업데이트일 : 2019-5-14

XI. VMware on KT Cloud

1. Virtual Private Cloud

목차

1.1 Virtual Private Cloud FAQ

▫ 가상 시스템에서 Org네트워크가 보이지 않아요.

○ 라이브러리를 통해 vAPP을 생성하지 않고, vAPP메뉴에서 바로 vAPP을 생성했을 경우에는 해당 vAPP에서 사용할 Org네트워크를 추가해야 가상시스템에서 Org네트워크를 고를 수 있습니다.

▫ vAPP 네트워크는 무엇인가요?

○ Org 네트워크와 달리 vAPP네트워크는 소형 라우터로 분리되는 격리된 네트워크이며 사용을 권고하지 않으며 더 나은 성능을 위해서 Org네트워크를 통한 구성을 권고합니다.

▫ Org 네트워크의 옵션에 대해 알고 싶어요.

○ Org 네트워크는 20개까지 생성할 수 있으며 '인터페이스 유형'은 '내부'로 사용하시면 됩니다. Edge 게이트웨이는 총 10개의 인터페이스를 가질 수 있으며, 격리된 네트워크가 아닌 더 많은 Org네트워크를 Edge게이트웨이로 연결하고자 할 경우에는 '인터페이스 유형'을 '하위 인터페이스'로 설정하시면 됩니다. '분산'의 경우 지원하지 않습니다.

▫ Public, Enterprise-cloud, Enterprise-Security 사용중입니다. VMware 추가 청약 가능할까요?

○ 네. 기존 사용하시는 포탈계정에서 사용이 가능합니다.

▫ Oracle BYOL 사용이 가능한가요?

○ VMware 가상화 환경에서 Oracle의 구동은 기술적으로 가능한 것으로 알려져 있으나, Oracle 벤더사의 라이선스 정책을 준수해야 합니다. 이에 현실적으로 벤더사의 H/W socket 라이선스 기준은 클라우드 가상화 환경에서 사용이 어렵습니다. Oracle DB 등 구매한 BYOL 가능한 환경으로 베어메탈(물리) 서버를 제공할 예정으로 있으니 참고 부탁드립니다.

1.2 VMware on KT Cloud 청약 및 서버이용방법

메뉴얼 구성

1.2.1 VMware on KT Cloud청약방법 및 접속방법

- VMware on KT Cloud 서비스 청약방법 및 접속방법

1.2.2 VMware on KT Cloud가상머신(VM) 이용방법

- 조직 네트워크 추가 및 외부 인터넷 설정
- 템플릿을 이용하여 vApp 생성
- vApp 기반의 VM 생성

1.2.3 VMware on KT Cloud Edge NAT/Firewall 이용방법

- Edge 게이트웨이 방화벽 규칙 추가

1.2.4 vCloud director를 통해 VM에 접속 및 기본설정

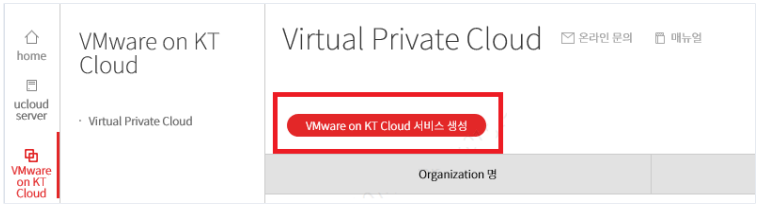
- vCloud director을 통한 VM 접속
- 정품 인증 (window OS)
- 초기 계정 설정 (centOS)

1.2.1 VMware on KT Cloud 청약방법 및 접속방법

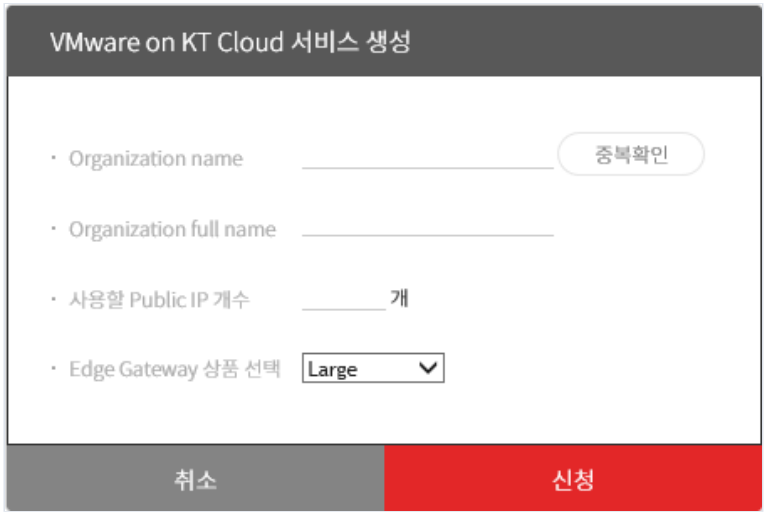
▫ VMware on KT Cloud Cloud 서비스 청약방법 및 접속방법

VMware on KT Cloud (Virtual Private Cloud 형태) 서비스를 청약하고 접속하는 방법을 설명합니다.

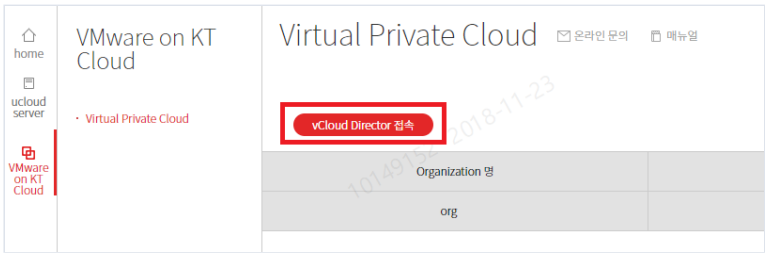
○ 클라우드콘솔 - VMware on KT cloud - VMware on KT cloud 서비스 생성 버튼을 클릭합니다
- 상품 청약은 KT 클라우드 콘솔을 통해 진행하실 수 있습니다.



○ 서비스 이용에 필요한 정보를 기입 후 신청 버튼을 클릭합니다
- Organization, Public IP(NSX edge 보유), NSX edge 크기를 선택하여 최초 구성을 진행합니다.



○ 서비스 생성이 완료된 후 'vCloud Director 접속' 버튼을 눌러 사용을 시작합니다
- Virtual Private Cloud 형태의 VMware on KTcloud을 제공하는 vCloud Director 프론트앤드 페이지에 접속할 수 있습니다.



1.2.2 VMware on KT Cloud 가상머신(VM) 이용방법

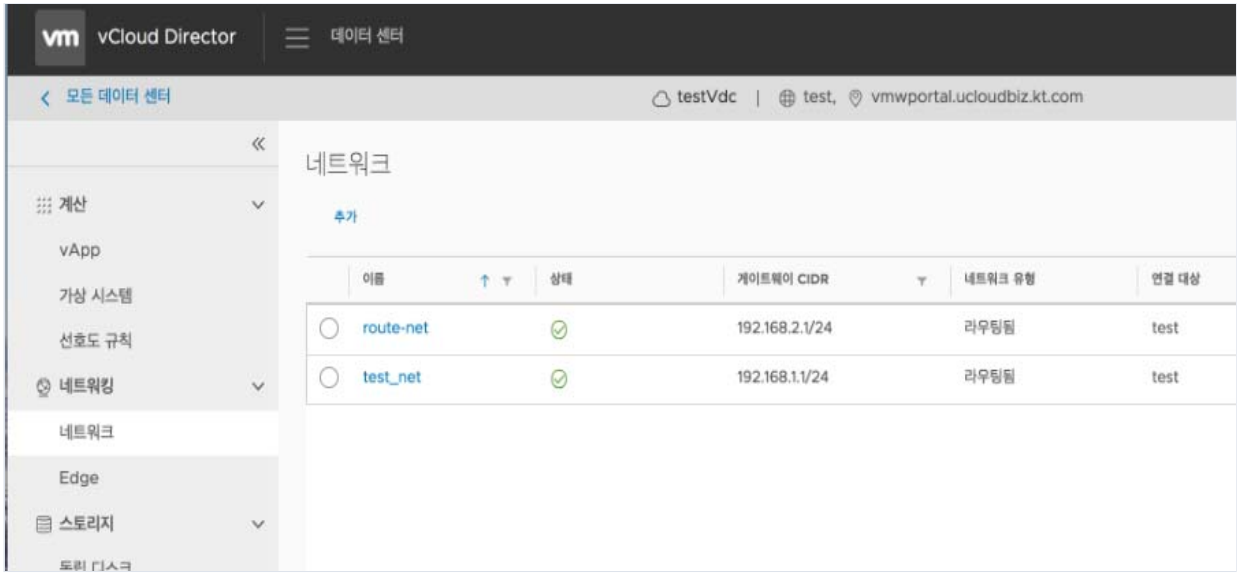
▫ VM 생성, 외부 인터넷 연결

○조직 네트워크 추가

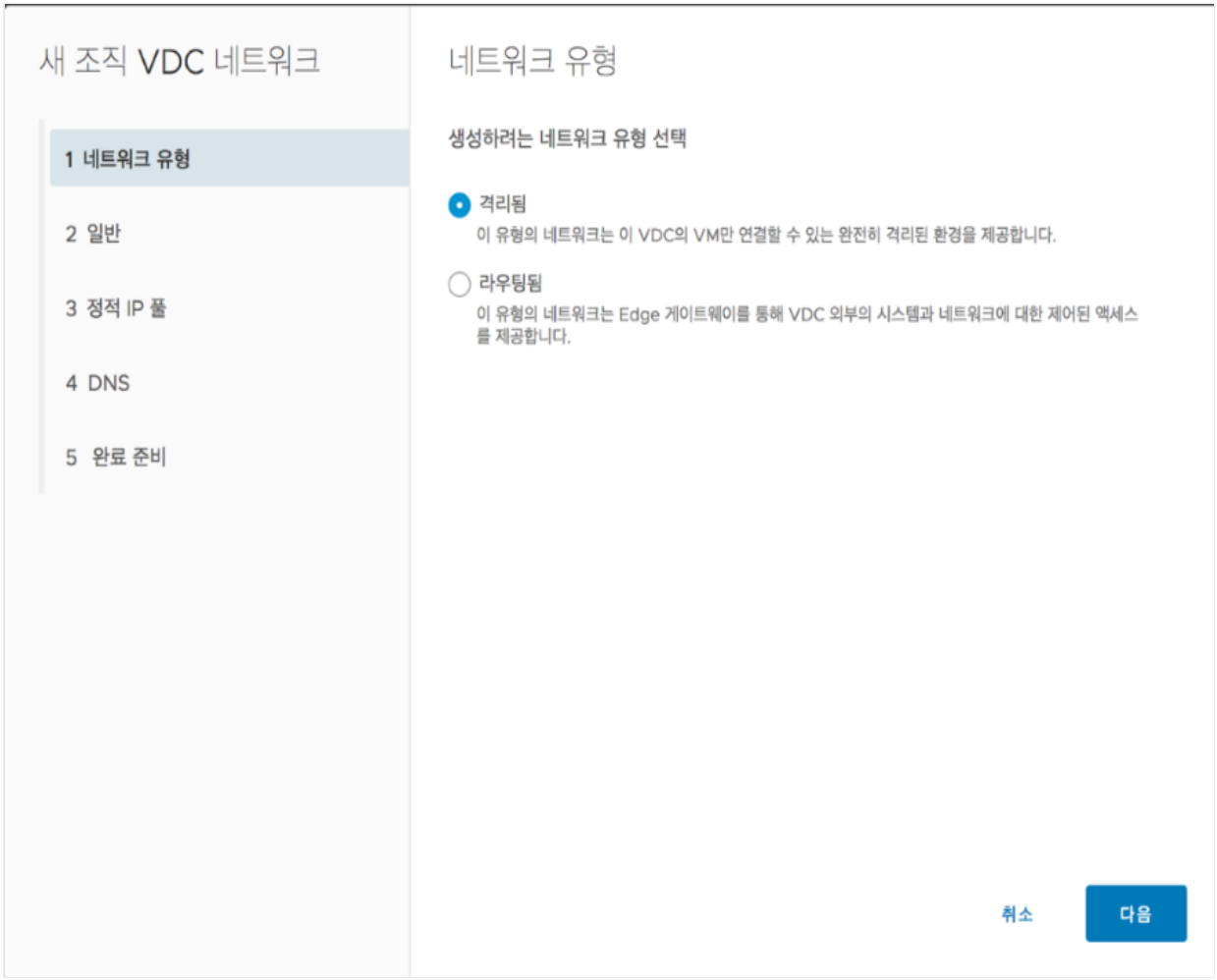
조직의 요구 사항에 따라 복수의 네트워크를 만들 수 있습니다. 필요에 맞게 내부(격리된) 또는 라우팅(인터넷)된 조직 VDC 네트워크를 추가할 수 있습니다.

예를 들어 중요한 정보가 포함된 네트워크를 격리하려면 내부로, 인터넷에 연결하려면 Edge 게이트웨이에 연결된 라우팅 네트워크를 만듭니다.

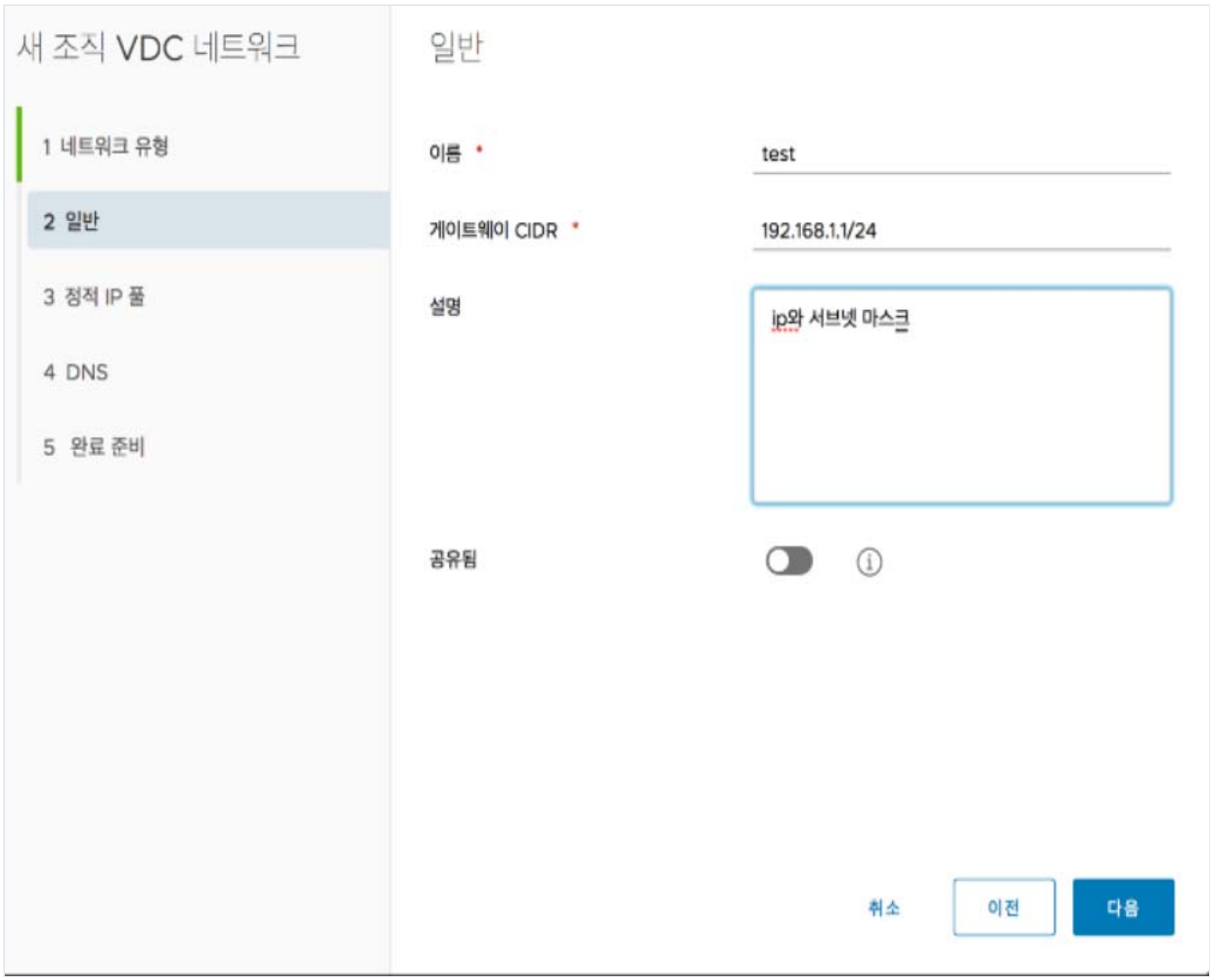
○ **가상 데이터 센터** 대시보드 화면에서 탐색할 가상 데이터 센터의 카드를 클릭하고 왼쪽 패널에서 **네트워크**를 선택, **새로만들기**를 클릭합니다.



○ 인터넷 라우팅 , 격리 옵션 중 하나를 선택합니다.



○ 네트워크의 서브넷을 구성하기 위해 네트워크 게이트웨이 CIDR(Classless Inter-Domain Routing) 설정을 입력합니다. 사설 네트워크에서 사용할 Gateway IP와
서브넷 마스크를 입력합니다.

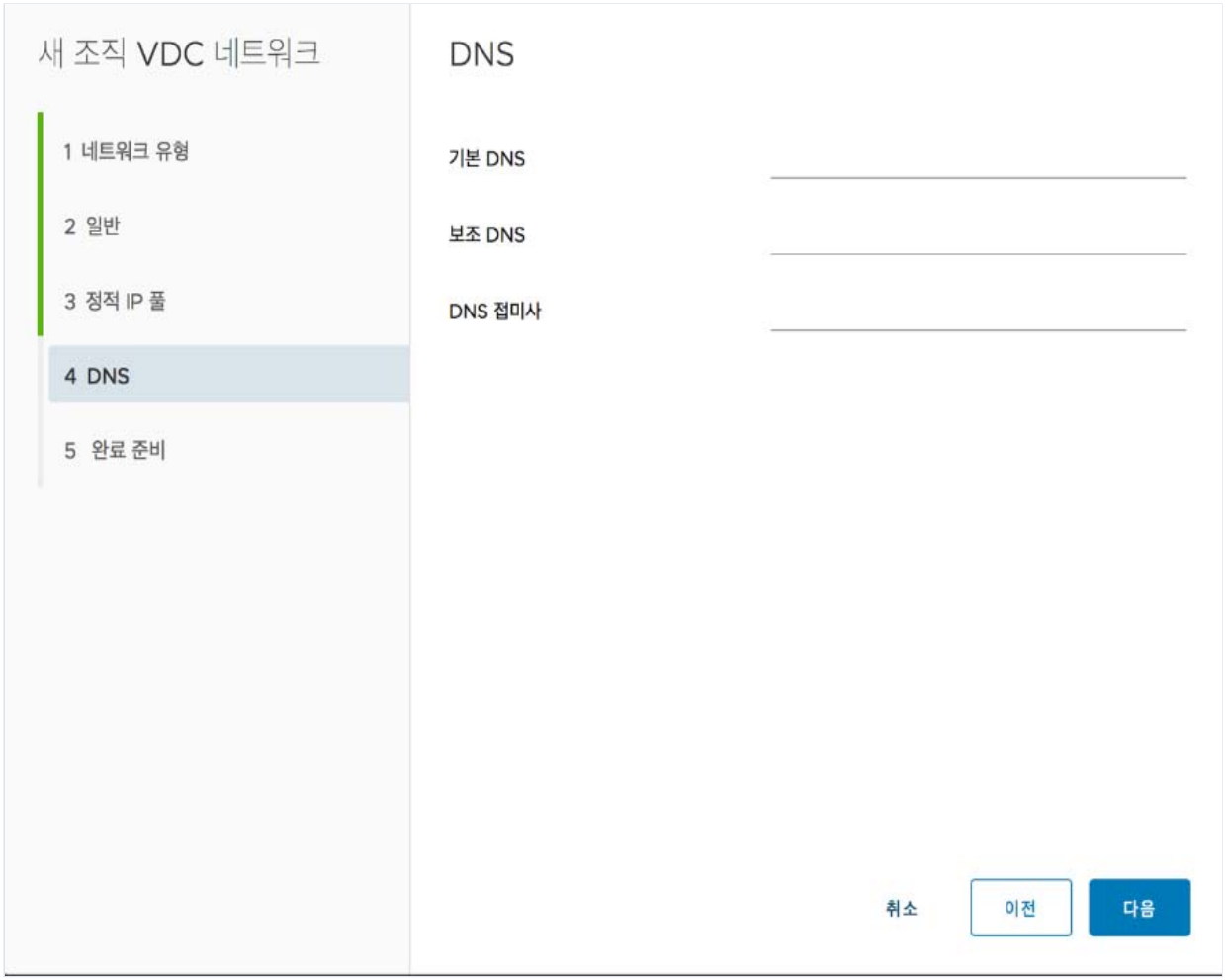


ㅇ (선택 사항) 이 네트워크에 대한 정적 IP 주소를 구성합니다. 정적 IP를 설정할 경우, 해당 네트워크에 연결되는 VM들에 대해 설정된 정적 IP 범위 내에서 IP를
부여합니다.

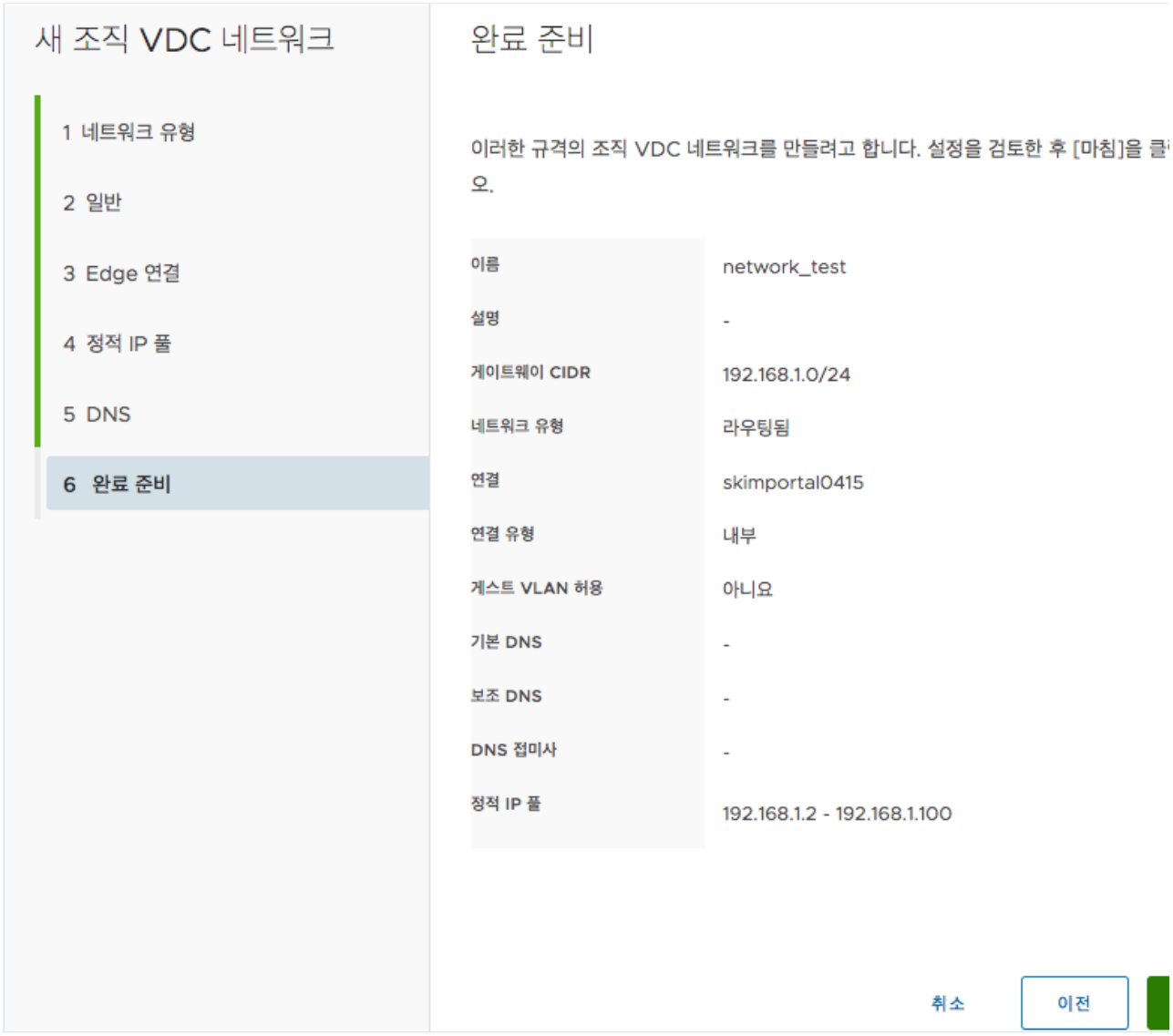
- DHCP를 구성하지 않고도 정적 IP풀을 통해 간단히 가상 시스템에 IP를 자동으로 부여할 수 있습니다. 할당할 하나 이상의 주소 범위를 입력하고 **추가**를 클릭합니다.

  ㅇ 여러 정적 IP 풀을 추가하려면 이 단계를 반복합니다.

ㅇ (선택 사항) DNS 설정을 구성합니다. 해당 사설 네트워크의 VM들이 동일한 DNS 설정을 사용하도록 구성하려면 **DNS** IP를 입력합니다.



