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **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 홑 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 홑을 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 홑에 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 **확인**을 클릭합니다.

6 **변경 내용 저장**을 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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.

b 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.

2 **라우팅 > 정적 경로**로 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 추가의 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. VMware Cloud Director 환경에서는 주로 VMware Cloud 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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 2 **라우팅 > OSPF**로 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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.


2 라우팅 > BGP로 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 저장을 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.
연결 억제 시간	소프트웨어가 연결 유지 메시지를 수신하지 못하게 된 후부터 피어가 비활성화임을 선언할 때까지의 간격입니다. 이 간격은 연결 유지 간격의 세 배여야 합니다. 기본 간격은 180초입니다. 조직의 필요에 맞게 조정합니다. 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.

옵션	설명
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 저장**을 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.
 - a 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 2 **라우팅 > 라우트 재분산**으로 이동합니다.
- 3 프로토콜 토글을 사용하여 라우트 재분산을 사용할 프로토콜을 켭니다.

4 IP 접두사를 화면의 테이블에 추가합니다.

- a **추가**() 버튼을 클릭합니다.
- b 네트워크의 이름 및 IP 주소를 CIDR 형식으로 입력합니다.
- c **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 저장**을 클릭합니다.

NSX Data Center for vSphere로 로드 밸런싱

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

로드 밸런싱 정보

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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **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 저장**을 클릭합니다.

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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 2 **로드 밸런서 > 애플리케이션 프로파일**로 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 패스스루를 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 독립적 클라이언트 기반의 독립적 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 변경 내용을 보존하려면 **유지**를 클릭합니다.

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

- Edge 게이트웨이 서비스를 엽니다.
 - 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 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 활성화되거나 비활성화됩니다.
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 변경 내용을 보존하려면 **유지**를 클릭합니다.

예제: 각 프로토콜에 대해 지원되는 확장

표 5-4. 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= <i>SECONDS</i>	문서가 <i>SECONDS</i> 이상 경과한 경우 경고합니다. 분의 경우 10m, 시간의 경우 10h 또는 일의 경우 10d의 형식으로 숫자를 입력할 수 있습니다.
content-type= <i>STRING</i>	POST 호출에 Content-Type 헤더 미디어 유형을 지정합니다.
linespan	정규식을 새 행으로 연장할 수 있습니다(-r 또는 -R에 선행해야 함).
regex= <i>STRING</i> 또는 ereg= <i>STRING</i>	정규식 <i>STRING</i> 의 페이지를 검색합니다.
eregi= <i>STRING</i>	대/소문자를 구분하지 않는 정규식 <i>STRING</i> 의 페이지를 검색합니다.
invert-regex	찾은 경우 CRITICAL을 반환하고 찾을 수 없는 경우 OK를 반환합니다.
proxy-authorization= <i>AUTH_PAIR</i>	기본 인증을 사용하는 프록시 서버의 username:password를 지정합니다.
useragent= <i>STRING</i>	HTTP 헤더의 문자열을 User Agent로 전송합니다.
header= <i>STRING</i>	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. sticky는 follow와 유사하지만 지정된 IP 주소에 고정됩니다. stickyport는 포트가 동일하게 유지되도록 합니다.
pagesize= <i>INTEGER:INTEGER</i>	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 5-5. HTTPS 프로토콜 전용 확장

모니터 확장	설명
sni	SSL/TLS 호스트 이름 확장 지원(SNI)을 사용하도록 설정합니다.
certificate= <i>INTEGER</i>	인증서의 최소 유효 기간을 지정합니다. 포트 기본값은 443입니다. 이 옵션을 사용하는 경우 URL이 검사되지 않습니다.
authorization= <i>AUTH_PAIR</i>	기본 인증을 사용하는 사이트의 username:password를 지정합니다.

표 5-6. 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

- Edge 게이트웨이 서비스를 엽니다.
 - 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 로드 밸런서 > 풀**로 이동합니다.
- 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 host 를 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 해제될 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 **투명**을 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 변경 내용을 보존하려면 **유지**를 클릭합니다.

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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.

b 편집할 Edge 게이트웨이를 선택하고 **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/2.2/configuration.html>의 내용을 참조하십시오.

6 변경 내용을 보존하려면 **유지**를 클릭합니다.

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

- Edge 게이트웨이 서비스를 엽니다.
 - 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 로드 밸런서 > 가상 서버**로 이동합니다.
- 추가() 버튼을 클릭합니다.
- 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.
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.

- (선택 사항) 애플리케이션 규칙을 가상 서버에 연결하려면 **고급** 탭을 클릭하고 다음 단계를 완료합니다.

- 추가() 버튼을 클릭합니다.

로드 밸런서에 대해 만들어진 애플리케이션 규칙이 표시됩니다. 필요한 경우 로드 밸런서에 대한 애플리케이션 규칙을 추가합니다. **애플리케이션 규칙 추가**의 내용을 참조하십시오.

- 변경 내용을 보존하려면 **유지**를 클릭합니다.

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.

NSX Data Center for vSphere Edge 게이트웨이에서 VPN을 사용하여 보안 액세스 구성

NSX Data Center for vSphere Edge 게이트웨이에서 NSX Data Center for vSphere 소프트웨어가 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.

VMware Cloud 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 VMware Cloud 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

VMware Cloud 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.

VMware Cloud 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. [NSX Data Center for vSphere Edge 게이트웨이의 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-Plus와 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. 활성화된 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 사용자에게 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 VMware Cloud Director 환경의 Edge 게이트웨이에 대한 일부 SSL VPN-Plus 설정을 설정합니다. 이러한 설정은 VMware Cloud 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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
- b 편집할 Edge 게이트웨이를 선택하고 **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** 구성에 설명된 사전 요구 사항을 충족했는지 확인합니다.

- 기본 인증서가 아닌 다른 서비스 인증서를 사용하는 경우 필수 인증서를 시스템으로 가져옵니다.
Edge 게이트웨이에 서비스 인증서 추가의 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 활성화되어 있습니다. 로깅할 메시지의 수준을 변경하거나 로깅을 비활성화할 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 활성화할지 비활성화할지 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 **유지**를 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-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. 활성화된 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-Plus**를 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 활성화하도록 선택하면 활성 모드의 FTP와 같은 일부 애플리케이션이 해당 서브넷 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 비활성화해야 합니다. 또한 해당 FTP 서버의 개인 네트워크가 활성화되어 TCP 최적화된 개인 네트워크 위의 화면 테이블에 나타나야 합니다.

사전 요구 사항

- [SSL-VPN Plus](#) 화면으로 이동.
- [NSX Data Center for vSphere Edge 게이트웨이](#)에서 [SSL VPN-Plus](#)와 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: 192169.1.0/24).
설명	(선택 사항) 네트워크에 대한 설명을 입력합니다.

옵션	작업
트래픽 보내기	<p>VPN 클라이언트가 개인 네트워크 및 인터넷 트래픽을 보내는 방법을 지정합니다.</p> <ul style="list-style-type: none"> ■ 터널을 통해 <p>VPN 클라이언트는 SSL VPN-Plus가 활성화된 Edge 게이트웨이를 통해 개인 네트워크 및 인터넷 트래픽을 보냅니다.</p> ■ 터널 우회 <p>VPN 클라이언트가 Edge 게이트웨이를 우회하고 트래픽을 개인 서버에 직접 보냅니다.</p>
TCP 최적화 사용	<p>(선택 사항) 인터넷 속도를 최적화하려면 트래픽을 보내는 방법으로 터널을 통해를 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 저해되고 연결 시간 초과가 발생합니다. TCP 최적화 사용을 선택하면 이 TCP-over-TCP 문제가 발생할 위험이 사라집니다.</p> <p>참고 TCP 최적화를 활성화하는 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.
포트	<p>터널을 통해를 선택한 경우, 원격 사용자가 내부 서버에 액세스할 수 있도록 열어 둘 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>
상태	<p>개인 네트워크를 활성화하거나 비활성화합니다.</p>

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 확인을 위해 Edge 게이트웨이에 **CA** 인증서 추가의 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) 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 잠기게 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 사용자에 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) 사용자에 대한 설명을 입력합니다.
사용	사용자가 활성화되었는지 비활성화되었는지 지정합니다.
암호가 만료되지 않음	(선택 사항) 이 사용자에 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 패키지의 활성화 또는 비활성화 여부를 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 모드**를 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 비활성화합니다.

자동 다시 연결 사용은 기본적으로 활성화되어 있습니다. 자동 다시 연결이 활성화되면 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 비활성화되어 있습니다. 이 옵션을 활성화하면 원격 사용자가 업그레이드 설치를 선택할 수 있습니다.

- 6 **변경 내용 저장**을 클릭합니다.

NSX Data Center for vSphere Edge 게이트웨이에 대한 일반 SSL VPN-Plus 설정 사용자 지정

기본적으로 시스템은 VMware Cloud Director 환경의 Edge 게이트웨이에 대한 일부 SSL VPN-Plus 설정을 설정합니다. 이러한 설정은 VMware Cloud 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 유효 시간 제한	세션 유효 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

VMware Cloud 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

VMware Cloud 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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
- b 편집할 Edge 게이트웨이를 선택하고 **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

VMware Cloud 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 VMware Cloud 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 Edge 게이트웨이 서비스를 엽니다.
 - a 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 2 IPsec VPN 탭에서 **IPsec VPN 사이트**를 클릭합니다.
- 3 **추가**() 버튼을 클릭합니다.
- 4 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>

옵션	작업
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>
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>

옵션	작업
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. ■ <code>passthroughSubnets=PeerSubnet/IPAddress</code> - 서브넷을 겹칠 수 있습니다.

5 **유지**를 클릭합니다.

6 **변경 내용 저장**을 클릭합니다.

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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **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 any로 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. [NSX Data Center for vSphere Edge 게이트웨이에 대한 통계 및 로그](#)의 내용을 참조하십시오.

L2 VPN 구성

VMware Cloud 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 연

결을 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.

[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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 2 **VPN > L2 VPN**으로 이동합니다.

다음에 수행할 작업

L2 VPN 서버를 구성합니다. [NSX Data Center for vSphere Edge 게이트웨이](#)를 L2 VPN 서버로 구성의 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	
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.

다음에 수행할 작업

이 Edge 게이트웨이에서 L2 VPN 서비스를 사용하도록 설정합니다. [NSX Data Center for vSphere Edge 게이트웨이에서 L2 VPN 서비스 사용의 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 추가의 내용](#)을 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.
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**을 클릭합니다.
- 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.

옵션	설명
포트	프록시 서버 포트를 입력합니다.
사용자 이름	프록시 서버 인증 자격 증명을 입력합니다.
암호	

6 서버 인증서 검증을 사용하도록 설정하려면 **CA 인증서 변경**을 클릭하고 적절한 CA 인증서를 선택합니다.

7 **변경 내용 저장**을 클릭합니다.

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 서비스도 비활성화됩니다.

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 비활성화되고 구성 세부 정보가 Edge 게이트웨이에서 제거됩니다.

NSX Data Center for vSphere Edge 게이트웨이의 SSL 인증서 관리

NSX Data Center for vSphere 소프트웨어는 VMware Cloud Director 환경에서 Edge 게이트웨이에 구성된 SSL VPN-Plus 및 IPsec VPN 터널과 함께 SSL(Secure Sockets Layer) 인증서를 사용할 수 있는 기능을 제공합니다.

VMware Cloud 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

VMware Cloud 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 Data Center for vSphere 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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **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: www.example.com). 일반 이름에 http:// 또는 https:// 접두사를 포함하지 마십시오.
조직 구성 단위	이 필드는 이 인증서가 연결된 VMware Cloud Director 조직 내의 사업부를 서로 구분하는 데 사용됩니다. 예를 들어 엔지니어링 또는 영업을 사용합니다.
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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 2 **인증서** 탭을 클릭합니다.
- 3 **CA 인증서**를 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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 2 **인증서** 탭을 클릭합니다.
- 3 **CRL**을 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 **유지**를 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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **서비스**를 클릭합니다.
- 2 **인증서** 탭을 클릭합니다.
- 3 **서비스 인증서**를 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.

FIPS 모드가 켜져 있으면, RSA 키 크기가 2048비트보다 크거나 같아야 합니다.

 - 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 입력합니다.
- 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.

NSX Data Center for vSphere Edge 게이트웨이에 대한 사용자 지정 개체 그룹화

NSX Data Center for vSphere 소프트웨어를 VMware Cloud 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.

VMware Cloud Director 테넌트 포털의 **개체 그룹화** 페이지를 사용하여 IP 집합을 만듭니다. **개체 그룹화** 페이지는 [서비스]와 [Edge 게이트웨이] 화면 모두에서 사용할 수 있습니다.

절차

- 1 **개체 그룹화** 페이지를 엽니다.

옵션	작업
Edge 게이트웨이 서비스를 통해 열기	a 네트워크 > Edge로 이동합니다. b 편집할 Edge 게이트웨이를 선택하고 서비스 구성 을 클릭합니다. c 개체 그룹화 를 클릭합니다.
보안 서비스를 통해 열기	a 네트워크 > 보안으로 이동합니다. b 편집할 보안 서비스를 선택하고 서비스 구성 을 클릭합니다. c 개체 그룹화 를 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 (선택 사항) [서비스] 화면의 **개체 그룹화** 페이지를 사용하여 IP 집합을 지정하는 경우 **상속** 토글을 사용하여 상속을 사용하도록 설정하고 기본 범위에서 볼 수 있도록 허용합니다.

상속은 기본적으로 사용됩니다.

- 6 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.

VMware Cloud Director 테넌트 포털의 **개체 그룹화** 페이지를 사용하여 MAC 집합을 만듭니다. [개체 그룹화] 페이지는 **서비스** 화면과 **Edge 게이트웨이** 화면에서 모두 사용할 수 있습니다.

절차

1 개체 그룹화 페이지를 엽니다.

옵션	작업
Edge 게이트웨이 서비스를 통해 열기	a 네트워킹 > Edge로 이동합니다. b 편집할 Edge 게이트웨이를 선택하고 서비스 구성 을 클릭합니다. c 개체 그룹화 를 클릭합니다.
보안 서비스를 통해 열기	a 네트워킹 > 보안으로 이동합니다. b 편집할 보안 서비스를 선택하고 서비스 구성 을 클릭합니다. c 개체 그룹화 를 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 (선택 사항) 서비스 화면의 개체 그룹화 페이지를 사용하여 MAC 집합을 지정하는 경우 **상속** 토글을 사용하여 상속을 사용하도록 설정하고 기본 범위에서 볼 수 있도록 허용합니다.

상속은 기본적으로 사용됩니다.

6 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.

VMware Cloud Director 테넌트 포털의 [개체 그룹화] 페이지를 사용하여 사용 가능한 서비스를 볼 수 있습니다. [개체 그룹화] 페이지는 [서비스] 화면과 [Edge 게이트웨이] 화면에서 모두 사용할 수 있습니다.

테넌트 포털에서 새 서비스를 목록에 추가할 수는 없습니다. 사용 가능한 서비스 집합은 VMware Cloud Director 시스템 관리자가 관리합니다.

절차

1 개체 그룹화 페이지를 엽니다.

옵션	작업
Edge 게이트웨이 서비스를 통해 열기	a 네트워킹 > Edge로 이동합니다. b 편집할 Edge 게이트웨이를 선택하고 서비스 구성 을 클릭합니다. c 개체 그룹화 를 클릭합니다.
보안 서비스를 통해 열기	a 네트워킹 > 보안으로 이동합니다. b 편집할 보안 서비스를 선택하고 서비스 구성 을 클릭합니다. c 개체 그룹화 를 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.

VMware Cloud Director 테넌트 포털의 [개체 그룹화] 페이지를 사용하여 사용 가능한 서비스 그룹을 볼 수 있습니다. [개체 그룹화] 페이지는 [서비스] 화면과 [Edge 게이트웨이] 화면에서 모두 사용할 수 있습니다.

테넌트 포털에서 서비스 그룹을 만들 수는 없습니다. 사용 가능한 서비스 그룹 집합은 VMware Cloud Director 시스템 관리자가 관리합니다.

절차

1 개체 그룹화 페이지를 엽니다.

옵션	작업
Edge 게이트웨이 서비스를 통해 열기	a 네트워킹 > Edge로 이동합니다. b 편집할 Edge 게이트웨이를 선택하고 서비스 구성 을 클릭합니다. c 개체 그룹화 를 클릭합니다.
보안 서비스를 통해 열기	a 네트워킹 > 보안으로 이동합니다. b 편집할 보안 서비스를 선택하고 서비스 구성 을 클릭합니다. c 개체 그룹화 를 클릭합니다.

2 서비스 그룹 탭을 클릭합니다.

결과

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

NSX Data Center for vSphere Edge 게이트웨이에 대한 통계 및 로그

NSX Data Center for vSphere 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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **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 게이트웨이를 통과하는 트래픽에 대한 그래프와 방화벽에 대한 그래프가 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

- **조직 관리자**인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.
- 역할에 **시스템 로깅 구성** 권한이 포함되어 있는지 확인합니다.

절차

- 1 Edge 게이트웨이 서비스를 엽니다.
 - a 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
 - b 편집할 Edge 게이트웨이를 선택하고 **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.

VMware Cloud Director 시스템 관리자가 VMware Cloud 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.

NSX Data Center for vSphere Edge 게이트웨이에 대한 SSH 명령줄 액세스 사용

Edge 게이트웨이에 대한 SSH 명령줄 액세스를 사용하도록 설정할 수 있습니다.

절차

1 Edge 게이트웨이 서비스를 엽니다.

- 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이**를 클릭합니다.
- 편집할 Edge 게이트웨이를 선택하고 **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 Data Center for vSphere Edge 게이트웨이에 대한 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 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 **네트워킹** 아래에서 **보안**을 선택합니다.
- 2 보안 서비스를 선택하고 **서비스 구성**을 클릭합니다.
- 3 **보안 태그** 탭을 클릭합니다.
- 4 **만들기**() 버튼을 클릭하고 보안 태그의 이름을 입력합니다.

5 (선택 사항) 보안 태그의 설명을 입력합니다.

6 (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.

7 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 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 **네트워킹** 아래에서 **보안**을 선택합니다.

2 보안 서비스를 선택하고 **서비스 구성**을 클릭합니다.

3 **보안 태그** 탭을 클릭합니다.

4 보안 태그 목록에서 편집할 보안 태그를 선택하고 **편집** 버튼을 클릭합니다.

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

오른쪽 패널의 가상 시스템에 보안 태그가 할당됩니다.

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

왼쪽 패널의 가상 시스템에는 할당된 보안 태그가 없습니다.

7 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 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 **네트워킹** 아래에서 **보안**을 선택합니다.
- 2 보안 서비스를 선택하고 **서비스 구성**을 클릭합니다.
- 3 **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.
- 4 **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 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 **네트워킹** 아래에서 **보안**을 선택합니다.

- 2 보안 서비스를 선택하고 **서비스 구성**을 클릭합니다.
- 3 **보안 태그** 탭을 클릭합니다.
- 4 보안 태그 목록에서 편집할 보안 태그를 선택합니다.
- 5 **편집** 버튼을 클릭합니다.
- 6 보안 태그의 이름과 설명을 편집합니다.
- 7 선택한 가상 시스템에 대해 태그를 할당하거나 태그 할당을 제거합니다.
- 8 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 [NSX Data Center for vSphere Edge 게이트웨이에 대한 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 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 **네트워킹** 아래에서 **보안**을 선택합니다.
- 2 보안 서비스를 선택하고 **서비스 구성**을 클릭합니다.
- 3 **보안 태그** 탭을 클릭합니다.
- 4 보안 태그 목록에서 삭제할 보안 태그를 선택합니다.
- 5 **삭제** 버튼을 클릭합니다.
- 6 **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 [NSX Data Center for vSphere Edge 게이트웨이에 대한 보안 그룹 작업](#) 항목을 참조하십시오.

NSX Data Center for vSphere Edge 게이트웨이에 대한 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 보안 서비스를 엽니다.

- a **네트워킹 > 보안**으로 이동합니다.
- b 보안 설정을 적용할 조직 VDC를 선택하고 **서비스 구성**을 클릭합니다.

테넌트 포털에서 보안 서비스가 열립니다.

- 2 **개체 그룹화 > 보안 그룹**으로 이동합니다.


보안 그룹 페이지가 열립니다.

- 3 **만들기**() 버튼을 클릭합니다.

- 4 보안 그룹의 이름과 설명(선택 사항)을 입력합니다.

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

- 5 (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.
- 6 (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.
- 7 (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.
- 8 변경 내용을 보존하려면 **유지**를 클릭합니다.

결과

이제 방화벽 규칙 같은 규칙에서 보안 그룹을 사용할 수 있습니다.

보안 그룹 편집

사용자 정의 보안 그룹을 편집할 수 있습니다.

절차

- 1 보안 서비스를 엽니다.
 - a **네트워킹 > 보안**으로 이동합니다.
 - b 보안 설정을 적용할 조직 VDC를 선택하고 **서비스 구성**을 클릭합니다.
테넌트 포털에서 보안 서비스가 열립니다.
- 2 **개체 그룹화 > 보안 그룹**으로 이동합니다.
보안 그룹 페이지가 열립니다.
- 3 편집할 보안 그룹을 선택합니다.
보안 그룹 목록 아래 보안 그룹의 세부 정보가 표시됩니다.
- 4 (선택 사항) 보안 그룹의 이름과 설명을 편집합니다.
- 5 (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.
- 6 (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.
- 7 (선택 사항) 삭제할 구성원 집합 옆에 있는 **삭제** 아이콘을 클릭하여 동적 구성원 집합을 삭제합니다.
- 8 (선택 사항) [구성원 포함] 목록 옆에 있는 **편집** 아이콘을 클릭하여 포함된 구성원 목록을 편집합니다.
- 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.
 - c [구성원 포함] 목록에서 개체를 제외하려면 오른쪽 패널에서 개체를 선택한 후 왼쪽 화살표를 클릭하여 왼쪽 패널로 이동합니다.
- 9 (선택 사항) [구성원 제외] 목록 옆에 있는 **편집** 아이콘을 클릭하여 제외된 구성원 목록을 편집합니다.
- 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.
 - c [구성원 제외] 목록에서 개체를 제외하려면 오른쪽 패널에서 개체를 선택한 후 왼쪽 화살표를 클릭하여 왼쪽 패널로 이동합니다.
- 10 **변경 내용 저장**을 클릭합니다.
- 보안 그룹에 대한 변경 내용이 저장됩니다.

보안 그룹 삭제

사용자 정의 보안 그룹을 삭제할 수 있습니다.

