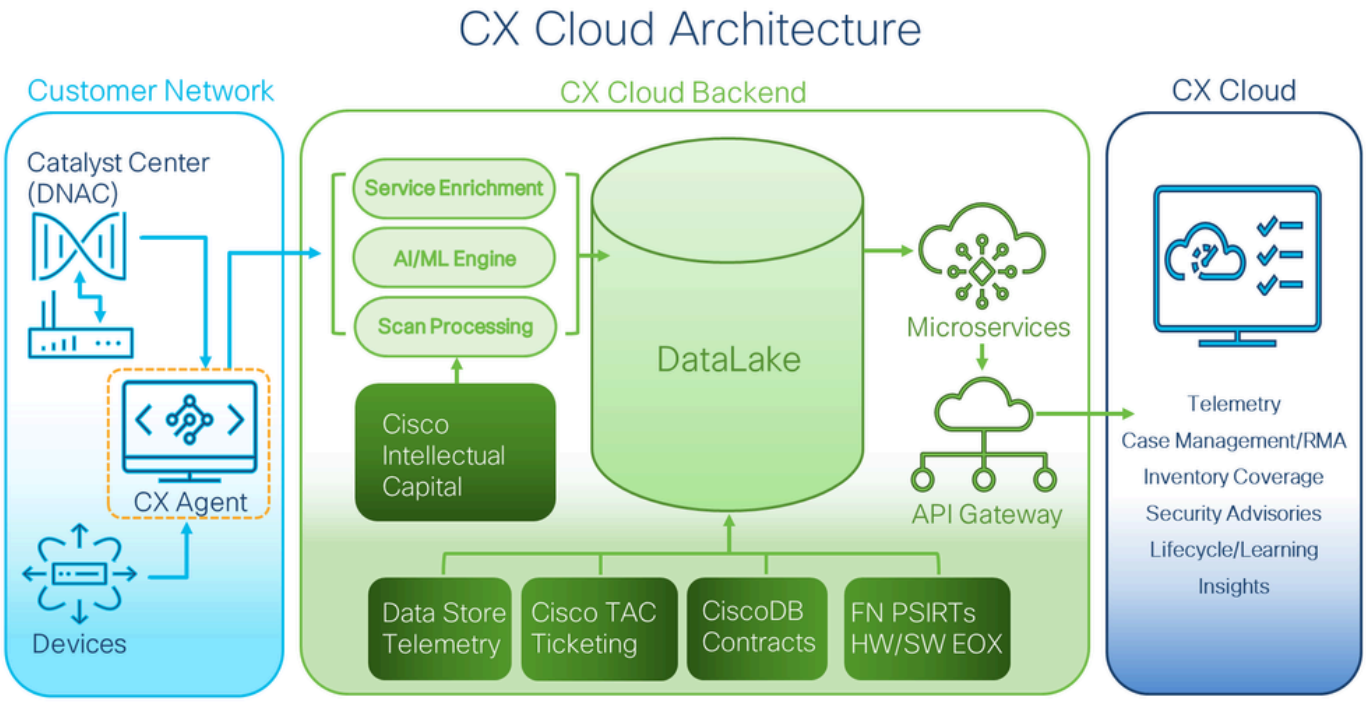
CX 에이전트 개요 가이드 v3.1

목차

소개

이 문서에서는 Cisco의 CX(Customer Experience) Agent에 대해 설명합니다. Cisco의 CX Agent는

확장성이 뛰어난 플랫폼으로 고객 네트워크 장치로부터 텔레메트리 데이터를 수집하여 고객에게 실행 가능한 통찰력을 제공합니다. CX Agent를 사용하면 AI(Artificial Intelligence)/ML(Machine Learning)에서 실행 중인 활성 구성 데이터를 CX 클라우드(Success Track, SNTC(Smart Net Total Care), BCS(Business Critical Services) 또는 LCS(Lifecycle Services) 제품 포함)에 표시되는 사전 대응적 및 예측 통찰력으로 변환할 수 있습니다.



CX 클라우드 아키텍처

이 설명서는 CX 클라우드 및 파트너 관리자만 사용할 수 있습니다. SUA(Super User Admin) 및 관리자 역할이 있는 사용자에게는 이 설명서에 설명된 작업을 수행하는 데 필요한 권한이 있습니다.

이 설명서는 CX Agent v3.1에만 적용됩니다. 이전 버전에 액세스하려면 Cisco CX Agent 페이지를 참조하십시오.

참고: 이 가이드의 이미지는 참조용으로만 제공됩니다. 실제 내용은 다를 수 있습니다.

사전 요구 사항

CX 에이전트는 VM(Virtual Machine)으로 실행되며 OVA(Open Virtual Appliance) 또는 VHD(Virtual Hard Disk)로 다운로드할 수 있습니다.

구축 요구 사항

- 새 설치를 수행하려면 다음 하이퍼바이저 중 하나가 필요합니다.
  - VMware ESXi v5.5 이상
  - Oracle Virtual Box v5.2.30 이상
  - Windows Hypervisor 버전 2012 - 2022 및 버전 2025
- 다음 표의 컨피그레이션은 VM 구축에 필요합니다.

CX 에이전트 구축 유형	CPU 코어 수	램	하드 디스크	*직접 최대 자산 수 CX 에이전트에 연결됨	지원되는 하이퍼바이저
작은 난자	8C	16GB	200GB	10,000	VMware ESXi, Oracle VirtualBox 및 Windows Hyper-V
중난자	16세기	32GB	600GB	20,000	VMware ESXi
큰 난자	섭씨 32도	64GB	1200GB	50,000:	VMware ESXi

*각 CX Cloud Agent 인스턴스에 대해 20개의 Cisco Catalyst Center(Catalyst Center) 비 클러스터 또는 10개의 Catalyst Center 클러스터를 연결하는 것 외에

참고:RADKit 서비스는 중대형 OVA 유형의 CX Agent 구축에만 사용할 수 있습니다.

- 지정된 미국 데이터 센터를 기본 데이터 영역으로 사용하여 CX 클라우드 데이터를 저장하는 고객의 경우, CX 에이전트가 FQDN(Fully Qualified Domain Name)을 사용하고 TCP 포트 443에서 HTTPS를 사용하여 여기에 표시된 서버에 연결할 수 있어야 합니다.
  - FQDN: agent.us.csco.cloud
  - FQDN: ng.acs.agent.us.csco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com
- 지정된 유럽 데이터 센터를 기본 데이터 영역으로 사용하여 CX 클라우드 데이터를 저장하는 고객의 경우: cx 에이전트는 FQDN을 사용하고 TCP 포트 443에서 HTTPS를 사용하여 여기에 표시된 두 서버 모두에 연결할 수 있어야 합니다.
  - FQDN: agent.us.csco.cloud
  - FQDN: agent.emea.csco.cloud
  - FQDN: ng.acs.agent.emea.csco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com
- CX 클라우드 데이터를 저장하기 위해 지정된 아시아 태평양 데이터 센터를 기본 데이터 영역으로 사용하는 고객의 경우: cx 에이전트는 FQDN을 사용하고 TCP 포트 443에서 HTTPS를 사용하여 여기에 표시된 두 서버 모두에 연결할 수 있어야 합니다.
  - FQDN: agent.us.csco.cloud
  - FQDN: agent.apjc.csco.cloud
  - FQDN: ng.acs.agent.apjc.csco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com
- 지정된 유럽 및 아시아 태평양 데이터 센터를 기본 데이터 지역으로 사용하는 고객의 경우, FQDN에 대한 연결: agent.us.csco.cloud는 초기 설정 중에 CX Cloud Agent를 CX Cloud에 등록하는 경우에만 필요합니다. CX Cloud Agent가 CX Cloud에 성공적으로 등록되면 이 연결은 더 이상 필요하지 않습니다.

- CX 클라우드 에이전트의 로컬 관리를 위해서는 포트 22에 액세스할 수 있어야 합니다.
- FQDN을 사용하는 RADKit 및 TCP 포트 443의 HTTPS를 사용하는 고객의 경우:
  - US FQDN: radkit.us.csco.cloud
  - EMEA FQDN: radkit.emea.csco.cloud
  - APJC FQDN radkit.apjc.csco.cloud
- RADKit가 서비스 요청에 출력을 연결하도록 하려면 CX Agent의 FQDN cxd.cisco.com에 액세스할 수 있어야 합니다.
- 다음 표는 CX Cloud Agent가 올바르게 작동하기 위해 열고 활성화해야 하는 포트 및 프로토콜에 대한 요약을 제공합니다.

CX Cloud Agent Traffic

Source	Destination	Protocol	Port	Purpose	Type
CX Cloud Agent	All regions: cloudsso.cisco.com api-cx.cisco.com agent.us.csco.cloud radkit.emea.csco.cloud Catalyst Center AMER region: ng.acs.agent.us.csco.cloud EMEA region: agent.emea.csco.cloud ng.acs.agent.emea.csco.cloud APJC region: agent.apjc.csco.cloud ng.acs.agent.apjc.csco.cloud	HTTPS	TCP/443	Initial configuration Upgrades Inventory & telemetry transfers Access to RADKit Cloud	Outbound to Cisco AWS regional data centers and Catalyst Center
CX Cloud Agent	Network Devices	SNMP	UDP/161	Initial discovery Ongoing inventory collections	Outbound to LAN
CX Cloud Agent	Network Devices	SSH	TCP/22	Collection of telemetry from CLI commands	Outbound to LAN
CX Cloud Agent	Network Devices	Telnet	TCP/23	Collection of telemetry from CLI commands	Outbound to LAN
Network Devices	CX Cloud Agent	Syslog	UDP/514	Transfer syslogs for Alert Fault Management	Inbound from LAN
Workstation	CX Cloud Agent	SSH	TCP/22	CX Cloud Agent Maintenance	Inbound from LAN

- VM 환경에서 DHCP(Dynamic Host Configuration Protocol)가 활성화된 경우 IP가 자동으로 탐지됩니다. 그렇지 않으면 사용 가능한 IPv4 주소, 서브넷 마스크, 기본 게이트웨이 IP 주소 및 DNS(Domain Name Service) 서버 IP 주소를 사용할 수 있어야 합니다.
- IPv4만 지원됩니다.
- 인증된 단일 노드 및 HA(High Availability) 클러스터 Catalyst Center 버전은 2.1.2.x~2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x와 Catalyst Center Virtual Appliance 및 Catalyst Center Virtual Appliance입니다.
- 네트워크에 SSL 가로채기가 있는 경우 permit-list CX Agent의 IP 주소.
- 직접 연결된 모든 자산의 경우 SSH 권한 레벨 15가 필요합니다.
- 제공된 호스트 이름만 사용하십시오. 고정 IP 주소를 사용할 수 없습니다.

중요 도메인 액세스

CX Cloud 여정을 시작하려면 사용자가 다음 도메인에 액세스해야 합니다. 제공된 호스트 이름만 사용하십시오. 고정 IP 주소를 사용하지 마십시오.

CX 에이전트 포털 관련 도메인

주요 도메인	기타 도메인

csco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

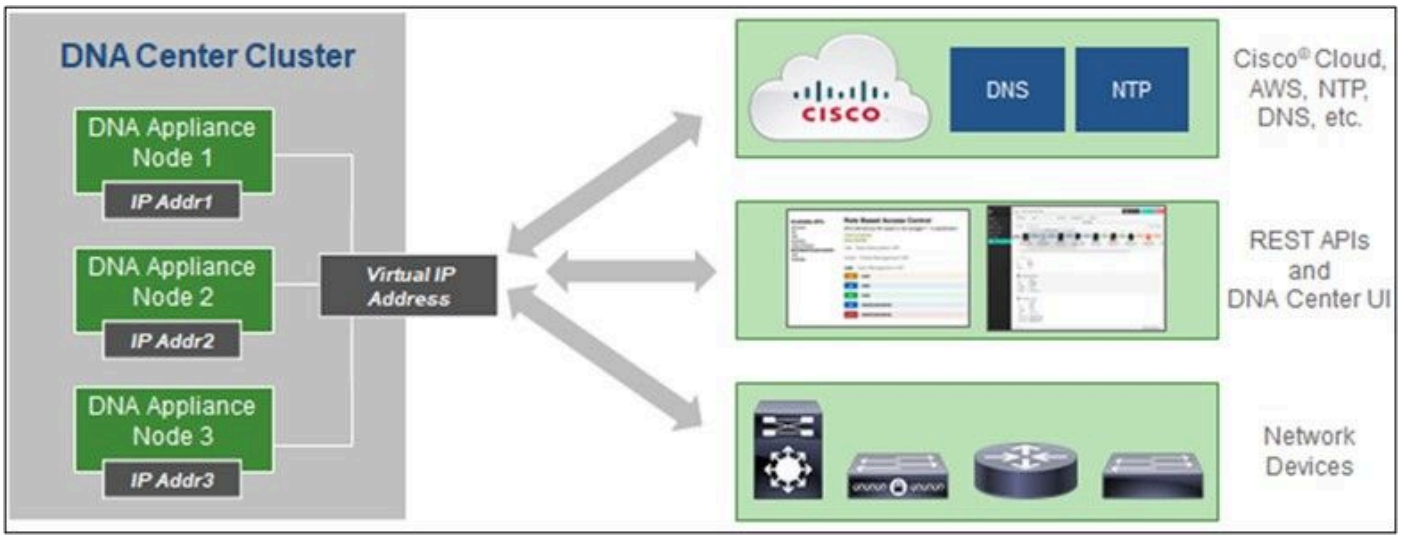
CX 에이전트 OVA 관련 도메인

AMERICA	EMEA	APJC
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.csco.cloud	agent.us.csco.cloud	agent.us.csco.cloud
ng.acs.agent.us.csco.cloud	agent.emea.csco.cloud	agent.apjc.csco.cloud
	ng.acs.agent.emea.csco.cloud	ng.acs.agent.apjc.csco.cloud

참고: 아웃바운드 액세스는 지정된 FQDN에 대해 포트 443에서 활성화된 리디렉션으로 허용되어야 합니다.

Catalyst Center 지원 버전

지원되는 단일 노드 및 HA Cluster Catalyst Center 버전은 2.1.2.x~2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x와 Catalyst Center Virtual Appliance 및 Catalyst Center Virtual Appliance입니다.



다중 노드 HA 클러스터 Cisco DNA Center

지원되는 브라우저

Cisco.com에 대한 최상의 경험을 위해 이러한 브라우저의 최신 공식 릴리스를 권장합니다.

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

지원되는 제품 목록

CX Agent에서 지원하는 제품 목록을 보려면 지원되는 제품 목록을 참조하십시오.

CX Agent v3.1 업그레이드/설치

- 새 버전으로 업그레이드하는 기존 고객은 CX Agent v3.1 업그레이드를 참조하십시오.
- 새로운 Flexible OVA v3.1 설치를 구현하는 신규 고객은 CX Agent 추가를 참조해야 합니다.

기존 VM을 대규모 및 중간 구성으로 업그레이드

고객은 네트워크 크기 및 복잡성을 기반으로 유연한 OVA 옵션을 사용하여 기존 VM 컨피그레이션을 중간 또는 대규모로 업그레이드할 수 있습니다.

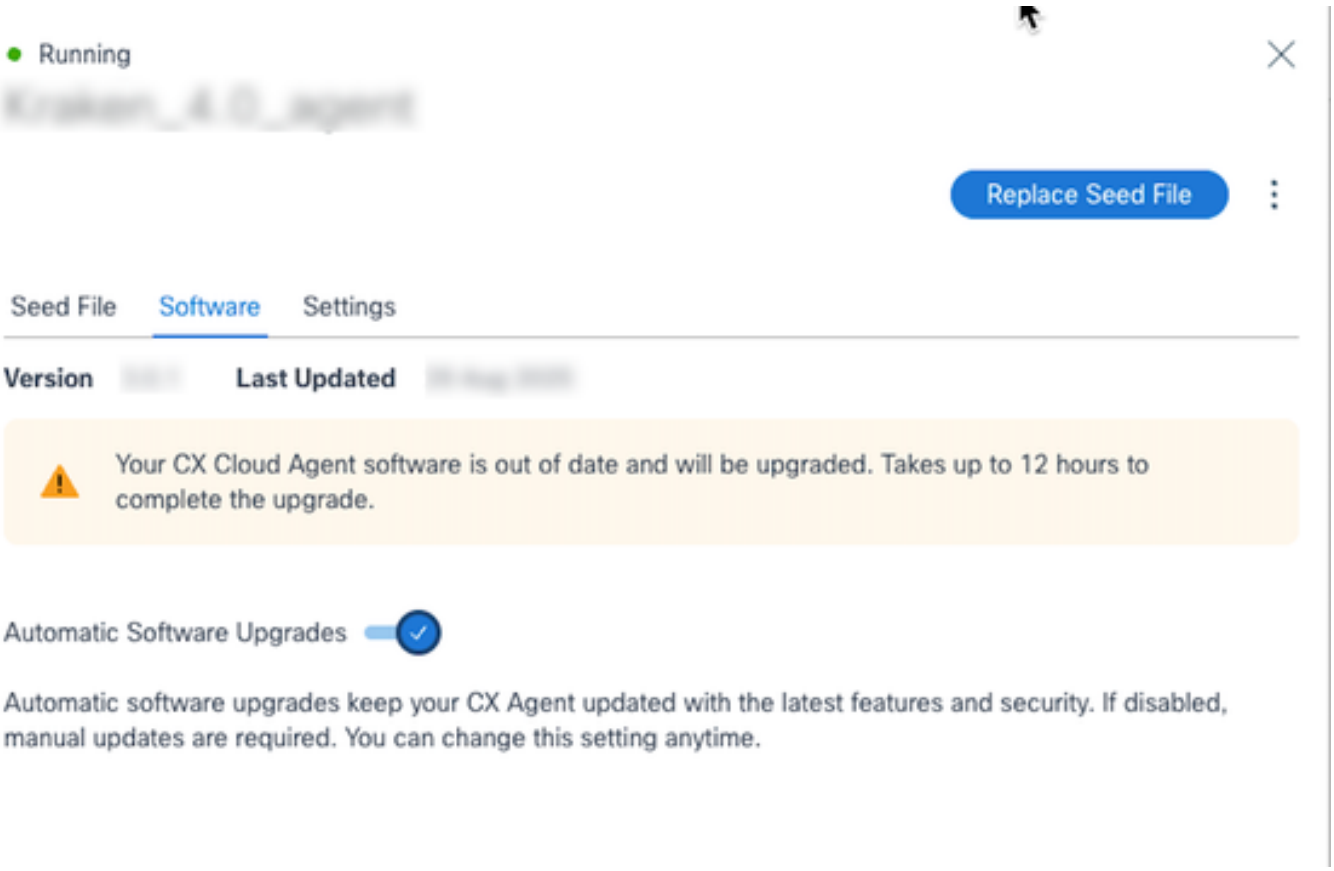
기존 VM 컨피그레이션을 Small에서 Medium 또는 Large로 업그레이드하려면 CX Agent VM을 Medium and Large 컨피그레이션으로 업그레이드 섹션을 참조하십시오.

CX Agent v3.1로 업그레이드

기존 고객은 자동 업그레이드를 활성화하거나 기존 버전에서 수동으로 업그레이드하도록 선택하여 최신 버전으로 업그레이드할 수 있습니다.

자동 업그레이드

고객은 새 버전이 릴리스될 때 시스템이 업데이트되도록 자동 소프트웨어 업그레이드 토글을 활성화할 수 있습니다. 이 옵션은 새 설치에 기본적으로 활성화되어 있지만, 회사 정책에 맞게 조정하거나 계획된 유지 관리 기간 동안 업그레이드를 예약하기 위해 언제든지 수정할 수 있습니다.



자동 업그레이드

참고: 자동 업그레이드는 기존 CX 에이전트 인스턴스에 대해 기본적으로 비활성화되어 있지만 사용자는 언제든지 활성화할 수 있습니다.

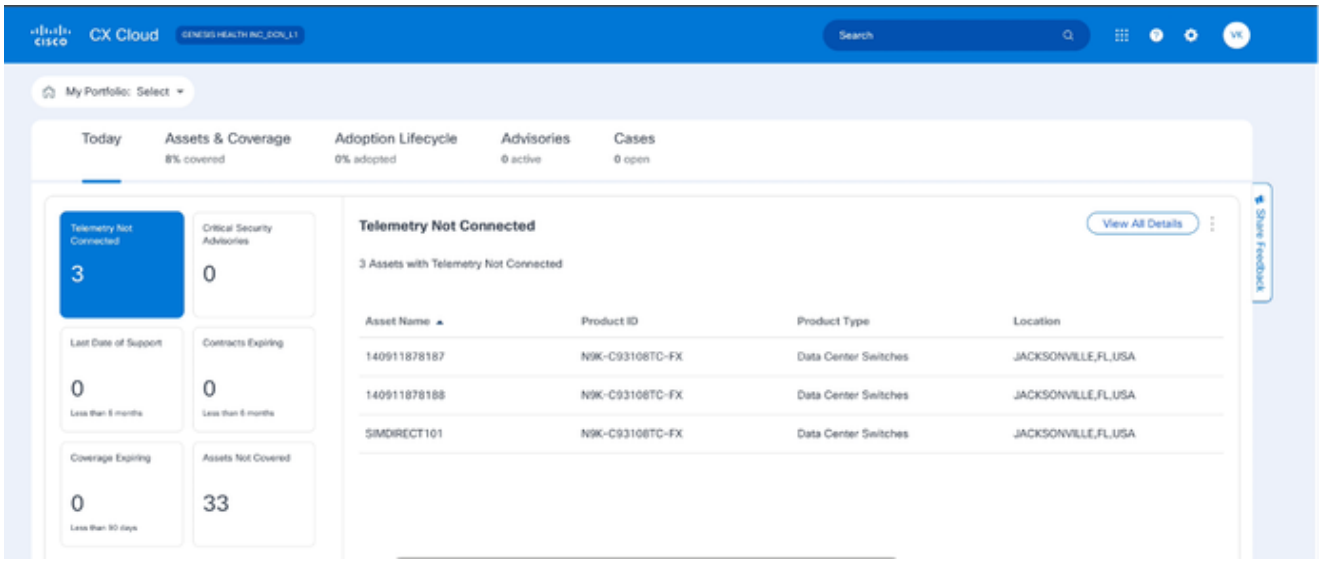
수동 업그레이드

자동 업그레이드를 사용하지 않고 자동 소프트웨어 업그레이드를 활성화하지 않은 고객은 수동으로 업그레이드할 수 있습니다. CX Agent v2.4.x 이상은 이 섹션에 설명된 단계에 따라 v3.1로의 직접 업그레이드를 지원합니다.

참고: CX Agent v2.3.x 이하 버전의 고객은 v3.1로 업그레이드하거나 신규 OVA 설치를 수행하기 전에 v2.4.x로 점진적으로 업그레이드해야 합니다.

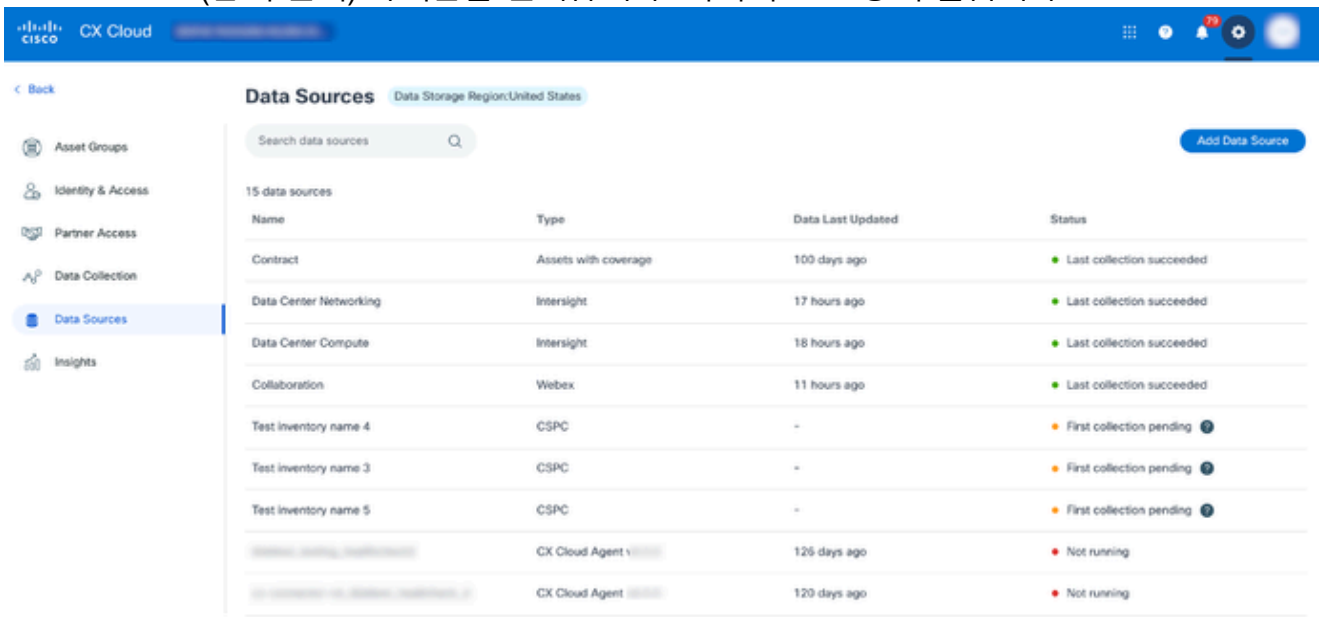
CX Cloud에서 CX Agent 업그레이드 v3.1을 설치하려면

1. CX 클라우드에 로그인합니다. 홈 페이지가 표시됩니다.



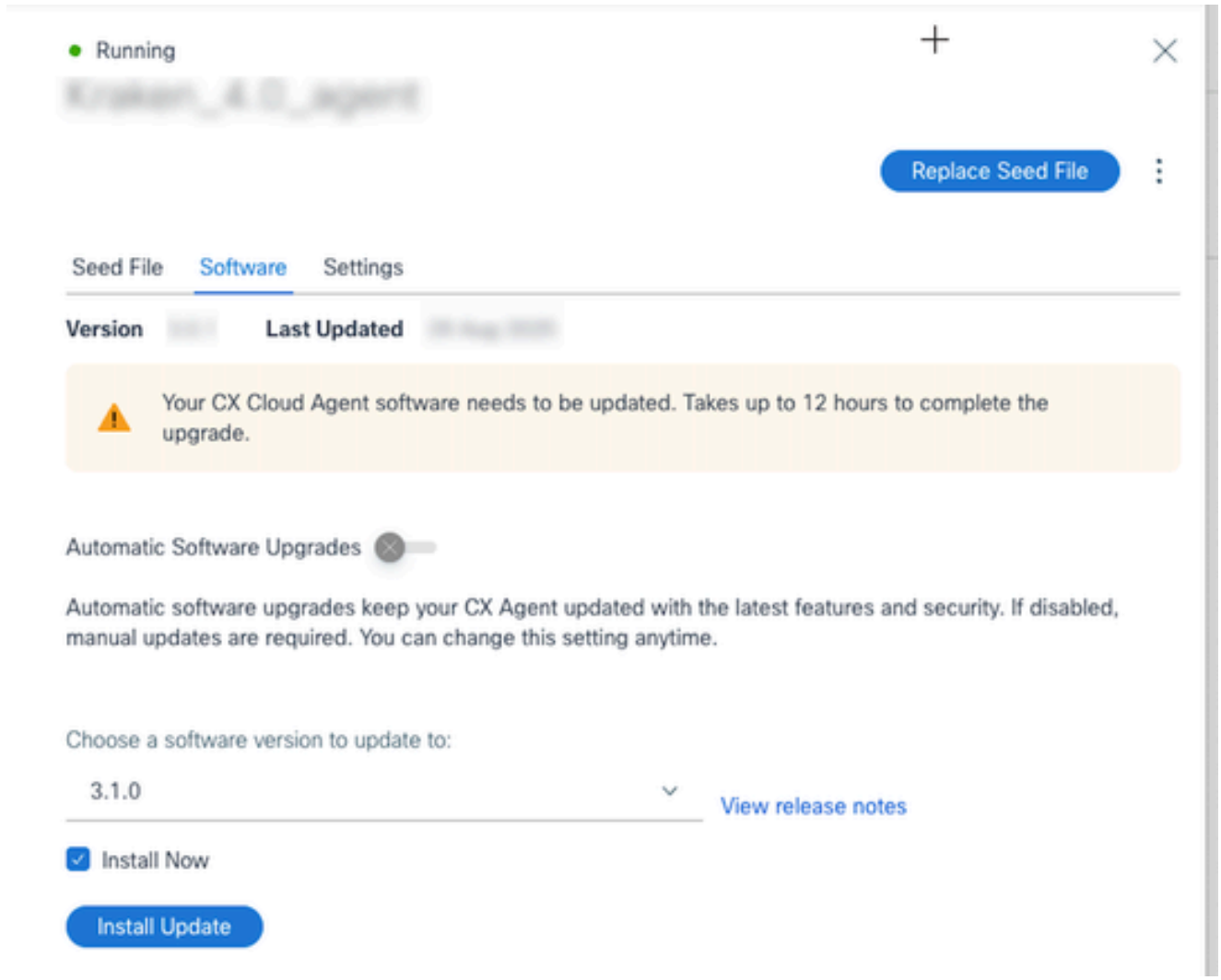
CX 클라우드 홈 페이지

2. Admin Center(관리 센터) 아이콘을 선택합니다. 데이터 소스 창이 열립니다.



데이터 소스

3. CX Agent Data Source(CX 에이전트 데이터 소스)를 클릭합니다. CX Agent 세부 정보 창이 열립니다.



수동 업그레이드

4. Choose a software version to update(업데이트할 소프트웨어 버전 선택) 드롭다운 목록에서 소프트웨어 버전 3.1.0을 선택합니다.
5. CX Agent v3.1을 설치하려면 Install Update(업데이트 설치)를 클릭합니다.

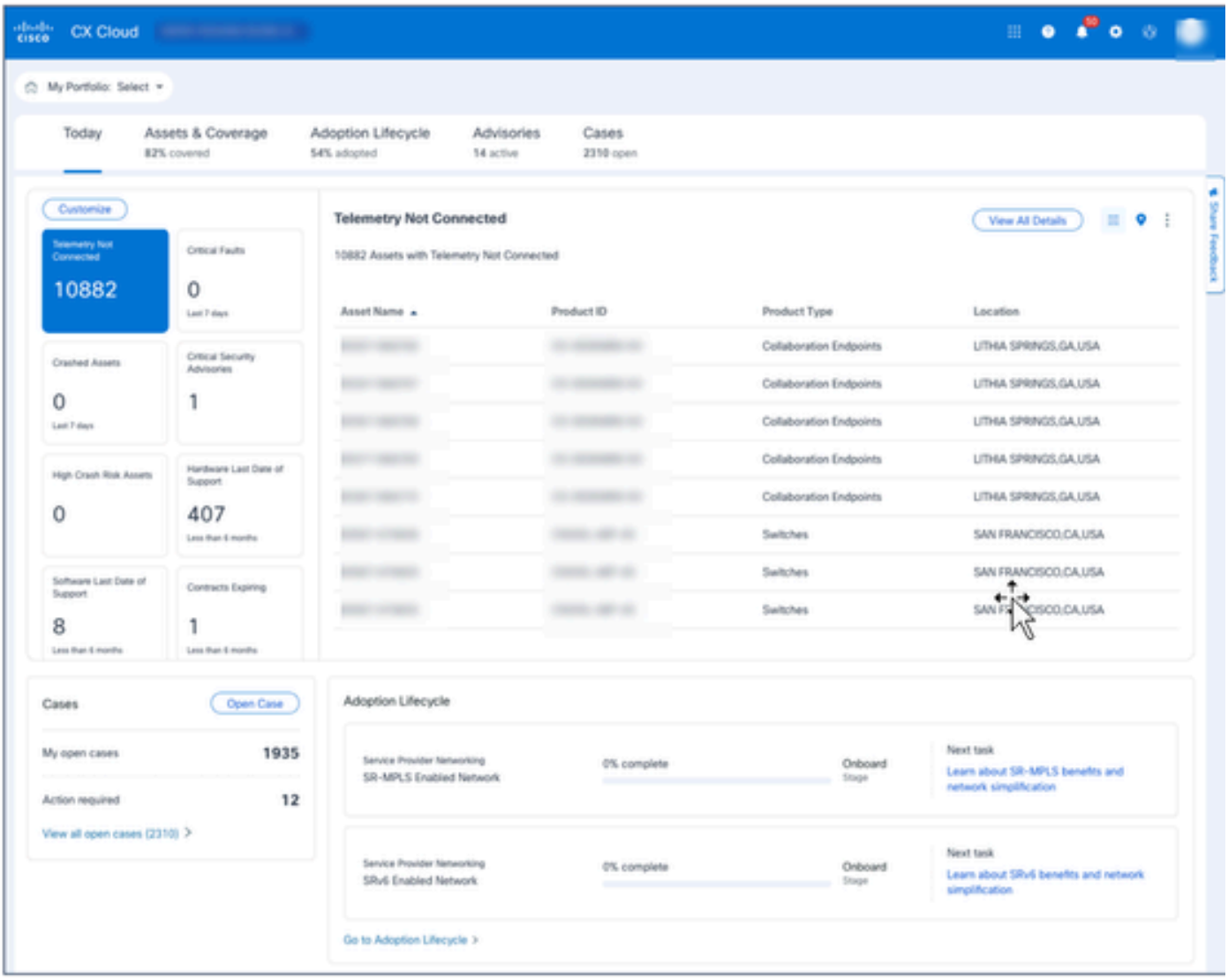
참고: 고객은 예약 옵션을 표시하는 Install Now(지금 설치) 확인란의 선택을 취소하여 업데이트를 나중에 예약할 수 있습니다.

CX 에이전트 추가

고객은 CX 클라우드에서 최대 20개의 CX 에이전트 인스턴스를 추가할 수 있습니다.

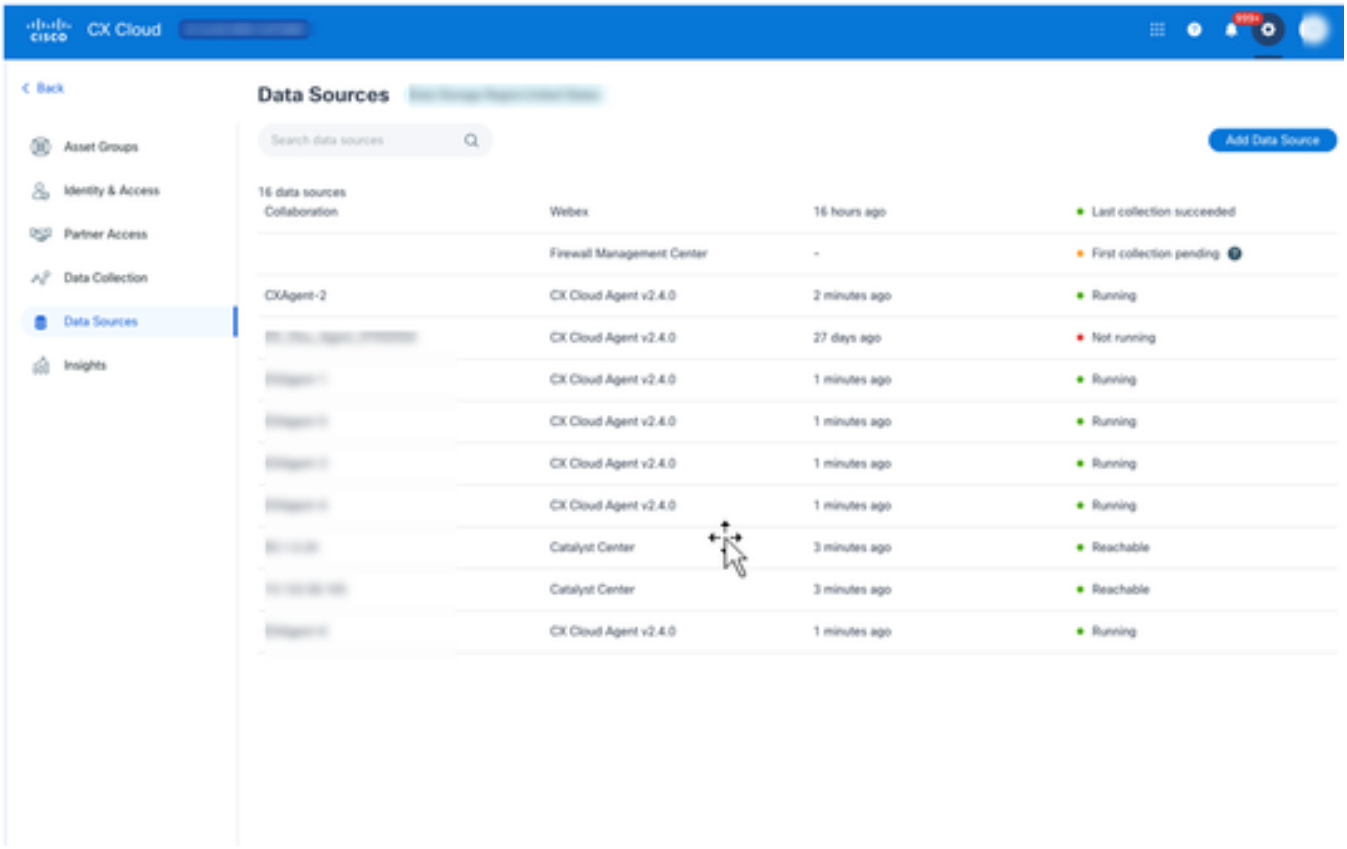
CX 에이전트를 추가하려면

1. CX 클라우드에 로그인합니다. 홈 페이지가 표시됩니다.



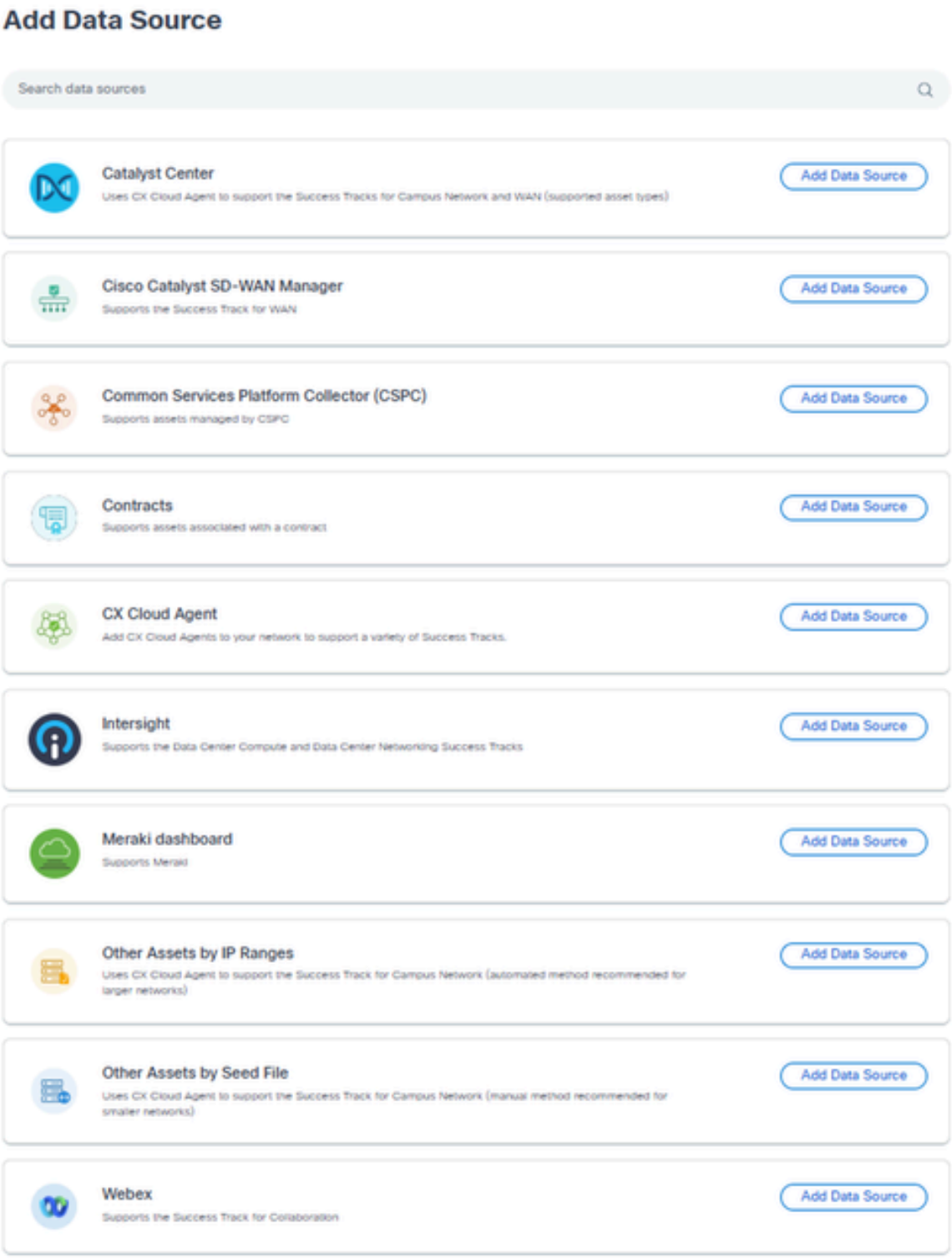
CX 클라우드 홈 페이지

2. Admin Center(관리 센터) 아이콘을 선택합니다. 데이터 소스 창이 열립니다.



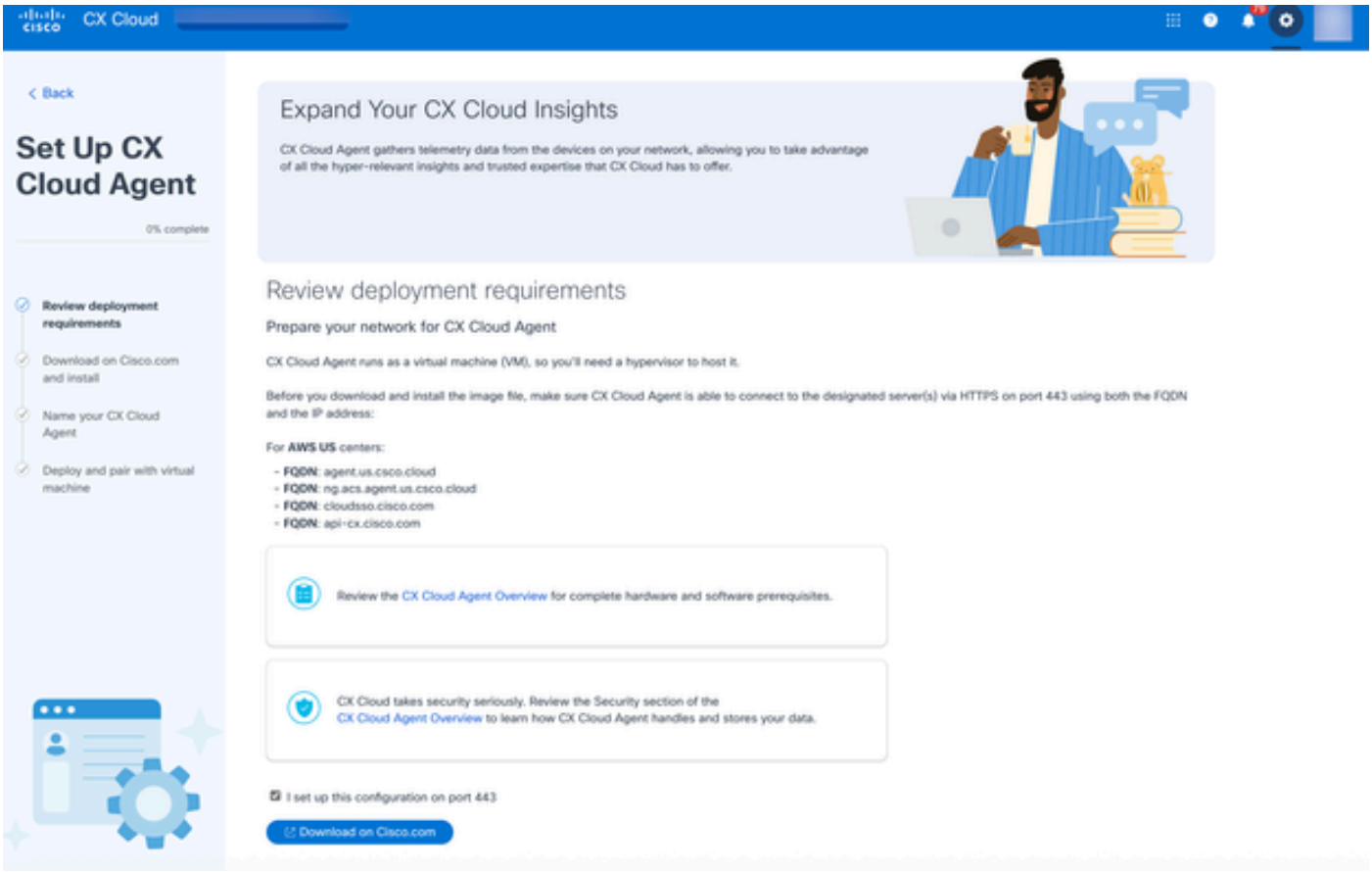
데이터 소스

3. 데이터 소스 추가를 클릭합니다. 데이터 소스 추가 페이지가 열립니다. 표시되는 옵션은 고객 서브스크립션에 따라 달라집니다.



데이터 원본 추가

4. CX 에이전트 옵션에서 데이터 소스 추가를 클릭합니다. Set Up CX Agent 창이 열립니다.



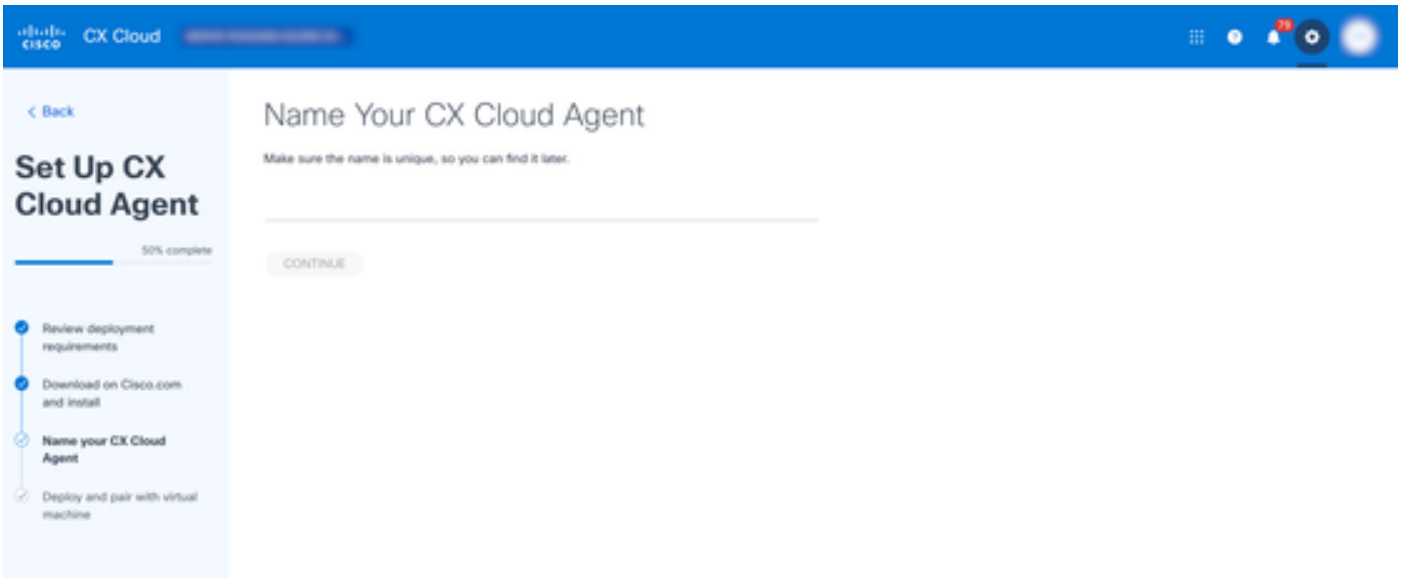
CX 에이전트 추가

5. Review deployment requirements(구축 요구 사항 검토) 섹션을 검토하고 I set up this configuration on port 443(포트 443에서 이 컨피그레이션을 설정함) 확인란을 선택합니다.
6. Cisco.com에서 다운로드를 클릭합니다. 다른 탭에서 소프트웨어 다운로드 창이 열립니다.
7. "CX Agent v3.1.0 OVA" 파일을 다운로드합니다.

참고: CX 에이전트 설정을 완료하는 데 필요한 페어링 코드는 "OVA" 파일을 배포한 후에 생성됩니다.

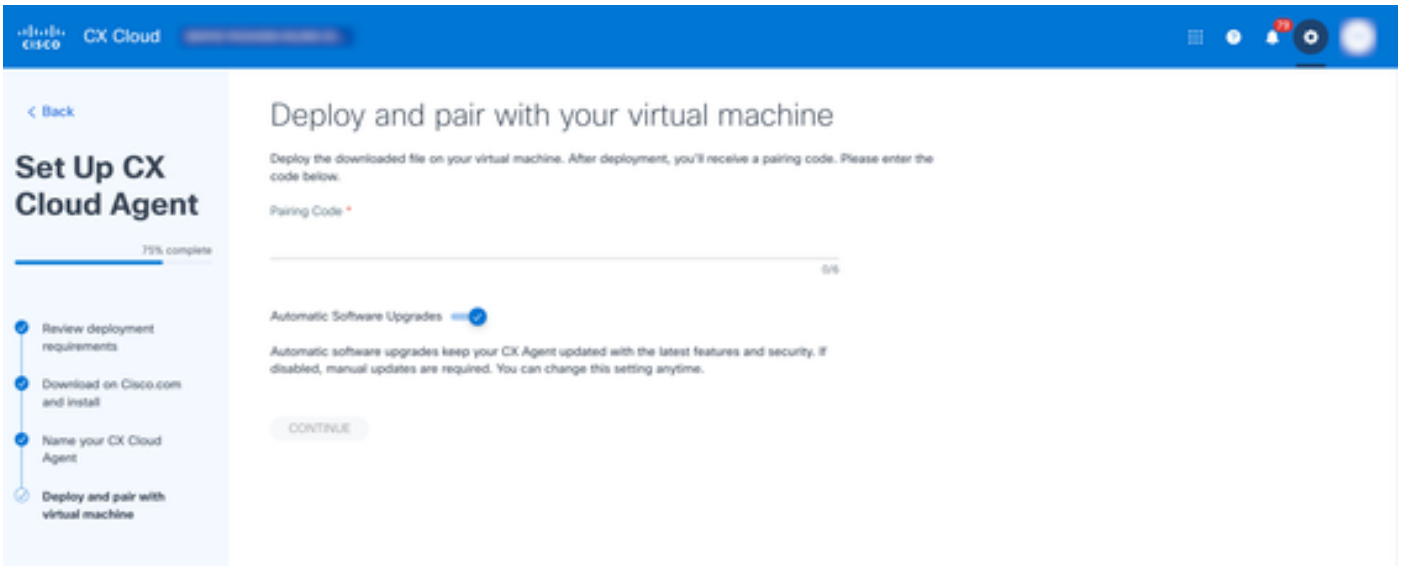
---

8. Name Your CX Cloud Agent(CX 클라우드 에이전트 이름) 필드에 CX 에이전트 이름을 입력합니다.



이름 CX 에이전트

9. 계속을 클릭합니다. Deploy and pair with your virtual machine 창이 열립니다.



페어링 코드

10. 다운로드한 "OVA" 파일을 배포한 후 받은 페어링 코드를 입력합니다.

11. 계속을 클릭합니다. 등록 진행률이 표시되고 확인 메시지가 나타납니다.

참고: 추가 CX 에이전트 인스턴스를 데이터 소스로 추가하려면 위 단계를 반복합니다.

BCS/LCS용 CX 에이전트 구성

Cisco의 새로운 Converged Collection 기능은 BCS/LCS에 대한 CX Agent v3.1 구성을 간소화하여 고객 경험을 간소화합니다.

참고:이 컨피그레이션은 BCS/LCS 고객의 컬렉터 설정을 담당하는 Cisco 지원 엔지니어에만

적용됩니다.

BCS/LCS 고객은 CX Cloud Community를 방문하여 사용자 온보딩 및 기타 관련 정보에 대해 자세히 알아볼 수 있습니다.

사전 요구 사항

SUA(Super User Administrator) 및 관리자 액세스 권한을 가진 지원 엔지니어는 BCS/LCS에 대한 CX 에이전트 컨피그레이션만 수행할 수 있습니다.

CX 에이전트 구성

BCS/LCS용 CX 에이전트를 구성하려면 Cisco 지원에 문의하십시오.