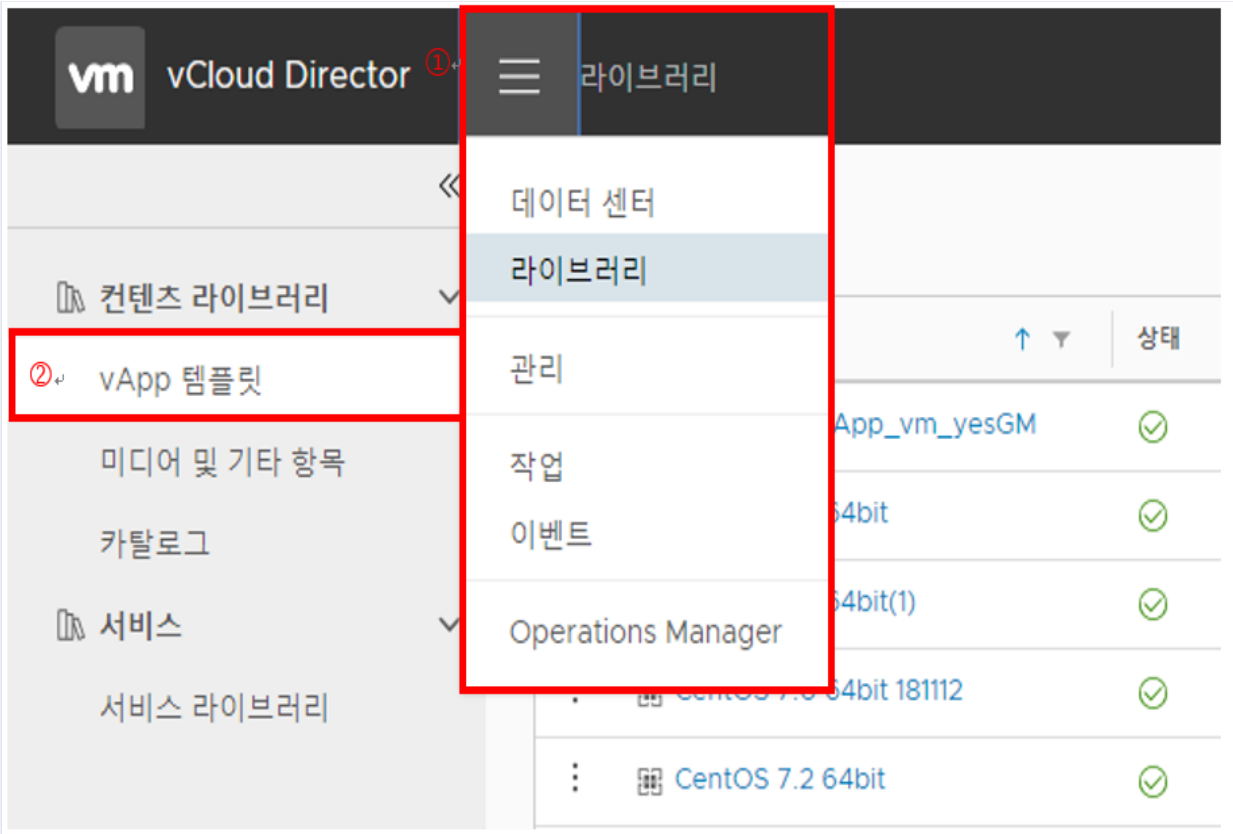
○ 설정 내역을 확인 한 후, 확인을 눌러 네트워크를 생성합니다.



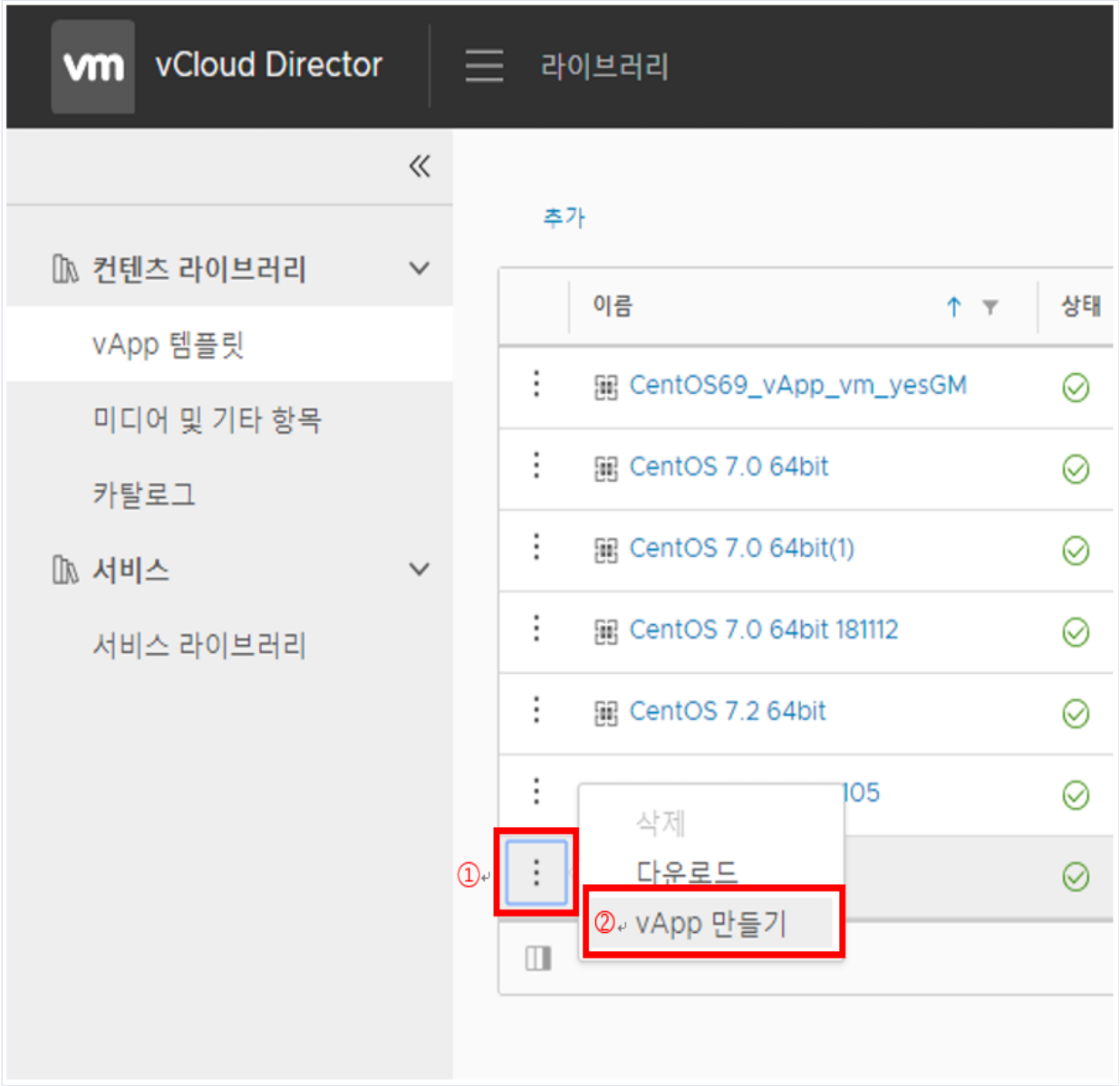
▫ 템플릿에서 vApp 만들기

KT가 제공하는 공개 카탈로그를 통해 표준화된 템플릿을 사용하여 새 vApp을 만들 수 있습니다.

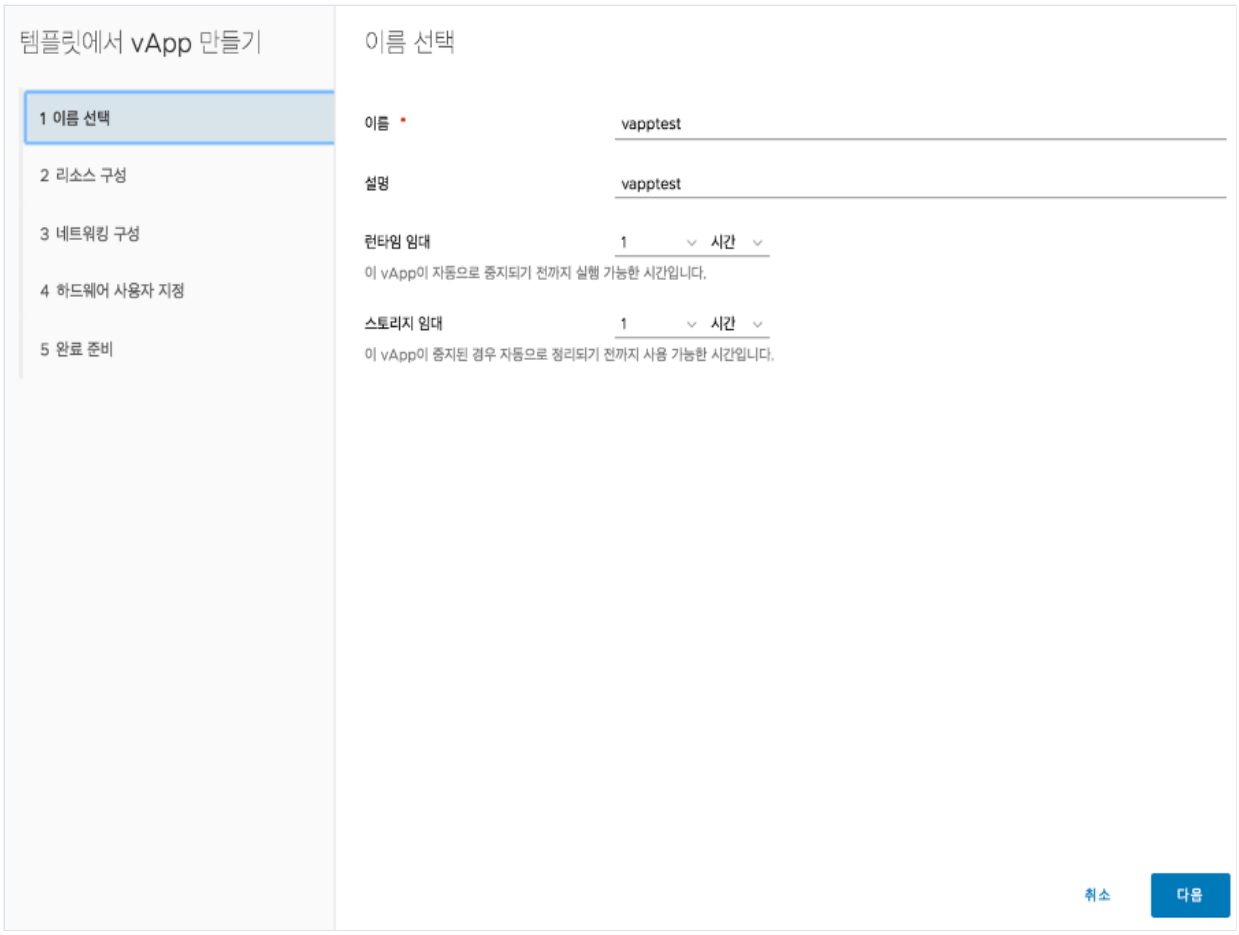
○ 기본 메뉴에서 라이브러리를 선택하고 왼쪽 패널에서 vApp 템플릿을 선택합니다. 템플릿 목록이 그리드 보기에 표시됩니다.



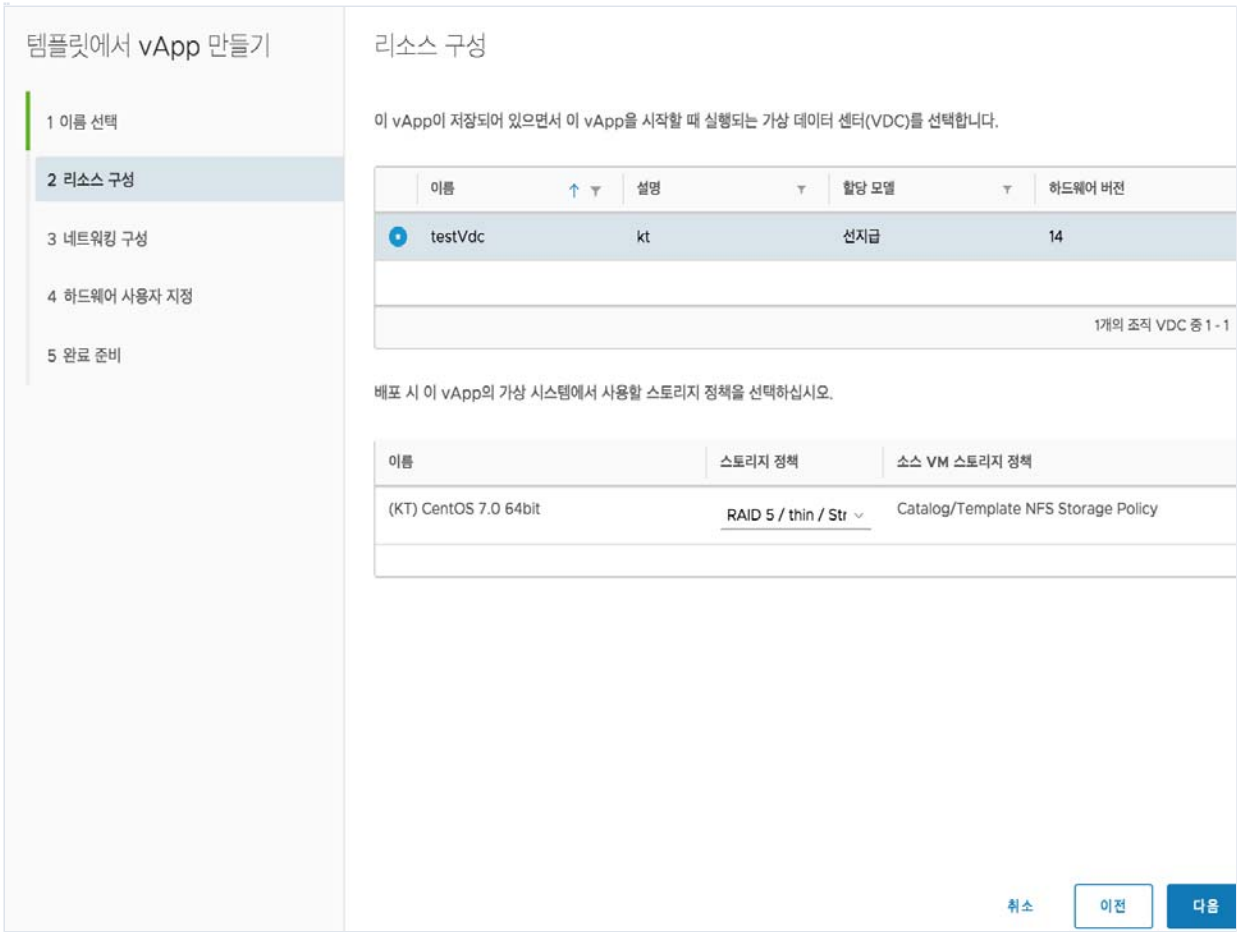
○ vApp으로 배포하려는 vApp 템플릿의 왼쪽에 있는 목록 표시줄( )을 클릭하고 vApp 만들기 를 선택합니다.



○ vApp 이름과 설명(선택 사항)을 입력합니다.
(이 vApp과 스토리지가 자동으로 중지되기 전까지 실행 가능한 시간을 지정합니다. 자동으로 중지 되길 원하지 않는다면 '만료 안 함'을 선택하세요.)

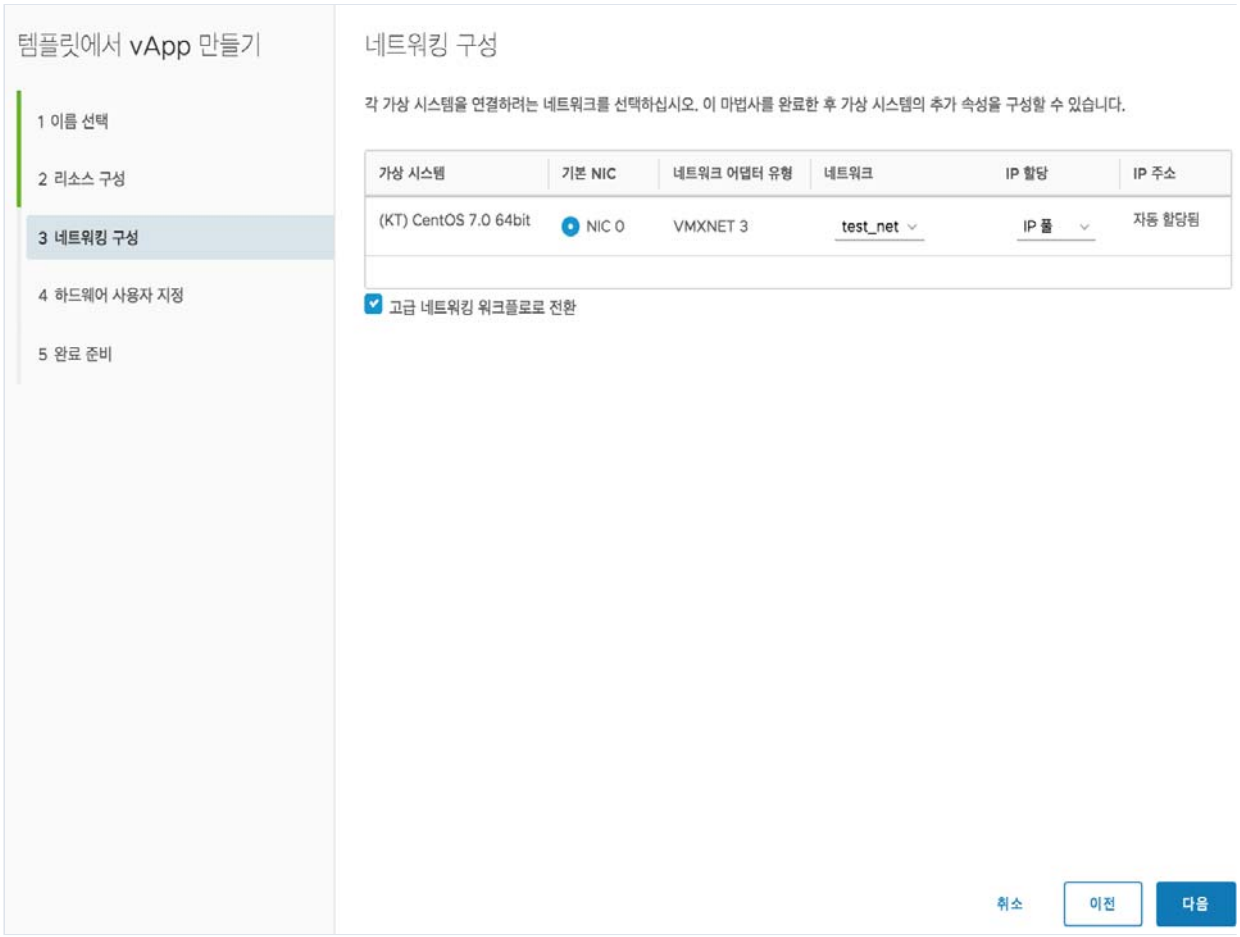


○ 스토리지 정책을 선택합니다.

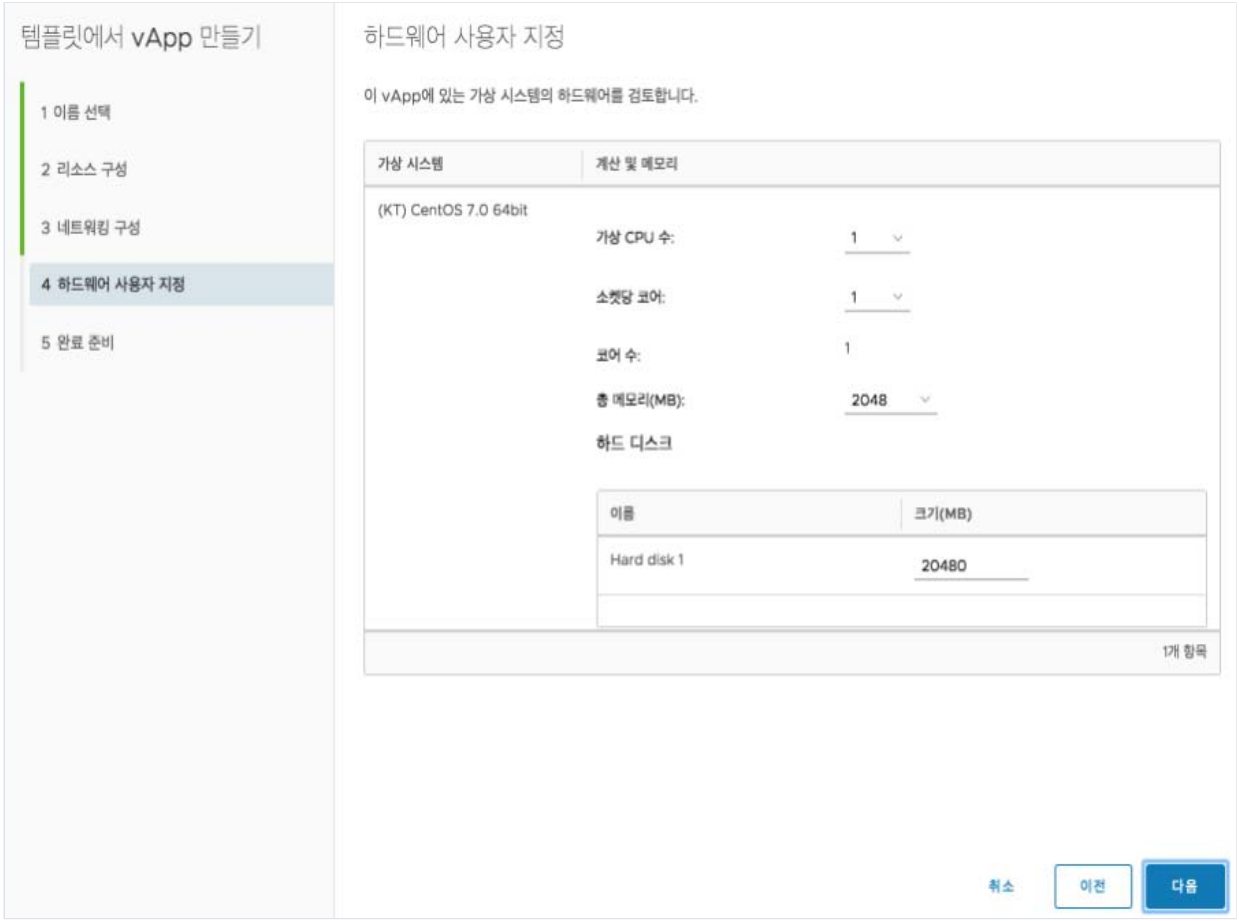


ㅇ 가상 시스템에 연결하려는 조직 네트워크를 선택하십시오.

(가상 시스템에 2개 이상의 NIC을 추가할 때는 vAPP메뉴를 통해 설정 가능합니다)



ㅇ 각vApp에 있는 가상 시스템의 하드웨어 사항을 선택합니다.



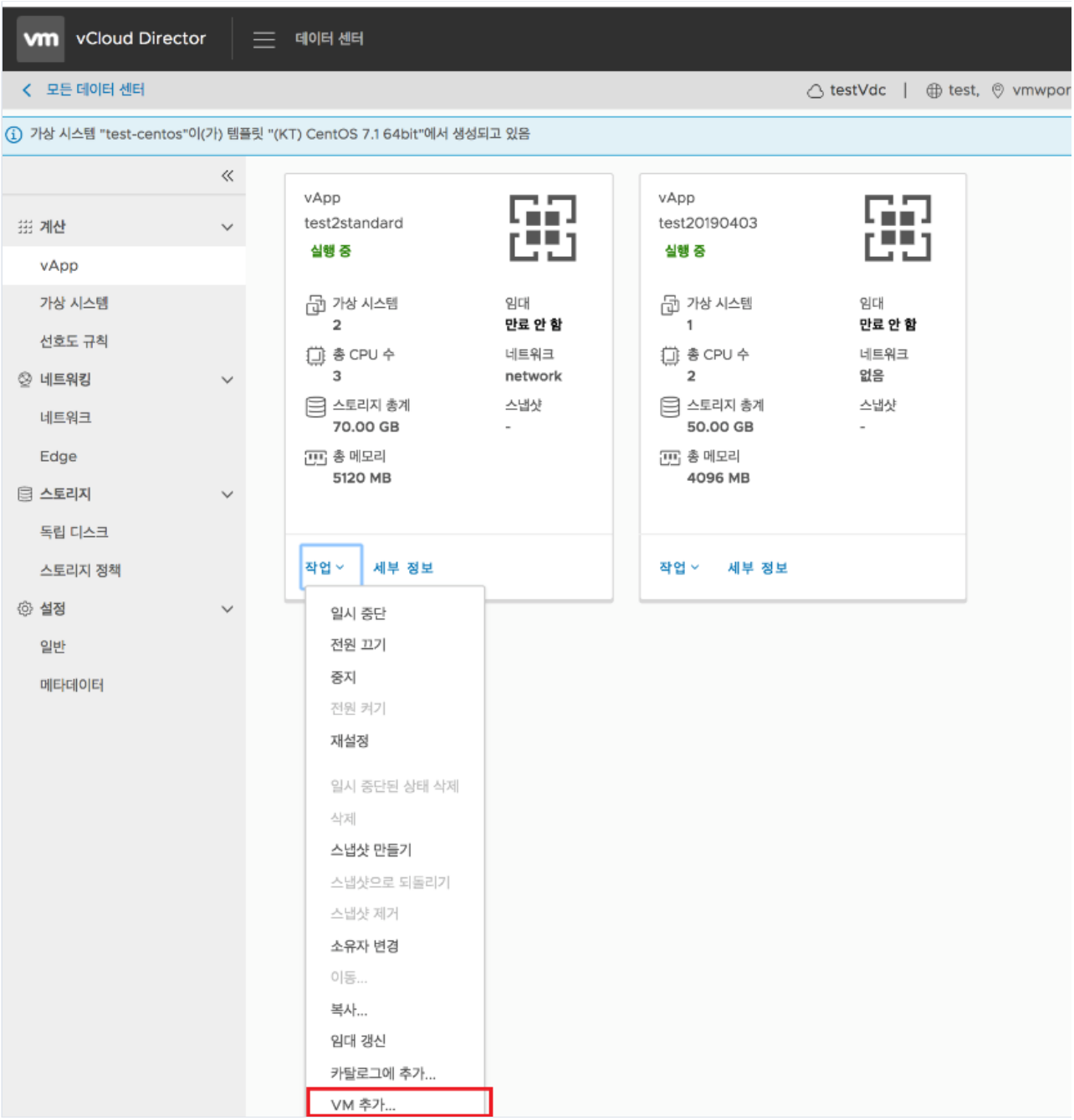
○ **확인**을 클릭합니다.