절차

- 1 보안 서비스를 엽니다.
 - a **네트워킹 > 보안**으로 이동합니다.
 - b 보안 설정을 적용할 조직 VDC를 선택하고 **서비스 구성**을 클릭합니다.

테넌트 포털에서 보안 서비스가 열립니다.
 - 2 **개체 그룹화 > 보안 그룹**으로 이동합니다.
- 보안 그룹** 페이지가 열립니다.
- 3 삭제할 보안 그룹을 선택합니다.
 - 4 **삭제** 버튼을 클릭합니다.
 - 5 **확인**을 클릭하여 삭제를 확인합니다.

결과

보안 그룹이 삭제됩니다.

NSX-T Data Center Edge 게이트웨이 관리

NSX-T Data Center Edge 게이트웨이는 IP 관리 속성 및 외부 네트워크에 연결할 수 있는 라우팅된 조직 VDC 네트워크 또는 데이터 센터 그룹 네트워크를 제공합니다. 방화벽, NAT(네트워크 주소 변환), IPSec VPN, DNS 전달 및 DHCP와 같은 서비스도 제공할 수 있으며, 이러한 서비스는 기본적으로 사용하도록 설정됩니다.

전용 외부 네트워크

가상 데이터 센터에서 완전히 라우팅된 네트워크 토폴로지를 제공하려는 경우 **시스템 관리자**가 외부 네트워크를 특정 NSX-T Data Center Edge 게이트웨이 전용으로 지정할 수 있습니다.

이 구성에서는 외부 네트워크와 NSX-T Data Center Edge 게이트웨이 간에 일대일 관계가 있으며 다른 Edge 게이트웨이는 외부 네트워크에 연결할 수 없습니다.

전용 외부 네트워크와 연결된 NSX-T Data Center Tier-0 논리적 라우터 또는 VRF 게이트웨이는 테넌트 네트워킹 스택의 일부입니다. 외부 네트워크는 VMware Cloud Director 네트워크 라우팅 도메인의 일부로 간주됩니다.

전용 외부 네트워크는 경로 보급 관리 및 BGP(경계 게이트웨이 프로토콜) 구성과 같은 추가적인 Edge 게이트웨이 라우팅 서비스를 제공합니다.

외부 네트워크에 알릴 Edge 게이트웨이에 연결된 네트워크를 결정할 수 있습니다. 이렇게 하면 NAT 라우팅 및 완전히 라우팅된 조직 가상 데이터 센터 네트워크를 혼합하여 사용할 수 있습니다.

NSX-T Data Center Edge 게이트웨이에 IP 집합 추가

방화벽 규칙을 생성하여 NSX-T Data Center Edge 게이트웨이에 추가하려면 먼저 IP 집합을 생성해야 합니다. IP 집합은 방화벽 규칙이 적용되는 개체 그룹입니다. 여러 개체를 IP 집합으로 결합하면, 생성되는 총 방화벽 규칙 수를 줄이는 데 도움이 됩니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 NSX-T Edge 게이트웨이를 클릭합니다.
- 3 **보안**에서 **IP 집합** 탭을 클릭하고 **새로 만들기**를 클릭합니다.
- 4 IP 집합의 이름과 설명(선택 사항)을 입력합니다.
- 5 IP 집합에 포함된 가상 시스템의 IP 주소 또는 IP 주소 범위를 입력하고 **추가**를 클릭합니다.
- 6 방화벽 그룹을 저장하려면 **저장**을 클릭합니다.

결과

IP 집합을 생성하여 NSX-T Edge 게이트웨이에 추가했습니다.

다음에 수행할 작업

[NSX-T Data Center Edge 게이트웨이 방화벽 규칙 추가](#)

NSX-T Data Center Edge 게이트웨이 방화벽 규칙 추가

NSX-T Data Center Edge 게이트웨이를 오가는 수신 및 송신 네트워크 트래픽을 제어하려면 방화벽 규칙을 생성합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 Edge 게이트웨이를 클릭합니다.
- 3 **방화벽** 화면이 [서비스] 섹션 아래에 아직 보이지 않으면 **방화벽** 탭을 클릭합니다.
- 4 **규칙 편집**을 클릭합니다.
- 5 **맨 위에 새로 만들기** 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.

옵션	설명
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 그룹으로 향하는 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. ■ 차단된 클라이언트에 알리지 않고 지정된 소스, 대상 및 서비스의 송신 또는 수신 트래픽을 차단하려면 삭제를 선택합니다. ■ 지정된 소스, 대상 및 서비스의 송신 또는 수신 트래픽을 차단하고 차단된 클라이언트에게 트래픽이 거부되었음을 알려려면 거부를 선택합니다.
IP 프로토콜	규칙을 IPv4 또는 IPv6 중 어느 트래픽에 적용할지 선택합니다.
방향	<p>규칙을 적용할 트래픽 방향을 선택합니다.</p> <p>참고 VMware Cloud Director 10.2.1 이상 버전에서는 이 옵션을 더 이상 사용할 수 없습니다.</p>
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.

VMware Cloud 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.

SNAT 없음 규칙은 조직 **VDC**에서 외부 네트워크 또는 다른 조직 **VDC** 네트워크로 전송되는 패킷의 내부 IP 주소 변환을 방지합니다.

DNAT 규칙은 외부 네트워크 또는 다른 조직 VDC 네트워크에서 조직 VDC 네트워크로 들어오는 패킷의 IP 주소(필요한 경우 포트 포함)를 변환합니다.

DNAT 없음 규칙은 외부 네트워크 또는 다른 조직 VDC 네트워크에서 조직 VDC로 들어오는 패킷의 외부 IP 주소 변환을 방지합니다.

NSX-T Data Center Edge 게이트웨이에서 NAT 서비스를 사용하는 경우 VMware Cloud Director는 자동 라우트 재분산을 지원합니다.

중요 Tanzu Kubernetes 클러스터를 사용하는 경우 충돌하는 규칙이 생성되지 않도록 Edge 게이트웨이에서 생성된 시스템 SNAT 규칙을 기록해 둡니다

사전 요구 사항

규칙을 추가할 Edge 게이트웨이 인터페이스에 공개 IP 주소가 추가된 상태여야 합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 Edge 게이트웨이를 클릭하고 **서비스**에서 **NAT**를 클릭합니다.
- 3 규칙을 추가하려면 **새로 만들기**를 클릭합니다.
- 4 SNAT 또는 SNAT 없음 규칙(내부에서 외부로 이동)을 구성합니다.

옵션	설명
이름	규칙의 의미 있는 이름을 입력합니다.
설명	(선택 사항) 규칙에 대한 설명을 입력합니다.
인터페이스 유형	드롭다운 메뉴에서 SNAT 또는 SNAT 없음을 선택합니다.
외부 IP	<p>생성하는 규칙의 유형에 따라 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> ■ SNAT 규칙을 생성하는 경우 SNAT 규칙을 구성하는 Edge 게이트웨이의 공개 IP 주소를 입력합니다. ■ SNAT 없음 규칙을 생성하는 경우 텍스트 상자를 비워 둡니다.
내부 IP	외부 네트워크로 트래픽을 보낼 수 있도록 SNAT를 구성하려는 가상 시스템의 IP 주소나 IP 주소 목록을 입력합니다.

옵션	설명
대상 IP	(선택 사항) 규칙을 특정 도메인으로 전송되는 트래픽에 대해서만 적용하려는 경우 이 도메인에 대한 IP 주소 또는 IP 주소 목록을 입력합니다. 이 텍스트 상자를 비워두는 경우 SNAT 규칙이 로컬 서브넷 외부의 모든 대상에 적용됩니다.
고급 설정(선택 사항)	<p>몇 가지 추가 설정을 보려면 고급 설정 탭을 클릭합니다.</p> <p>상태</p> <p>생성 시 규칙을 활성화하려면 상태 옵션을 사용하도록 전환합니다.</p> <p>로깅</p> <p>이 규칙에 의해 수행된 주소 변환을 기록하려면 로깅 옵션을 토글하여 켭니다.</p> <p>우선순위</p> <p>주소에 여러 NAT 규칙이 있는 경우 규칙에 서로 다른 우선 순위를 할당하여 규칙이 적용되는 순서를 결정할 수 있습니다. 값이 낮을수록 규칙의 우선 순위는 더 높습니다.</p> <p>방화벽 일치</p> <p>방화벽 일치 규칙을 설정하여 NAT 중에 방화벽이 적용되는 방식을 결정할 수 있습니다. 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> ■ NAT 규칙의 내부 주소에 방화벽 규칙을 적용하려면 내부 주소 일치를 선택합니다. ■ NAT 규칙의 외부 주소에 방화벽 규칙을 적용하려면 외부 주소 일치를 선택합니다. ■ 방화벽 규칙 적용을 건너뛰려면 우회를 선택합니다.

5 DNAT 또는 DNAT 없음 규칙(외부에서 내부로 이동)을 구성합니다.

옵션	설명
이름	규칙의 의미 있는 이름을 입력합니다.
설명	(선택 사항) 규칙에 대한 설명을 입력합니다.
인터페이스 유형	드롭다운 메뉴에서 DNAT 또는 DNAT 없음을 선택합니다.
외부 IP	DNAT 규칙을 구성하는 Edge 게이트웨이의 공개 IP 주소를 입력합니다. 입력하는 IP 주소는 Edge 게이트웨이에 하위 할당되어야 합니다.
외부 포트	(선택 사항) 가상 시스템으로 인바운드된 패킷에 대해 DNAT 규칙이 변환되는 포트를 입력합니다.
내부 IP	<p>생성하는 규칙의 유형에 따라 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> ■ DNAT 규칙을 생성하는 경우 외부 네트워크에서 들어오는 트래픽을 수신할 수 있도록 DNAT를 구성하려는 가상 시스템의 IP 주소나 IP 주소 목록을 입력합니다. ■ DNAT 없음 규칙을 생성하는 경우 텍스트 상자를 비워 둡니다.

옵션	설명
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.
고급 설정(선택 사항)	몇 가지 추가 설정을 보려면 고급 설정 탭을 클릭합니다.
	<p>상태</p> <p>생성 시 규칙을 활성화하려면 상태 옵션을 사용하도록 전환합니다.</p> <p>로깅</p> <p>이 규칙에 의해 수행된 주소 변환을 기록하려면 로깅 옵션을 토글하여 켭니다.</p> <p>우선순위</p> <p>주소에 여러 NAT 규칙이 있는 경우 규칙에 서로 다른 우선 순위를 할당하여 규칙이 적용되는 순서를 결정할 수 있습니다. 값이 낮을수록 규칙의 우선 순위는 더 높습니다.</p> <p>방화벽 일치</p> <p>방화벽 일치 규칙을 설정하여 NAT 중에 방화벽이 적용되는 방식을 결정할 수 있습니다. 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> ■ NAT 규칙의 내부 주소에 방화벽 규칙을 적용하려면 내부 주소 일치를 선택합니다. ■ NAT 규칙의 외부 주소에 방화벽 규칙을 적용하려면 외부 주소 일치를 선택합니다. ■ 방화벽 규칙 적용을 건너뛰려면 우회를 선택합니다.

6 **저장**을 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

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 Edge 게이트웨이를 클릭하고 **IP 관리**에서 **DNS**를 클릭합니다.
- 3 **DNS 전달자** 섹션에서 **편집**을 클릭합니다.
- 4 DNS 전달자 서비스를 사용하도록 설정하려면 **상태** 토글을 설정합니다.
- 5 기본 DNS 영역의 이름과 설명(선택 사항)을 입력합니다.
- 6 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.

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 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 Edge 게이트웨이를 클릭합니다.
- 3 **보안**에서 **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 쉼표로 구분하여 입력하고 **저장**을 클릭합니다.

다음에 수행할 작업

애플리케이션 포트 프로파일을 사용하여 방화벽 및 NAT 규칙을 생성합니다. [NSX-T Data Center Edge 게이트웨이 방화벽 규칙 추가](#) 및 [NSX-T Edge 게이트웨이에 SNAT 또는 DNAT 규칙 추가](#) 항목을 참조하십시오.

NSX-T Data Center Edge 게이트웨이의 IPsec 정책 기반 VPN

버전 10.1부터 VMware Cloud Director는 NSX-T Data Center Edge 게이트웨이 인스턴스와 원격 사이트 사이에 사이트 간 정책 기반 IPsec VPN을 지원합니다.

IPsec VPN은 NSX-T Data Center를 사용하는 원격 사이트 또는 IPsec을 지원하는 VPN 게이트웨이나 타사 하드웨어 라우터가 있는 원격 사이트와 Edge 게이트웨이 사이에 사이트 간 연결을 제공합니다.

정책 기반 IPsec VPN을 사용하려면 VPN 정책을 패킷에 적용하여 VPN 터널을 통과하기 전에 IPsec에서 보호할 트래픽을 결정해야 합니다. 이러한 유형의 VPN은 로컬 네트워크 토폴로지 및 구성이 변경될 때 변경 내용을 수용하도록 VPN 정책 설정도 업데이트되어야 하기 때문에 정적으로 간주됩니다.

NSX-T Data Center Edge 게이트웨이는 IPsec 트래픽이 라우팅 우선 순위를 갖는 분할 터널 구성을 지원합니다.

NSX-T Edge 게이트웨이에서 IPsec VPN을 사용하는 경우 VMware Cloud Director는 자동 라우트 재분산을 지원합니다.

NSX-T 정책 기반 IPsec VPN 구성

NSX-T Data Center Edge 게이트웨이와 원격 사이트 간에 사이트 간 연결을 구성할 수 있습니다. 원격 사이트는 NSX-T Data Center를 사용하거나 IPsec을 지원하는 VPN 게이트웨이 또는 타사 하드웨어 라우터를 사용해야 합니다.

NSX-T Data Center Edge 게이트웨이에서 IPsec VPN을 구성하는 경우 VMware Cloud Director는 자동 라우트 재분산을 지원합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 Edge 게이트웨이를 클릭합니다.
- 3 **서비스**에서 **IPsec VPN**을 클릭합니다.
- 4 IPsec VPN 터널을 구성하려면 **새로 만들기**를 클릭합니다.
- 5 IPsec VPN 터널의 이름과 설명(선택 사항)을 입력합니다.
- 6 생성 시 터널을 사용하도록 설정하려면 **사용** 옵션을 사용하도록 전환합니다.
- 7 입력할 미리 공유한 키를 선택합니다.

참고 미리 공유한 키는 IPsec VPN 터널의 다른 쪽 끝에서 동일해야 합니다.

- 8 로컬 끝점에 대해 Edge 게이트웨이에서 사용할 수 있는 IP 주소 중 하나를 입력합니다.

참고 IP 주소는 Edge 게이트웨이의 기본 IP이거나 외부 네트워크에서 Edge 게이트웨이에 개별적으로 할당된 IP 주소여야 합니다.

- 9 IPsec VPN 터널에 사용할 하나 이상의 로컬 IP 서브넷 주소를 CIDR 표기법으로 입력합니다.
- 10 원격 사이트의 IP 주소를 입력합니다.
- 11 IPsec VPN 터널에 사용할 하나 이상의 원격 IP 서브넷 주소를 CIDR 표기법으로 입력합니다.
- 12 (선택 사항) 로깅을 사용하도록 설정하려면 **로깅** 옵션을 전환합니다.
- 13 **저장**을 클릭합니다.

14 터널이 작동하는지 확인하려면 해당 터널을 선택하고 **통계 보기**를 클릭합니다.

터널이 작동하는 경우 **터널 상태** 및 **IKE 서비스 상태**가 모두 작동으로 표시됩니다.

결과

새로 만들어진 IPSec VPN 터널은 **IPSec VPN** 보기에 나열됩니다. IPSec VPN 터널은 기본 보안 프로파일과 함께 만들어집니다.

다음에 수행할 작업

IPSec VPN 터널 설정을 편집하고 필요에 따라 해당 보안 프로파일을 사용자 지정할 수 있습니다.

IPSec VPN 터널의 보안 프로파일 사용자 지정

생성 시 IPSec VPN 터널에 할당되었던 시스템 생성 보안 프로파일을 사용하지 않기로 결정한 경우 이를 사용자 지정할 수 있습니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 Edge 게이트웨이를 클릭합니다.
- 3 **서비스**에서 **IPSec VPN**을 클릭합니다.
- 4 IPSec VPN 터널을 선택하고 **보안 프로파일 사용자 지정**을 클릭합니다.
- 5 IKE 프로파일을 구성합니다.

IKE(Internet Key Exchange) 프로파일은 IKE 터널을 설정할 때 네트워크 사이트 간에 공유 암호를 인증, 암호화 및 설정하는 데 사용되는 알고리즘에 대한 정보를 제공합니다.

- a IPSec 프로토콜 그룹에서 **SA(보안 연결)**를 설정할 IKE 프로토콜 버전을 선택합니다.

옵션	설명
IKEv1	이 옵션을 선택하면 IPSec VPN이 시작되고 IKEv1 프로토콜에만 응답합니다.
IKEv2	기본 옵션입니다. 이 버전을 선택하면 IPSec VPN이 시작되고 IKEv2 프로토콜에만 응답합니다.
IKE-Flex	이 옵션을 선택하는 경우 IKEv2 프로토콜을 사용한 터널 설정이 실패하면 소스 사이트가 폴백되지 않고 IKEv1 프로토콜을 사용한 연결을 시작합니다. 대신 원격 사이트에서 IKEv1 프로토콜을 사용한 연결을 시작하면 연결이 허용됩니다.

- b IKE(Internet Key Exchange) 협상 중에 사용할 지원되는 암호화 알고리즘을 선택합니다.
- c **다이제스트** 드롭다운 메뉴에서 IKE 협상 중에 사용할 보안 해싱 알고리즘을 선택합니다.
- d **Diffie-Hellman 그룹** 드롭다운 메뉴에서 피어 사이트 및 Edge 게이트웨이가 비보안 통신 채널을 통해 공유 암호를 설정하도록 허용하는 암호화 체계 중 하나를 선택합니다.
- e (선택 사항) **연결 수명** 텍스트 상자에서 IPSec 터널을 재설정해야 하는 기본 시간(초)을 수정합니다.

6 IPSec VPN 터널을 구성합니다.

- a 전달 완전 보안을 사용하도록 설정하려면 옵션의 토글을 켭니다.
- b 조각 모음 정책을 선택합니다.

조각 모음 정책은 내부 패킷에 있는 조각 모음 비트를 처리하는 데 도움이 됩니다.

옵션	설명
복사	조각 모음 비트를 내부 IP 패킷에서 외부 패킷으로 복사합니다.
지우기	내부 패킷에 있는 조각 모음 비트를 무시합니다.

- c IKE(Internet Key Exchange) 협상 중에 사용할 지원되는 암호화 알고리즘을 선택합니다.
- d **다이제스트** 드롭다운 메뉴에서 IKE 협상 중에 사용할 보안 해싱 알고리즘을 선택합니다.
- e **Diffie-Hellman 그룹** 드롭다운 메뉴에서 피어 사이트 및 Edge 게이트웨이가 비보안 통신 채널을 통해 공유 암호를 설정하도록 허용하는 암호화 체계 중 하나를 선택합니다.
- f (선택 사항) **연결 수명** 텍스트 상자에서 IPSec 터널을 재설정해야 하는 기본 시간(초)을 수정합니다.

7 (선택 사항) **검색 간격** 텍스트 상자에서 비활성 피어 감지를 위한 기본 시간(초)을 수정합니다.

8 저장을 클릭합니다.

결과

IPSec VPN 보기에서 IPSec VPN 터널의 보안 프로파일이 **사용자 정의**로 표시됩니다.

전용 외부 네트워크 서비스 구성

가상 데이터 센터에서 완전히 라우팅된 네트워크 토폴로지를 제공하려는 경우 **시스템 관리자**가 외부 네트워크를 특정 NSX-T Data Center Edge 게이트웨이 전용으로 지정할 수 있습니다.

전용 외부 네트워크를 사용할 때 경로 보급 관리 및 BGP(경계 게이트웨이 프로토콜) 구성과 같은 추가적인 라우팅 서비스를 구성할 수 있습니다.

절차

1 경로 보급 관리

경로 보급을 사용하여 조직 VDC(가상 데이터 센터)에서 완전히 라우팅된 네트워크 환경을 생성할 수 있습니다.

2 BGP 일반 설정 구성

전용 외부 네트워크가 있는 NSX-T Data Center Edge 게이트웨이와 물리적 인프라의 라우터 간에 eBGP(외부 경계 게이트웨이 프로토콜) 또는 iBGP(내부 경계 게이트웨이 프로토콜) 연결을 구성할 수 있습니다.

3 IP 접두사 목록 만들기

하나 또는 여러 개의 IP 주소가 들어 있는 IP 접두사 목록을 만들 수 있습니다. IP 접두사 목록을 사용하면 경로 보급에 대해 액세스 권한이 있는 BGP 인접 라우터를 할당할 수 있습니다.

4 BGP 인접 라우터 추가

BGP 라우팅 인접 라우터를 추가할 때 개별 설정을 구성할 수 있습니다.

경로 보급 관리

경로 보급을 사용하여 조직 VDC(가상 데이터 센터)에서 완전히 라우팅된 네트워크 환경을 생성할 수 있습니다.

전용 외부 네트워크에 보급할 NSX-T Data Center Edge 게이트웨이에 연결된 네트워크 서브넷을 결정할 수 있습니다.

서브넷이 보급 필터에 추가되지 않은 경우 해당 경로는 외부 네트워크에 보급되지 않으며 서브넷은 개인으로 유지됩니다.

참고 VMware Cloud Director는 보급된 경로 내에 속하는 모든 조직 VDC 네트워크를 보급합니다. 따라서 서 보급된 네트워크의 일부인 각 서브넷에 대해 필터를 생성할 필요가 없습니다.

경로 보급은 NSX-T Data Center Edge 게이트웨이에 자동으로 구성됩니다.

NSX-T Edge 게이트웨이에서 경로 보급을 사용하는 경우 VMware Cloud Director는 자동 라우트 재분산을 지원합니다. 라우트 재분산은 전용 외부 네트워크를 나타내는 Tier-0 논리적 라우터에 자동으로 구성됩니다.

사전 요구 사항

- **시스템 관리자**가 조직의 NSX-T Data Center Edge 게이트웨이 전용으로 사용할 수 있는 외부 네트워크를 지정했는지 확인합니다.
- **조직 관리자**인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 Edge 게이트웨이를 클릭합니다.
- 3 **라우팅**에서 **경로 보급** 및 **편집**을 클릭합니다.
- 4 보급될 서브넷을 추가하려면 **추가**를 클릭합니다.
- 5 IPv4 또는 IPv6 서브넷을 추가합니다.