RADKit 기능 구성

CX Agent v3.1은 CX Cloud에서 Cisco 디바이스의 원격 관리 및 문제 해결을 향상시키도록 설계된 선택적 RADKit 컨피그레이션을 제공합니다. 활성화되면 인증된 사용자는 원격으로 데이터 캡처, 구성 및 소프트웨어 업그레이드와 같은 작업을 안전하게 수행할 수 있습니다. 이러한 설정은 고객의 운영 요구 사항에 따라 언제든지 활성화 또는 비활성화할 수 있습니다.

RADKit에 대한 자세한 내용은 Cisco RADKit를 참조하십시오.

CLI를 통한 RADKit 클라이언트 통합

RADKit 클라이언트 서비스를 통합하려면 관리자 계정을 만들고 다음 단계를 완료하여 서비스를 등록합니다.

참고: 다음 단계에서는 CX 에이전트 VM에 대한 루트 액세스가 필요합니다.

1. 터미널과 SSH(Secure Shell)를 적절한 자격 증명을 사용하여 VM에 엽니다. 예를 들면 다음과 같습니다.

```
ssh your_username@your_vm_ip
```

2. 다음 명령을 실행하여 네트워크 연결을 활성화합니다.

```
kubectl get netpol deny-from-other-namespaces -o yaml >
/home/cxcadmin/deny-from-other-namespaces.yaml

kubectl delete netpol deny-from-other-namespaces
```

3. 로컬 시스템에서 관리자 계정을 만들기 위해 관리자 엔드포인트에 POST 요청을 보냅니다. 요청 본문에는 다음이 포함되어야 합니다.

- admin_name(필수): 관리자 계정의 사용자 이름
- 이메일(선택 사항): 관리자 계정의 전자 메일 주소

- full_name(선택 사항): 관리자의 전체 이름입니다.
- 설명(선택 사항): 관리자 계정에 대한 설명

다음 예는 cURL을 사용하여 이 요청을 전송하는 방법을 보여줍니다.

```
curl -X POST \

  http://<your_vm_ip>:30100/radkitmanager/v1/createAdmin \

  -H "콘텐츠 형식: application/json" \

  -d '{

        "admin_name": "admin_user123",

        "이메일": "admin@example.com",

        "전체 이름": "관리자 사용자",

        "설명": "시스템 관리를 위한 관리자 계정"

      }'
```

관리자 계정이 생성되면 서버는 관리자 계정이 성공적으로 생성되었음을 나타내는 확인 메시지로 응답합니다. 이 응답에는 첫 번째 로그인 시 변경해야 하는 임시 비밀번호도 포함됩니다. 그러나 관리자 계정이 이미 있으면 서버는 "Admin already created" 메시지와 함께 400 상태 코드를 반환합니다.

4. 웹 브라우저를 열고 RADKit 웹 UI로 이동합니다. https://<your_vm_ip>:30101/.
5. 관리자 사용자 이름(admin_name) 및 응답에 제공된 임시 비밀번호를 사용하여 로그인합니다.

참고: 처음 로그인하면 비밀번호를 변경하라는 메시지가 표시됩니다. 지침에 따라 새 비밀번호를 설정합니다.

---

6. 로컬 컴퓨터에서 RADKit 클라이언트를 실행하여 서비스를 등록합니다.
7. 인증 후 다음 명령을 실행하여 일회용 비밀번호를 생성합니다.

```
grant_service_otp()
```

8. 로컬 시스템에서 관리자 엔드포인트로 POST 요청을 전송하여 서비스를 등록합니다. 요청 본문에는 다음이 포함되어야 합니다.

- OTP(필수): 1회 비밀번호 문자열

다음 예는 cURL을 사용하여 이 요청을 전송하는 방법을 보여줍니다.

```
curl -X POST \

  http://<your_vm_ip>:30100/radkitmanager/v1/enrollService \
```

```
  -H "콘텐츠 형식: application/json" \

  -d '{

        "one_time_password": "PROD1234-1234-1234"

      }'
```

등록이 완료되면 확인 메시지가 표시되고 사용자는 관리자 계정을 사용하여 RADKit 서비스를 관리할 수 있습니다.

네트워크 연결을 비활성화하려면 다음 명령을 실행합니다.

```
kubectl apply -f /home/cxcadmin/deny-from-other-namespaces.yaml
```

기존 CX 에이전트에 대한 볼트(Vault) 구성

선택적 저장소 구성 기능을 사용하면 CX Cloud에서 최신 자격 증명을 사용하여 토큰 및 인벤토리 목록과 같은 중요한 데이터에 액세스하기 위해 저장소 서비스에 안전하게 연결할 수 있습니다. 활성화되면 CX 클라우드는 구성된 주소 및 토큰을 자동으로 사용합니다. 이 설정은 언제든지 활성화 또는 비활성화할 수 있습니다. 현재 HashiCorp의 보관소 컨피그레이션만 지원됩니다.

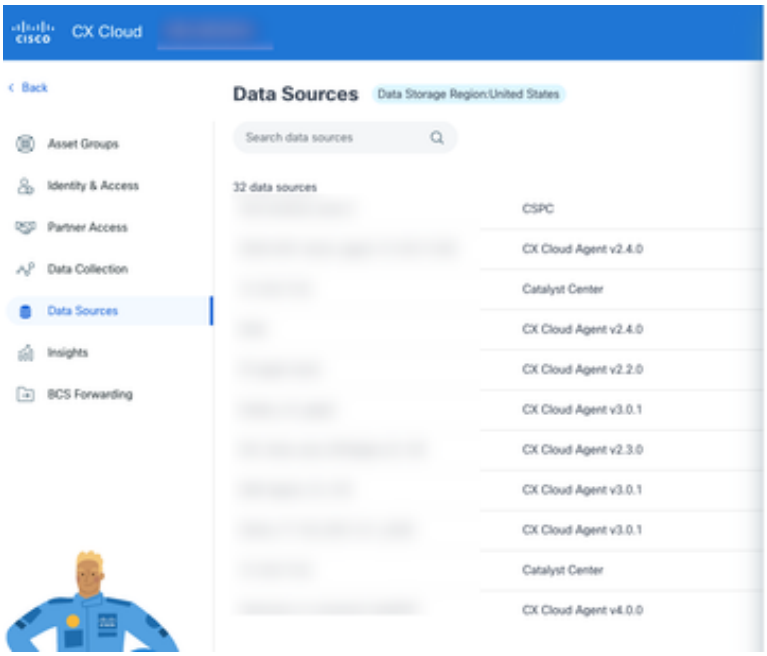
자격 증명 모음은 두 가지 방법으로 구성할 수 있습니다.

- CX 클라우드 UI를 통해
- CLI를 통해

CX 클라우드 UI에서 HashiCorp Vault 구성

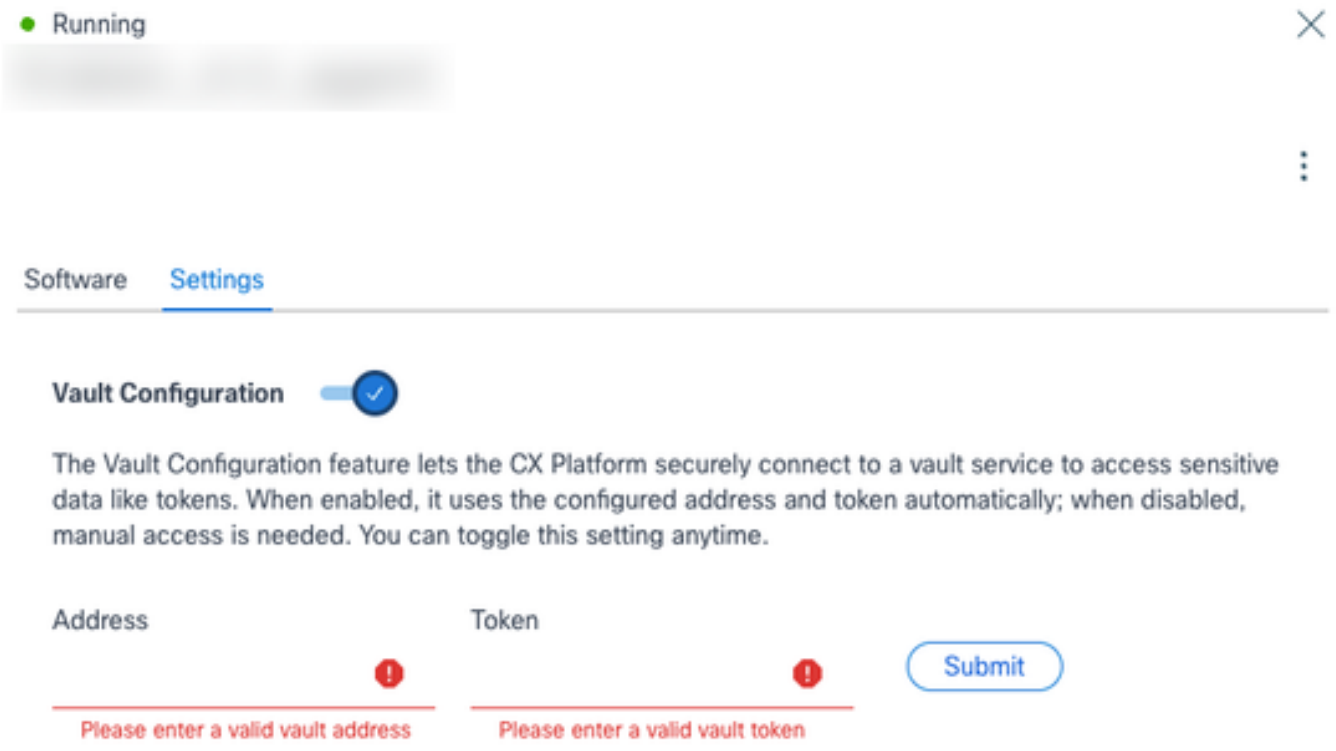
기존 CX Agent에 대해 HashiCorp 볼트를 구성하려면

1. Admin Center(관리 센터) 아이콘을 선택합니다. 데이터 소스 창이 열립니다.
2. CX 에이전트 데이터 소스를 클릭합니다. CX Agent 세부 정보 창이 열립니다.



설정

3. Settings(설정) 탭을 클릭합니다.
4. 보관소 구성 토글을 활성화합니다.



보관소 구성

5. 주소 및 토큰 필드에 상세내역을 입력합니다.

6. 제출을 클릭합니다. 확인 및 추가된 IP 주소가 표시됩니다.

고객은 Remove(제거)를 클릭하여 구성된 자격 증명 모음을 제거할 수 있습니다.

CLI를 통해 CX 에이전트를 HashiCorp Vault와 통합

이 섹션에서는 Cisco CX Agent와 HashiCorp Vault 인스턴스 간의 연결을 구성하는 절차를 간략하게 설명합니다. 이러한 통합을 통해 장치 자격 증명을 안전하게 저장하고 검색할 수 있으므로 전반적인 보안 상태가 향상됩니다.

사전 요구 사항

- cx 에이전트 VM에 대한 cxcroot 액세스
- 실행 중이며 액세스 가능한 저장소 인스턴스

HashiCorp Vault와 통합

- 저장소 통합을 활성화하려면 다음 명령을 실행합니다.

`cxcli 상담원 자격 증명 모음`

- 저장소 통합을 비활성화하려면 다음 명령을 실행합니다.

`cxcli 에이전트 볼팅 오프`

- 현재 자격 증명 모음 통합 상태를 확인하려면 다음 명령을 실행합니다.

`cxcli 에이전트 자격 증명 모음 상태`

HashiCorp 볼트(Vault) 통합 활성화

저장소 통합을 활성화하려면 다음을 수행합니다.

1. CX 에이전트에 액세스하려면 cxcroot 사용자 계정을 사용하여 SSH를 통해 CX 에이전트에 로그인합니다.
2. 다음 명령을 실행하여 권한을 높이려면 root 사용자로 전환합니다.

수도수

3. 다음 명령을 실행하여 현재 저장소 통합 상태를 확인합니다.

`root@cxcloudagent: /home/cxcroot# cxcli 상담원 자격 증명 모음 상태`

자격 증명 모음 통합 사용 안 함

4. 다음 명령을 실행하여 저장소 통합을 활성화합니다.

`cxcli 상담원 자격 증명 모음`

5. 다음 필드를 갱신합니다.

- 저장소 주소
- 저장소 루트 토큰

6. 확인하려면 자격 증명 모음과의 통합 상태를 확인하십시오. 응답 메시지는 통합이 활성화되었는지 확인해야 합니다.

`root@cxcloudagent: /home/cxcroot# cxcli 에이전트 자격 증명 모음`

`HashiCorp Vault Address`를 입력합니다.

`HashiCorp 자격 증명 모음 토큰 입력:`

`볼트(vault) 통합 사용 root@cxcloudagent: /home/cxcroot#`

HashiCorp 볼트(Vault) 통합 비활성화

CX Agent에 액세스하려면

1. cxcroot 사용자 계정을 사용하여 SSH를 통해 CX 에이전트에 로그인합니다.
2. 다음 명령을 실행하여 권한을 높이려면 root 사용자로 전환합니다.

수도수

3. 다음 명령을 실행하여 HashiCorp 볼트(Vault) 통합을 비활성화합니다.

`root@cxcloudagent: /home/cxcroot# cxcli 에이전트 볼팅 오프`

자격 증명 모음 통합 사용 안 함

`root@cxcloudagent: /home/cxcroot# |`

하시코프 자격 증명 모음 장치 자격 증명 스키마

자격 증명 모음 스키마: 사용 가능한 옵션 및 디바이스 자격 증명에 지원되는 필드에 대한 자세한 내용은 "자격 증명 모음 스키마" 파일(vault-credentials-schema.json)을 다운로드하십시오.

예: 다음은 스키마를 기반으로 하는 JSON 자격 증명의 예입니다.

-

```
{
"targetIp": "5.0.1.*",
"credentials": {
"snmpv3": {
"user": "cisco",
"authPassword": "*******",
"authAlgorithm": "MD5",
"privacyPassword": "*******",
"privacyAlgorithm": "AES-256"
},
"telnet": {
"user": "cisco",
"password": "*******",
```

```
"enableUser": "cisco",
"enablePassword": "*******"
}
}
}
```

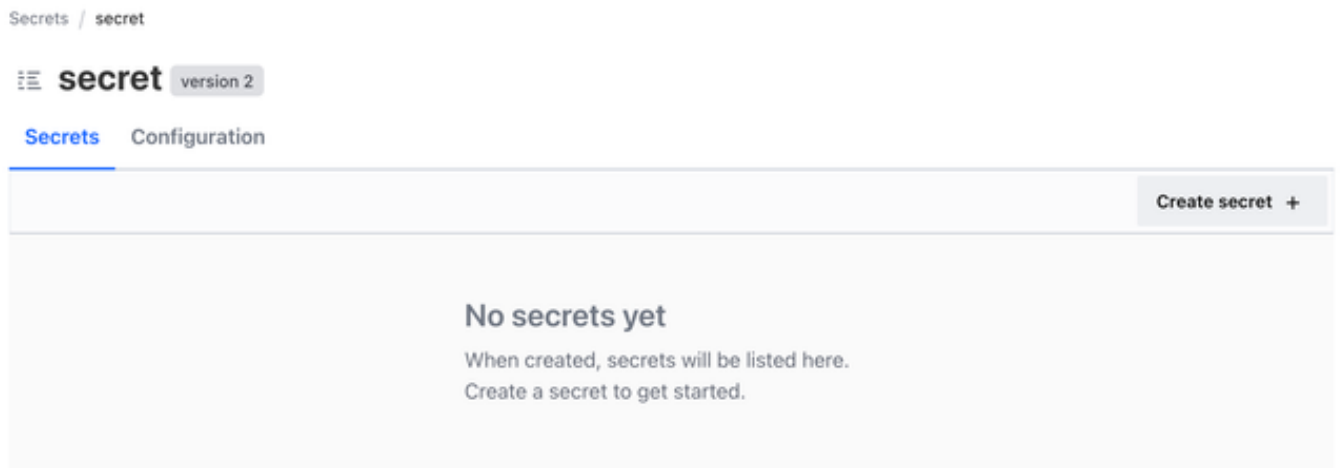
참고:사용자는 단일 자격 증명 JSON 파일 내에서 여러 프로토콜을 지정할 수 있습니다. 그러나 동일한 패밀리의 중복 프로토콜은 포함하지 마십시오(예: 동일한 자격 증명 파일에 SNMPv2c 및 SNMPv3 모두 포함하지 않음).

HashiCorp 자격 증명 모음에서 디바이스 자격 증명 구성(처음으로)

1. Vault 인스턴스에 로그인합니다.

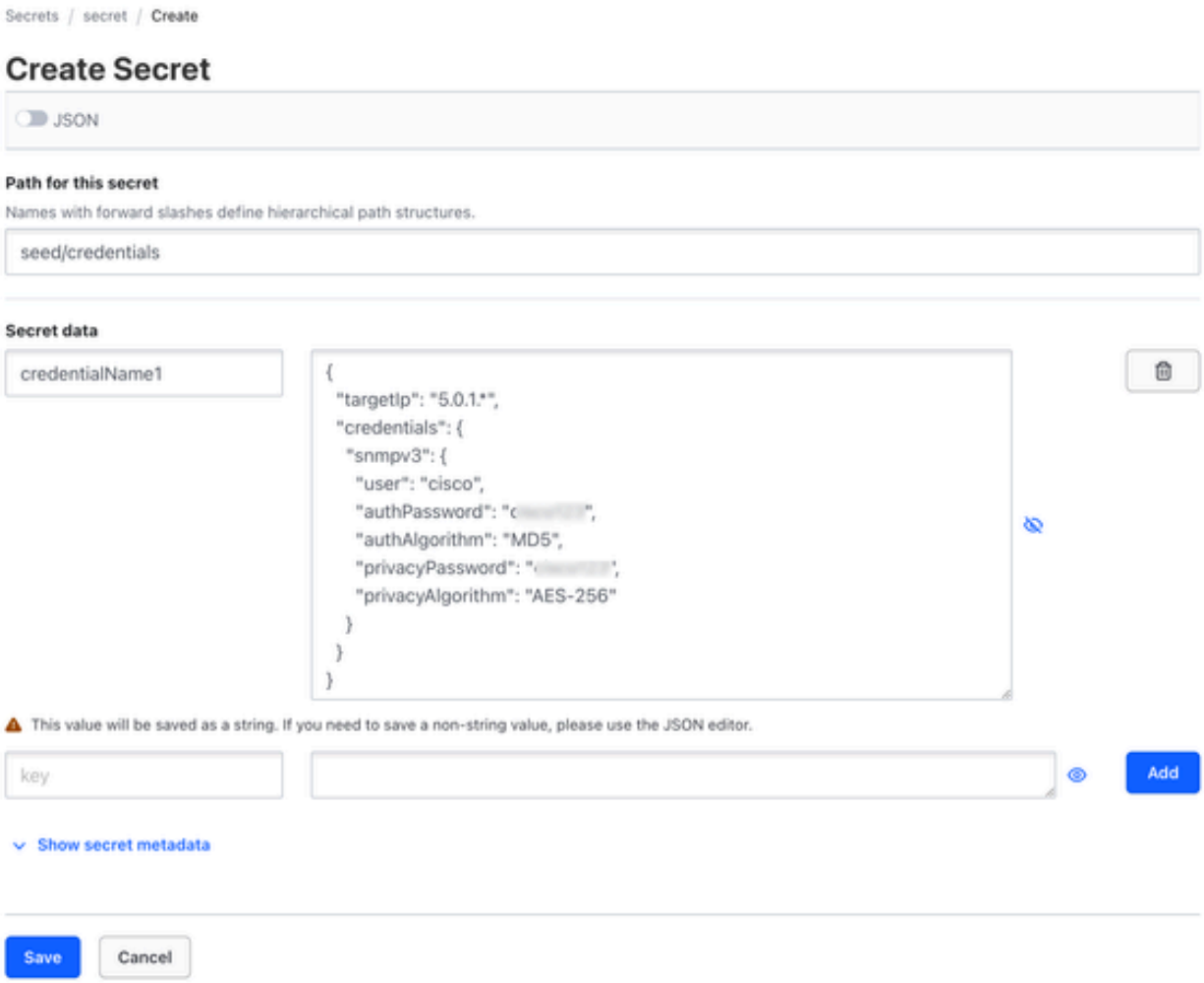
비밀

2. 다음 경로를 사용하여 새 키 값 암호를 만듭니다. 암호/시드/자격 증명.
3. key-value secret storage engine(secret/)을 선택합니다.



키 값 암호

4. Create secret(암호 생성)을 클릭합니다. Create Secret 창이 열립니다.

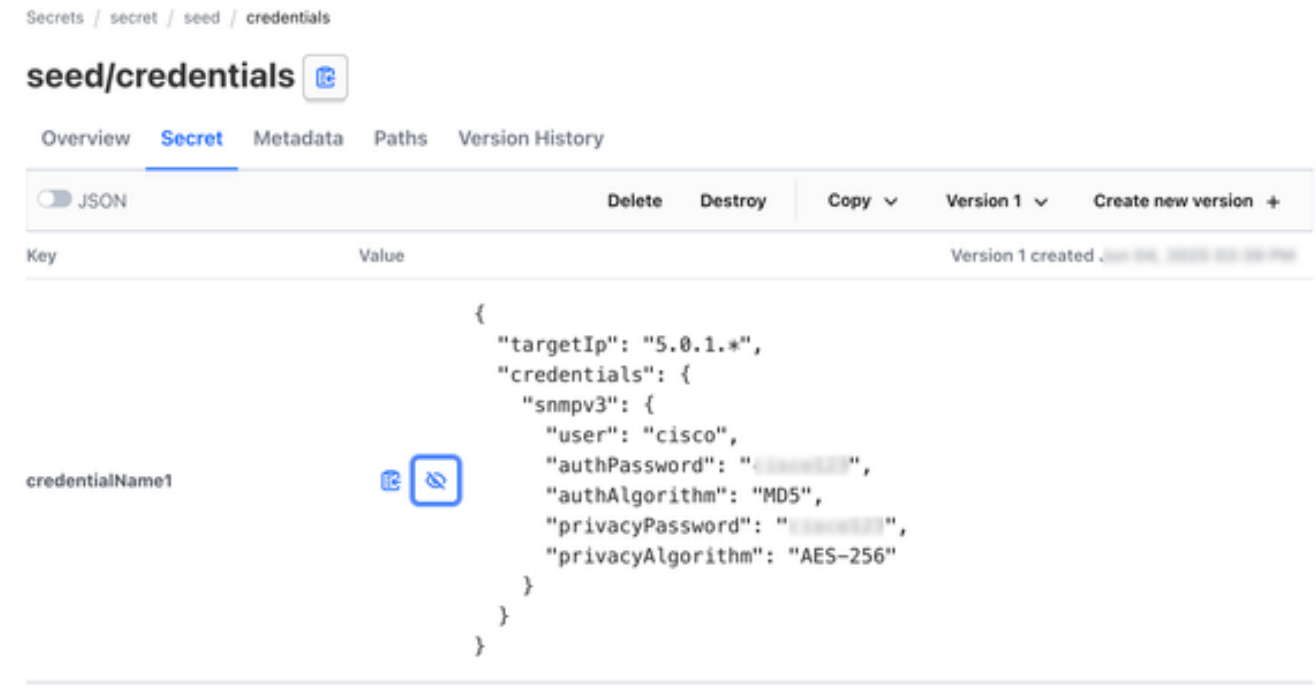


클라이언트 암호

5. 다음 필드를 갱신합니다.

- 암호 경로: 시드/자격 증명
- 비밀 데이터: key - value secrets 컬렉션
- 키: 사용자 지정 고유 자격 증명 이름
- 가치: 자격 증명 JSON

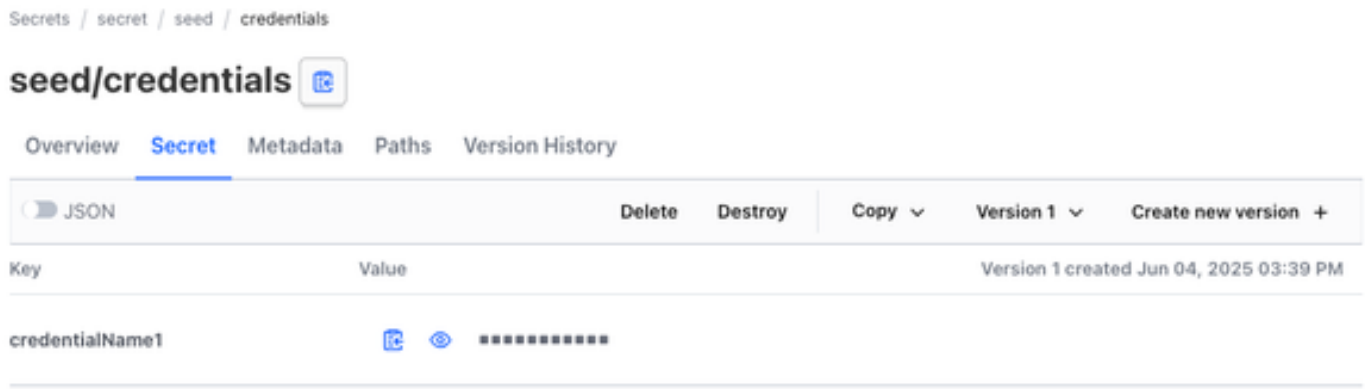
6. 저장을 클릭합니다. 이제 비밀은 HashiCorp Vault에 저장되어야 합니다.



자격 증명

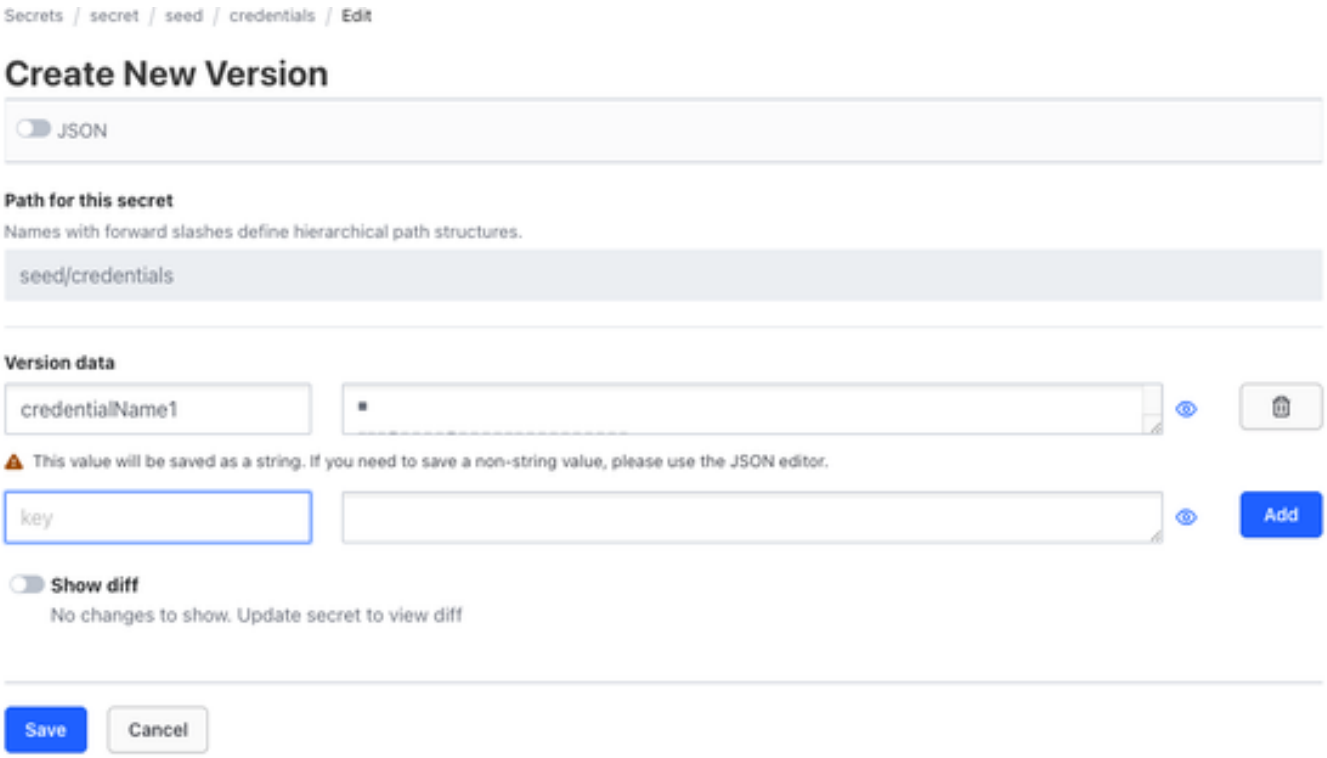
HashiCorp 자격 증명 모음에 추가

1. HashiCorp 볼트 인스턴스에 로그인합니다.



자격 증명 추가

2. 이미 생성된 Secret(비밀) "secret/seed/credentials(비밀/시드/자격 증명)"로 이동합니다.



버전 생성

3. 새 버전 생성을 클릭합니다.

4. 필요에 따라 키-값 쌍을 얼마든지 제공하여 새로운 비밀을 추가합니다.

5. 저장을 클릭합니다.

기본 자격 증명이 있는 CX 클라우드 시드 파일

- 시드 파일 단순화: Hashicorp 자격 증명을 통해 구성한 경우 중요한 정보를 생략하여 시드 파일을 단순화합니다
- IP 주소 또는 호스트 이름만 지정: 사용자는 시드 파일의 IP 주소 또는 호스트 이름만 전달하여 다른 필드는 비워둘 수 있습니다

```
5.0.1.2,,,,,,,,,,,,,,,,,,
5.0.1.3,,,,,,,,,,,,,,,,,,
5.0.1.4,,,,,,,,,,,,,,,,,,
```

IP 또는 호스트 이름

- HashiCorp 자격 증명과 시드 파일 자격 증명을 모두 사용합니다. 자격 증명 모음을 사용하여 다른 디바이스의 자격 증명을 관리하는 동시에 시드 파일에 있는 일부 디바이스의 자격 증명을 제공합니다.

```
5.0.1.1,snmpv3,,username,,,,,,,cliUser,cliPassword,,enablePassword,,,
25.0.1.2,snmpv2c,readOnlyPassword,,,,,,,sshv2,,cliUser,cliPassword,,,,
5.0.1.3,,,,,,,,,,,,,,,,,,
5.0.1.4,,,,,,,,,,,,,,,,,,
```

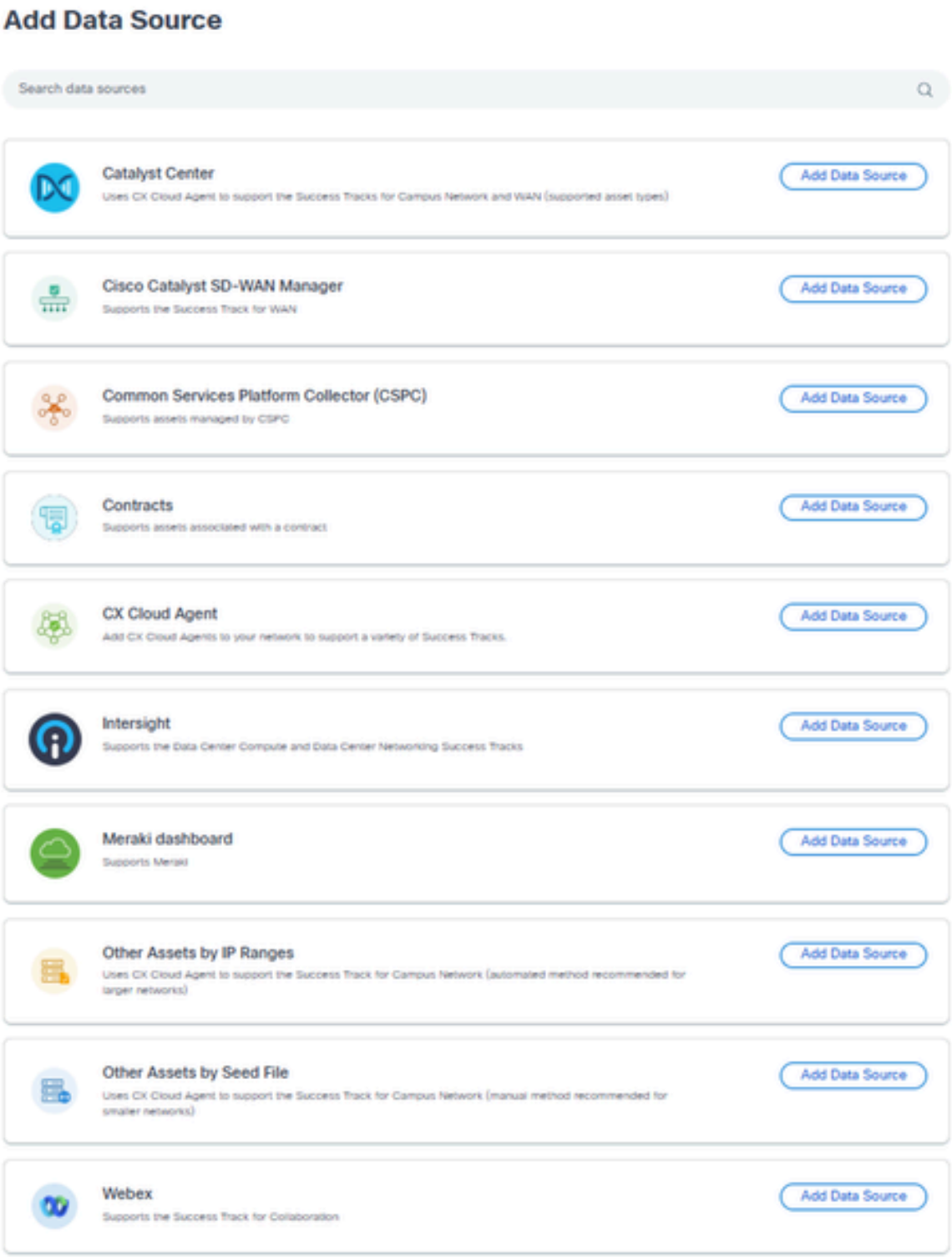
IP 또는 호스트 이름

데이터 소스로 Catalyst Center 추가

수퍼 관리자 사용자 역할의 사용자는 Catalyst Center 데이터 소스를 추가할 수 있습니다.

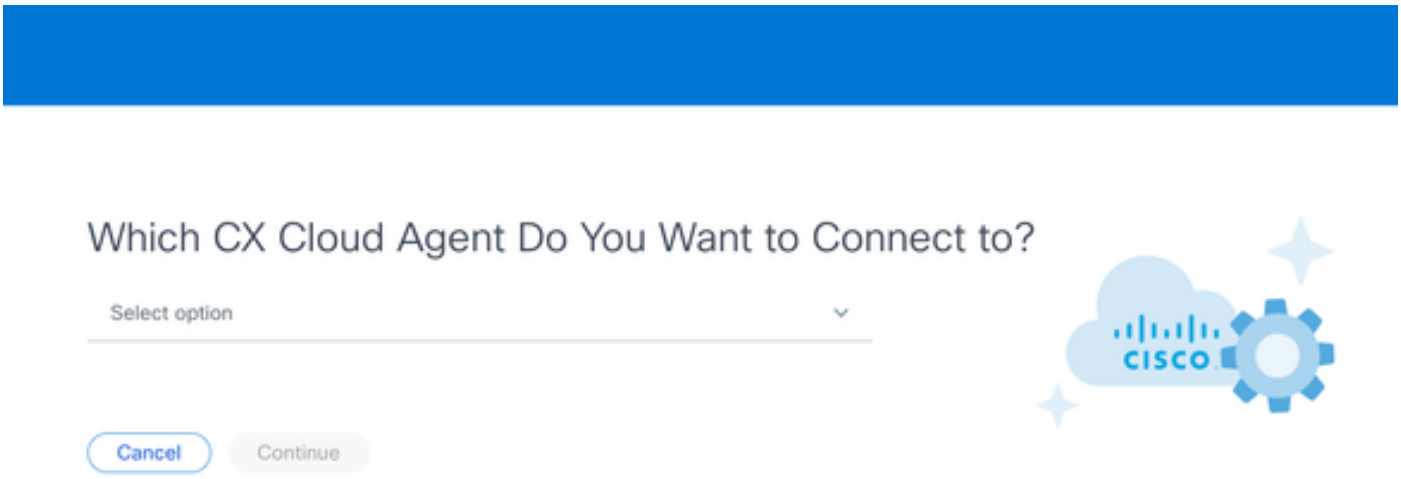
Catalyst Center를 데이터 소스로 추가하려면

1. 관리 센터 아이콘을 선택합니다. 데이터 소스 창이 열립니다.
2. 데이터 소스 추가를 클릭합니다. 데이터 소스 추가 페이지가 표시됩니다.



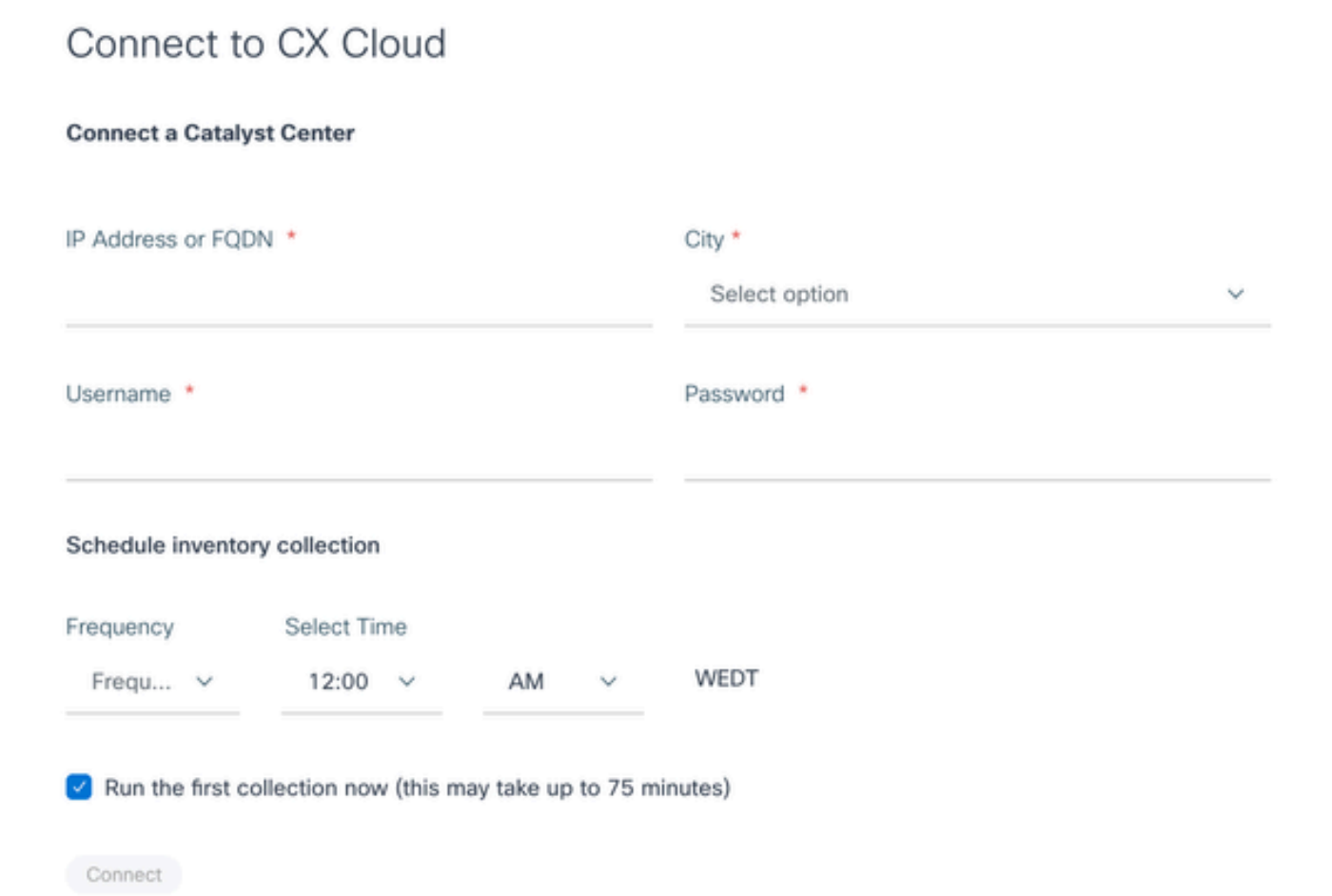
데이터 원본 추가

3. Catalyst Center 옵션에서 Add Data Source(데이터 소스 추가)를 클릭합니다.



CX 에이전트 선택

4. Which CX Agent Do You Want to Connect(연결할 CX 에이전트) 드롭다운 목록에서 CX 에이전트를 선택합니다.
5. Continue(계속)를 클릭합니다. Connect to CX Cloud(CX 클라우드에 연결) 창이 열립니다.



빈도

6. 다음 세부 정보를 입력합니다.

- 가상 IP 주소 또는 FQDN(예: Catalyst Center IP 주소)
- 시(예: Catalyst Center 위치)
- 사용자 이름
- 암호
- CX 에이전트가 네트워크 스캔을 수행하는 빈도를 나타내는 빈도 및 선택 시간

참고: 지금 모음을 실행하려면 [지금 첫 번째 모음 실행] 확인란을 선택합니다.

7. 연결을 클릭합니다. 확인 메시지가 Catalyst Center IP 주소와 함께 표시됩니다.

SolarWinds®를 데이터 소스로 추가

참고: SolarWinds® 데이터 소스를 추가해야 하는 경우 Cisco 지원에 문의하십시오.

BCS/LCS 고객은 이제 CX Agent 기능을 사용하여 SolarWinds®와 외부 통합을 수행할 수 있으므로, 향상된 자동화를 통해 투명성, 관리 용이성 및 향상된 사용자 환경을 제공할 수 있습니다. CX Agent는 인벤토리 및 기타 필요한 데이터를 수집하여 형식, 데이터 완전성 및 데이터 정확성 면에서 일관적인 다양한 보고서를 생성하고 Operational Insights Collector에서 생성한 현재 보고서로 통합합니다. CX Agent는 BCS/LCS 고객이 SolarWinds®에서 데이터를 수집하기 위해 OIC를 CX Agent로 교체할 수 있도록 함으로써 SolarWinds®와의 통합을 지원합니다. Solarwinds® Data Source를 비롯한 이 기능은 BCS/LCS 고객에게만 독점적으로 제공됩니다.

CX 에이전트는 첫 번째 수집 전에 BCS Forwarding에서 구성해야 합니다. 그렇지 않으면 파일이 처리되지 않은 상태로 유지됩니다. BCS 포워딩 컨피그레이션에 대한 자세한 내용은 BCS 또는 LCS용 CX 에이전트 구성 섹션을 참조하십시오.

참고:

- 동일한 SolarWinds® 인스턴스의 여러 컬렉션이 이전 파일을 덮어씁니다(나중에 업로드하는 것이 우선함).
- 여러 소스가 지원되지만 각 SolarWinds® 인스턴스에는 고유한 IP 및 어플라이언스 ID가 있어야 합니다

기타 자산을 데이터 소스로 추가

텔레메트리 수집은 Catalyst Center에서 관리하지 않는 디바이스까지 확장되어 사용자가 텔레메트리 기반 통찰력 및 분석을 보고 상호 작용하여 더 광범위한 디바이스를 지원할 수 있게 되었습니다. 초기 CX Agent 설정 후 사용자는 CX Cloud에서 모니터링하는 인프라 내의 20개의 추가 Catalyst Center에 연결하도록 CX Agent를 구성할 수 있습니다.

사용자는 시드 파일을 사용하여 그러한 디바이스를 고유하게 식별하거나 CX Agent에서 스캔해야 하는 IP 범위를 지정하여 CX 클라우드에 통합할 디바이스를 식별할 수 있습니다. 두 방식 모두 검색을 위해 SNMP(Simple Network Management Protocol)를 사용하고 연결을 위해 SSH(Secure Shell)를 사용합니다. 성공적인 텔레메트리 수집을 활성화하려면 이러한 항목을 올바르게 구성해야 합니다.

다른 에셋을 데이터 소스로 추가하려면 다음 옵션 중 하나를 사용합니다.

- 시드 파일 템플릿을 사용하여 시드 파일 업로드
- IP 주소 범위 제공

검색 프로토콜

시드 파일 기반 직접 디바이스 검색과 IP 범위 기반 검색 모두 SNMP를 검색 프로토콜로 사용합니다. 서로 다른 버전의 SNMP가 있지만 CX Agent는 SNMPv2c 및 SNMPv3을 지원하며 둘 중 하나 또는 둘 다 구성할 수 있습니다. 컨피그레이션을 완료하고 SNMP 관리 디바이스와 SNMP 서비스 관리자 간의 연결을 활성화하려면 아래에서 자세히 설명하는 동일한 정보를 사용자가 제공해야 합니다.

SNMPv2c와 SNMPv3은 보안 및 원격 컨피그레이션 모델 면에서 다릅니다. SNMPV3는 SHA 암호화를 지원하는 고급 암호화 보안 시스템을 사용하여 메시지를 인증하고 개인 정보를 보장합니다. 보안 위험과 위협으로부터 보호하기 위해 모든 공용 및 인터넷 연결 네트워크에서 SNMPv3를 사용하는 것이 좋습니다. CX 클라우드에서는 SNMPv3를 기본적으로 지원하지 않는 이전 레거시 디바이스를 제외하고 SNMPv2c가 아닌 SNMPv3를 구성하는 것이 좋습니다. 사용자가 두 버전의 SNMP를 모두 구성하면 CX Agent는 기본적으로 SNMPv3를 사용하여 각 디바이스와 통신을 시도하고 통신을 협상할 수 없는 경우 SNMPv2c로 돌아갑니다.

연결 프로토콜

직접 디바이스 연결 설정의 일부로, 사용자는 디바이스 연결 프로토콜의 세부 정보를 지정해야 합니다. SSH(또는 텔넷). SSHv2를 사용해야 합니다. 단, 적절한 기본 제공 지원이 없는 개별 레거시 자산의 경우는 예외입니다. SSHv1 프로토콜에는 기본 취약성이 포함되어 있습니다. 추가 보안이 없으면 SSHv1에 의존할 때 이러한 취약성으로 인해 텔레메트리 데이터 및 기본 자산이 손상될 수 있습니다. 텔넷도 안전하지 않습니다. 텔넷을 통해 제출된 자격 증명 정보(예: 사용자 이름 및 비밀번호)는 암호화되지 않으므로 보안상의 문제가 발생할 수 있습니다.

장치에 대한 텔레메트리 처리 제한

다음은 디바이스에 대한 텔레메트리 데이터를 처리할 때 제한 사항입니다.

- 일부 디바이스는 Collection Summary(수집 요약)에서 연결 가능한 것으로 표시될 수 있지만 CX Cloud Assets(CX 클라우드 자산) 페이지에는 표시되지 않습니다.
- 시드 파일 또는 IP 범위 컬렉션의 디바이스도 Catalyst Center 인벤토리의 일부인 경우 디바이스는 Catalyst Center 항목에 대해 한 번만 보고됩니다. 시드 파일 또는 IP 범위 항목 내의 각 디바이스는 중복을 방지하기 위해 건너뜁니다.
- Cisco IP Phone은 CX Agent에 의한 데이터 수집을 위해 CX 클라우드에서 지원되지 않습니다. 따라서 Cisco IP Phone은 에셋 목록에 표시되지 않습니다.

시드 파일을 사용하여 기타 에셋 추가

시드 파일은 .csv 파일이며 각 행은 시스템 데이터 레코드를 나타냅니다. 시드 파일에서 모든 시드 파일 레코드는 CX Agent에서 텔레메트리를 수집해야 하는 고유한 디바이스에 해당합니다. 가져오는 시드 파일의 각 디바이스 항목에 대한 모든 오류 또는 정보 메시지는 작업 로그 세부사항의 일부

로 캡처됩니다. 초기 컨피그레이션 시 디바이스에 연결할 수 없는 경우에도 시드 파일의 모든 디바이스는 관리되는 디바이스로 간주됩니다. 이전 파일을 대체하기 위해 새 시드 파일을 업로드하는 경우 마지막 업로드 날짜가 CX 클라우드에 표시됩니다.

CX Agent는 디바이스에 연결을 시도하지만 PID 또는 일련 번호를 확인할 수 없는 경우 Assets 페이지에 표시할 각 디바이스를 처리하지 못할 수 있습니다.

시드 파일에서 세미콜론으로 시작하는 모든 행은 무시됩니다. 시드 파일의 헤더 행은 세미콜론으로 시작하며 고객 시드 파일을 생성하는 동안 그대로 유지하거나(권장 옵션) 삭제할 수 있습니다.

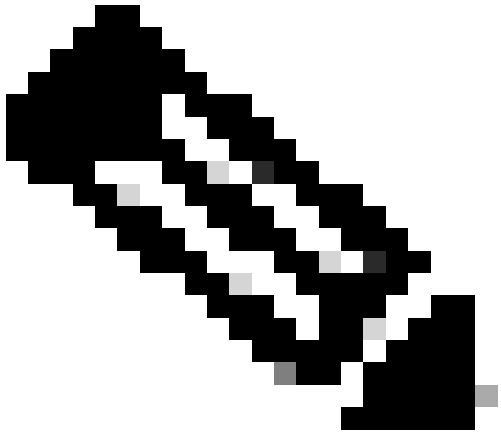
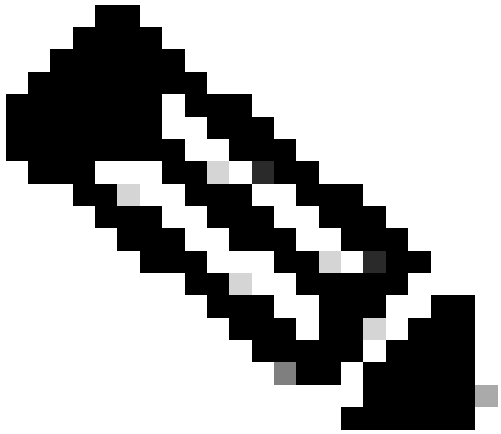
사용자는 표준 CX 클라우드 시드 파일과 동일한 방법으로 CSPC(Common Services Platform Collector) 시드 파일을 업로드할 수 있으며, 필요한 모든 재포맷은 CX 클라우드에서 관리됩니다.

CX Agent v3.1 이상에서는 CSPC 또는 CX 형식으로 시드 파일을 업로드할 수 있습니다. 이전 CX 에이전트 버전에서는 CX 형식 시드 파일만 지원됩니다.

열 헤더를 비롯한 샘플 시드 파일의 형식은 어떤 식으로든 변경되지 않는 것이 중요합니다.

다음 표에서는 필요한 모든 시드 파일 열과 각 열에 포함해야 할 데이터를 식별합니다.

Seed File(시드 파일) 열	열 헤더/식별자	열의 목적
A	IP 주소 또는 호스트 이름	디바이스의 유효한 고유 IP 주소 또는 호스트 이름을 제공합니다.
B	SNMP 프로토콜 버전	SNMP 프로토콜은 CX Agent에 필요하며 고객 네트워크 내에서 디바이스를 검색하는 데 사용됩니다. 값은 snmpv2c 또는 snmpv3이 될 수 있지만 보안 고려 사항으로 인해 snmpv3이 권장됩니다.
C	snmpRo: col#=3이 'snmpv2c'로 선택된 경우 필수	특정 디바이스에 대해 SNMPv2의 레거시 변형을 선택한 경우 디바이스 SNMP 컬렉션에 대한 snmpRO(읽기 전용) 자격 증명을 지정해야 합니다. 그렇지 않으면 항목을 비워 둘 수 있습니다.
D	snmpv3사용자 이름: col#=3이 'snmpv3'으로 선택된 경우 필수	특정 디바이스와 통신하도록 SNMPv3을 선택한 경우 해당 로그인 사용자 이름을 제공해야 합니다.
E	snmpv3AuthAlgorithm: 값은 MD5 또는 SHA일 수 있습니	SNMPv3 프로토콜은 MD5(Message Digest) 또는 SHA(Secure Hash Algorithm)를 통한 인증

Seed File(시드 파일) 열	열 헤더/식별자	열의 목적
	다	을 허용합니다. 디바이스가 보안 인증으로 구성된 경우 각 인증 알고리즘을 제공해야 합니다.  참고: MD5는 안전하지 않은 것으로 간주되며 이를 지원하는 모든 디바이스에서 SHA를 사용할 수 있습니다.
F	snmpv3AuthPassword: 암호	MD5 또는 SHA 암호화 알고리즘이 디바이스에 구성된 경우 디바이스 액세스를 위해 관련 인증 비밀번호를 제공해야 합니다.
G	snmpv3PrivAlgorithm: 값은 DES , 3DES일 수 있습니다.	디바이스가 SNMPv3 프라이버시 알고리즘으로 구성된 경우(이 알고리즘은 응답을 암호화하는 데 사용됨), 해당 알고리즘을 제공해야 합니다. 