▫ vApp에 VM 추가

완성된 Vapp에 VM을 추가 합니다.

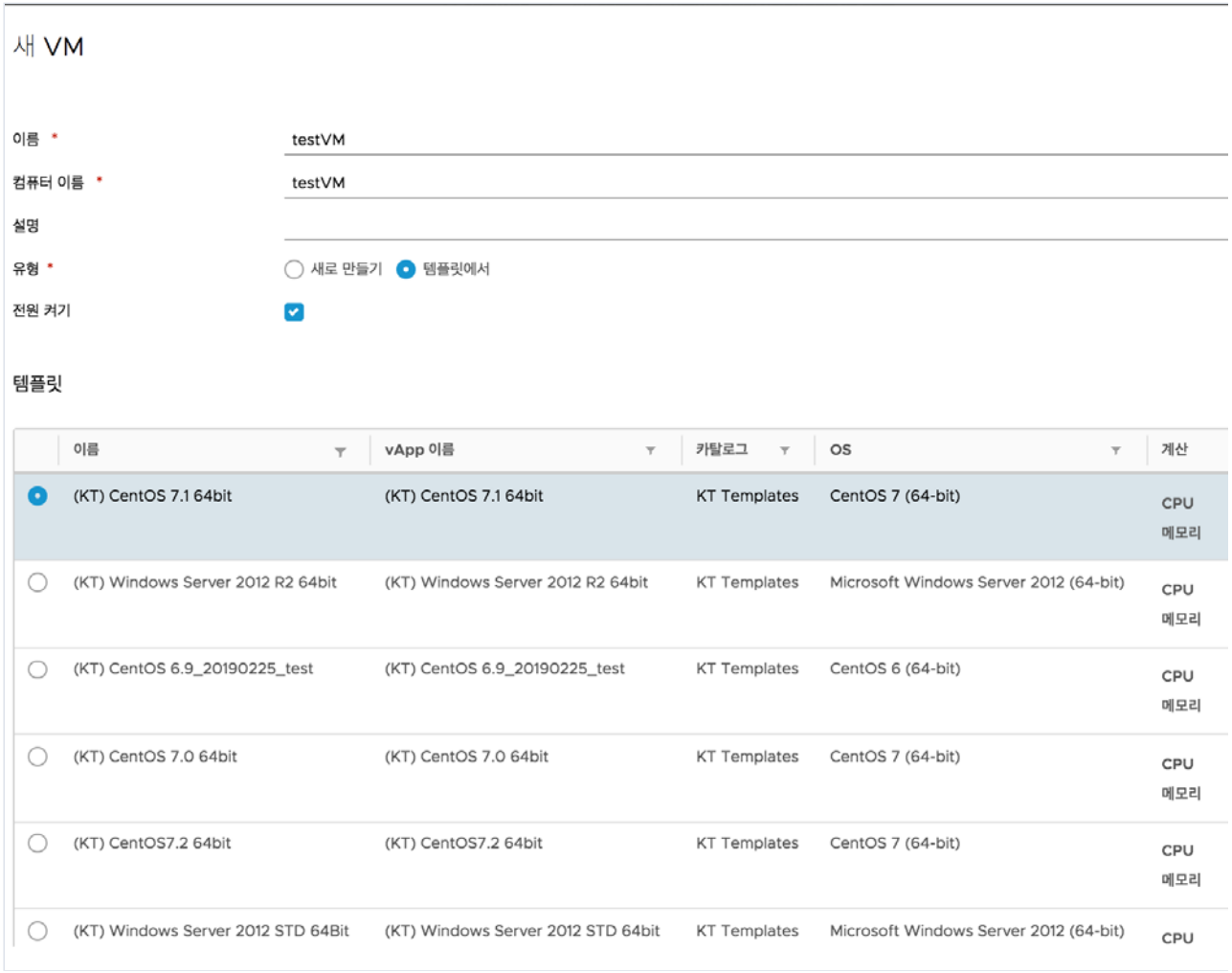
다음의 절차를 통해 생성할 수 있습니다.

- Vcloud Director의 **Vapp** 메뉴에 접속 합니다.
- Vm을 생성할 Vapp의 **작업** 버튼을 클릭 합니다.
- **VM 추가**를 선택합니다.



- **가상 시스템 추가**를 선택합니다.

- VM 설정을 작성합니다.



- 좌측 메뉴의 가상 시스템 메뉴로 이동 후 VM 생성을 확인합니다.

- Window OS VM의 경우, 정품 인증 절차가 필요합니다. 해당 항목을 참조하십시오.
- 완성된 VM에 접속하는 방법에 대해서는 Vm에 접속 항목을 참조하십시오

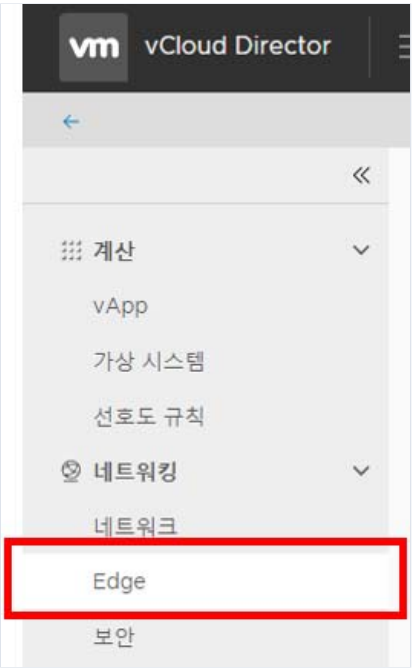
1.2.3 VMware on KT Cloud NAT/Firewall 이용방법

▫ Edge 게이트웨이 방화벽 규칙 추가

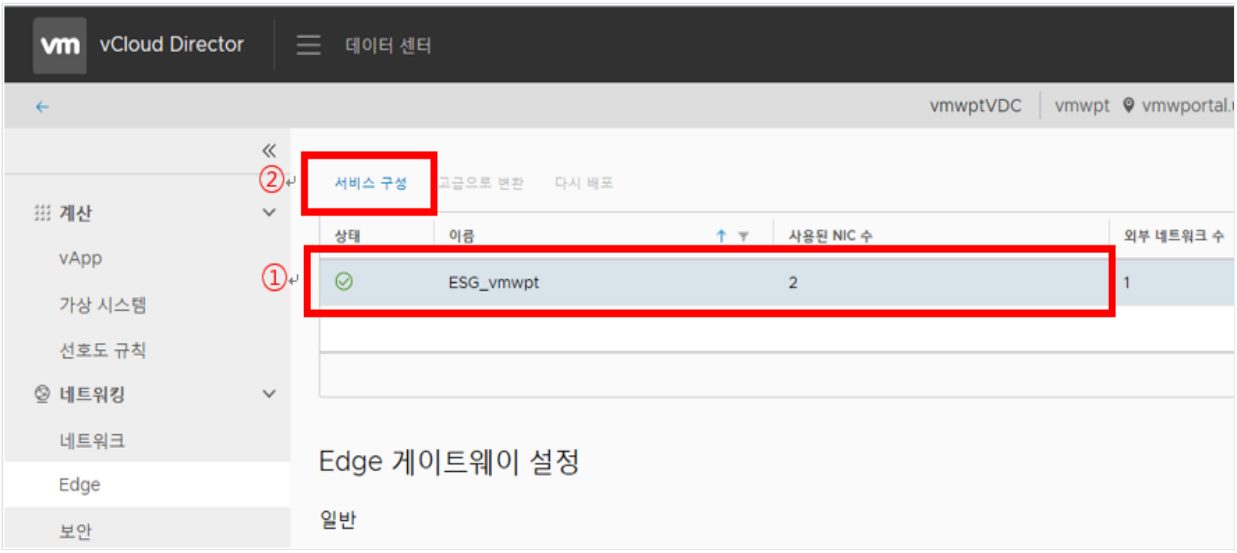
테넌트 포털에서 Edge 게이트웨이 [방화벽] 화면을 사용하여 해당 Edge 게이트웨이에 대한 방화벽 규칙을 추가합니다. 이러한 방화벽 규칙의 소스와 대상으로 여러 개의 NSX Edge 인터페이스와 여러 개의 IP 주소 그룹을 추가할 수 있습니다.

절차

- Edge 게이트웨이 서비스를 엽니다. **네트워킹** > **Edge**로 이동합니다.



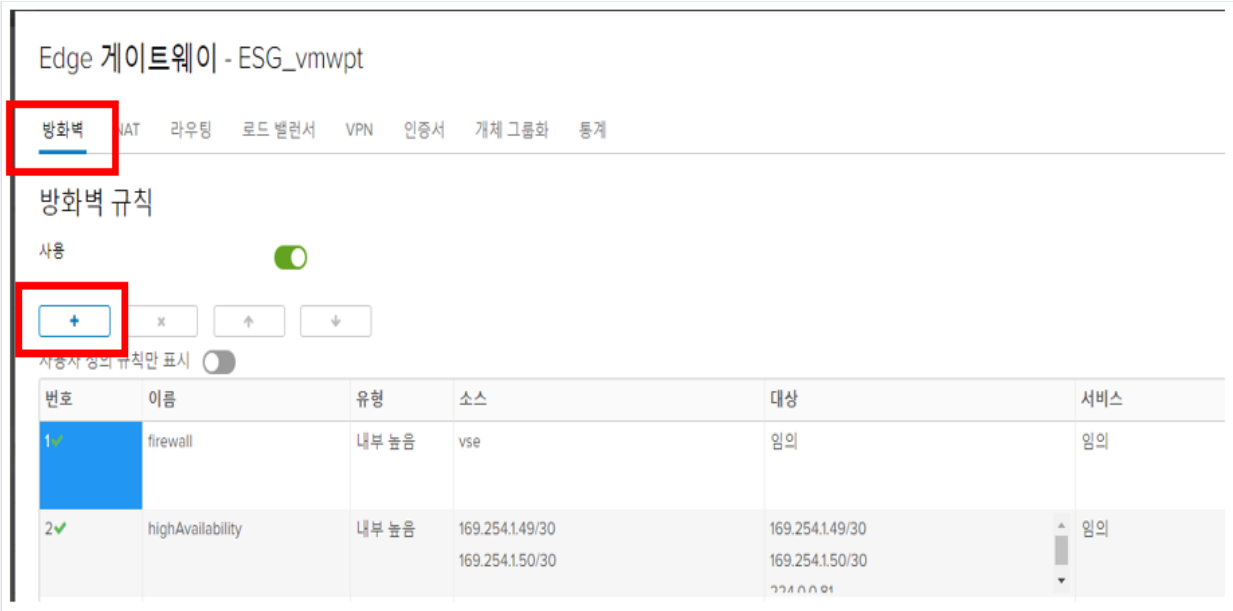
편집할 Edge 게이트웨이를 선택하고 **서비스 구성**을 클릭합니다.



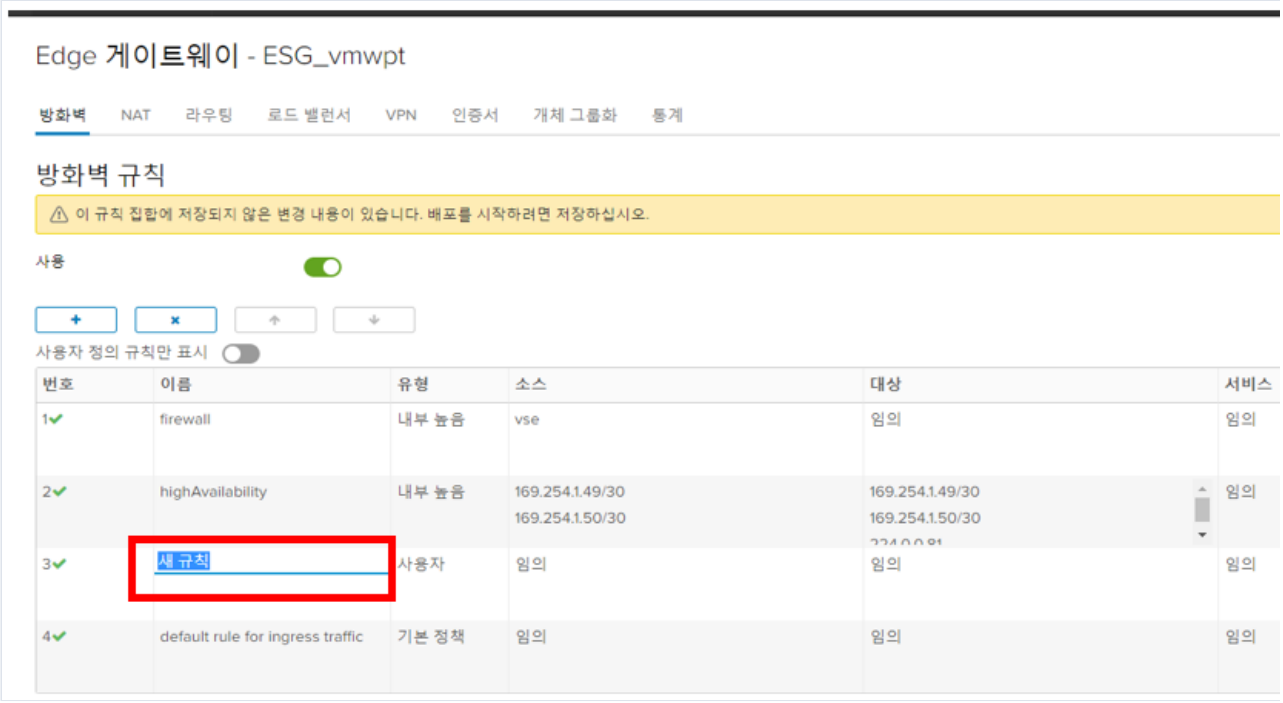
○ [방화벽 규칙] 화면이 표시되지 않으면 **방화벽** 탭을 클릭합니다.

○ 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.



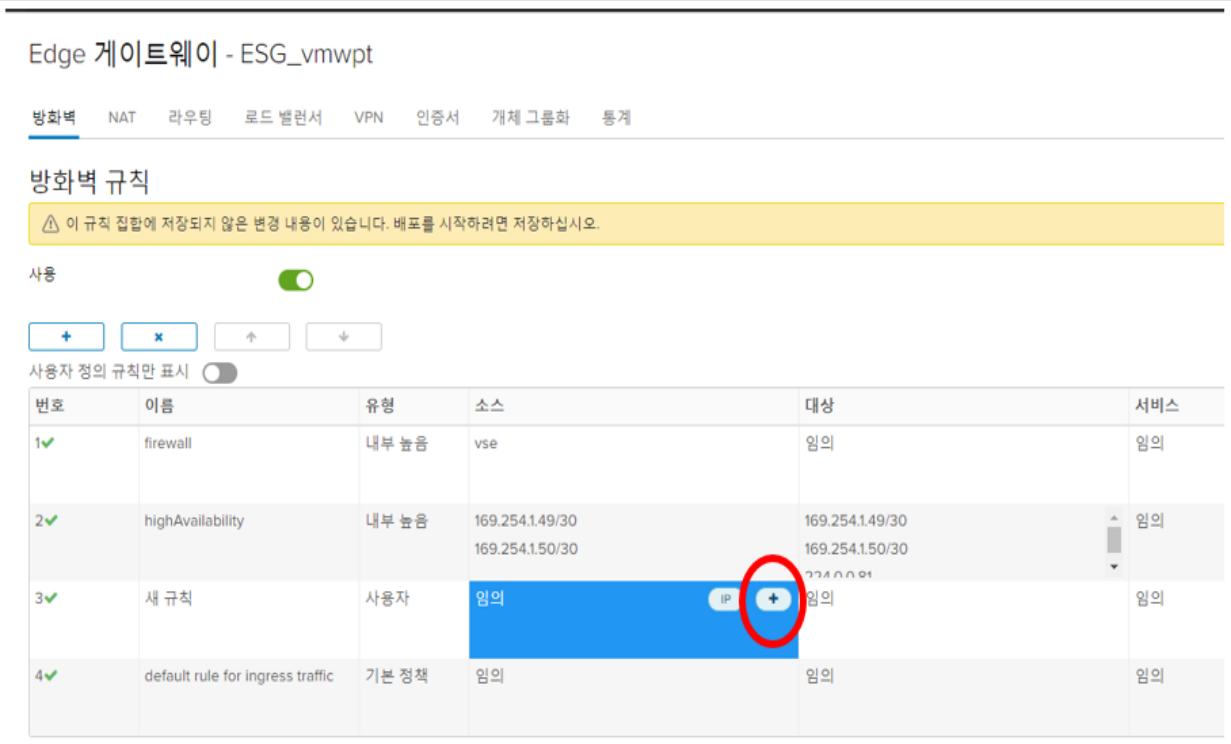
○ **이름** 셀을 클릭하고 이름을 입력합니다.



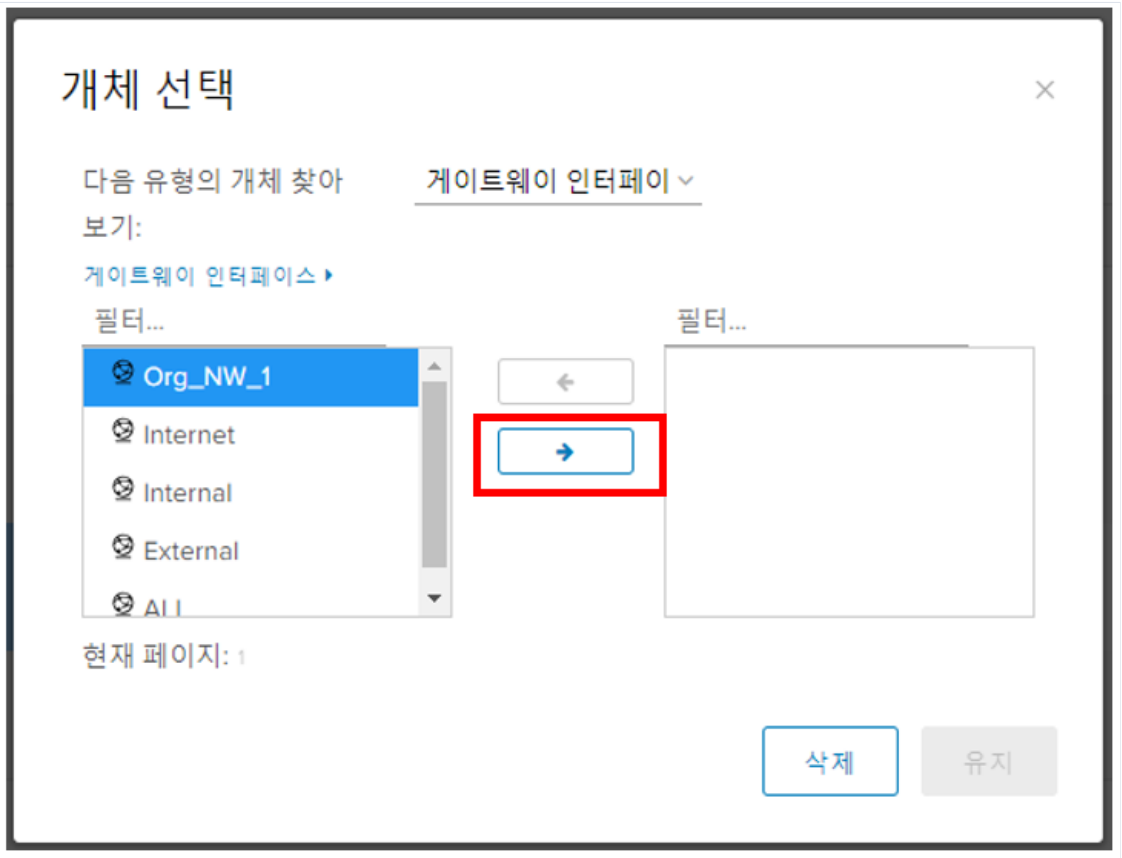
○ **소스** 셀을 클릭하고 이제 표시되는 아이콘을 사용하여 규칙에 추가할 소스를 선택합니다.

옵션	설명
IP 아이콘 클릭	사용할 소스 값을 입력합니다. 올바른 값은 IP 주소, CIDR, IP 범위 또는 키워드 **any**입니 게이트웨이 방화벽은 IPv4 및 IPv6 형식을 모두 지원합니다.
+ 아이콘 클릭	특정 IP 주소가 아닌 개체로 소스를 지정하려면 + 아이콘을 사용합니다. - **개체 선택** 창을 사용하여 선택 사항과 일치하는 개체를 추가하고 **유지**를 클릭하 체를 규칙에 추가합니다. - 규칙에서 소스를 제외하려면 **개체 선택** 창을 사용하여 이 규칙에 소스를 추가한 전환 아이콘을 선택하여 이 규칙에서 해당 소스를 제외합니다.

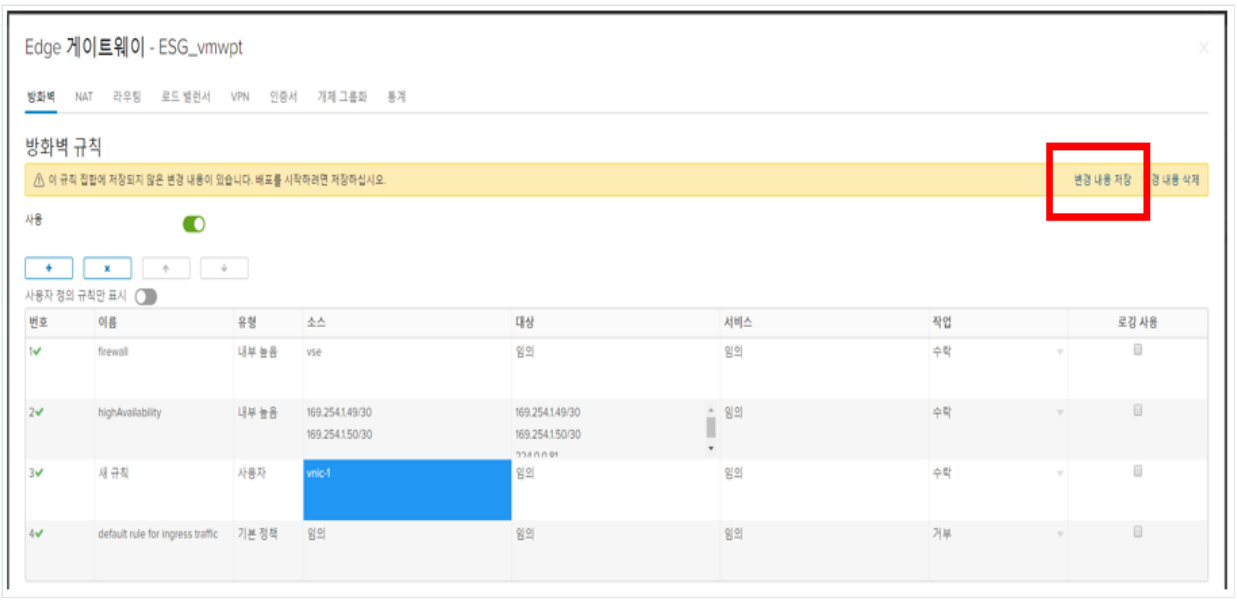
	소스에서 제외 전환을 선택하면 해당 소스를 제외한 모든 소스에서 들어오는 모 든 트이 적용됩니다. 제외 전환을 선택하지 않으면 **개체 선택** 창에 서 지정한 소스에서 들어픽에 규칙이 적용됩니다.



- 소스를 적용할 Edge 게이트웨이 인터페이스를 선택하고, 유지 버튼을 클릭합니다.



○ **변경 내용 저장**을 클릭합니다. 저장 작업을 완료하는 데 몇 분이 걸릴 수 있습니다.



▫ Edge 게이트웨이에서 SNAT 또는 DNAT 규칙 추가

vCloud Director 조직 가상 데이터 센터의 Edge 게이트웨이에서 SNAT(소스 NAT) 규칙을 만들어 사설 소스 IP 주소를 공인 IP 주소로 변경할 수 있습니다.
DNAT(대상 NAT) 규칙은 공인 IP 주소를 사설IP 주소로 변경할 수 있습니다.
NAT 규칙을 만들 때 다음 형식을 사용하여 원래 IP 주소와 변환된 IP 주소를 지정할 수 있습니다.