`network_gateway_IP_address/subnet_prefix_length` 형식(예: `192.167.1.1/24`)을 사용합니다.

BGP 일반 설정 구성

전용 외부 네트워크가 있는 NSX-T Data Center Edge 게이트웨이와 물리적 인프라의 라우터 간에 eBGP(외부 경계 게이트웨이 프로토콜) 또는 iBGP(내부 경계 게이트웨이 프로토콜) 연결을 구성할 수 있습니다.

BGP는 AS(독립 시스템) 간 여러 경로를 지정하는 접두사 또는 IP 네트워크 테이블을 사용하여 라우팅과 관련된 핵심 결정을 내립니다.

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.

참고 VRF 게이트웨이에서 지원하는 외부 네트워크에 연결된 Edge 게이트웨이에서 로컬 AS 번호 및 정당한 다시 시작 설정은 읽기 전용입니다. **시스템 관리자**는 NSX-T Data Center의 상위 Tier-0 게이트웨이에서 이러한 설정을 편집할 수 있습니다.

사전 요구 사항

- **시스템 관리자**가 조직의 NSX-T Data Center Edge 게이트웨이 전용으로 사용할 수 있는 외부 네트워크를 지정했는지 확인합니다.
- **조직 관리자**인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 Edge 게이트웨이를 클릭합니다.
- 3 **라우팅**에서 **BGP**를 클릭하고 **구성**에서 **편집**을 클릭합니다.
- 4 **상태** 옵션을 사용하도록 전환하여 BGP를 활성화합니다.
- 5 프로토콜의 로컬 **AS**(독립 시스템) 기능에 사용할 **AS ID** 번호를 입력합니다.

VMware Cloud Director는 로컬 AS 번호를 Edge 게이트웨이에 할당합니다. Edge 게이트웨이는 다른 독립 시스템의 해당 BGP 인접 라우터에 연결할 때 이 ID를 알립니다.

6 드롭다운 메뉴에서 **정상적인 다시 시작 모드** 옵션을 선택합니다.

옵션	설명
도우미 및 정상적인 다시 시작	모든 게이트웨이의 BGP 피어링은 항상 활성 상태이므로 Edge 게이트웨이에서 정상적인 다시 시작 기능을 활성화하는 것은 좋지 않습니다. 페일오버의 경우 정상적인 다시 시작 기능은 원격 인접 라우터가 대체 Tier-0 게이트웨이를 선택하는 데 걸리는 시간을 증가시킵니다. 이로 인해 BFD 기반 컨버전스에 지연이 발생합니다. 참고 Edge 게이트웨이 구성은 인접 라우터 관련 구성이 이를 재정의하지 않으면 모든 BGP 인접 라우터에 적용됩니다.
도우미만	정상적인 다시 시작이 가능한 인접 라우터에서 학습한 경로와 연결된 트래픽의 중단을 줄이거나 제거하는 데 유용합니다. 인접 라우터는 다시 시작이 진행되는 동안 해당 전달 테이블을 보존할 수 있어야 합니다.
사용 안 함	Edge 게이트웨이에서 정상적인 다시 시작 모드를 비활성화합니다.

7 (선택 사항) 정상적인 다시 시작 타이머의 기본값을 변경합니다.

8 (선택 사항) 오래된 경로 타이머의 기본값을 변경합니다.

9 **ECMP** 옵션을 사용하도록 전환하여 ECMP를 활성화합니다.

10 **저장**을 클릭합니다.

다음에 수행할 작업

- [IP 접두사 목록 만들기](#)
- [BGP 인접 라우터 추가](#)

IP 접두사 목록 만들기

하나 또는 여러 개의 IP 주소가 들어 있는 IP 접두사 목록을 만들 수 있습니다. IP 접두사 목록을 사용하면 경로 보급에 대해 액세스 권한이 있는 BGP 인접 라우터를 할당할 수 있습니다.

IP 접두사 목록은 BGP 인접 라우터 필터를 통해 참조되어 BGP 피어 간에 교환되는 BGP 업데이트의 수를 제한합니다. 경로 필터링을 사용하여 BGP 업데이트에 필요한 시스템 리소스의 수를 줄일 수 있습니다.

예를 들어 IP 접두사 목록에 IP 주소 192.168.100.3/27을 추가하고 경로가 Edge 게이트웨이에 재분산되지 못하도록 거부할 수 있습니다.

또한 IP 주소에 less than or equal to(le) 및 greater than or equal to(ge) 한정자를 추가하여 경로 재분산을 허용하거나 제한할 수 있습니다. 예를 들어 192.168.100.3/27 ge 26 le 32 한정자는 길이가 26비트보다 크거나 같고 32비트보다 작거나 같은 서브넷 마스크와 일치합니다.

사전 요구 사항

- **시스템 관리자**가 조직의 NSX-T Data Center Edge 게이트웨이 전용으로 사용할 수 있는 외부 네트워크를 지정했는지 확인합니다.
- **조직 관리자**인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.

■ BGP 일반 설정 구성.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 Edge 게이트웨이를 클릭합니다.
- 3 **라우팅**에서 **BGP** 및 **IP 접두사 목록**을 클릭합니다.
- 4 IP 접두사 목록을 추가하려면 **새로 만들기**를 클릭합니다.
- 5 접두사 목록의 이름과 설명(선택 사항)을 입력합니다.
- 6 **새로 만들기**를 클릭하고 접두사에 대한 CIDR 표기법을 추가합니다.
- 7 드롭다운 메뉴에서 접두사에 적용할 작업을 선택합니다.
- 8 (선택 사항) greater than or equal to 및 less than or equal to 한정자를 입력하여 경로 재분산을 허용하거나 제한합니다.

다음에 수행할 작업

- 필요에 따라 IP 접두사 목록을 편집하거나 삭제할 수 있습니다.
- 경로 필터링을 구성합니다. **BGP 인접 라우터** 추가의 내용을 참조하십시오.

BGP 인접 라우터 추가

BGP 라우팅 인접 라우터를 추가할 때 개별 설정을 구성할 수 있습니다.

사전 요구 사항

- **시스템 관리자**가 조직의 NSX-T Data Center Edge 게이트웨이 전용으로 사용할 수 있는 외부 네트워크를 지정했는지 확인합니다.
- **조직 관리자**인지 또는 동등한 권한 집합을 포함하는 역할을 할당 받았는지 확인합니다.
- Edge 게이트웨이에 대한 글로벌 BGP 설정을 구성했는지 확인합니다. **BGP 일반 설정 구성**의 내용을 참조하십시오.
- 경로 필터링을 사용하는 경우 IP 접두사 목록을 생성했는지 확인합니다. **IP 접두사 목록 만들기**의 내용을 참조하십시오.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 Edge 게이트웨이를 클릭합니다.
- 3 **라우팅**에서 **BGP** 및 **인접 라우터**를 클릭합니다.
- 4 새 BGP 인접 라우터를 추가하려면 **새로 만들기**를 클릭합니다.

5 새 BGP 인접 라우터에 대한 일반 설정을 입력합니다.

- a 새 BGP 인접 라우터에 대한 IPv4 또는 IPv6 주소를 입력합니다.
- b 원격 AS(독립 시스템) 번호를 ASPLAIN 형식으로 입력합니다.
- c BGP 피어에 연결 유지 메시지를 보내는 시간 간격을 입력합니다.
- d BGP 피어 비활성 상태를 선언하기 전 시간 간격을 입력합니다.
- e 드롭다운 메뉴에서 이 인접 라우터에 대한 **정상적인 다시 시작 모드** 옵션을 선택합니다.

옵션	설명
사용 안 함	글로벌 Edge 게이트웨이 설정을 재정의하고 이 인접 라우터에 대해 정상적인 다시 시작 모드를 비활성화합니다.
도우미만	글로벌 Edge 게이트웨이 설정을 재정의하고 이 인접 라우터에 대해 정상적인 다시 시작 모드를 도우미만 으로 구성합니다.
정상적인 다시 시작 및 도우미	글로벌 Edge 게이트웨이 설정을 재정의하고 이 인접 라우터에 대해 정상적인 다시 시작 모드를 정상적인 다시 시작 및 도우미 로 구성합니다.

- f **AllowAS-in** 토글을 전환하여 AS가 동일한 경로를 수신하도록 설정합니다.
- g BGP 인접 라우터에 인증이 필요한 경우 BGP 인접 라우터에 대한 암호를 입력합니다.

6 새 BGP 인접 라우터에 대한 BFD(Bidirectional Forwarding Detection) 설정을 구성합니다.

- a (선택 사항) **BFD** 옵션을 전환하여 실패 감지를 위해 BFD를 사용하도록 설정합니다.
- b [BFD 간격] 텍스트 상자에 하트비트 패킷을 보내기 위한 시간 간격을 정의합니다.
- c **다중 비활성** 텍스트 상자에 BFD가 다운되었음을 선언하기 전 BGP 인접 라우터가 하트비트 패킷을 보내지 못할 수 있는 횟수를 입력합니다.

7 (선택 사항) 경로 필터링을 구성합니다.

- a **IP 주소 패밀리** 드롭다운 메뉴에서 IP 주소 패밀리를 선택합니다.
- b 인바운드 필터를 구성하려면 IP 접두사 목록을 선택합니다.
- c 아웃바운드 필터를 구성하려면 IP 접두사 목록을 선택합니다.

8 저장을 클릭합니다.

다음에 수행할 작업

각 BGP 인접 라우터의 상태를 볼 수 있으며, 필요에 따라 BGP 인접 라우터를 편집 또는 삭제할 수 있습니다.

NSX Advanced 로드 밸런싱 사용

조직 관리자는 여러 서버 풀에 트래픽을 분산하는 가상 서비스를 구성하여 NSX-T Data Center에서 지원하는 데이터 센터의 워크로드 균형을 조정할 수 있습니다.

VMware Cloud Director는 버전 10.2부터 VMware NSX Advanced Load Balancer(Avi Networks)의 기능을 사용하여 로드 밸런싱 서비스를 제공합니다.

VMware Cloud Director는 NSX-T Data Center Edge 게이트웨이에서 구성할 수 있는 L4 및 L7 로드 밸런싱 기능을 지원합니다.

수준 4 로드 밸런싱(L4)은 네트워크 및 전송 계층 프로토콜(예: IP 주소 및 TCP 포트)의 데이터를 기반으로 트래픽을 전송합니다.

수준 7 로드 밸런싱(L7)은 HTTP 헤더, URI(Uniform Resource Identifier), SSL 세션 ID, HTML 양식 데이터와 같은 특성을 기반으로 트래픽을 분산합니다.

NSX-T Data Center Edge 게이트웨이에서 로드 밸런서 사용

조직 관리자가 로드 밸런싱 서비스를 구성할 수 있으려면 먼저 **시스템 관리자**가 NSX-T Data Center Edge 게이트웨이에서 로드 밸런서를 사용하도록 설정해야 합니다.

사전 요구 사항

- **시스템 관리자** 권한이 있는지 확인합니다.
- 클라우드 인프라에 VMware NSX Advanced Load Balancer를 통합했는지 확인합니다. NSX Advanced Load Balancer 관리에 대한 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드" 항목을 참조하십시오.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 로드 밸런싱을 사용하도록 설정하려는 NSX-T Data Center Edge 게이트웨이를 클릭합니다.
- 3 [로드 밸런서]에서 **일반 설정**을 클릭합니다.
- 4 **편집**을 클릭하고 **로드 밸런서 상태** 옵션을 사용하도록 전환합니다.
- 5 가상 서비스를 만들기 위해 IP 주소를 사용할 서비스 네트워크 서브넷에 대한 네트워크 CIDR을 입력합니다.

기본값 사용 확인란을 선택하면 기본 서비스 네트워크 서브넷을 사용할 수 있습니다.

- 6 **저장**을 클릭합니다.

다음에 수행할 작업

[NSX-T Data Center Edge 게이트웨이에 서비스 엔진 그룹 할당](#).

NSX-T Data Center Edge 게이트웨이에 서비스 엔진 그룹 할당

조직 관리자가 NSX-T Data Center Edge 게이트웨이에서 로드 밸런싱 서비스를 구성할 수 있으려면 먼저 **시스템 관리자**가 Edge 게이트웨이에 서비스 엔진 그룹을 할당해야 합니다.

NSX Advanced Load Balancer에서 제공하는 로드 밸런싱 계산 인프라는 서비스 엔진 그룹으로 구성됩니다. **시스템 관리자**는 하나 이상의 서비스 엔진 그룹을 NSX-T Data Center Edge 게이트웨이에 할당할 수 있습니다.

단일 Edge 게이트웨이에 할당된 모든 서비스 엔진 그룹은 동일한 서비스 네트워크를 사용합니다.

사전 요구 사항

- **시스템 관리자** 권한이 있는지 확인합니다.
- **NSX-T Data Center Edge** 게이트웨이에서 로드 밸런서 사용

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 서비스 엔진 그룹을 할당하려는 NSX-T Data Center Edge 게이트웨이를 클릭합니다.
- 3 [로드 밸런서] 아래에서 **서비스 엔진 그룹**을 클릭합니다.
- 4 **추가**를 클릭합니다.
- 5 목록에서 사용 가능한 서비스 엔진 그룹을 선택합니다.
- 6 Edge 게이트웨이에 배치할 수 있는 최대 가상 서비스 수에 해당하는 숫자를 입력합니다.
- 7 Edge 게이트웨이에서 사용할 수 있는 보장된 가상 서비스 수를 입력합니다.
- 8 설정을 확인하려면 **저장**을 클릭합니다.

서비스 엔진 그룹의 설정 편집

시스템 관리자는 서비스 엔진 그룹의 지원되는 최대 가상 서비스 수와 예약된 가상 서비스 수를 편집할 수 있습니다.

서비스 엔진 그룹을 동기화한 후 지원되는 가상 서비스의 새로운 최대 수가 예약된 가상 서비스의 수보다 적으면 서비스 엔진 그룹이 초과 할당된 것으로 표시됩니다.

서비스 엔진 그룹이 초과 할당되면, 가상 서비스를 만드는 Edge 게이트웨이에 충분한 예약 용량이 있는 경우에도 새 가상 서비스 생성이 실패할 수 있습니다.

가상 서비스 만들기 실패를 방지하려면 서비스 엔진 그룹의 설정을 편집할 때 지원되는 최대 가상 서비스 수를 초기에 예약된 가상 서비스 수 미만으로 줄이지 마십시오.

사전 요구 사항

- **시스템 관리자** 권한이 있는지 확인합니다.
- **NSX-T Data Center Edge** 게이트웨이에서 로드 밸런서 사용
- **NSX-T Data Center Edge** 게이트웨이에 서비스 엔진 그룹 할당에 서비스 엔진 그룹을 할당합니다.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.

2 서비스 엔진 그룹이 할당된 NSX-T Data Center Edge 게이트웨이를 클릭합니다.

3 [로드 밸런서] 아래에서 **서비스 엔진 그룹**을 클릭합니다.

4 **편집**을 클릭합니다.

5 Edge 게이트웨이에서 사용할 수 있는 최대 허용 가상 서비스 수를 편집합니다.

필수인 경우가 아니면 숫자를 줄이지 마십시오. 그렇지 않으면 가상 서비스를 생성할 때 장애가 발생할 수 있습니다.

6 Edge 게이트웨이에서 사용할 수 있는 보장된 가상 서비스 수를 편집합니다.

7 **저장**을 클릭합니다.

로드 밸런서 서버 풀 추가

서버 풀은 동일한 애플리케이션을 실행하고 고가용성을 제공하기 위해 구성하는 하나 이상 서버의 그룹입니다.

사전 요구 사항

- **조직 관리자** 권한이 있는지 확인합니다.
- **시스템 관리자**가 NSX-T Edge 게이트웨이에서 로드 밸런싱을 사용하도록 설정했는지 확인합니다.
- **시스템 관리자**가 Edge 게이트웨이에 서비스 엔진 그룹을 하나 이상 할당했는지 확인합니다.

절차

1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.

2 로드 밸런서 풀을 구성하려는 NSX-T Data Center Edge 게이트웨이를 클릭합니다.

3 [로드 밸런서]에서 **풀**을 클릭한 다음 **추가**를 클릭합니다.

4 로드 밸런서 풀에 대한 일반 설정을 구성합니다.

- a 서버 풀의 의미 있는 이름과 설명(선택 사항)을 입력합니다.
- b 알고리즘 밸런싱 방법을 선택합니다.

로드 밸런싱 알고리즘은 들어오는 연결이 서버 풀의 구성원 간에 분산되는 방식을 정의합니다.

옵션	설명
최소 연결	현재 연결 수가 가장 적은 서버로 새 연결이 전송됩니다.
라운드 로빈	풀의 다음 적격 서버에 순차적으로 새 연결이 전송됩니다.
가장 빠른 응답	새 연결 또는 요청에 대해 가장 빠른 응답을 제공하는 서버로 새 연결이 전송됩니다.
일관된 해시	클라이언트의 IP 주소를 사용해 IP 해시 키를 생성하여 서버 전체에 새 연결이 분산됩니다.
최소 로드	서버에 있는 연결 수에 관계없이 로드가 가장 적은 서버로 새 연결이 전송됩니다.
최소 서버	모든 연결 또는 요청을 모든 서버에 분산하려고 시도하는 대신 로드 밸런서가 현재 클라이언트 로드를 충족하는 데 필요한 최소 서버 수를 결정합니다.
임의	로드 밸런서가 서버를 임의로 선택합니다.
가장 적은 작업	서버 피드백에 따라 로드가 적절히 밸런싱됩니다.
코어 선호도	각 CPU 코어가 서버 하위 집합을 사용하고 각 서버는 코어의 하위 집합에서 사용됩니다. 기본적으로 서버와 코어 간에 다대다 매핑을 제공합니다.

- c 생성 시 서버 풀을 사용하도록 설정하려면 **상태** 옵션을 사용하도록 전환합니다.
- d 풀 구성원으로 전송되는 트래픽에 사용할 기본 대상 서버 포트를 입력합니다.
- e (선택 사항) **정상적인 사용 안 함 시간 초과** 텍스트 상자에 풀 멤버를 정상적으로 비활성화하는 최대 시간(분)을 입력합니다.
가상 서비스는 비활성화된 구성원에 대한 기존 연결을 닫기 전에 지정된 시간 동안 대기합니다.
- f (선택 사항) 패시브 상태 모니터를 활성화하려면 **패시브 상태 모니터** 옵션을 사용하도록 전환합니다.
- g (선택 사항) [활성 상태 모니터]를 선택합니다.

옵션	설명
HTTP	상태를 검증하는 데 HTTP 요청 및 응답이 사용됩니다.
HTTPS	HTTPS 암호화된 웹 서버에 대해 상태를 검증하는 데 사용됩니다.
TCP	상태를 검증하는 데 TCP 연결이 사용됩니다.
UDP	상태를 검증하는 데 UDP 데이터그램이 사용됩니다.
PING	상태를 검증하는 데 ICMP ping이 사용됩니다.

5 서버 풀에 구성원을 추가합니다.

- a **구성원** 탭을 클릭하고 **추가**를 클릭합니다.
- b 풀 구성원의 IP 주소를 입력합니다.
- c **상태** 옵션을 사용하도록 전환하여 풀 구성원을 사용하도록 설정합니다.
- d (선택 사항) 서버 풀 구성원에 대한 사용자 지정 포트를 추가합니다.
포트 번호는 기본적으로 풀에 대해 입력한 대상 포트에 설정됩니다.
- e 풀 구성원에 대한 비율을 입력합니다.

각 풀 구성원의 비율은 각 서버 풀 구성원으로 이동하는 트래픽을 나타냅니다. 비율이 2인 서버는 비율이 1인 서버보다 두 배 많은 트래픽을 가져옵니다. 기본값은 1입니다.

6 SSL 설정 탭에서 로드 밸런서 풀의 구성원이 제공한 인증서의 유효성을 검사하기 위한 SSL 설정을 구성합니다.

- a SSL을 활성화하려면 **SSL 사용** 옵션을 사용하도록 전환합니다.
- b 개인 키가 있는 인증서를 숨기고 CA 인증서 목록만 표시하려면 **서비스 인증서 숨기기** 확인란을 선택합니다.

7 서버 인증서에 대한 일반 이름 확인을 활성화하려면 **일반 이름 확인** 옵션을 사용하도록 전환하고 풀에 대한 도메인 이름을 10개까지 입력합니다.

8 **저장**을 클릭합니다.

다음에 수행할 작업

가상 서비스 만들기.

가상 서비스 만들기

가상 서비스는 IP 주소에 대한 트래픽을 수신하고, 클라이언트 요청을 처리하며, 유효한 요청을 로드 밸런서 서버 풀의 구성원에게 보냅니다.

가상 서비스는 IP 주소와 단일 네트워크 프로토콜을 사용하는 포트의 조합입니다. 가상 서비스는 외부 네트워크에 보급되고 클라이언트 요청을 수신합니다. 클라이언트가 가상 서비스에 연결되면 로드 밸런서가 구성된 로드 밸런서 서버 풀의 구성원에게 요청을 보냅니다.

가상 서비스에 대한 SSL 종료를 보호하기 위해 인증서 라이브러리의 인증서를 사용할 수 있습니다. 자세한 내용은 [인증서 라이브러리에 인증서 가져오기](#) 항목을 참조하십시오.

사전 요구 사항

- **조직 관리자** 권한이 있는지 확인합니다.
- **시스템 관리자**가 NSX-T Edge 게이트웨이에서 로드 밸런싱을 사용하도록 설정했는지 확인합니다.
- **시스템 관리자**가 Edge 게이트웨이에 서비스 엔진 그룹을 하나 이상 할당했는지 확인합니다.
- **로드 밸런서 서버 풀** 추가.

절차

- 1 위쪽 탐색 모음에서 **네트워킹**을 클릭하고 **Edge 게이트웨이** 탭을 클릭합니다.
- 2 가상 서비스를 만들려는 NSX-T Data Center Edge 게이트웨이를 클릭합니다.
- 3 [로드 밸런서]에서 **가상 서비스**를 클릭한 다음 **추가**를 클릭합니다.
- 4 가상 서비스의 의미 있는 이름과 설명(선택 사항)을 입력합니다.
- 5 생성 시 가상 서비스를 활성화하려면 **사용** 옵션을 사용하도록 전환합니다.
- 6 가상 서비스에 대한 서비스 엔진 그룹을 선택합니다.
- 7 가상 서비스에 대한 로드 밸런서 풀을 선택합니다.
- 8 가상 서비스의 IP 주소를 입력합니다.
- 9 가상 서비스 유형을 선택합니다.