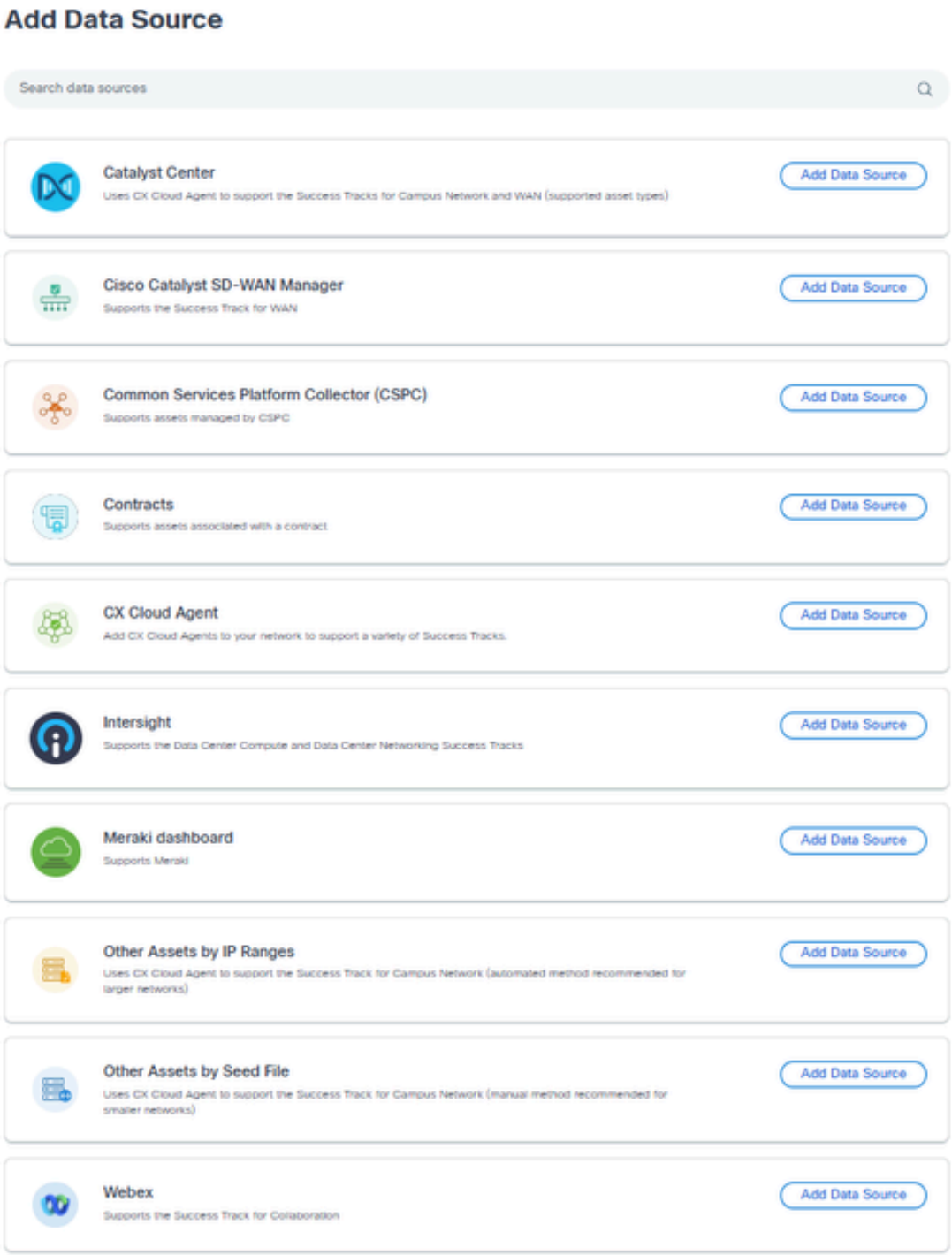
Seed File(시드 파일) 열	열 헤더/식별자	열의 목적
		참고: DES(Data Encryption Standard)에서 사용하는 56비트 키는 암호화 보안을 제공하기에 너무 짧은 것으로 간주되며, 3DES(Triple Data Encryption Standard)는 이를 지원하는 모든 장치에서 사용할 수 있습니다.
H	snmpv3Priv비밀번호: 암호	SNMPv3 프라이버시 알고리즘이 디바이스에 구성된 경우 디바이스 연결을 위해 해당 프라이버시 비밀번호를 제공해야 합니다.
I	snmpv3EngineId: engineID, 디바이스를 나타내는 고유 ID, 디바이스에 수동으로 구성된 경우 엔진 ID 지정	SNMPv3 EngineID는 각 디바이스를 나타내는 고유한 ID입니다. 이 엔진 ID는 CX Agent에서 SNMP 데이터 세트를 수집하는 동안 참조로 전송됩니다. 고객이 EngineID를 수동으로 구성하는 경우 해당 EngineID를 제공해야 합니다.
제이	cli 프로토콜: 값은 'telnet', 'sshv1', 'sshv2'가 될 수 있습니다. 비어 있는 경우 기본적으로 'sshv2'로 설정할 수 있습니다.	CLI(Command Line Interface)는 디바이스와 직접 상호 작용하도록 설계되었습니다. CX Agent는 특정 디바이스의 CLI 수집에 이 프로토콜을 사용합니다. 이 CLI 수집 데이터는 CX 클라우드 내의 Assets 및 기타 Insights 보고에 사용됩니다. SSHv2를 사용하는 것이 좋습니다. 다른 네트워크 보안 조치가 없으면 그 자체로는 SSHv1 및 텔넷 프로토콜이 적절한 전송 보안을 제공하지 않습니다.
케이	cli 포트: CLI 프로토콜 포트 번호	CLI 프로토콜을 선택한 경우 해당 포트 번호를 제공해야 합니다. 예를 들어, SSH의 경우 22, 텔넷의 경우 23입니다.
L	cli 사용자: CLI 사용자 이름 (CLI 사용자 이름/비밀번호 또는 둘 다 제공할 수 있지만 두 열(col#=12 및 col#=13)은 모두 비워 둘 수 없습니다.)	디바이스의 각 CLI 사용자 이름을 제공해야 합니다. 이는 CLI 수집 중에 디바이스에 연결할 때 CX Cloud Agent에서 사용됩니다.

Seed File(시드 파일) 열	열 헤더/식별자	열의 목적
M	cli비밀번호: CLI 사용자 비밀번호(CLI 사용자 이름/비밀번호 또는 둘 다 제공할 수 있지만 두 열(col#=12 및 col#=13)은 모두 비워 둘 수 없습니다.)	디바이스의 각 CLI 비밀번호를 제공해야 합니다. CLI 수집 중에 디바이스에 연결할 때 CX Agent에서 사용됩니다.
네트워킹	cliEnable사용자	디바이스에 enable이 구성된 경우 디바이스의 enableUsername 값을 제공해야 합니다.
O	cliEnable비밀번호	디바이스에 enable이 구성된 경우 디바이스의 enablePassword 값을 제공해야 합니다.
P	향후 지원(입력 필요 없음)	향후 사용을 위해 예약됨
Q	향후 지원(입력 필요 없음)	향후 사용을 위해 예약됨
R	향후 지원(입력 필요 없음)	향후 사용을 위해 예약됨
초	향후 지원(입력 필요 없음)	향후 사용을 위해 예약됨

새 시드 파일을 사용하여 기타 에셋 추가

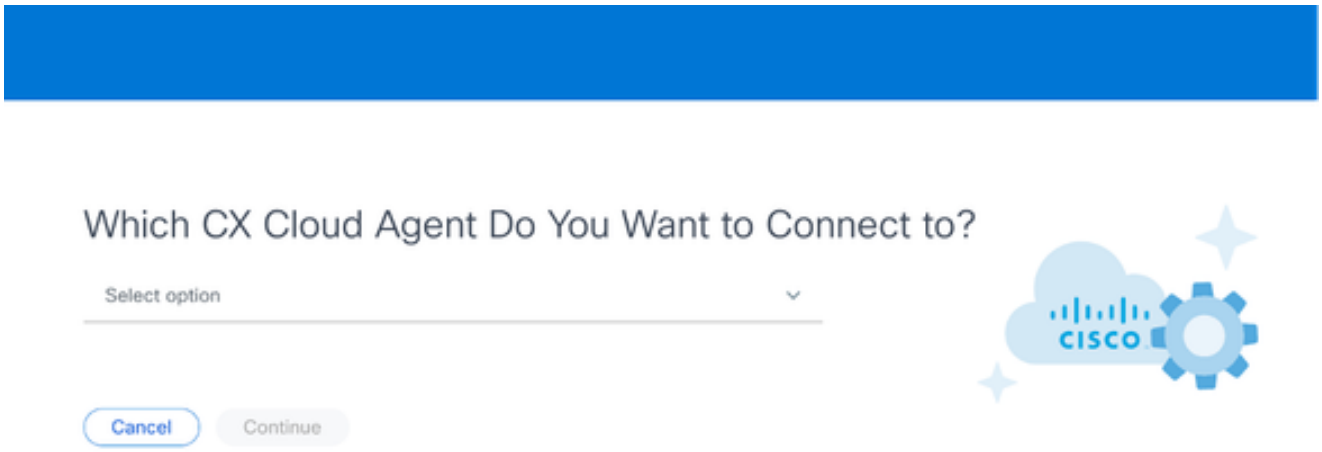
새 시드 파일을 사용하여 다른 에셋을 추가하려면

1. Admin Center(관리 센터) > Data Sources(데이터 소스) 창에서 Add Data Source(데이터 소스 추가)를 클릭합니다.



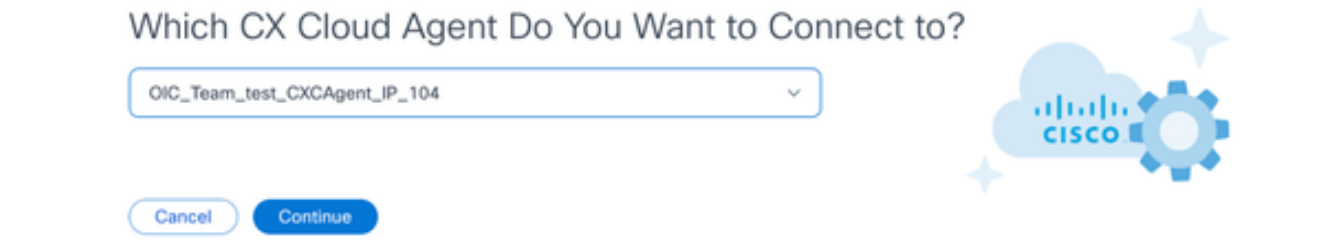
데이터 원본 추가

2. Other Assets by Seed File(시드 파일별 기타 자산) 옵션에서 Add Data Source(데이터 소스 추가)를 클릭합니다.



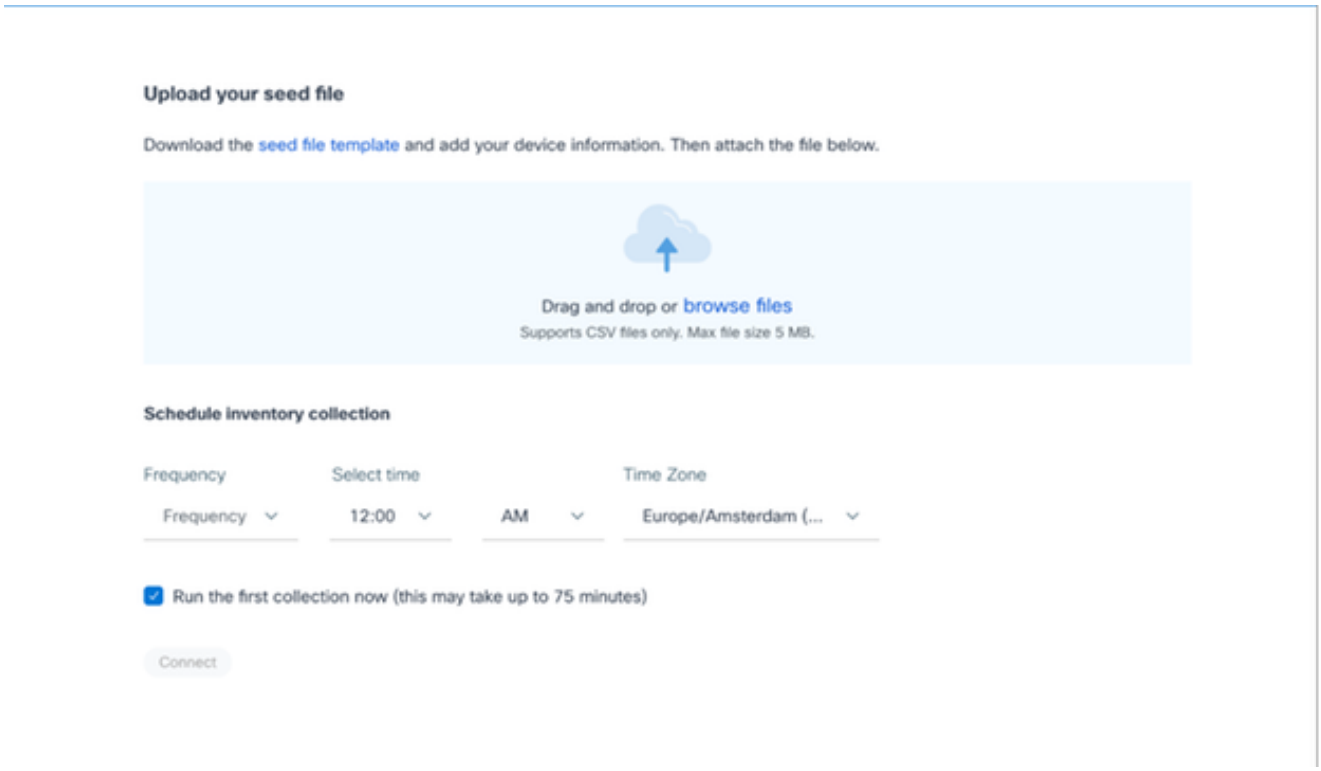
CX 에이전트 선택

3. Which CX Cloud Agent Do You Want to Connect(연결할 CX 클라우드 에이전트) 드롭다운 목록에서 CX 에이전트를 선택합니다.



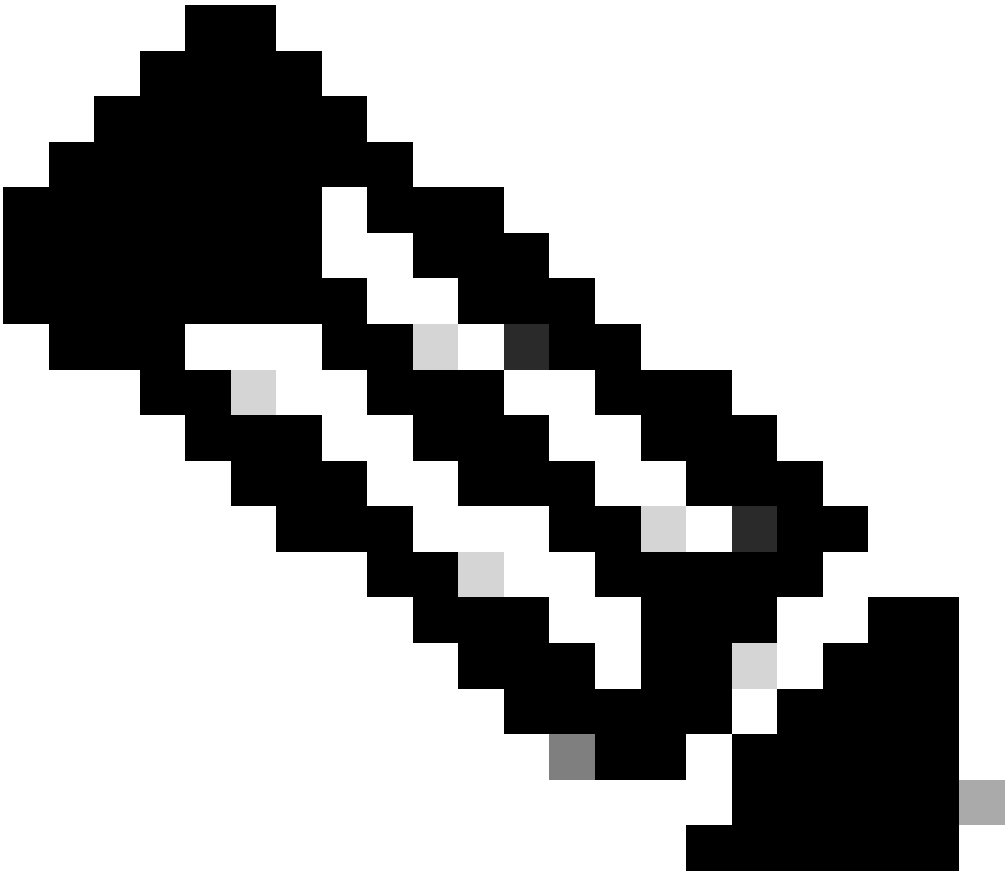
계속

4. Continue(계속)를 클릭합니다. Upload Your Seed File(시드 파일 업로드) 페이지가 표시됩니다.



시드 파일 업로드

5. 하이퍼링크된 시드 파일 템플릿을 클릭하여 템플릿을 다운로드합니다.
6. 수동으로 데이터를 입력하거나 파일로 가져옵니다. 완료되면 템플릿을 .csv 파일로 저장하여 파일을 CX Agent로 가져옵니다.
7. .csv 파일을 업로드하려면 끌어서 놓거나 파일 찾아보기를 클릭합니다.
8. Schedule inventory collection(인벤토리 수집 예약) 섹션을 완료합니다.



참고: CX 클라우드의 초기 컨피그레이션이 완료되기 전에 CX 클라우드 에이전트는 시드 파일을 처리하고 식별된 모든 디바이스와의 연결을 설정하여 첫 번째 텔레메트리 수집을 수행해야 합니다. 수집은 온디맨드 방식으로 시작하거나 여기에 정의된 일정에 따라 실행할 수 있습니다. 사용자는 Run the first collection now(지금 첫 번째 수집 실행) 확인란을 선택하여 첫 번째 텔레메트리 연결을 수행할 수 있습니다. 시드 파일에 지정된 항목 수 및 기타 요인에 따라 이 프로세스는 상당한 시간이 걸릴 수 있습니다.

9. 연결을 클릭합니다. 데이터 소스 창이 열리고 확인 메시지가 표시됩니다.

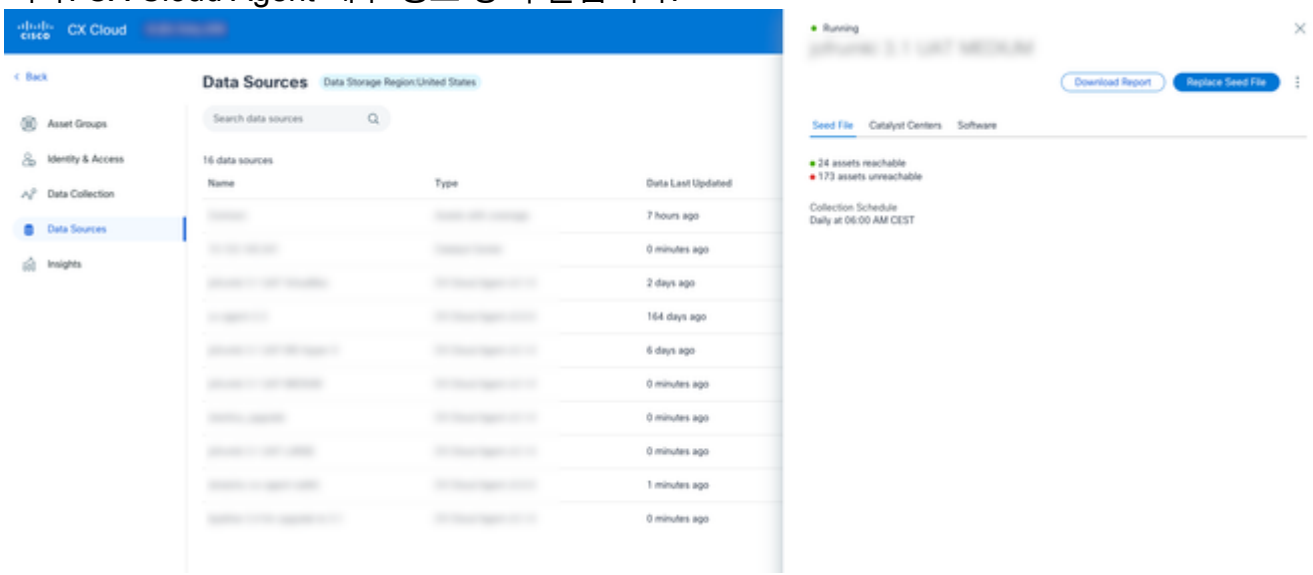
수정된 시드 파일을 사용하여 기타 에셋 추가

현재 시드 파일을 사용하여 디바이스를 추가, 수정 또는 삭제하려면

1. 이전에 생성한 시드 파일을 열고 필요한 사항을 변경한 다음 파일을 저장합니다.

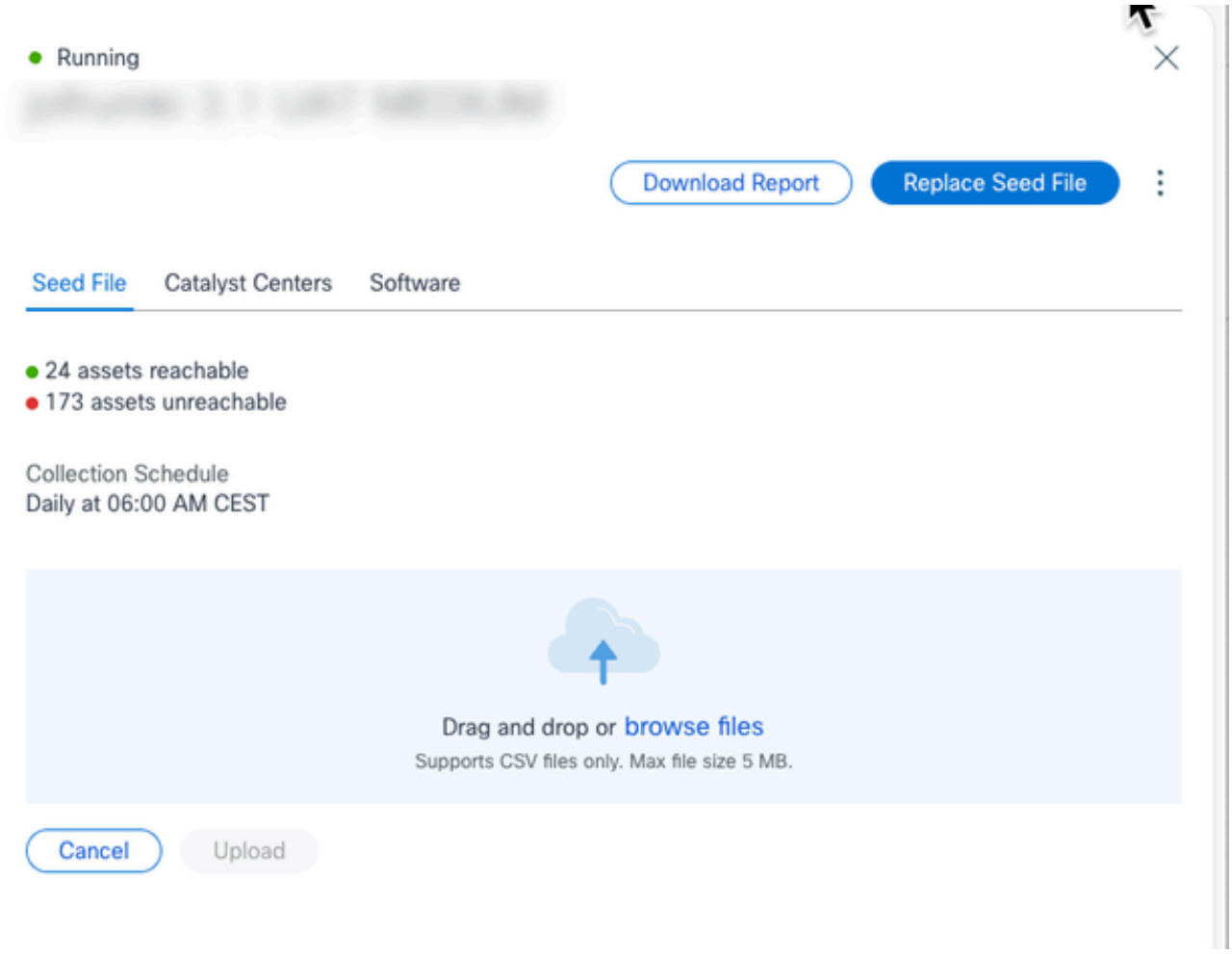
참고: 시드 파일에 에셋을 추가하려면 이전에 생성한 시드 파일에 해당 에셋을 추가하고 파일을 다시 로드합니다. 새 시드 파일을 업로드하면 현재 시드 파일이 대체되므로 이 작업이 필요합니다. 최신 업로드된 시드 파일만 검색 및 수집에 사용됩니다.

2. 데이터 소스 페이지에서 업데이트된 시드 파일이 필요한 CX 에이전트 데이터 소스를 클릭합니다. CX Cloud Agent 세부 정보 창이 열립니다.



시드 파일

3. 시드 파일 교체를 클릭합니다.



시드 파일 바꾸기

4. 수정된 시드 파일을 업로드하려면 드래그 앤 드롭 또는 찾아보기 파일을 클릭합니다.
5. Upload를 클릭합니다.

시드 파일의 기본 자격 증명

CX Agent는 고객이 Agent에서 로컬로 설정할 수 있는 기본 자격 증명을 제공하므로 중요한 비밀번호를 Seed File에 직접 포함할 필요가 없습니다. 이를 통해 기밀 정보의 노출을 줄이고 고객의 주요 문제를 해결하여 보안을 강화할 수 있습니다.

IP 범위를 사용하여 기타 자산 추가

IP 범위를 통해 사용자는 하드웨어 자산을 식별하고, IP 주소를 기반으로 해당 디바이스에서 텔레메트리를 수집할 수 있습니다. SNMP 프로토콜을 사용하여 CX Agent에서 스캔할 수 있는 단일 네트워크 레벨 IP 범위를 지정하여 텔레메트리 수집용 디바이스를 고유하게 식별할 수 있습니다. 직접 연결된 디바이스를 식별하기 위해 IP 범위를 선택하는 경우 참조되는 IP 주소를 최대한 제한하면서 모든 필수 자산에 대한 커버리지를 허용할 수 있습니다.

- 특정 IP를 제공하거나, 범위를 생성하기 위해 IP의 옥텟을 대체하는 데 와일드카드를 사용할 수 있습니다.
- 특정 IP 주소가 설정 중에 식별된 IP 범위에 포함되지 않은 경우 CX Agent는 해당 IP 주소가 있는 디바이스와의 통신을 시도하지 않으며 해당 디바이스로부터 텔레메트리를 수집하지도 않습니다.
- *.*.*.*를 입력하면 CX 에이전트가 모든 IP에서 사용자 제공 자격 증명을 사용할 수 있습니다. 예를 들면 다음과 같습니다. 172.16.*.*에서는 172.16.0.0/16 서브넷의 모든 디바이스에 자격 증명을 사용할 수 있습니다.
- 네트워크 또는 IB(Installed Base)에 변경 사항이 있을 경우 IP 범위를 수정할 수 있습니다. IP 범위 수정 섹션을 참조하십시오.

CX Agent는 디바이스에 연결을 시도하지만 PID 또는 일련 번호를 확인할 수 없는 경우 Assets(자산) 보기에 표시할 각 디바이스를 처리하지 못할 수 있습니다.

참고:
Edit IP Address Range(IP 주소 범위 수정)를 클릭하면 온디맨드 디바이스 검색이 시작됩니다. 지정된 IP 범위에 새 디바이스가 추가되거나 삭제되면(내부 또는 외부) 고객은 항상 IP 주소 범위 수정(IP 범위 수정 섹션 참조)을 클릭하고 CX 에이전트 컬렉션 인벤토리에 새로 추가된 디바이스를 포함하도록 온디맨드 디바이스 검색을 시작하는 데 필요한 단계를 완료해야 합니다.

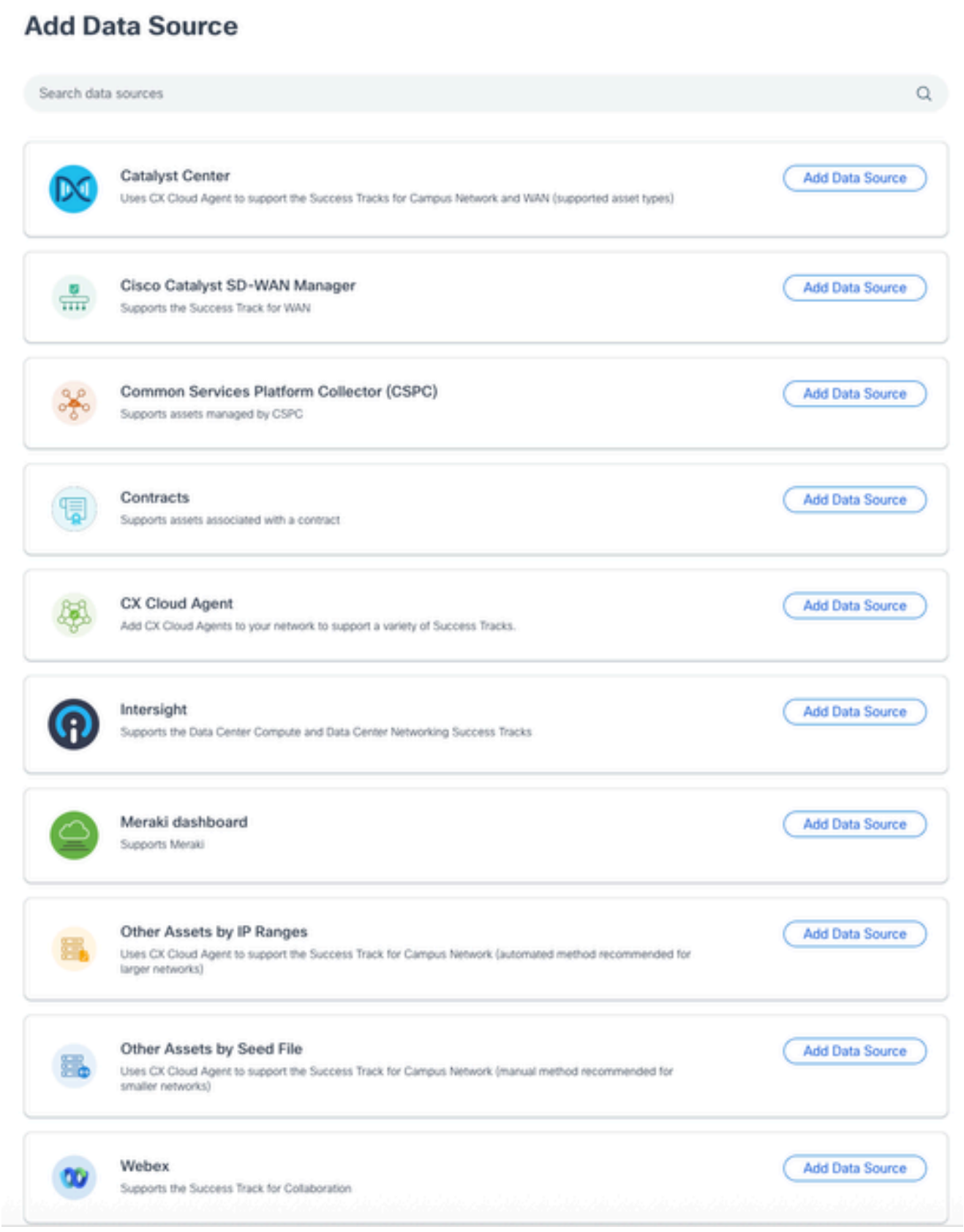
IP 범위를 사용하여 디바이스를 추가하려면 사용자가 컨피그레이션 UI를 통해 적용 가능한 모든 자격 증명을 지정해야 합니다. 표시되는 필드는 이전 창에서 선택한 프로토콜에 따라 달라집니다. SNMPv2c와 SNMPv3을 둘 다 선택하거나 SSHv2와 SSHv1을 둘 다 선택하는 등 동일한 프로토콜에 대해 여러 항목을 선택한 경우, CX Agent는 개별 디바이스 기능에 따라 프로토콜 선택을 자동으로 자동 협상합니다.

IP 주소를 사용하여 디바이스를 연결할 경우, 고객은 IP 범위의 모든 관련 프로토콜과 함께 SSH 버전 및 텔넷 자격 증명이 유효한지 확인해야 합니다. 그렇지 않으면 연결에 실패합니다.

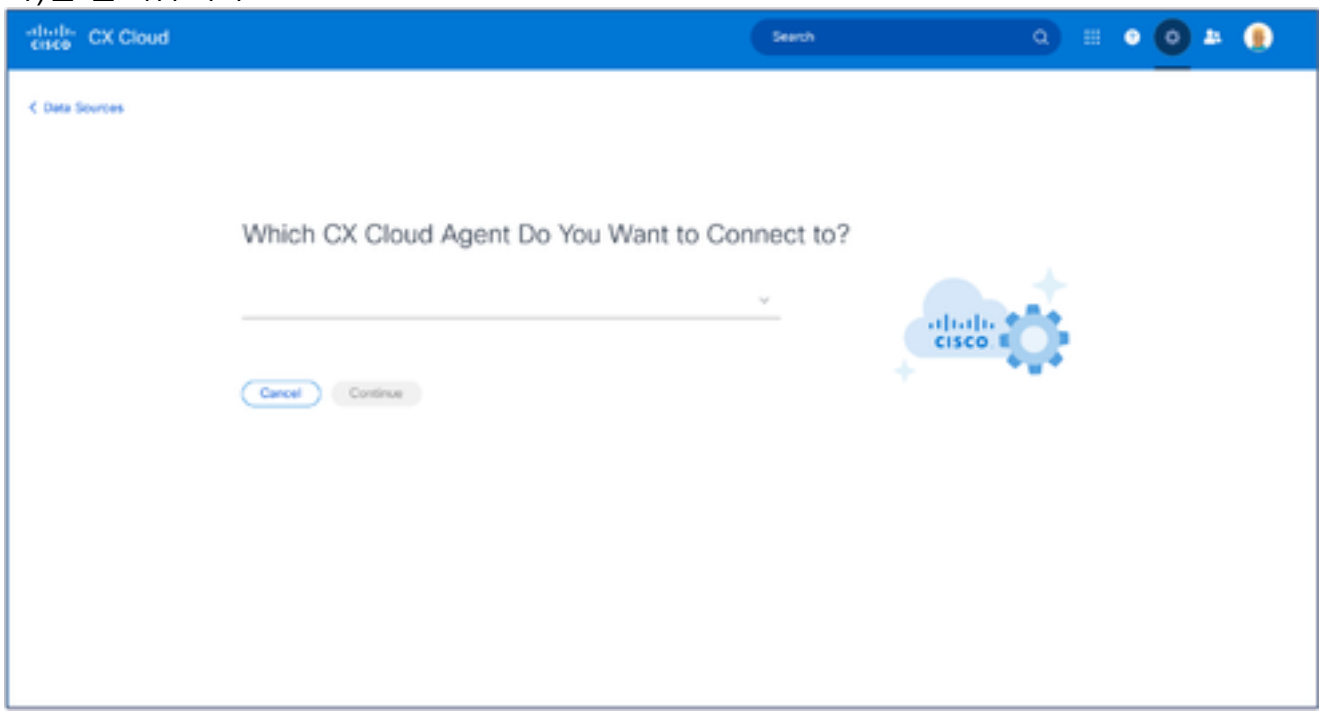
IP 범위별 기타 자산 추가

IP 범위를 사용하여 디바이스를 추가하려면

1. 관리 센터 아이콘을 선택합니다. 데이터 소스 창이 열립니다.
2. Admin Center(관리 센터) > Data Sources(데이터 소스) 창에서 Add Data Source(데이터 소스 추가)를 클릭합니다.

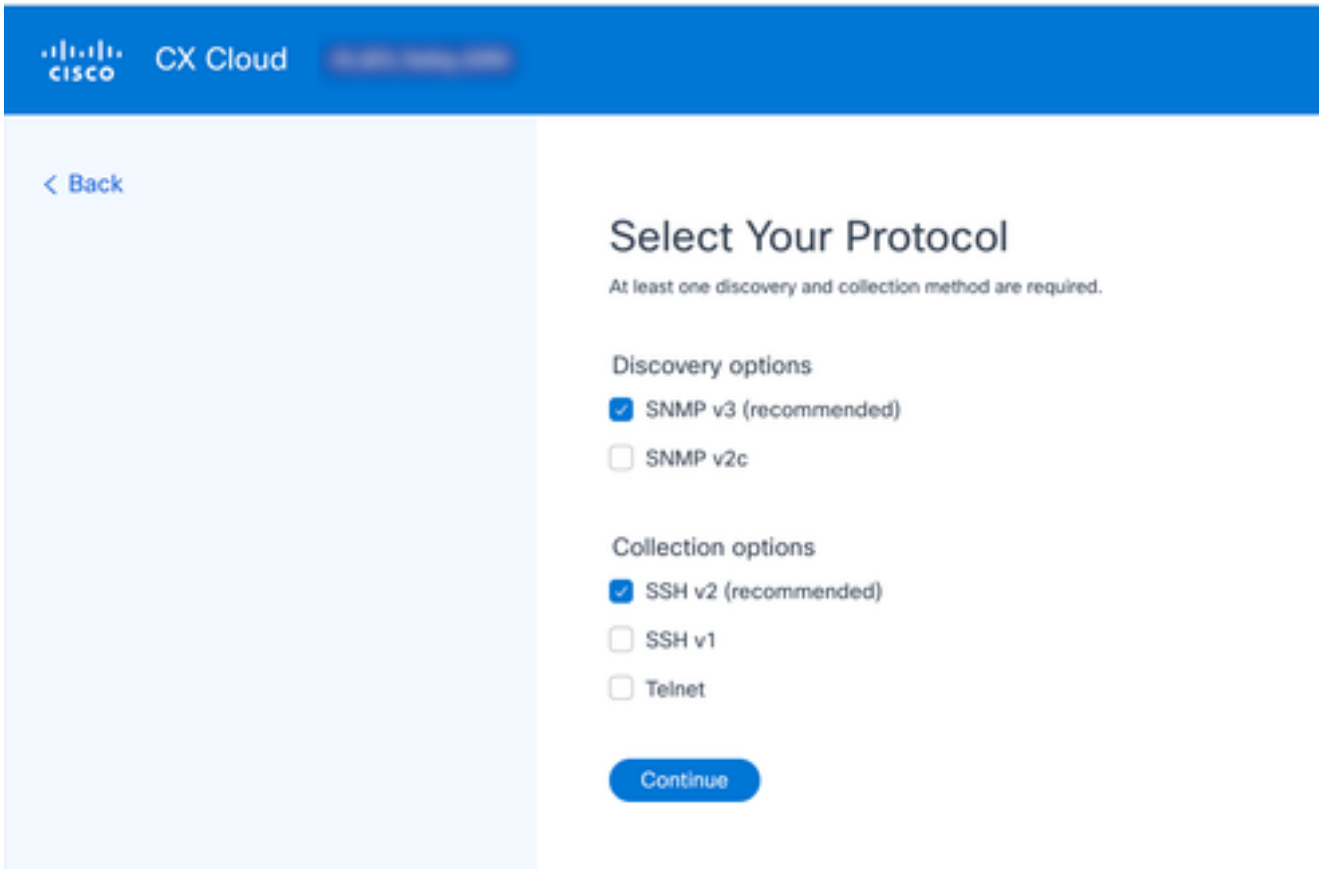


3. Other Assets by IP Ranges(IP 범위별 기타 자산) 옵션에서 Add Data Source(데이터 소스 추가)를 클릭합니다.



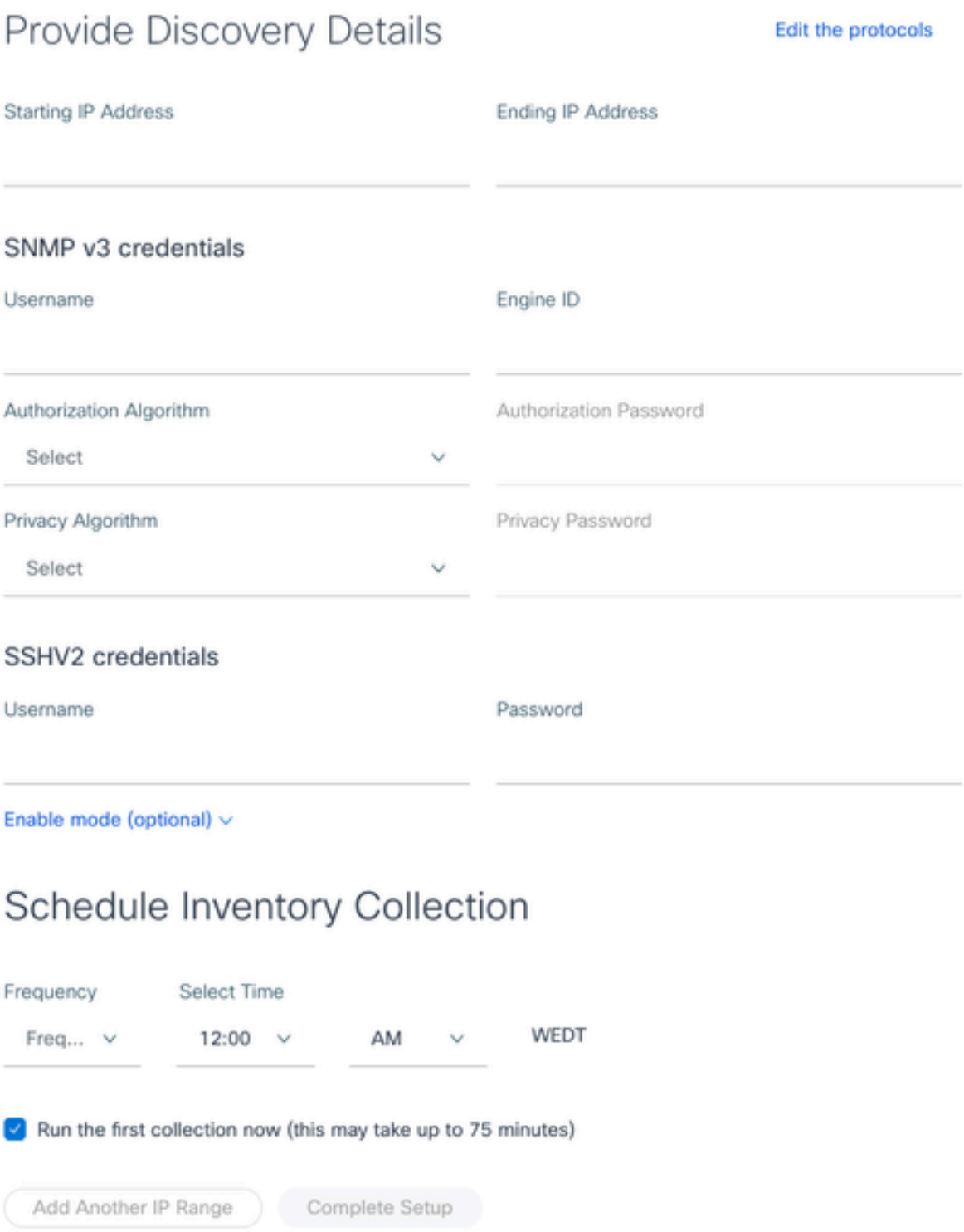
CX 클라우드 에이전트 선택

4. Which CX Cloud Agent Do You Want to Connect(연결할 CX 클라우드 에이전트) 드롭다운 목록에서 CX 에이전트를 선택합니다.
5. Continue(계속)를 클릭합니다. Select Your Protocol 창이 열립니다.



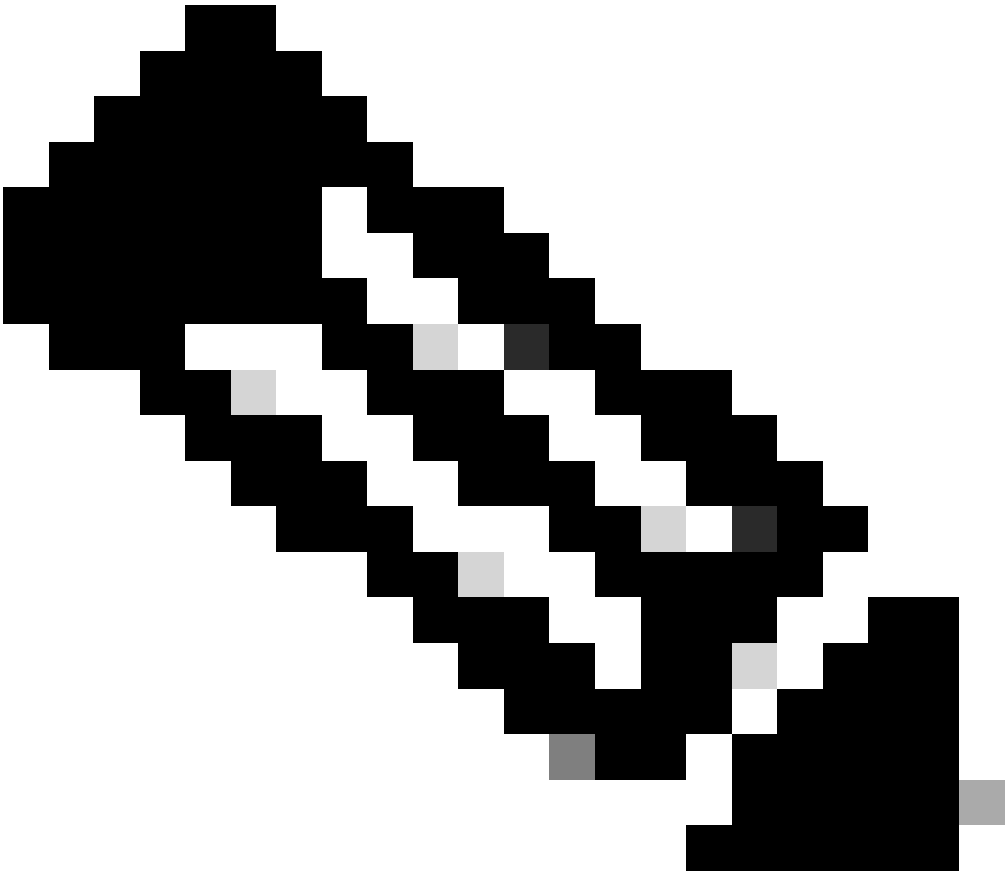
프로토콜 선택

6. Discovery(검색) 옵션과 Collection(수집) 옵션에 해당하는 확인란을 선택합니다.
7. Continue(계속)를 클릭합니다.



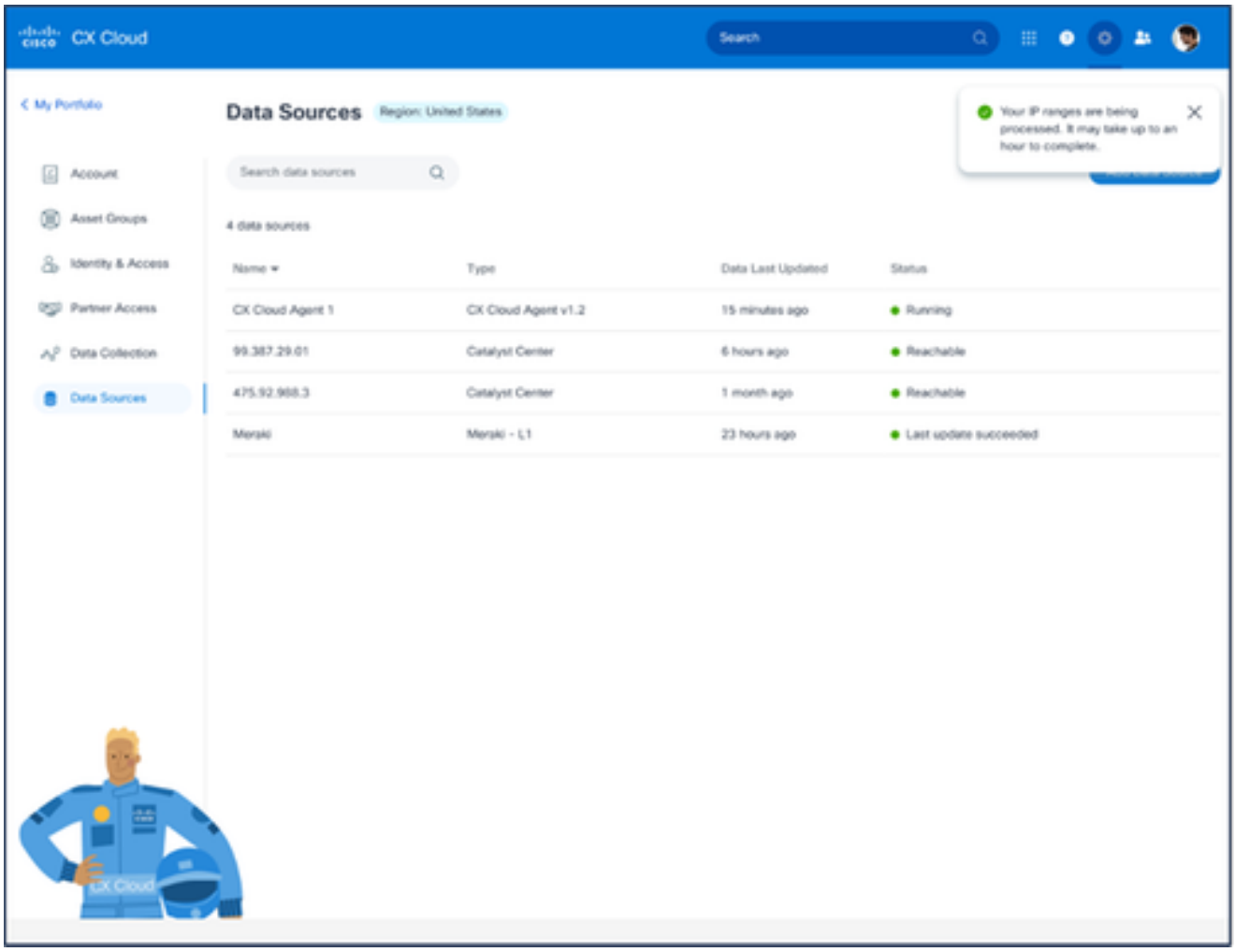
검색 세부 정보

8. Provide Discovery Details(검색 세부 정보 제공) 및 Schedule Inventory Collection(인벤토리 수집 예약) 섹션에서 필요한 세부 정보를 입력합니다.



참고: 선택한 CX Agent에 대해 다른 IP 범위를 추가하려면 다른 IP 범위 추가를 클릭하여 프로토콜 설정 창으로 다시 이동하고 이 섹션의 단계를 반복합니다.