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

vCloud Director 환경의 Edge 게이트웨이에 SNAT 또는 DNAT 규칙을 구성할 때는 항상 조직 가상 데이터 센터의 관점에서 규칙을 구성해야 합니다. SNAT 규칙은 조직 가상 데이터 센터 네트워크에 서 외부 네트워크 또는 다른 조직 가상 데이터 센터 네트워크로 전송되는 패킷의 소스 IP 주소를 변환 합니다. DNAT 규칙은 외부 네트워크 또는 다른 조직 가상 데이터 센터 네트워크에서 들어오는 조직 가상 데이터 센터 네트워크에서 수신한 패

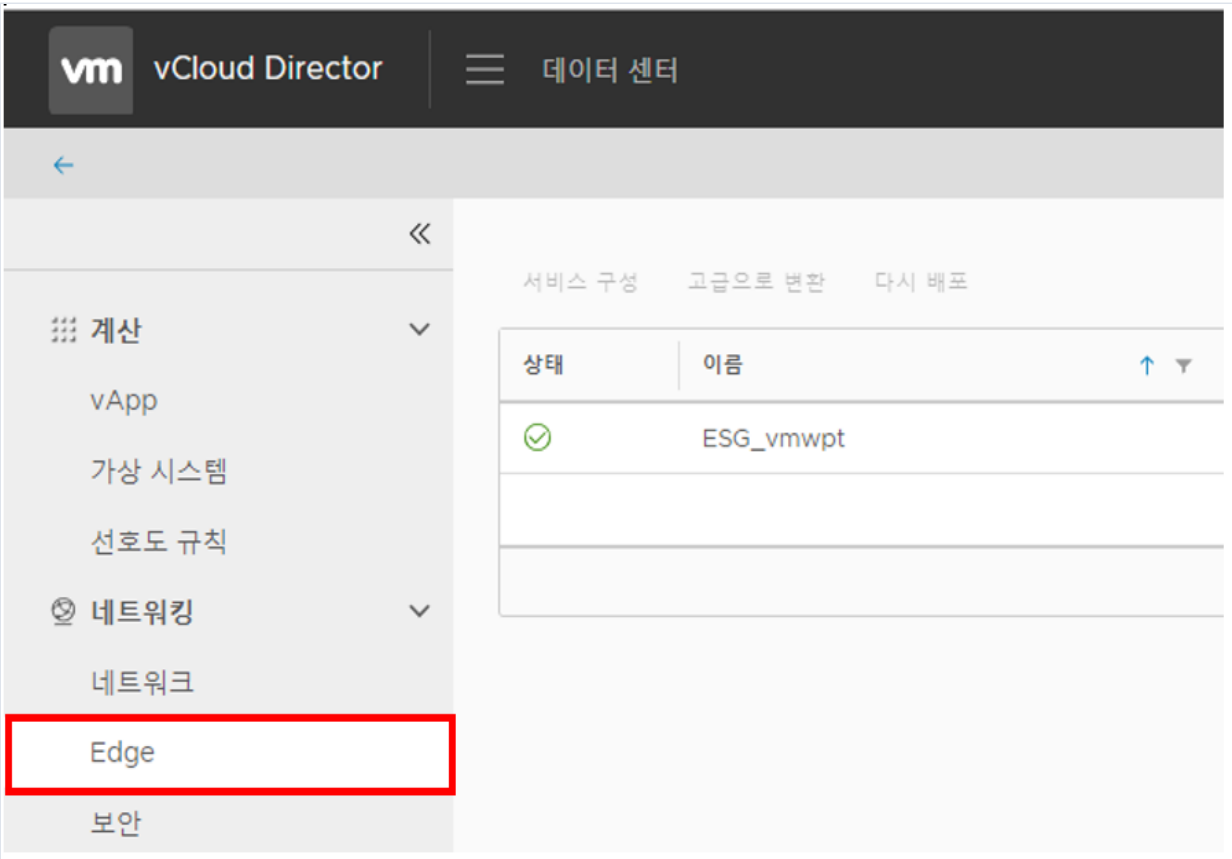
킷의 IP 주소(필요한 경우 포트 포함)를 변환합니다.

사전 요구 사항

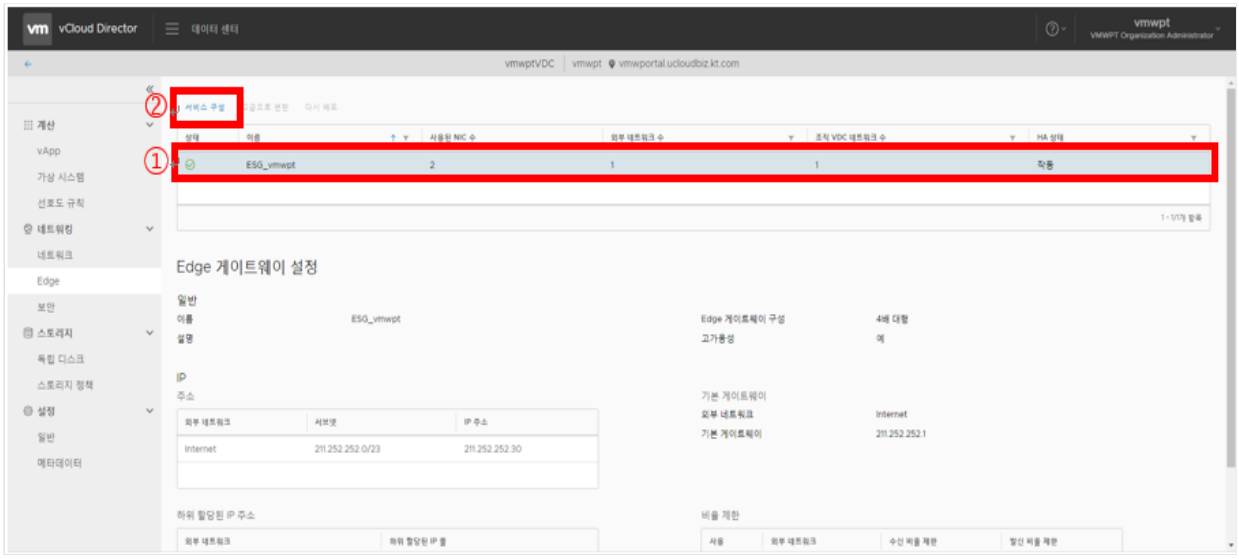
규칙을 추가할 Edge 게이트웨이 인터페이스에 공개 IP 주소가 추가된 상태여야 합니다. DNAT 규칙 의 경우 원래(공용) IP 주소가 Edge 게이트웨이 인터페이스에 추가되어 있어야 하고 SNAT 규칙의 경우 변환된(공용) IP 주소가 인터페이스에 추가되어 있어야 합니다.
vCloud Director 테넌트 포털을 사용하여 Edge 게이트웨이 서비스 작업을 수행하려면 Edge 게이 트웨이를 고급 Edge 게이트웨이로 변환해야 합니다. vCloud Director 웹 콘솔 또는 테넌트 포털에 서 Edge 게이트웨이에 이 작업을 수행할 수 있습니다.

절차

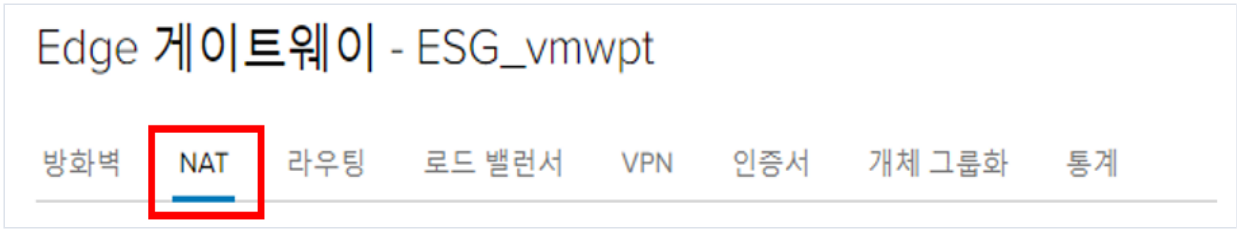
- Edge 게이트웨이 서비스를 엽니다.
  - 네트워킹 > Edge로 이동합니다.



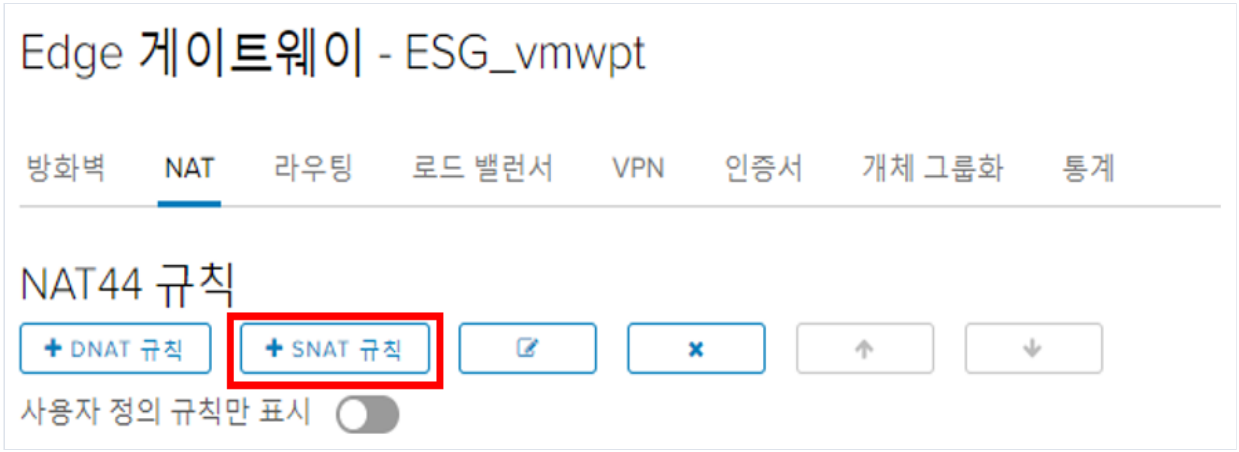
- 편집할 Edge 게이트웨이를 선택하고 서비스 구성을 클릭합니다.



○ **NAT**를 클릭하여 [NAT 규칙] 화면을 표시합니다.



○ **SNAT 규칙**을 클릭합니다.



○ (참고) 대상 NAT 규칙(외부에서 내부로 들어옴)을 구성합니다.

옵션	설명
적용 대상	규칙을 적용할 인터페이스를 선택합니다.
원래 IP/범위	필요한 IP 주소를 입력합니다. 이 주소는 DNAT 규칙을 구성하는 Edge 게이트웨이의 공개 IP 주소여야 합니다. 검사 중인 패서 이 IP 주소 또는 범위는 패킷의 대상 IP 주소로 나타나는 주소 또는 범위입니다. 이러한 패상 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 임의로 설정된 경우에는 포트 또는 포트 범위를 선택할 수 없습니다.

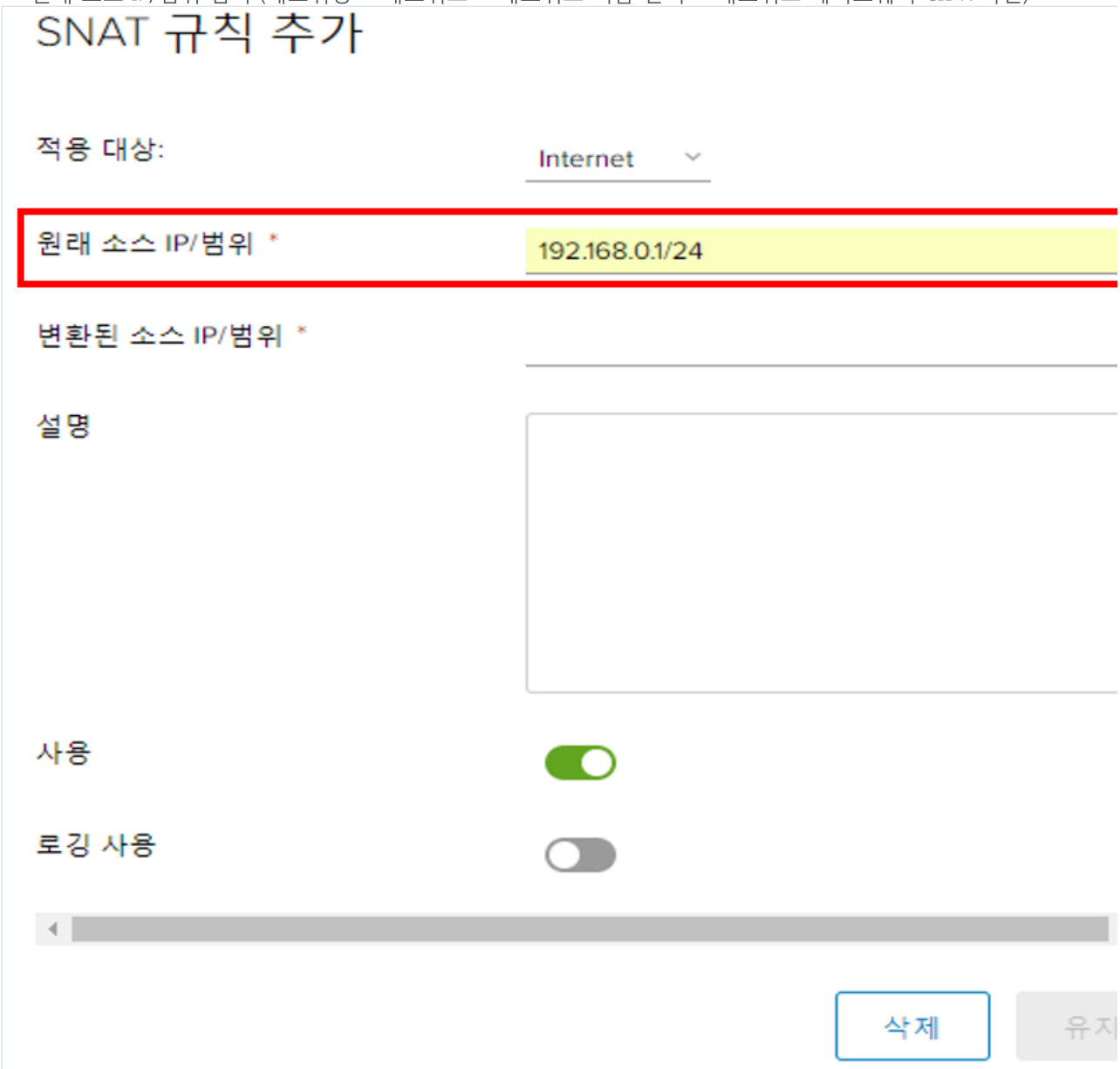
옵션	설명
ICMP 유형	**ICMP**(디바이스 간 오류 정보 전달에 사용되는 오류 보고 및 진단 유틸리티)를 **프로토콜**로 선택하는 경우 드롭다운 메뉴에서 **ICMP 유형**을 선택합니다. ICMP 메시지는 유형 필드로 식별됩니다. 기본적으로 ICMP 유형은 [임의]로 설정됩니다.
변환된 IP/범위	인바운드 패킷의 대상 주소를 변환할 IP 주소 또는 IP 주소 범위를 입력합니다. 이러한 주소는 외부 네트워크의 트래픽을 수신할 수 있도록 DNAT를 구성하는 하나 이상의 가상 시스템에 대한 IP 주소입니다.
변환된 포트	(선택 사항) 인바운드 트래픽이 내부 네트워크의 가상 시스템에서 연결하는 포트 또는 포트 범위를 선택합니다. 이러한 포트는 DNAT 규칙이 가상 시스템에 대한 인바운드 패킷에 대해 변환하는 포트입니다.
설명	(선택 사항) 이 규칙의 작업을 식별하는 데 도움이 되는 설명을 입력합니다.
사용	이 규칙을 사용하도록 설정하려면 토글을 켭니다.
로깅 사용	이 규칙에 의해 수행된 주소 변환을 기록하려면 토글을 켭니다.

○ (참고) 소스 NAT 규칙(내부에서 외부로 나감)을 구성합니다.

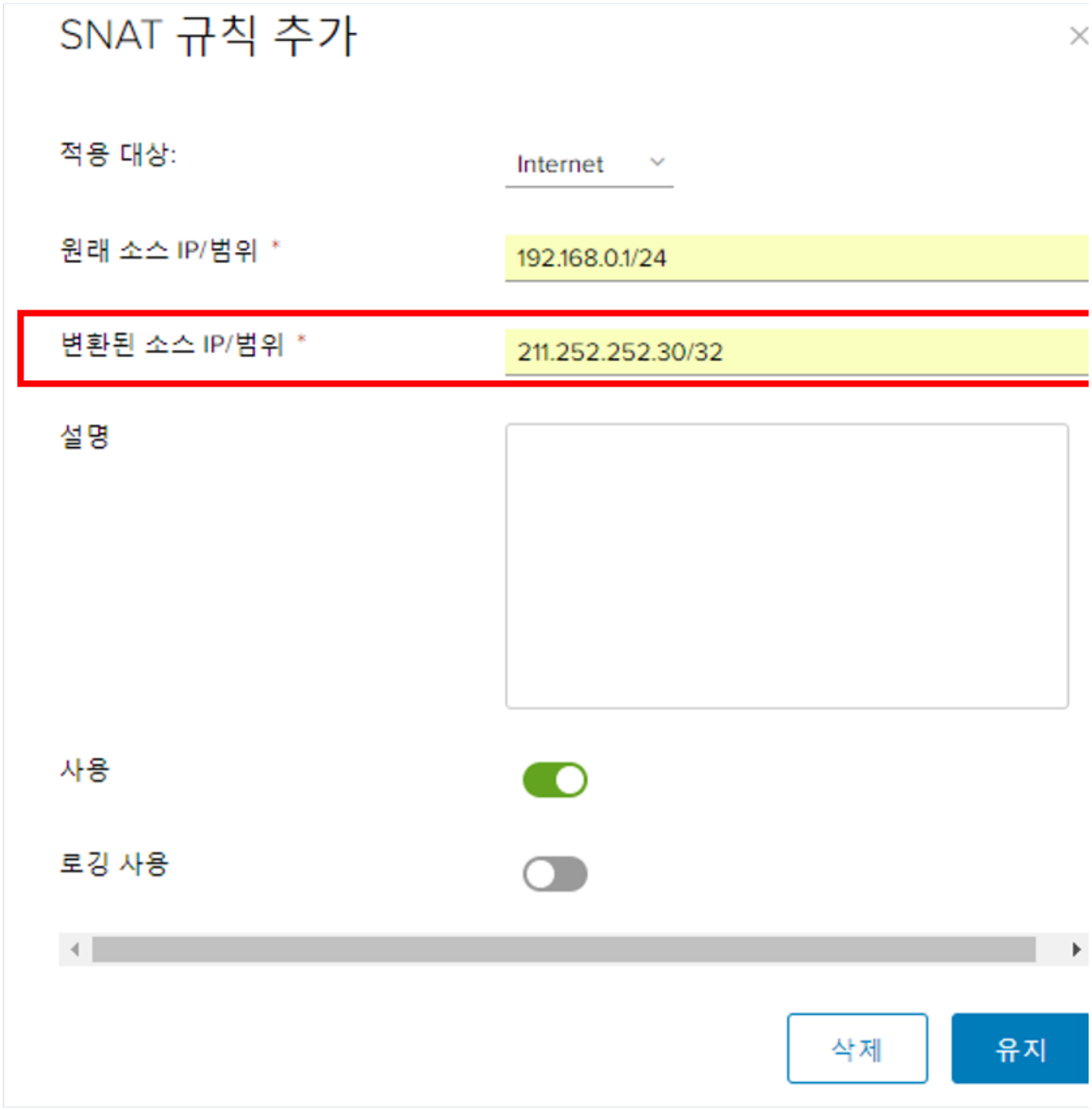
옵션	설명
적용 대상	규칙을 적용할 인터페이스를 선택합니다.
원래 소스 IP/범위	이 규칙에 적용할 원래 IP 주소 또는 IP 주소 범위를 입력합니다.

	이러한 주소는 외부 네트워크로 트래픽을 전송할 수 있도록 SNAT 규칙을 구성하는 하나 상의 가상 시스템에 대한 IP 주소입니다.
변환된 소스 IP/범위	필요한 IP 주소를 입력합니다. 이 주소는 항상 SNAT 규칙을 구성하는 게이트웨이의 공개 IP 주소입니다. 외부 네트워크 트래픽을 전송할 때 아웃바운드 패킷의 소스 주소(가상 시스템)를 변환할 IP 주소를 지정 다.
설명	(선택 사항) 이 규칙의 작업을 식별하는 데 도움이 되는 설명을 입력합니다.
사용	이 규칙을 사용하도록 설정하려면 토글을 켭니다.
로깅 사용	이 규칙에 의해 수행된 주소 변환을 기록하려면 토글을 켭니다.

○ 원래 소스 IP/범위 입력 (네트워킹 > 네트워크 > 네트워크 이름 선택 > 네트워크 게이트웨이 CIDR 확인)



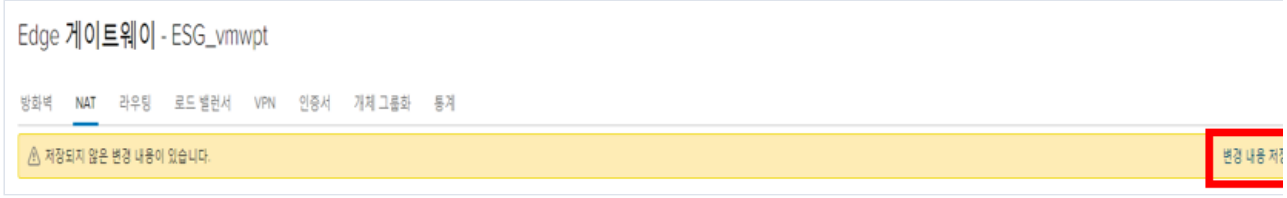
○ 변환된 소스 IP범위 입력 (네트워킹 > Edge > Edge 이름 선택 > Edge 게이트 웨이 설정 > IP 주소 확인)



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

○ 추가 규칙을 구성하려면 단계를 반복합니다.

○ **변경 내용 저장**을 클릭하여 시스템에 규칙을 저장합니다.



1.2.4 vCloud director 또는 콘솔을 통해VM에 접속 및 기본 설정

사전 요구 사항

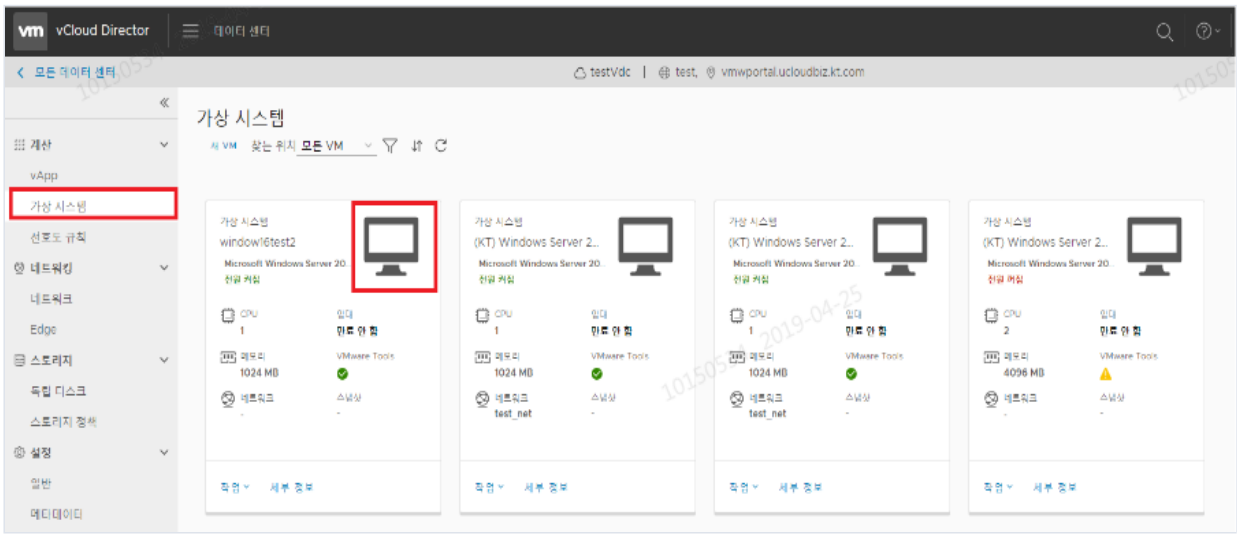
○ 접속 가능한 VM이 생성되어있어야 합니다.

(VM 생성에 관해서는 VM생성법 항목을 참조하십시오.)

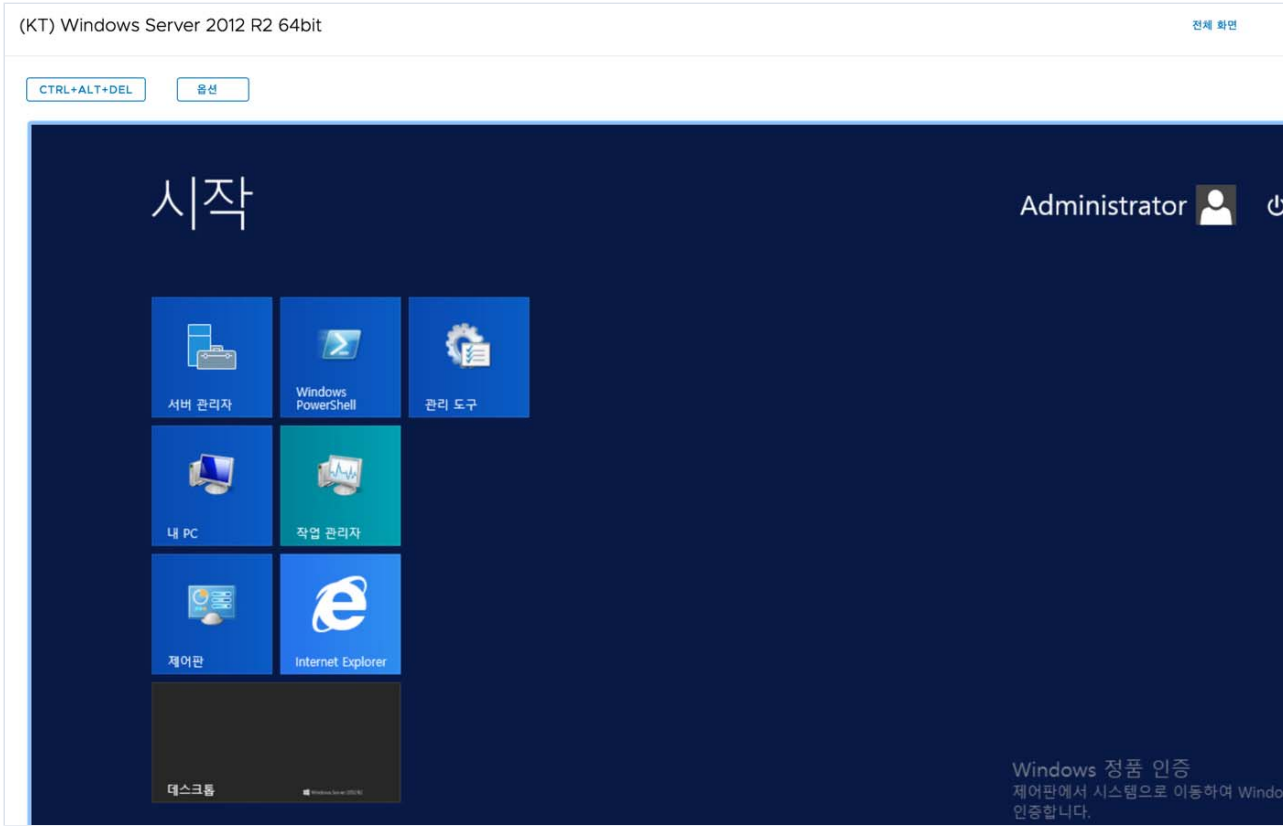
◘ vCloud director을 통해 접속

○ 가상 시스템 메뉴로 접속하고, 접속할 VM의 모니터 버튼을 클릭합니다.