옵션	설명
HTTP	가상 서비스에서 비보안 레이어 7 HTTP 요청을 수신합니다. 이 서비스 유형을 선택하면 자동으로 서비스 포트 텍스트 상자가 80으로 채워집니다. 이 번호는 다른 유효한 포트 번호로 바꿀 수 있습니다.
HTTPS	가상 서비스에서 보안 수준 7 HTTPS 요청을 수신합니다. 이 서비스 유형을 선택하면 자동으로 서비스 포트 텍스트 상자가 포트 443으로 채워집니다. 이 번호는 다른 유효한 포트 번호로 바꿀 수 있습니다. SSL 종료에 사용할 SSL 인증서를 선택합니다.
L4	가상 서비스에서 레이어 4 요청을 수신합니다. 이 서비스 유형을 선택하면 자동으로 서비스 포트 텍스트 상자가 80으로 채워집니다. 이 번호는 다른 유효한 포트 번호로 바꿀 수 있습니다.
L4 TLS	가상 서비스에서 보안 레이어 4 TLS 요청을 수신합니다. 이 서비스 유형을 선택하면 자동으로 서비스 포트 텍스트 상자가 TCP 포트 443으로 채워집니다. 이 번호는 다른 유효한 포트 번호로 바꿀 수 있습니다. SSL 종료에 사용할 SSL 인증서를 선택합니다.

- 10 **저장**을 클릭합니다.

명명된 디스크 사용 및 스토리지 정책 검토

6

VMware Cloud Director 테넌트 포털을 사용하면 명명된 디스크를 생성 및 관리하고 조직 가상 데이터 센터 스토리지 정책을 검토할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 명명된 디스크 생성 및 사용
- 스토리지 정책 속성 검토

명명된 디스크 생성 및 사용

명명된 디스크는 조직 VDC에서 생성하는 독립형 가상 디스크입니다. **조직 관리자** 및 해당 권한이 있는 사용자는 명명된 디스크를 만들고, 제거하고, 업데이트하고, 가상 시스템에 연결할 수 있습니다.

명명된 디스크를 만들면 조직 VDC와 연결되지만 가상 시스템과는 연결되지 않습니다. VDC에서 디스크를 만든 후에 디스크 소유자나 관리자가 VDC에 배포된 가상 시스템에 디스크를 연결할 수 있습니다. **공유 디스크 생성** 권한이 있으면 여러 VM에 연결할 수 있는 명명된 공유 디스크를 생성할 수 있습니다. 디스크 소유자는 디스크 속성을 수정하고 가상 시스템에서 분리하고 VDC에서 제거할 수 있습니다. **시스템 관리자**와 **조직 관리자**는 디스크 소유자와 동일한 디스크 사용 및 수정 권한을 갖습니다.

참고 vSphere는 WSFC(Windows Server Failover Cluster)와 같은 구성을 지원하며 물리적 SCSI 버스 공유를 통해 공유 디스크를 생성할 수 있지만 VMware Cloud Director 10.2는 이러한 기능을 지원하지 않습니다. VMware Cloud Director에서 공유 디스크를 생성할 때는 다중 작성기 모드를 사용하도록 설정된 vSphere에서 기본 독립 영구 디스크만 생성하십시오.

명명된 디스크를 연결하면 VM 스냅샷을 생성할 수 없습니다. 공유 디스크가 VM에 연결된 경우 VM 세부 정보 보기에서 하드 디스크 설정을 편집할 수 없습니다.

조직 VDC에 VM 암호화를 사용하도록 설정된 스토리지 정책이 있는 경우 VM과 디스크를 VM 암호화 기능이 있는 스토리지 정책에 연결하여 VM과 디스크를 암호화할 수 있습니다. **가상 시스템 암호화**의 내용을 참조하십시오.

명명된 디스크 만들기

명명된 디스크를 생성하고 이후 단계에서 하나 이상의 가상 시스템에 연결할 수 있습니다.

명명된 디스크를 만들려면 이름과 크기를 지정해야 합니다. 필요한 경우 설명을 포함시키고 디스크에 사용될 스토리지 프로파일을 선택할 수 있습니다. 여러 VM에 연결할 수 있는 공유 디스크를 만들 수 있습니다.

참고 vSphere는 WSFC(Windows Server Failover Cluster)와 같은 구성을 지원하며 물리적 SCSI 버스 공유를 통해 공유 디스크를 생성할 수 있지만 VMware Cloud Director 10.2는 이러한 기능을 지원하지 않습니다. VMware Cloud Director에서 공유 디스크를 생성할 때는 다중 작성기 모드를 사용하도록 설정된 vSphere에서 기본 독립 영구 디스크만 생성하십시오.

사전 요구 사항

- 1 **조직 관리자** 역할 또는 디스크 소유자 권한이 있어야 합니다.
- 2 공유 디스크를 생성하려면 **공유 디스크 생성** 권한이 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 아래 왼쪽 패널의 **스토리지**에서 **명명된 디스크**를 선택합니다.
- 2 **새로 만들기**를 클릭합니다.
- 3 디스크의 이름과 설명(선택 사항)을 입력합니다.
- 4 **스토리지 정책** 드롭다운 메뉴에서 스토리지 정책을 선택합니다.
- 5 명명된 디스크의 크기를 입력합니다.
- 6 **버스 유형** 및 **버스 하위 유형** 드롭다운 메뉴에서 버스 유형 및 하위 유형을 각각 선택합니다.
- 7 명명된 디스크를 여러 VM에 연결하려면 **공유 가능** 확인란을 선택합니다.
이 설정은 나중에 편집할 수 없습니다.

- 8 **저장**을 클릭합니다.

다음에 수행할 작업

VMware Cloud Director API를 사용하여 독립 디스크를 가상 시스템에 연결합니다. [VMware {code}](#)에서 "VMware Cloud Director API 프로그래밍 가이드"의 내용을 참조하십시오.

명명된 디스크 편집

디스크를 만든 후에 디스크의 이름, 설명, 스토리지 정책 및 크기를 수정할 수 있습니다.

명명된 디스크의 **공유 가능** 설정은 편집할 수 없습니다.

사전 요구 사항

- 1 **조직 관리자** 역할 또는 디스크 소유자 권한이 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 아래 왼쪽 패널의 **스토리지**에서 **명명된 디스크**를 선택합니다.

- 2 수정할 디스크를 선택하고 **편집**을 클릭합니다.
- 3 이름, 설명, 스토리지 정책 및 크기와 같은 설정을 편집합니다.
- 4 **저장**을 클릭합니다.

가상 시스템에 명명된 디스크 연결

VDC에 명명된 디스크를 생성한 후 VDC에 배포된 가상 시스템에 연결할 수 있습니다. 명명된 공유 디스크를 여러 VM에 연결할 수 있습니다.

사전 요구 사항

조직 관리자 역할 또는 디스크 소유자 권한이 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 아래 왼쪽 패널의 **스토리지**에서 **명명된 디스크**를 선택합니다.
- 2 가상 시스템에 연결할 명명된 디스크 이름 옆에 있는 라디오 버튼을 클릭하고 **연결**을 클릭합니다.
- 3 드롭다운 메뉴에서 명명된 디스크를 연결할 가상 시스템을 선택하고 **적용**을 클릭합니다.
- 4 다른 VM을 공유 디스크에 연결하려면 **단계 2**와 **단계 3**를 반복합니다.

다음에 수행할 작업

필요에 따라 명명된 디스크를 VM에 더 많이 연결하거나 분리할 수 있습니다.

명명된 디스크 삭제

명명된 디스크가 필요하지 않으면 삭제할 수 있습니다.

사전 요구 사항

조직 관리자 역할 또는 디스크 소유자 권한이 있어야 합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 아래 왼쪽 패널의 **스토리지**에서 **명명된 디스크**를 선택합니다.
- 2 삭제할 디스크를 선택하고 **삭제**를 클릭합니다.
- 3 **확인**을 클릭합니다.

스토리지 정책 속성 검토

스토리지 정책 및 스토리지 정책 세부 정보를 검토할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

1 가상 데이터 센터 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭합니다.

2 스토리지에서 **스토리지 정책**을 클릭합니다.

사용 가능한 스토리지 정책 목록이 표시됩니다.

3 스토리지 정책에 대한 세부 정보를 보려면 스토리지 정책의 이름을 클릭합니다.

4 일반 및 메타데이터 탭에서 세부 정보를 검토하고 **확인**을 클릭합니다.

스토리지 정책의 이름, 제한, IOPS 설정 및 메타데이터 세부 정보를 검토할 수 있습니다.

가상 데이터 센터 속성 검토 및 편집

7

조직 관리자는 가상 데이터 센터 속성을 검토할 수 있습니다. 조직의 사용자 및 그룹별로 조직 VDC에 대한 액세스를 제어할 수도 있습니다.

본 장은 다음 항목을 포함합니다.

- 가상 데이터 센터 속성 검토
- 가상 데이터 센터 메타데이터 검토
- 조직 VDC에 대한 액세스를 조직의 특정 사용자 및 그룹으로 제한

가상 데이터 센터 속성 검토

조직에 할당된 가상 데이터 센터의 속성을 검토할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭합니다.
- 2 **설정**에서 **일반**을 클릭합니다.

결과

가상 데이터 센터의 이름, 설명 및 상태와 같은 속성을 검토할 수 있습니다. 데이터 센터에 대한 메트릭 정보에는 할당 모델과 vCPU는 물론 CPU 및 메모리 사용량도 포함됩니다.

가상 데이터 센터 메타데이터 검토

VMware Cloud Director에서는 사용자 정의 메타데이터를 개체와 연결하기 위한 범용 기능을 제공합니다. 시스템 관리자가 조직 가상 데이터 센터에 대한 메타데이터를 생성한 경우에는 조직 데이터 센터 메타데이터를 검토할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

1 **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭합니다.

2 **설정**에서 **메타데이터**를 클릭합니다.

사용 가능한 메타데이터 목록이 표시됩니다.

조직 VDC에 대한 액세스를 조직의 특정 사용자 및 그룹으로 제한

조직 관리자는 조직에서 각 조직 VDC에 대한 액세스를 특정 사용자 및 그룹으로 제한할 수 있습니다.

기본적으로 조직 VDC는 **모든 조직 VDC에 대한 액세스 허용** 권한이 포함된 역할이 있는 모든 사용자 및 그룹과 공유됩니다.

조직에 여러 조직 VDC가 있고 이러한 VDC를 별도로 관리하려는 경우 조직 VDC 관리자 역할을 하는 사용자 지정 역할을 생성하여 조직 내의 특정 사용자 또는 그룹에 할당하여 특정 VDC의 계산 및 네트워킹 리소스에 대한 액세스 권한만 제공할 수 있습니다.

사전 요구 사항

1 **조직 관리자** 권한이 있는지 확인합니다.

2 특정 조직 VDC에 대한 액세스 권한을 제공하려는 사용자 및 그룹에 대한 사용자 지정 역할을 생성합니다. 이 역할에는 **모든 조직 VDC에 대한 액세스 허용** 권한이 제외되어야 합니다. [장 13 사용자, 그룹 및 역할 관리](#)의 내용을 참조하십시오.

절차

1 **가상 데이터 센터** 대시보드 화면에서 액세스를 제한할 가상 데이터 센터의 카드를 클릭합니다.

2 **설정**에서 **공유**를 클릭합니다.

VDC에 액세스할 수 있는 조직 내의 사용자 및 그룹 목록이 나타납니다.

3 조직 VDC에 대한 액세스 설정을 변경하려면 **편집**을 클릭합니다.

4 **특정 사용자 및 그룹**을 선택합니다.

5 **사용자** 목록에서 VDC에 대한 액세스 권한을 제공하려는 사용자를 선택합니다.

6 **그룹** 목록에서 VDC에 대한 액세스 권한을 제공하려는 그룹을 선택합니다.

7 선택한 사용자 및 그룹과 VDC를 공유하려면 **공유**를 클릭합니다.

결과

조직 VDC에 대한 액세스는 선택한 사용자 및 그룹으로 제한됩니다.

전용 vCenter Server 인스턴스, 끝점 및 프록시 사용

8

VMware Cloud Director Tenant Portal에서 전용 vCenter Server 환경 또는 vCenter Server 구성 요소에 액세스할 수 있습니다.

전용 vSphere 데이터 센터

VMware Cloud Director에서 SDDC(소프트웨어 정의 데이터 센터)는 전용 vCenter Server 환경 전체를 캡슐화합니다.

VMware Cloud Director의 전용 vCenter Server 인스턴스는 vCenter Server 인스턴스에 공개적으로 액세스할 수 있어야 한다는 요구 사항을 제거합니다.

시스템 관리자는 조직에 하나 이상의 전용 vCenter Server 인스턴스를 게시할 수 있습니다. 끝점을 사용하여 프록시 설정되었거나 프록시 설정되지 않은 구성 요소의 UI 또는 API에 액세스할 수 있습니다.

끝점

전용 vCenter Server 인스턴스에는 기본 환경의 다양한 구성 요소에 대한 액세스를 제공하는 하나 이상의 끝점이 포함될 수 있습니다. 끝점은 vCenter Server 인스턴스, ESXi 호스트, NSX Manager 인스턴스 또는 NSX-T Manager 인스턴스와 같은 데이터 센터 구성 요소에 대한 액세스 지점을 제공합니다.

끝점은 프록시에 연결되거나 연결되지 않을 수 있습니다.

프록시

VMware Cloud Director는 HTTPS 프록시 서버로 작동할 수 있고 전용 vCenter Server 인스턴스 및 환경을 백업하는 공유 또는 전용 vCenter Server 인스턴스의 다른 구성 요소에 대한 액세스를 제공할 수 있습니다.

자신의 VMware Cloud Director 계정을 사용하여 프록시 설정된 구성 요소의 UI 또는 API에 로그인할 수 있습니다.

프록시 설정된 구성 요소에 액세스하려면 Chrome Browser Extension for VMware Cloud Director를 사용하거나 프록시 설정을 사용하여 브라우저를 수동으로 구성해야 합니다.

본 장은 다음 항목을 포함합니다.

- [Chrome Browser Extension for VMware Cloud Director 사용](#)

- 프록시 설정으로 브라우저 구성
- 끝점을 사용하여 구성 요소의 UI에 로그인

Chrome Browser Extension for VMware Cloud Director 사용

Chrome Browser Extension for VMware Cloud Director를 사용하여 환경의 프록시 설정된 vSphere 구성 요소에 로그인할 수 있습니다.

Chrome Browser Extension for VMware Cloud Director는 프록시 구성 및 인증을 제공합니다.

Chrome Browser Extension for VMware Cloud Director는 다중 사이트 환경을 지원합니다.

[Chrome 웹 스토어](#)를 통해 Chrome 브라우저에 확장 프로그램을 추가할 수 있습니다.

프록시 설정으로 브라우저 구성

프록시 설정된 vSphere 구성 요소의 UI에 액세스하려면 먼저 조직에 게시되는 프록시를 설정해야 합니다.

게시된 프록시를 사용하도록 브라우저를 구성하려면 PAC(프록시 자동 구성) 파일의 URL을 브라우저에 복사합니다.

참고 시스템 관리자가 조직에 전용 vSphere 데이터 센터를 게시하거나 전용 vSphere 데이터 센터 중 하나에 프록시를 추가하면, 제공된 URL에서 브라우저가 PAC를 다시 가져오는 데 몇 분이 걸릴 수 있습니다. 브라우저를 강제로 새로 고치려면 이 절차를 반복하면 됩니다.

사전 요구 사항

- 시스템 관리자가 사용하도록 설정된 전용 vCenter Server 인스턴스를 조직에 하나 이상 게시했는지 확인합니다.
- 시스템 관리자가 **SDDC_VIEW** 및 **토큰: 관리** 권한을 조직에 게시했는지 확인하고 이러한 권한이 역할에 포함되어 있는지 확인합니다.
- 시스템 관리자가 조직에 **CPOM 확장** 플러그인을 게시했고 사용하도록 설정했는지 확인합니다. 이 플러그인은 VMware Cloud Director Tenant Portal에서 전용 vSphere 데이터 센터를 볼 수 있고 사용할 수 있는 기능을 제공합니다.

절차

- 1 위쪽 탐색 모음에서 **데이터 센터**를 클릭한 다음, **가상 데이터 센터**를 클릭합니다.
- 2 **전용 vSphere 데이터 센터** 창에서 **프록시 구성 가이드를 보려면 여기를 클릭하십시오.**를 클릭합니다.
- 3 PAC URL을 복사하고 **다음**을 클릭합니다.
- 4 지침에 따라 브라우저가 PAC URL을 가리키도록 구성합니다.

- 5 프록시 설정된 구성 요소가 자체 서명된 인증서를 사용하는 경우 인증서를 브라우저로 가져옵니다.
 - a 대상 vSphere 데이터 센터 카드에서 **작업**을 클릭하고 **인증서 가져오기**를 클릭합니다.
 - b 인증서 및 CRL(인증서 해지 목록)을 다운로드합니다.
 - c 다운로드한 인증서를 브라우저로 가져옵니다.

브라우저에 대한 사용자 지침을 참조하십시오.

끝점을 사용하여 구성 요소의 UI에 로그인

끝점을 사용하여 VMware Cloud Director 계정으로 프록시 설정되었거나 프록시 설정되지 않은 구성 요소의 UI에 액세스할 수 있습니다.

사전 요구 사항

프록시 설정된 구성 요소에 액세스하려면 **프록시 설정으로 브라우저 구성**하거나 [Chrome Browser Extension for VMware Cloud Director](#) 사용 합니다.

절차

- 1 위쪽 탐색 모음에서 **데이터 센터**를 클릭한 다음, **가상 데이터 센터**를 클릭합니다.
- 2 **전용 vSphere 데이터 센터** 탭을 선택합니다.
- 3 전용 vCenter Server 인스턴스의 끝점을 엽니다.
 - 기본 끝점을 열려면 **vSphere 열기**를 클릭합니다.
 - 기본이 아닌 끝점을 열려면 다음 단계를 수행합니다.
 - **작업** 메뉴를 클릭하고 **끝점 보기**를 클릭합니다.
 - 끝점 URL을 클릭합니다.

프록시 설정된 구성 요소에 액세스하는 경우 프록시 자격 증명이 있는 새 카드가 열립니다.

- 4 프록시 설정된 구성 요소에 로그인하는 경우 자격 증명을 사용하여 구성 요소에 액세스합니다.
 - a 사용자 이름과 암호를 복사합니다.
 - b 프록시를 활성화하려면 **열기**를 클릭합니다.

새 카드가 열리고 프록시에 대한 인증을 요청하는 메시지가 표시됩니다.
 - c **사용자 이름** 텍스트 상자에 복사한 사용자 이름을 붙여넣습니다.
 - d **암호** 텍스트 상자에서 복사한 암호를 붙여넣고 **확인**을 클릭합니다.

vApp 템플릿 작업

9

vApp 템플릿은 운영 체제, 응용 프로그램 및 데이터와 함께 로드되는 가상 시스템 이미지입니다. 이러한 템플릿을 사용하면 조직 전체에서 가상 시스템의 구성이 일관되도록 할 수 있습니다. vApp 템플릿은 카탈로그에 추가됩니다.

본 장은 다음 항목을 포함합니다.

- vApp 템플릿 보기
- OVF 파일에서 vApp 템플릿 만들기
- vApp 템플릿으로 vCenter Server에서 가상 시스템 가져오기
- vApp 템플릿에 VM 배치 정책 및 VM 크기 조정 정책 할당
- vApp 템플릿 다운로드
- vApp 템플릿 삭제

vApp 템플릿 보기

액세스 가능한 카탈로그에서 사용할 수 있는 vApp 템플릿의 목록을 볼 수 있습니다. vApp 템플릿을 볼 수 있고 여기에 포함된 가상 시스템을 탐색할 수 있습니다.

공유된 카탈로그 항목에 있는 vApp 템플릿에만 액세스할 수 있습니다. 카탈로그 공유에 대한 자세한 내용은 [카탈로그 공유](#) 섹션을 참조하십시오.


사전 요구 사항

이 작업을 수행하려면 미리 정의된 **vApp 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **vApp 템플릿**을 선택합니다.
템플릿 목록이 그리드 보기에 나타납니다.


2 (선택 사항) 보고 싶은 요소를 포함하도록 그리드 보기를 구성합니다.

- a 그리드 보기에서 vApp 템플릿 목록 아래에 있는 그리드 편집기 아이콘()을 클릭합니다.
- b 그리드 보기에 포함하려는 요소(예: 버전, 상태, 카탈로그, 소유자 등)를 선택합니다.
- c **확인**을 클릭합니다.

목록의 각 vApp 템플릿에 대해 선택한 요소가 그리드에 표시됩니다.

3 vApp 템플릿에 포함된 가상 시스템을 보려면 vApp 템플릿 이름을 클릭합니다.

vApp 템플릿에 포함되는 가상 시스템이 그리드에 표시됩니다.

4 (선택 사항) 그리드 보기에 표시할 요소를 선택하려면 가상 시스템 목록 아래에 있는 그리드 편집기 아이콘()을 클릭합니다.

- a 그리드 보기에 포함시킬 요소를 선택합니다.
- b **확인**을 클릭합니다.

OVF 파일에서 vApp 템플릿 만들기

OVF 패키지를 업로드하여 카탈로그에서 vApp 템플릿을 생성할 수 있습니다.

VMware Cloud Director는 OVF(Open Virtualization Format) 및 OVA(Open Virtualization Appliance) 규격을 지원합니다. 해당 가상 시스템을 사용자 지정하기 위해 OVF 속성이 포함된 OVF 파일을 업로드하는 경우 해당 속성은 vApp 템플릿에 보존됩니다. OVF 패키지 생성에 대한 자세한 내용은 "OVF Tool 사용자 가이드" 및 "VMware vCenter Converter 사용자 가이드"를 참조하십시오.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **카탈로그 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **vApp 템플릿**을 선택합니다.

템플릿 목록이 그리드 보기에 나타납니다.

2 **새로 만들기**를 클릭합니다.

3 OVF 파일의 URL 주소를 입력하거나 **업로드** 아이콘을 클릭하고 컴퓨터에서 액세스할 수 있는 위치를 찾아서 OVF/OVA 템플릿 파일을 선택합니다.

이 위치는 로컬 하드 드라이브, 네트워크 공유 또는 CD/DVD 드라이브일 수 있습니다. 지원되는 파일 확장명은 .ova, .ovf, .vmdk, .mf, .cert 및 .strings입니다. 업로드하려는 파일(예: VMDK 파일)보다 많은 파일을 참조하는 OVF 파일을 업로드하도록 선택한 경우, 모든 파일을 찾아서 선택해야 합니다.