9. Complete Setup(설정 완료)을 클릭합니다. 구축이 완료되면 확인 메시지가 표시됩니다.

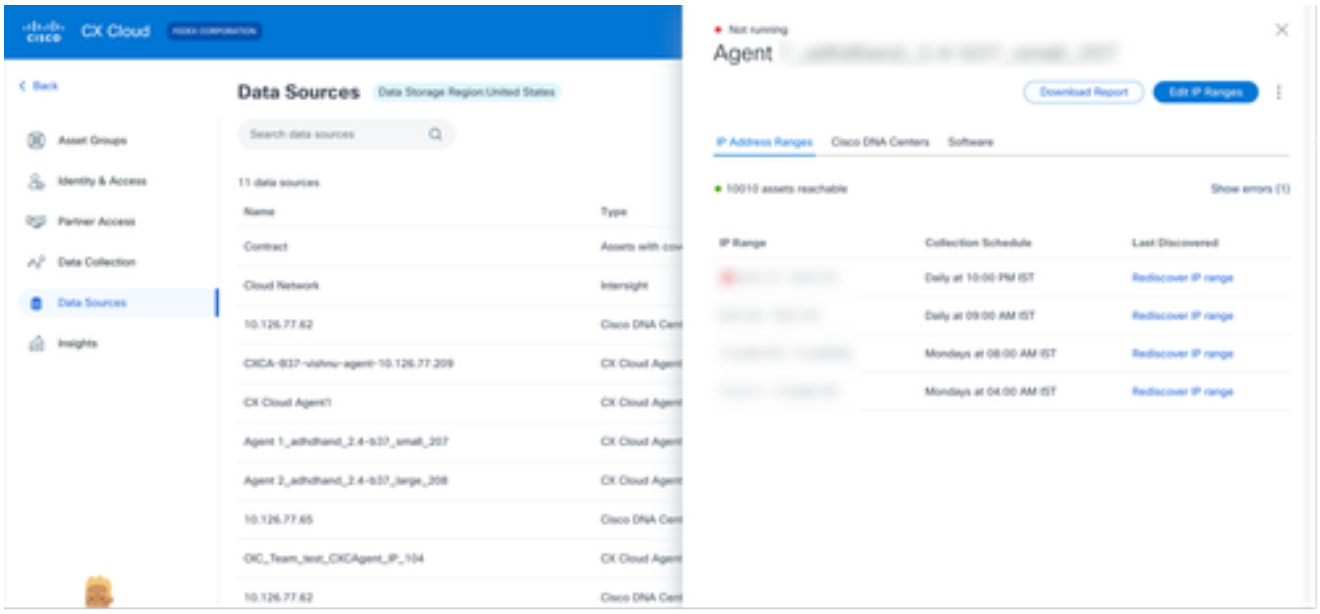


확인 메시지

IP 범위 수정

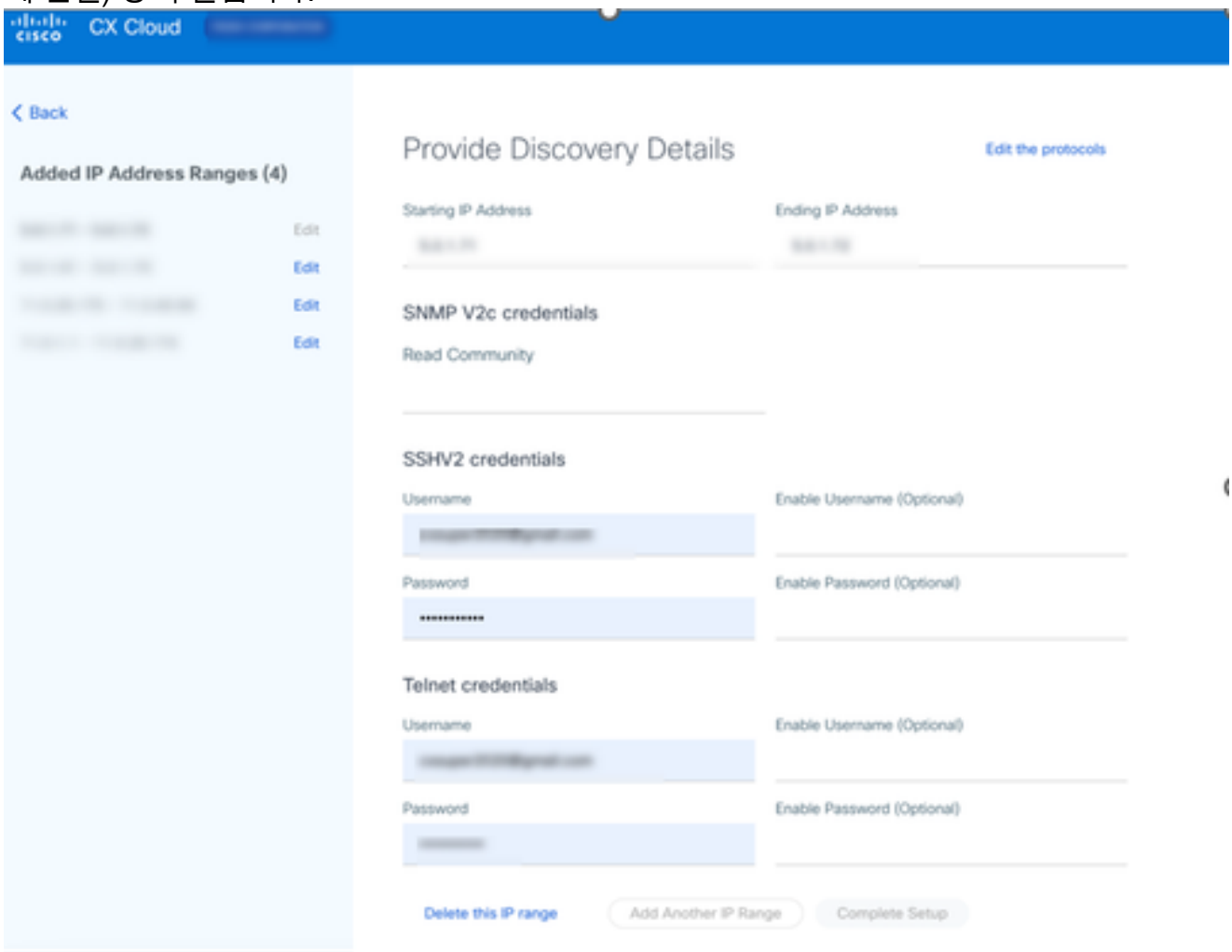
IP 범위를 수정하려면

1. 데이터 소스 창으로 이동합니다.
2. 데이터 소스에서 IP 범위를 수정해야 하는 CX 에이전트를 클릭합니다. 세부내용 창이 열립니다.

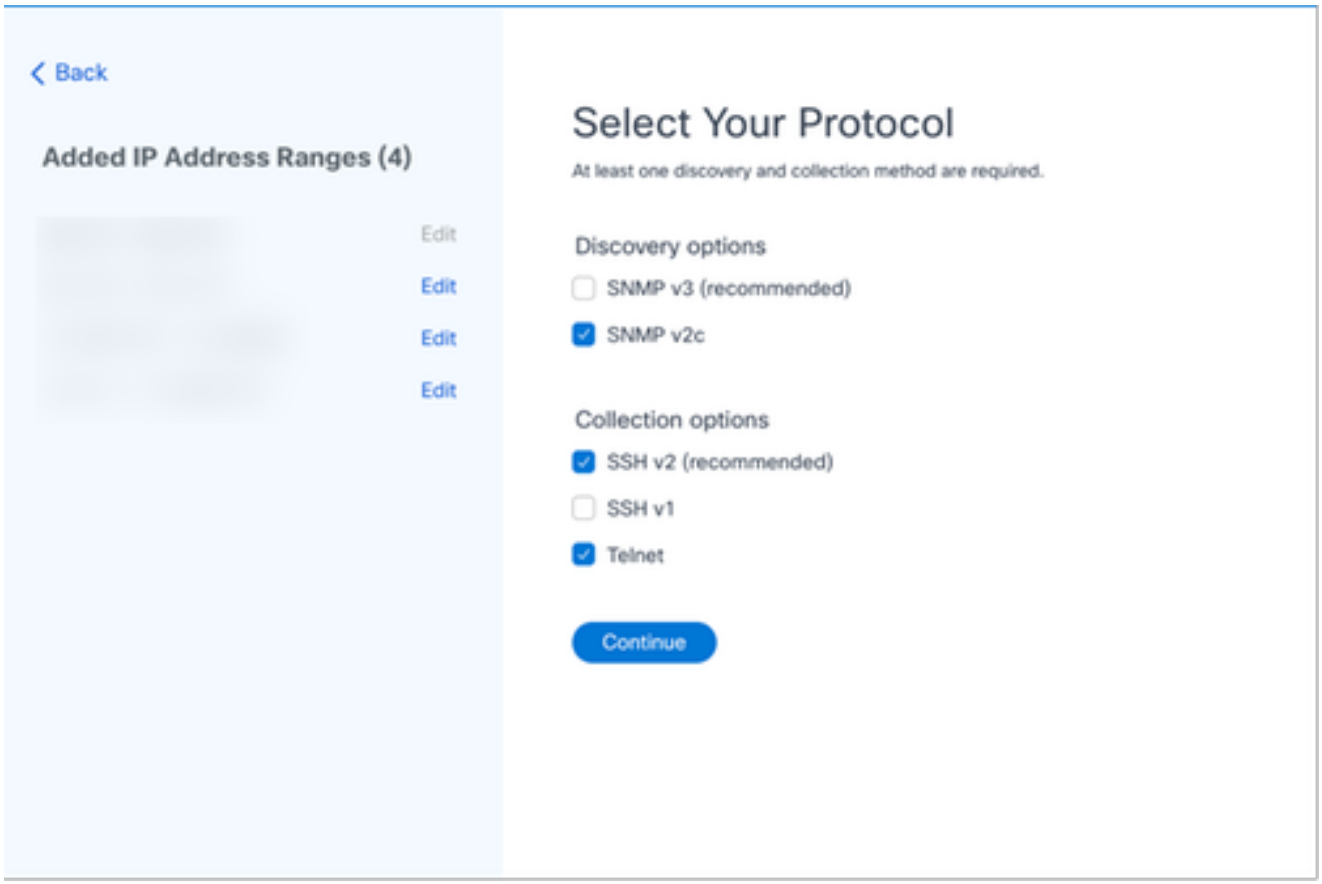


데이터 소스

3. Edit IP Address Range(IP 주소 범위 수정)를 클릭합니다. Connect to CX Cloud(CX 클라우드에 연결) 창이 열립니다.

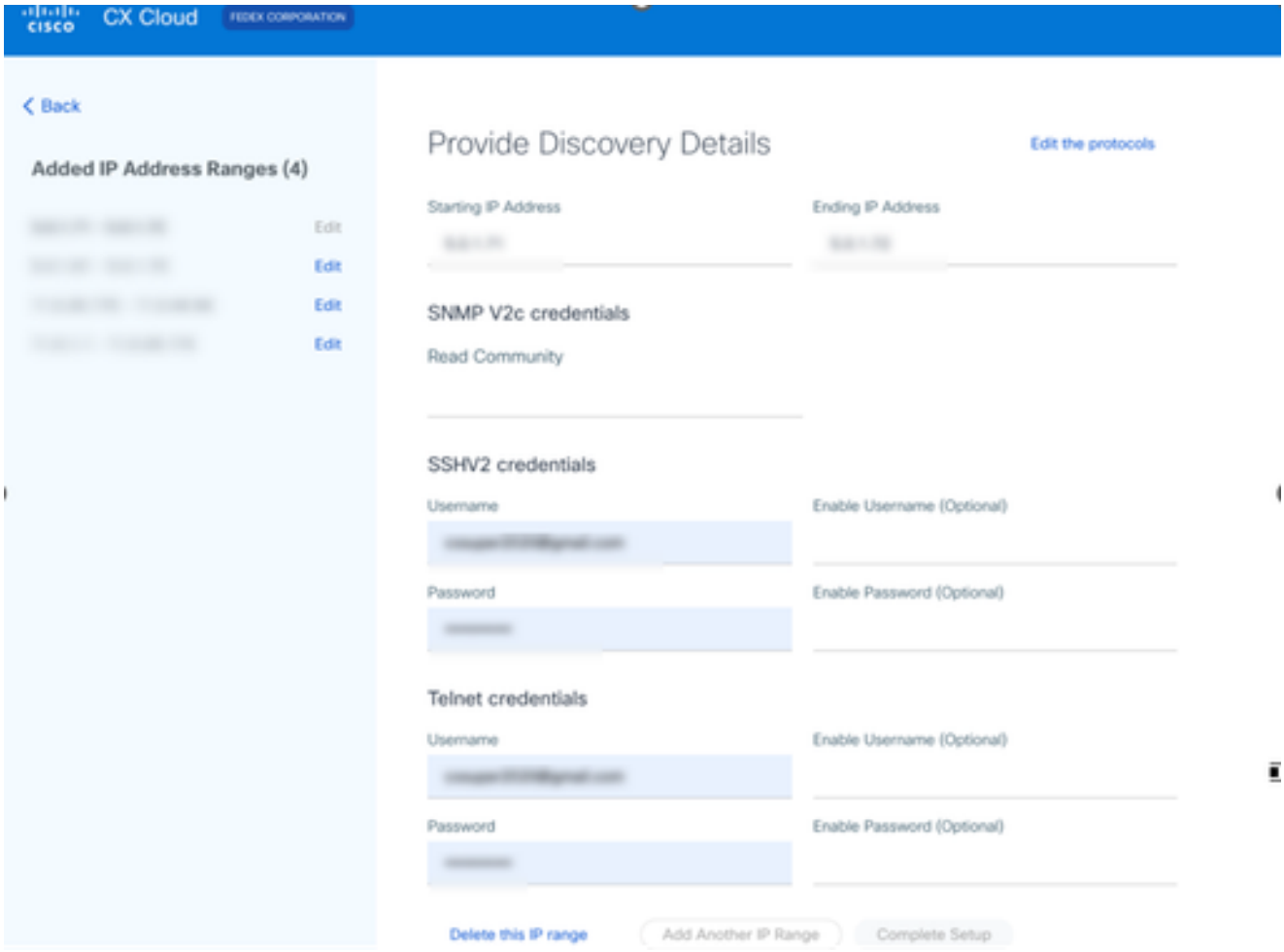


4. Edit the protocols를 클릭합니다. Select Your Protocol 창이 열립니다.



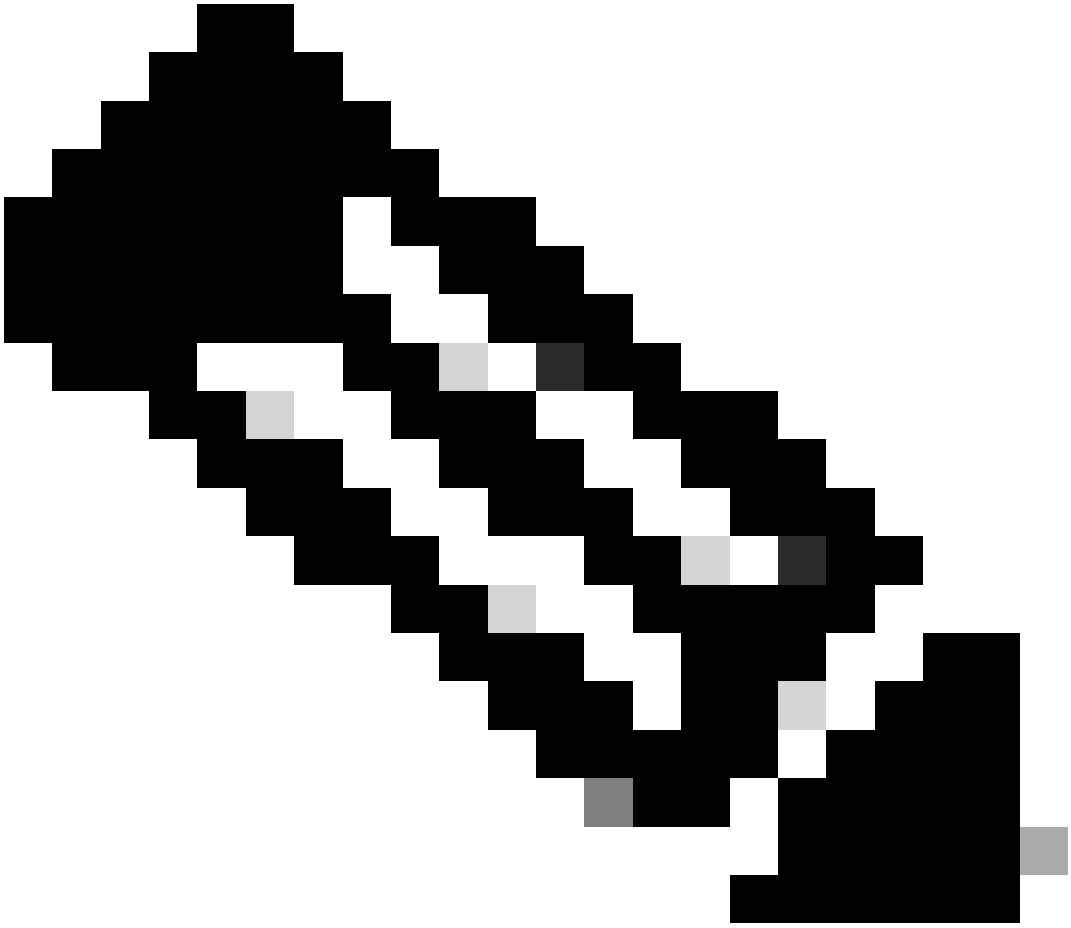
프로토콜 선택

5. 적절한 확인란을 선택하여 적용 가능한 프로토콜을 선택하고 계속을 눌러 검색 세부 정보 제공 창으로 돌아갑니다.

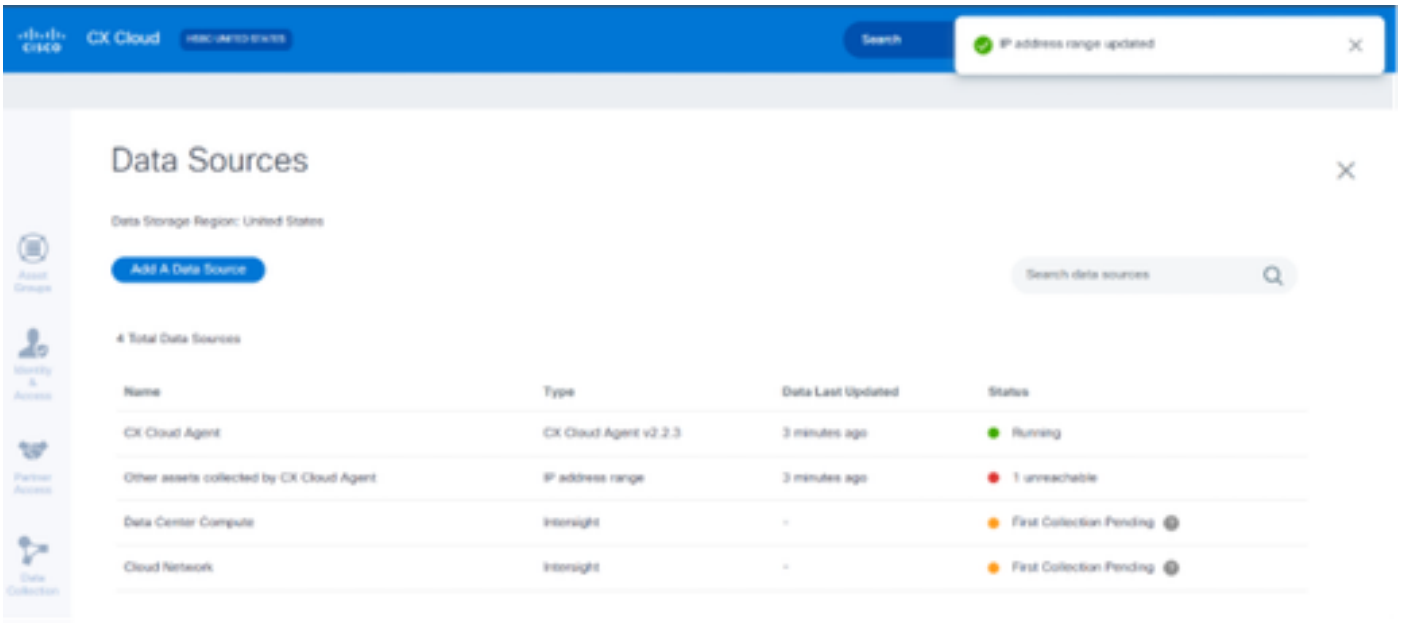


검색 세부 정보 제공

6. 필요에 따라 상세내역을 편집하고 설정 완료를 클릭합니다. Data Sources(데이터 소스) 창이 열리고 새로 추가된 IP 주소 범위를 추가했음을 확인하는 메시지가 표시됩니다.



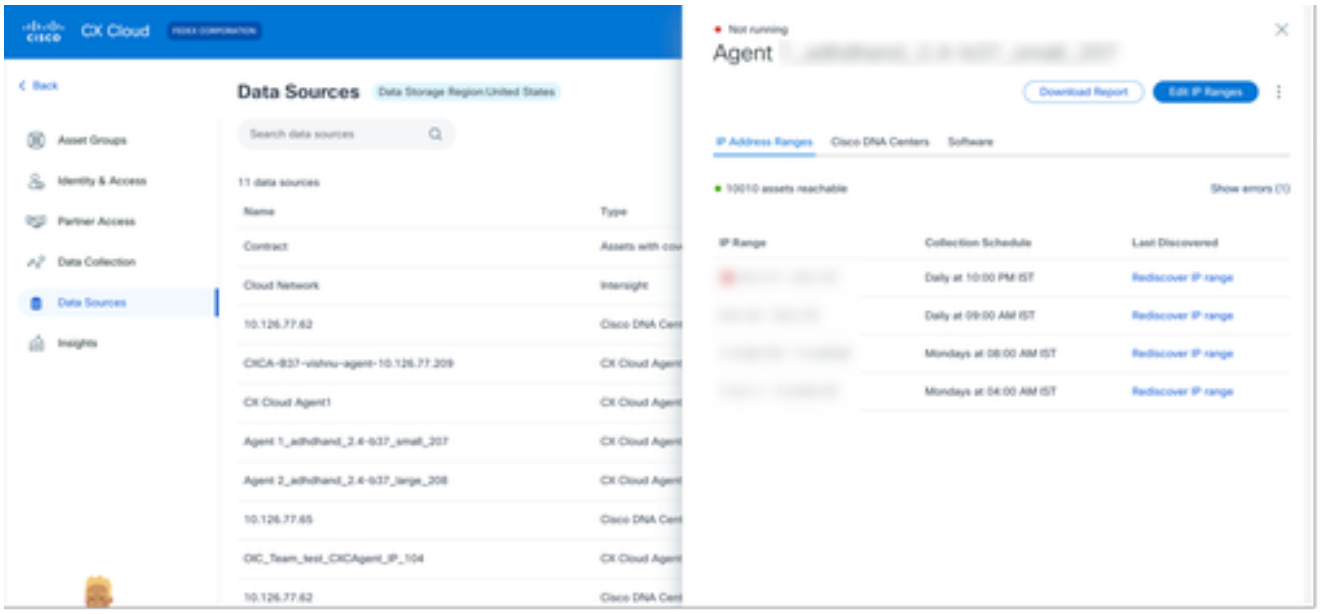
참고: 이 확인 메시지는 수정된 범위 내의 디바이스에 연결할 수 있는지 또는 해당 자격 증명이 허용되는지 여부를 확인하지 않습니다. 이 확인은 고객이 검색 프로세스를 시작할 때 발생합니다.



IP 범위 삭제

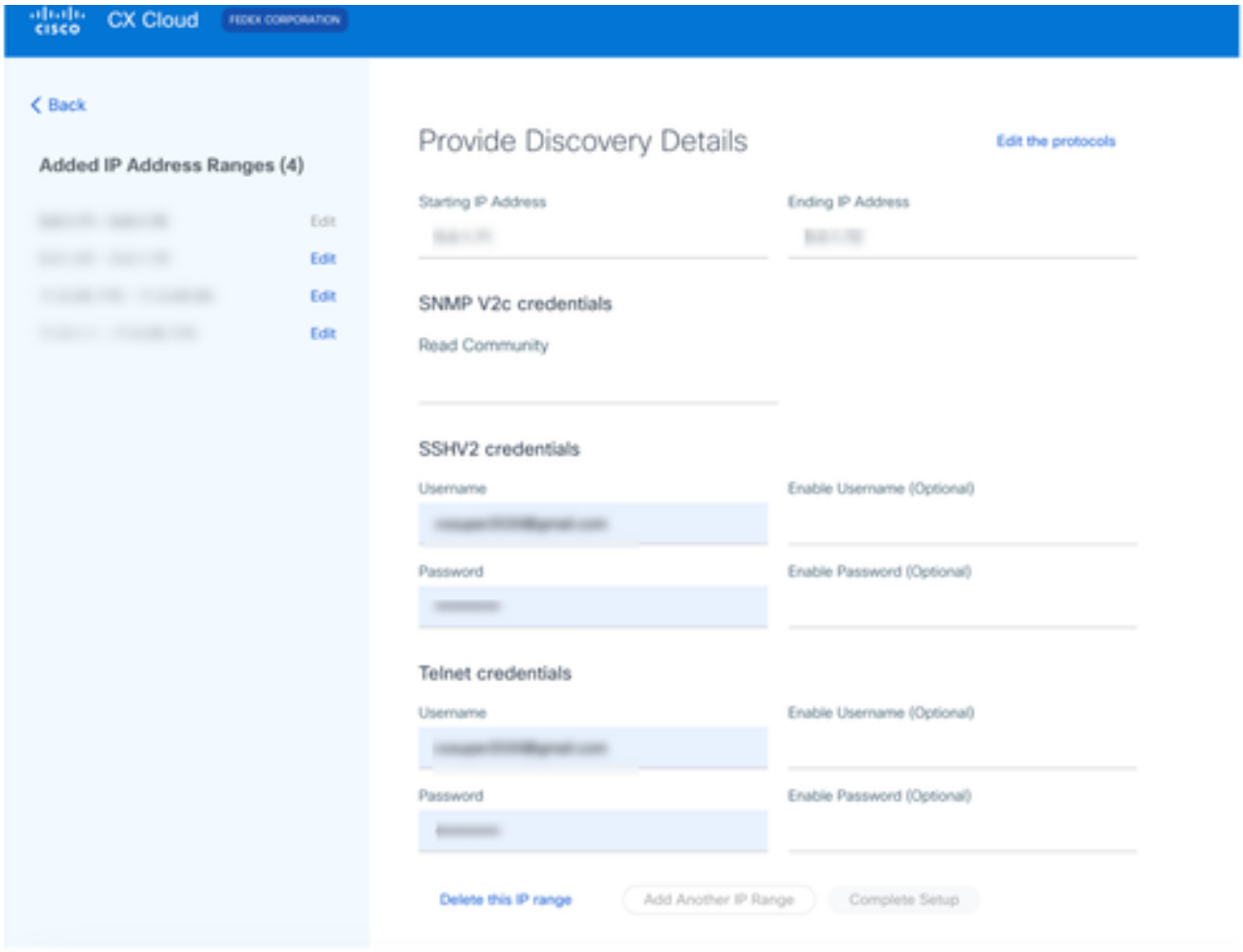
IP 범위를 삭제하려면

1. 데이터 소스 창으로 이동합니다.
2. 삭제해야 하는 IP 범위가 있는 해당 CX 에이전트를 선택합니다. 세부내용 창이 열립니다.



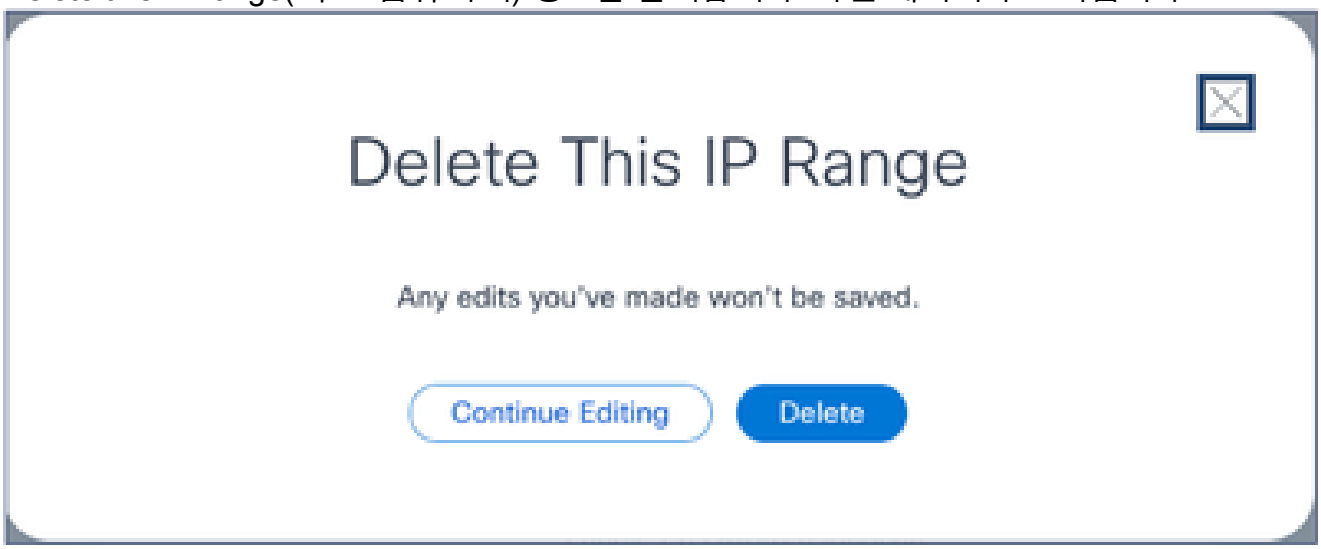
데이터 소스

3. Edit IP Ranges(IP 범위 수정)를 클릭합니다. 검색 세부 정보 제공 창이 열립니다.



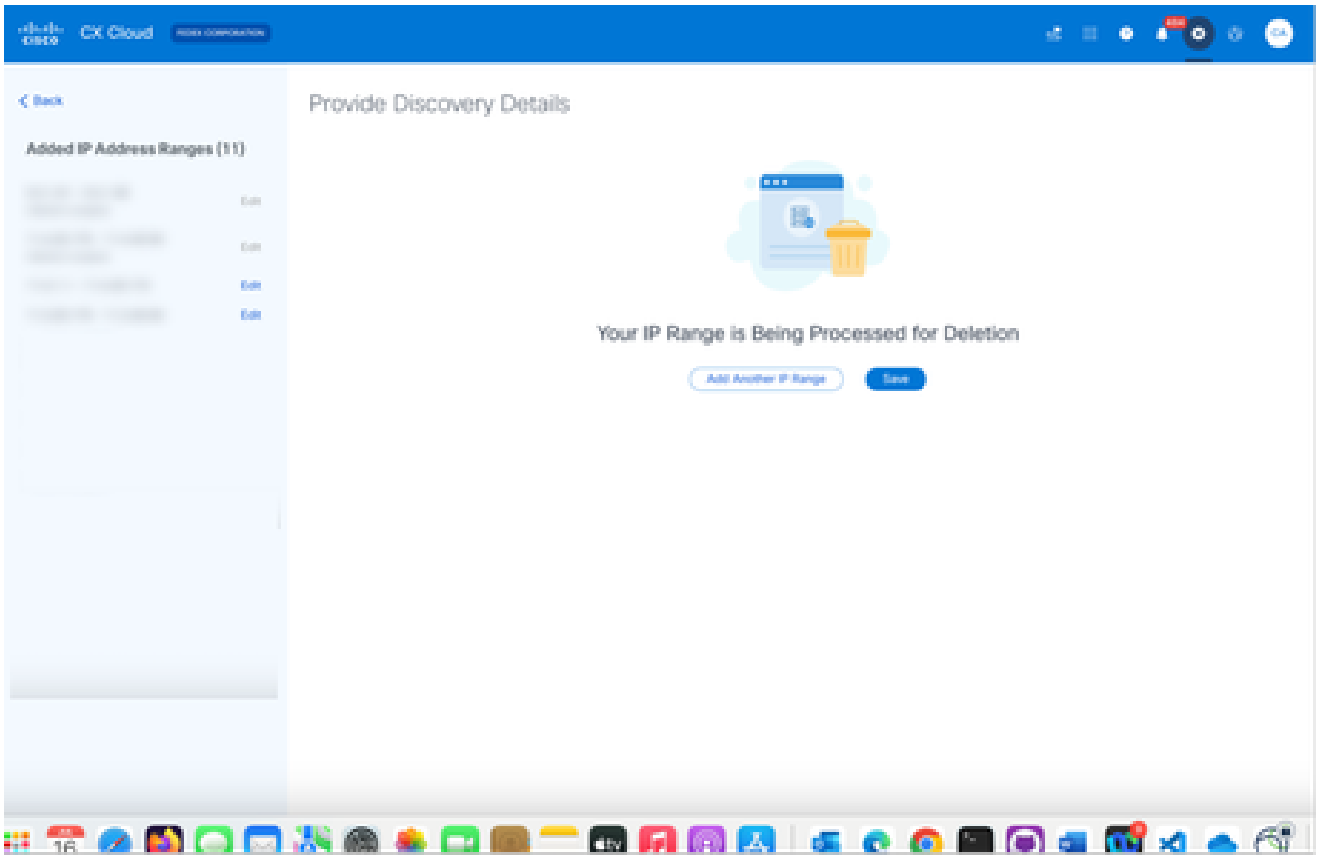
검색 세부 정보 제공

4. Delete this IP range(이 IP 범위 삭제) 링크를 클릭합니다. 확인 메시지가 표시됩니다.



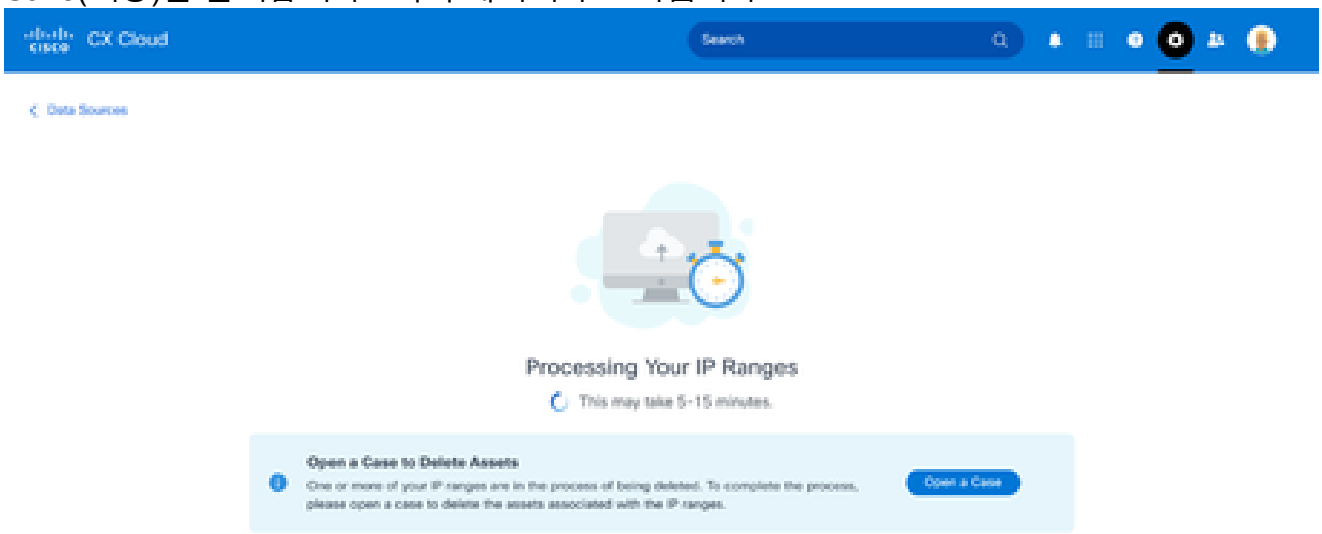
메시지 삭제 확인

5. 삭제를 클릭합니다.



IP 범위 삭제

6. Save(저장)를 클릭합니다.. 처리 메시지가 표시됩니다.



7. Open a Case(케이스 열기)를 클릭하여 IP 범위와 연결된 에셋을 삭제할 케이스를 생성합니다. 데이터 소스 창이 열리고 확인 메시지가 표시됩니다.

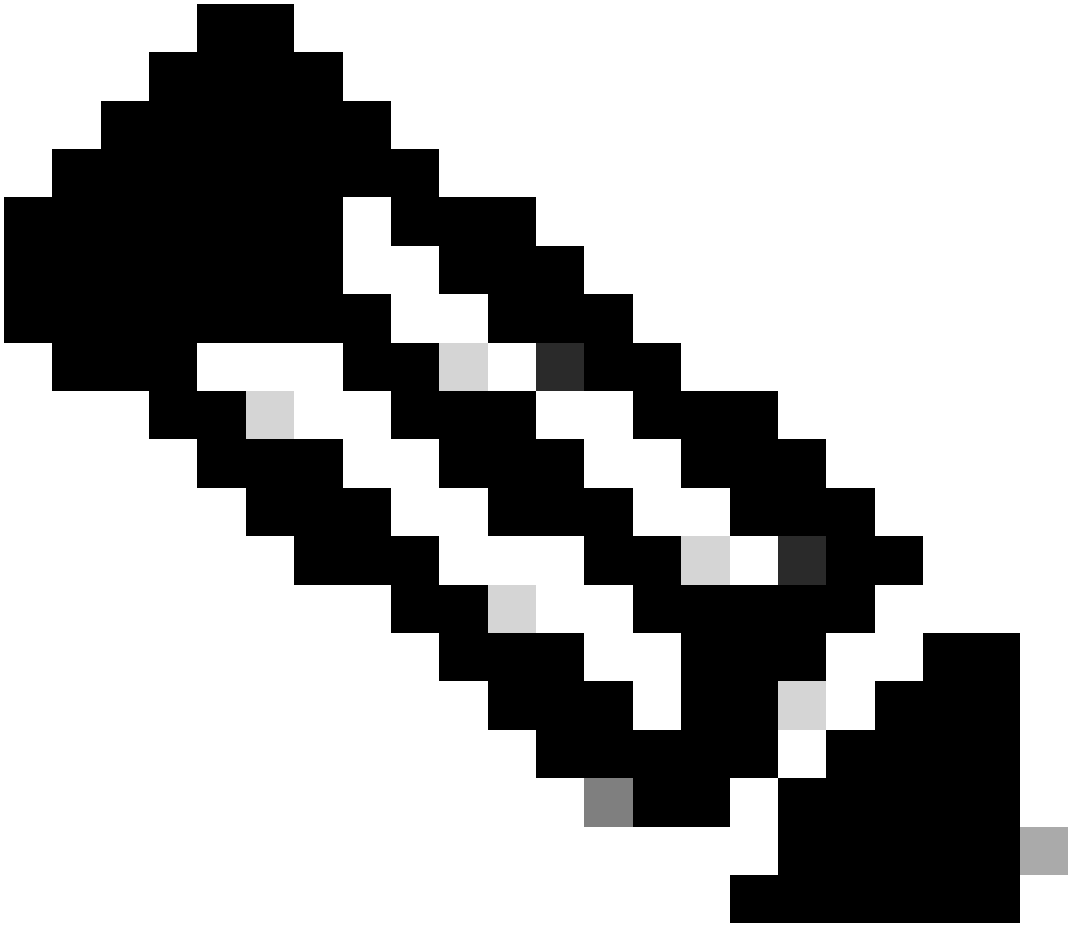
여러 컨트롤러에서 검색된 디바이스 정보

Catalyst Center 및 CX Agent에서 수집한 기타 자산(직접 디바이스 연결)이 동일한 CX Agent에 있는 경우 Cisco Catalyst Center 및 CX Agent에 대한 직접 디바이스 연결 둘 다에서 일부 디바이스를 검색하면 해당 디바이스에서 중복 데이터가 수집될 수 있습니다. 중복 데이터를 수집하고 하나의 컨트롤러로 디바이스를 관리하지 않으려면 CX Agent에서 디바이스를 관리하는 우선 순위를 결정해야 합니다.

- Cisco Catalyst Center에서 디바이스를 먼저 검색한 다음 직접 디바이스 연결(시드 파일 또는 IP 범위 사용)을 통해 다시 검색한 경우 Cisco Catalyst Center가 디바이스를 제어하는 데 우선합니다.
- CX Agent에 대한 직접 디바이스 연결을 통해 디바이스를 먼저 검색한 다음 Cisco Catalyst Center에서 다시 검색한 경우 Cisco Catalyst Center가 디바이스를 제어하는 데 우선적으로 적용됩니다.

진단 검사 예약

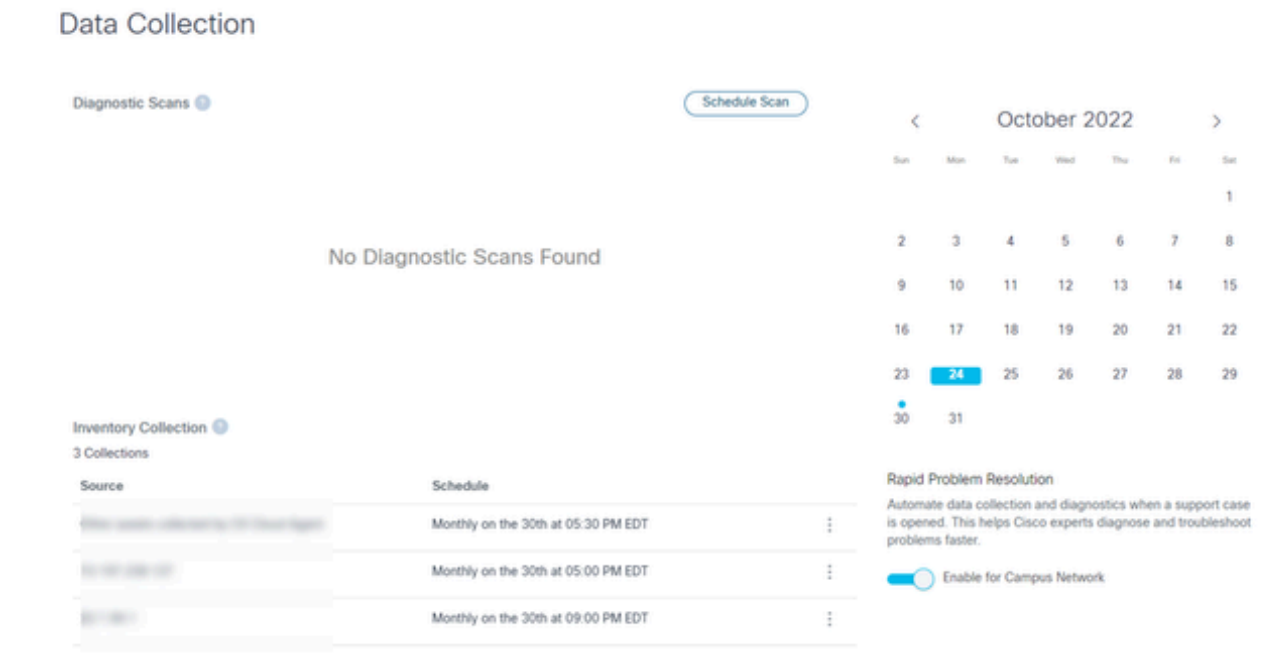
고객은 CX 클라우드에서 온디맨드 진단 검사를 예약하여 적격 성공 트랙과 지원 범위에 포함된 디바이스를 대상으로 Advisories의 Priority Bug를 입력할 수 있습니다.



참고: Cisco에서는 인벤토리 수집 일정과 최소 6~7시간 간격을 두고 진단 스캔을 예약하거나 온디맨드 스캔을 시작하여 중복되지 않도록 할 것을 권장합니다. 여러 진단 스캔을 동시에 실행하면 스캔 프로세스가 느려지고 스캔 실패가 발생할 수 있습니다.

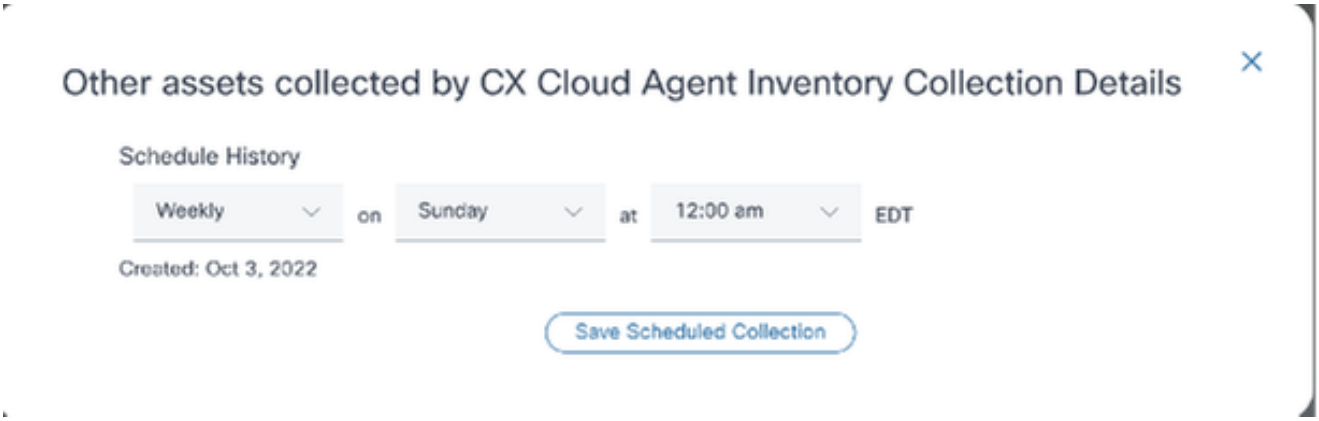
진단 스캔을 예약하려면

1. 홈 페이지에서 설정(기어) 아이콘을 클릭합니다.
2. 데이터 소스 페이지의 왼쪽 창에서 데이터 수집을 선택합니다.
3. Schedule Scan(스캔 예약)을 클릭합니다.



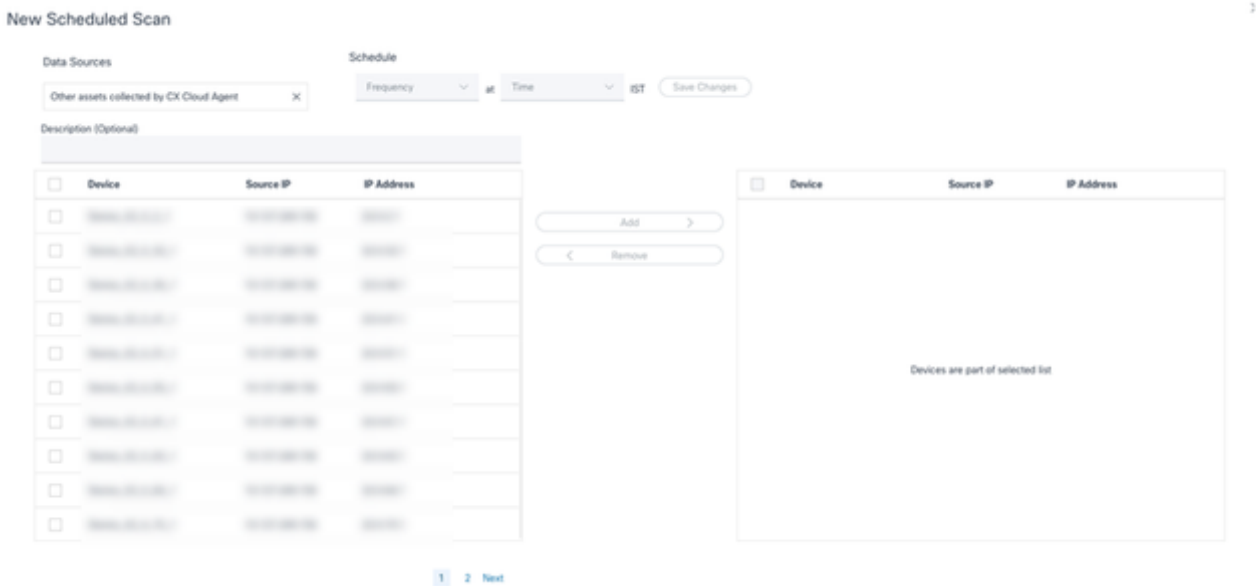
스캔 예약

4. 이 스캔에 대한 일정을 구성합니다.



스캔 일정 구성

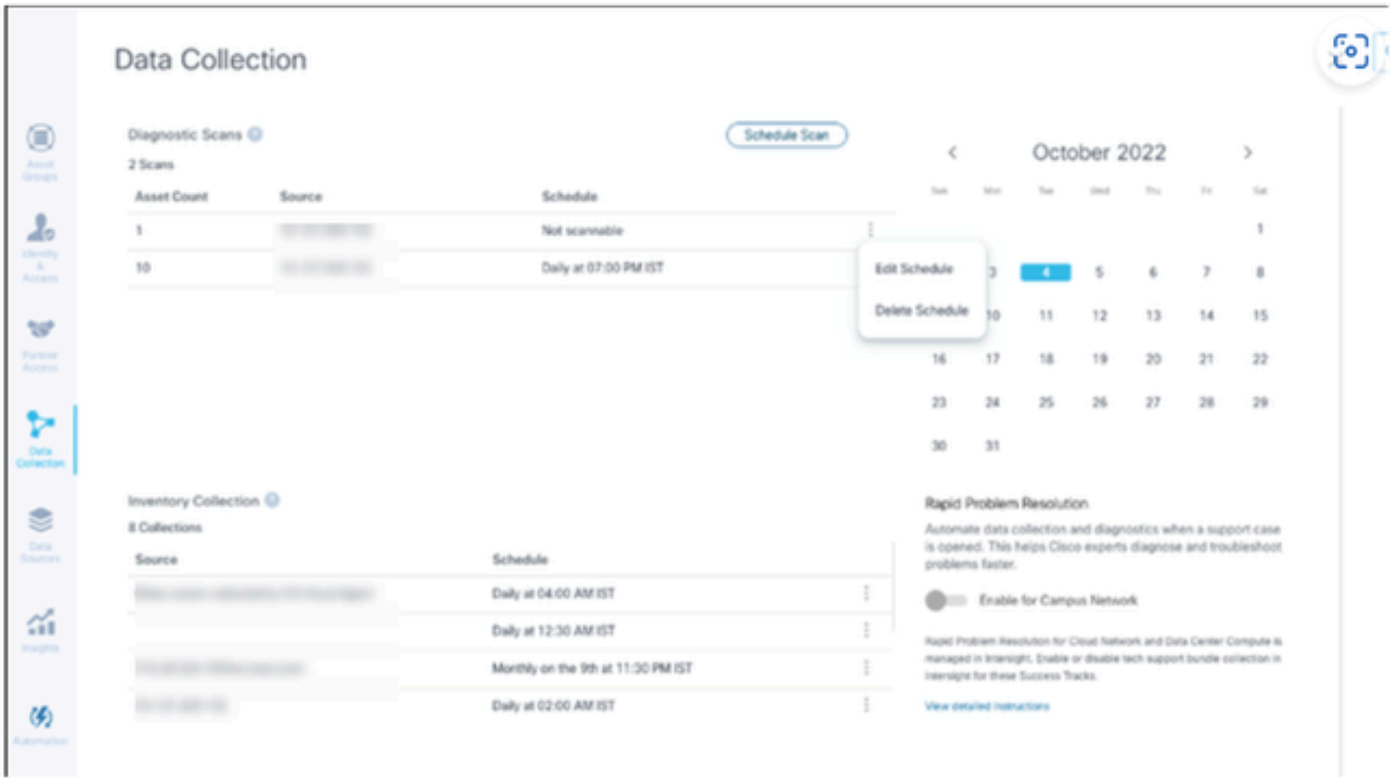
5. Devices(디바이스) 목록에서 스캔할 모든 디바이스를 선택하고 Add(추가)를 클릭합니다.



스캔 예약

6. 예약이 완료되면 Save Changes(변경 사항 저장)를 클릭합니다.

진단 검사 및 인벤토리 수집 일정은 데이터 수집 페이지에서 편집하고 삭제할 수 있습니다.



Edit and Delete Schedule 옵션이 있는 데이터 수집

CX 에이전트 VM을 중대형 구성으로 업그레이드

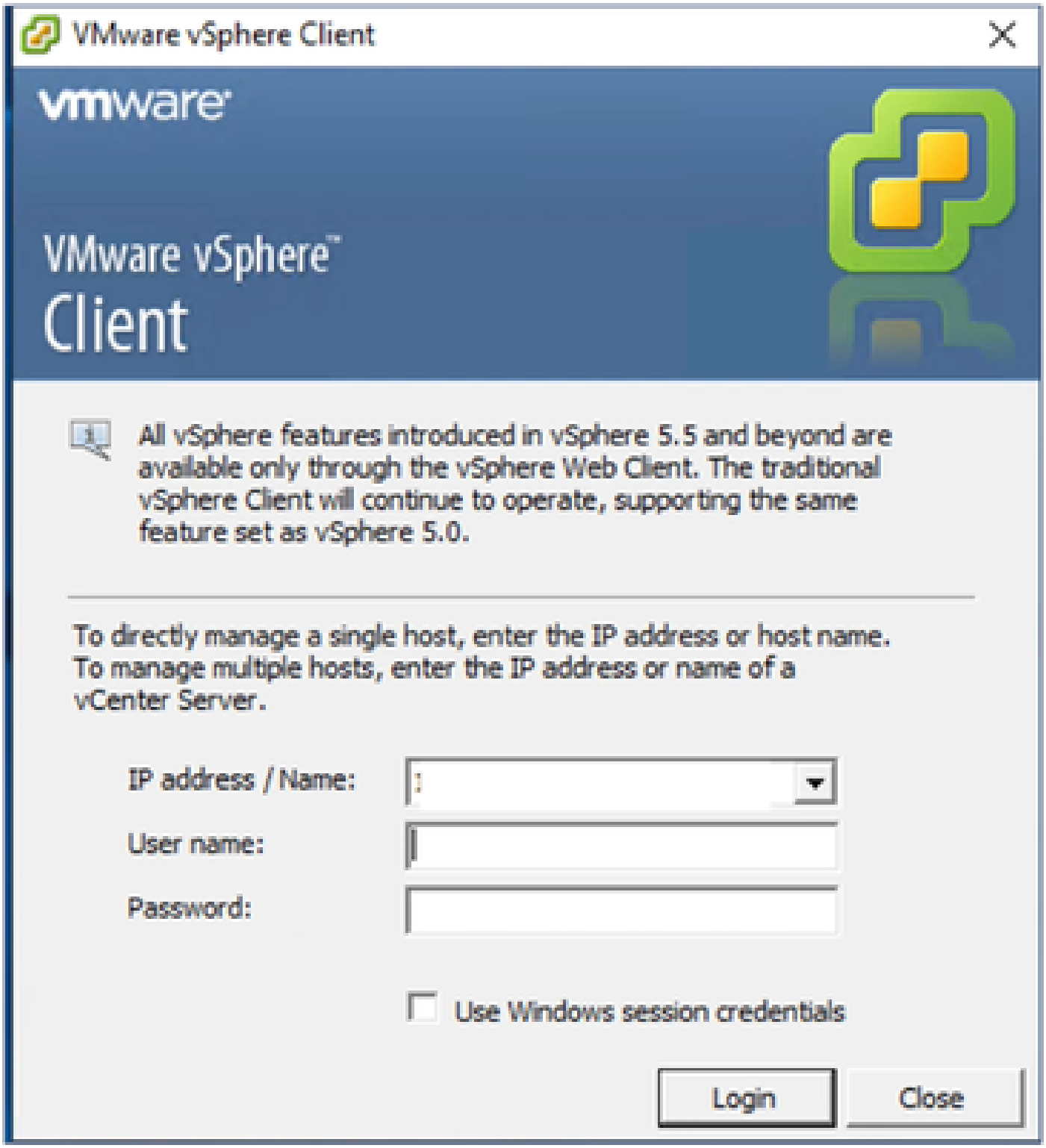
VM이 업그레이드되면 다음을 수행할 수 없습니다.