(VM 전원이 켜져있어야 합니다.)



○ VM 데스크톱에 접속됩니다.



◘ 정품 인증 (Window OS)

윈도우 기반 VM은 정품 인증을 진행해야 합니다.

◘ 초기 계정 설정 (Cent OS)

centOS 기반 템플릿으로 생성된 VM은 다음과 같은 초기 계정을 가집니다.

ID : root / PW: password

초기 접속 이후 VM 내의 명령어를 통해 루트 계정 외의 다른 계정을 생성하거나, 루트 계정의 비밀번호를 변경하는 것을 권장합니다.

1. ID: root / PW : password 의 루트 계정으로 VM에 접속 합니다.

2. 명령어를 통해 새 계정을 생성합니다.

```
useradd testuser
```

3. 생성한 계정의 패스워드를 변경합니다. (예시 : testPassword@)

```
echo 'testPassword@' | passwd --stdin testuser
```

4. 기본 계정(root)의 경우 sudo passwd 명령어를 통해 변경하실 수 있습니다.

```
sudo password
```

1.3 VMware on KT Cloud Edge 이용방법

메뉴얼 구성

1.3.1 VMware on KT Cloud Edge 로드 밸런서 설정

- 로드밸런서 구성 탭 개요
- 애플리케이션 프로파일 생성
- 서비스 모니터 생성 로드
- 밸런싱을 위한 서버 풀 추가
- 애플리케이션 규칙 추가
- 가상 서버 추가

1.3.2 VMware on KT Cloud Edge IPsec-VPN 설정

- IPSec VPN 구성

1.3.1 VMware on KT Cloud Edge 로드 밸런서 설정

NSX Advanced Networking 로드 밸런서를 사용하면 네트워크 트래픽이 특정 대상에 대한 여러 경로를 추적할 수 있습니다.
로드 분산이 사용자에게 투명하도록 여러 서버에 들어오는 서비스 요청을 균등하게 분배합니다.
NSX Edge Gateway 로드 밸런싱을 사용하면 최적의 리소스 활용, 처리량 극대화, 응답 시간 최소화, 과부하 방지 등의 효과를 얻을 수 있습니다.
NSX Edge는 레이어7까지 로드 밸런싱을 제공합니다.
동작 원리에 관한 더 자세한 사항은 VPC vCloud Director 공급사 메뉴얼을 참조해 주십시오.

다음은 NSX Advanced Networking Edge에서 로드 균형 조정을 사용하는 방법에 대한 세부 정보입니다.

ㅁ 로드 밸런서 구성 탭 개요

ㅇ 글로벌 구성: 서비스 워크로드에 대해 작동하는 로드 균형 조정 기능을 얻는 데 필요한 세부 정보를 구성할 수 있습니다.

ㅇ 애플리케이션 프로파일: 애플리케이션 프로파일을 만들어 특정 유형의 네트워크 트래픽의 동작을 정의합니다.
프로파일을 구성한 후에는 프로파일을 가상 서버와 연관시킵니다.
그런 다음 가상 서버는 프로파일에 지정된 값에 따라 트래픽을 처리합니다.
프로파일을 사용하면 네트워크 트래픽 관리에 대한 제어가 향상되고 트래픽 관리 작업을 보다 쉽고 효율적으로 수행할 수 있습니다.

ㅇ 서비스 모니터링: 서비스 모니터를 작성하여 특정 유형의 네트워크 트래픽에 대한 상태 점검 매개 변수를 정의합니다.
서비스 모니터를 풀과 연관시키면 서비스 모니터 매개 변수에 따라 풀 구성원이 모니터됩니다.

ㅇ 풀: 백엔드 서버를 유연하고 효율적으로 관리하고 공유하기 위해 서버 풀을 추가할 수 있습니다.
풀은 로드 밸런서 배포 방법을 관리하며 상태 확인 매개 변수를 위해 풀에 서비스 모니터가 연결되어 있습니다.

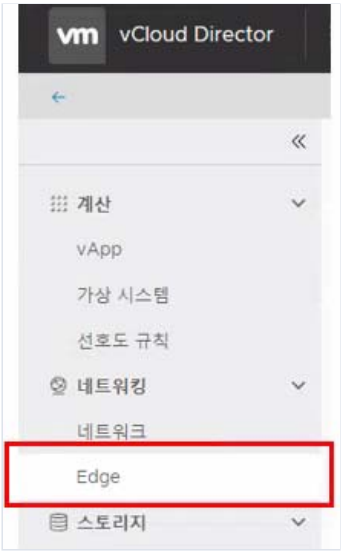
ㅇ 애플리케이션 규칙: 애플리케이션 규칙을 작성하여 IP 애플리케이션 트래픽을 직접 조작하고 관리할 수 있습니다.

ㅇ 가상 서버: NSX Edge 내부 또는 업 링크 인터페이스를 추가하여 로드 밸런싱 서비스의 가상 서버로 작동합니다.

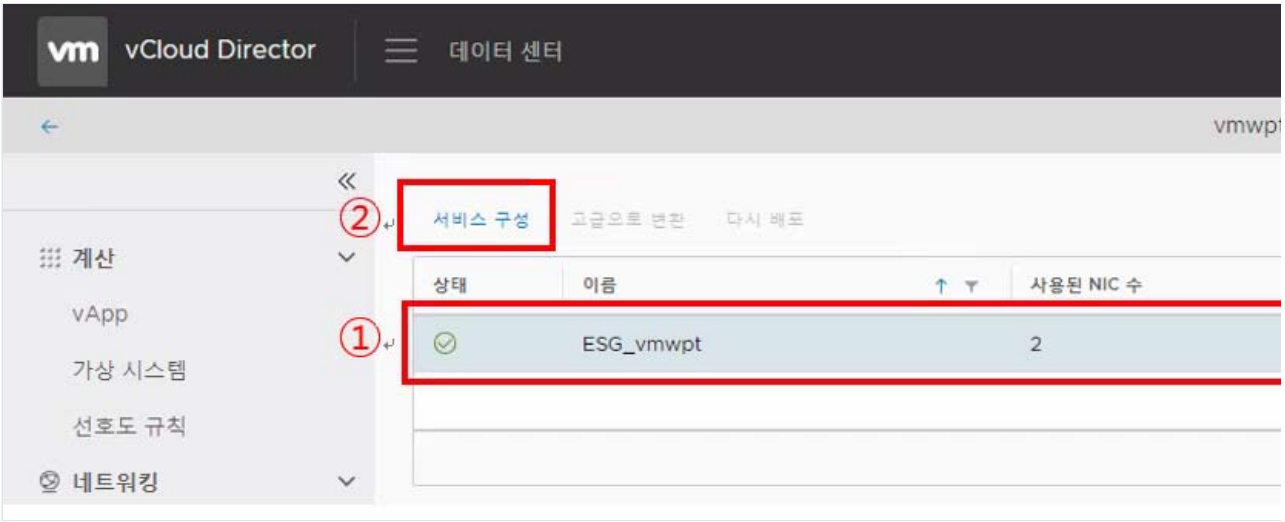
절차

ㅇ Edge 게이트웨이 서비스를 엽니다.

- **네트워킹** > **Edge**로 이동합니다.



- 편집할 Edge 게이트웨이를 선택하고 **서비스 구성**을 클릭합니다.

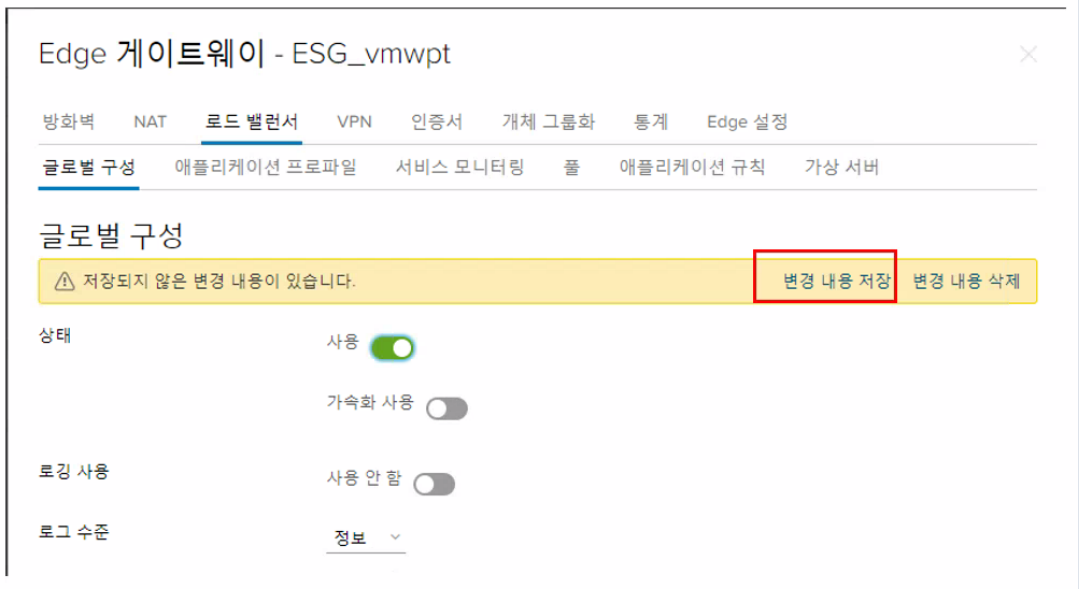


○ **로드 밸런서** > **글로벌 구성**으로 이동합니다.

○ 사용하도록 설정할 옵션을 선택합니다.

옵션	작업
상태	토글 아이콘을 클릭하여 로드 밸런서를 사용하도록 설정합니다. 로드 밸런서가 L7 엔진보다 빠른 L4 엔진을 사용하도록 구성하려면 **가속화 사용**을 설정합니다. L4 TCP VIP가 Edge 게이트웨이 방화벽보다 먼저 처리되므로 방화벽 허용 규칙이 필요하지 않습니다.
	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.
로깅 사용	Edge 게이트웨이 로드 밸런서가 트래픽 로그를 수집할 수 있도록 로깅을 사용하도록 설정합니다.
로그 수준	로그에 수집될 이벤트의 심각도 선택합니다.

○ **변경 내용 저장**을 클릭합니다.



저장 작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

ㅁ 애플리케이션 프로파일 만들기

애플리케이션 프로파일은 특정 유형의 네트워크 트래픽에 대한 로드 밸런서의 동작을 정의합니다.
프로 파일을 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.

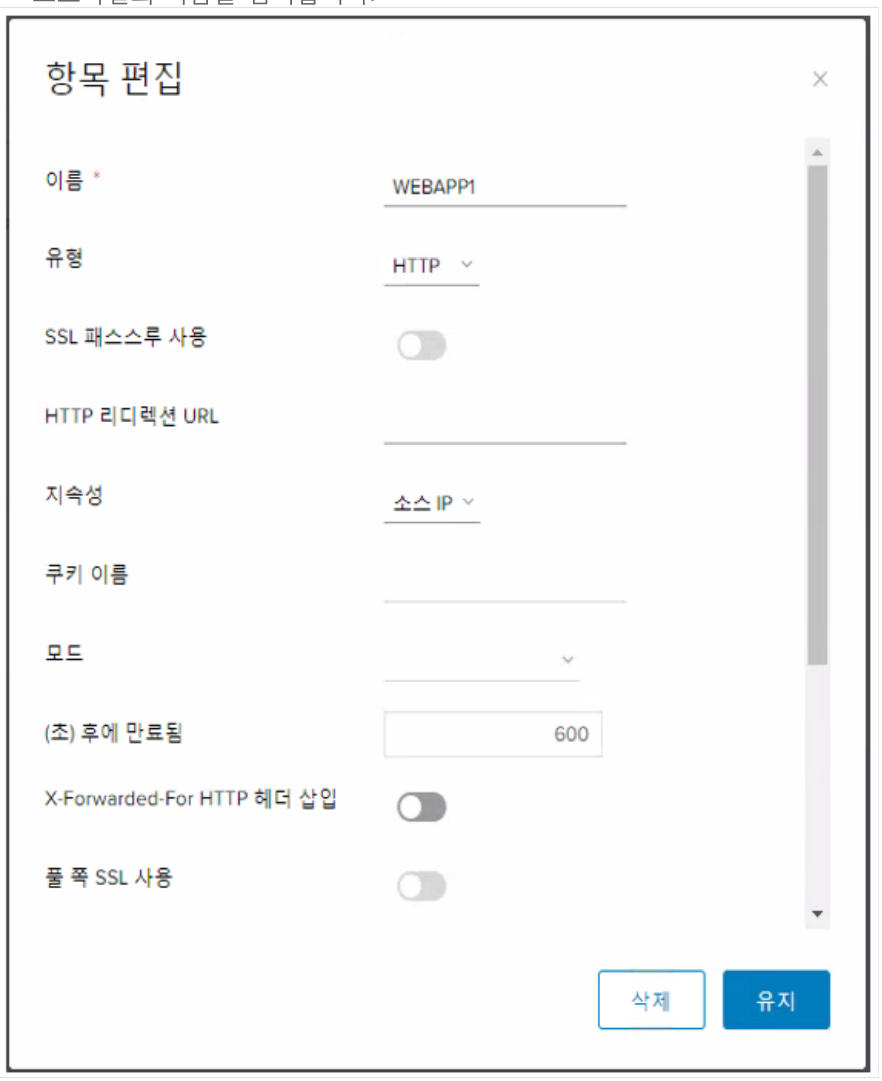
- 클라이언트 -> HTTPS -> LB(SSL 종료) -> HTTP -> 서버
- 클라이언트 -> HTTPS -> LB(SSL 종료) -> HTTPS -> 서버
- 클라이언트 -> HTTPS -> LB(SSL 패스스루) -> HTTPS -> 서버
- 클라이언트 -> HTTP-> LB -> HTTP -> 서버

절차

- **로드 밸런서 > 애플리케이션 프로파일**로 이동합니다.

- **추가** (+) 버튼을 클릭합니다.

○ 프로파일의 이름을 입력합니다.



○ 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 입력 합니다.

옵션	**설명**
지속성	프로파일에 대한 지속성 메커니즘을 지정합니다. 지속성은 세션 데이터(예: 클라이언트 요청에 서비스를 제공한 특정 풀 구성원)을 추적하고 저장합니다. 따라서 클라이언트 요청이 세션 수명 전체 또는 후속 세션에서 동일한 풀 구성원에 전달될 수 있습니다. 옵션은 다음과 같습니다. **- 소스 IP** 소스 IP 지속성은 소스 IP 주소를 기반으로 세션을 추적합니다. 클라이언트가 소스 주소 선호도 지속성을 지원하는 가상 서버에 대한 연결을 요청할 경 우 로드 밸런서는 해당 클라이언트가 이전에 연결한 적이 있는지 여부를 확 인한 후 연결한 적이 있으면 클라이언트를 동일한 풀 구성원에 할당합니다. **- MSRDP** (TCP만 해당) MSRDP(Microsoft 원격 데스크톱 프로토콜) 지속성은 Microsoft RDP(원격 데스크톱 프로토콜) 서비스를 실행하는 서버와 Windows 클라이언트 간에 영구 세션을 유지합니다. MSRDP 지속성 사 용에 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.
쿠키 이름	(HTTP 및 HTTPS) 지속성 메커니즘으로 **쿠키**를 지정한 경우 쿠키 이름을 입 력합니다. 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.
모드	쿠키를 삽입할 때 사용할 모드를 선택합니다. 다음 모드가 지원됩니다. **- 삽입** 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. **- 접두사** 클라이언트가 둘 이상의 쿠키를 지원하지 않는 경우 이 옵션을 선택합니다.
	참고 모든 브라우저는 다중 쿠키를 수락합니다. 그러나 단일 쿠키만 지원 하는 독점적 클라이

	언트 기반의 독점적 애플리케이션의 경우는 다릅니다. 웹 서버는 평소대로 쿠키를 전송합니다. Edge 게이트웨이는 쿠키 정보를 서버 쿠키 값에 접두사로 주입합니다. 이 추가 쿠키 정보는 Edge 게이트웨이가 쿠키 정보를 서버로 보낼 때 제거됩니다. **- 애플리케이션 세션** 이 옵션의 경우 서버가 쿠키를 전송하지 않고 사용자 세션 정보를 URL로 전송합니다. 예를 들어 http://example.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD URL로 전송합니다. 여기서 jsessionid가 사용자 세션 정보이며 지속성을 위해 사용됩니다. 애플리케이션 세션 지속성 테이블은 문제 해결용으로 확 인할 수 없습니다.
(초) 후에 만료됨	지속성을 유효한 상태로 유지할 시간(초)을 입력합니다. 1~86400 범위의 양 수여야 합니다. **참고** TCP 소스 IP 지속성을 사용하는 L7 로드 밸런싱의 경우 새 TCP 연결 이 일정 기간 동안 생성되지 않으면 기존 연결이 유지되는 경우에도 지속성 항 목이 시간 초과됩니다.

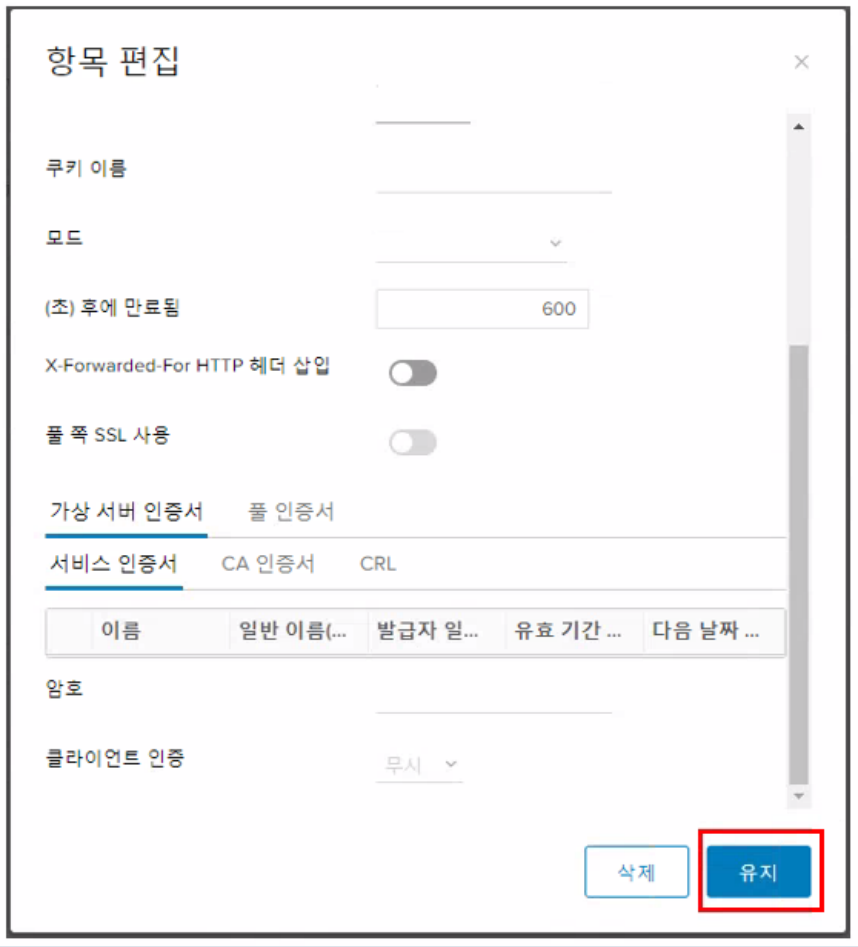
옵션	설명
X-Forwarded-For HTTP 헤더 삽입	(HTTP 및 HTTPS) **X-Forwarded-For HTTP 헤더 삽입**을 선택하면 로드 밸런서를 통해 웹 서버에 연결하는 클라이언트의 원래 IP 주소가 식별됩니다.
풀 쪽 SSL 사용	(HTTPS만 해당) [풀 인증서] 탭에서 **풀 쪽 SSL 사용**을 선택하여 서버 측 로 드 밸런서 인증에 사용할 인증서, CA 또는 CRL을 정의합니다.

○ (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 사용**을 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.

○ **유지** 를 클릭하여 변경 내용을 유지합니다.



작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

▫ 서비스 모니터 만들기

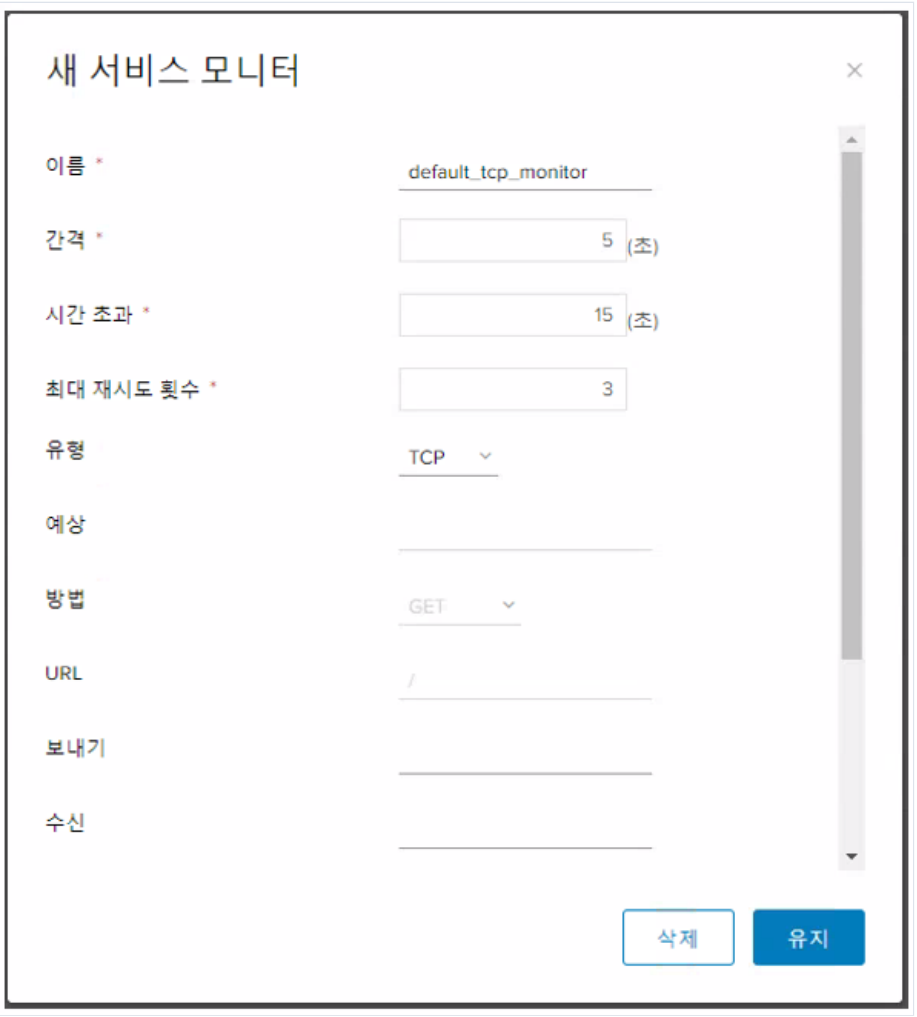
특정 유형의 네트워크 트래픽에 대한 상태 점검 매개 변수를 정의하는 서비스 모니터를 만듭니다.
서비스 모니터를 풀에 연결하면 풀 구성원이 서비스 모니터 매개 변수에 따라 모니터링됩니다.

절차

○ **로드 밸런서** > **서비스 모니터링**으로 이동합니다.