4 배포하려는 OVF/OVA 템플릿의 세부 정보를 확인하고 **다음**을 클릭합니다.

- 5 vApp 템플릿의 이름과 설명(선택 사항)을 입력하고 **다음**을 클릭합니다.
- 6 **카탈로그** 드롭다운 메뉴에서 템플릿을 추가할 카탈로그를 선택합니다.
- 7 vApp 템플릿 설정을 검토하고 **마침**을 클릭합니다.

결과

새 vApp 템플릿이 템플릿 그리드 보기에 표시됩니다.

vApp 템플릿으로 vCenter Server에서 가상 시스템 가져오기

시스템 관리자 권한이 있는 경우 vCenter Server VM을 카탈로그의 vApp으로 VMware Cloud Director에 가져올 수 있습니다.

사전 요구 사항

vApp 템플릿으로 vCenter Server에서 VM을 보고 가져오려면 **시스템 관리자** 권한이 있는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **vApp 템플릿**을 선택합니다.
템플릿 목록이 그리드 보기에 나타납니다.
- 2 **vCenter에서 가져오기**를 클릭합니다.
- 3 드롭다운 메뉴에서 vApp 템플릿을 가져올 vCenter Server 인스턴스를 선택합니다.
- 4 가상 시스템 목록에서 템플릿을 선택합니다.
- 5 vApp 템플릿의 이름과 설명(선택 사항)을 입력합니다.
- 6 드롭다운 메뉴에서 vApp 템플릿을 추가할 카탈로그를 선택합니다.
- 7 (선택 사항) 소스 가상 시스템을 삭제하려면 **가상 시스템 이동** 옵션을 설정합니다.
- 8 (선택 사항) vApp 템플릿을 카탈로그에서 기본 템플릿으로 표시합니다.
- 9 **가져오기**를 클릭합니다.

vApp 템플릿에 VM 배치 정책 및 VM 크기 조정 정책 할당

vApp 템플릿의 VM을 특정 VM 배치 및 VM 크기 조정 정책과 연결하려면, vApp 템플릿의 개별 VM에 할당 정책으로 태그를 지정하면 됩니다.

VMware Cloud Director 10.0부터는 VM을 편집하는 동안 사용자가 미리 정의된 VM 배치 또는 VM 크기 조정 정책을 변경하도록 허용할 수 있습니다.

참고 VMware Cloud Director 10.0 이상으로 업그레이드하면 모든 기존 템플릿 태그를 수정할 수 있게 됩니다. 미리 정의된 VM 배치 또는 VM 크기 조정 정책에 대한 변경을 허용하지 않으려면, 변경을 허용하지 않을 정책에 대한 **수정 가능** 확인란의 선택을 취소해야 합니다.

사전 요구 사항

- 이 작업을 수행하려면 vApp 템플릿을 편집할 수 있는 권한이 필요합니다.
- VMware Cloud Director 환경에 vApp 템플릿이 하나 이상 있는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **vApp 템플릿**을 선택합니다.
템플릿 목록이 그리드 보기에 나타납니다.
- 2 태그를 지정할 vApp 템플릿 옆의 라디오 버튼을 선택하고 **계산 정책으로 태그 지정**을 클릭합니다.
- 3 vApp 템플릿의 VM에 VM 배치 정책을 할당하려면 VM에 해당하는 행의 **VM 배치 정책** 드롭다운 메뉴에서 정책을 선택합니다.
- 4 vApp 템플릿의 VM에 VM 크기 조정 정책을 할당하려면 VM에 해당하는 행의 **VM 크기 조정 정책** 드롭다운 메뉴에서 정책을 선택합니다.
- 5 (선택 사항) VM을 편집하는 동안 사용자가 미리 정의된 VM 배치 또는 VM 크기 조정 정책을 변경할 수 있도록 하려면, 정책 드롭다운 메뉴에서 **수정 가능** 확인란을 선택합니다.
- 6 **태그**를 클릭합니다.


vApp 템플릿 다운로드

vApp 템플릿은 카탈로그에서 OVA 파일로 로컬 시스템에 다운로드할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **카탈로그 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **vApp 템플릿**을 선택합니다.
템플릿 목록이 그리드 보기에 나타납니다.
- 2 다운로드할 vApp 템플릿의 왼쪽에 있는 목록 표시줄()을 클릭하고 **다운로드**를 선택합니다.

참고 조직 카탈로그에서 vApp 템플릿을 다운로드할 수 있습니다. 조직 관리자인 경우 공개 카탈로그에서 vApp 템플릿을 다운로드할 수 있습니다. 그렇지 않으면 **다운로드** 버튼이 흐리게 표시됩니다.

- 3 (선택 사항) 다운로드한 OVA 패키지에 있는 가상 시스템의 UUID 및 MAC 주소를 보존하려면 **ID 정보 보존** 확인란을 선택합니다.
- 4 **확인**을 클릭하고 다운로드가 완료될 때까지 기다립니다.
OVA 파일은 웹 브라우저의 기본 다운로드 위치에 저장됩니다.


vApp 템플릿 삭제

조직 카탈로그에서 vApp 템플릿을 삭제할 수 있습니다. 카탈로그가 게시된 경우 vApp 템플릿도 공개 카탈로그에서 삭제됩니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **vApp 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **vApp 템플릿**을 선택합니다.
템플릿 목록이 그리드 보기에 나타납니다.
- 2 삭제할 vApp 템플릿의 왼쪽에 있는 목록 표시줄()을 클릭하고 **삭제**를 선택합니다.
- 3 삭제를 확인합니다.
삭제된 vApp 템플릿이 그리드 보기에서 제거됩니다.

카탈로그를 사용하여 미디어 파일을 업로드, 복사 및 이동하고, 해당 속성을 편집할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 미디어 파일 업로드
- 미디어 파일 삭제
- 미디어 파일 다운로드

미디어 파일 업로드

새 미디어 파일 또는 기존 미디어 파일의 새 버전을 카탈로그에 업로드할 수 있습니다. 카탈로그에 대한 액세스 권한이 있는 사용자는 가상 시스템에서 미디어 파일을 열 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **카탈로그 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **미디어 및 기타 항목**을 선택합니다.
미디어 파일 목록이 그리드 보기에 나타납니다.
- 2 **추가**를 클릭합니다.
- 3 **카탈로그** 드롭다운 메뉴에서 미디어 파일을 업로드하려는 카탈로그를 선택합니다.
- 4 미디어 파일의 이름을 입력합니다.
이름을 입력하지 않으면 미디어 파일 이름이 이름 텍스트 상자에 자동으로 채워집니다.
- 5 업로드 아이콘을 클릭하여 디스크 이미지 파일(예: .iso 파일)을 찾아 선택합니다.
- 6 **확인**을 클릭합니다.
업로드가 시작되면 미디어 파일이 그리드에 나타납니다.

다음에 수행할 작업

파일 크기에 따라 업로드가 완료되는 데 다소 시간이 걸릴 수 있습니다. **최근 작업** 보기에서 다운로드의 상태를 모니터링할 수 있습니다. 자세한 내용은 [작업 보기](#)를 참조하십시오.


미디어 파일 삭제

더 이상 사용하지 않으려는 미디어 파일은 카탈로그에서 삭제할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **카탈로그 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **미디어 및 기타 항목**을 선택합니다.
미디어 파일 목록이 그리드 보기에 나타납니다.
- 2 삭제할 미디어 파일의 왼쪽에 있는 목록 표시줄()을 클릭하고 **삭제**를 선택합니다.
- 3 삭제를 확인합니다.
삭제된 미디어 파일이 그리드 보기에서 제거됩니다.


미디어 파일 다운로드

카탈로그에서 미디어 파일을 다운로드할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **카탈로그 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **미디어 및 기타 항목**을 선택합니다.
미디어 파일 목록이 그리드 보기에 나타납니다.
- 2 다운로드할 미디어 파일의 왼쪽에 있는 목록 표시줄()을 클릭하고 **다운로드**를 선택합니다.
다운로드 작업이 시작되고 웹 브라우저의 기본 다운로드 위치에 파일이 저장됩니다.

다음에 수행할 작업

파일 크기에 따라 다운로드가 완료되는 데 다소 시간이 걸릴 수 있습니다. **최근 작업** 패널에서 다운로드의 상태를 모니터링할 수 있습니다. 자세한 내용은 [작업 보기](#)를 참조하십시오.

카탈로그는 조직의 vApp 템플릿 및 미디어 파일을 위한 컨테이너입니다. 조직 관리자와 카탈로그 작성자는 조직에서 카탈로그를 만들 수 있습니다. 카탈로그 콘텐츠를 VMware Cloud Director 설치 환경의 다른 사용자 또는 조직과 공유하거나 VMware Cloud Director 설치 환경 외부의 조직이 액세스할 수 있도록 외부에 게시할 수 있습니다.

VMware Cloud Director에는 개인 카탈로그, 공유 카탈로그 및 외부 액세스 가능 카탈로그가 포함됩니다. 개인 카탈로그에는 조직의 다른 사용자와 공유할 수 있는 vApp 템플릿 및 미디어 파일이 포함됩니다. 시스템 관리자가 조직에 카탈로그 공유 기능을 사용하도록 설정한 경우 조직 카탈로그를 공유하여 VMware Cloud Director 설치 환경의 다른 조직에서 액세스할 수 있는 카탈로그를 만들 수 있습니다. 시스템 관리자가 조직에 외부 카탈로그 게시 기능을 사용하도록 설정한 경우에는 VMware Cloud Director 설치 환경 외부의 조직에서 액세스할 수 있도록 조직 카탈로그를 게시할 수 있습니다. VMware Cloud Director 설치 환경 외부의 조직은 외부에 게시된 카탈로그를 구독해야만 해당 콘텐츠에 액세스할 수 있습니다.

OVF 패키지를 카탈로그에 직접 업로드하거나, vApp을 vApp 템플릿으로 저장하거나, vSphere에서 vApp 템플릿을 가져올 수 있습니다. [OVF 파일에서 vApp 템플릿 만들기](#) 및 [vApp을 vApp 템플릿으로 카탈로그에 저장](#) 섹션을 참조하십시오.

조직의 구성원은 자신이 소유하고 있거나 공유된 vApp 템플릿 및 미디어 파일에 액세스할 수 있습니다. 조직 관리자와 시스템 관리자는 카탈로그를 조직의 모든 사용자나 조직의 특정 사용자 및 그룹과 공유할 수 있습니다. 자세한 내용은 [카탈로그 공유](#)를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- 카탈로그 보기
- 카탈로그 만들기
- 카탈로그 공유
- 카탈로그 삭제
- 카탈로그의 소유자 변경
- 카탈로그에 대한 메타데이터 관리
- 카탈로그 게시
- 외부 카탈로그 구독
- 구독된 카탈로그의 위치 URL 및 암호 업데이트



■ 구독된 카탈로그 동기화

카탈로그 보기

조직 내에서 나와 공유된 카탈로그에 액세스할 수 있습니다. 조직 관리자가 조직 내에서 공개 카탈로그를 액세스 가능한 상태로 설정한 경우에는 해당 공개 카탈로그에 액세스할 수 있습니다.

카탈로그 액세스는 역할 내 권한이 아니라 카탈로그 공유에 의해 제어됩니다. 나와 공유된 카탈로그 또는 카탈로그 항목에만 액세스할 수 있습니다. 자세한 내용은 [카탈로그 공유](#)를 참조하십시오.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **카탈로그**를 선택합니다.
카탈로그 목록이 그리드 보기에 나타납니다.
- 2 (선택 사항) 그리드 보기를 구성하여 표시할 요소를 보기에 포함합니다.
 - a 그리드 보기에서 카탈로그 목록 아래에 표시된 그리드 편집기 아이콘()을 클릭합니다.
 - b 그리드 보기에 포함하려는 요소(예: 버전, 설명, 상태 등)를 선택합니다.
 - c **확인**을 클릭합니다.
 각 카탈로그에 대해 선택한 요소가 그리드에 표시됩니다.
- 3 (선택 사항) 그리드 보기에서 목록 표시줄()을 사용하여 각 카탈로그에 대해 수행할 수 있는 작업을 표시합니다.
예를 들어 카탈로그를 공유하거나 삭제할 수 있습니다.

카탈로그 만들기

새 카탈로그를 만들어서 스토리지 정책에 연결할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **카탈로그 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **카탈로그**를 선택합니다.
카탈로그 목록이 그리드 보기에 나타납니다.
- 2 **새로 만들기**를 클릭하여 새 카탈로그를 만듭니다.
- 3 카탈로그의 이름과 설명(선택 사항)을 입력합니다.
- 4 (선택 사항) 카탈로그에 스토리지 정책 할당 여부를 선택하고 스토리지 정책을 선택합니다.
- 5 **확인**을 클릭합니다.

결과

카탈로그 탭의 그리드 보기에 새 카탈로그가 나타납니다.


카탈로그 공유

카탈로그를 조직의 모든 구성원 또는 특정 구성원과 공유할 수 있습니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **카탈로그 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- 카탈로그의 소유자여야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **카탈로그**를 선택합니다.
카탈로그 목록이 그리드 보기에 나타납니다.
- 2 공유할 카탈로그의 왼쪽에 있는 목록 표시줄()을 클릭하고 **공유**를 선택합니다.
카탈로그에 액세스할 수 있는 사용자 목록이 **카탈로그 공유** 창의 그리드 보기에 표시됩니다.
- 3 **추가**를 클릭하면 카탈로그를 다른 사용자와 공유할 수 있습니다.

옵션	설명
이 조직의 모든 사람과 공유	조직의 모든 사용자 및 그룹에 액세스 권한을 부여합니다.
특정 사용자 및 그룹과 공유	카탈로그 액세스 권한을 부여할 사용자 또는 그룹을 선택하고 추가 를 클릭합니다.

- 4 액세스 수준을 선택합니다.

옵션	설명
읽기 전용	이 카탈로그에 액세스할 수 있는 사용자가 카탈로그의 vApp 템플릿 및 ISO 파일에 대한 읽기 권한을 갖습니다.
읽기/쓰기	이 카탈로그에 액세스할 수 있는 사용자가 카탈로그의 vApp 템플릿 및 ISO 파일에 대한 읽기 권한을 가지며 카탈로그에 vApp 템플릿 및 ISO 파일을 추가할 수 있습니다.
모든 권한	이 카탈로그에 액세스할 수 있는 사용자가 카탈로그의 내용 및 설정에 대한 모든 권한을 갖습니다.

- 5 **확인**을 클릭합니다.

이제 카탈로그에 액세스할 수 있는 사용자 또는 그룹이 **카탈로그 공유** 대화 상자의 그리드 보기에 표시됩니다.

- 6 (선택 사항) 다른 모든 조직의 관리자에게 읽기 전용 액세스 권한을 공유하도록 선택합니다.
- 7 **저장**을 클릭합니다.

결과

카탈로그 탭의 그리드 보기에 표시되는 이 카탈로그의 [공유됨] 상태가 변경됩니다.

카탈로그 삭제


조직에서 카탈로그를 삭제할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **카탈로그 작성자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

참고 카탈로그에 vApp 템플릿 또는 미디어 파일이 포함되어 있지 않아야 합니다. 이러한 항목은 다른 카탈로그로 이동하거나 삭제할 수 있습니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **카탈로그**를 선택합니다.
카탈로그 목록이 그리드 보기에 나타납니다.
- 2 삭제할 카탈로그의 왼쪽에 있는 목록 표시줄()을 클릭하고 **삭제**를 선택합니다.
- 3 삭제를 확인합니다.
삭제된 카탈로그 항목이 그리드 보기에서 제거됩니다.

카탈로그의 소유자 변경


조직 관리자는 카탈로그의 소유자를 변경할 수 있습니다.

카탈로그를 소유한 사용자를 삭제하려면 우선 소유자를 변경하거나 카탈로그를 삭제해야 합니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **카탈로그**를 선택합니다.
카탈로그 목록이 그리드 보기에 나타납니다.
- 2 카탈로그 왼쪽에 있는 목록 표시줄()을 클릭하고 **소유자 변경**을 선택합니다.
카탈로그에 액세스할 수 있는 사용자 목록이 **소유자 변경** 창의 그리드 보기에 표시됩니다.
- 3 카탈로그의 새 소유자를 만들 사용자를 선택하고 **확인**을 클릭합니다.


결과

카탈로그 탭의 그리드 보기에 표시되는 카탈로그의 소유자 이름이 변경됩니다.

카탈로그에 대한 메타데이터 관리

조직 관리자 또는 **카탈로그 소유자**는 자신이 소유하는 카탈로그에 대한 메타데이터를 만들거나 업데이트할 수 있습니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **카탈로그**를 선택합니다.
카탈로그 목록이 그리드 보기에 나타납니다.
- 2 카탈로그 왼쪽에 있는 목록 표시줄()을 클릭하고 **메타데이터**를 선택합니다.
선택한 카탈로그에 대한 메타데이터가 그리드 보기에 표시됩니다.
- 3 (선택 사항) 메타데이터를 추가하려면 **추가**를 클릭합니다.
 - a 메타데이터 이름을 입력합니다.
이 이름은 이 개체에 연결된 메타데이터 이름 내에서 고유해야 합니다.
 - b 메타데이터 유형(예: **텍스트**, **숫자**, **날짜 및 시간** 또는 **예 또는 아니오**)을 선택합니다.
 - c 메타데이터 값을 입력합니다.
 - d **저장**을 클릭합니다.
- 4 (선택 사항) 기존 메타데이터를 업데이트합니다.
메타데이터 이름은 업데이트할 수 없습니다.
 - a 메타데이터 유형을 업데이트합니다.
 - b 새 메타데이터 값을 입력합니다.
 - c **저장**을 클릭합니다.
- 5 (선택 사항) 기존 메타데이터를 삭제합니다.
 - a 삭제 아이콘을 클릭합니다.
 - b **저장**을 클릭합니다.


카탈로그 게시

시스템 관리자가 사용자에게 카탈로그 액세스 권한을 부여한 경우 사용자는 외부에 카탈로그를 게시하여 VMware Cloud Director 설치 환경 외부의 조직에서 해당 vApp 템플릿과 미디어 파일을 구독할 수 있게 할 수 있습니다.

사전 요구 사항

시스템 관리자가 조직에 외부 카탈로그 게시 기능을 사용하도록 설정하고 사용자에게 카탈로그 액세스 권한을 부여했는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **카탈로그**를 선택합니다.
카탈로그 목록이 그리드 보기에 나타납니다.
- 2 게시할 카탈로그의 왼쪽에 있는 목록 표시줄()을 클릭하고 **게시 설정**을 선택합니다.
- 3 **게시 사용**을 선택하고 필요한 경우 카탈로그 액세스를 위한 암호를 입력합니다.
ASCII 문자만 지원됩니다.
- 4 **저장**을 클릭합니다.

외부 카탈로그 구독

외부 카탈로그를 구독하면 외부에서 게시된 카탈로그의 읽기 전용 복사본을 만들 수 있습니다. 구독된 카탈로그는 수정할 수 없습니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- **시스템 관리자**가 조직에 외부 카탈로그 구독 권한을 부여해야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **카탈로그**를 선택합니다.
카탈로그 목록이 그리드 보기에 나타납니다.
- 2 **새로 만들기**를 클릭하여 새 카탈로그를 만듭니다.
- 3 카탈로그의 이름과 설명(선택 사항)을 입력합니다.
- 4 외부 카탈로그를 구독하도록 선택하고 구독 URL을 제공합니다.
- 5 카탈로그에 액세스하는 데 사용할 암호(선택 사항)를 입력합니다.
- 6 외부 카탈로그에서 콘텐츠를 자동으로 다운로드할지 여부를 선택합니다.
- 7 **확인**을 클릭합니다.


구독된 카탈로그의 위치 URL 및 암호 업데이트

구독된 카탈로그를 생성한 후에 구독된 카탈로그의 위치 URL과 암호를 업데이트할 수 있습니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- 구독된 카탈로그가 만들어져 있어야 합니다.
- **시스템 관리자**가 조직에 외부 카탈로그 구독 권한을 부여해야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **카탈로그**를 선택합니다.
카탈로그 목록이 그리드 보기에 나타납니다.
- 2 구독된 카탈로그 왼쪽에 있는 목록 표시줄()을 클릭하고 **구독 설정**을 선택합니다.
구독된 카탈로그가 아니면 옵션이 흐리게 표시됩니다.
- 3 이 구독된 카탈로그의 위치 URL 및 암호를 업데이트하십시오.
- 4 외부 카탈로그에서 콘텐츠를 자동으로 다운로드할지 여부를 선택합니다.
- 5 **저장**을 클릭합니다.


구독된 카탈로그 동기화

구독된 카탈로그를 만든 후에 원래 카탈로그와 동기화하여 변경 내용이 있는지 확인할 수 있습니다. 예를 들어 원래 카탈로그의 메타데이터가 변경된 경우 동기화를 수행하면 구독된 카탈로그의 메타데이터가 업데이트됩니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- 구독된 카탈로그가 만들어져 있어야 합니다.
- **시스템 관리자**가 조직에 외부 카탈로그 구독 권한을 부여해야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **카탈로그**를 선택합니다.
카탈로그 목록이 그리드 보기에 나타납니다.
- 2 구독된 카탈로그 왼쪽에 있는 목록 표시줄()을 클릭하고 **동기화**를 선택합니다.
구독된 카탈로그가 아니면 옵션이 흐리게 표시됩니다.
구독된 카탈로그가 원래 카탈로그와 동기화됩니다.

조직 가상 데이터 센터 템플릿 작업

12

조직 관리자 또는 조직 가상 데이터 센터 템플릿을 보고 인스턴스화할 수 있는 권한을 가진 모든 역할의 사용자는 조직 가상 데이터 센터를 추가로 만들 수 있습니다.

조직 가상 데이터 센터 템플릿은 조직 가상 데이터 센터 및 필요한 경우, Edge 게이트웨이와 조직 가상 데이터 센터 네트워크에 대한 구성을 지정합니다. 시스템 관리자는 조직 관리자가 자신의 조직에 이러한 리소스를 만들 수 있도록 조직 가상 데이터 센터 템플릿을 만들어 해당 조직과 공유할 수 있습니다.