- 대규모 또는 중간 규모에서 소규모 구성으로 다운스케일
- 대규모 구성에서 중간 구성으로 다운스케일
- 중형 구성에서 대형 구성으로 업그레이드

VM을 업그레이드하기 전에 장애 시 복구를 위해 스냅샷을 생성하는 것이 좋습니다. 자세한 내용은 CX 클라우드 VM 백업 및 복원을 참조하십시오.

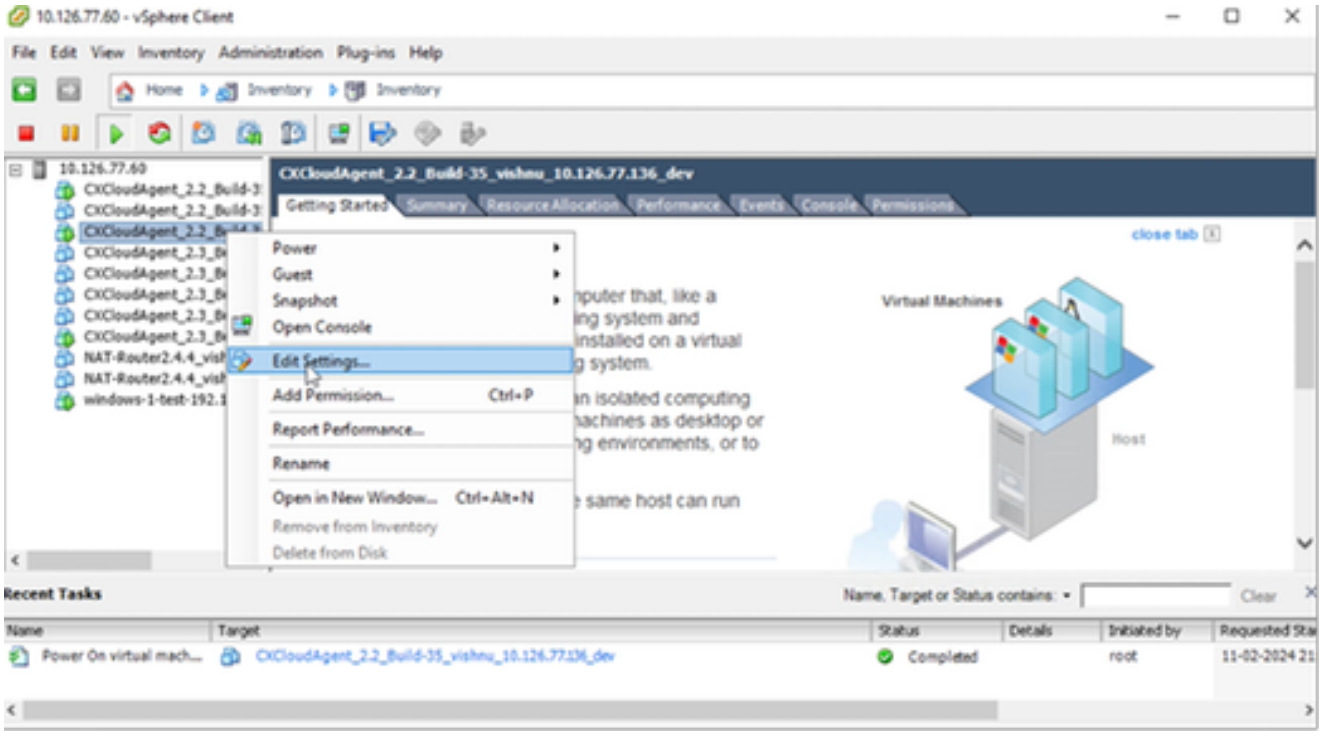
VMware vSphere Thick Client를 사용하여 재구성

기존 VMware vSphere Thick Client를 사용하여 VM 컨피그레이션을 업그레이드하려면



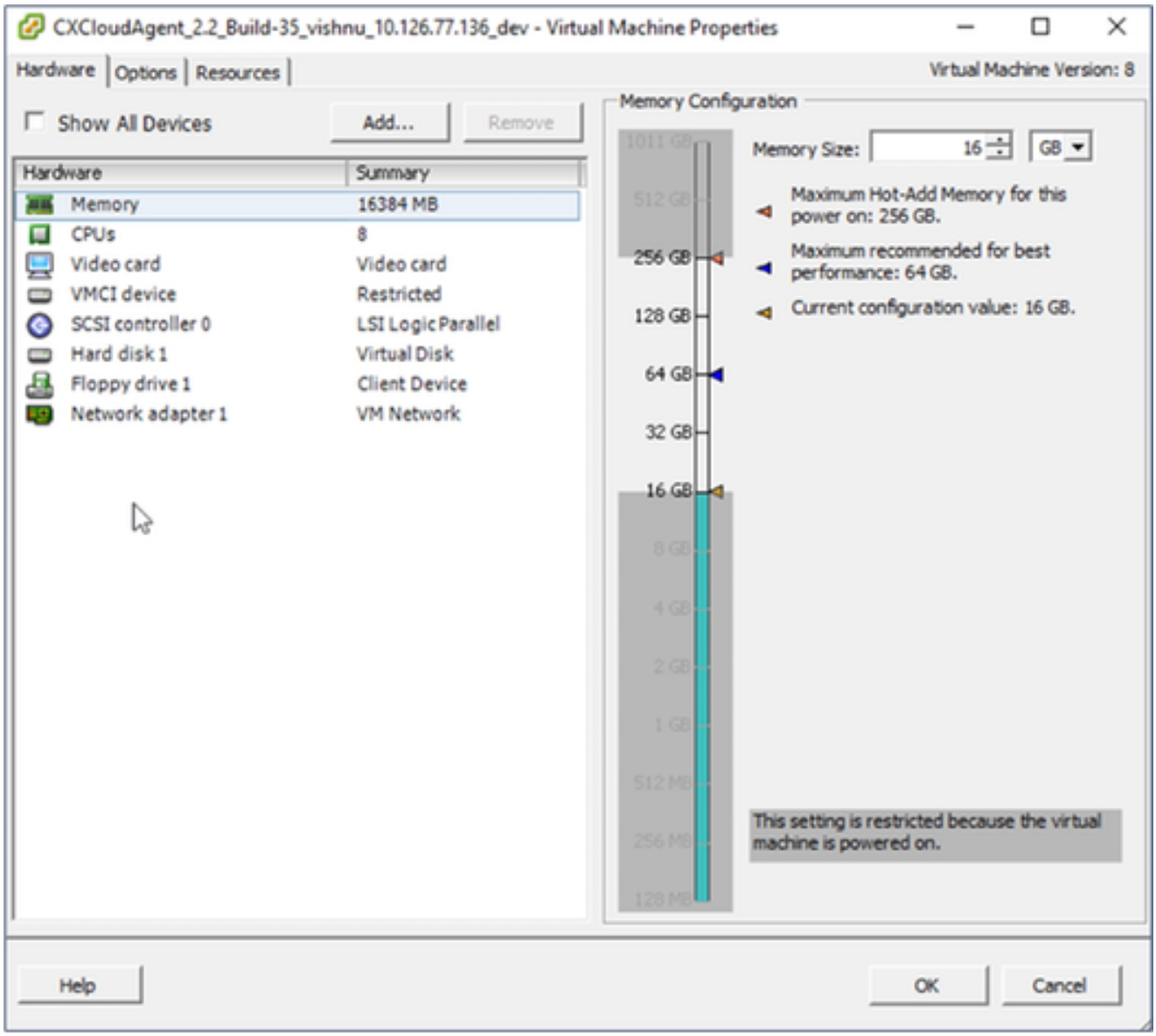
vSphere Client

1. VMware vSphere Client에 로그인합니다. 홈 페이지에 VM 목록이 표시됩니다.



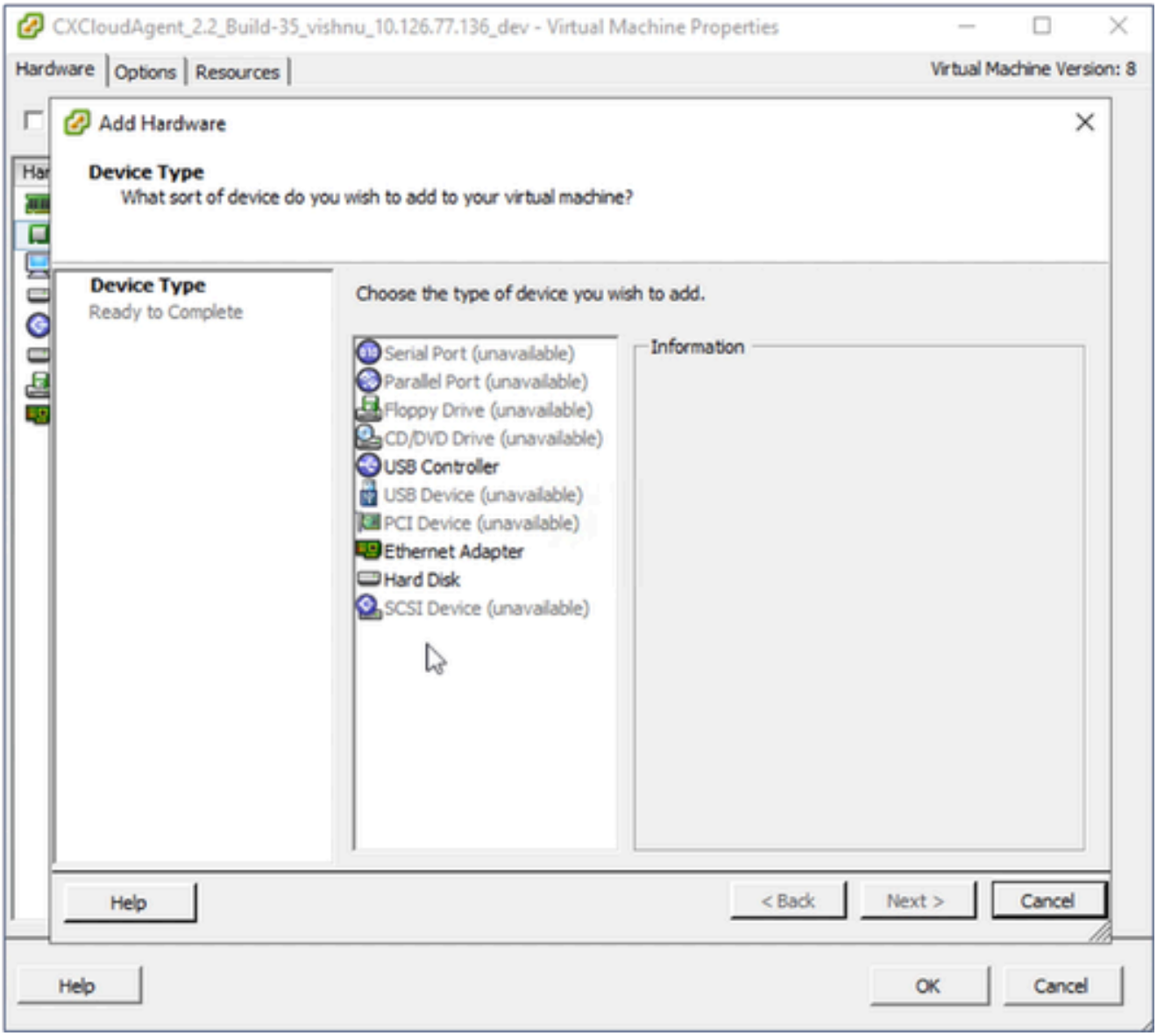
설정 편집

2. 대상 VM을 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 Edit Settings(설정 편집)를 선택합니다. VM Properties(VM 속성) 창이 열립니다.



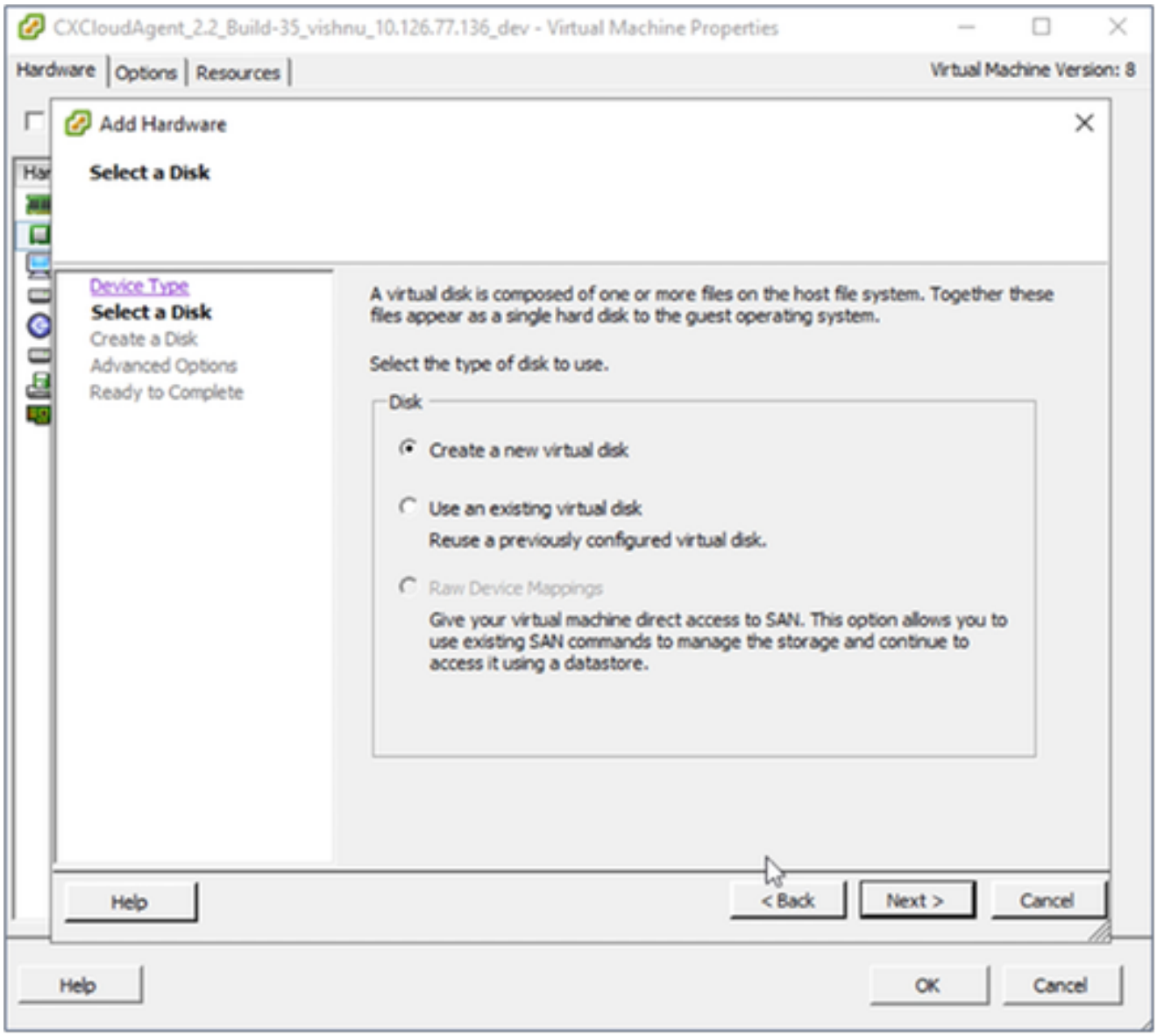
VM 속성

3. 지정된 대로 메모리 크기 값을 업데이트합니다.
   보통: 32GB(32768MB)
   큼: 64GB(65536MB)
4. CPU를 선택하고 지정된 대로 값을 업데이트합니다.
   보통: 16코어(8소켓 *2코어/소켓)
   대형: 32코어(16소켓 *2코어/소켓)
5. Add(추가)를 클릭합니다. Add Hardware 창이 열립니다.



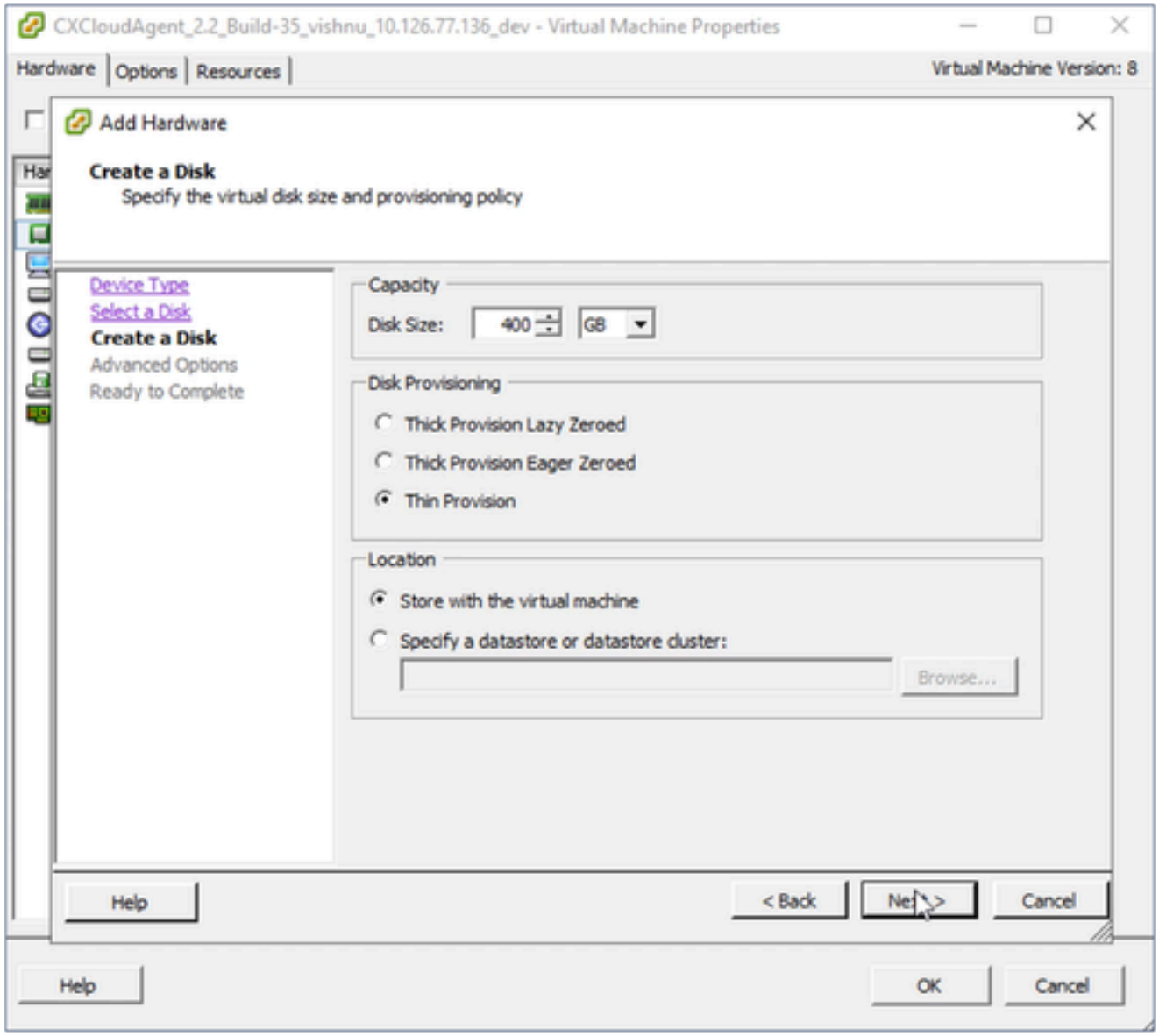
디바이스 유형

6. Device Type(디바이스 유형)으로 Hard Disk(하드 디스크)를 선택합니다.
7. Next(다음)를 클릭합니다.



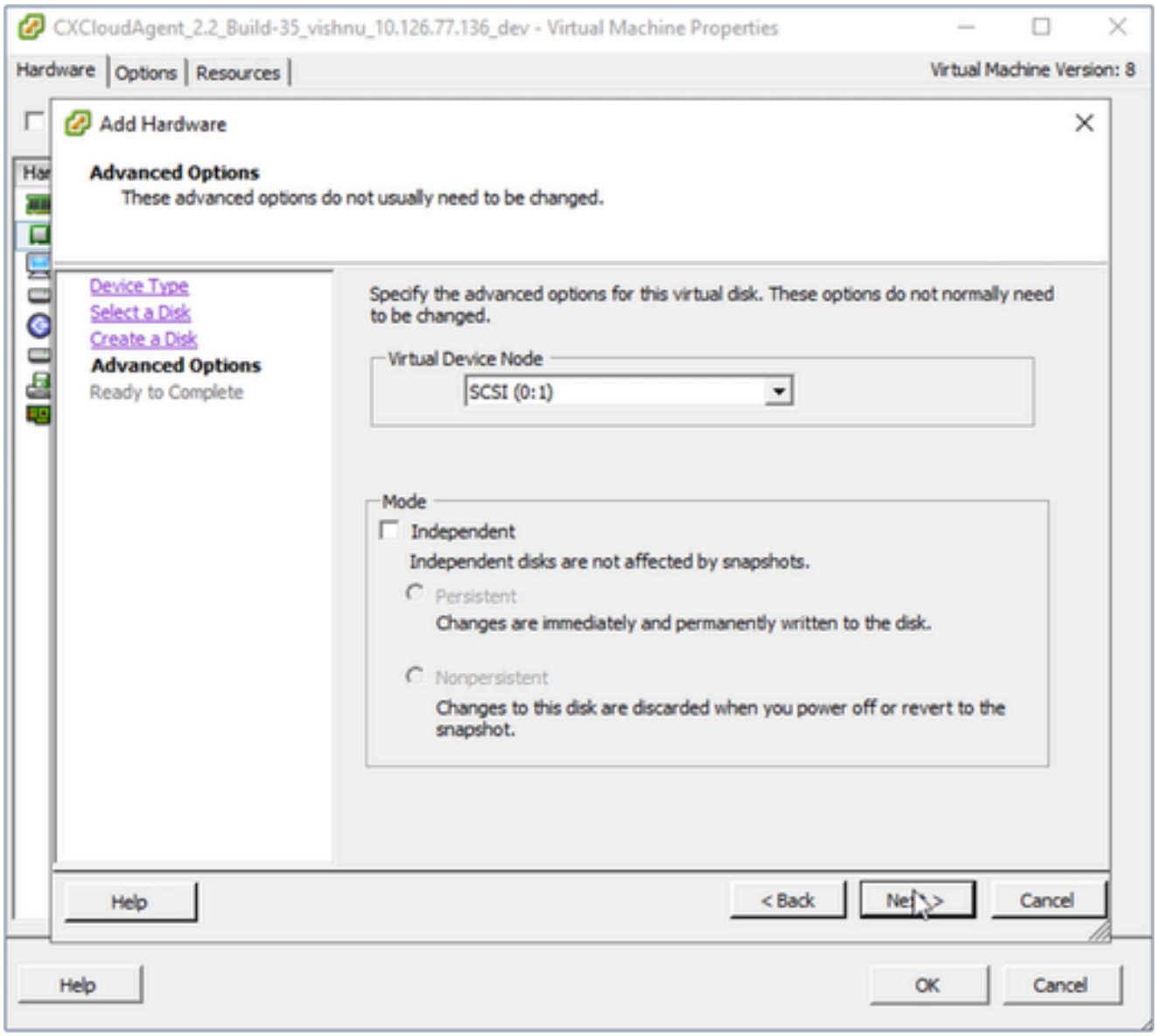
디스크 선택

8. Create a new virtual disk(새 가상 디스크 생성) 라디오 버튼을 선택하고 Next(다음)를 클릭합니다.



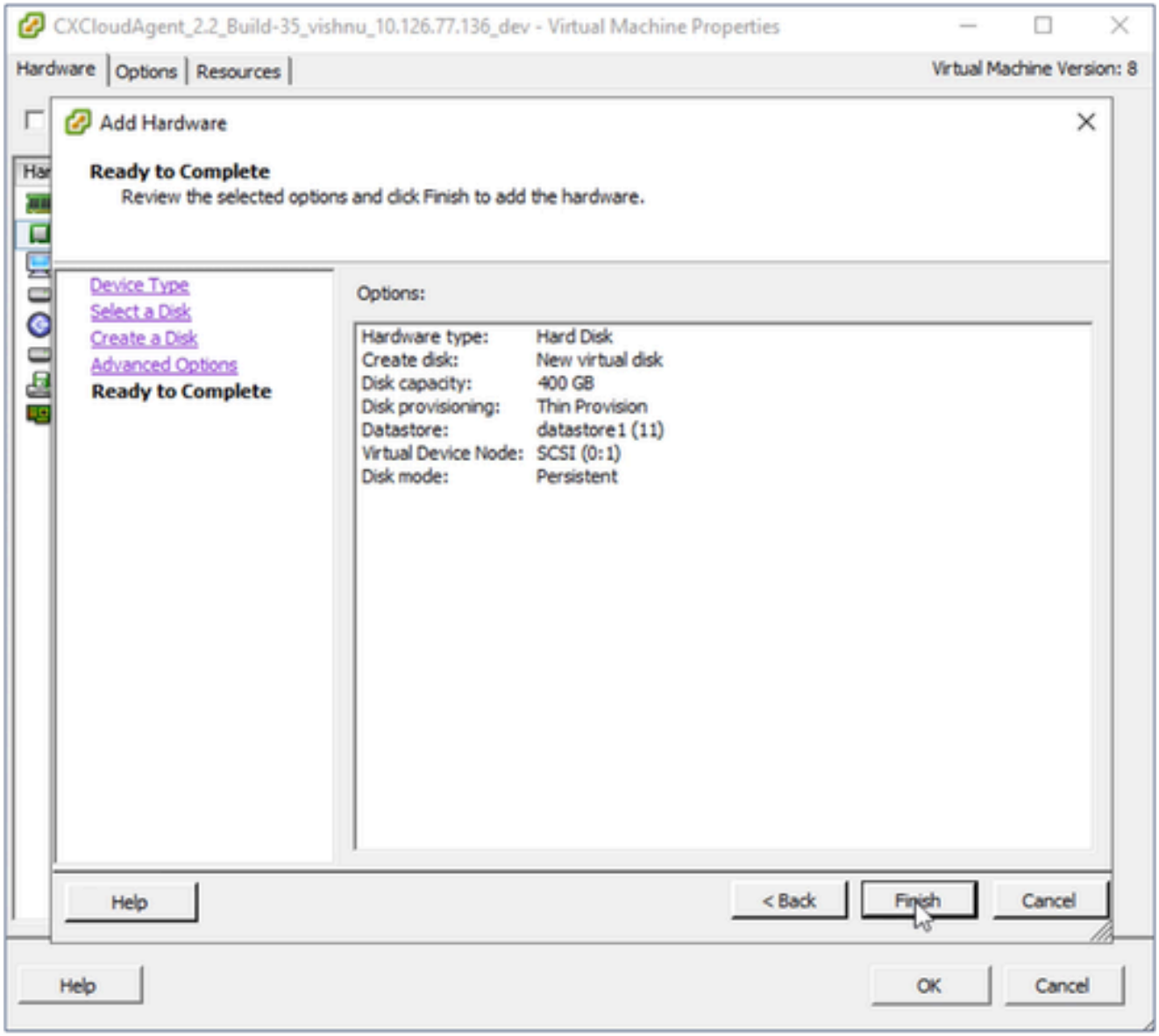
디스크 생성

9. 지정된 대로 Capacity(용량) > Disk Size(디스크 크기)를 업데이트합니다.
   중소 규모: 400GB(초기 크기 200GB, 총 공간 600GB 증가)
   소형 ~ 대형: 1000GB(초기 크기 200GB, 총 공간 1200GB로 증가)
10. Disk Provisioning(디스크 프로비저닝)에 대한 Thin Provision(씬 프로비저닝) 라디오 버튼을 선택합니다.
11. Next(다음)를 클릭합니다. 고급 옵션 창이 표시됩니다.



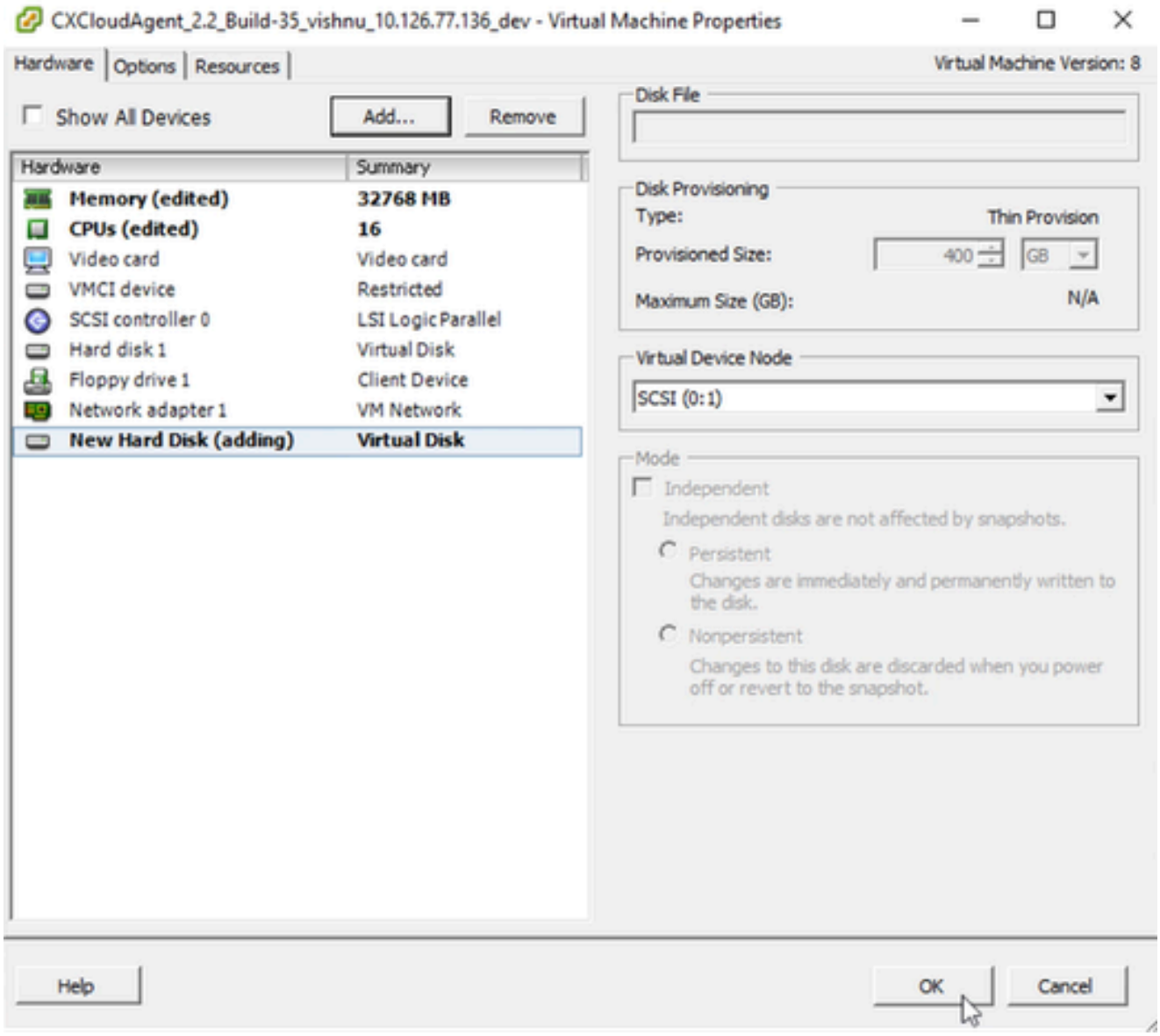
고급 옵션

12. 변경하지 마십시오. 계속하려면 다음을 클릭합니다.



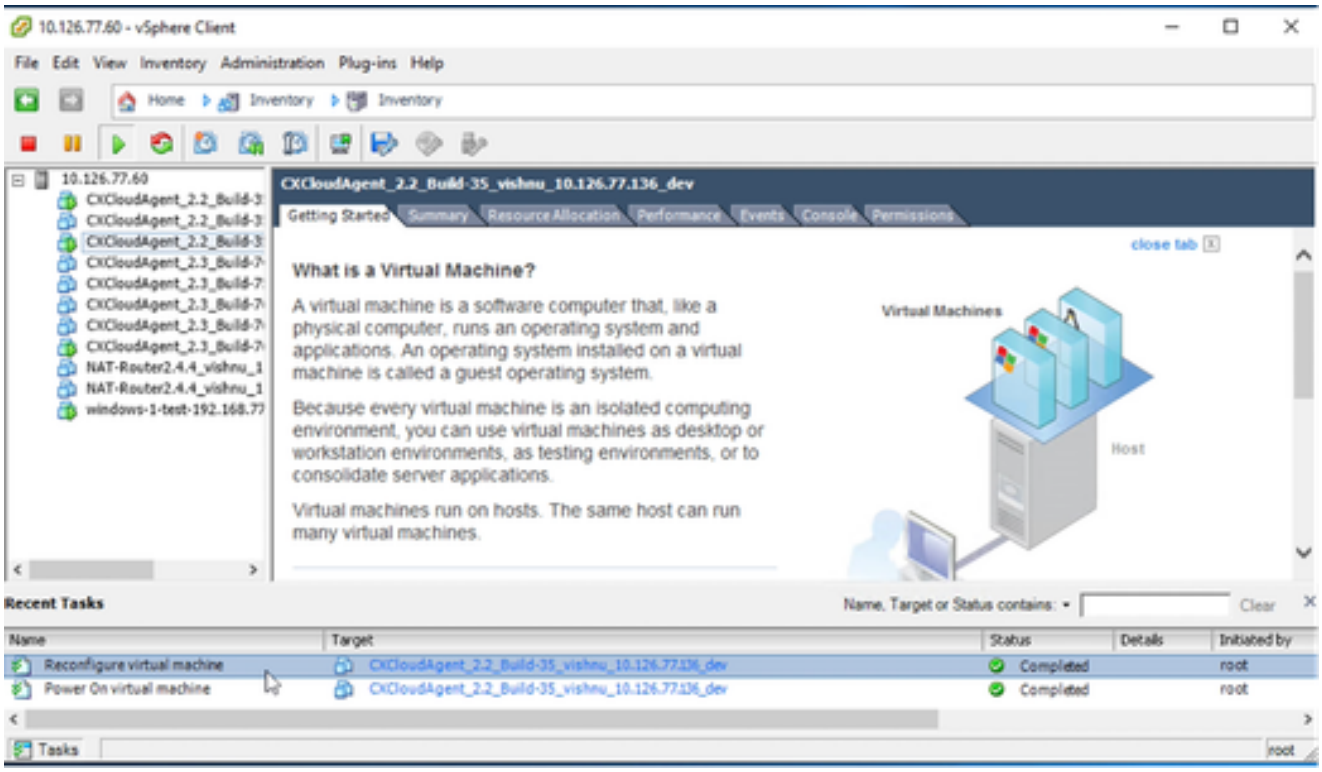
완료 준비

13. Finish(마침)를 클릭합니다.

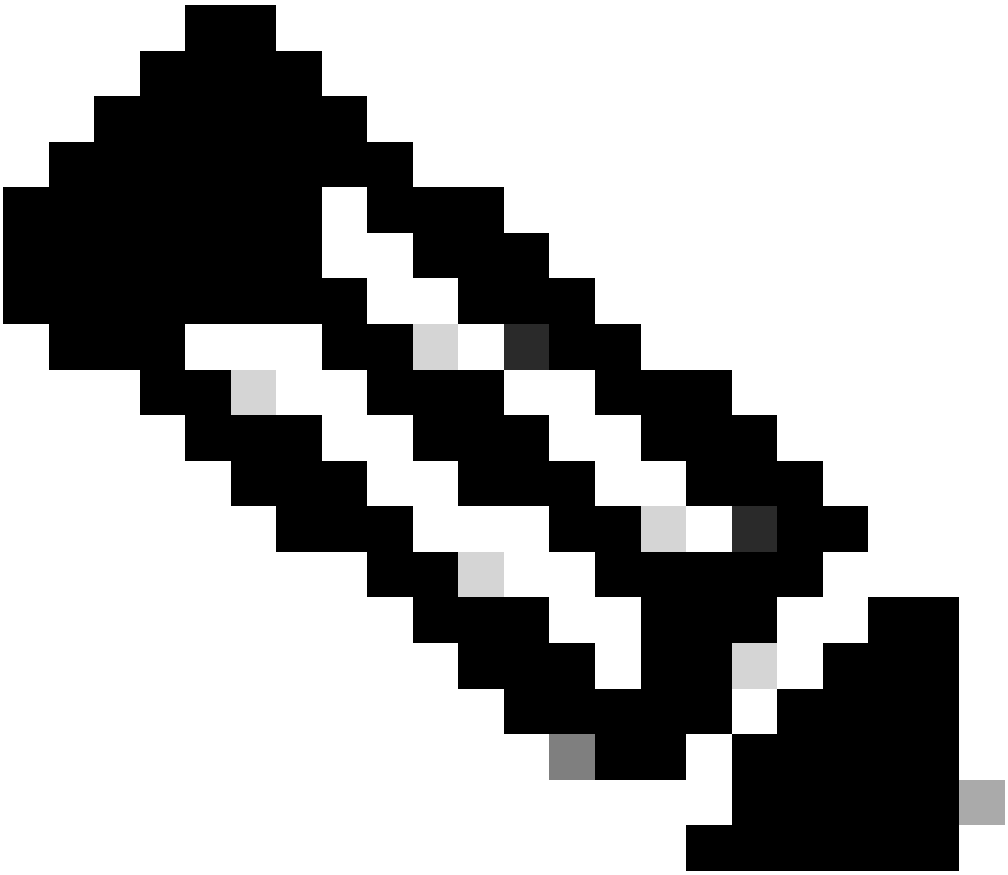


하드웨어

14. OK(확인)를 클릭하여 재컨피그레이션을 완료합니다. 완료된 재구성이 최근 작업 패널에 표시됩니다.


10.126.77.60 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
10.126.77.60
CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev
Getting Started Summary Resource Allocation Performance Events Console Permissions
close tab
What is a Virtual Machine?
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.
Virtual machines run on hosts. The same host can run many virtual machines.
Virtual Machines
Host
Recent Tasks
Name, Target or Status contains:
Clear
Name
Target
Status
Details
Initiated by
Reconfigure virtual machine
CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev
Completed
root
Power On virtual machine
CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev
Completed
root
Tasks
root

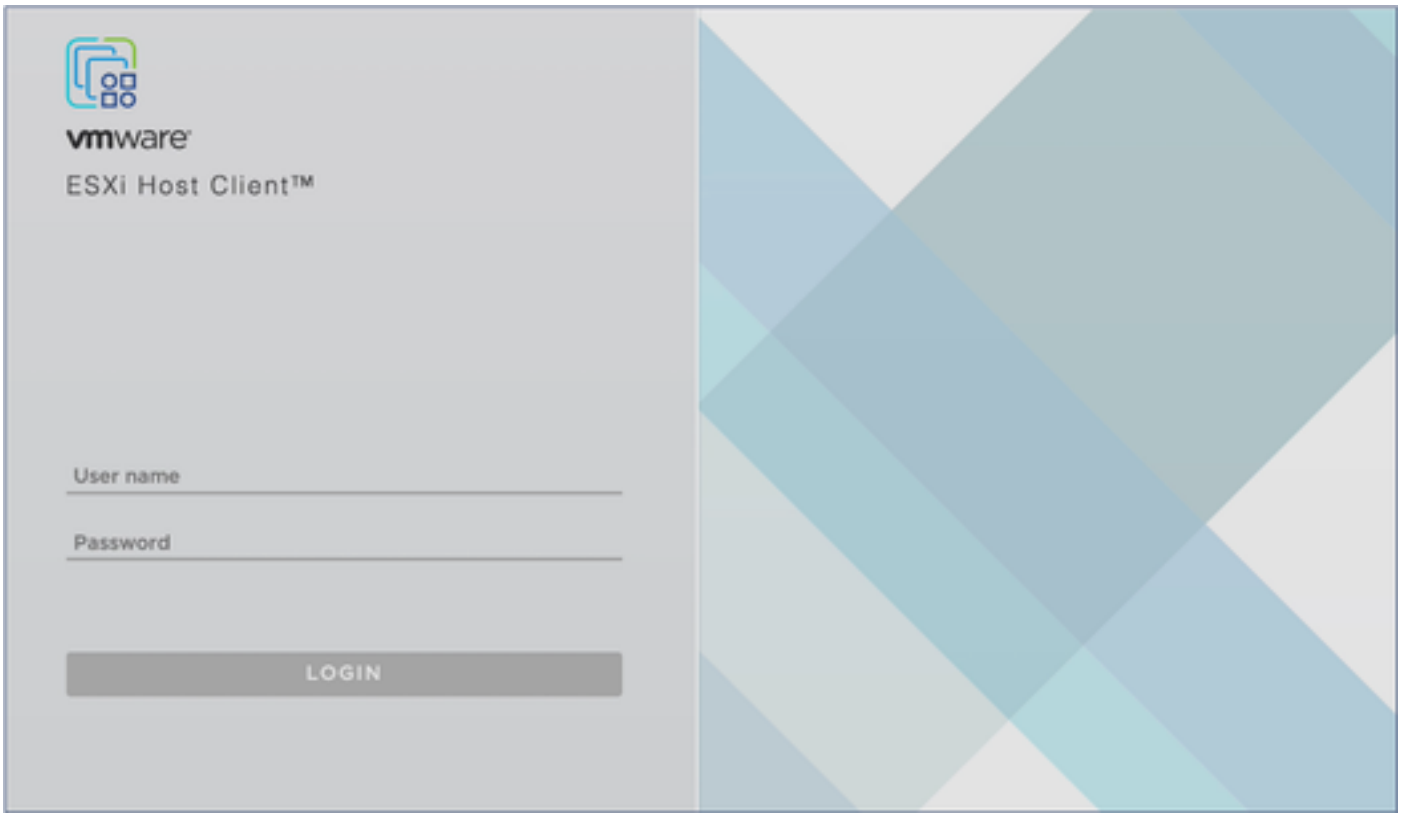
최근 작업



참고: 컨피그레이션 변경을 완료하는 데 약 5분이 소요됩니다.

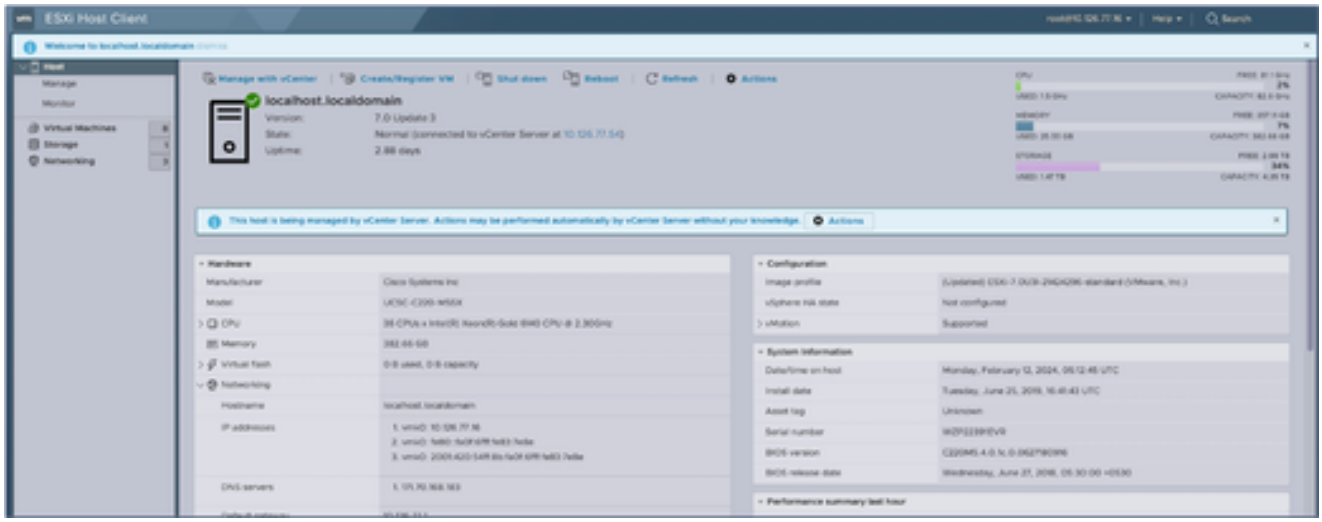
웹 클라이언트 ESXi v6.0을 사용하여 재구성

웹 클라이언트 ESXi v6.0을 사용하여 VM 컨피그레이션을 업데이트하려면



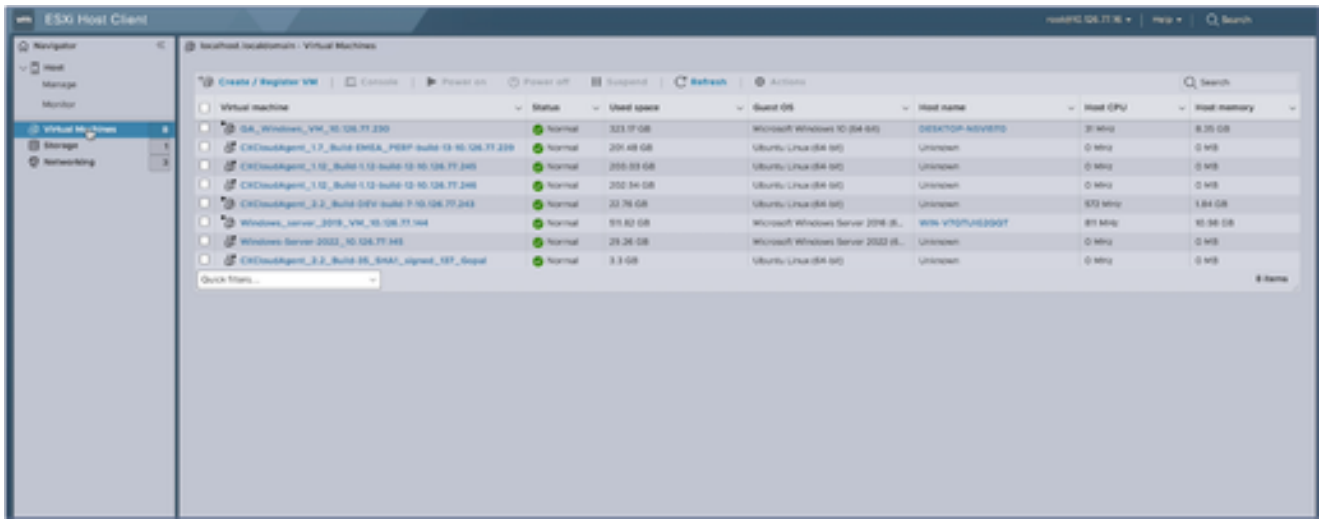
ESXi 클라이언트

1. VMware ESXi 클라이언트에 로그인합니다. 홈 페이지가 표시됩니다.



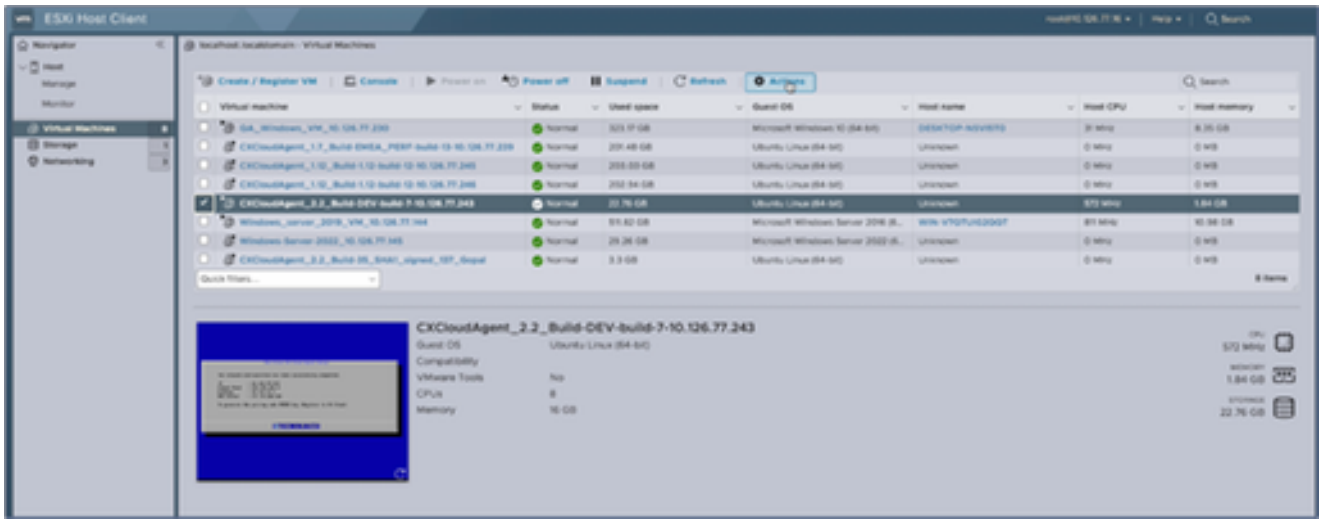
ESXi 홈 페이지

2. VM 목록을 표시하려면 Virtual Machine(가상 머신)을 클릭합니다.



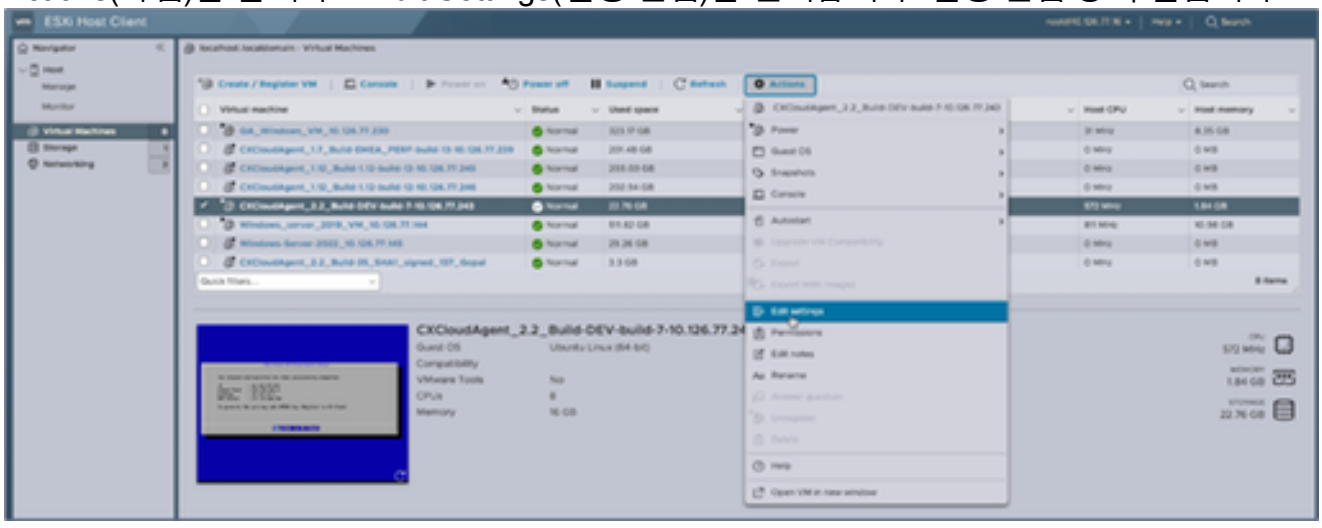
VM 목록

3. 대상 VM을 선택합니다.