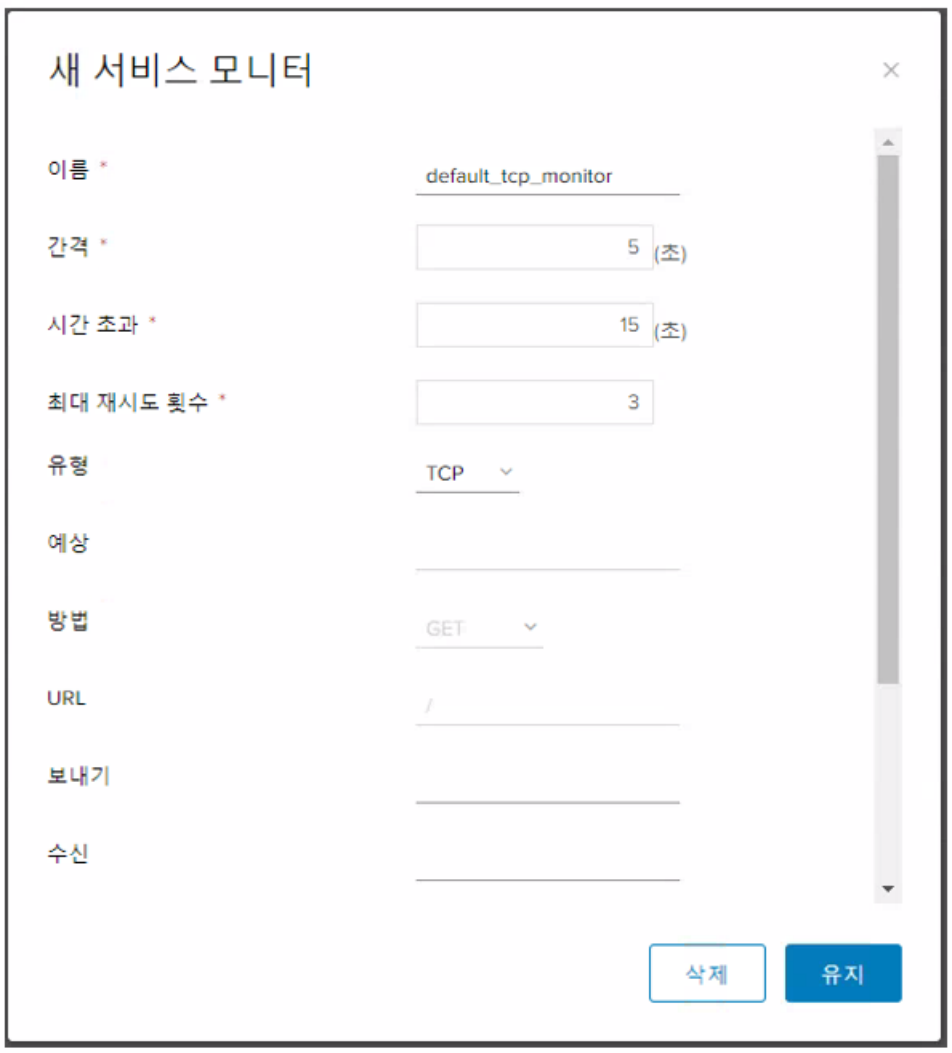
- **추가(+)** 버튼을 클릭합니다.

- (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	서버를 비활성화로 선언하기 전에 지정된 모니터링 **방법**이 연속으로 실패해야 하는 횟수를 입력합니다.
유형	상태 점검 요청을 서버로 보낼 때 사용할 방법(HTTP, HTTPS, TCP, ICMP 또는 UDP)을 선택합니다. 선택한 유형에 따라 **새 서비스 모니터** 대화 상자의 나머지 옵션이 사용되거나 사용되지 않습니다.
예상	(HTTP 및 HTTPS) 모니터가 HTTP 또는 HTTPS 응답의 상태 라인에서 일 치할 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 컨텐츠에서 일치할 문자열을 입력합니다. **참고** **예상**이 일치하지 않으면 모니터가 **받기** 컨텐츠의 일치를 시도하지 않습 니다.
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. <extension>delay=2 critical=3 escape</extension>

○ **유지** 를 클릭하여 변경 내용을 유지합니다.



작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

예제:각 프로토콜에 대해 지원되는 확장

표 5-1. HTTP/HTTPS 프로토콜에 대한 확장

모니터 확장	설명
no-body	문서 본문을 기다리지 않고 HTTP/HTTPS 헤더까지만 읽습니다.
	참고 HTTP GET 또는 HTTP POST는 계속 전송되고 HEAD 방법은 전송되지 않습니다.
max-age=SECONDS	문서가 SECONDS 이상 경과한 경우 경고합니다. 분의 경우 10m, 시간의 경우 10h 또는 일의 경우 10d의 형식으로 숫자를 입력할 수 있습니다.

content-type=STRING	POST 호출에 Content-Type 헤더 미디어 유형을 지정합니다.

표 5-1. HTTP/HTTPS 프로토콜에 대한 확장 (계속)

모니터 확장	설명
linespan	정규식을 새 행으로 연장할 수 있습니다(-r 또는 -R에 선행해야 함).
regex=STRING 또는 ereg=STRING	정규식 STRING의 페이지를 검색합니다.
eregi=STRING	대/소문자를 구분하지 않는 정규식 STRING의 페이지를 검색합니다.
invert-regex	찾은 경우 CRITICAL을 반환하고 찾을 수 없는 경우 OK를 반환합니다.
proxy-authorization=AUTH_PAIR	기본 인증을 사용하는 프록시 서버의 username:password를 지정합니다.
useragent=STRING	HTTP 헤더의 문자열을 User Agent로 전송합니다.
header=STRING	HTTP 헤더의 다른 모든 태그를 전송합니다. 추가 헤더가 있는 경우 여러 번 사용합니다.
onredirect=ok|warning|critical|follow|sticky| stickyport	리디렉션된 페이지를 처리하는 방법을 나타냅니다. sticky는 follow와 유사하지만 지정된 IP 주소에 고정됩니다. stickyport는 포트가 동일하게 유지되도록 합니다.
pagesize=INTEGER:INTEGER	필요한 최소 및 최대 페이지 크기(바이트)를 지정합니다.

warning=DOUBLE	경고 상태를 야기하는 응답 시간(초)을 지정합니다.
critical=DOUBLE	위험 상태를 야기하는 응답 시간(초)을 지정합니다.

표 5-2. HTTPS 프로토콜 전용 확장

모니터 확장	설명
sni	SSL/TLS 호스트 이름 확장 지원(SNI)을 사용하도록 설정합니다.
certificate=**INTEGER**	인증서의 최소 유효 기간을 지정합니다. 포트 기본값은 443입니다. 이 옵션을 사용하는 경우 URL이 검사되지 않습니다.
authorization=AUTH_PAIR	기본 인증을 사용하는 사이트의 username:password를 지정합니다.

표 5-3. TCP 프로토콜에 대한 확장

모니터 확장	설명
escape	send 또는 quit 문자열에 ₩n, ₩r, ₩t 또는 ₩ 문자를 사용할 수 있습니다. send 또는 quit 옵션의 앞에 사용해야 합니다. 기본적으로 send에는 아무 문자도 추가되지 않으며 quit의 끝에는 ₩r₩n 문자가 추가됩니다.
모든	서버 응답에 있어야 하는 모든 예상 문자열을 지정합니다. 기본적으로 any가 사용됩니다.
quit=STRING	서버로 문자열을 보내 연결을 완전히 닫습니다.
refuse=ok|warn|crit	ok, warn 또는 criti 상태를 사용하여 TCP 거부를 수락합니다. 기본적으로 crit 상태가 사용됩니다.

표 5-3. TCP 프로토콜에 대한 확장 (계속)

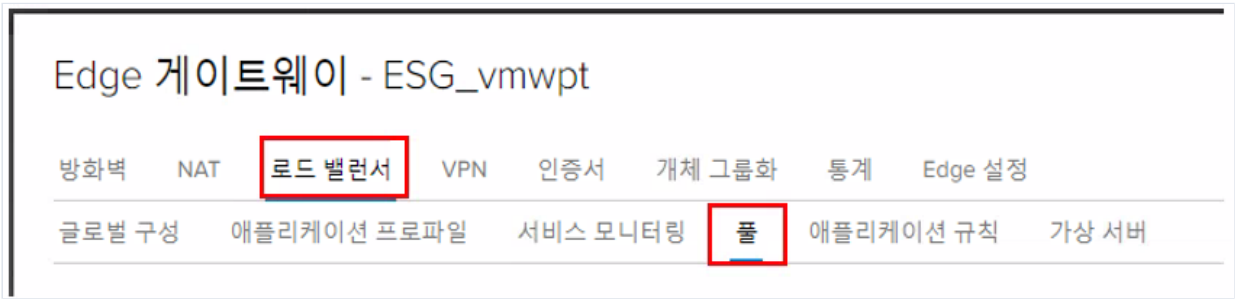
모니터 확장	설명
mismatch=ok|warn|crit	ok, warn 또는 crit 상태를 사용하여 예상되는 문자열 불일치를 수락합니다. 기본적으로 warn 상태가 사용됩니다.
jail	TCP 소켓의 출력을 숨깁니다.
maxbytes=INTEGER	지정된 바이트 수보다 많은 바이트가 수신되는 경우 연결을 닫습니다.
delay=INTEGER	문자열을 보내고 지정된 시간(초) 동안 대기한 후 응답을 폴링합니다.
certificate=INTEGER[,INTEGER]	인증서의 최소 유효 기간을 지정합니다. 첫 번째 값은 경고에 대한 #days이고 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.

▫ 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.

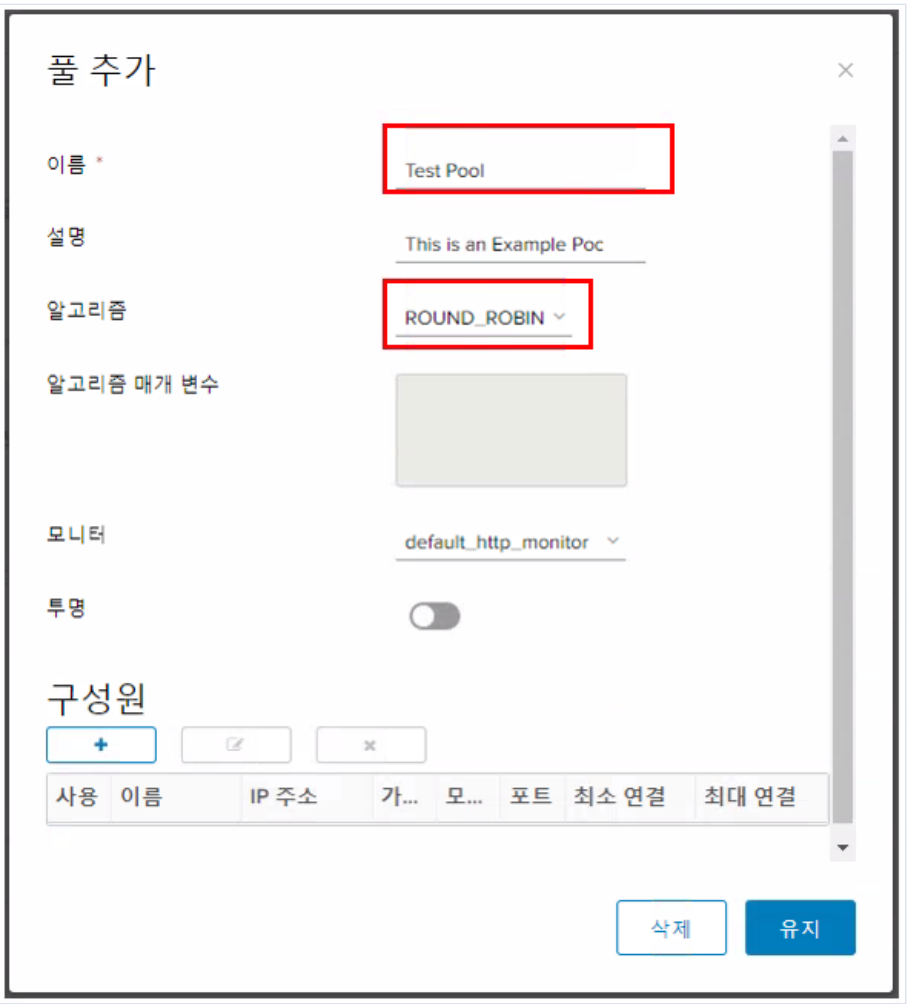
절차

○ **로드 밸런서** > **풀로** 이동합니다.



○ **추가 버튼(** + **)**을 클릭합니다.

○ 로드 밸런서 풀의 이름과 설명(선택 항목)을 입력합니다.
○ **알고리즘** 드롭다운 메뉴에서 서비스의 밸런싱 방법을 선택합니다.

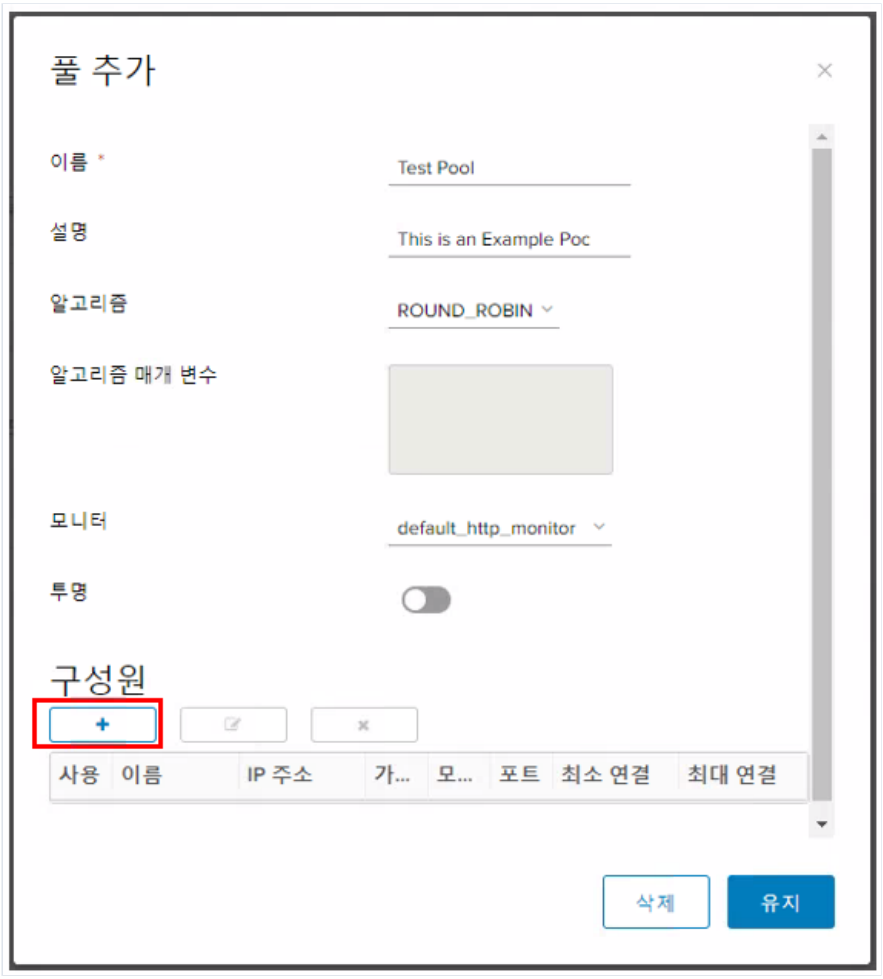


옵션	설명
ROUND-ROBIN	각 서버에 할당된 가중치 순서대로 서버가 사용됩니다. 이는 서버의 처리 시간이 균등하게 분산된 상태를 유지하는 가장 유연하고 공정한 알고리즘입니다.

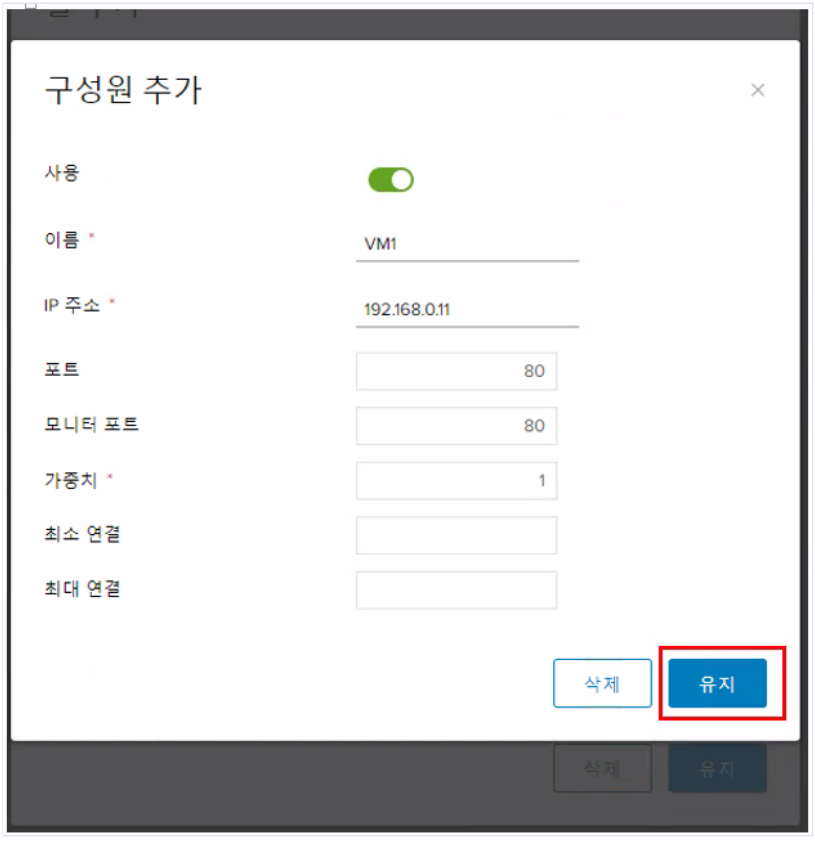
IP-HASH	각 패킷에 대해 소스 및 대상 IP 주소의 해시를 기반으로 서버를 선택합니다.
LEASTCONN	서버에 이미 열려 있는 연결 수를 기반으로 하여 클라이언트 요청을 여러 서버로 분산합니다. 새 연결은 열린 연결 수가 가장 적은 서버로 전송됩니다.

옵션	**설명**
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 않는한 동일한 사용자 ID가 항상 동일한 서버로 전송되도록 합니다. 값 또는 매개변수가 없는 경우 라운드 로빈 알고리즘이 적용됩니다. URL 알고리즘 매개 변수에는 urlParam=<url> 옵션이 하나 있습니다.

- 풀에 구성원을 추가합니다.
  추가 () 버튼을 클릭합니다.



○ 구성원 정보를 입력합니다.



- 풀 구성원의 이름을 입력합니다.
- 풀 구성원의 IP 주소를 입력합니다.

- 구성원이 로드 밸런서의 트래픽을 수신할 포트를 입력합니다.

- 구성원이 상태 모니터 요청을 수신할 모니터 포트를 입력합니다.

- **가중치** 텍스트 상자에 이 구성원이 처리할 트래픽의 비율을 입력합니다. 1~256 범위의 정수 여야 합니다.

- (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 해 제될 때까지 대기합니다.

- (선택 사항) **최소 연결** 텍스트 상자에 구성원이 항상 수락해야 하는 최소 동시 연결 수를 입력 합니다.

- **유지**를 클릭하여 새 구성원을 풀에 추가합니다.

  작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

○ (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.

○ **유지**를 클릭하여 변경 내용을 유지합니다.

작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

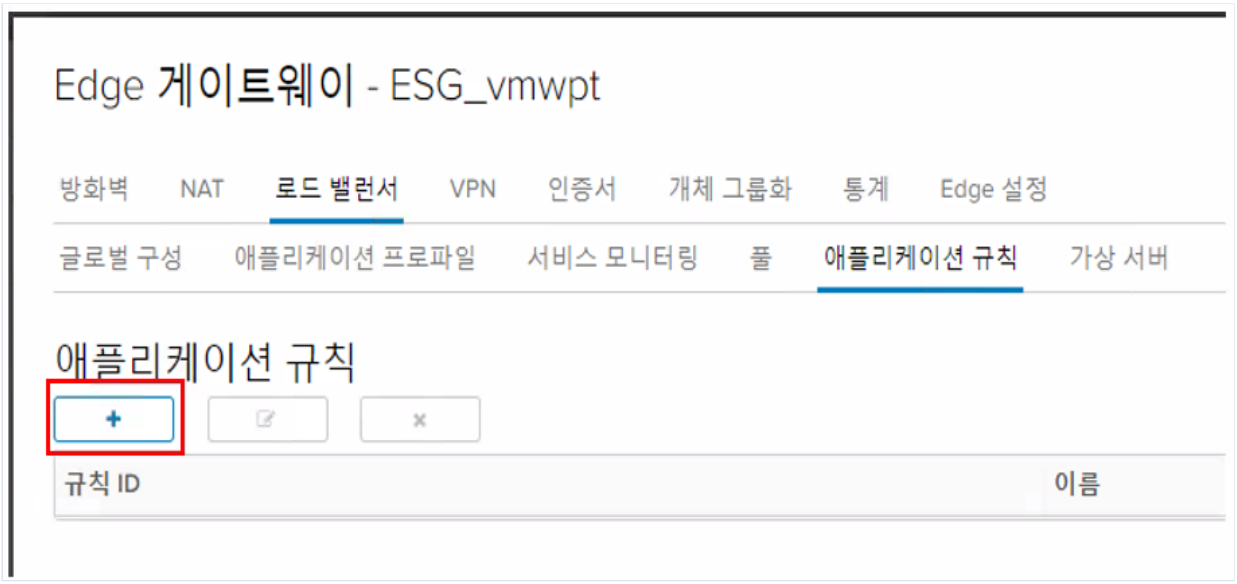
▫ 애플리케이션 규칙 추가

애플리케이션 규칙을 작성하여 IP 애플리케이션 트래픽을 직접 조작하고 관리할 수 있습니다.

절차

○ **로드 밸런서** > **애플리케이션 규칙**으로 이동합니다.

○ **추가** (+)버튼을 클릭합니다.



○ 애플리케이션 규칙의 정보를 입력합니다.

- 애플리케이션 규칙의 스크립트를 입력합니다.

애플리케이션 규칙 구문에 대한 자세한 내용은

http://cbonte.github.io/haproxy-dconv/configuration-1.5.html을 참조하십시오.

○ **유지** 를 클릭하여 변경 내용을 유지합니다.

작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

▫ 가상 서버 추가

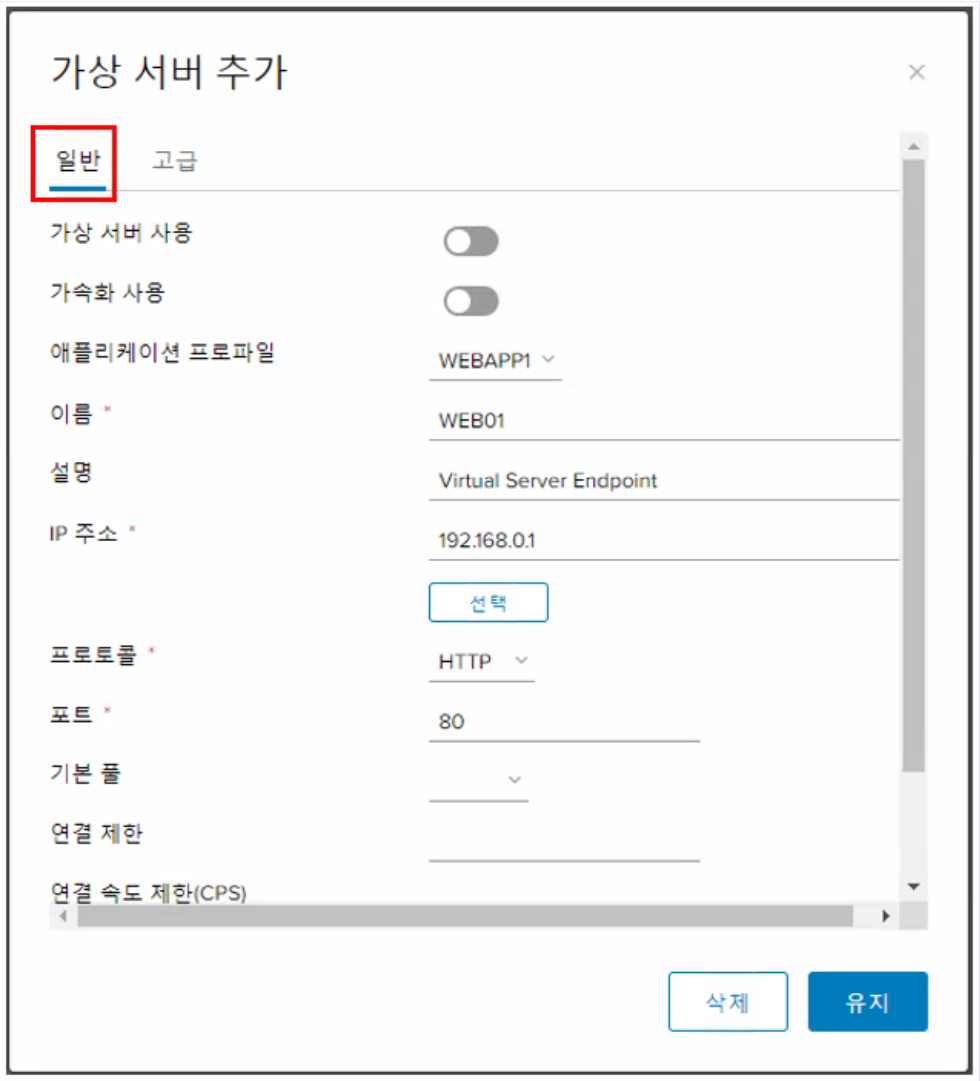
Edge 게이트웨이 내부 또는 업링크 인터페이스를 가상 서버로 추가합니다.
가상 서버는 공개 IP 주소를 사용하며 모든 수신 클라이언트 요청을 처리합니다.
기본적으로 로드 밸런서는 각 클라이언트 요청 후 서버 TCP 연결을 닫습니다.

절차

○ **로드 밸런서** > **가상 서버**로 이동합니다.

○ **추가** 버튼을 클릭합니다.

○ **일반** 탭에서 가상 서버에 대한 다음 옵션을 구성합니다.