시스템 관리자는 가상 데이터 센터 템플릿을 만들고 공유하여 제공자 가상 데이터 센터 및 외부 네트워크 등 시스템 리소스 할당에 대한 관리 제어를 유지하면서 조직 가상 데이터 센터의 셀프 서비스 프로비저닝을 가능케 할 수 있습니다.

시스템 관리자는 조직 가상 데이터 센터 템플릿을 만들고 여러 조직에 템플릿에 대한 액세스 권한을 제공합니다.

조직에 가상 데이터 센터 템플릿에 대한 액세스 권한이 제공되면, VMware Cloud Director Tenant Portal을 사용하여 사용 가능한 템플릿에서 가상 데이터 센터를 만들 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 사용 가능한 가상 데이터 센터 템플릿 보기
- 템플릿에서 가상 데이터 센터 인스턴스화

사용 가능한 가상 데이터 센터 템플릿 보기

시스템 관리자가 만든 조직 가상 데이터 센터 템플릿을 볼 수 있습니다.

가상 데이터 센터 템플릿에서 조직 가상 데이터 센터를 새로 만들기 전에 가상 데이터 센터 템플릿을 봅니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 조직 가상 데이터 센터 템플릿을 보고 인스턴스화할 수 있는 권한을 가진 역할이 필요합니다.

절차

- ◆ 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **조직 VDC 템플릿**을 선택합니다.

가상 데이터 센터 템플릿 목록이 그리드 보기에 나타납니다.

다음에 수행할 작업

조직 가상 데이터 센터 템플릿의 설명을 검토하고, 새 조직 가상 데이터 센터를 만들 템플릿을 선택합니다.

템플릿에서 가상 데이터 센터 인스턴스화

시스템 관리자가 조직 VDC(가상 데이터 센터) 템플릿을 생성하고 이 템플릿을 조직에 게시하면 템플릿에서 조직 VDC를 만들 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 조직 VDC 템플릿을 보고 인스턴스화할 수 있는 권한을 가진 역할이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 왼쪽 패널에서 **조직 VDC 템플릿**을 선택합니다.

가상 데이터 센터 템플릿 목록이 그리드 보기에 나타납니다.

- 2 템플릿을 선택하고 **새 VDC**를 클릭합니다.

VMware Cloud Director 10.2.2부터는 템플릿을 선택한 후 **VDC 인스턴스화**를 클릭해야 합니다.

- 3 VDC의 이름과 설명(선택 사항)을 입력합니다.

- 4 **만들기**를 클릭합니다.

결과

새 조직 가상 데이터 센터 만들기가 인스턴스화되고 이 작업은 몇 분 정도 소요될 수 있습니다. **최근 작업** 패널에서 작업의 진행률을 볼 수 있습니다.

다음에 수행할 작업

가상 시스템과 vApp을 만들고 네트워크 및 보안 설정을 관리하는 등 새로 만든 조직 가상 데이터 센터를 관리할 수 있습니다.

사용자, 그룹 및 역할 관리

13

VMware Cloud Director에 개별적으로 또는 LDAP 그룹의 일부로 조직 관리자를 추가할 수 있습니다. 조직 내에서 사용자가 갖는 권한을 결정하는 역할을 추가하고 수정할 수도 있습니다.

중요 조직 내에서 사용자, 그룹 및 역할을 관리하려면 **조직 관리자**여야 합니다. **시스템 관리자**는 테넌트에 글로벌 테넌트 역할을 하나 이상 게시할 수 있으며, **조직 관리자**는 역할 목록에서 이러한 역할을 볼 수 있습니다. 이러한 역할에는 **카탈로그 작성자**, **vApp 작성자**, **vApp 사용자**, **조직 관리자** 등이 있습니다. 미리 정의된 글로벌 테넌트 역할은 수정할 수 없지만 유사한 사용자 지정 테넌트 역할은 만들고 업데이트할 수 있으며 테넌트 내의 사용자에게 할당할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 사용자 관리
- 그룹 관리
- 역할 및 권한

사용자 관리

테넌트 포털에서 사용자를 만들고, 편집하고, 가져오고, 삭제할 수 있습니다. 또한, 사용자가 잘못된 암호로 로그인하려고 시도하여 자신의 사용자 계정을 잠근 경우 사용자 계정의 잠금을 해제할 수도 있습니다.

사용자 생성

VMware Cloud Director 조직 내에 사용자를 생성할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **사용자**를 클릭합니다.
사용자 목록이 나타납니다.
- 3 **새로 만들기**를 클릭합니다.

4 사용자 이름 및 사용자의 암호 설정을 입력합니다.

최소 암호 길이는 6자입니다.

5 생성 시 사용자를 사용하도록 설정할지 여부를 선택합니다.

6 사용자가 사용할 수 있는 리소스에 특정한 제한을 설정하려면 **사용자 할당량 구성** 토글을 설정합니다.

토글을 설정하면 이 마법사를 완료한 후 VMware Cloud Director가 **할당량** 페이지로 리디렉션됩니다. Tanzu Kubernetes 클러스터의 수, 사용자가 관리하는 모든 또는 실행 중인 VM, 사용된 CPU, 메모리 및 스토리지에 대한 할당량을 추가할 수 있습니다. 선택한 유형의 리소스를 사용자가 무제한으로 사용하도록 하려면 **무제한**을 선택합니다.

7 사용자에게 할당하려는 역할을 선택합니다.

사용 가능한 역할 메뉴는 미리 정의된 역할 및 사용자 또는 시스템 관리자가 만든 사용자 지정 역할의 목록으로 구성됩니다.

미리 정의된 역할	설명
vApp 작성자	미리 정의된 vApp 작성자 역할과 연결된 권한이 있는 사용자는 카탈로그를 사용하고 vApp을 만들 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.
vApp 사용자	미리 정의된 vApp 사용자 역할과 연결된 권한이 있는 사용자는 기존 vApp을 사용할 수 있습니다.
조직 관리자	미리 정의된 조직 관리자 역할이 있는 사용자는 VMware Cloud Director 테넌트 포털이나 Cloud Director OpenAPI를 사용하여 조직 내의 사용자와 그룹을 관리하고, 미리 정의된 조직 관리자 역할을 비롯한 역할을 사용자와 그룹에 할당할 수 있습니다. 조직 관리자 는 Cloud Director OpenAPI를 사용하여 조직의 로컬 역할 개체를 만들거나 업데이트할 수 있습니다. 조직 관리자 가 만들거나 수정한 역할은 다른 조직에 표시되지 않습니다.
ID 제공자로 지연	미리 정의된 ID 제공자로 지연 역할과 연결된 권한은 사용자의 OAuth 또는 SAML ID 제공자로부터 수신한 정보에 기반하여 결정됩니다. 사용자에게 ID 제공자로 지연 역할을 할당할 때 여기에 포함될 수 있으려면 ID 제공자가 제공하는 역할 이름이 조직에 정의된 역할 또는 이름과 대/소문자를 구분하여 정확히 일치해야 합니다.
카탈로그 작성자	미리 정의된 카탈로그 작성자 역할과 연결된 권한이 있는 사용자는 카탈로그를 만들고 게시할 수 있습니다.

8 (선택 사항) 이름, 이메일 주소, 전화 번호 및 메신저 ID와 같은 연락처 정보를 입력합니다.

9 **저장**을 클릭합니다.

다음에 수행할 작업

사용자에 대한 할당량 구성을 사용하도록 설정하고 VMware Cloud Director가 **할당량** 페이지로 리디렉션되는 경우 **사용자의 리소스 할당량 관리** 항목을 참조하십시오.

사용자 가져오기

LDAP 사용자 또는 SAML 사용자를 가져와서 특정 역할을 할당하여 사용자를 조직에 추가할 수 있습니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- LDAP 서버에 올바르게 연결되어 있는지 또는 조직에서 **SAML ID 제공자**를 사용하도록 설정했는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **사용자**를 클릭합니다.
사용자 목록이 나타납니다.
- 3 **사용자 가져오기**를 클릭합니다.
- 4 사용자를 가져올 소스를 선택합니다.

ID 제공자로 구성된 소스 LDAP 서버 또는 SAML 서버만 볼 수 있습니다.

소스	작업
LDAP	<p>LDAP 서버에서 사용자를 가져옵니다.</p> <ol style="list-style-type: none"> a 텍스트 상자에 전체 또는 일부 이름을 입력하고 검색을 클릭합니다. b 가져올 사용자를 선택하고 추가를 클릭합니다.
SAML	<p>SAML 서버에서 사용자를 가져옵니다. 가져올 사용자의 사용자 이름을 입력합니다. 사용자 이름은 이 조직에 대해 구성된 SAML ID 제공자가 지원하는 이름 식별자 형식이어야 합니다.</p> <p>참고 vCenter Single Sign-On을 SAML ID 제공자로 사용하는 경우 vCenter Single Sign-On 도메인에서 가져오는 사용자 이름은 UPN(사용자 계정 이름) 형식(예: jdoe@mydomain.com)이어야 합니다.</p> <p>각 사용자 이름을 새 줄에 입력합니다.</p>

- 5 가져올 사용자에게 할당할 역할을 선택합니다.
- 6 **저장**을 클릭합니다.

사용자 수정

조직 관리자는 기존 사용자의 암호, 연락처 및 가상 시스템 할당량 설정을 수정할 수 있습니다. 사용자의 역할도 변경할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **사용자**를 클릭합니다.
사용자 목록이 나타납니다.
- 3 편집할 사용자의 이름 옆에 있는 라디오 버튼을 클릭하고 **수정**을 클릭합니다.
- 4 수정하려는 설정을 업데이트합니다.
 - a 필요에 따라 암호를 변경합니다.
 - b 사용자를 활성화할지 또는 비활성화할지 선택합니다.
 - c 사용자 역할을 업데이트합니다.
 - d 이름, 이메일 주소, 전화 번호 및 메신저 ID와 같은 연락처 정보를 업데이트합니다.
 - e 사용자에 대한 가상 시스템 할당량을 편집합니다.
- 5 **저장**을 클릭합니다.

사용자 계정 비활성화 또는 활성화

사용자가 VMware Cloud Director에 로그인하지 못하도록 사용자 계정을 비활성화할 수 있습니다. 사용자를 삭제하려면 먼저 해당 계정을 비활성화해야 합니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **사용자**를 클릭합니다.
사용자 목록이 나타납니다.
- 3 사용자 계정을 비활성화하려면 사용자 이름 옆에 있는 라디오 버튼을 클릭하고 **사용 안 함**을 클릭한 후 확인합니다.
- 4 이미 비활성화한 사용자 계정을 활성화하려면 사용자 이름 옆에 있는 라디오 버튼을 클릭하고 **사용**을 클릭합니다.

사용자 삭제

사용자 계정을 삭제하여 VMware Cloud Director 조직에서 사용자를 제거할 수 있습니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- 삭제하려는 계정을 비활성화합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **사용자**를 클릭합니다.
사용자 목록이 나타납니다.
- 3 삭제할 사용자의 이름 옆에 있는 라디오 버튼을 클릭하고 **삭제**를 클릭합니다.
- 4 사용자 계정을 삭제하는 것을 확인하려면 **확인**을 클릭합니다.

잠긴 사용자 계정 잠금 해제

VMware Cloud Director 조직에서 잠금 정책을 사용하도록 설정한 경우에는 잘못된 로그인 시도를 일정 횟수 반복하면 사용자 계정이 잠깁니다. 잠긴 사용자 계정은 잠금을 해제할 수 있습니다. 가장 좋은 방법은 사용자의 암호를 변경하고 계정의 잠금을 해제하는 것입니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **사용자**를 클릭합니다.
사용자 목록이 나타납니다.
- 3 사용자 이름 옆에 있는 라디오 버튼을 클릭하고 **잠금 해제**를 클릭합니다.

사용자의 리소스 할당량 관리

사용자의 전체 리소스 소비 제한을 관리할 수 있습니다. VM, Tanzu Kubernetes 클러스터, CPU, 메모리 또는 스토리지에 대한 사용자의 할당량을 추가, 편집 및 제거할 수 있습니다.

사용자는 자신의 사용자 유형과 관련된 할당량만 볼 수 있습니다. 사용자는 자신이 속한 그룹에서 할당량을 상속합니다. 사용자가 그룹에서 리소스 할당량을 상속한 경우 해당 리소스에 대해 사용자 수준 할당량이 명시적으로 정의되어 있으면, 사용자 수준 할당량이 그룹 수준 할당량보다 우선합니다.

사용자 생성 또는 가져오기에 대한 자세한 내용은 [사용자 생성](#) 또는 [사용자 가져오기](#) 항목을 참조하십시오.

사전 요구 사항

리소스 할당량을 추가, 편집 및 삭제하는 데 필요한 권한이 있는지 확인합니다. 기본적으로 **조직 관리자**는 사용자의 할당량을 변경할 수 있습니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **사용자**를 클릭합니다.
- 3 사용자 이름을 선택하고 **할당량** 탭을 선택합니다.

사용자에게는 기본적으로 할당량이 없습니다. 그룹에 속하는 모든 사용자는 그룹의 할당량을 상속합니다. 리소스에 대한 할당량이 있는 그룹에 사용자가 속하는 경우, 사용자의 할당량 목록에 할당량이 편집 불가능으로 표시됩니다.

- 4 **편집**을 클릭합니다.
- 5 선택한 사용자에 대한 할당량을 수정합니다.

Tanzu Kubernetes 클러스터의 수, 사용자가 관리하는 모든 또는 실행 중인 VM, 사용된 CPU, 메모리 및 스토리지에 대한 할당량을 추가, 편집 또는 제거할 수 있습니다. 선택한 유형의 리소스를 사용자가 무제한으로 사용하도록 하려면 **무제한**을 선택합니다.

- 6 **저장**을 클릭합니다.

그룹 관리

LDAP 서버에 올바르게 연결되어 있거나 조직에서 SAML ID 제공자를 사용하도록 설정했으면 LDAP 그룹 또는 SAML 그룹을 가져올 수 있습니다. 가져온 그룹을 편집하거나 삭제할 수도 있습니다.

그룹 가져오기

사용자 그룹을 추가하려면 LDAP 그룹 또는 SAML 그룹을 가져오면 됩니다.

사전 요구 사항

- 이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- LDAP 서버에 올바르게 연결되어 있는지 또는 조직에서 SAML ID 제공자를 사용하도록 설정했는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **그룹**을 클릭합니다.

사용자 그룹 목록이 나타납니다.

- 3 **그룹 가져오기**를 클릭합니다.

4 사용자 그룹을 가져올 소스를 선택합니다.

ID 제공자로 구성된 소스 LDAP 서버 또는 SAML 서버만 볼 수 있습니다.

소스	작업
LDAP	LDAP 서버에서 사용자 그룹을 가져옵니다. a 텍스트 상자에 전체 또는 일부 이름을 입력하고 검색 을 클릭합니다. b 가져올 사용자 그룹을 선택하고 추가 를 클릭합니다.
SAML	SAML 서버에서 사용자 그룹을 가져옵니다. 가져올 그룹의 이름을 입력합니다. 각 그룹 이름을 새 줄에 입력합니다.

5 가져올 사용자 그룹에 할당할 역할을 선택합니다.

6 **저장**을 클릭합니다.

다음에 수행할 작업

그룹에 대한 할당량 구성을 사용하도록 설정하고 VMware Cloud Director가 **할당량** 페이지로 리디렉션되는 경우 [그룹의 리소스 할당량 관리](#) 항목을 참조하십시오.

그룹 삭제

LDAP 그룹을 삭제하여 VMware Cloud Director 조직에서 그룹을 제거할 수 있습니다.

LDAP 그룹을 삭제하면 해당 그룹의 구성원 자격만을 기반으로 VMware Cloud Director 계정이 있는 사용자가 격리되어 로그인할 수 없게 됩니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 왼쪽 패널의 **액세스 제어** 아래에서 **그룹**을 클릭합니다.
사용자 그룹 목록이 나타납니다.
- 삭제할 그룹의 이름 옆에 있는 라디오 버튼을 클릭하고 **삭제**를 클릭합니다.
- 그룹을 삭제하는 것을 확인하려면 **확인**을 클릭합니다.

그룹 편집

VMware Cloud Director 테넌트 포털에서 그룹을 편집할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **그룹**을 클릭합니다.
사용자 그룹 목록이 나타납니다.
- 3 편집할 그룹의 이름 옆에 있는 라디오 버튼을 클릭하고 **편집**을 클릭합니다.
- 4 필요에 따라 그룹을 편집합니다.
 - a 설명을 변경합니다.
 - b 필요에 따라 그룹 구성원의 역할을 변경합니다.
- 5 **저장**을 클릭합니다.

그룹의 리소스 할당량 관리

그룹에 대한 할당량을 직접 설정하여 그룹에 속한 각 사용자의 전체 리소스 소비 제한을 관리할 수 있습니다. VM, Tanzu Kubernetes 클러스터, CPU, 메모리 또는 스토리지에 대한 그룹의 할당량을 추가, 편집 및 제거할 수 있습니다. 그룹의 할당량은 그룹의 각 구성원에게 적용됩니다.

사용자는 자신이 속한 그룹에서 할당량을 상속합니다. 사용자가 그룹에서 리소스 할당량을 상속한 경우 해당 리소스에 대해 사용자 수준 할당량이 명시적으로 정의되어 있으면, 사용자 수준 할당량이 그룹 수준 할당량보다 우선합니다.

그룹 가져오기에 대한 자세한 내용은 [그룹 가져오기](#) 항목을 참조하십시오.

사전 요구 사항

리소스 할당량을 추가, 편집 및 삭제하는 데 필요한 권한이 있는지 확인합니다. 기본적으로 **조직 관리자**는 그룹의 할당량을 변경할 수 있습니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **그룹**을 클릭합니다.
- 3 그룹의 이름을 선택하고 **할당량** 탭을 선택합니다.

그룹에는 기본적으로 할당량이 없습니다. 그룹에 속하는 모든 사용자는 그룹의 할당량을 상속합니다. 리소스에 대한 할당량이 있는 그룹에 사용자가 속하는 경우, 사용자의 할당량 목록에 할당량이 편집 불가능으로 표시됩니다.

- 4 **편집**을 클릭합니다.
- 5 선택한 그룹에 대한 할당량을 수정합니다.

Tanzu Kubernetes 클러스터의 수, 그룹에서 관리하는 모든 또는 실행 중인 VM, 사용된 CPU, 메모리 및 스토리지에 대한 할당량을 추가, 편집 또는 제거할 수 있습니다. 선택한 유형의 리소스를 사용자 그룹에서 무제한으로 사용하도록 하려면 **무제한**을 선택합니다.

6 저장을 클릭합니다.

역할 및 권한

VMware Cloud Director는 역할과 권한을 사용하여 사용자가 조직에서 수행할 수 있는 작업을 결정합니다. VMware Cloud Director에는 특정 권한이 있는 미리 정의된 역할이 여러 개 포함되어 있습니다.

시스템 관리자와 **조직 관리자**는 각 사용자 또는 그룹에 역할을 할당해야 합니다. 동일한 사용자가 여러 조직에서 서로 다른 역할을 가질 수 있습니다. **시스템 관리자**는 전체 시스템에 대해 역할을 만들고 기존 역할을 수정할 수 있는 반면, **조직 관리자**는 자신이 관리하는 조직에 대해서만 역할을 만들고 수정할 수 있습니다.

조직 관리자는 VMware Cloud Director 테넌트 포털을 통해 자신의 조직에서 역할을 관리할 수 있습니다. **시스템 관리자**가 미리 정의된 테넌트 역할을 조직에 하나 이상 게시한 경우 **조직 관리자**는 이러한 역할을 볼 수 있지만 수정할 수는 없습니다. 하지만 유사한 권한을 가진 사용자 지정 테넌트 역할을 만들어 조직 내의 사용자에게 할당할 수 있습니다.

미리 정의된 역할과 해당 권한에 대한 자세한 내용은 [미리 정의된 역할 및 역할 권한](#) 항목을 참조하십시오.

미리 정의된 역할 및 역할 권한

미리 정의된 각 VMware Cloud 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 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"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 **다중 사이트: 시스템 작업**이라는 단일 권한이 있으며, 사이트 연결의 원격 구성원 상태를 검색하는 Cloud Director OpenAPI 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 되려면 ID 제공자가 제공한 역할 또는 그룹 이름이 조직에 정의된 역할 또는 그룹 이름과 대/소문자를 구분하여 정확히 일치해야 합니다.

- OAuth ID 제공자가 사용자를 정의하는 경우 사용자의 OAuth 토큰의 `roles` 어레이에 명명된 역할이 사용자에게 할당됩니다.
- SAML ID 제공자가 사용자를 정의하는 경우 SAML 특성에 명명된 역할이 사용자에게 할당됩니다. 이 이름은 조직의 `OrgFederationSettings`에 있는 `SamlAttributeMapping` 요소에 있는 `RoleAttributeName` 요소에 표시됩니다.

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

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.

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.