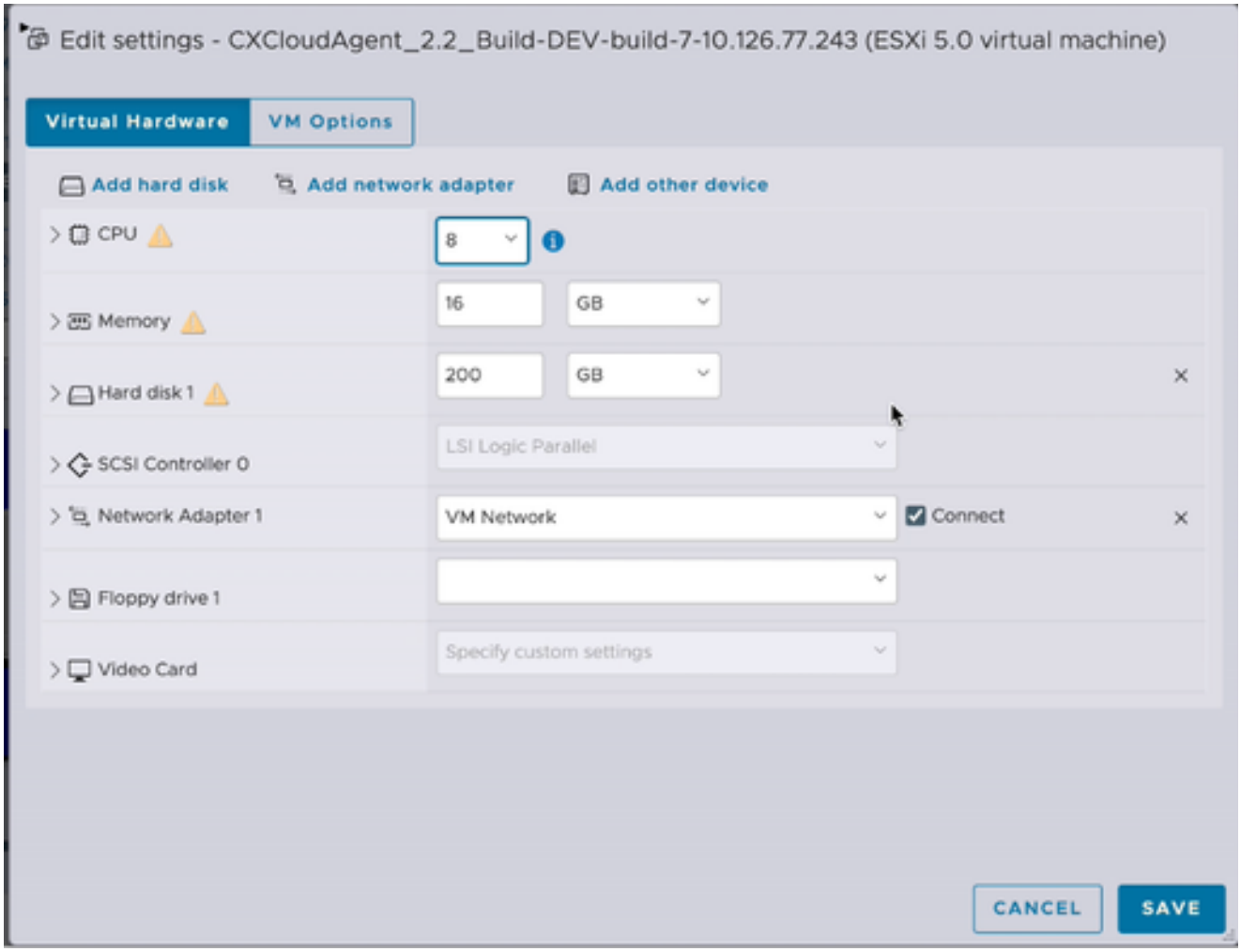


대상 VM

4. Actions(작업)를 클릭하고 Edit Settings(설정 편집)를 선택합니다. 설정 편집 창이 열립니다.

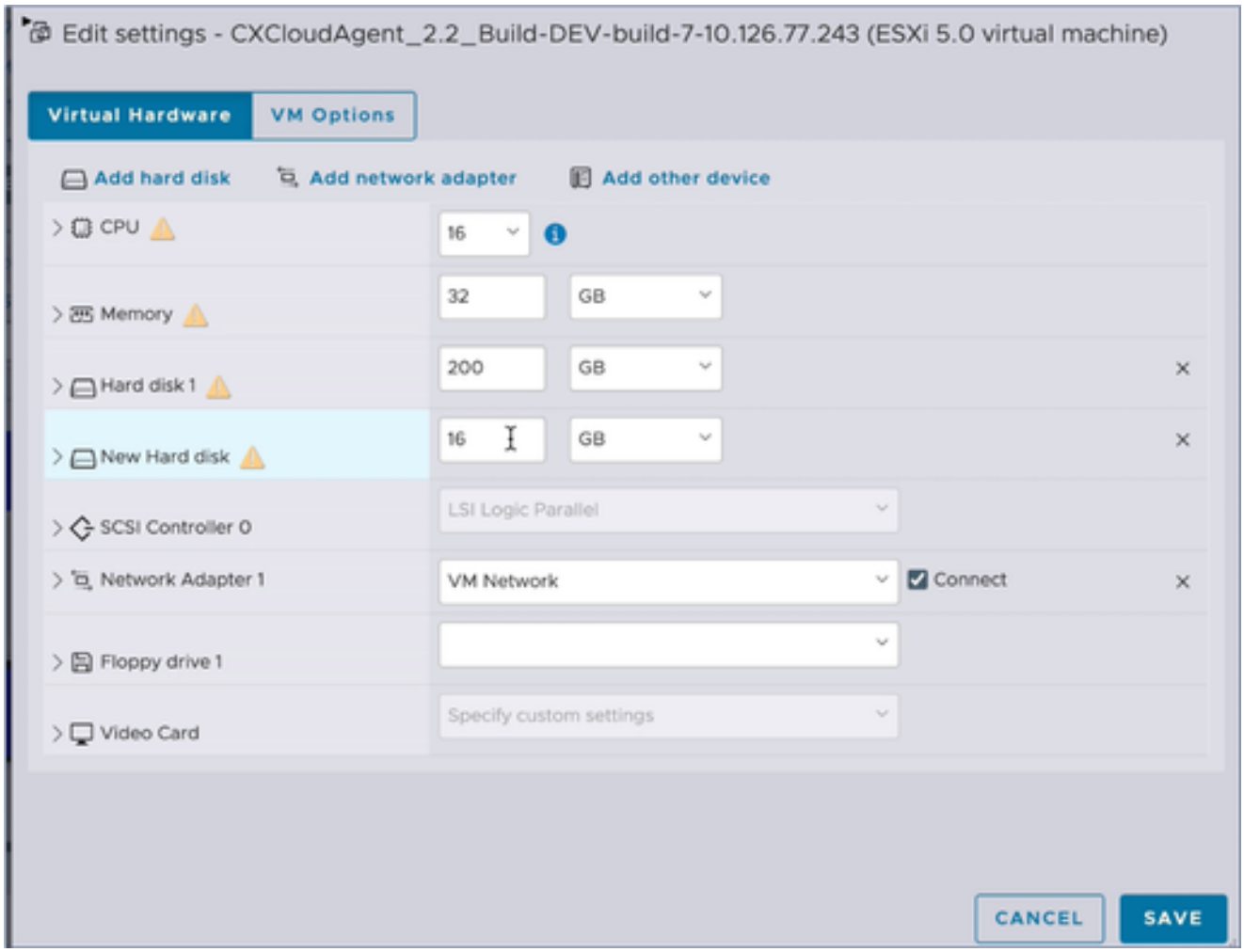


작업



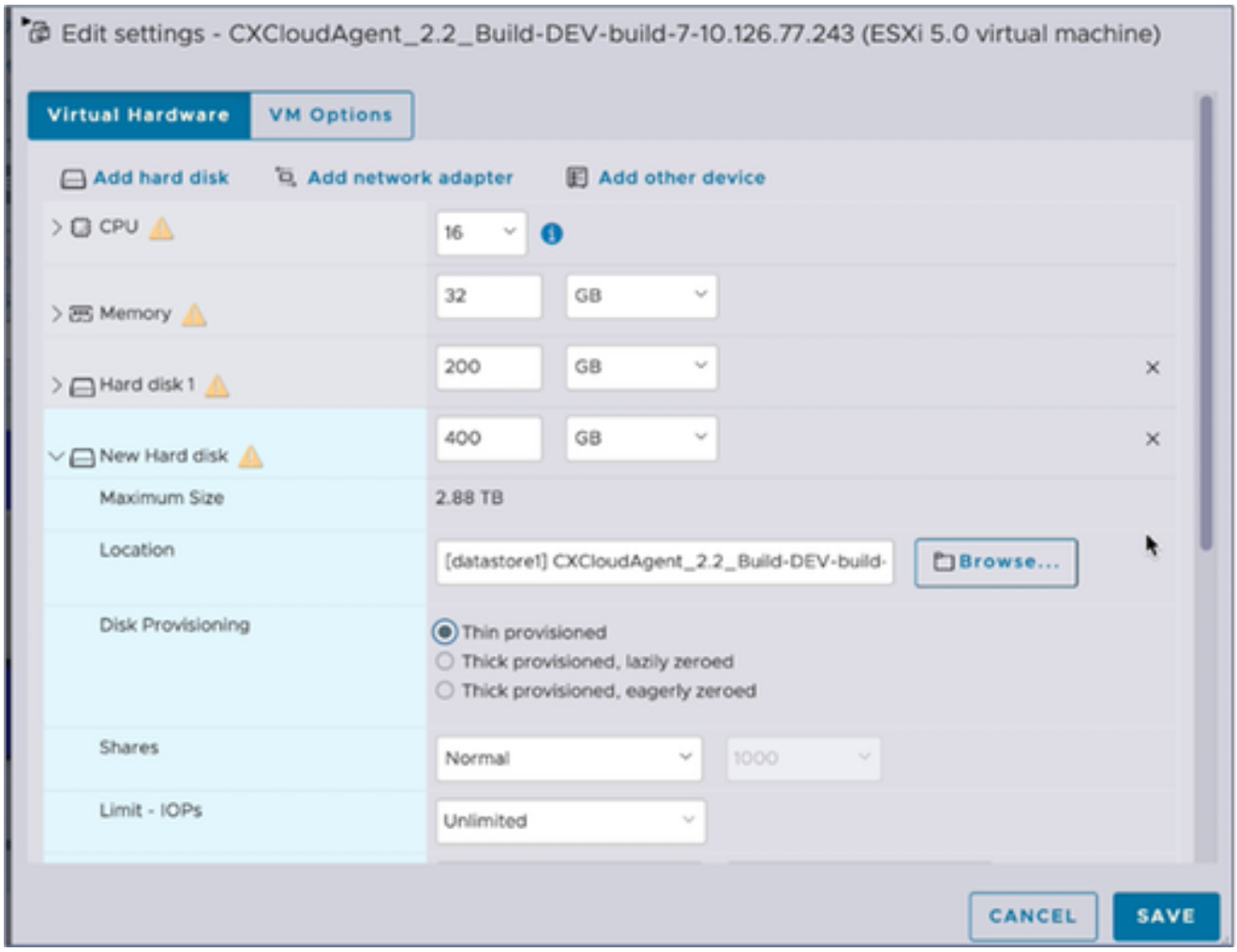
설정 편집

5. 지정된 대로 CPU 값을 업데이트합니다.
   보통: 16코어(8소켓 *2코어/소켓)
   대형: 32코어(16소켓 *2코어/소켓)
6. 지정된 대로 메모리 값을 업데이트합니다.
   중간: 32GB
   크게: 64GB
7. Add hard disk(하드 디스크 추가) > New standard hard disk(새 표준 하드 디스크)를 클릭합니다. 새 하드 디스크 항목이 설정 편집 창에 표시됩니다.



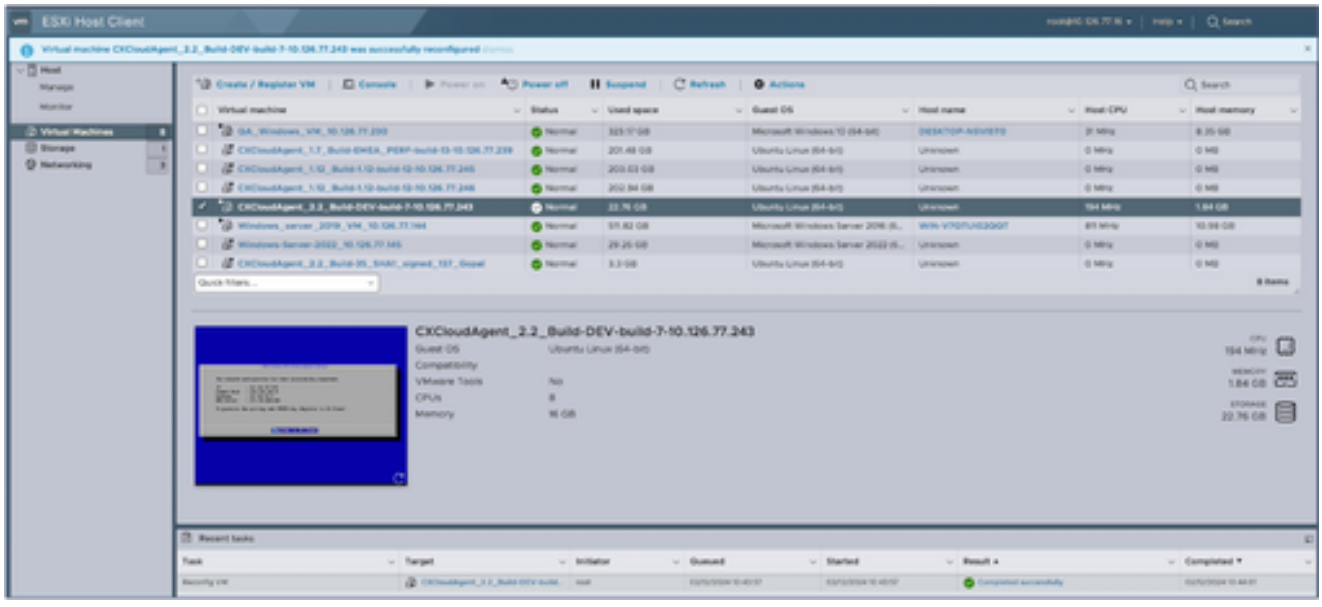
설정 편집

8. 지정된 대로 새 하드 디스크 값을 업데이트합니다.
   중소 규모: 400GB(초기 크기 200GB, 총 공간 600GB 증가)
   소형 ~ 대형: 1000GB(초기 크기 200GB, 총 공간 1200GB로 증가)
9. 화살표를 클릭하여 새 하드 디스크를 확장합니다. 속성이 표시됩니다.



설정 편집

10. Thin provisioned(씬 프로비저닝) 라디오 버튼을 선택합니다.
11. Save(저장)를 클릭하여 컨피그레이션을 완료합니다. 구성 업데이트가 최근 작업에 표시됩니다.



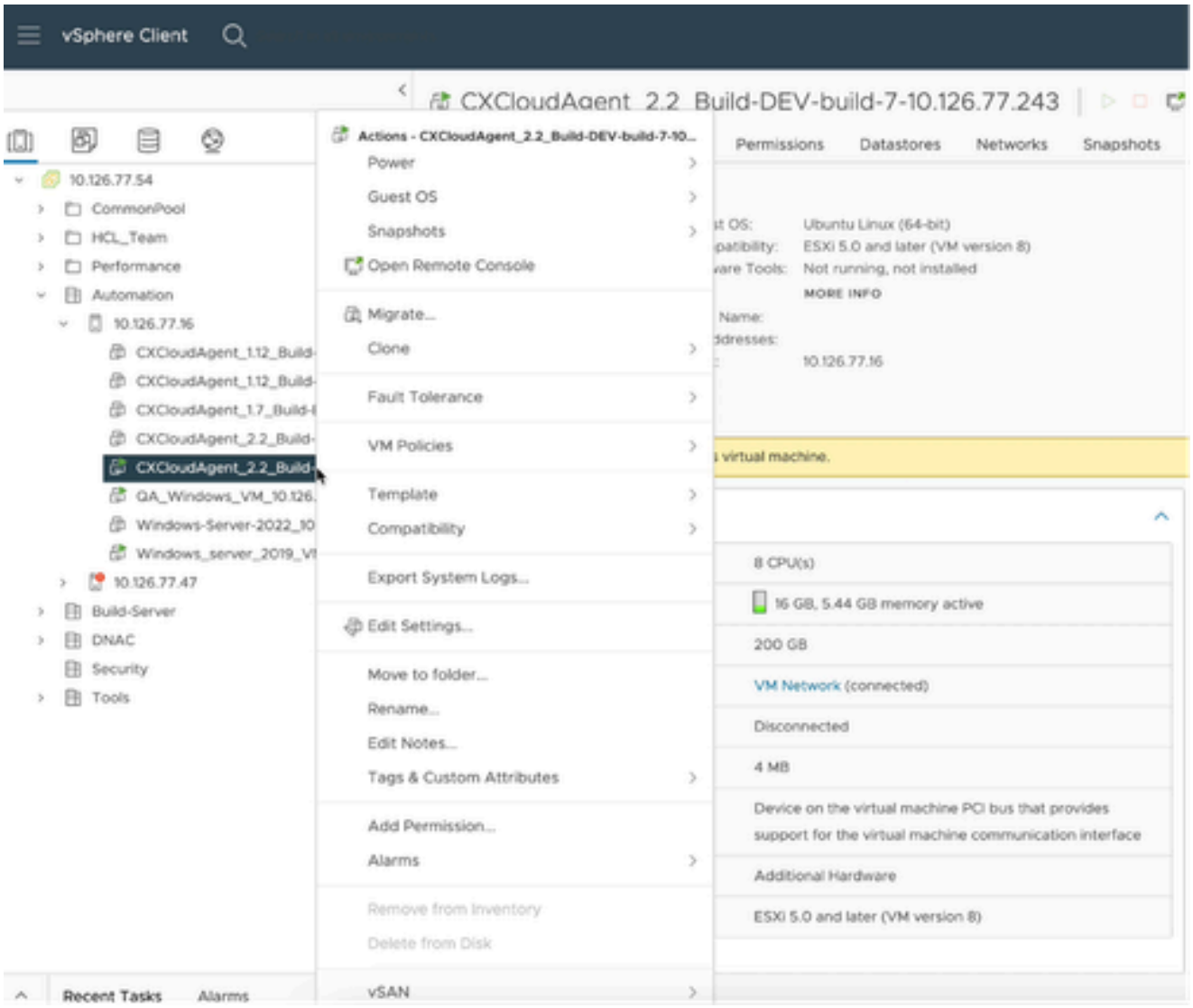
최근 작업

Web Client vCenter를 사용하여 재구성

웹 클라이언트 vCenter를 사용하여 VM 컨피그레이션을 업데이트하려면

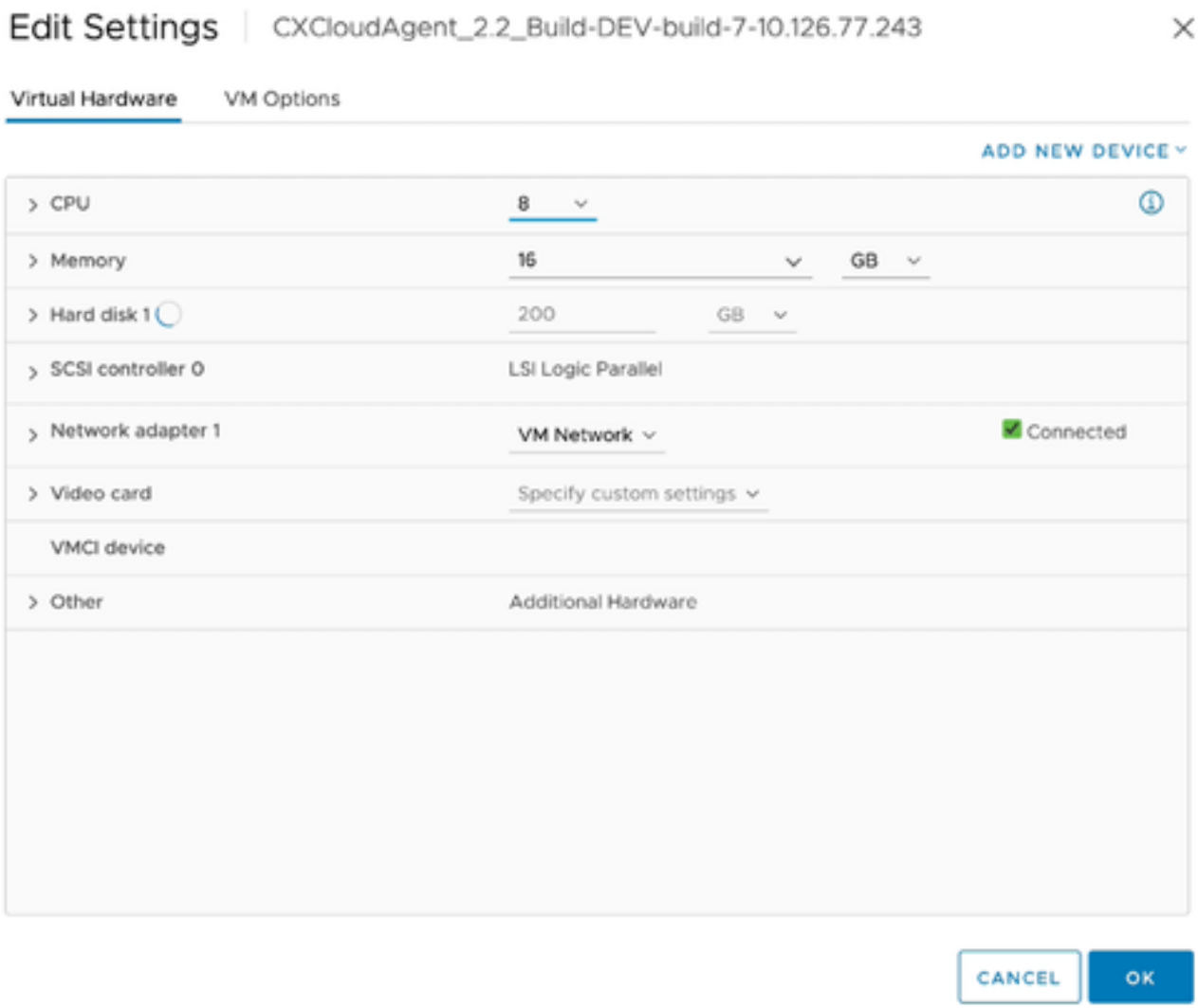
vCenter

1. vCenter에 로그인합니다. 홈 페이지가 표시됩니다.



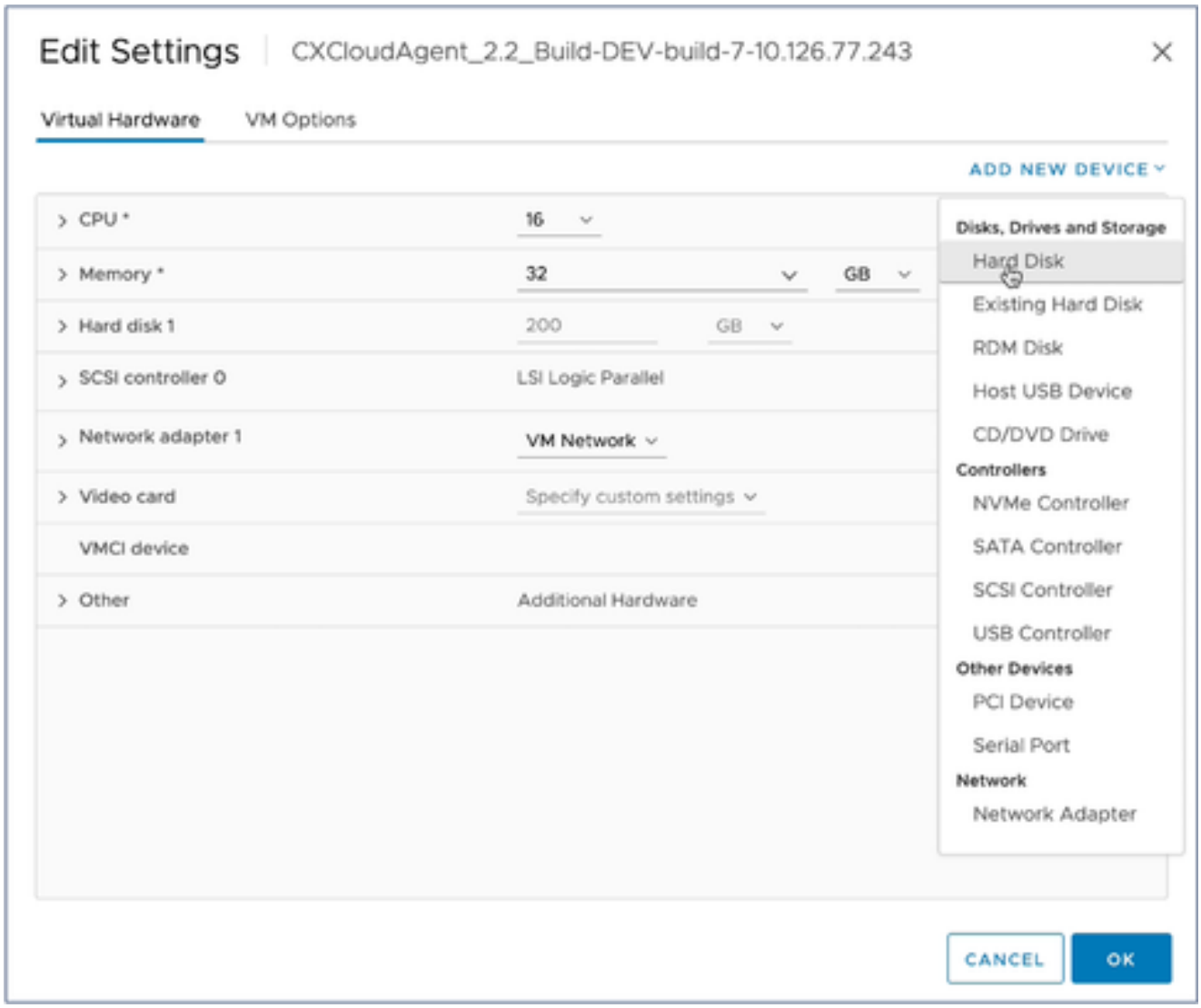
VM 목록

2. 대상 VM을 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 Edit Settings(설정 편집)를 선택합니다. 설정 편집 창이 열립니다.



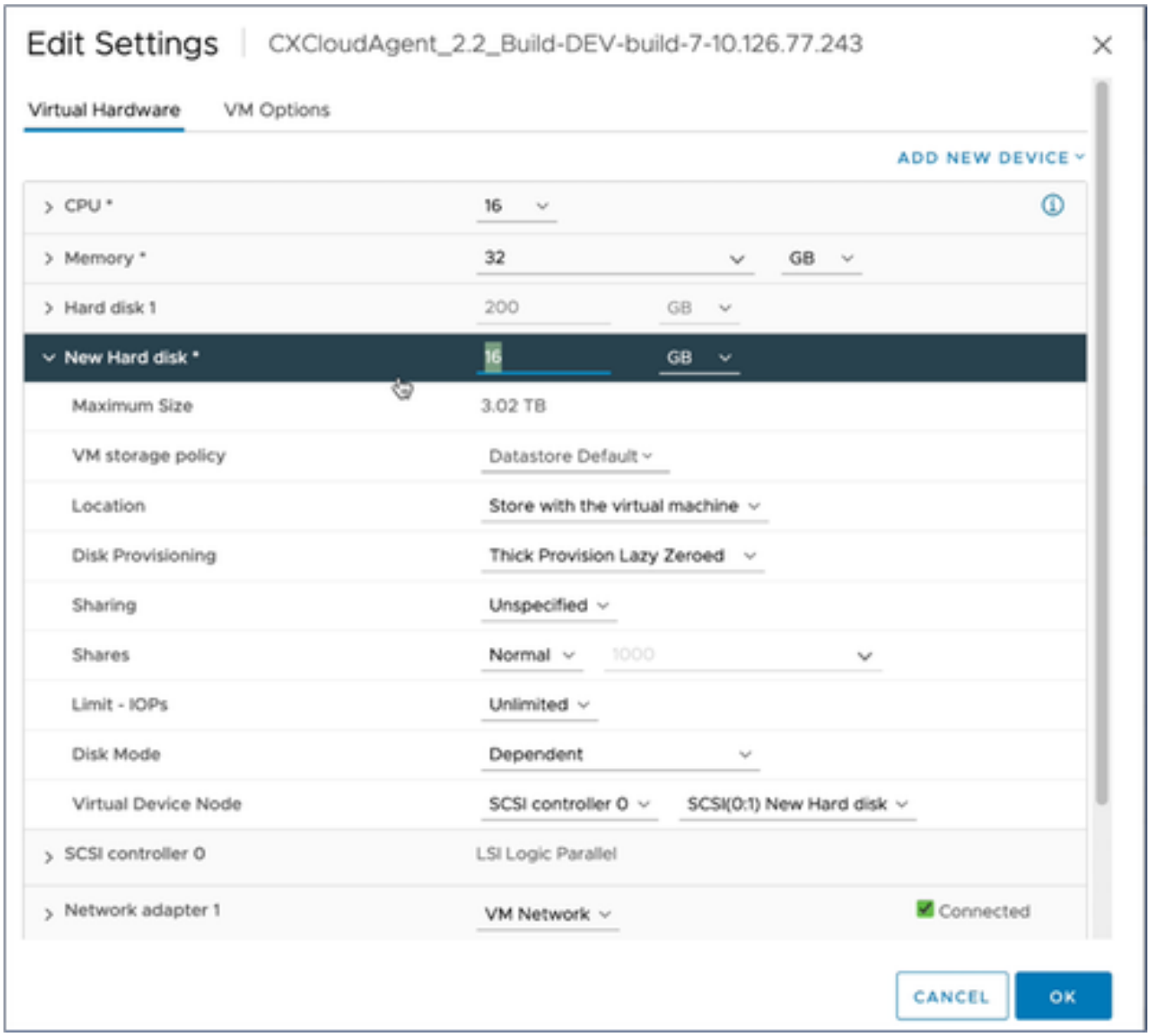
설정 편집

3. 지정된 대로 CPU 값을 업데이트합니다.:
   보통: 16코어(8소켓 *2코어/소켓)
   대형: 32코어(16소켓 *2코어/소켓)
4. 지정된 대로 메모리 값을 업데이트합니다.
   중간: 32GB
   크게: 64GB



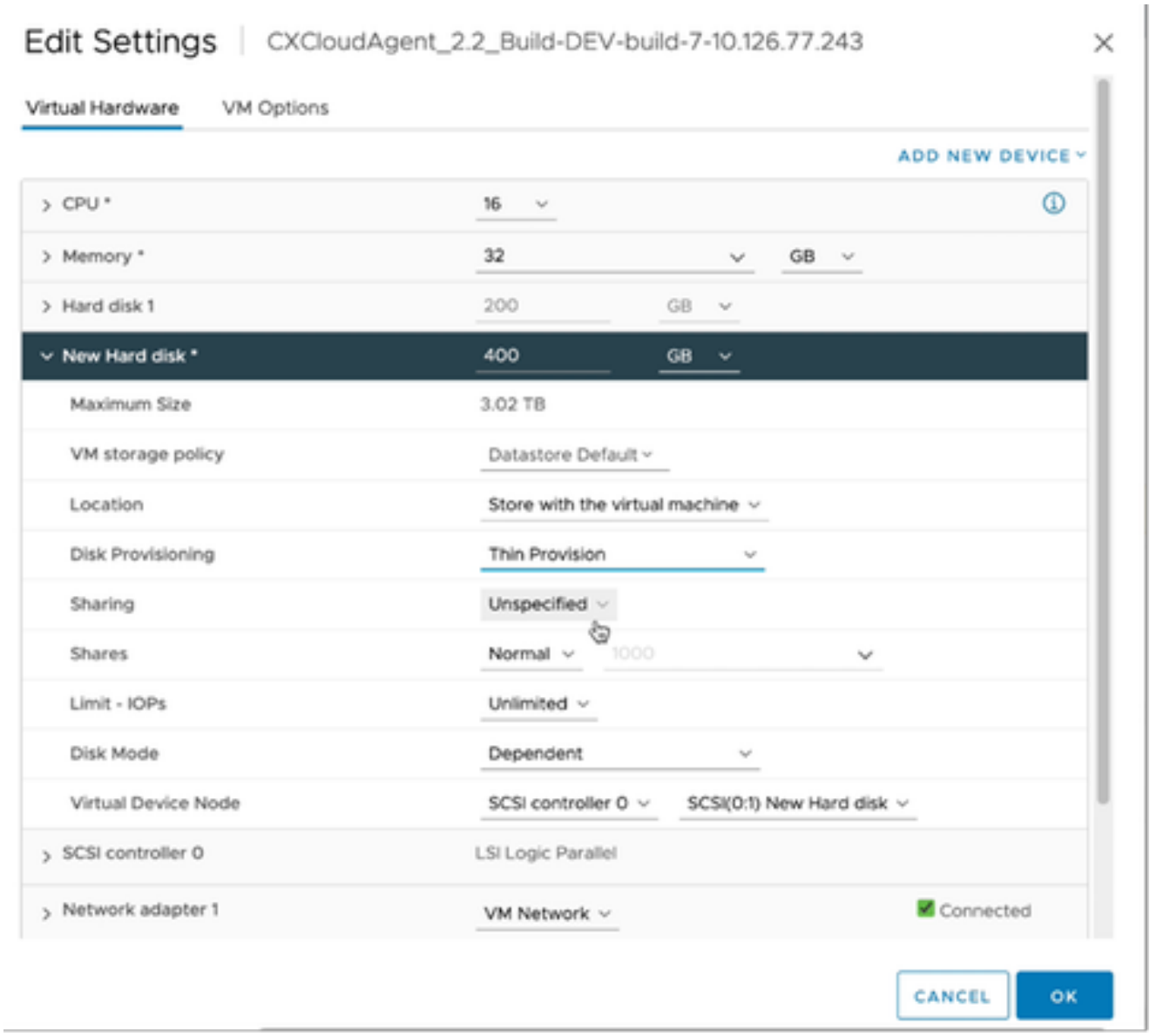
설정 편집

5. Add New Device(새 디바이스 추가)를 클릭하고 Hard Disk(하드 디스크)를 선택합니다. 새 하드 디스크 항목이 추가됩니다.



설정 편집

6. 지정된 대로 새 하드 디스크 메모리를 업데이트합니다.
   중소 규모: 400GB(초기 크기 200GB, 총 공간 600GB 증가)
   소형 ~ 대형: 1000GB(초기 크기 200GB, 총 공간 1200GB로 증가)



설정 편집

7. Disk Provisioning 드롭다운 목록에서 Thin Provisioning을 선택합니다.
8. OK(확인)를 클릭하여 업그레이드를 완료합니다.

구축 및 네트워크 설정

CX 에이전트를 구축하려면 다음 옵션 중 하나를 선택합니다.

- VMware vSphere/vCenter Thick Client ESXi 5.5/6.0
- VMware vSphere/vCenter Web Client ESXi 6.0 또는 Web Client vCenter 설치
- Oracle Virtual Box 7.0.12
- Microsoft Hyper-V 설치

OVA 구축

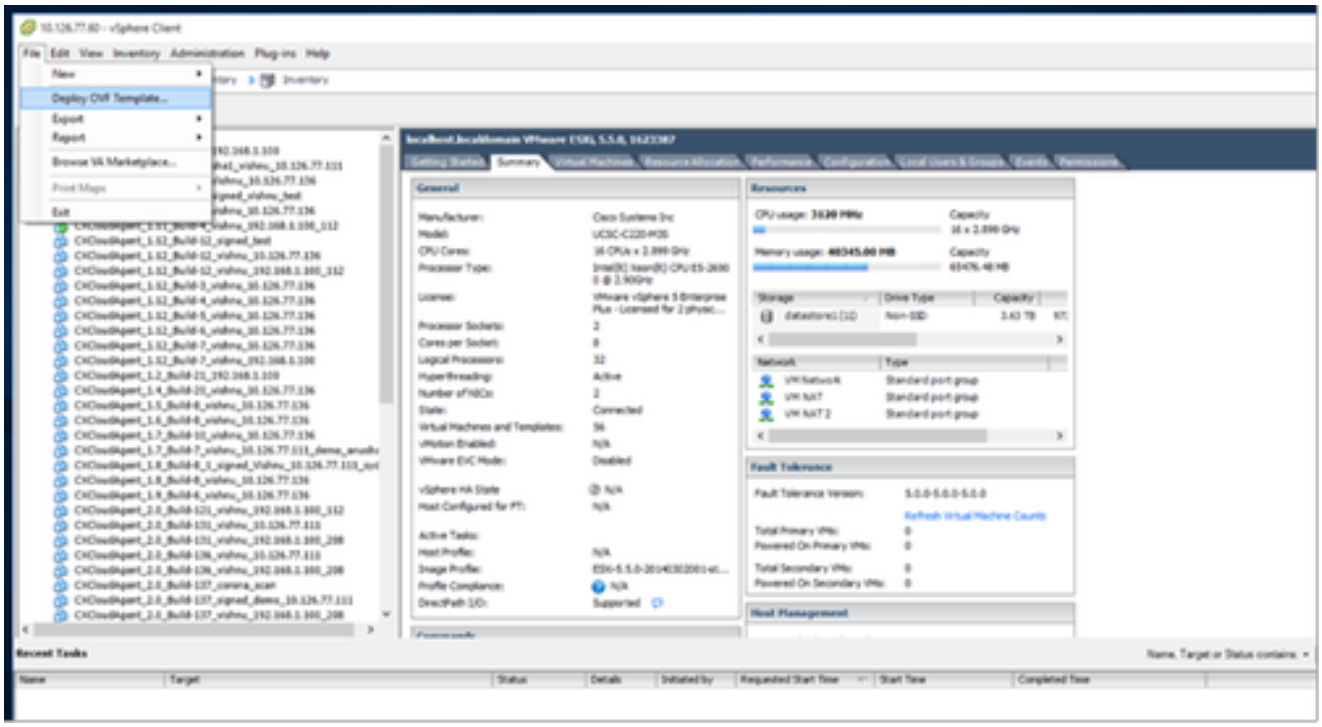
Thick Client ESXi 5.5/6.0 설치

이 클라이언트에서는 vSphere 씩 클라이언트를 사용하여 CX 에이전트 OVA를 구축할 수 있습니다.

1. 이미지를 다운로드한 후 VMware vSphere Client를 시작하고 로그인합니다.

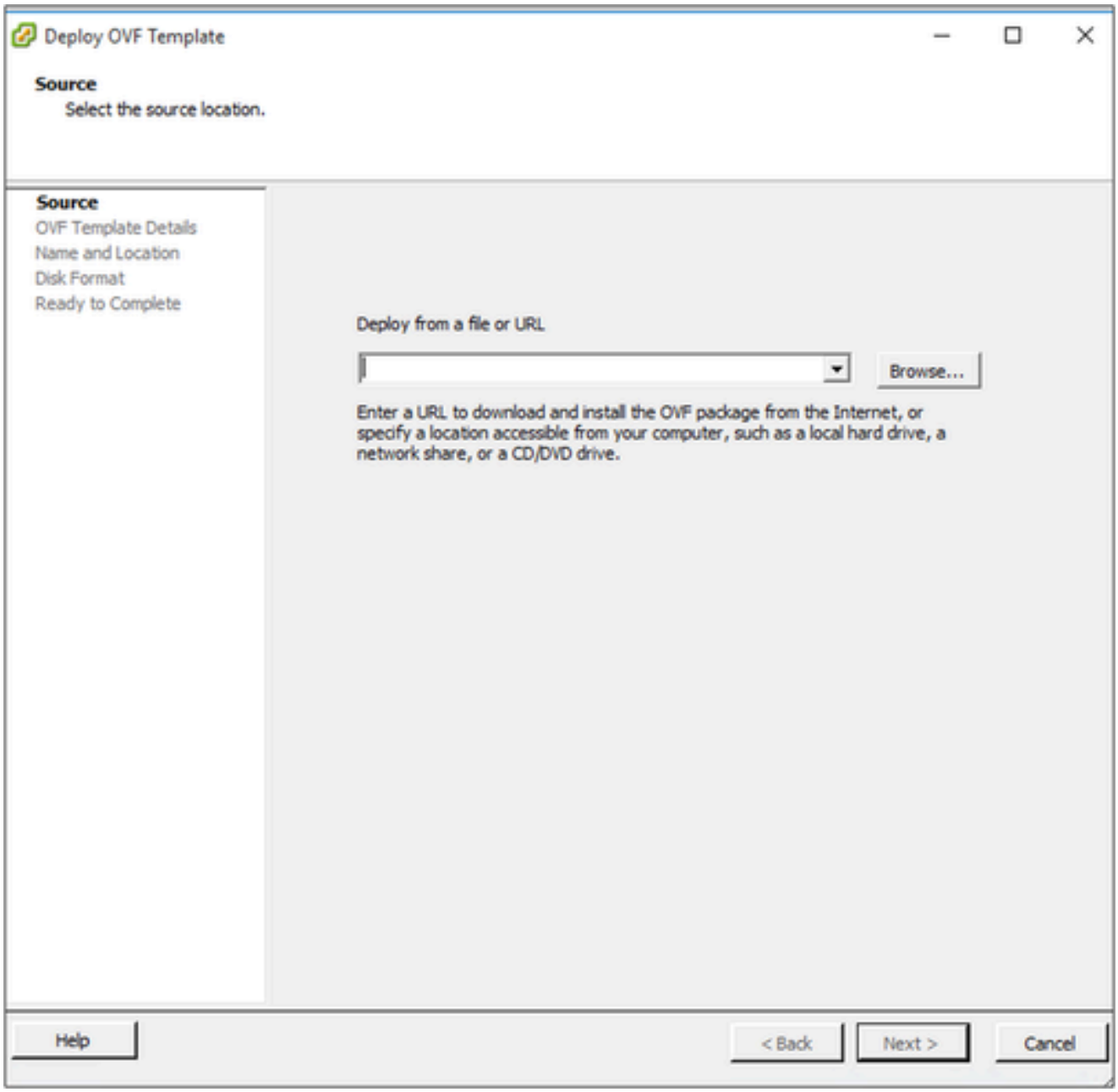
로그인

2. 메뉴에서 File(파일) > Deploy OVF Template(OVF 템플릿 구축)을 선택합니다.



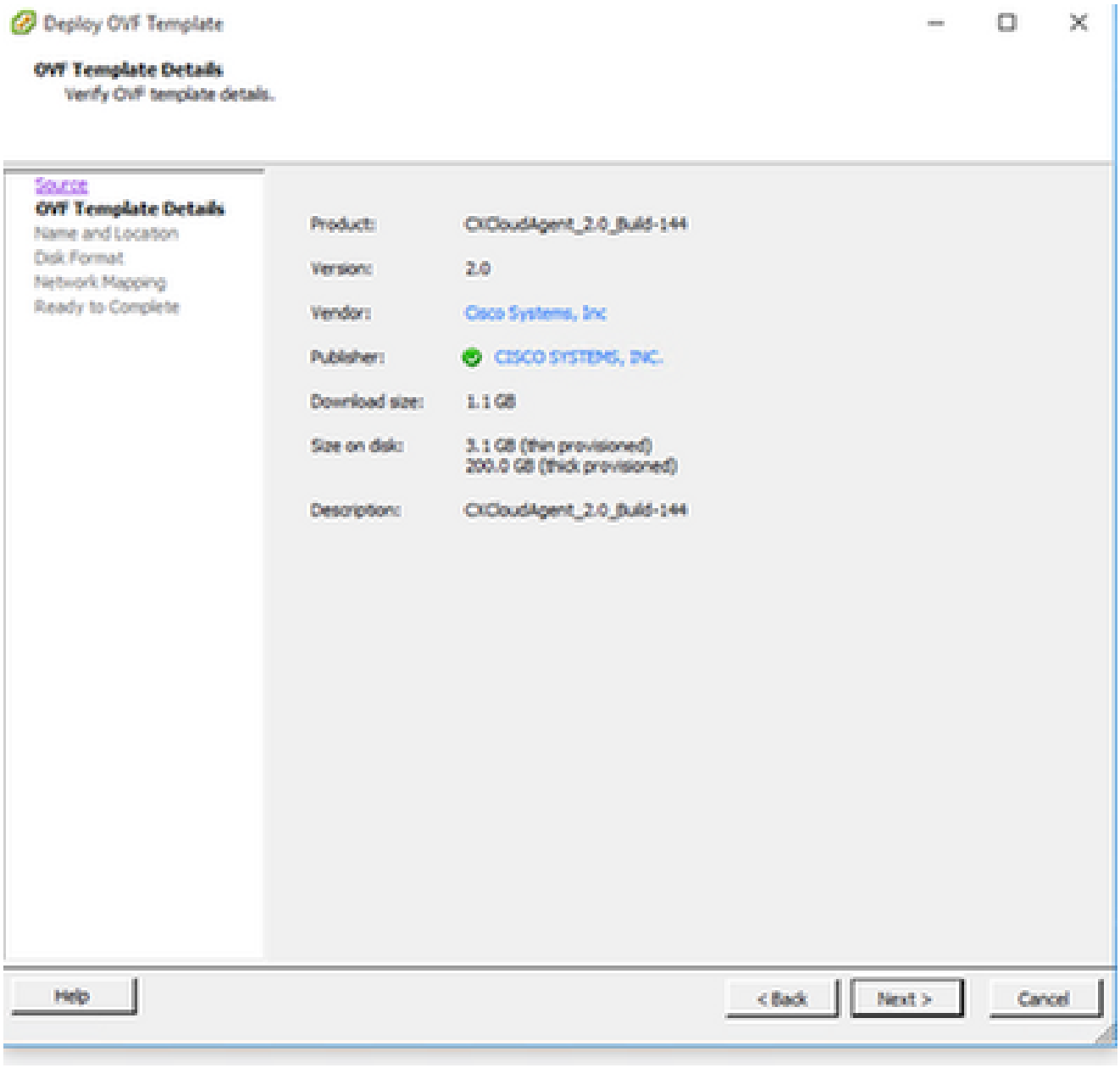
vSphere Client

3. OVA 파일을 찾아 선택하고 Next(다음)를 클릭합니다.



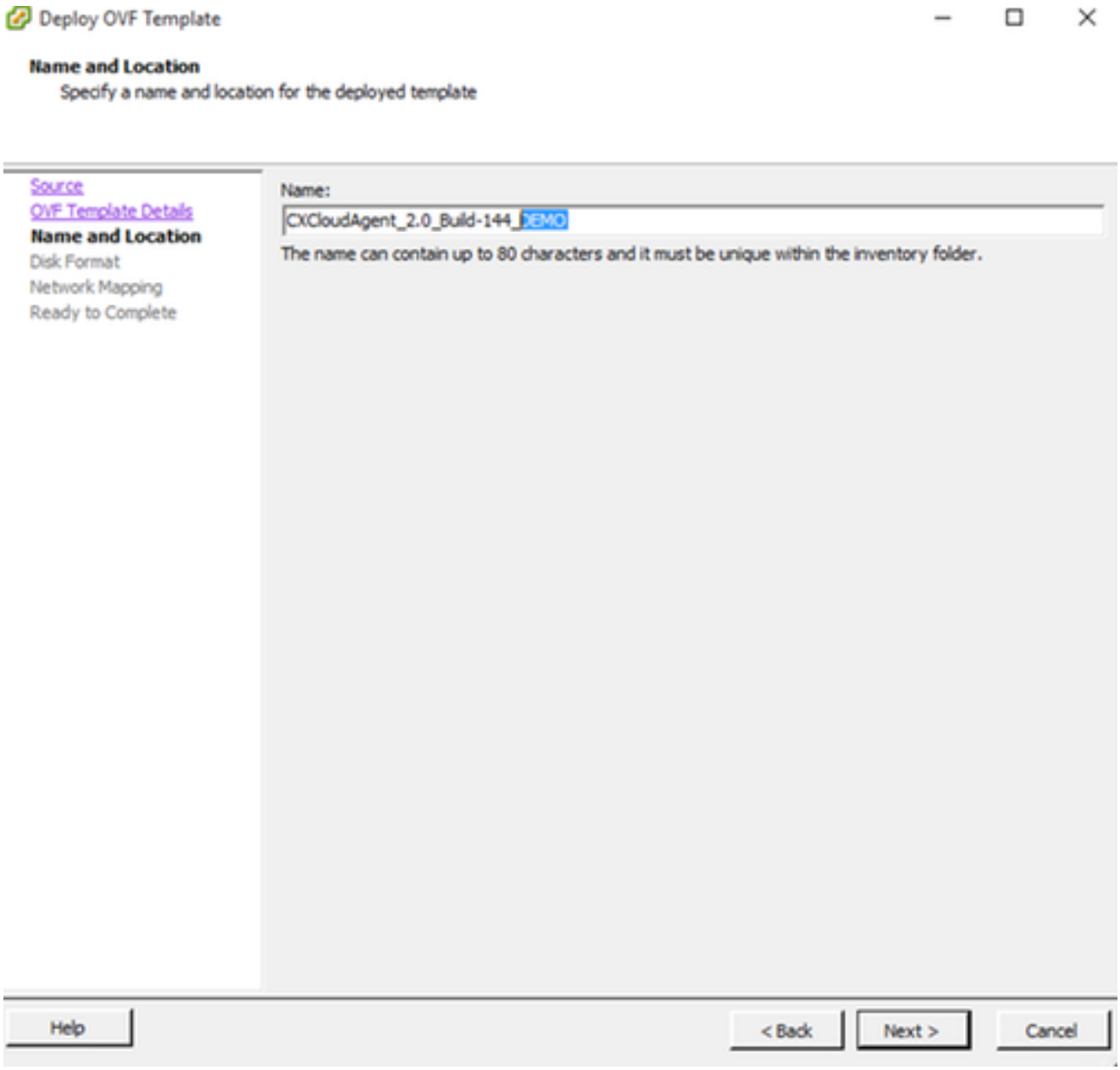
OVA 경로

4. OVF Details(OVF 세부사항)를 확인하고 Next(다음)를 클릭합니다.



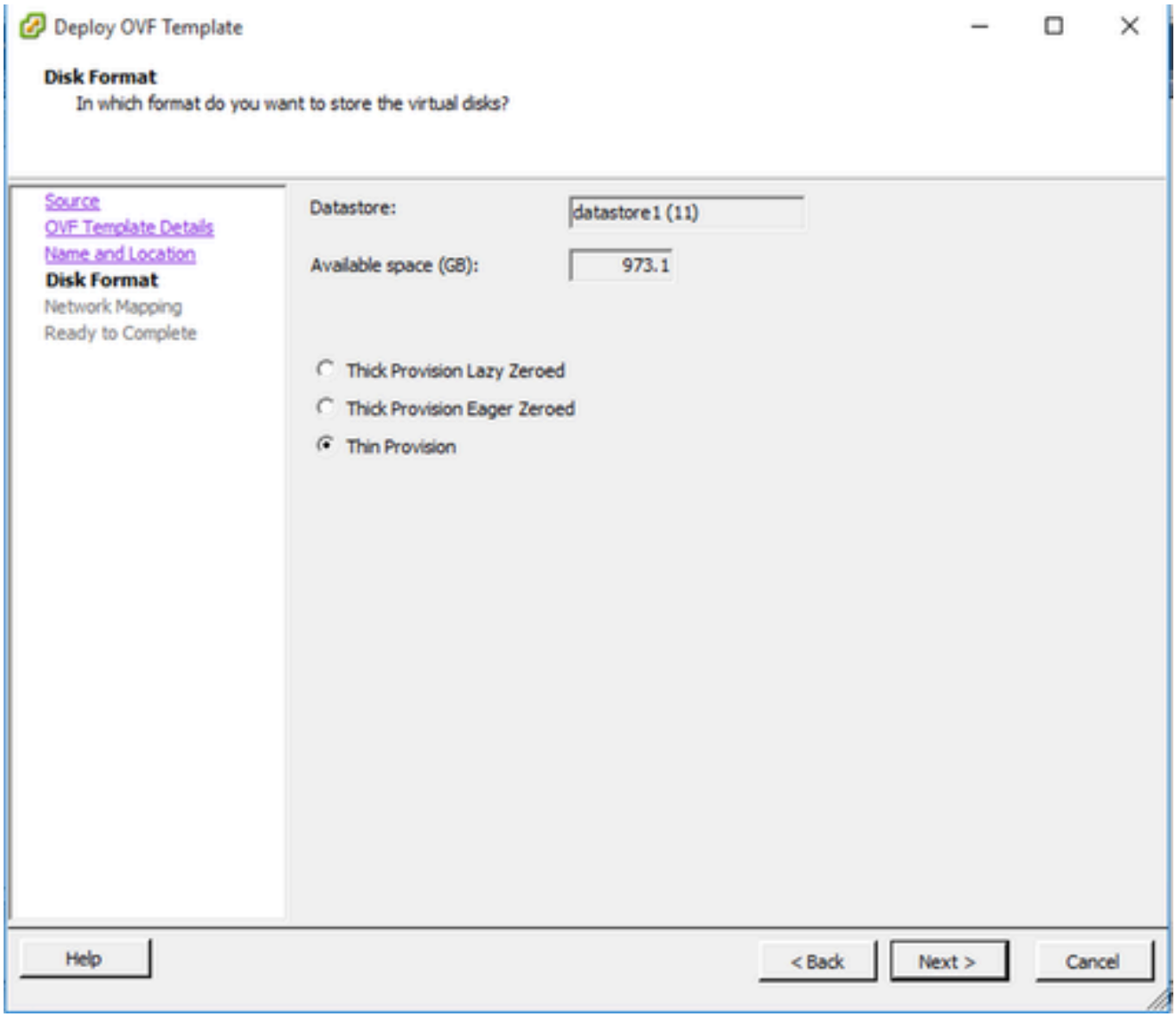
템플릿 세부 정보

5. Unique Name(고유 이름)을 입력하고 Next(다음)를 클릭합니다.



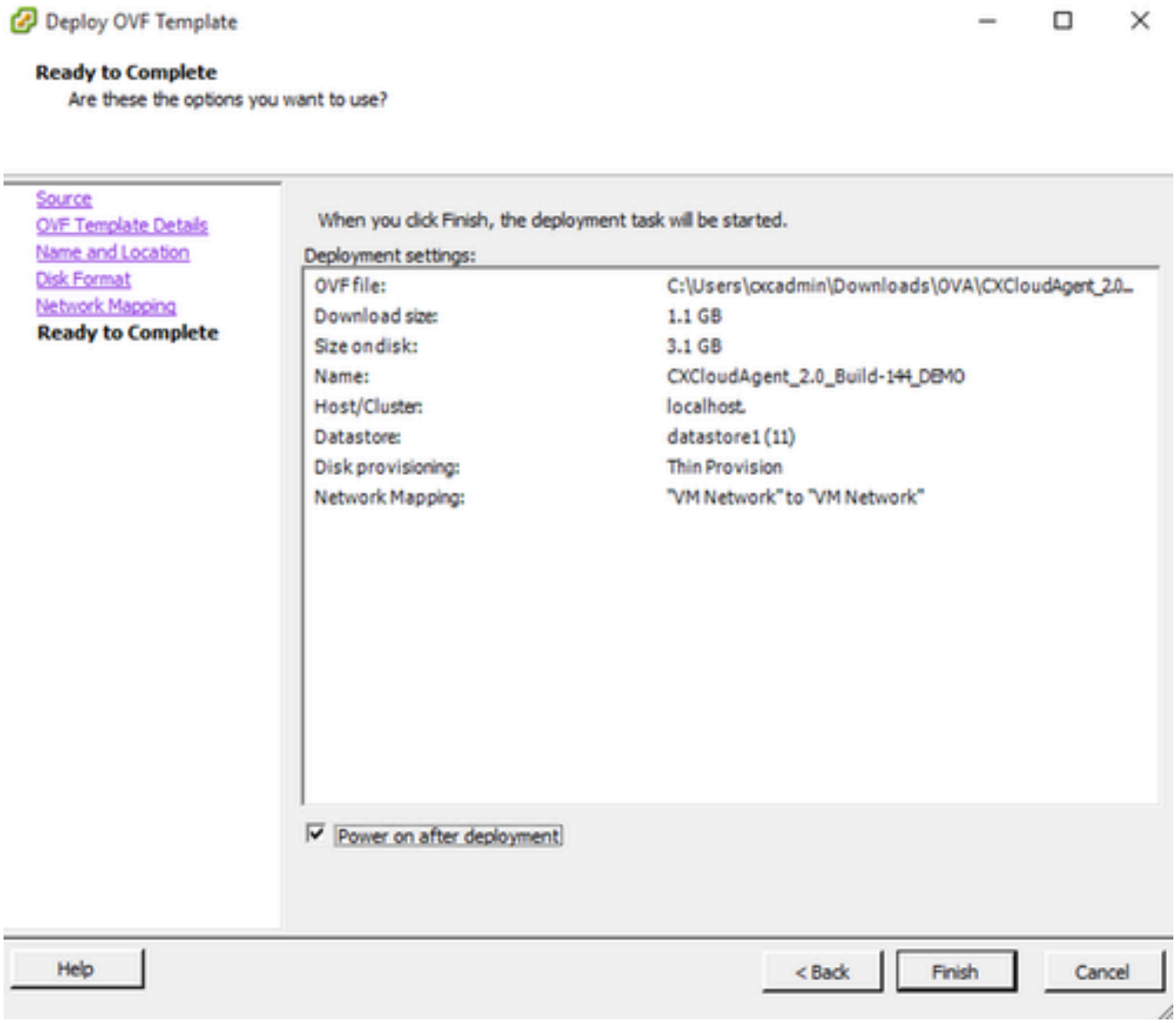
이름 및 위치

6. 디스크 형식을 선택하고 다음 을 클릭합니다(씬 프로비저닝 권장).