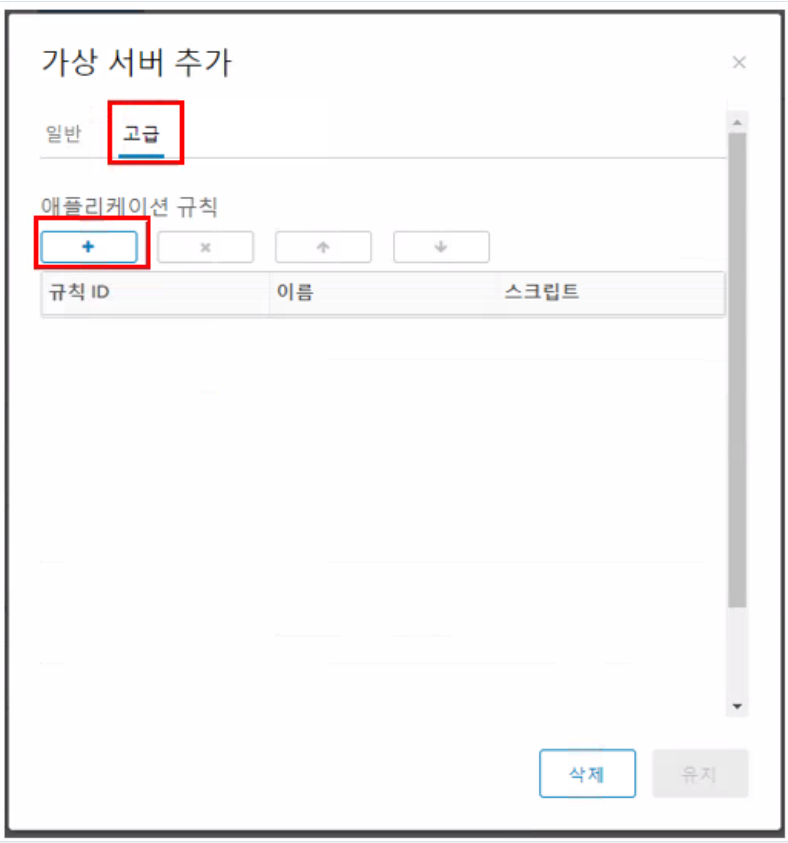


옵션	설명
가상 서버 사용	가상 서버를 사용하도록 설정하려면 클릭합니다.
가속화 사용	가속화를 사용하도록 설정하려면 클릭합니다.
애플리케이션 프로파일	가상 서버와 연결할 애플리케이션 프로파일을 선택합니다.
이름	가상 서버의 이름을 입력합니다.
설명	가상 서버에 대한 설명(선택 사항)을 입력합니다.
IP 주소	로드 밸런서가 수신 대기하는 IP 주소를 입력하거나 찾아서 선택합니다.

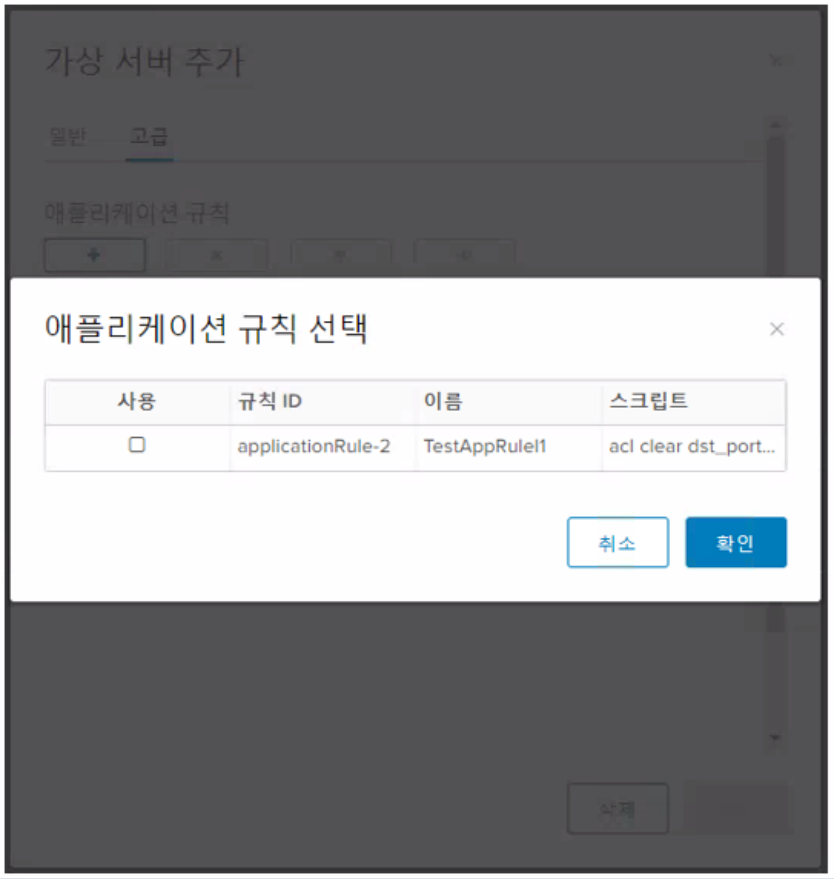
프로토콜	가상 서버가 수락하는 프로토콜을 선택합니다. 선택한 **애플리케이션 프로파일**에 사용되는 동일한 프로토콜을 선택해야 합니다.
포트	로드 밸런서가 수신하는 포트 번호를 입력합니다.
기본 풀	로드 밸런서가 사용할 서버 풀을 선택합니다.
연결 제한	(선택 사항) 가상 서버가 처리할 수 있는 최대 동시 연결 수를 입력합니다.
연결 속도 제한(CPS)	(선택 사항) 초당 수신되는 새 연결 요청의 최대 수를 입력합니다.

ㅇ (선택 사항) 애플리케이션 규칙을 가상 서버에 연결하려면 **고급** 탭을 클릭하고 다음 단계를 완료합니다.

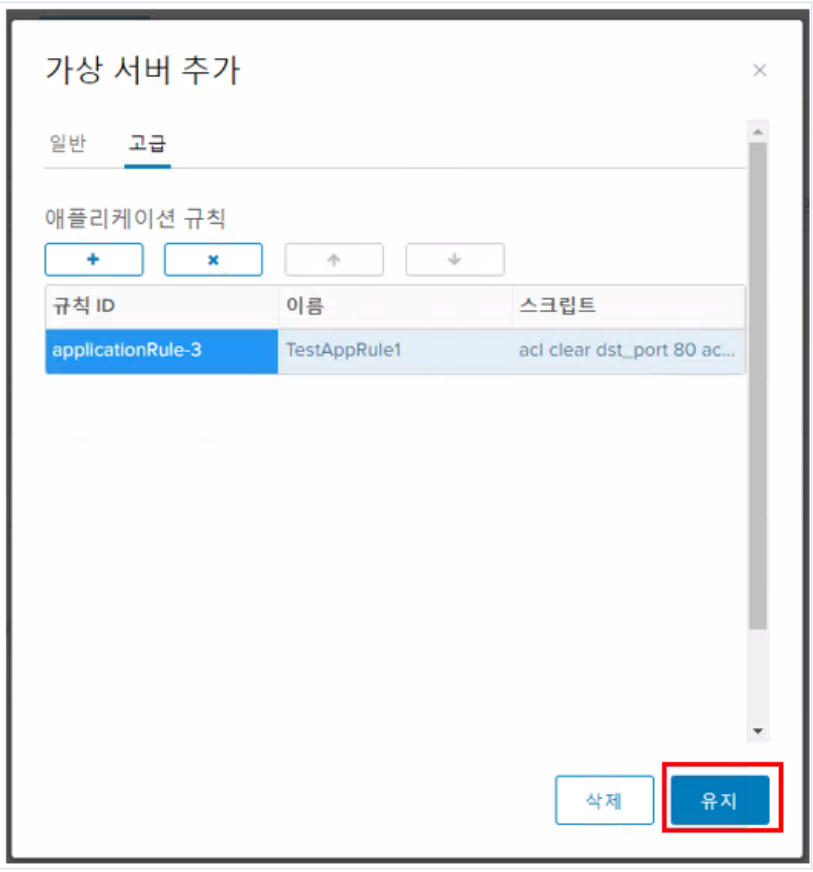
- **추가** 버튼을 클릭합니다.



ㅇ 로드 밸런서에 대해 만들어진 애플리케이션 규칙이 표시됩니다. 필요한 경우 로드 밸런서에 대한 애플리케이션 규칙을 추가합니다.



○ **유지** 를 클릭하여 변경 내용을 유지합니다.



작업을 완료하는 데 몇 분이 걸릴 수 있습니다.

1.3.2 VMware on KT Cloud Edge IPsec-VPN 설정

NSX Advanced Edge는 NSX Edge 인스턴스와 원격 사이트 간의 사이트 간 IPSec VPN을 지원합니다.
각 원격 VPN 라우터 뒤에는 IPSec 터널을 통해 NSX Edge 뒤에있는 내부 네트워크에 연결하도록 여러 서브넷을 구성 할 수 있습니다.
이러한 서브넷과 NSX Edge 뒤의 내부 네트워크에는 중복되지 않는 주소 범위가 있어야합니다.
필요한 터널의 수는 로컬 서브넷의 수에 피어 서브넷의 수를 곱한 값으로 정의됩니다.
예를 들어 10 개의 로컬 서브넷과 10 개의 피어 서브넷이있는 경우 100 개의 터널이 필요합니다.
지원되는 터널의 최대 수는 다음과 같이 ESG 크기에 의해 결정됩니다.

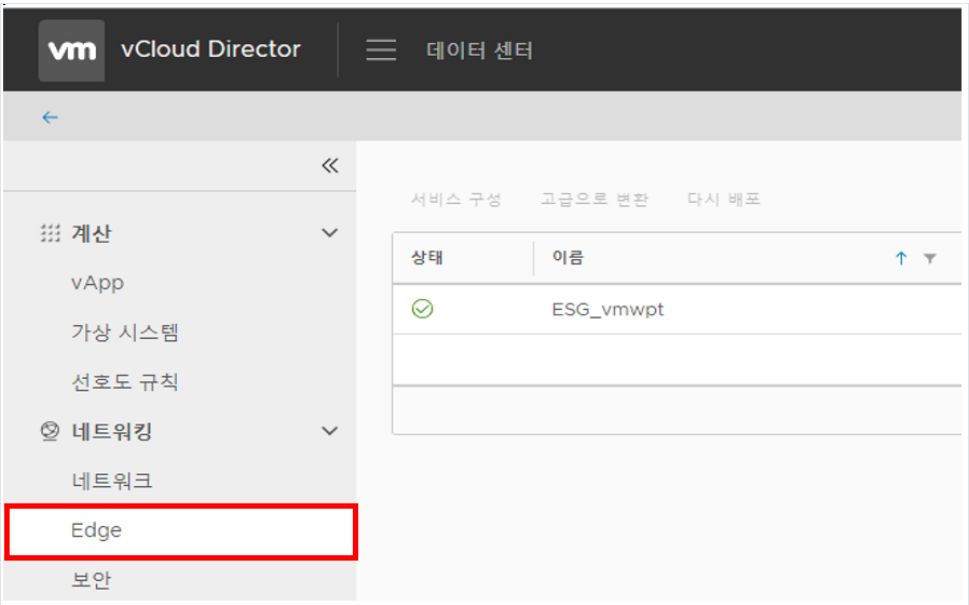
▫ IPSec VPN 구성

VMware VDC에 IPSec VPN을 사용하려면 다음을 수행하십시오.

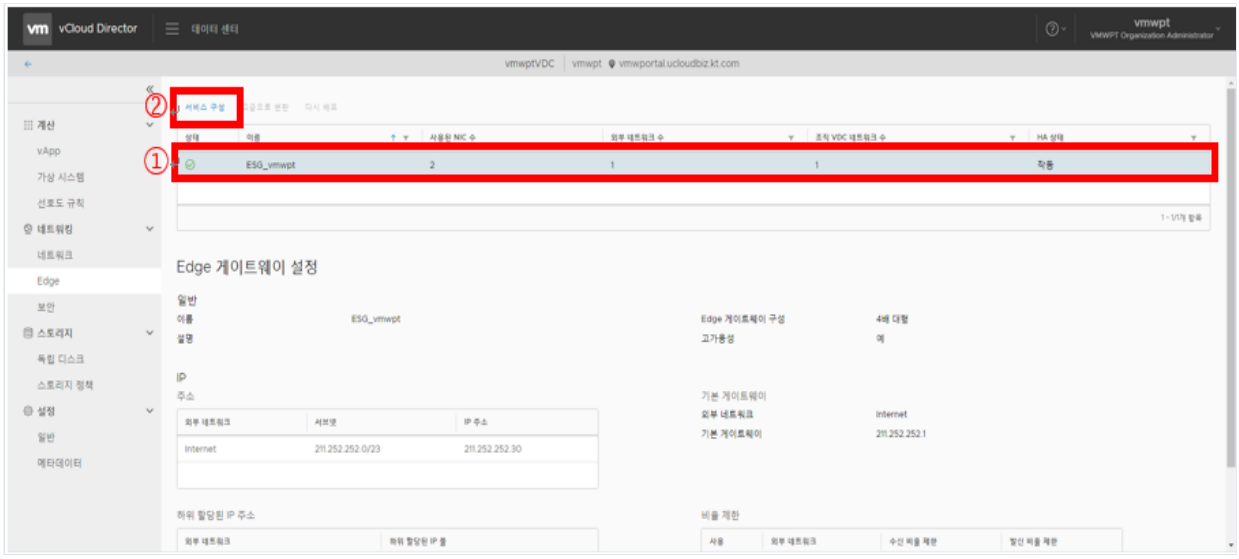
절차

○ Edge 게이트웨이 서비스를 엽니다.

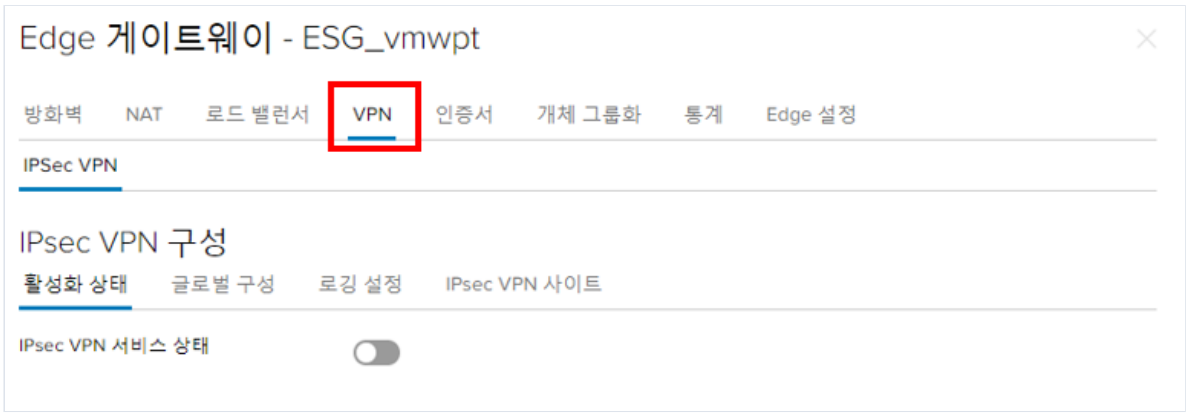
- 네트워킹 > Edge로 이동합니다.



○ 편집할 Edge 게이트웨이를 선택하고 서비스 구성을 클릭합니다.



○ VPN 탭을 클릭합니다.



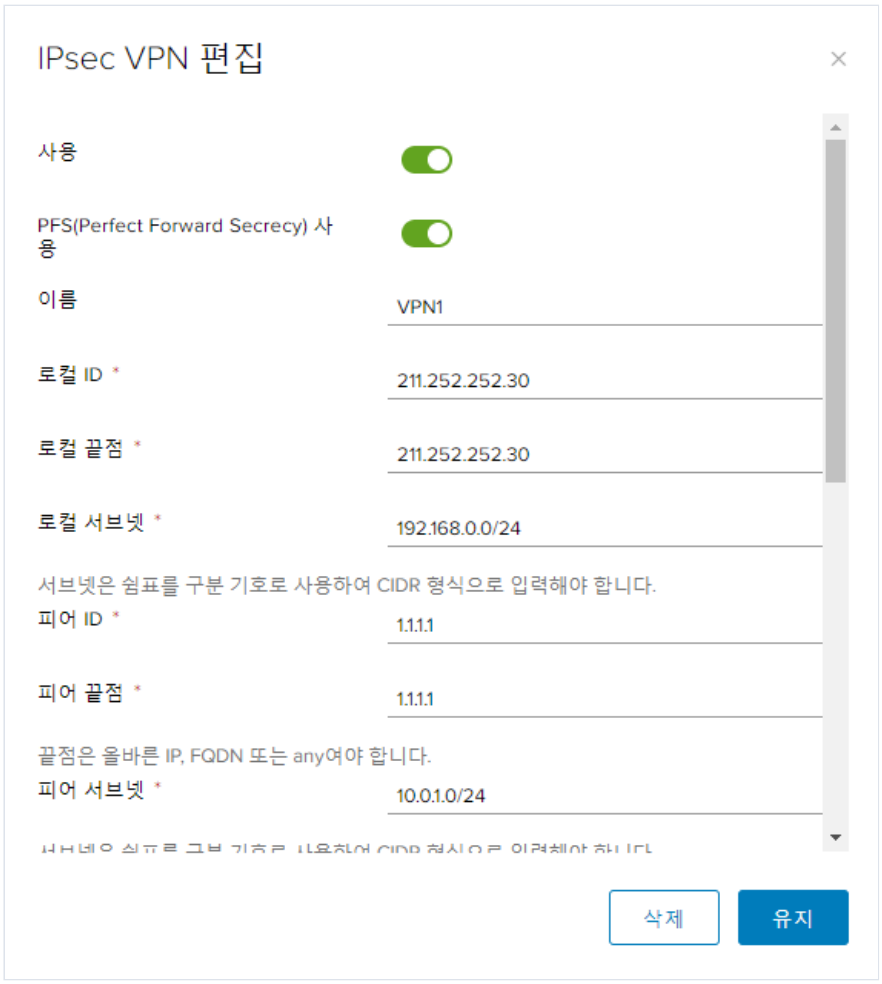
○ [IPsec VPN 구성] 아래 IPsec VPN 사이트 탭을 선택한 후 +(추가) 버튼을 클릭합니다.

○ [IPsec VPN 추가] 페이지에서 세부사항을 입력합니다.

필드	설명	필수여부
VPN 사용여부	이 항목이 사용으로 설정되어 있는지 확인하세요	예
PFS 사용여부	이 기능이 활성화 되어 있는지 확인하세요. PFS는 동일한 키가 다시 생성되지 않	예

	도록 보장하므로 새로운 diffie-hellman 키 교환을 강제 수행합니다		
이름	VPN 터널의 이름을 입력하세요	아니오	
로컬 ID	로컬 엔드 포인트를 설명하는 데 사용됩니다. 일반적으로 Local Public IP가 사용됩니다	예	
로컬 끝점	Edge Gateway의 업 링크 인터페이스 IP를 선택하십시오 (VDC의 “개요” 탭에서 사용 가능)	예	
로컬 서브넷	VPN의 내부 네트워크로 지정할 네트워크를 입력하세요. 서브넷은 쉼표를 구분 기호로 사용하여 CIDR 형식으로 입력해야 합니다	예	
피어 ID	원격 엔드 포인트를 설명하는데 사용됩니다. 일반적으로 원격 공용 IP가 사용됩니다	예	
피어 끝점	VPN을 설정하는 원격 장치의 공용 IP 주소를 입력하세요	예	
피어 서브넷	VPN에 대한 원격 네트워크로 지정할 네트워크를 입력하세요. 서브넷은 쉼표를 구분 기호로 사용하여 CIDR 형식으로 입력해야 합니다.	예	
암호화 알고리즘	암호화 프로토콜은 원격사이트 VPN 장치에 구성된 내용을 반영합니다	예	
인증	인증방법을 선택합니다	예	
미리 공유한 키	NSX Edge와 피어 사이트간에 공유되는 비밀 키가 인증에 사용됨을 나타냅니다. 비밀 키는 최대 길이가 128 바이트 인 문자열이 될 수 있습니다.	예	
공유 키 표시	글로벌 PSK(미리 공유한 키)는 피어 끝점이 '임의'로 설정된 모든 사이트에서 공유됩니다. 글로벌 PSK가 이미 설정된 경우 PSK를 빈 값으로 변경하고 저장해도 기존 설정에 영향을 주지 않습니다.	예	
Diffie-Hellman 그룹	피어 사이트 및 NSX Edge가 안전한지 않은 통신 채널을 통해 공유된 비밀을 수립할 수 있도록 하는 암호화 기법	예	
확장	securelocaltrafficbyip = IPAddress는 IPSec VPN 터널을 통해 Edge의 로컬 트래픽을 재전송합니다. 중복되는 서브넷을 지원하는 기본값은passthroughSubnets = PeerSubnetIPAddress입니다	아니오	

ㅇ 유지 버튼을 클릭합니다.


IPsec VPN 편집
사용
PFS(Perfect Forward Secrecy) 사용
이름
VPN1
로컬 ID *
211.252.252.30
로컬 끝점 *
211.252.252.30
로컬 서브넷 *
192.168.0.0/24
서브넷은 쉼표를 구분 기호로 사용하여 CIDR 형식으로 입력해야 합니다.
피어 ID *
1.1.1.1
피어 끝점 *
1.1.1.1
끝점은 올바른 IP, FQDN 또는 any여야 합니다.
피어 서브넷 *
10.0.1.0/24
삭제
유지

○ 변경 내용을 저장합니다


Edge 게이트웨이 - ESG_vmwpt
IPsec VPN
IPsec VPN 구성
변경 내용 저장
변경 내용 삭제
IPsec VPN 사이트
사이트 이름
로컬 끝점
로컬 서브넷
피어 끝점
피어 서브넷
사이트 사용
VPN1
211.252.252.30
192.168.0.0/24
1.1.1.1
10.0.1.0/24

1.4 VPC-vCloud Director Import/Export 이용방법

메뉴얼 구성

1.4.1 패키지 Import / Export 서비스

- Import 서비스 : OVA에서 vAPP템플릿 만들기
- Import 서비스 : OVA에서 vAPP 만들기
- Export 서비스 : OVA로 vAPP을 다운로드
- Export 서비스 : OVA파일로 vApp 템플릿 다운로드

1.4.2 미디어 파일 업로드 / 다운로드

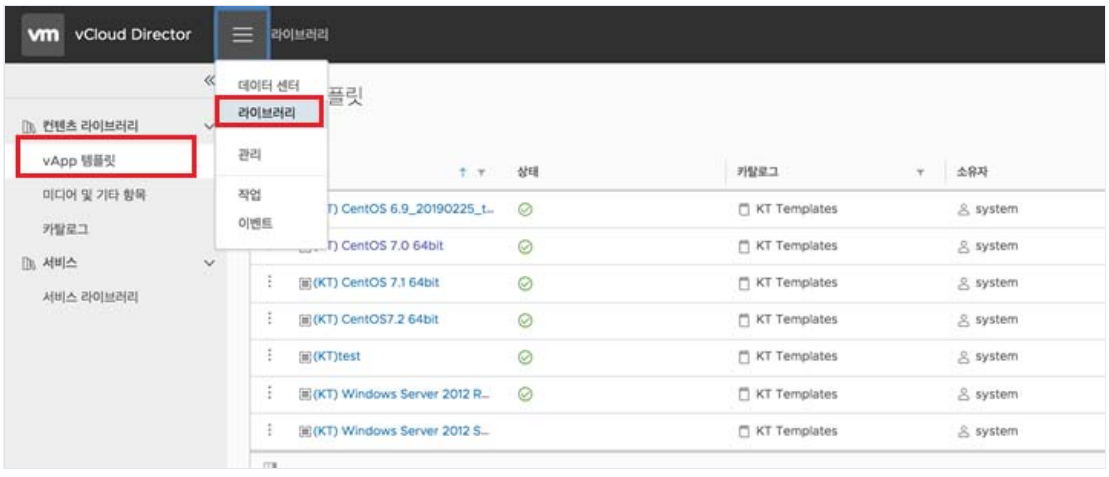
- 미디어 파일 업로드
- 미디어 파일 다운로드
- 미디어 파일 삭제

1.4.1 패키지 Import / Export

▫ Import 서비스 : OVA에서 vAPP템플릿 만들기

- OVA를 업로드하여 vApp 템플릿을 생성할 수 있습니다.

(1) 기본 메뉴에서 라이브러리를 선택하고 왼쪽 패널에서 vApp 템플릿을 선택합니다. 템플릿 목록이 표시됩니다.