VMware Cloud 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	✓				
	사용자 지정 엔티티: 사용자 지정 엔티티 인스턴스 보기	✓				
	디스크: 소유자 변경	✓	✓			

이 릴리스의 새로운 기능	권한 이름	조직 관리자	카탈로그 작성자	vApp 작성자	vApp 사용자	콘솔 액세스 전용
	디스크: 만들기	✓	✓	✓		
	디스크: 삭제	✓	✓	✓		
	디스크: 속성 편집	✓	✓	✓		
	디스크: 암호화 상태 보기	✓		✓		
	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	✓	✓	✓	✓	
	조직 vDC 분산 방화벽: 규칙 구성	✓				
	조직 vDC 분산 방화벽: 규칙 보기	✓				

이 릴리스의 새로운 기능	권한 이름	조직 관리자	카탈로그 작성자	vApp 작성자	vApp 사용자	콘솔 액세스 전용
	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	✓				
	조직 vDC 네트워크: 속성 편집	✓				
	조직 vDC 네트워크: 속성 보기	✓		✓		
	조직 vDC 스토리지 정책: 기능 보기	✓				
	조직 vDC 스토리지 프로파일: 기본값 설정	✓				
	조직 vDC: 편집	✓				
	조직 vDC: ACL 편집	✓				
	조직 vDC: 방화벽 관리	✓				

이 릴리스의 새로운 기능	권한 이름	조직 관리자	카탈로그 작성자	vApp 작성자	vApp 사용자	콘솔 액세스 전용
	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	✓				
✓	할당량 정책 기능: 보기	✓				
	역할: 만들기, 편집, 삭제 또는 복사	✓				
	서비스 라이브러리: 서비스 라이브러리 보기	✓				
	UI 플러그인: 보기	✓	✓	✓	✓	
	vApp 템플릿/미디어: 복사	✓	✓	✓		
	vApp 템플릿/미디어: 만들기/업로드	✓	✓			
	vApp 템플릿/미디어: 편집	✓	✓	✓		
	vApp 템플릿/미디어: 보기	✓	✓	✓	✓	
	vApp 템플릿: 소유자 변경	✓	✓			
	vApp 템플릿: 체크 아웃	✓	✓	✓	✓	
	vApp 템플릿: 다운로드	✓	✓			

이 릴리스의 새로운 기능	권한 이름	조직 관리자	카탈로그 작성자	vApp 작성자	vApp 사용자	콘솔 액세스 전용
	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 및 VM의 디스크 암호화 상태 보기	✓		✓		
	vApp: VM 메트릭 보기	✓		✓	✓	
	vApp: VM 부팅 옵션	✓	✓	✓		
	vApp: vCenter에 대한 VM 메타데이터	✓	✓	✓		
✓	VDC 그룹: 구성	✓				
✓	VDC 그룹: 보기	✓				
✓	VDC 그룹: 로깅 구성	✓				

이 릴리스의 새로운 기능	권한 이름	조직 관리자	카탈로그 작성자	vApp 작성자	vApp 사용자	콘솔 액세스 전용
	VDC 템플릿: 인스턴스화	✓				
	VDC 템플릿: 보기	✓				

사용자 지정 테넌트 역할 만들기

조직 관리자는 테넌트 포털을 사용하여 자신이 관리하는 조직 내에서 사용자 지정 테넌트 역할 개체를 만들 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **역할**을 클릭합니다.
역할 목록이 나타납니다.
- 3 **추가**를 클릭합니다.
- 4 역할의 이름과 설명(선택 사항)을 입력합니다.
- 5 역할에 대한 권한을 확장하고 역할에 대한 권한을 선택합니다.

권한은 개체를 보거나 관리할 수 있는 범주 및 하위 범주로 그룹화됩니다.

옵션	설명
액세스 제어	특정 개체를 보고 관리할 수 있는 액세스를 제어하는 권한입니다.
관리	관리 액세스를 제어하는 권한입니다.
계산	조직 및 제공자 가상 데이터 센터, vApp, 조직 가상 데이터 센터 템플릿, 가상 시스템 그룹 및 가상 시스템 모니터링에 대한 액세스 및 관리를 제어하는 권한입니다.
확장	추가 플러그인 및 VMware Cloud Director 확장에 대한 액세스를 제어하는 권한입니다.
인프라	데이터스토어, 디스크, 호스트 등과 같은 인프라 개체의 액세스 및 관리를 제어하는 권한입니다.
라이브러리	카탈로그 및 카탈로그 항목의 액세스 및 관리를 제어하는 권한입니다.
네트워킹	네트워크 설정의 액세스 및 관리를 제어하는 권한입니다.

- 6 **저장**을 클릭합니다.

사용자 지정 테넌트 역할 편집

조직 관리자는 테넌트 포털을 사용하여 자신이 관리하는 조직 내에서 사용자 지정 테넌트 역할 개체를 편집할 수 있습니다. 조직 관리자는 자신의 조직에 시스템 관리자가 게시한 글로벌 테넌트 역할만 볼 수 있습니다. 글로벌 테넌트 역할은 편집할 수 없습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **역할**을 클릭합니다.
역할 목록이 나타납니다.
- 3 편집할 역할 옆에 있는 라디오 버튼을 클릭하고 **편집**을 클릭합니다.
- 4 필요에 따라 역할 설정을 수정합니다.
 - a 역할의 이름과 설명(선택 사항)을 변경합니다.
 - b 역할의 권한을 편집합니다.
- 5 **저장**을 클릭합니다.

역할 삭제

조직 관리자는 테넌트 포털을 사용하여 자신이 관리하는 조직 내에서 역할 개체를 삭제할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **액세스 제어** 아래에서 **역할**을 클릭합니다.
역할 목록이 나타납니다.
- 3 삭제할 역할의 옆에 있는 라디오 버튼을 클릭하고 **삭제**를 클릭합니다.
- 4 **확인**을 클릭하여 역할을 삭제하는 것을 확인합니다.

클라우드를 외부 ID 제공자와 통합하여 사용자와 그룹을 조직에 가져올 수 있습니다.

조직에서 SAML ID 제공자를 사용하도록 설정하거나 LDAP 서버 연결을 구성할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 조직에서 SAML ID 제공자를 사용하도록 설정
- 조직에 대한 LDAP 설정 편집
- LDAP 연결 구성, 테스트 및 동기화

조직에서 SAML ID 제공자를 사용하도록 설정

조직에서 SAML ID 제공자(Single Sign-On이라고도 함)를 사용하도록 설정하면 SAML ID 제공자의 사용자와 그룹을 가져와서 해당 사용자가 SAML ID 제공자에 설정된 자격 증명으로 조직에 로그인할 수 있도록 허용할 수 있습니다.

사용자와 그룹을 가져오면 시스템에서는 SAML 토큰(사용할 수 있는 경우)에서 특성 목록을 추출하여, 로그인을 시도하는 사용자에 대한 해당 정보를 해석하는 데 사용합니다.

- email address = "EmailAddress"
- user name = "UserName"
- full name = "FullName"
- user's groups = "Groups"
- user's roles = "Roles"

역할 특성은 구성할 수 있습니다.

그룹 정보는 사용자를 직접 가져오지 않았지만 가져온 그룹의 구성원 자격으로 사용자가 로그인할 수 있어야 하는 경우에 필요합니다. 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, 이 특성 이름은 API를 통해서만 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

- 이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.
- SAML 2.0을 준수하는 ID 제공자에 액세스할 수 있는지 확인합니다.
- SAML ID 제공자로부터 필수 메타데이터를 받았는지 확인합니다. 메타데이터를 수동으로 또는 XML 파일로 VMware Cloud Director에 가져와야 합니다. 메타데이터에는 다음 정보가 포함되어 있어야 합니다.
 - 단일 로그인 서비스의 위치
 - 단일 로그아웃 서비스의 위치
 - 서비스의 X.509 인증서 위치

SAML ID 제공자의 메타데이터를 구성하고 확보하는 방법에 대한 자세한 내용은 SAML ID 제공자의 설명서를 참조하십시오.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 **ID 제공자**에서 **SAML**을 클릭합니다.
- 3 **편집**을 클릭합니다.
- 4 **서비스 제공자** 탭에서 엔티티 ID를 입력합니다.

엔티티 ID는 ID 제공자에 대한 조직의 고유 식별자입니다. 조직의 이름 또는 SAML ID 제공자의 요구 사항을 충족하는 기타 문자열을 사용할 수 있습니다.

중요 엔티티 ID는 지정한 후에 삭제할 수 없습니다. 엔티티 ID를 변경하려면 조직에 대해 전체 SAML 재구성을 수행해야 합니다. 엔티티 ID에 대한 자세한 내용은 [Assertions and Protocols for the OASIS Security Assertion Markup Language \(SAML\) 2.0](#)을 참조하십시오.

- 5 **메타데이터** 링크를 클릭하여 조직의 SAML 메타데이터를 다운로드합니다.
다운로드한 메타데이터는 있는 그대로 ID 제공자에 제공해야 합니다.
- 6 인증서 만료 날짜를 검토하고, 필요한 경우 재생성을 클릭하여 페더레이션 메시지에 서명하는 데 사용되는 인증서를 재생성합니다.
인증서는 SAML 메타데이터에 포함되어 있으며 암호화 및 서명에 모두 사용됩니다. 조직과 SAML ID 제공자 간에 신뢰가 설정된 방식에 따라 암호화 및 서명 중 하나 또는 둘 모두 필요할 수 있습니다.
- 7 **ID 제공자** 탭에서 **SAML ID 제공자** 토글을 사용하도록 설정합니다.
- 8 ID 제공자로부터 수신한 SAML 메타데이터를 복사하여 텍스트 상자에 붙여 넣거나, **업로드**를 클릭한 후 XML 파일의 메타데이터를 찾아 업로드합니다.
- 9 **저장**을 클릭합니다.

다음에 수행할 작업

- VMware Cloud Director 메타데이터를 사용하여 SAML 제공자를 구성합니다. SAML ID 제공자 설명서 및 "VMware Cloud Director 설치, 구성 및 업그레이드 가이드"의 내용을 참조하십시오.
- SAML ID 제공자에서 사용자 및 그룹을 가져옵니다. [장 13 사용자, 그룹 및 역할 관리](#) 항목을 참조하십시오.

조직에 대한 LDAP 설정 편집

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.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.
- 2 왼쪽 패널의 **ID 제공자** 아래에서 **LDAP**를 클릭합니다.
현재 LDAP 설정이 표시됩니다.
- 3 **LDAP 설정** 탭에서 **편집**를 클릭합니다.
- 4 조직에 대한 사용자 및 그룹의 LDAP 소스를 구성하고 **저장**을 클릭합니다.

옵션	설명
LDAP 사용 안 함	조직에서 LDAP 서버를 조직 사용자 및 그룹의 소스로 사용하지 않습니다.
VMware Cloud Director 시스템 LDAP 서비스	조직에서는 서비스 제공자가 구성한 VMware Cloud Director 시스템 LDAP 연결을 사용합니다. 조직 구성 단위에 대한 고유 이름을 입력합니다.
사용자 지정 LDAP 서비스	조직에서 개인 LDAP 서버를 조직 사용자 및 그룹의 소스로 사용합니다.

다음에 수행할 작업

사용자 지정 LDAP 서비스를 선택한 경우 **사용자 지정 LDAP** 탭을 클릭하여 [LDAP 연결 구성, 테스트 및 동기화](#)합니다.

LDAP 연결 구성, 테스트 및 동기화

LDAP 연결을 구성하려면 LDAP 서버의 세부 정보를 설정합니다. 연결을 테스트하여 올바른 설정을 입력했는지, 사용자 및 그룹 특성이 올바르게 매핑되었는지 확인할 수 있습니다. LDAP 연결에 성공하면 언제든지 사용자 및 그룹 정보를 LDAP 서버와 동기화할 수 있습니다.

사전 요구 사항

LDAPS(SSL을 통한 LDAP 서버)에 연결할 계획인 경우 LDAP 서버의 인증서가 Java 8 업데이트 181에 도입된 끝점 ID를 준수하는지 확인합니다. 인증서의 CN(일반 이름) 또는 SAN(주체 대체 이름)은 LDAP 서버의 FQDN과 일치해야 합니다. 자세한 내용은 <https://www.java.com>에서 "Java 8 릴리스 변경 내용"을 참조하십시오.

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

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 VMware Cloud Director가 연결할 LDAP 디렉토리 내의 위치입니다. 루트 수준에서 연결하려면 도메인 구성 요소만 입력합니다(예: DC=example,DC=com). 도메인 트리 구조의 노드에 연결하려면 해당 노드의 고유 이름을 입력합니다(예: OU=ServiceDirector,DC=example,DC=com). 노드에 연결하면 VMware Cloud 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 버튼을 클릭하고 LDAP SSL 인증서를 가져오거나, 모든 인증서 수락 을 선택합니다.
인증 방법	단순 인증은 사용자의 DN과 암호를 LDAP 서버로 전송하는 작업으로 구성됩니다. LDAP를 사용하는 경우에는 LDAP 암호가 네트워크를 통해 일반 텍스트로 전송됩니다. Kerberos를 사용하려면 vCloud API를 사용하여 LDAP 연결을 구성해야 합니다.

필요한 정보	설명
사용자 이름	도메인 관리자 권한을 가진 서비스 계정의 전체 LDAP DN(고유 이름)을 입력합니다. VMware Cloud Director는 이 계정을 사용하여 LDAP 디렉토리를 쿼리하고 사용자 정보를 검색합니다. LDAP 서버에 익명 읽기 지원을 사용하도록 설정되어 있으면 이러한 텍스트 상자를 비워둘 수 있습니다.
암호	LDAP 서버에 연결하는 서비스 계정의 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.
- 5 **SSL 사용** 확인란을 선택하고 LDAPS 서버의 인증서를 아직 신뢰할 수 없는 경우 **인증서 신뢰** 창에서 서버 끝점에 표시된 인증서를 신뢰하는지 확인합니다.
- 6 LDAP 연결 설정 및 LDAP 특성 매핑을 테스트하려면 다음을 수행합니다.
 - a **테스트**를 클릭합니다.
 - b 구성된 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.
 - c 종료하려면 **취소**를 클릭합니다.
- 7 VMware Cloud Director를 구성된 LDAP 서버와 동기화하려면 **동기화**를 클릭합니다.
VMware Cloud 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.

VMware Cloud Director에서 인증서를 가져오고, 다운로드하고, 편집하고, 삭제할 수 있습니다. 인증서 PEM 데이터를 클립보드에 복사할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 신뢰할 수 있는 인증서 가져오기
- 인증서 라이브러리에 인증서 가져오기

신뢰할 수 있는 인증서 가져오기

vCenter Server, NSX Manager 등과 같이 VMware Cloud Director가 통신하는 서버의 인증서를 가져올 수 있습니다.

FIPS 모드에서 VMware Cloud Director를 사용하는 경우 FIPS 호환 개인 키를 사용해야 합니다. pyOpenSSL을 사용하여 FIPS 호환 PKCS#8 형식으로 개인 키를 생성할 수 있습니다. OpenSSL을 사용하여 PKCS#8 개인 키를 생성하는 경우 개인 키는 FIPS와 호환되지 않습니다. FIPS 모드에 대한 자세한 내용은 서버 그룹의 셀에서 **FIPS 모드 활성화** 또는 **VMware Cloud Director** 장치에서 **FIPS 모드 활성화** 또는 **비활성화**를 참조하십시오.

사전 요구 사항

시스템 관리자 또는 **조직 관리자**로 로그인했는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **인증서 관리**에서 **신뢰할 수 있는 인증서**를 선택하고 **가져오기**를 클릭합니다.
- 3 가져올 인증서가 들어 있는 PEM 파일을 업로드하고 **가져오기**를 클릭합니다.
- 4 (선택 사항) 인증서 이름을 편집합니다.
- 5 **가져오기**를 클릭합니다.

다음에 수행할 작업

- 인증서를 다운로드합니다.
- 인증서 이름을 편집합니다.

- 인증서를 삭제합니다.
- PEM 데이터를 클립보드에 복사합니다.

인증서 라이브러리에 인증서 가져오기

VMware Cloud Director 인증서 라이브러리에서 서버, Edge 게이트웨이 등과 같이 보호해야 하는 엔티티를 만들 때 사용되는 인증서를 가져올 수 있습니다.

인증서 라이브러리에는 단일 인증서, 인증서 체인, 개인 키, 인증서 만료 날짜, 인증서가 보호하는 엔티티 등에 대한 정보가 포함됩니다.

FIPS 모드에서 VMware Cloud Director를 사용하는 경우 자체 서명된 FIPS 호환 인증서 및 개인 키를 사용해야 합니다. pyOpenSSL을 사용하여 자체 서명된 암호화되지 않은 인증서 및 개인 키를 생성할 수 있습니다. OpenSSL을 사용하여 자체 서명된 인증서 및 개인 키를 생성하는 경우 인증서 및 개인 키는 FIPS와 호환되지 않습니다. FIPS 모드에 대한 자세한 내용은 [서버 그룹의 셀에서 FIPS 모드 활성화](#) 또는 [VMware Cloud Director 장치에서 FIPS 모드 활성화 또는 비활성화](#)를 참조하십시오.

사전 요구 사항

시스템 관리자 또는 **조직 관리자**로 로그인했는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **인증서 관리**에서 **인증서 라이브러리**를 선택하고 **가져오기**를 클릭합니다.
- 3 인증서 라이브러리에 이 인증서의 이름과 설명(선택 사항)을 입력하고 **다음**을 클릭합니다.
- 4 가져올 인증서 체인이 들어 있는 PEM 파일을 업로드하고 **다음**을 클릭합니다.
- 5 (선택 사항) 개인 키 파일을 업로드합니다.

개인 키 파일이 암호로 보호되어 있지 않을 수 있습니다.

- 6 **가져오기**를 클릭합니다.

결과

가져온 인증서는 보호해야 하는 엔티티를 만드는 동안 사용 가능한 인증서 목록에 나타납니다.

다음에 수행할 작업

- 인증서를 다운로드합니다.
- 인증서의 이름과 설명을 편집합니다.
- 인증서를 삭제합니다. 엔티티를 보호하지 않는 인증서만 삭제할 수 있습니다.
- 인증서 PEM 데이터를 클립보드에 복사합니다.

조직 관리자는 조직 내에서 다양한 설정을 수정할 수 있습니다. 조직 이름, e-메일 설정, 도메인 설정, 메타 데이터, 정책 등을 수정할 수 있습니다.

VMware Cloud Director API를 사용하여 MQTT 프로토콜을 통해 조직의 이벤트 및 작업에 대한 메시지를 구독할 수 있습니다. "VMware Cloud Director 설치, 구성 및 업그레이드 가이드"에서 MQTT 클라이언트를 사용하여 이벤트 및 작업 구독에 대한 정보를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- 조직 이름 및 설명 편집
- e-메일 설정 수정
- SMTP 설정 테스트
- 조직의 가상 시스템에 대한 도메인 설정 수정
- 다중 사이트 작업
- 다중 사이트 배포 구성 및 관리
- 임대 이해
- 조직 내의 vApp 및 vApp 템플릿 임대 정책 수정
- 조직 내의 암호 및 사용자 계정 정책 수정
- 권고 대시보드 만들기

조직 이름 및 설명 편집

조직의 전체 이름과 설명을 편집할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.

2 설정에서 일반을 클릭합니다.

조직 이름, 기본 URL, 전체 이름 및 설명과 같은 일반 설정 목록이 표시됩니다.

3 조직의 전체 이름과 설명을 수정하려면 편집을 클릭합니다.

4 필요한 변경 사항을 적용하고 저장을 클릭합니다.

e-메일 설정 수정

시스템 관리자가 조직을 만들 때 설정한 기본 e-메일 설정을 검토하고 수정할 수 있습니다.

VMware Cloud Director는 보고할 중요한 정보가 있으면, 예를 들어 데이터스토어의 공간이 부족하면, 경고 e-메일을 보냅니다. 기본적으로 조직은 시스템 수준에 지정된 SMTP 서버를 사용하여 시스템 관리자 또는 시스템 수준에 지정된 e-메일 주소 목록에 e-메일 경고를 보냅니다. VMware Cloud Director에서 시스템 수준에 지정된 것과 다른 e-메일 주소 집합에 해당 조직에 관한 경고를 보내거나, 조직에서 시스템 수준에 지정된 것과 다른 SMTP 서버를 사용하여 경고를 보내려는 경우에는 조직 수준에서 e-메일 설정을 수정할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

1 위쪽 탐색 모음에서 관리를 클릭합니다.

2 설정에서 e-메일을 클릭합니다.

조직에 대한 e-메일 설정이 표시됩니다.

3 편집을 클릭합니다.

4 SMTP 서버 탭에서 SMTP 서버 설정을 편집합니다.

a 사용자 지정 SMTP 서버를 사용할지 또는 기본값을 사용할지 선택합니다.

b 사용자 지정 SMTP 서버를 사용하도록 선택한 경우 **SMTP 서버 이름** 텍스트 상자에 SMTP 서버의 DNS 호스트 이름 또는 IP 주소를 입력합니다.

c (선택 사항) SMTP 서버 포트를 입력합니다.

d (선택 사항) 인증 필요 여부를 선택하고 사용자 이름과 암호를 입력합니다.

5 알림 설정을 편집하려면 알림 설정 탭을 클릭합니다.

a 사용자 지정 알림 설정을 사용하도록 선택합니다.

b 조직 e-메일에 보낸 사람으로 표시될 e-메일 주소를 입력합니다.

c (선택 사항) e-메일 제목 접두사로 사용할 텍스트를 입력합니다.

d (선택 사항) 알림을 모든 조직 관리자에게 보낼지 또는 특정 e-메일 주소에 보낼지 선택합니다.

e (선택 사항) 특정 e-메일 주소에 알림을 보내도록 선택하는 경우에는 e-메일 주소를 쉼표로 구분하여 입력합니다.

6 **저장**을 클릭합니다.

SMTP 설정 테스트

조직의 e-메일 설정을 수정한 후 SMTP 설정을 테스트할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

1 위쪽 탐색 모음에서 **관리**를 클릭합니다.

2 **설정**에서 **e-메일**을 클릭합니다.

조직에 대한 e-메일 설정이 표시됩니다.

3 **테스트**를 클릭합니다.

4 SMTP 설정을 테스트하기 위한 대상 e-메일 주소와 SMTP 서버 암호를 입력하고 **테스트** 버튼을 클릭합니다.

조직의 가상 시스템에 대한 도메인 설정 수정

조직에서 만들어진 가상 시스템이 가입할 수 있는 기본 Windows 도메인을 설정할 수 있습니다. 가상 시스템은 기본 도메인 지정 여부와 관계없이 항상 자격 증명이 있는 도메인에 가입할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

1 위쪽 탐색 모음에서 **관리**를 클릭합니다.

2 **설정**에서 **게스트 개인 설정**을 클릭합니다.

3 조직의 가상 시스템에 도메인 가입을 사용하도록 선택합니다.

4 도메인 이름, 사용자 이름 및 암호를 입력합니다.

입력한 자격 증명은 도메인 관리자가 아닌 일반 도메인 사용자에게 적용됩니다.

5 (선택 사항) 계정 조직 구성 단위를 입력합니다.

6 저장을 클릭합니다.

다중 사이트 작업

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

조직 관리자는 VMware Cloud Director 테넌트 포털에서 조직을 연결된 사이트에 연결할 수 있습니다.

사이트 연결에 대한 자세한 정보는 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"의 내용을 참조하십시오.

다중 사이트 배포 구성 및 관리

시스템 관리자가 두 사이트를 연결한 후 모든 구성원 사이트의 **조직 관리자**는 조직 연결을 시작할 수 있습니다.

두 조직(여기서는 조직 A와 조직 B로 칭함) 간의 연결을 만들려면 두 조직의 **조직 관리자**여야 합니다. 그래야 각 조직에 로그인하고, 로컬 연결 데이터를 검색하고, 검색한 데이터를 다른 조직에 제출할 수 있습니다.