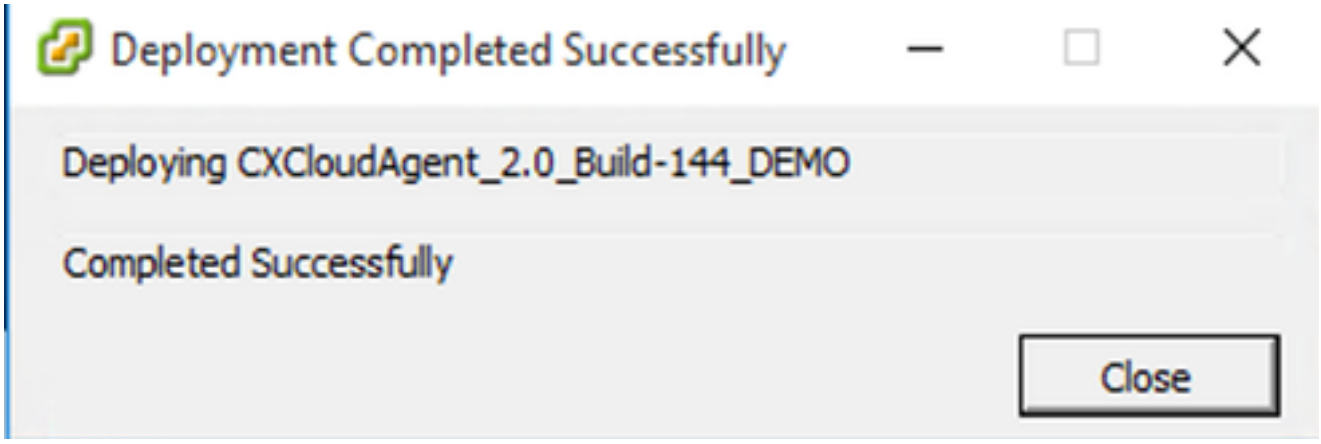
디스크 형식

7. Power on after deployment(구축 후 전원 켜기) 확인란을 선택하고 Close(닫기)를 클릭합니다.



완료 준비

구축에는 몇 분 정도 걸릴 수 있습니다. 구축이 성공하면 확인이 표시됩니다.



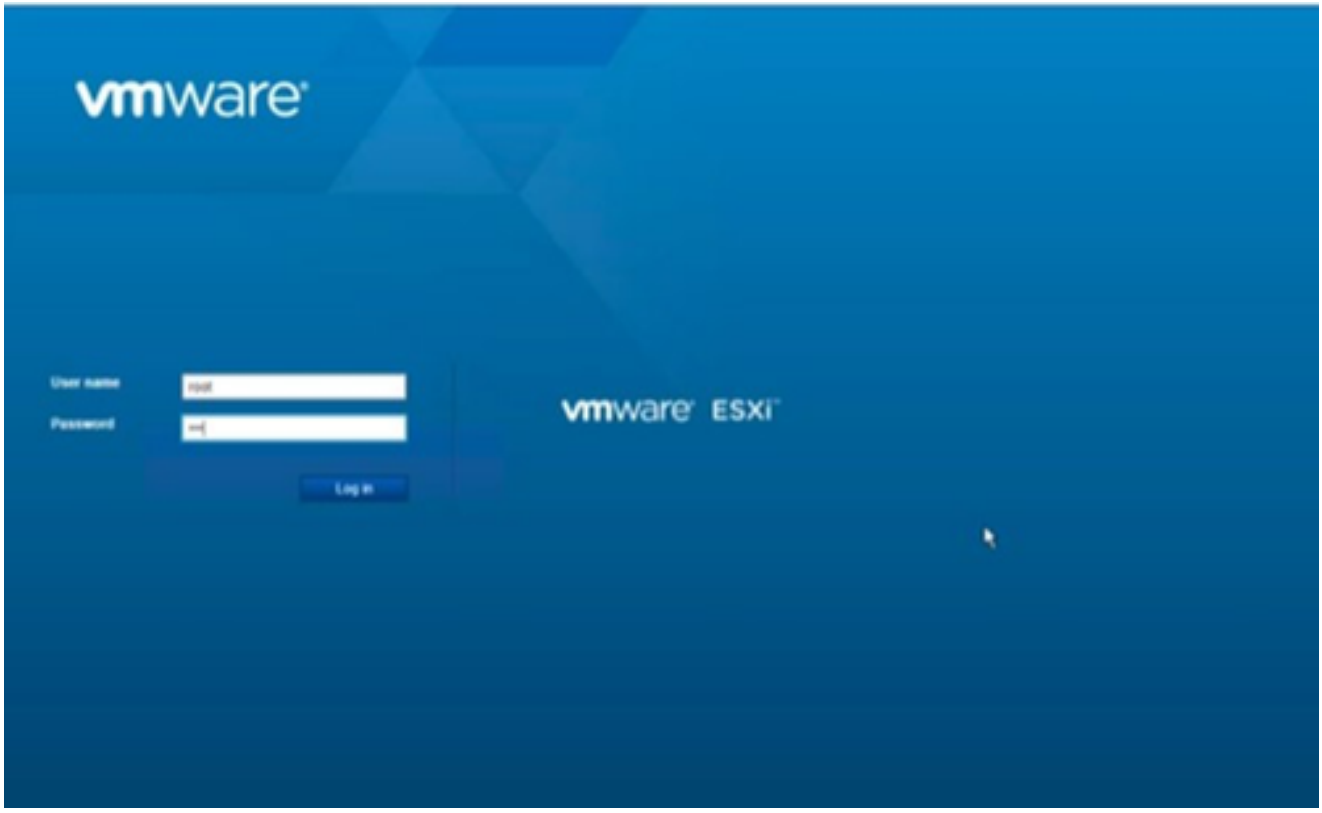
구축 완료

8. 구축된 VM을 선택하고 콘솔을 연 다음 네트워크 구성으로 이동하여 다음 단계를 진행합니다.

Web Client ESXi 6.0 설치

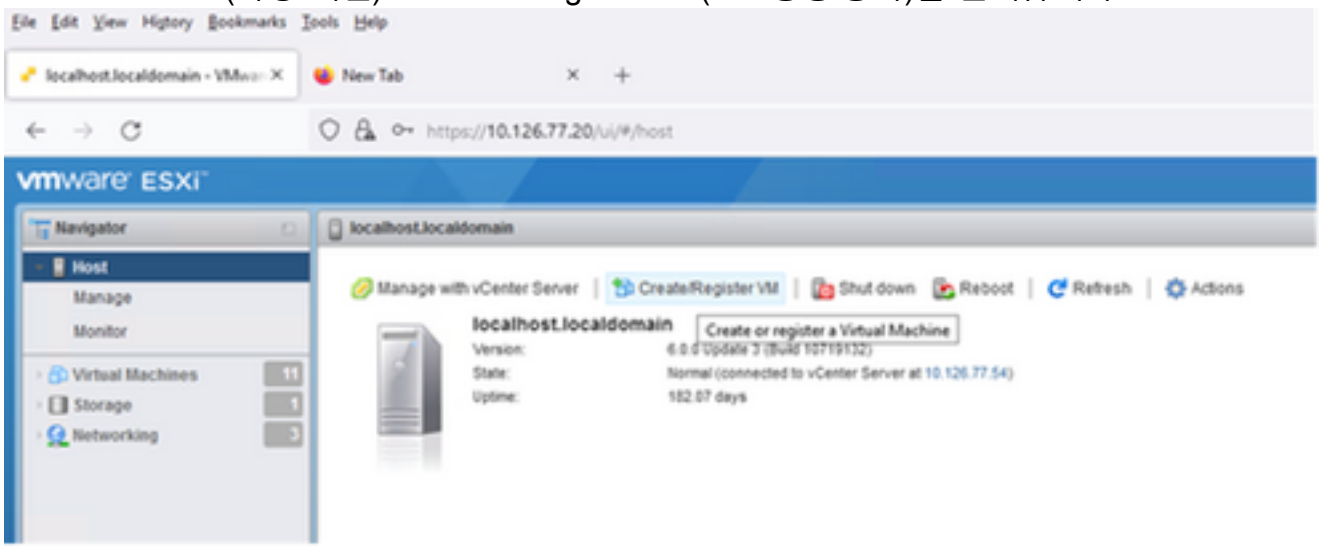
이 클라이언트는 vSphere 웹을 사용하여 CX 클라우드 OVA를 구축합니다.

1. VM 구축에 사용된 ESXi/하이퍼바이저 자격 증명을 사용하여 VMware UI에 로그인합니다.



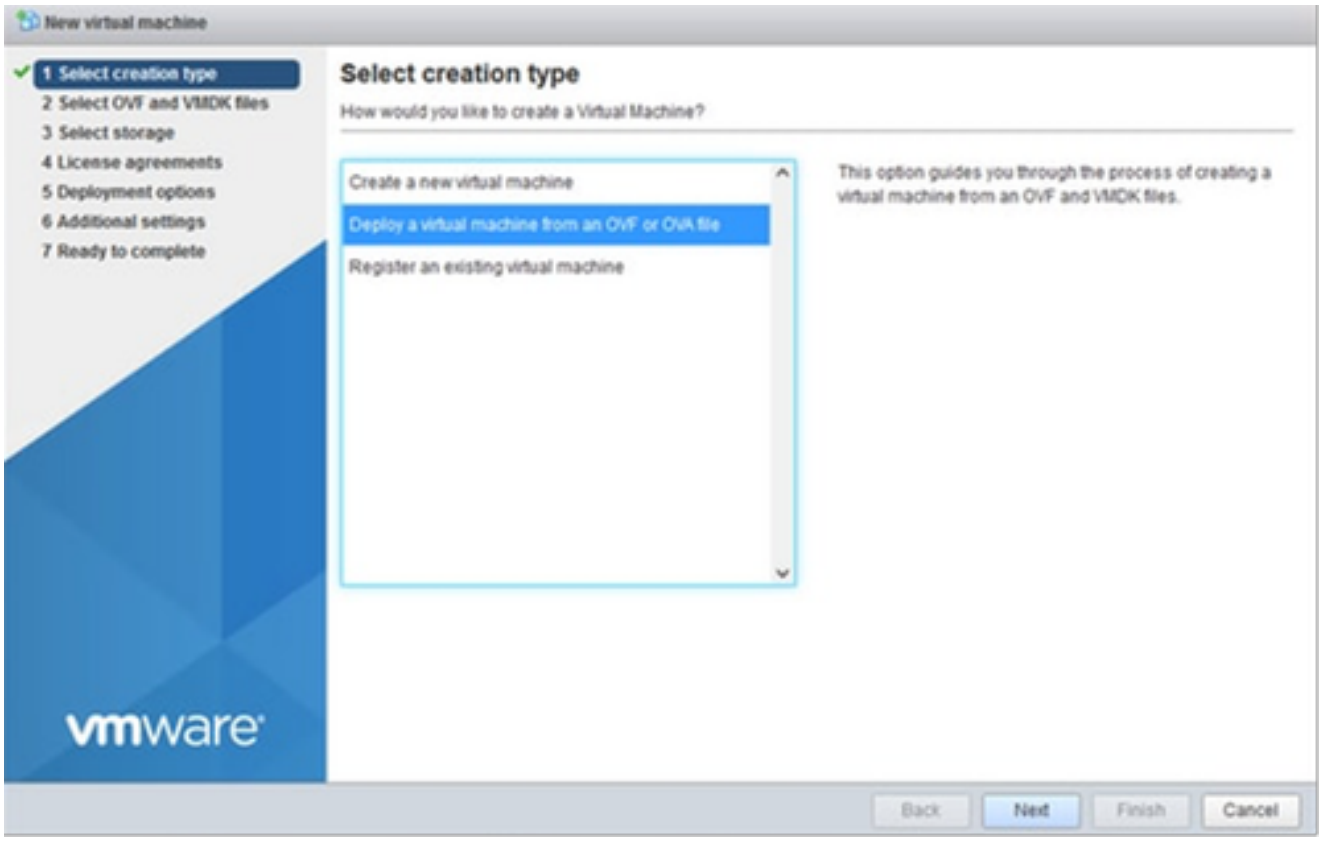
VMware ESXi 로그인

2. Virtual Machine(가상 머신) > Create/Register VM(VM 생성/등록)을 선택합니다.



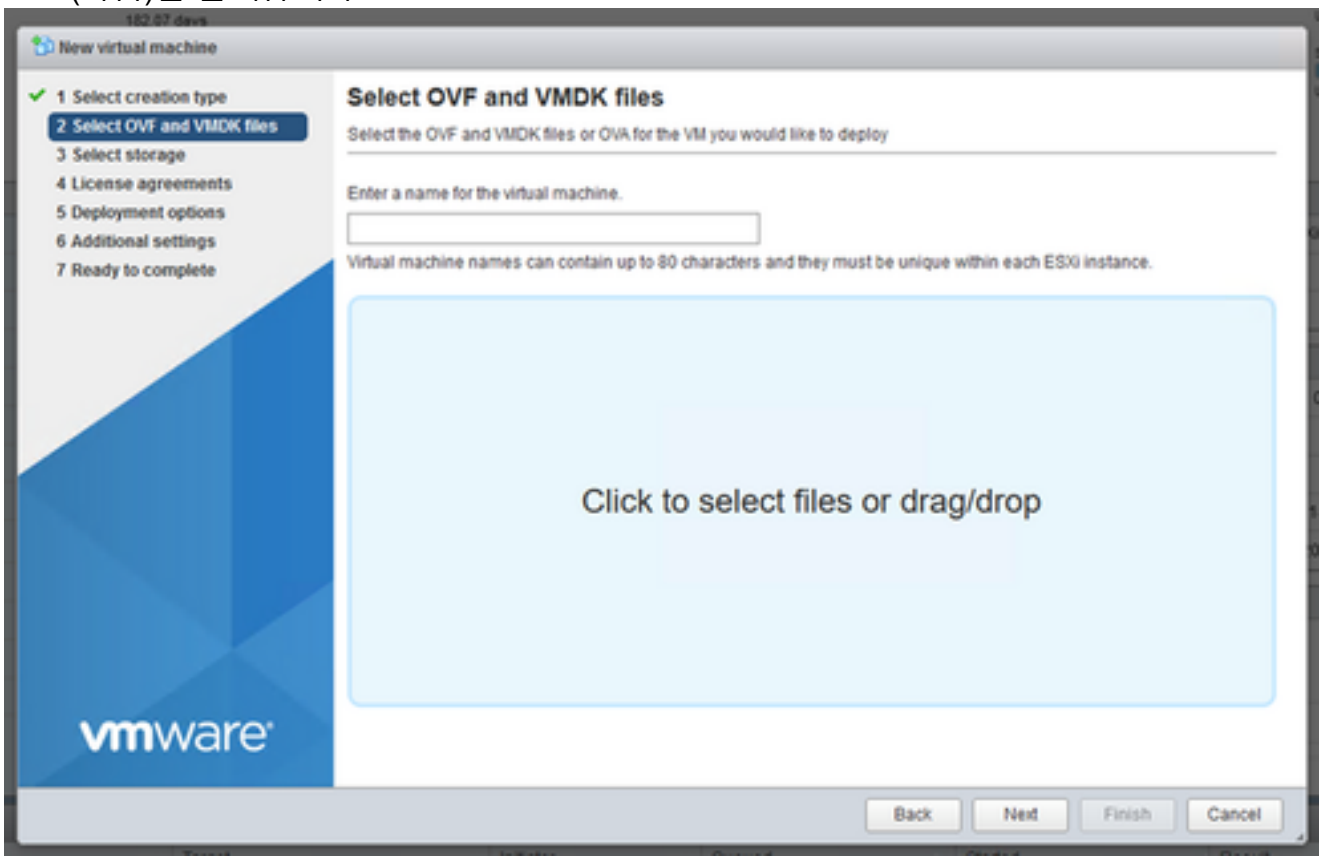
VM 생성

3. Deploy a virtual machine from an OVF or OVA file(OVF 또는 OVA 파일에서 가상 머신 구축)을 선택하고 Next(다음)를 클릭합니다.



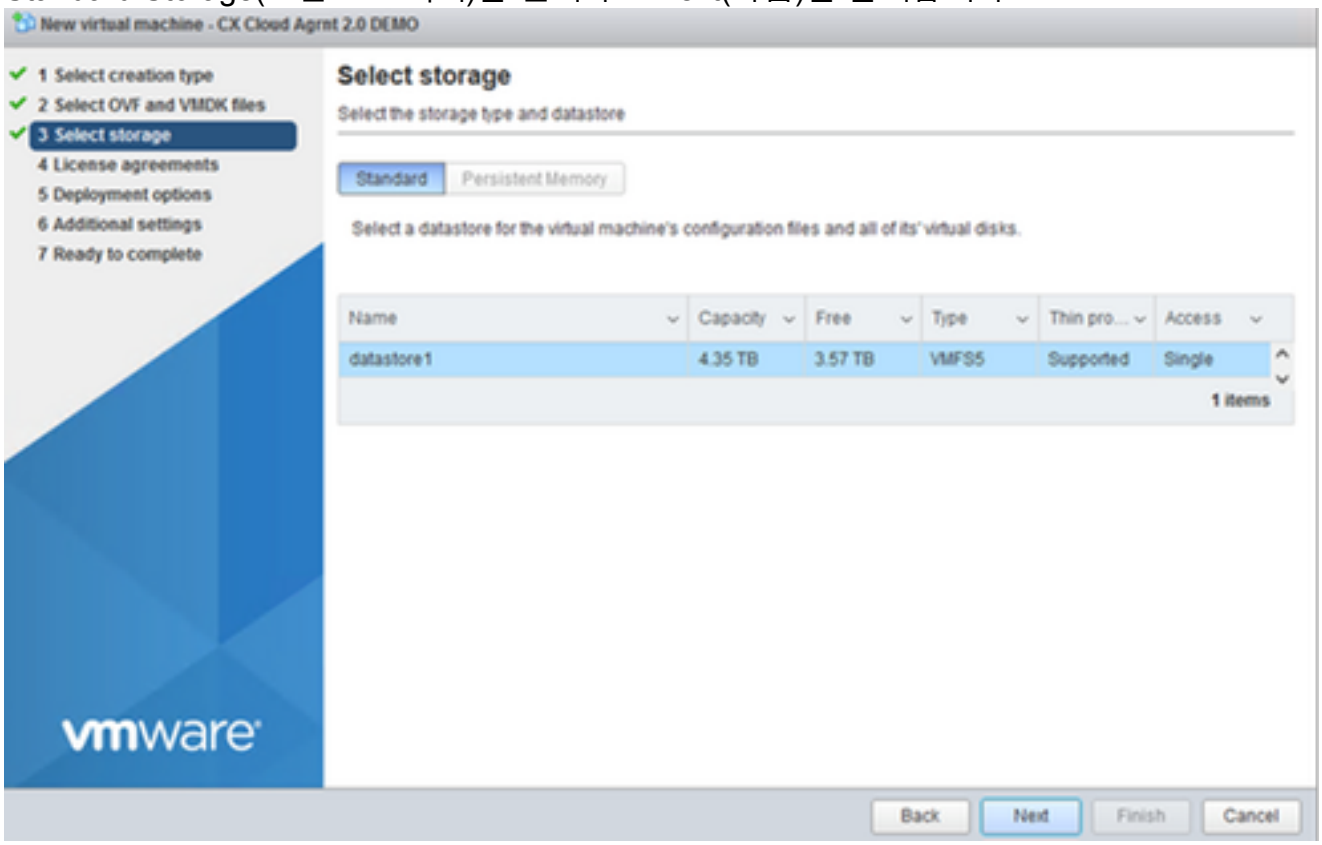
생성 유형 선택

4. VM의 이름을 입력하거나, 파일을 찾아 선택하거나, 다운로드한 OVA 파일을 끌어서 놓습니다 .
5. Next(다음)를 클릭합니다.



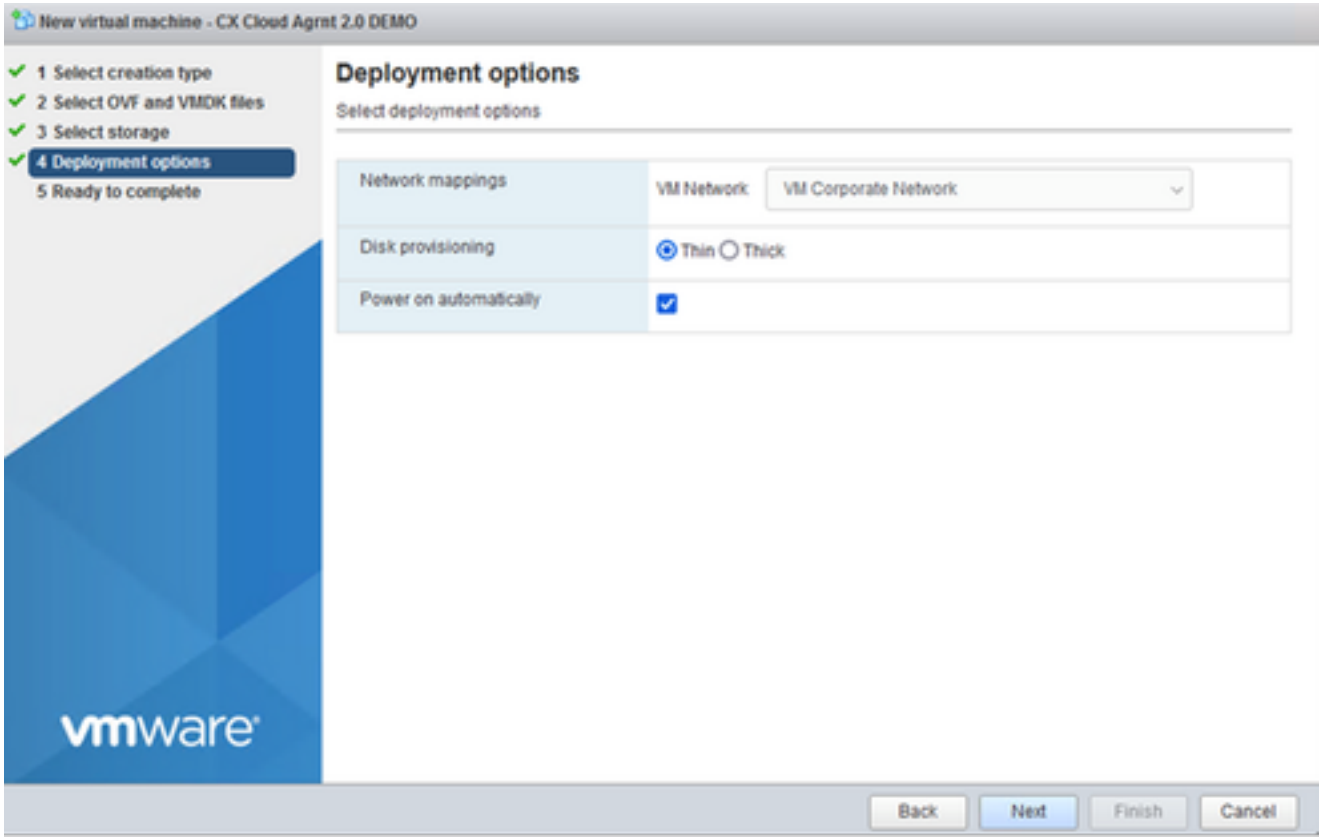
OVA 선택

6. Standard Storage(표준 스토리지)를 선택하고 Next(다음)를 클릭합니다.



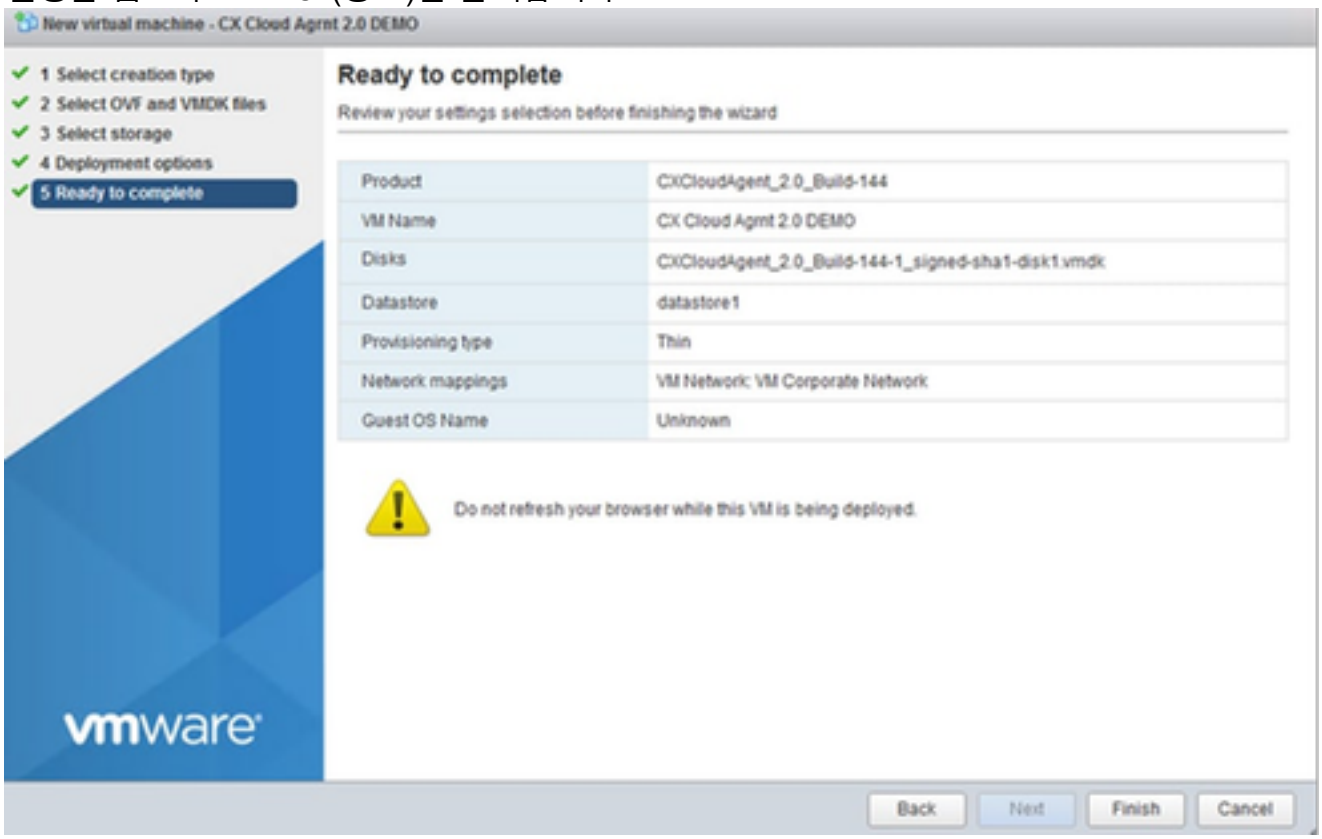
스토리지 선택

7. 적절한 구축 옵션을 선택하고 다음을 클릭합니다.

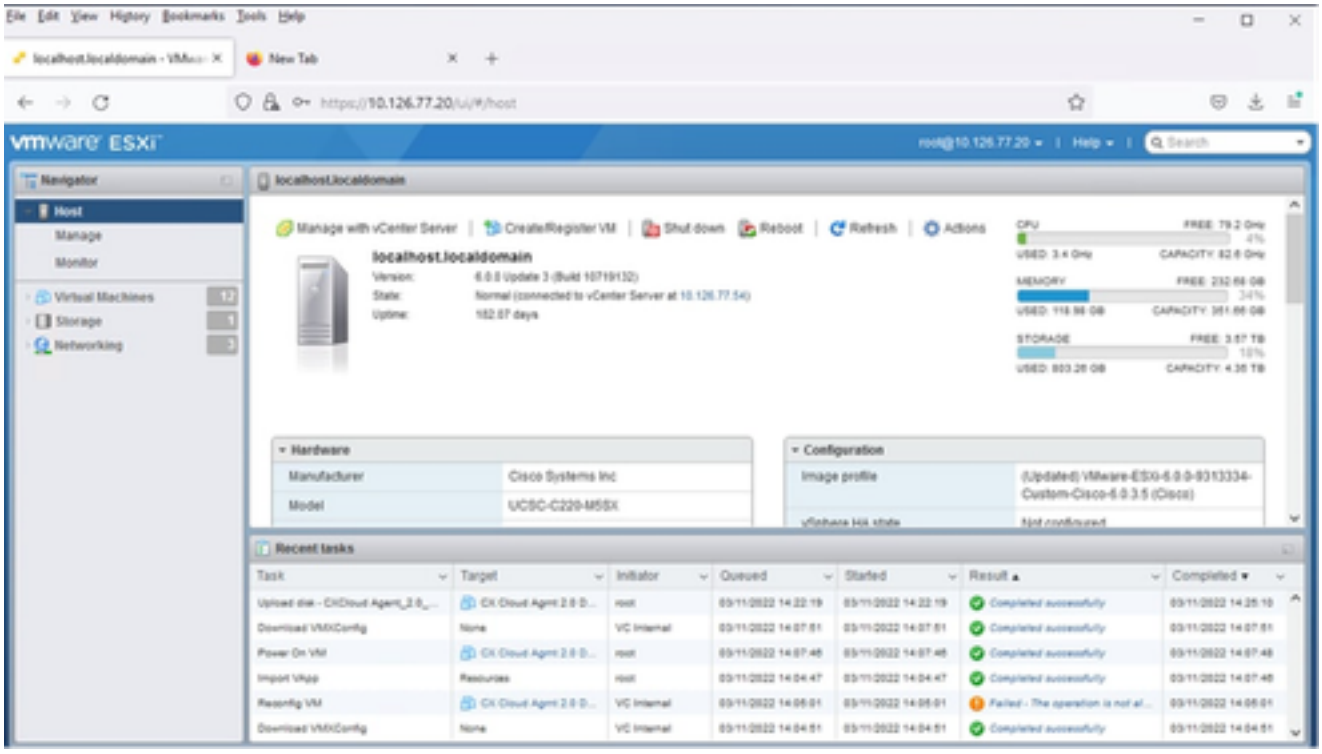


구축 옵션

8. 설정을 검토하고 Finish(종료)를 클릭합니다.

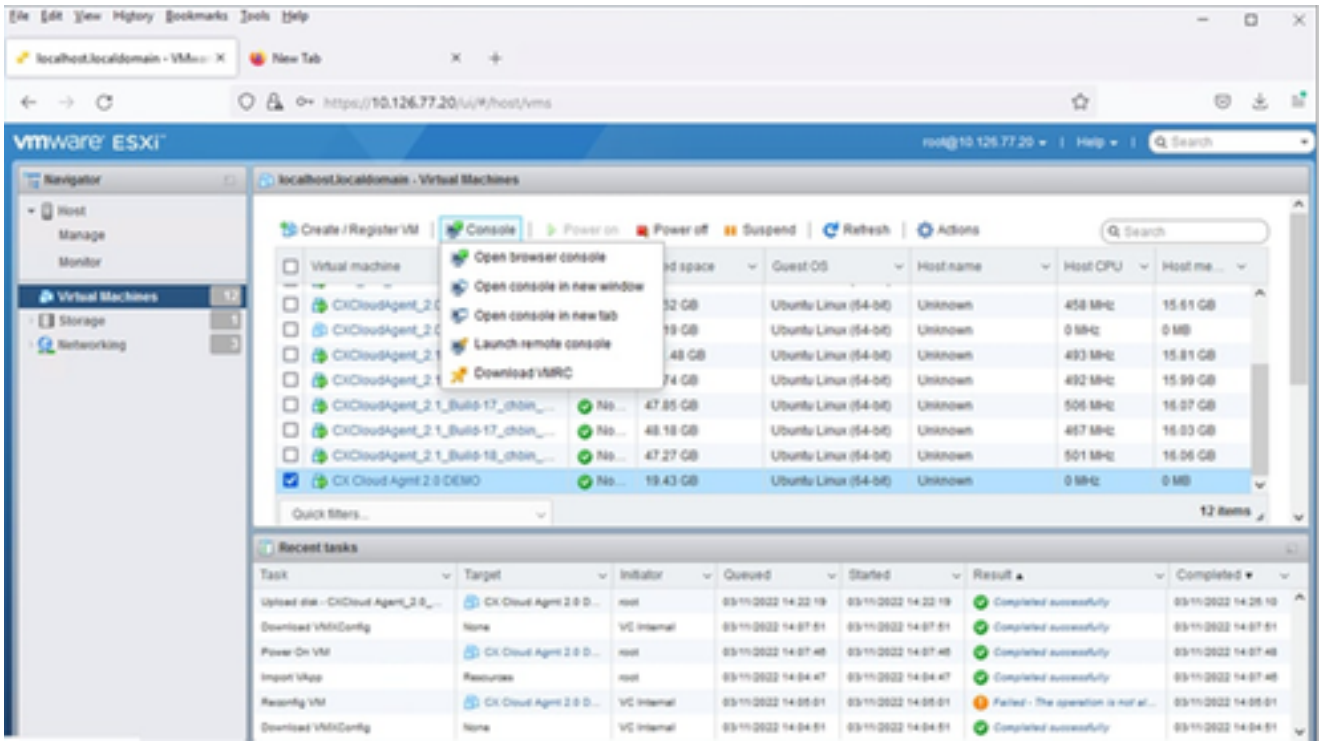


완료 준비



성공적인 완료

9. 방금 구축한 VM을 선택하고 Console(콘솔) > Open browser console(브라우저 콘솔 열기)을 선택합니다.



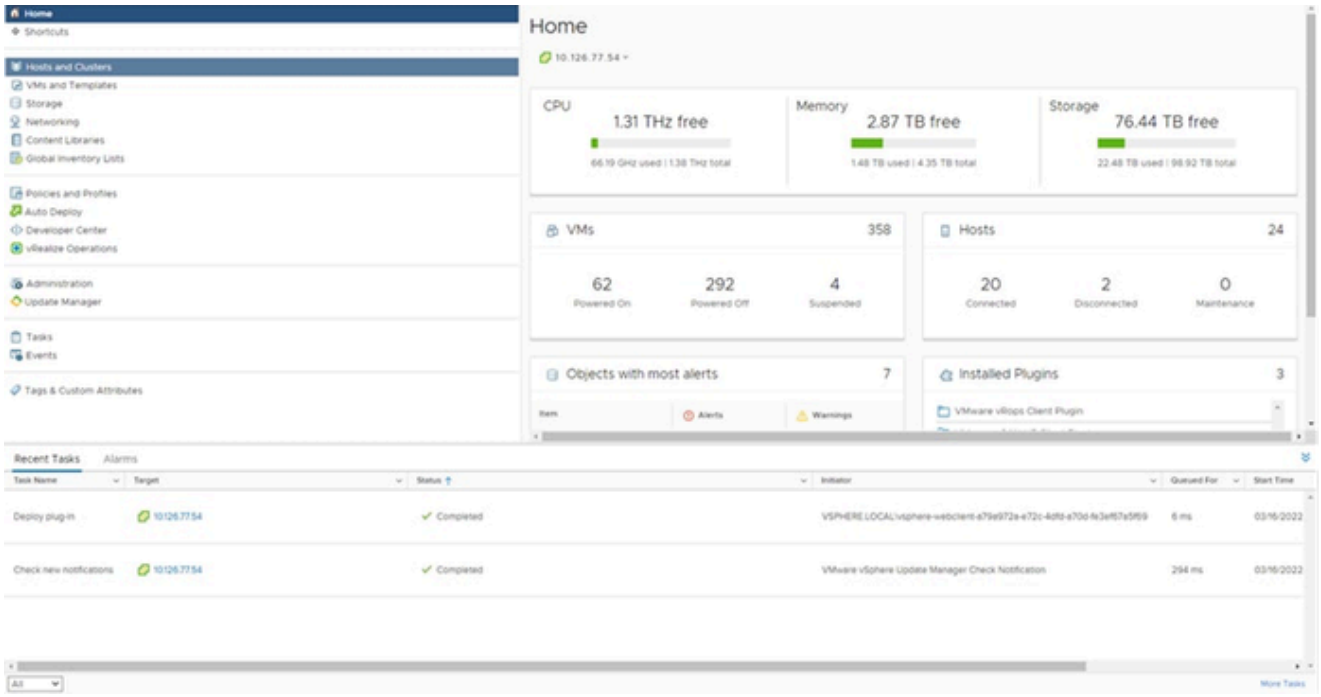
Console

10. 다음 단계를 진행하려면 Network Configuration(네트워크 컨피그레이션)으로 이동합니다.

Web Client vCenter 설치

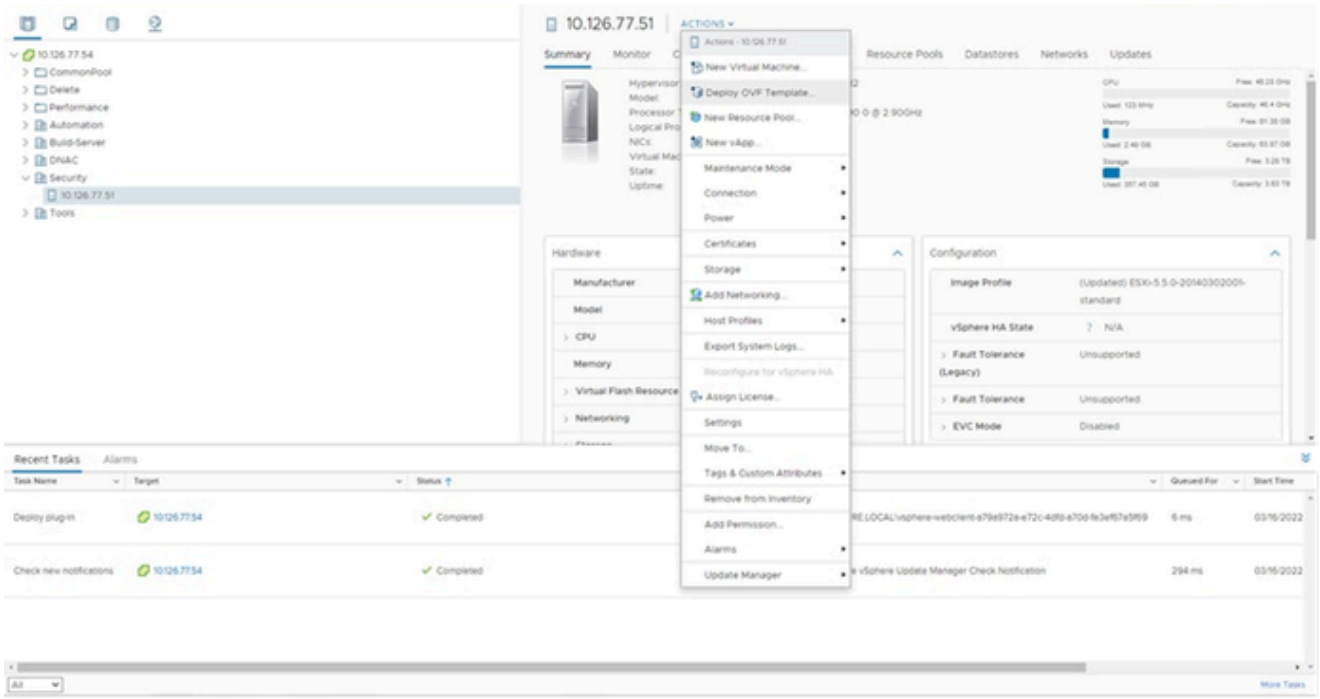
이 클라이언트에서는 웹 클라이언트 vCenter를 사용하여 CX 에이전트 OVA를 구축할 수 있습니다.

1. ESXi/하이퍼바이저 자격 증명을 사용하여 vCenter 클라이언트에 로그인합니다.



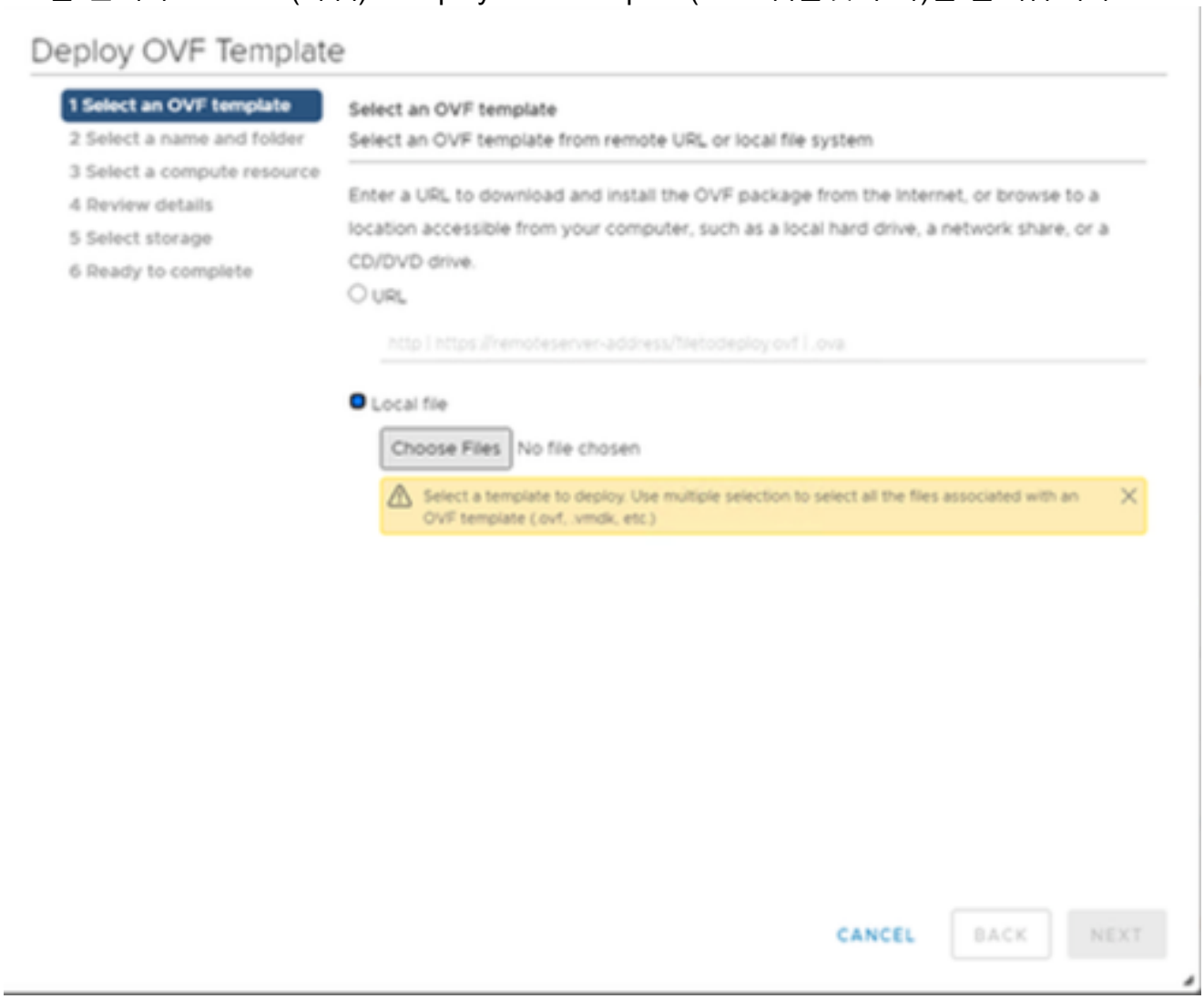
홈 페이지

2. 홈 페이지에서 호스트 및 클러스터를 누릅니다.