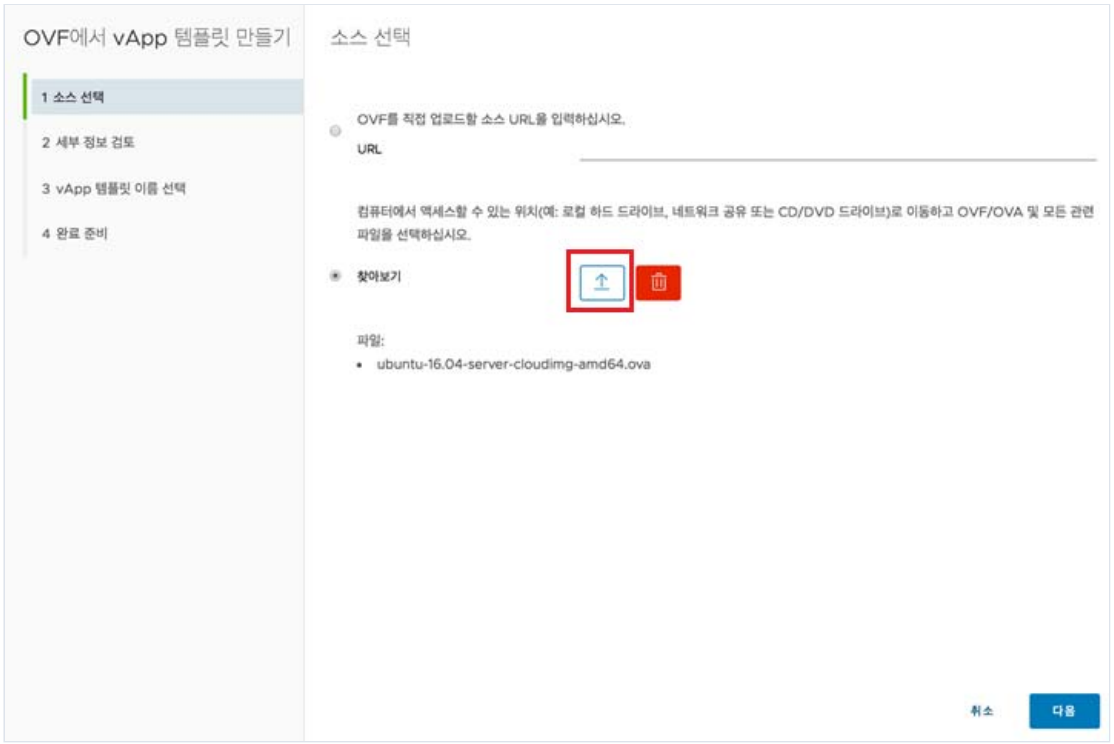


(2) 추가를 클릭합니다.

(3) OVA 파일 업로드 아이콘을 클릭하고 컴퓨터에서 액세스할 수 있는 위치를 찾아서 템플릿 파일을 선택합니다.

* 고객님의 로컬 하드드라이브, 네트워크 공유드라이브, CD/DVD 등 매체에서 올리시면 됩니다.

* 지원되는 파일 확장명은 .ova .ovf .vmdf .mf .cert 및 .strings 입니다.



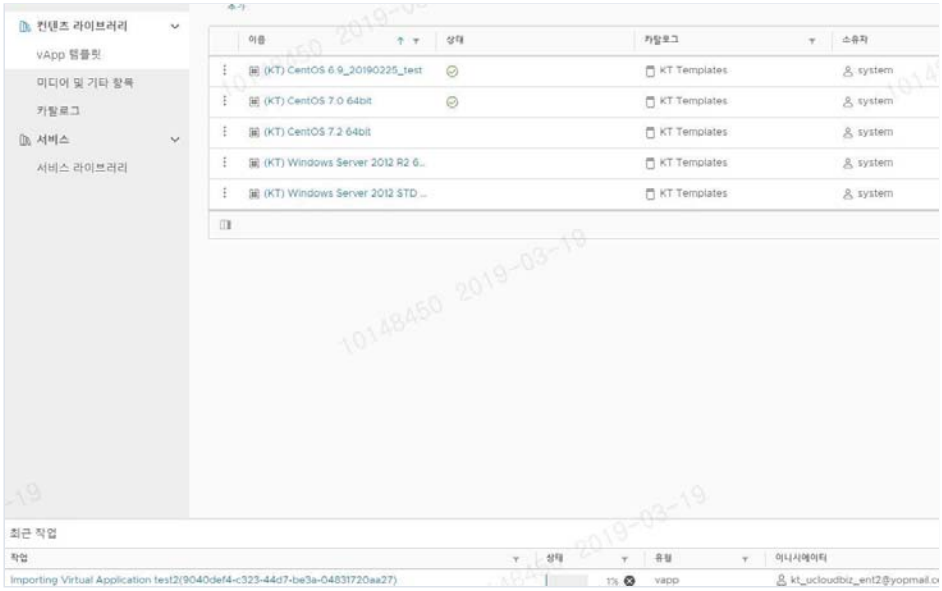
(4) 다음의 세부탭의 내용들을 확인하고 다음을 클릭합니다.

* 세부 정보 검토 탭 : OVA/OVF 템플릿의 세부정보를 확인합니다.

* vApp 템플릿 이름 선택 : vAPP 템플릿의 이름/설명을 확인합니다. 템플릿을 추가할 카탈로그를 선택합니다. (default KT Template)

* 완료 준비 탭 : vApp 템플릿 설정을 검토하고 마침을 클릭합니다.

(5) 위 단계를 마치면 하단 모니터링 툴로 진행상황을 확인할 수 있습니다.

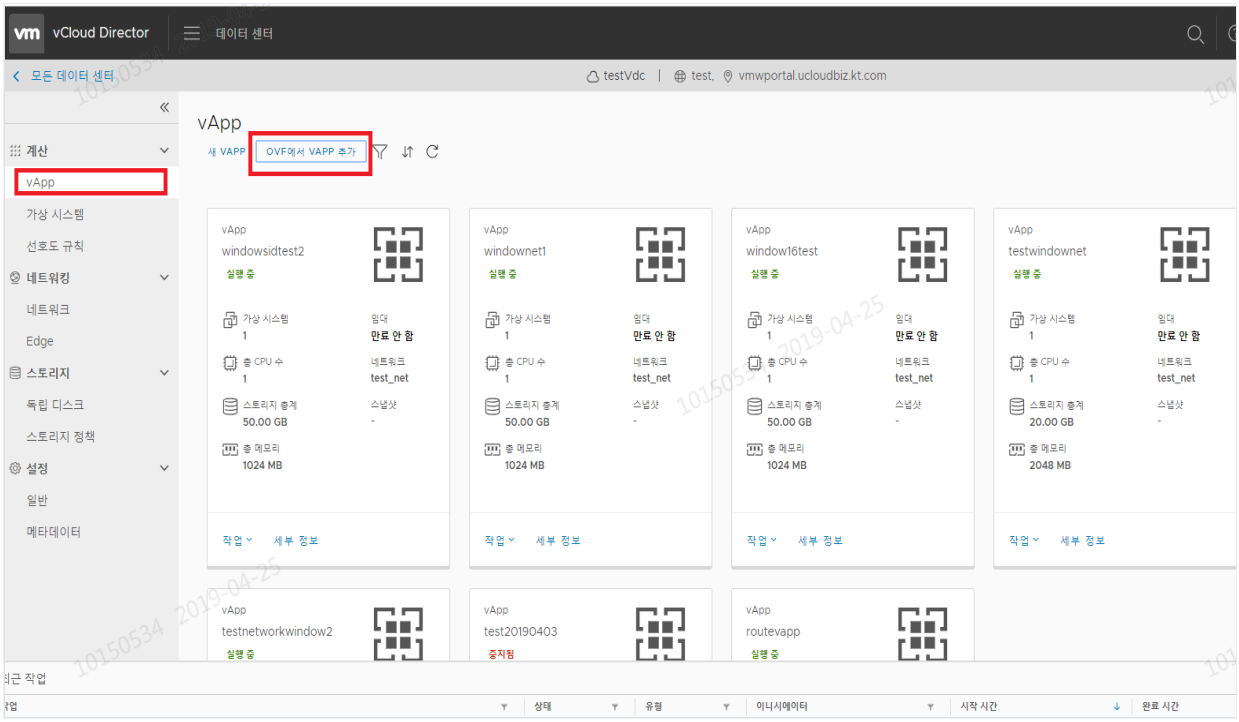


□ Import 서비스 : OVA에서 vAPP 만들기

- OVA에서 직접 vAPP을 만들어 배포할 수 있습니다.

(1) 가상 데이터 센터 대시보드에서 가상 데이터센터 카드를 클릭하여 vAPP 대시보드에 접속합니다.

(2) 'OVF에서 vAPP 추가'를 클릭합니다.



(3) 업로드 버튼 클릭하여 OVF/OVA 템플릿 파일을 올릴 수 있습니다.

* 고객님의 로컬 하드드라이브, 네트워크 공유드라이브, CD/DVD 등 매체에서 올리시면 됩니다.

* 지원되는 파일 확장명은 .ova .ovf .vmdf .mf .cert 및 .strings 입니다.

(4) OVF/OVA 템플릿의 다음 정보들을 확인하면서 다음을 클릭합니다.

* 세부정보 검토탭 : 세부 정보를 확인합니다.

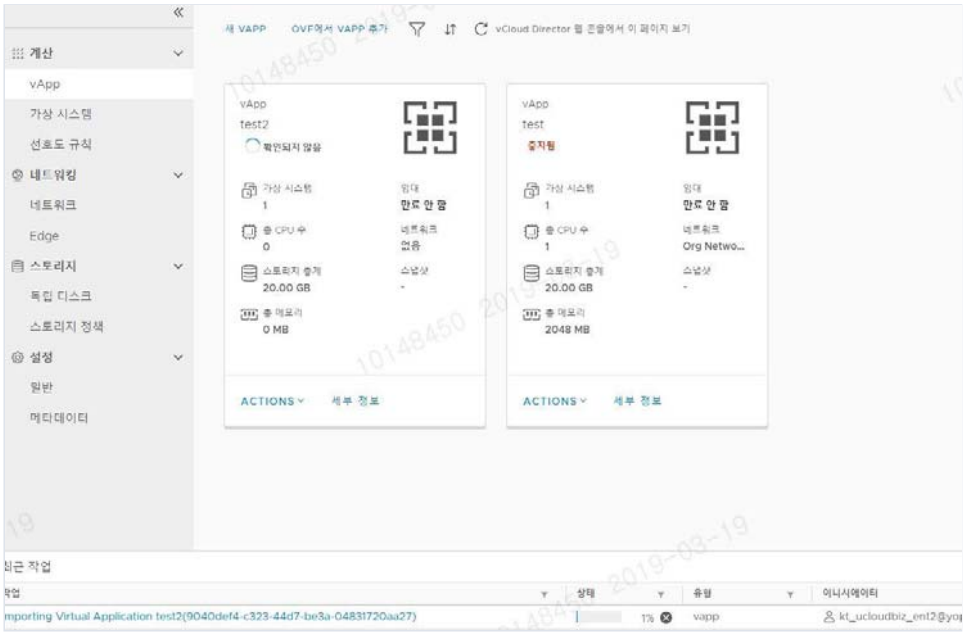
* vAPP 이름 선택탭 : vAPP의 이름/설명을 확인합니다.

* 리소스 구성탭 : vAPP 컴퓨터 이름을 영숫자로만 작성합니다. 스토리지 정책 드롭다운 메뉴에서 vApp의 각 가상시스템에 대한 정책을 선택합니다.

* 네트워킹 구성탭 : 각 가상 시스템에 연결할 네트워크를 선택합니다. 고급 네트워킹 워크플로를 클릭하여, 네트워크 유형/IP 할당을 바로 진행합니다.

* 하드웨어 사용자 지정탭 : vApp 에 있는 가상 시스템의 하드웨어를 사용자 지정합니다.

(5) 위 단계를 마치면 하단 모니터링 툴로 진행상황을 확인할 수 있습니다.

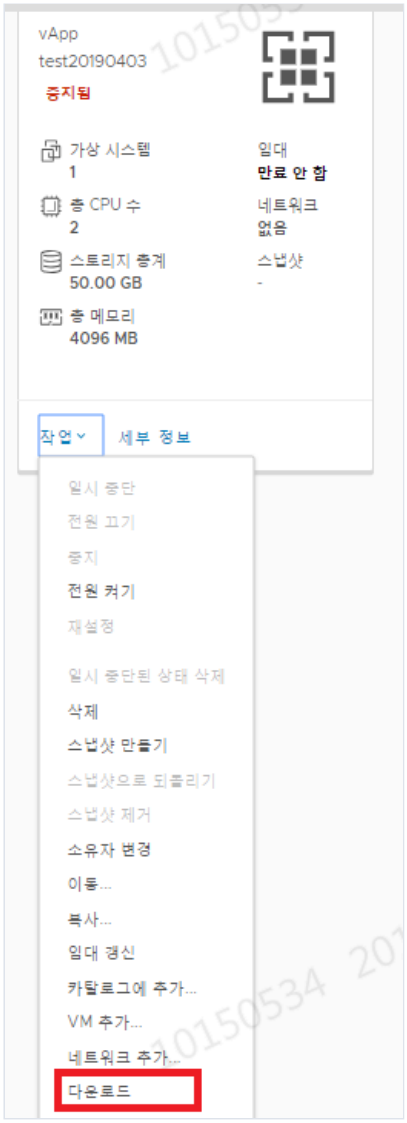


□ Export 서비스 : OVA로 vAPP을 다운로드

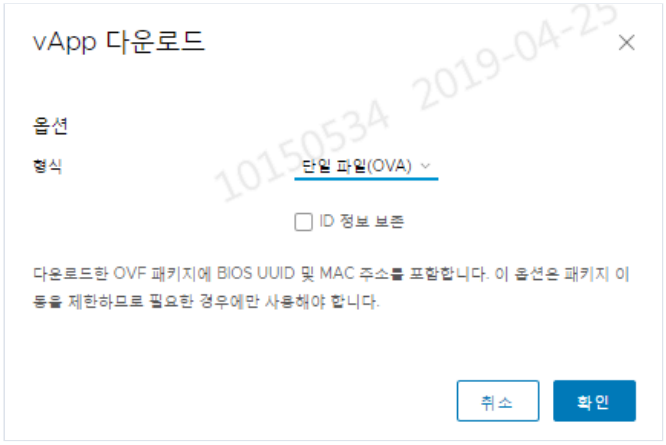
- vApp 를 OVF 패키지로 다운로드할 수 있습니다. - vApp 가 전원이 꺼져 있고 배포 취소되어 있는지 확인합니다.

(1) 가상 데이터센터 대시보드 -> 가상 데이터센터 카드클릭 -> vApp 탭클릭 -> vApp을 카드보기에서 확인합니다.

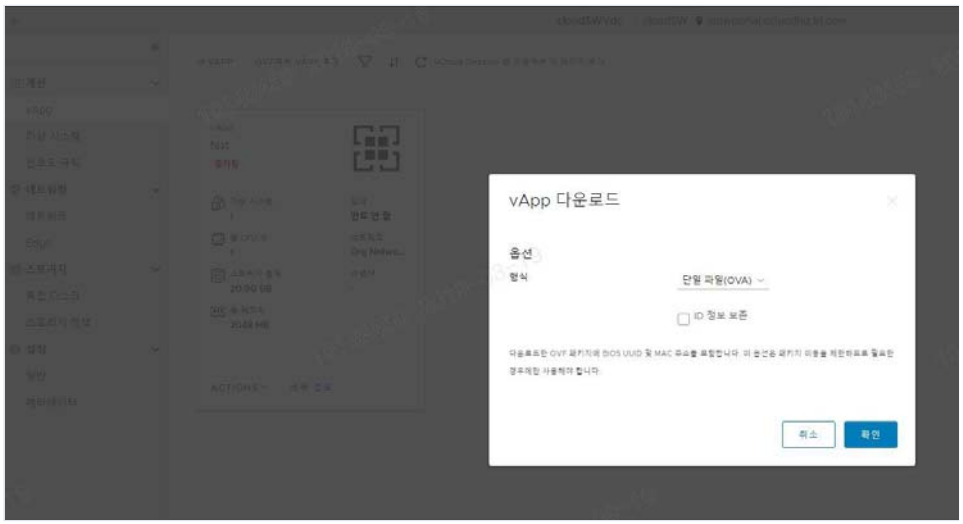
(2) 다운로드할 vApp 의 더 보기 메뉴에서 다운로드를 선택합니다.



(3) (선택 사항) 다운로드되는 OVA에 vApp 가상 시스템의 UUID 및 MAC 주소를 포함하려면 ID정보 보존을 선택합니다.



(4) 확인을 클릭하여 다운로드를 완료합니다

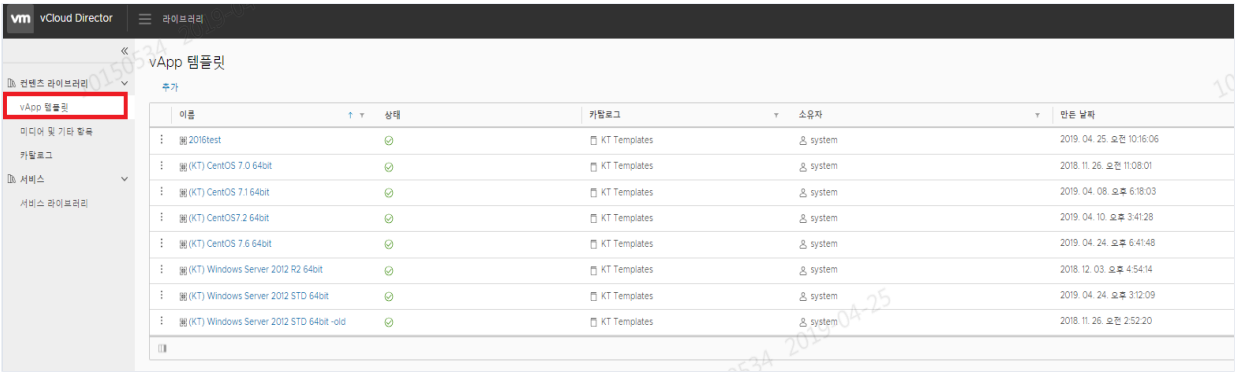


(5) 진행상황을 하단의 모니터링에서 확인하실 수 있습니다.

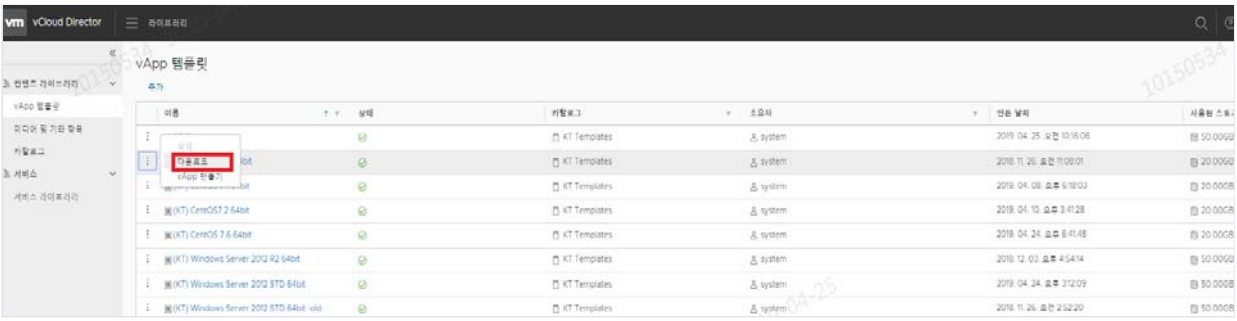
ㅁ Export 서비스 : OVA파일로 vApp 템플릿 다운로드

- 컨텐츠 라이브러리의 vApp 템플릿은 OVA 파일로 로컬 시스템에 다운로드할 수 있습니다.

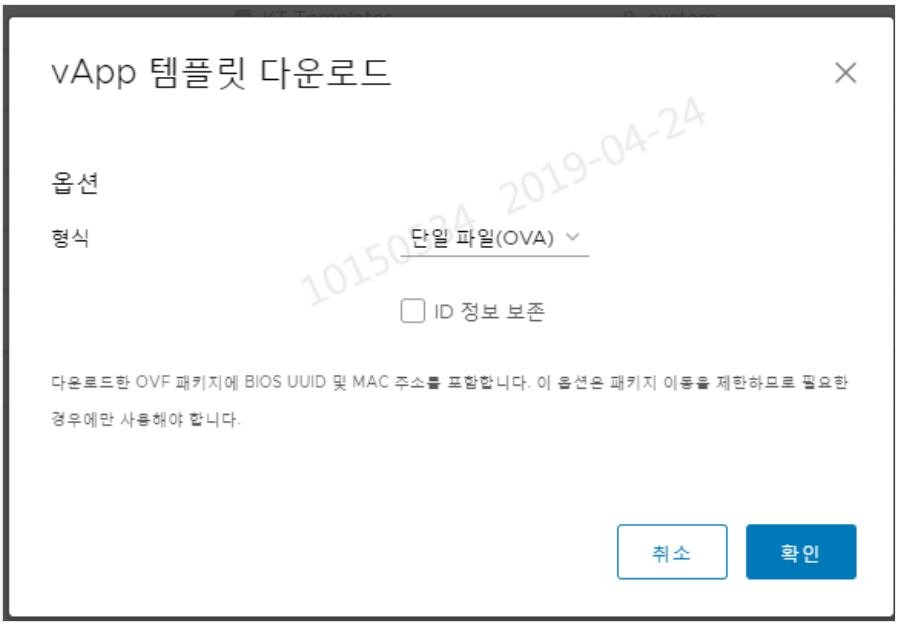
(1) 상단탭에서 '라이브러리'를 선택하고 왼쪽 패널에서 'vApp 템플릿'을 선택합니다. 템플릿 목록이 표시됩니다.



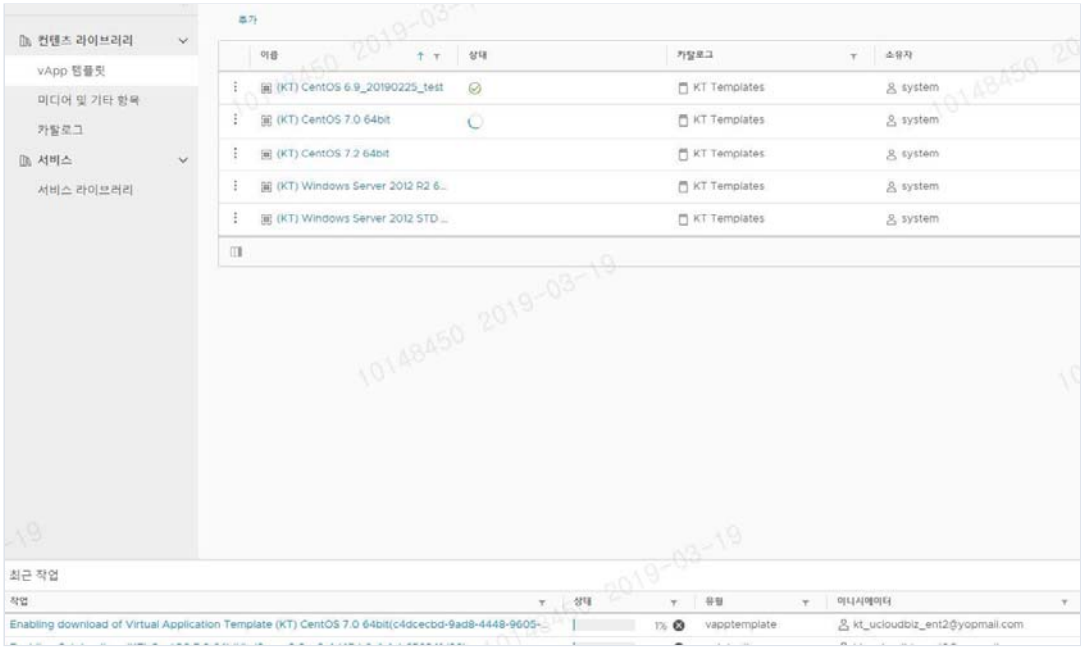
(2) vApp 템플릿의 왼쪽에 있는 목록 표시줄을 클릭하고 다운로드를 선택합니다.



(3) OVA 패키지에 있는 가상 시스템의 UUID 및 MAC 주소를 보존하려면 ID정보 보존 확인란을 선택합니다.



(4) 확인을 클릭하고 다운로드가 완료될 때까지 기다립니다. OVA 파일은 웹 브라우저의 기본 다운로드 위치에 저장됩니다.



1.4.2 미디어 파일 업로드 / 다운로드

미디어 파일을 업로드, 복사 및 이동하고, 해당 속성을 편집할 수 있습니다.

▫ 미디어 파일 업로드

- 새 미디어 파일 또는 기존 미디어 파일의 새 버전을 업로드할 수 있습니다.

(1) 기본 메뉴에서 라이브러리를 선택하고 왼쪽 패널에서 미디어 및 기타 항목을 선택합니다. 미디어 파일 목록을 확인합니다.

(2) 미디어 및 기타항목 왼쪽 패널을 클릭한 후, 추가를 누릅니다. 드롭다운 메뉴에서 업로드용 미디어 파일을 선택합니다.

(3) 미디어 파일의 이름을 입력합니다. 이름을 입력하지 않으면 미디어 파일 이름이 이름 텍스트 상자에 자동으로 채워집니다.

(4) 업로드 아이콘을 클릭하여 디스크 이미지 파일(예: .iso 파일)을 찾아 선택합니다.

(5) 확인을 클릭합니다. 업로드가 시작되면 미디어 파일이 목록에 나타납니다.

▫ 미디어 파일 다운로드

- 카탈로그에서 미디어 파일을 다운로드할 수 있습니다

(1) 기본 메뉴에서 라이브러리를 선택하고 왼쪽 패널에서 미디어 및 기타 항목을 선택합니다. 미디어 파일 목록이 표시됩니다.

(2) 다운로드할 미디어 파일의 왼쪽에 있는 목록 표시줄을 클릭하고 다운로드를 선택합니다.

(3) 다운로드 작업이 시작되고 웹 브라우저의 기본 다운로드 위치에 파일이 저장됩니다.

▫미디어 파일 삭제

- 더 이상 사용하지 않으려는 미디어 파일은 카탈로그에서 삭제할 수 있습니다.

(1) 기본 메뉴에서 라이브러리를 선택하고 왼쪽 패널에서 미디어 및 기타 항목을 선택합니다. 미디어 파일 목록이 표시됩니다.

(2) 삭제할 미디어 파일의 왼쪽에 있는 목록 표시줄을 클릭하고 삭제를 선택합니다.

(3) 삭제를 확인합니다. 삭제된 미디어 파일이 목록에서 제거됩니다