중요 두 조직을 연결하는 프로세스는 논리적으로 두 개의 상호 보완적인 연결 작업으로 나눌 수 있습니다. 이 예에서 첫 번째 작업은 사이트 A의 조직 A를 사이트 B의 조직 B와 연결합니다. 그런 다음 사이트 B의 조직 B를 사이트 A의 조직 A와 연결합니다. 두 연결이 완료되기 전까지는 연결이 완전하지 않습니다.

사전 요구 사항

- 조직이 사용하는 사이트를 연결해야 합니다.
- 두 사이트의 **시스템 관리자**이거나 두 조직의 **조직 관리자**여야 합니다.

절차

- 1 사이트 A에 있는 조직 A의 VMware Cloud Director 테넌트 포털에 로그인하여 로컬 연결 데이터를 검색합니다.
 - a **관리**를 클릭합니다.
 - b **설정**에서 **다중 사이트**를 클릭합니다.
 - c XML 형식으로 데이터를 다운로드하려면 **로컬 연결 데이터 내보내기**를 클릭합니다.
브라우저의 다운로드 폴더에 있는 파일에 데이터가 저장됩니다.
- 2 사이트 B에 있는 조직 B의 VMware Cloud Director 테넌트 포털에 로그인하여 사이트 A에 있는 조직 A의 로컬 연결 데이터를 제출합니다.
 - a **관리**를 클릭합니다.
 - b **설정**에서 **다중 사이트**를 클릭합니다.

c **새 조직 연결 만들기**를 클릭합니다.

새 연결 XML 텍스트 상자 아래에서 위쪽 화살표를 클릭하고 **단계 1단계**에서 다운로드한 로컬 연결 데이터를 선택하여 **단계 1단계**에서 다운로드한 연결 데이터를 조직 B에 제출합니다.

d **다음**을 클릭하여 데이터를 확인하고 제출합니다.

시스템에서 사이트 A의 조직 A가 사이트 B의 조직 B와 쌍으로 구성됩니다.

e **완료**를 클릭하여 연결된 조직을 확인합니다.

f 연결된 조직의 세부 정보를 보거나 연결을 삭제하려면 **조직 이름** 카드를 클릭합니다.

3 1단계와 2단계를 반복하여 연결을 완료하고 조직 B에서 로컬 연결 데이터를 검색하여 조직 A에 제출합니다.

임대 이해

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

런타임 임대의 목표는 비활성 vApp이 계산 리소스를 소비하지 못하도록 막는 것입니다. 예를 들어 어떤 사용자가 vApp을 시작한 다음 중지하지 않고 휴가를 떠나면 vApp에서 계속 리소스가 소비됩니다.

런타임 임대는 사용자가 vApp을 시작하면 시작됩니다. 런타임 임대가 만료되면 VMware Cloud Director가 vApp을 중지합니다.

스토리지 임대의 목적은 사용되지 않는 vApp 및 vApp 템플릿이 스토리지 리소스를 사용하지 못하도록 하는 것입니다. vApp 스토리지 임대는 사용자가 vApp을 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 VMware Cloud Director에서는 관리자가 설정한 조직 정책에 따라 vApp 또는 vApp 템플릿을 만료된 것으로 표시하거나 삭제합니다.

조직 내의 vApp 및 vApp 템플릿 임대 정책 수정

시스템 관리자가 조직을 만들 때 설정한 기본 정책을 검토하고 수정할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

1 위쪽 탐색 모음에서 **관리**를 클릭합니다.

2 **설정**에서 **정책**을 클릭합니다.

시스템 관리자가 설정한 기본 정책을 볼 수 있습니다.

3 편집을 클릭합니다.**4 vApp 임대**를 편집합니다.

vApp 임대는 vApp을 실행할 수 있고 vApp을 저장할 수 있는 최대 시간을 지정하여 조직 스토리지 및 계산 리소스에 대해 일정 수준의 제어를 제공합니다. 스토리지 임대가 만료되면 vApp을 어떻게 처리할지 지정할 수도 있습니다.

- a vApp이 자동으로 중지되기 전에 실행될 수 있는 기간을 정의하려면, 최대 런타임 임대를 입력합니다.
- b 런타임 만료 작업(예: 전원 끄기 또는 일시 중단)을 선택합니다.
- c 중지된 vApp이 자동으로 정리되기 전에 사용 가능한 상태로 유지되는 기간을 정의하려면, 최대 스토리지 임대를 입력합니다.
- d 스토리지 정리 작업(예: vApp 영구 삭제 또는 vApp을 만료된 항목으로 이동)을 선택합니다.

5 vApp 템플릿 임대를 편집합니다.

vApp 템플릿 임대는 vApp 템플릿을 저장할 수 있는 최대 시간을 지정하여 조직 스토리지 및 계산 리소스에 대해 일정 수준의 제어를 제공합니다. 스토리지 임대가 만료되면 vApp 템플릿을 어떻게 처리할지 지정할 수도 있습니다.

- a vApp 템플릿이 자동으로 정리되기 전에 사용 가능한 상태로 유지되는 기간을 정의하려면, 최대 스토리지 임대를 입력합니다.
- b 스토리지 정리 작업(예: vApp 템플릿 영구 삭제 또는 vApp 템플릿을 만료된 항목으로 이동)을 선택합니다.

6 확인을 클릭합니다.

조직 내의 암호 및 사용자 계정 정책 수정

시스템 관리자가 조직을 만들 때 설정한 기본 암호 및 사용자 계정 정책을 검토하고 수정할 수 있습니다.

암호 및 사용자 계정 정책은 사용자가 잘못된 암호를 입력하는 경우 VMware Cloud Director의 동작을 정의합니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 **조직 관리자** 역할에 포함된 권한 또는 이와 동등한 권한 집합이 필요합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 클릭합니다.

- 2 **설정**에서 **정책**을 클릭합니다.

시스템 관리자가 설정한 기본 정책을 볼 수 있습니다.

- 3 **편집**을 클릭합니다.

- 4 잘못된 로그인 이 수차례 시도된 후에는 사용자 계정 잠금이 사용되도록 설정합니다.
- 5 계정이 잠기기 전에 잘못된 로그인 시도 횟수를 입력합니다.
- 6 계정이 잠긴 사용자가 다시 로그인할 수 없는 시간 간격을 분 단위로 입력합니다.
- 7 **확인**을 클릭합니다.

권고 대시보드 만들기

Tenant Portal의 UI 페이지 위에 나타나는 알림을 만들 수 있습니다. 이 메시지를 조직 내의 사용자 또는 모든 조직의 사용자에게 표시할 수 있습니다.

권고를 만든 후에는 편집할 수 없습니다.

사전 요구 사항

시스템 관리자로 로그인했는지 확인합니다.

절차

- 1 위쪽 탐색 모음에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **설정**에서 **권고**를 선택하고 **새로 만들기**를 클릭합니다.
- 3 설명 상자에 알림 텍스트를 추가합니다.

기본 마크다운을 사용하여 알림에 링크를 추가할 수 있습니다.

- 4 메시지의 우선 순위를 선택합니다.

우선 순위 메시지가 각기 다른 색으로 표시됩니다. 알림은 우선 순위에 따라 표시됩니다. 필수 권고는 해제하거나 연기할 수 없습니다.

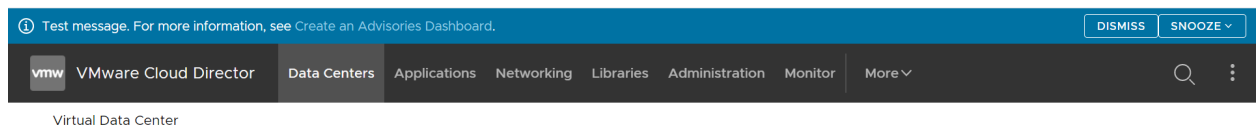
- 5 UI에서 알림을 표시할 기간을 선택합니다.

권고 탭에서 모든 권고를 볼 수 있지만 선택한 기간 동안에만 선택한 사용자 그룹에 표시됩니다.

- 6 **확인**을 클릭합니다.

결과

선택한 포털의 위쪽 탐색 모음 위에 알림이 표시됩니다.



다음에 수행할 작업

알림 옆에 있는 라디오 버튼을 선택하고 **삭제**를 클릭하여 알림을 삭제합니다. 권고는 만료 후에도 **권고** 탭에 표시됩니다. 목록에서 제거하려면 삭제해야 합니다.

서비스 라이브러리 작업

17

VMware Cloud Director의 서비스 라이브러리 항목은 클라우드 관리 기능을 확장하고 제공자 또는 테넌트의 관리자가 서로 다른 서비스를 모니터링하고 조작할 수 있게 하는 vRealize Orchestrator 워크플로입니다.

본 장은 다음 항목을 포함합니다.

- 서비스 검색
- 서비스 실행

서비스 검색

VMware Cloud Director 테넌트 포털의 **서비스 라이브러리** 페이지에는 VMware Cloud Director로 가져와서 조직에 게시된 vRealize Orchestrator 워크플로의 집합이 나열됩니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 사용자 역할에 서비스 라이브러리 권한이 포함되어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 **서비스**에서 **서비스 라이브러리**를 선택합니다.

서비스 항목 목록이 알파벳순으로 이름이 정렬되어 카드 보기에 나타납니다(페이지당 12개 항목). 각 카드는 서비스의 이름과 vRealize Orchestrator를 가져온 서비스 범주에 해당하는 태그를 표시합니다.

- 2 페이지 상단의 **검색** 텍스트 상자에서 서비스 이름 또는 서비스가 속한 범주 이름의 첫 번째 단어를 입력합니다.

- a 서비스 이름 또는 범주에서 검색할지 선택합니다.

검색 결과가 카드 보기에 이름을 기준으로 알파벳 순서로 정렬되어 페이지당 12개 항목으로 표시됩니다.

서비스 실행

VMware Cloud Director 테넌트 포털의 [서비스 라이브러리] 페이지에서 서비스를 실행할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 사용자 역할에 서비스 라이브러리 권한이 포함되어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 **서비스**에서 **서비스 라이브러리**를 선택합니다.

서비스 항목 목록이 알파벳순으로 이름이 정렬되어 카드 보기에 나타납니다(페이지당 12개 항목). 각 카드는 서비스의 이름과 vRealize Orchestrator를 가져온 서비스 범주에 해당하는 태그를 표시합니다.

- 2 실행하려는 서비스를 검색합니다.

- 3 서비스의 카드에서 **실행**을 클릭합니다.

새 대화 상자가 열립니다. 서비스의 필수 입력 매개 변수에 대한 값을 입력해야 합니다.

- 4 **마침**을 클릭하여 서비스의 실행을 확인합니다.

다음에 수행할 작업

최근 작업 보기에서 실행의 상태를 모니터링할 수 있습니다. 자세한 내용은 [작업 보기](#)를 참조하십시오.

VMware Cloud Director 10.2부터 서비스 제공자는 VMware Cloud Director API를 사용하여 테넌트에 추가 VMware Cloud Director 기능을 제공하는 확장을 만들 수 있습니다. 서비스 제공자가 액세스 권한을 부여한 경우 정의된 엔티티를 관리하고 이를 다른 테넌트와 공유할 수 있습니다.

서비스 제공자는 RDE(Runtime Defined Entities)를 만들고 확장을 사용하도록 설정하여 VMware Cloud Director에서 확장 관련 정보를 저장하고 조작할 수 있습니다. 예를 들어 Kubernetes 확장은 RDE에서 해당 확장이 관리하는 Kubernetes 클러스터에 대한 정보를 저장할 수 있습니다. 그런 다음 확장은 RDE의 정보를 사용하여 이러한 클러스터를 관리하기 위한 확장 API를 제공할 수 있습니다.

정의된 엔티티에 액세스

두 가지 보조 메커니즘이 RDE에 대한 액세스를 제어합니다.

- 권한 - 서비스 제공자가 RDE 유형을 만들 때 해당 유형에 대한 권한 번들을 만듭니다. 서비스 제공자는 5가지 유형별 권한(**보기: TYPE**, **편집: TYPE**, **모든 권한: TYPE**, **관리자 보기: TYPE** 및 **관리자 모든 권한: TYPE**) 중 하나 이상을 할당해야 합니다.

보기: TYPE, **편집: TYPE** 및 **모든 권한: TYPE** 권한은 ACL 항목과 함께만 작동합니다.

- ACL(Access Control List) - ACL 테이블에는 시스템의 특정 엔티티에 대한 사용자 액세스를 정의하는 항목이 포함됩니다. 이는 엔티티에 대한 추가 제어 수준을 제공합니다. 예를 들어 **편집: TYPE** 권한은 사용자가 액세스 권한이 있는 엔티티를 수정할 수 있도록 지정합니다. ACL 테이블은 사용자가 액세스할 수 있는 엔티티를 정의합니다.

표 18-1. RDE 작업에 대한 권한 및 ACL 항목

엔티티 작업	옵션	설명
읽기	관리자 보기: TYPE 권한	이 권한을 가진 사용자는 조직 내에서 이 유형의 모든 RDE를 볼 수 있습니다.
	보기: TYPE 권한 및 ACL 항목 >= 보기	이 권한 및 읽기 수준 ACL이 있는 사용자는 이 유형의 RDE를 볼 수 있습니다.
수정	관리자 모든 권한: TYPE 권한	이 권한을 가진 사용자는 모든 조직에서 이 유형의 RDE를 만들고, 보고, 수정하고, 삭제할 수 있습니다.

표 18-1. RDE 작업에 대한 권한 및 ACL 항목 (계속)

엔티티 작업	옵션	설명
	편집: TYPE 권한 및 ACL 항목 >= 변경	이 권한 및 수정 수준 ACL이 있는 사용자는 이 유형의 RDE를 만들고, 보고, 수정할 수 있습니다.
삭제	관리자 모든 권한: TYPE 권한	이 권한을 가진 사용자는 모든 조직에서 이 유형의 RDE를 만들고, 보고, 수정하고, 삭제할 수 있습니다.
	모든 권한: TYPE 권한 및 ACL 항목 = 모든 권한	이 권한 및 모든 권한 수준 ACL이 있는 사용자는 이 유형의 RDE를 만들고, 보고, 수정하고, 삭제할 수 있습니다.

정의된 엔티티를 다른 사용자와 공유

시스템 관리자가 정의된 엔티티 유형에 대한 권한 번들을 게시하고 사용자에게 ReadWrite 또는 FullControl 액세스 권한을 부여했거나 사용자가 정의된 엔티티 소유자인 경우 해당 엔티티에 대한 액세스 권한을 다른 사용자와 공유할 수 있습니다.

- 1 번들에서 **보기: TYPE**, **편집: TYPE** 또는 **모든 권한: TYPE** 권한을 정의된 엔티티에 대해 특정 수준의 액세스 권한을 가지려는 사용자 역할에 할당합니다.

참고 권한을 할당하려면 **시스템 관리자** 또는 **조직 관리자**로 로그인해야 합니다.

예를 들어 **tkg_viewer** 역할을 가진 사용자가 조직 내에서 Tanzu Kubernetes 클러스터를 볼 수 있게 하려면 역할에 **보기: Tanzu Kubernetes 게스트 클러스터** 권한을 추가해야 합니다. **tkg_author** 역할을 가진 사용자가 이 조직 내에서 Tanzu Kubernetes 클러스터를 만들고, 보고, 수정할 수 있게 하려면 해당 역할에 **편집: Tanzu Kubernetes 게스트 클러스터**를 추가합니다. **tkg_admin** 역할을 가진 사용자가 이 조직 내에서 Tanzu Kubernetes 클러스터를 만들고, 보고, 수정하고, 삭제할 수 있게 하려면 역할에 **모든 권한: Tanzu Kubernetes 게스트 클러스터** 권한을 추가합니다.

- 2 다음과 같은 REST API호출을 수행하여 특정 사용자에게 ACL(Access Control List)을 부여합니다.

```
POST https://[address]/cloudapi/1.0.0/entities/urn:vcloud:entity:[vendor]:[type name]:
[version]:[UUID]/accessControls
{
  "grantType" : "MembershipAccessControlGrant",
  "accessLevelId" : "urn:vcloud:accessLevel:[Access_level]",
  "memberId" : "urn:vcloud:user:[User_ID]"
}
```

*Access_level*은 ReadOnly, ReadWrite 또는 FullControl이어야 합니다. *User_ID*는 정의된 엔티티에 대한 액세스 권한을 부여하려는 사용자의 ID여야 합니다.

엔티티에 대한 ACL 액세스 권한을 부여하려면 해당 엔티티에 대해 ReadWrite 또는 FullControl 액세스 권한이 있어야 합니다.

예에 설명된 **tkg_viewer** 역할을 가진 사용자는 ACL 액세스 권한을 부여할 수 없습니다. **tkg_author** 또는 **tkg_admin** 역할을 가진 사용자는 API 요청을 통해 ACL 액세스 권한을 부여하여 **tkg_viewer**, **tkg_author** 또는 **tkg_admin** 역할을 가진 사용자와 VMWARE:TKGCLUSTER 엔티티에 대한 액세스를 공유할 수 있습니다.

관리자 모든 권한: Tanzu Kubernetes 게스트 클러스터 권한을 가진 사용자는 모든 VMWARE:TKGCLUSTER 엔티티에 대한 ACL 액세스 권한을 부여할 수 있습니다.

또한 REST API 호출을 사용하여 액세스를 해지하거나 엔티티에 대해 액세스 권한이 있는 사용자를 볼 수 있습니다. code.vmware.com에서 VMware Cloud Director REST API 설명서를 참조하십시오.

정의된 엔티티의 소유자 변경

정의된 엔티티의 소유자 또는 **관리자 모든 권한: TYPE** 권한을 가진 사용자는 정의된 엔티티 모델을 업데이트하고 소유자 필드를 새 소유자의 ID로 변경하여 소유권을 다른 사용자에게 이전할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 사용자 지정 엔티티 정의 작업

사용자 지정 엔티티 정의 작업

VMware Cloud Director의 사용자 지정 엔티티 정의는 vRealize Orchestrator 개체 유형에 바인딩된 개체 유형입니다. VMware Cloud Director 조직 내의 사용자는 필요에 따라 이러한 유형을 소유, 관리 및 변경할 수 있습니다. 조직 사용자는 서비스를 실행하여 사용자 지정 엔티티를 인스턴스화하고 개체의 인스턴스에 작업을 적용할 수 있습니다.

사용자 지정 엔티티 검색

조직에 게시된 사용자 지정 엔티티를 검색할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 사용자 역할에 사용자 지정 엔티티 권한이 포함되어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 **서비스**에서 **사용자 지정 엔티티 정의**를 선택합니다.

사용자 지정 엔티티 목록이 알파벳순으로 이름이 정렬되어 카드 보기에 나타납니다(페이지당 12개 항목). 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. 엔티티의 유형 또는 엔티티가 바인딩되어 있는 vRealize Orchestrator 개체 유형을 변경할 수 없습니다. 이것은 사용자 지정 엔티티의 기본 속성입니다. 기본 속성을 수정하려는 경우 사용자 지정 엔티티 정의를 삭제한 후 다시 만들어야 합니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 사용자 역할에 사용자 지정 엔티티 권한이 포함되어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 **서비스**에서 **사용자 지정 엔티티 정의**를 선택합니다.
사용자 지정 엔티티 목록이 알파벳순으로 이름이 정렬되어 카드 보기에 나타납니다(페이지당 12개 항목). 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.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 사용자 역할에 사용자 지정 엔티티 권한이 포함되어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 **서비스**에서 **사용자 지정 엔티티 정의**를 선택합니다.
사용자 지정 엔티티 목록이 알파벳순으로 이름이 정렬되어 카드 보기에 나타납니다(페이지당 12개 항목). 각 카드는 사용자 지정 엔티티의 이름, 엔티티가 매핑된 vRealize Orchestrator 유형, 엔티티의 유형 및 설명(사용 가능한 경우)을 표시합니다.
- 2 새 사용자 지정 엔티티를 추가하려면 **새로 만들기**를 클릭합니다.
새 대화 상자가 열립니다.

3 사용자 지정 엔티티 정의 마법사의 단계를 따릅니다.

단계	
이름 및 설명	새 엔티티의 이름과 설명(선택 사항)을 입력합니다.
명	엔티티 유형의 이름(예: sshHost)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 아이콘을 클릭하여 플러그인별로 그룹화된 사용 가능한 vRealize Orchestrator 개체 유형을 찾아봅니다. 예를 들어 SSH > 호스트 입니다. 유형의 이름을 아는 경우 직접 텍스트 상자에 입력할 수 있습니다. 예: SSH:Host.
검토	지정한 세부 정보를 검토하고 완료 를 클릭하여 만들기를 완료합니다.

결과

새 사용자 지정 엔티티 정의가 카드 보기에 표시됩니다.

사용자 지정 엔티티 인스턴스

VMware Cloud 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.


사전 요구 사항

이 작업을 수행하려면 미리 정의된 사용자 역할에 사용자 지정 엔티티 권한이 포함되어야 합니다.

절차

- 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 **서비스**에서 **사용자 지정 엔티티 정의**를 선택합니다.

사용자 지정 엔티티 목록이 알파벳순으로 이름이 정렬되어 카드 보기에 나타납니다(페이지당 12개 항목). 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.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 사용자 역할에 사용자 지정 엔티티 권한이 포함되어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 **서비스**에서 **사용자 지정 엔티티 정의**를 선택합니다.

사용자 지정 엔티티 목록이 알파벳순으로 이름이 정렬되어 카드 보기에 나타납니다(페이지당 12개 항목). 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 엔티티 정의에서 작업 분리

연결된 작업 목록에서 vRealize Orchestrator 워크플로를 제거할 수 있습니다.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 사용자 역할에 사용자 지정 엔티티 권한이 포함되어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 **서비스**에서 **사용자 지정 엔티티 정의**를 선택합니다.

사용자 지정 엔티티 목록이 알파벳순으로 이름이 정렬되어 카드 보기에 나타납니다(페이지당 12개 항목). 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.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 사용자 역할에 사용자 지정 엔티티 권한이 포함되어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 **서비스**에서 **사용자 지정 엔티티 정의**를 선택합니다.
사용자 지정 엔티티 목록이 알파벳순으로 이름이 정렬되어 카드 보기에 나타납니다(페이지당 12개 항목). 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.

사전 요구 사항

이 작업을 수행하려면 미리 정의된 사용자 역할에 사용자 지정 엔티티 권한이 포함되어야 합니다.

절차

- 1 위쪽 탐색 모음에서 **라이브러리**를 클릭하고 **서비스**에서 **사용자 지정 엔티티 정의**를 선택합니다.
사용자 지정 엔티티 목록이 알파벳순으로 이름이 정렬되어 카드 보기에 나타납니다(페이지당 12개 항목). 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.