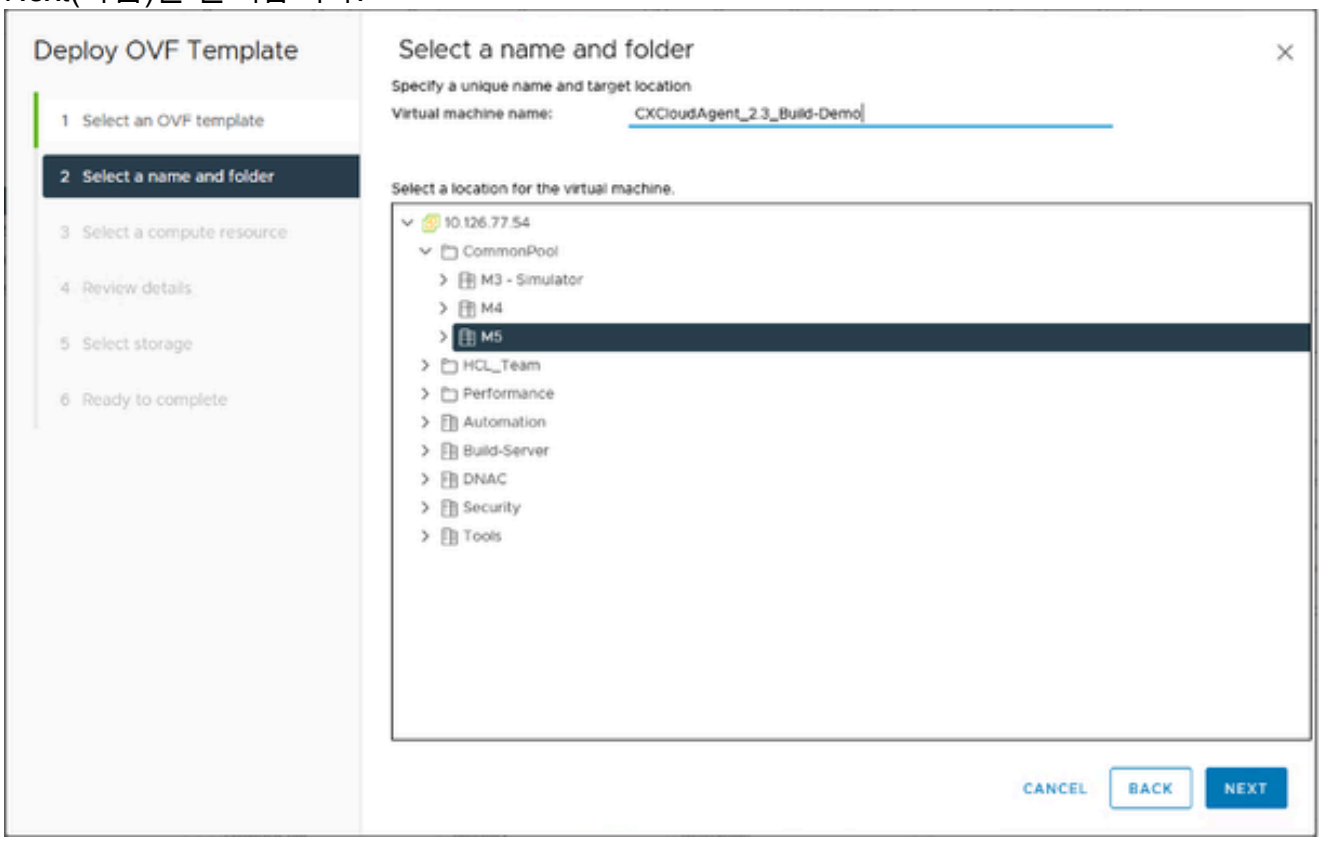


호스트 및 클러스터

3. VM을 선택하고 Action(작업) > Deploy OVF Template(OVF 템플릿 구축)을 클릭합니다.

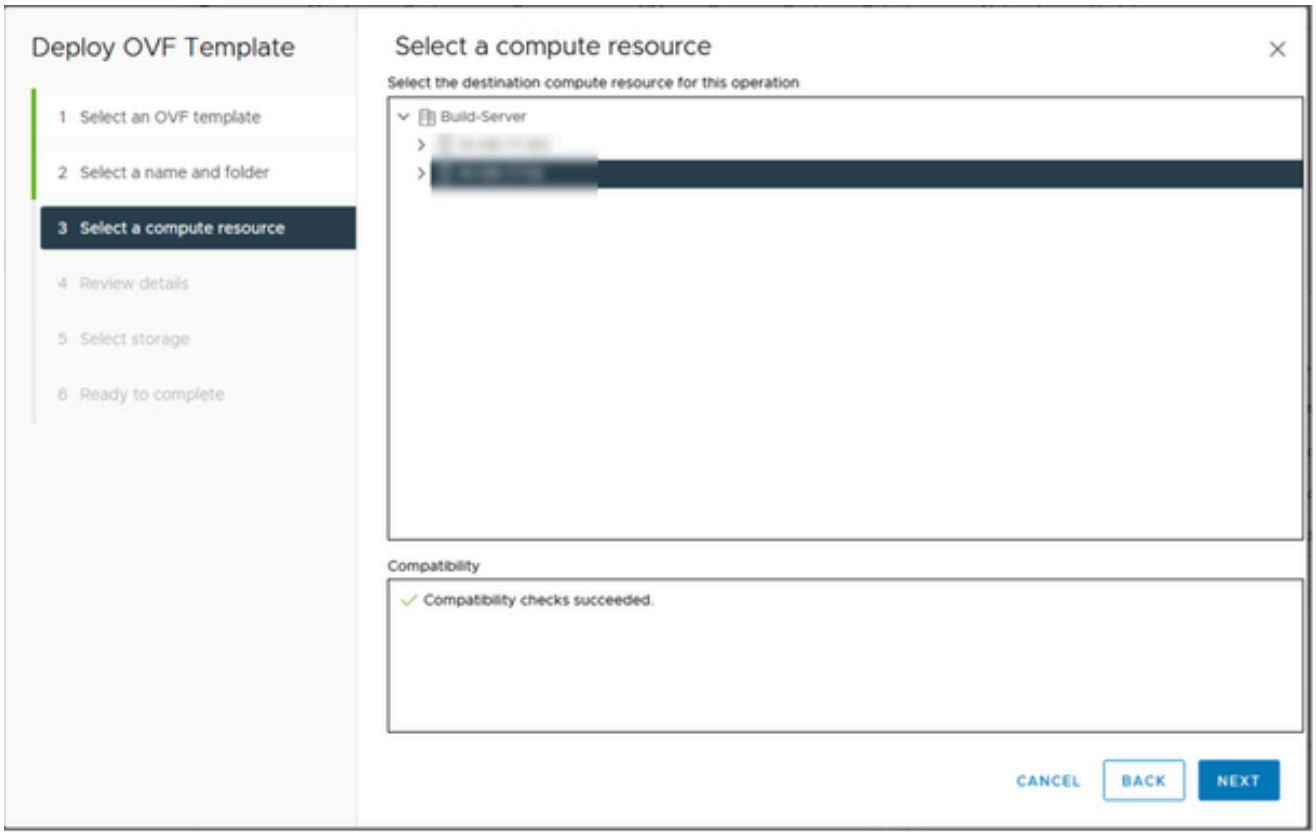


4. URL을 직접 추가하거나 OVA 파일을 찾아 선택합니다.
5. Next(다음)를 클릭합니다.



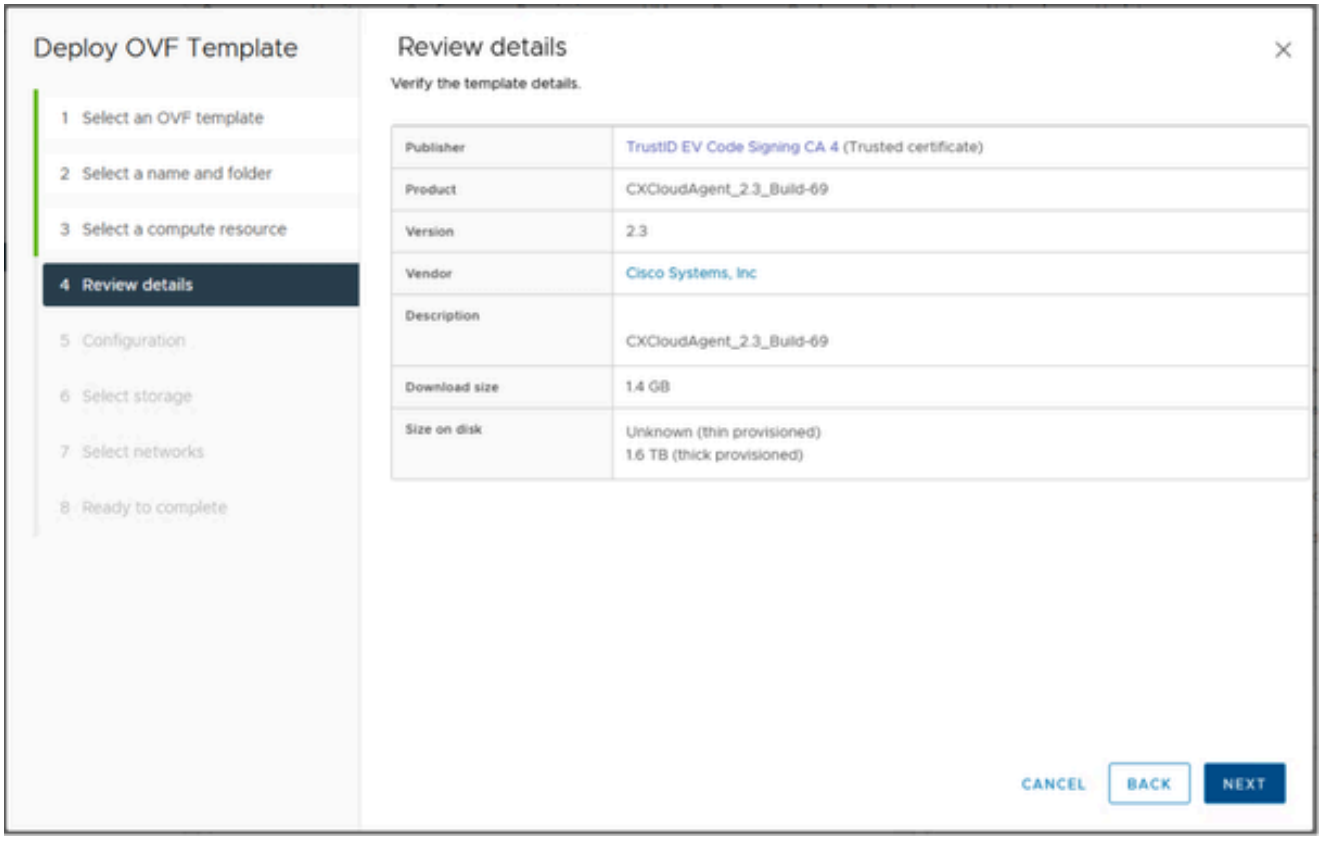
이름 및 폴더

6. 고유한 이름을 입력하고 필요한 경우 위치를 찾습니다.
7. Next(다음)를 클릭합니다.



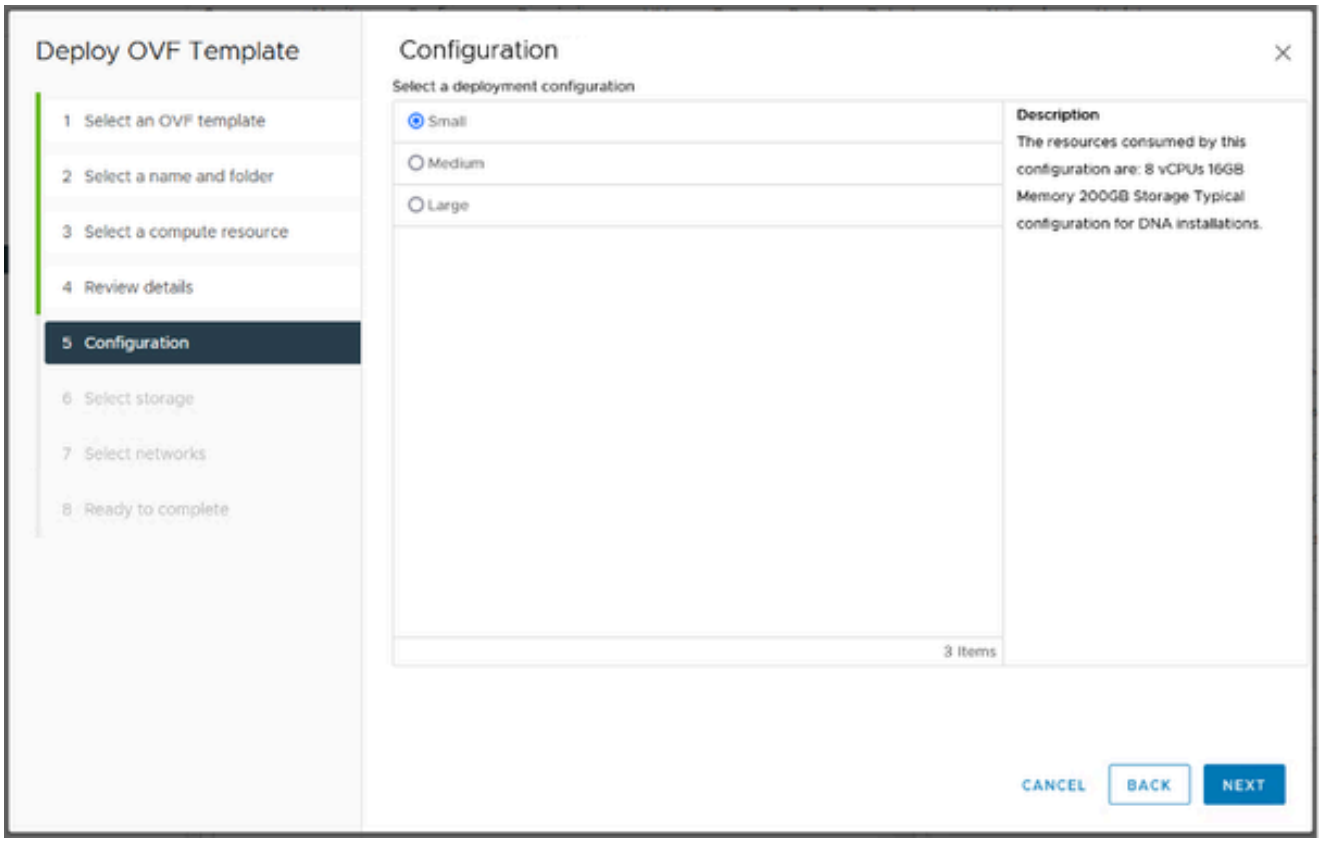
계산 리소스 선택

8. 컴퓨팅 리소스를 선택하고 다음을 누릅니다.



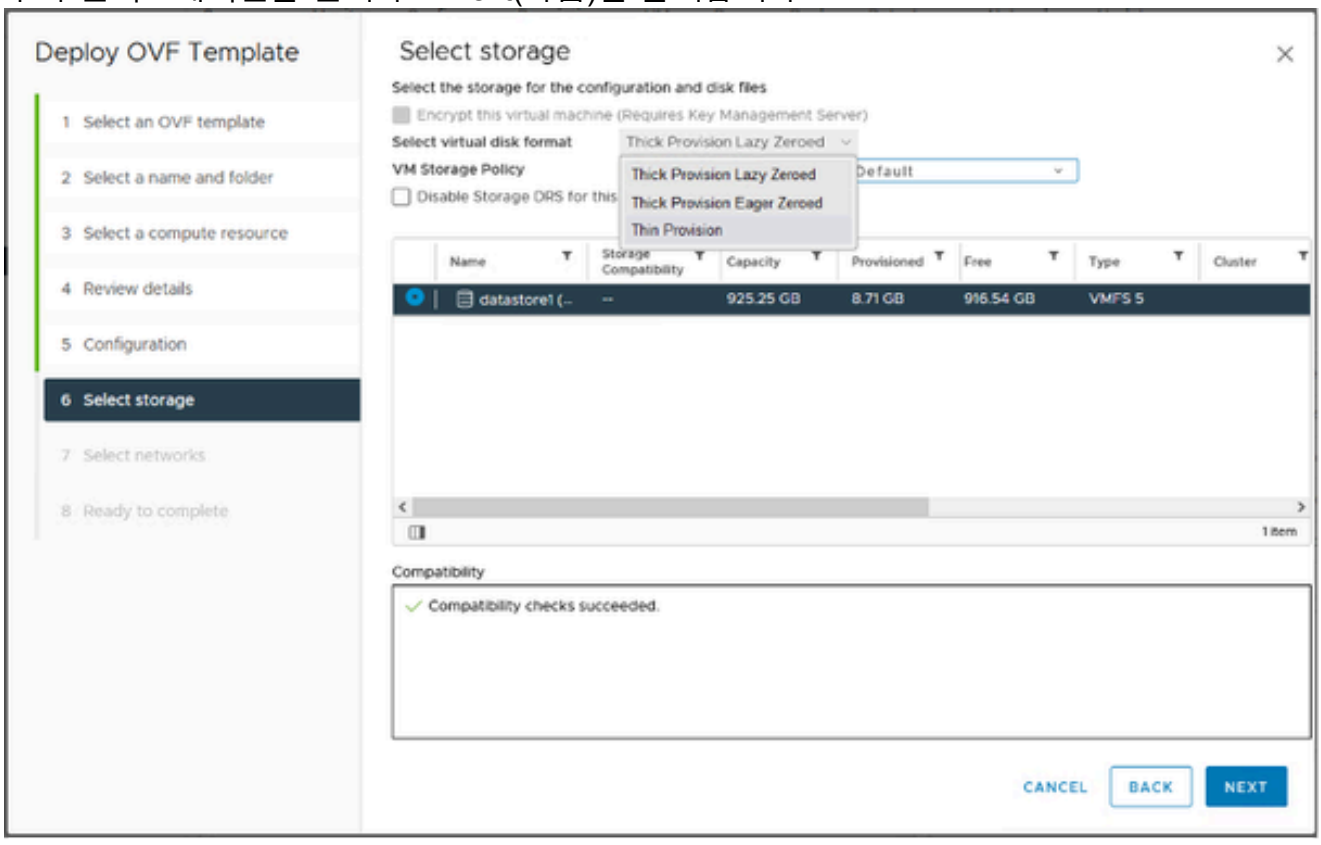
세부 사항 검토

9. 세부 정보를 검토하고 Next(다음)를 클릭합니다.



설정

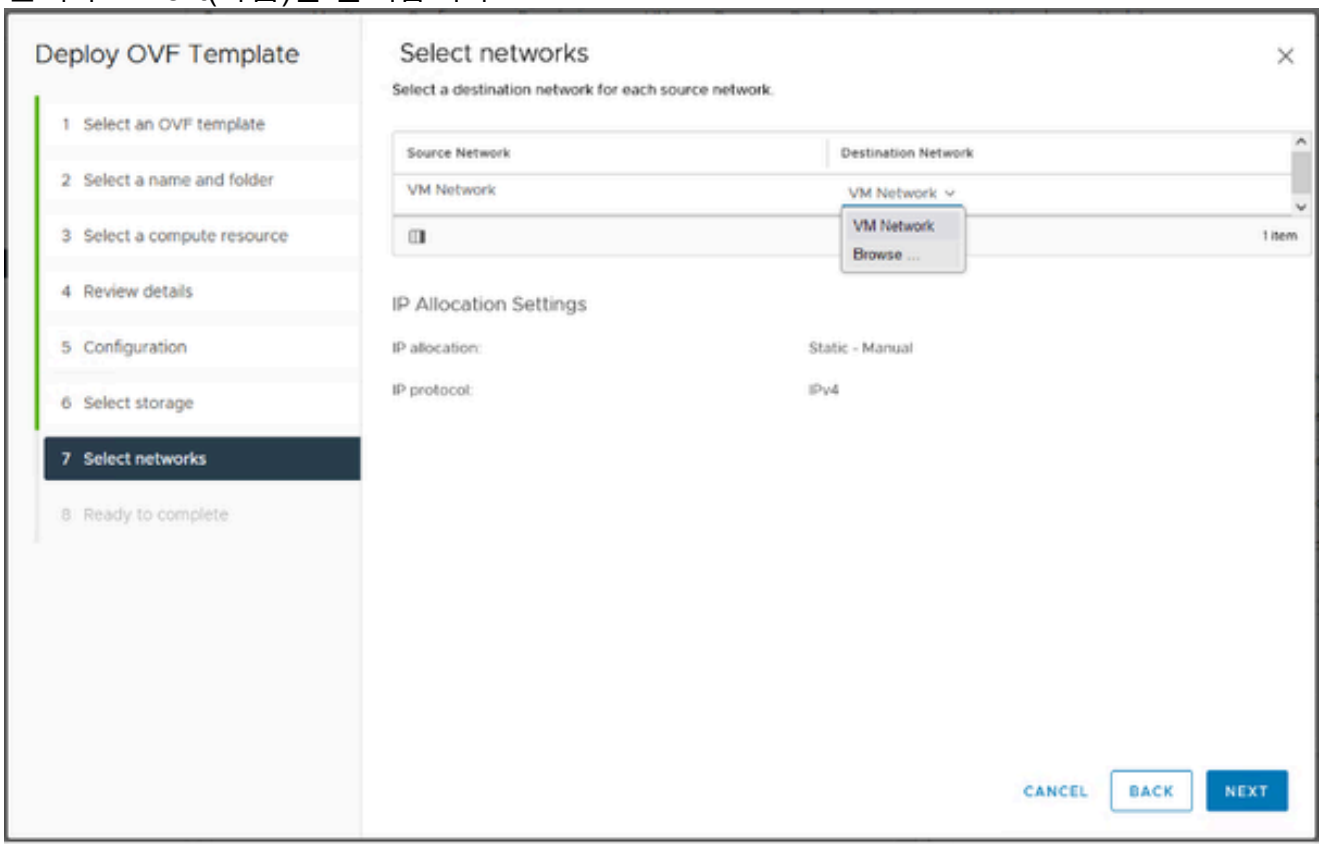
10. 구축 컨피그레이션을 선택하고 Next(다음)를 클릭합니다.



설정

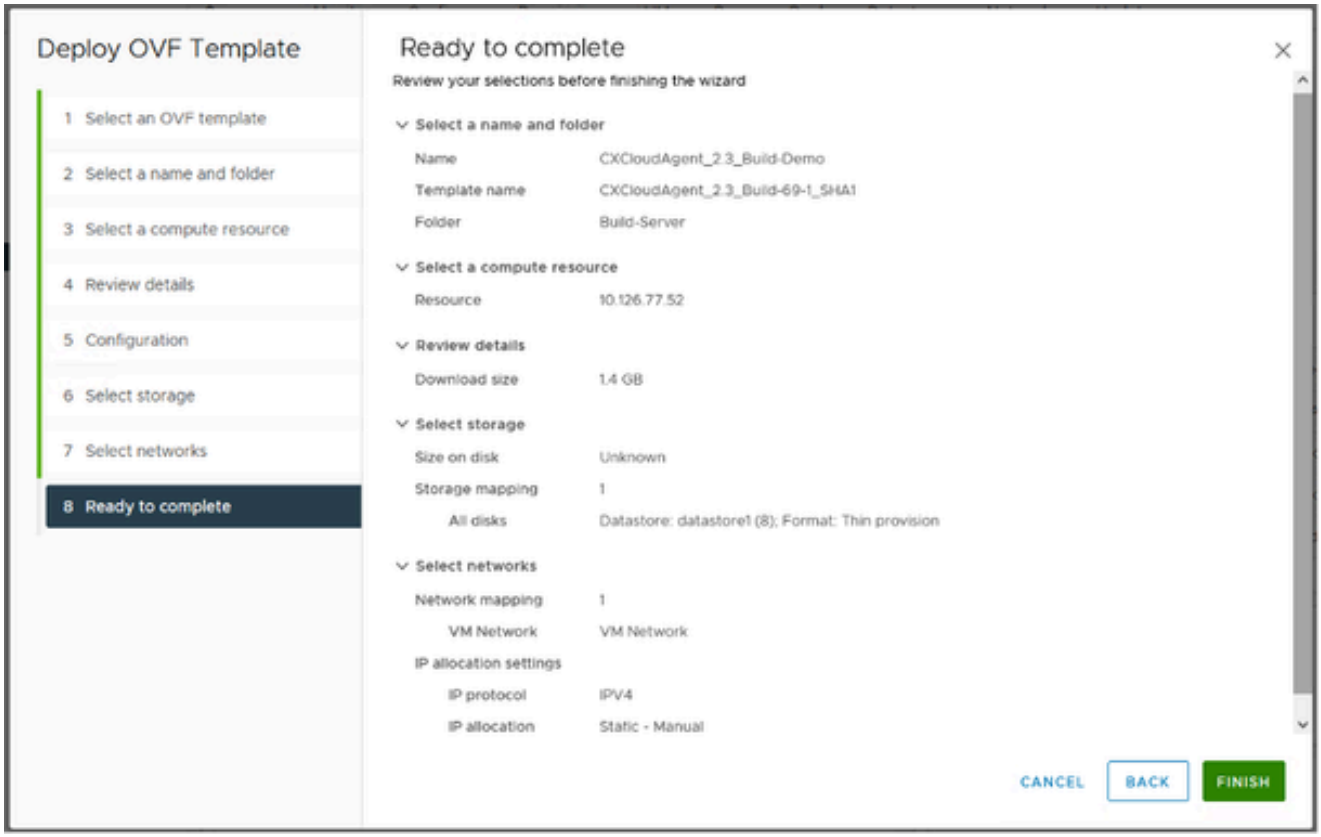
11. 드롭다운 목록에서 Storage(스토리지) > Select virtual disk format(가상 디스크 형식 선택) 을

선택하고 Next(다음)를 클릭합니다.



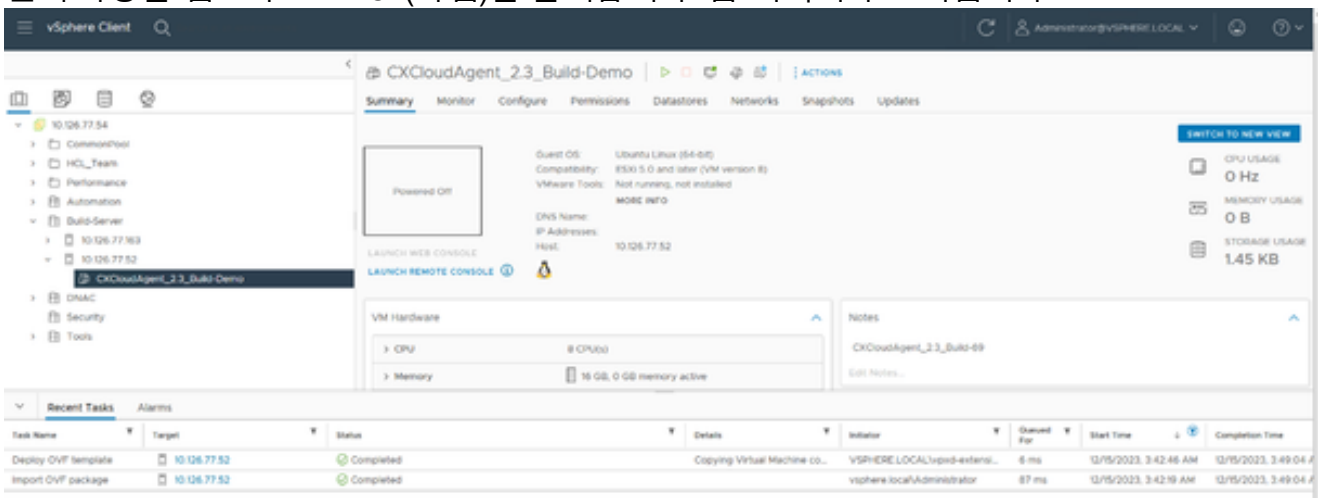
네트워크 선택

12. 네트워크 선택에서 적절한 항목을 선택하고 다음 을 클릭합니다.



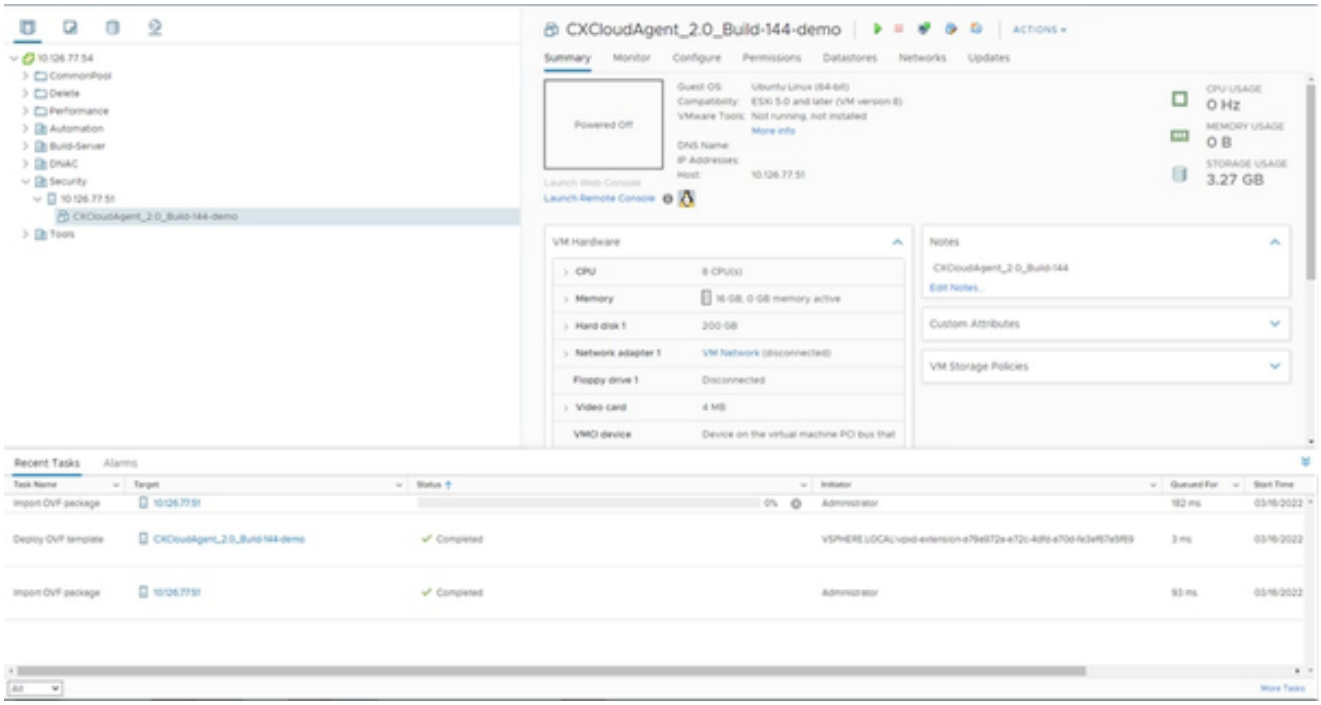
완료 준비

13. 선택 사항을 검토하고 Finish(마침)를 클릭합니다. 홈 페이지가 표시됩니다.



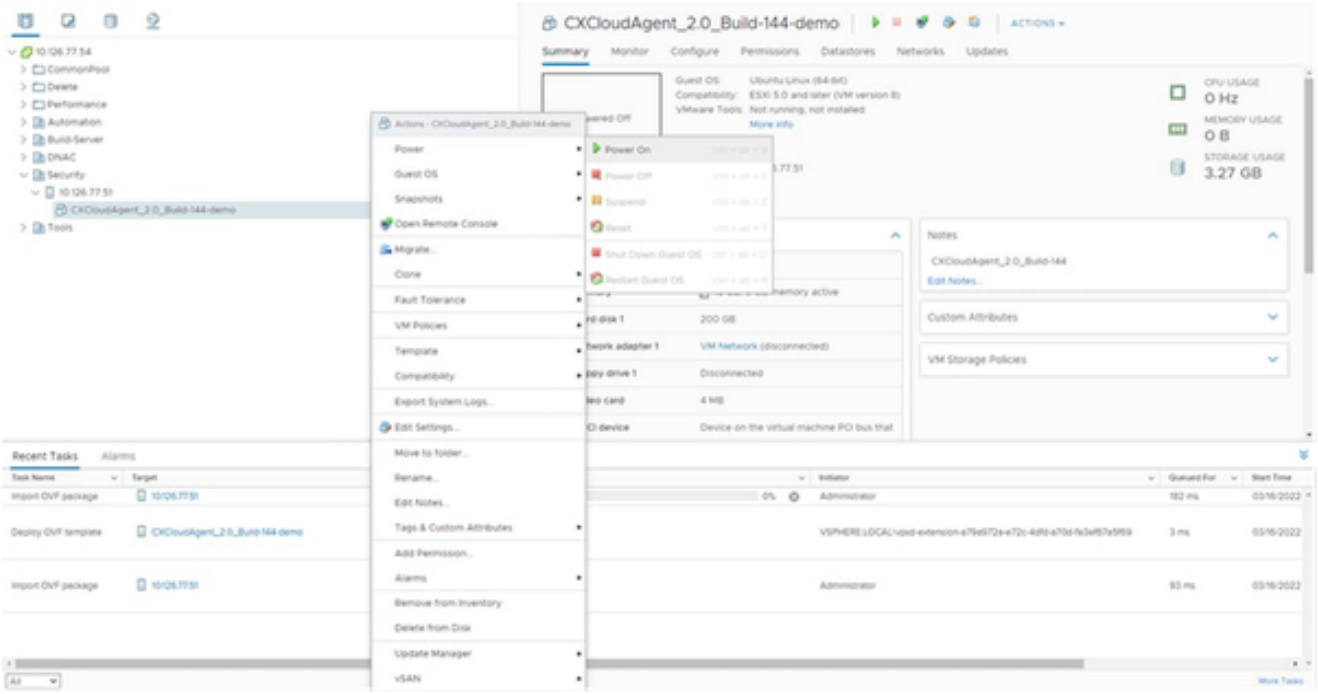
VM 추가됨

14. 새로 추가된 VM을 클릭하여 상태를 확인합니다.



VM 추가됨

15. 설치가 완료되면 VM의 전원을 켜고 콘솔을 엽니다.



콘솔 열기

16. 다음 단계를 진행하려면 Network Configuration(네트워크 컨피그레이션)으로 이동합니다.

Oracle Virtual Box 7.0.12 설치

이 클라이언트는 Oracle Virtual Box를 통해 CX 에이전트 OVA를 구축합니다.

1. CXCloudAgent_3.1 OVA를 모든 폴더에 Windows 상자에 다운로드합니다.
2. 명령줄 인터페이스를 사용하여 폴더를 찾습니다.
3. tar -xvf D:\CXCloudAgent_3.1_Build-xx.ova 명령을 사용하여 OVA 파일의 압축을 폽니다.

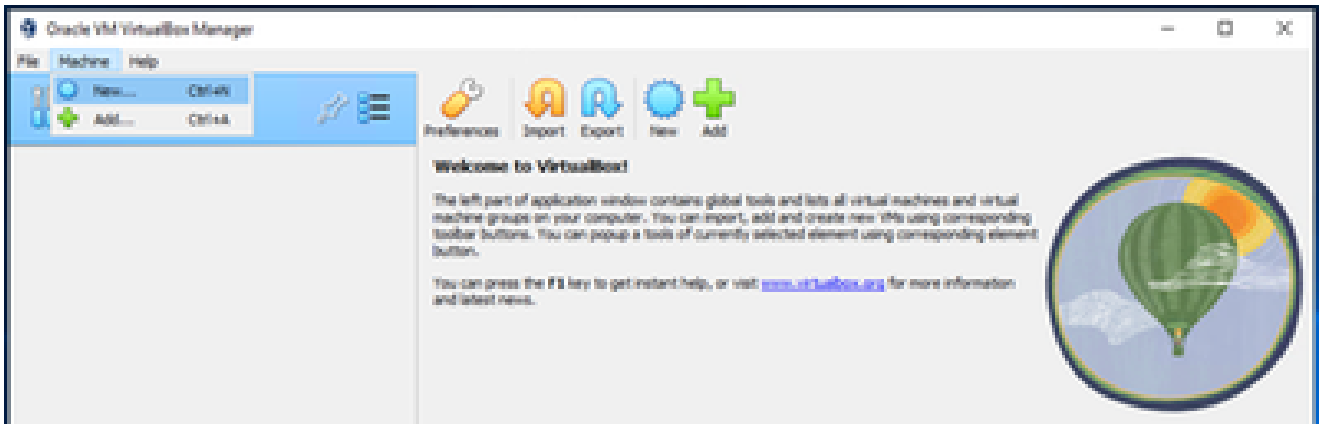
```
D:\>cd CXCAGENT

D:\CXCAGENT>tar -xvf CXCloudAgent_2.3_Build-69-1_SHA1_signed.ova
x CXCloudAgent_2.3_Build-69-1_SHA1.ovf
x CXCloudAgent_2.3_Build-69-1_SHA1.mf
x CXCloudAgent_2.3_Build-69-1_SHA1.cert
x CXCloudAgent_2.3_Build-69-1_SHA1-disk1.vmdk

D:\CXCAGENT>_
```

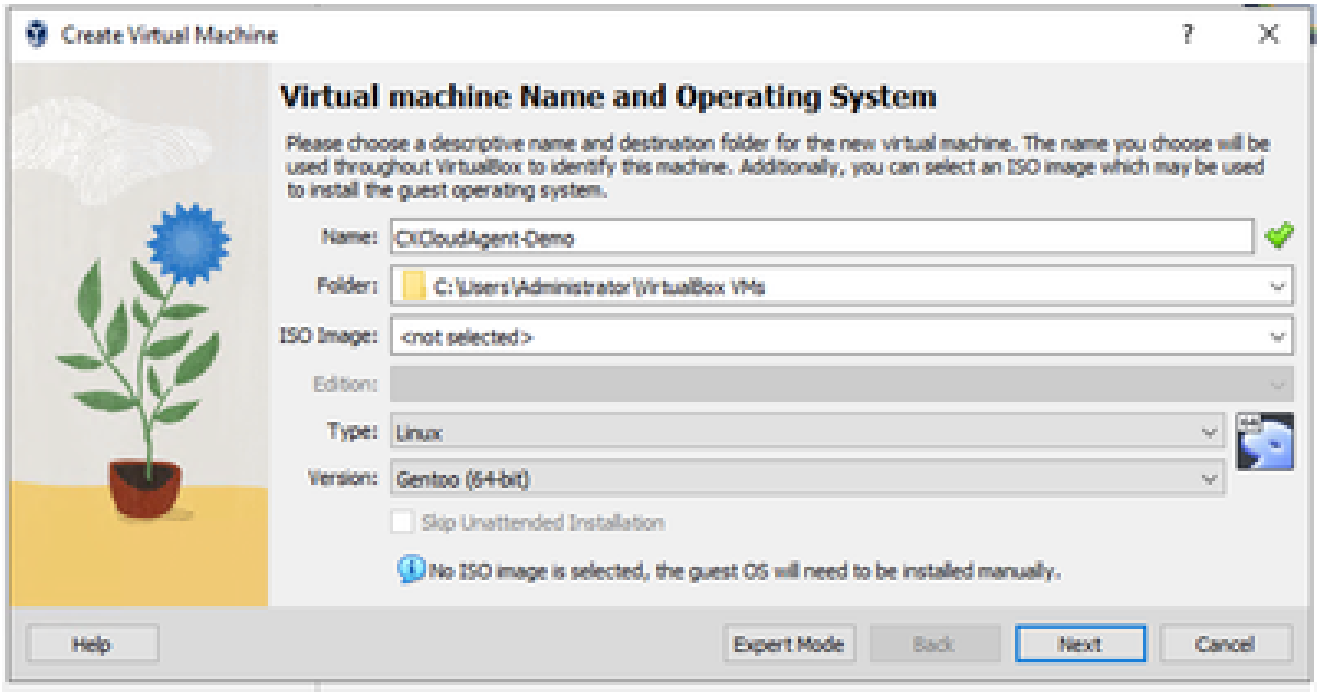
OVA 파일 압축 해제

4. Oracle VM UI를 엽니다.



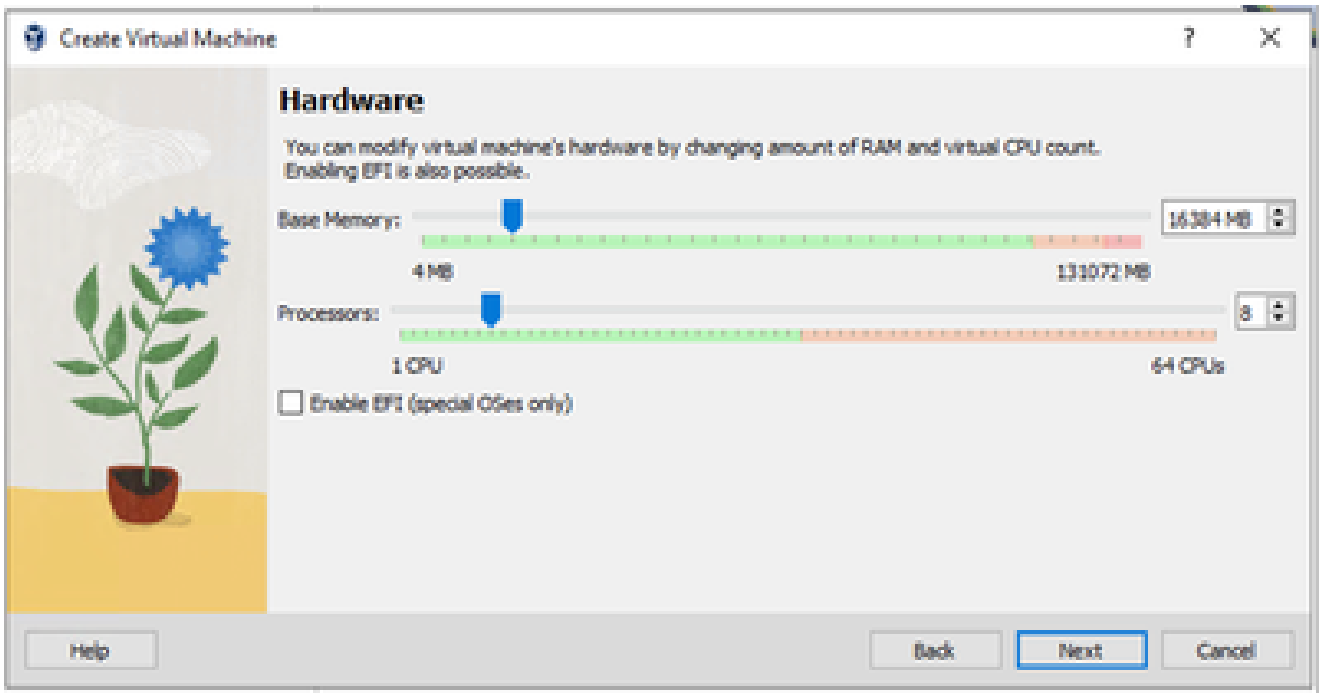
Oracle VM

5. 메뉴에서 머신>새로 만들기를 선택합니다. Create Virtual Machine(가상 머신 생성) 창이 열립니다.



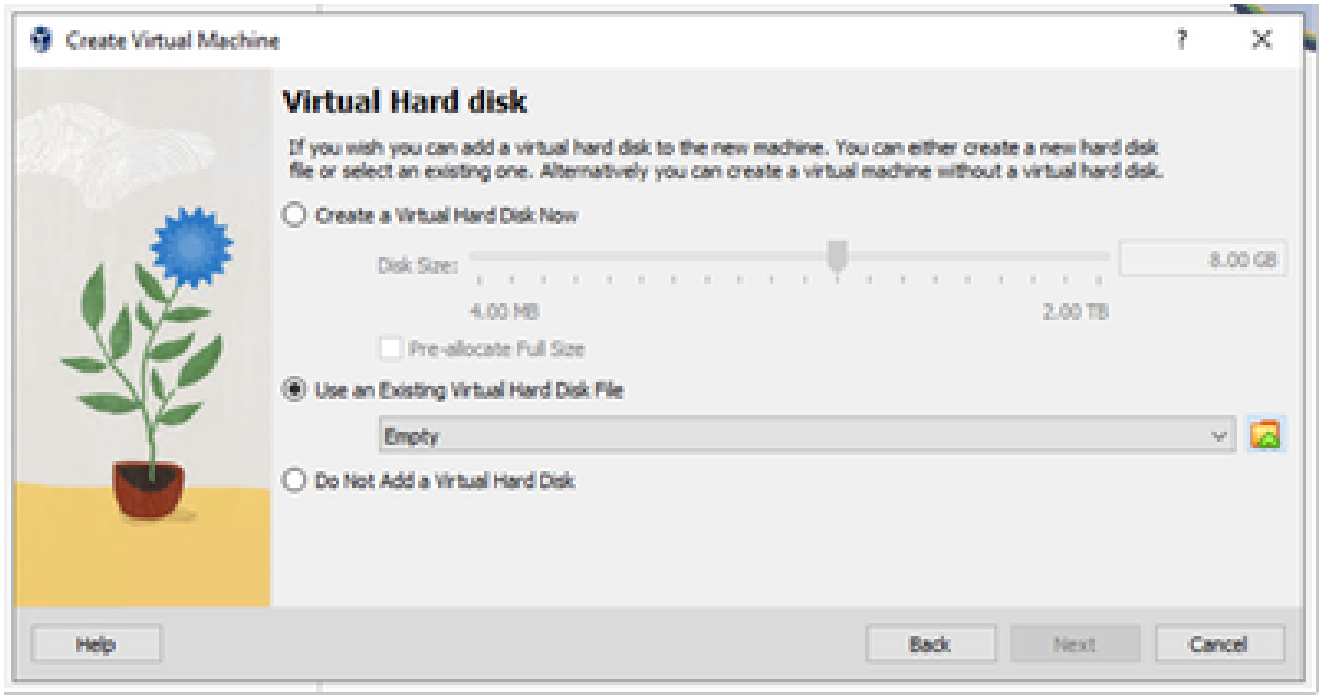
가상 컴퓨터 만들기

6. Virtual machine Name and Operating System(가상 머신 이름 및 운영 체제) 창에서 다음 세부 정보를 입력합니다.
   이름: VM 이름
   폴더: VM 데이터를 저장할 위치
   ISO 이미지: none
   유형: Linux
   버전: 젠토(64비트)
7. Next(다음)를 클릭합니다. Hardware(하드웨어) 창이 열립니다.



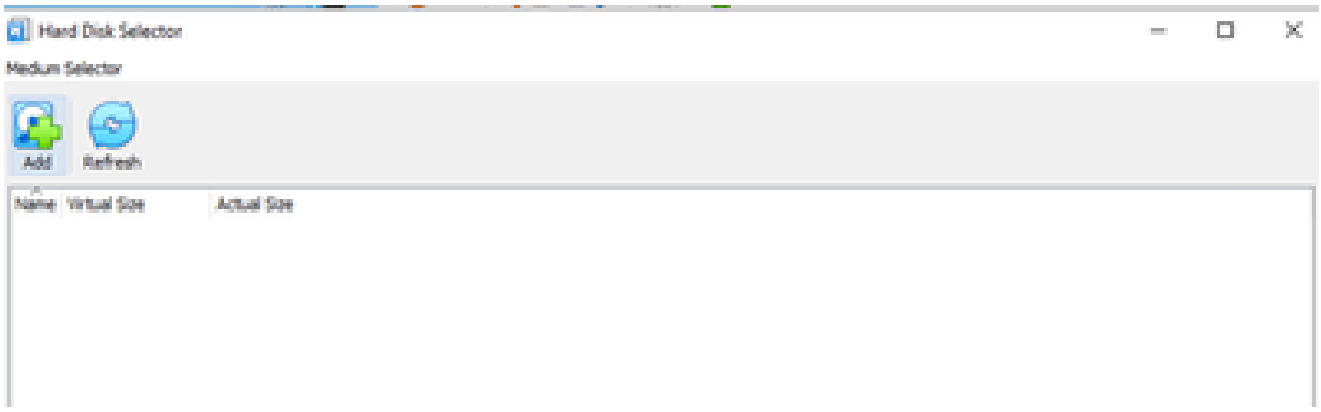
하드웨어

8. 기본 메모리(16384MB) 및 프로세서(8 CPU)를 입력하고 다음을 클릭합니다. 가상 하드 디스크 창이 열립니다.



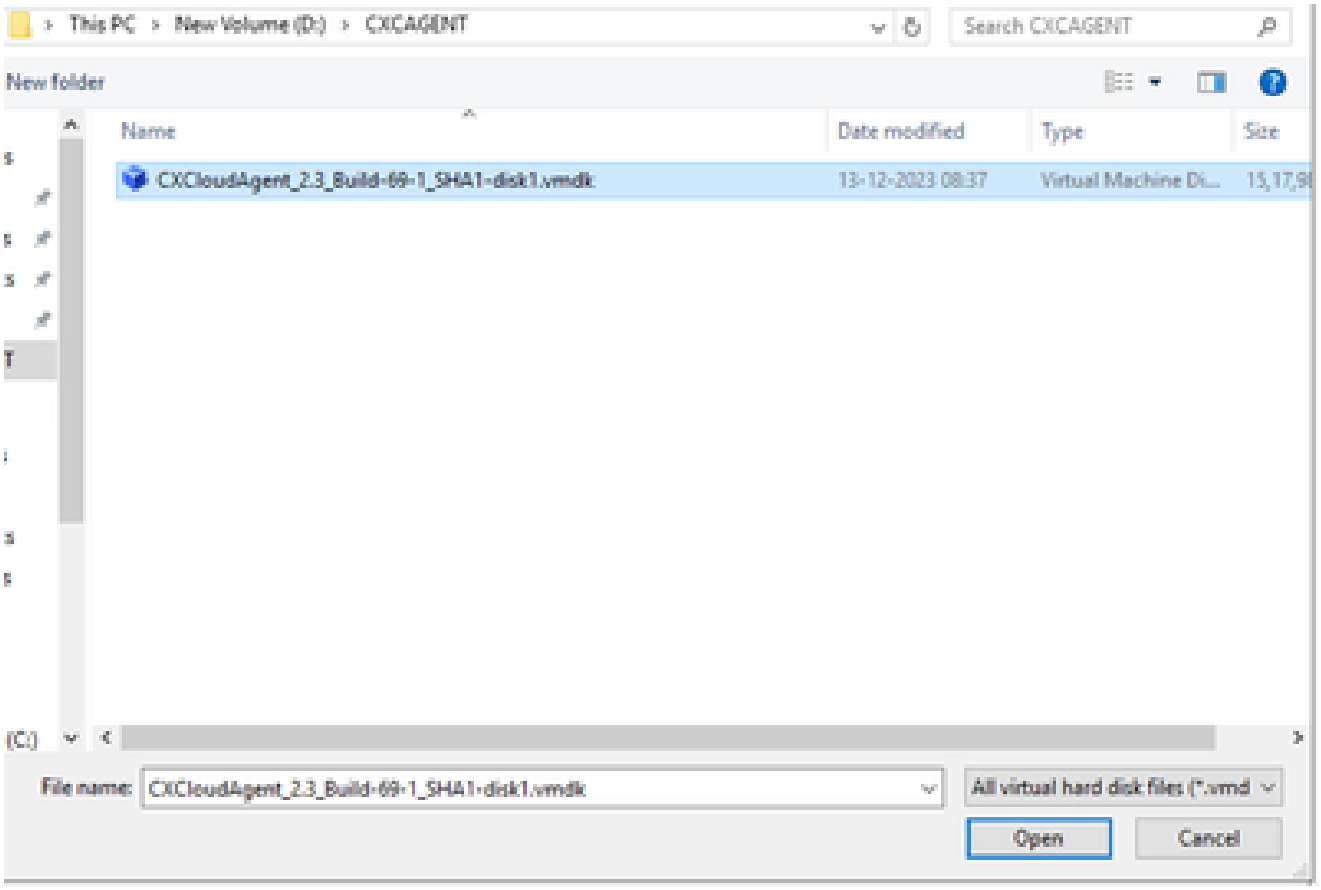
가상 하드 디스크

9. Use an Existing Virtual Hard Disk File(기존 가상 하드 디스크 파일 사용) 라디오 버튼을 선택하고 Browse(찾아보기) 아이콘을 선택합니다. Hard Disk Selector 창이 열립니다.



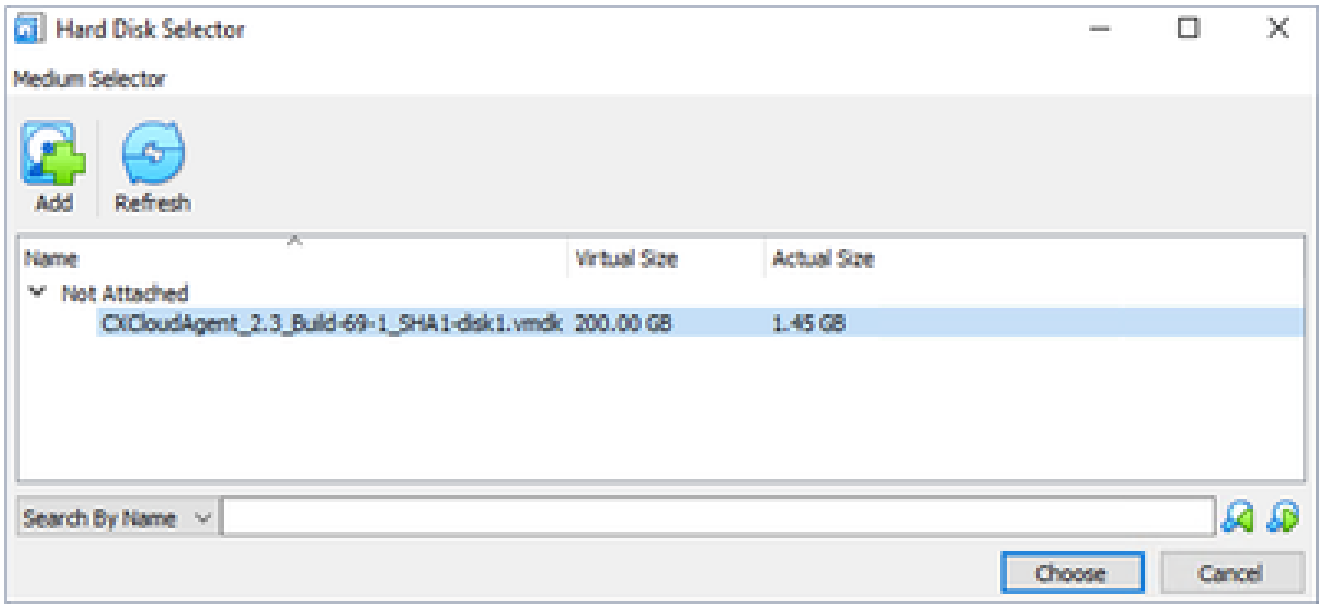
하드 디스크 선택기

10. OVA 폴더로 이동하여 VMDK 파일을 선택합니다.



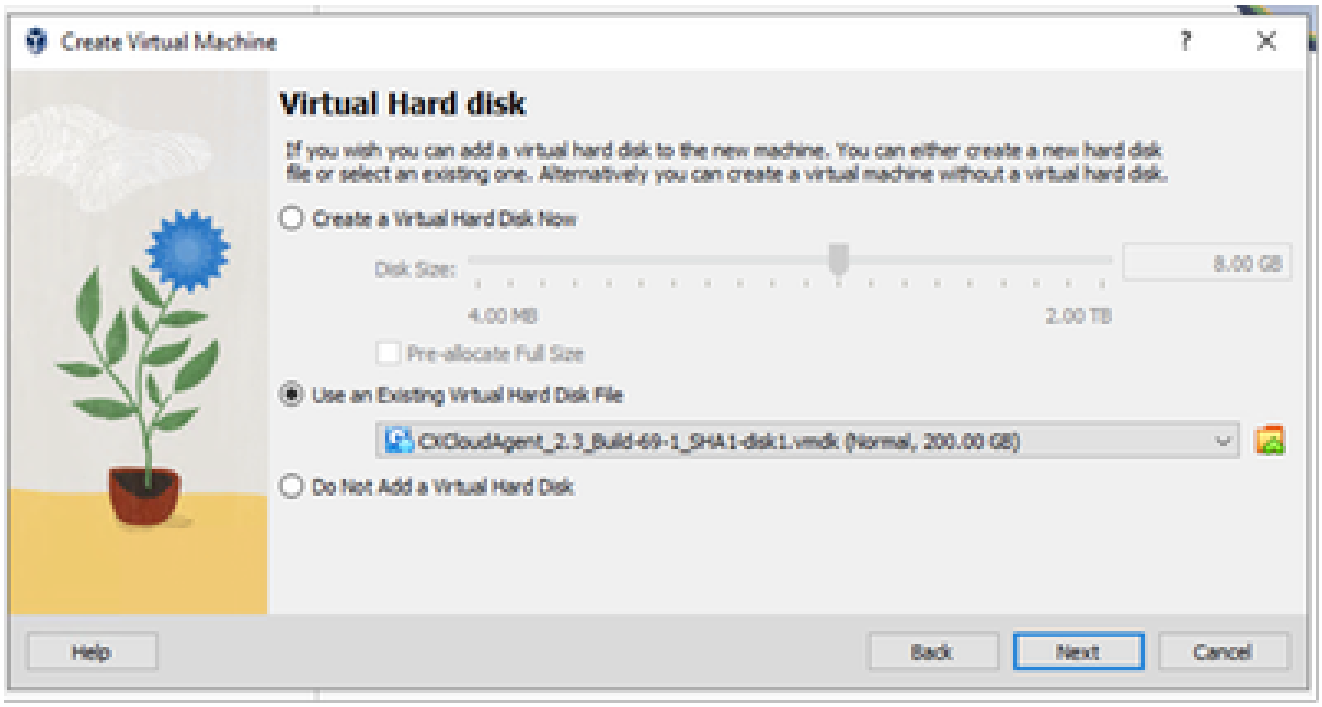
OVA 폴더

11. 열기를 클릭하십시오. 파일이 Hardware Disk Selector 창에 표시됩니다.



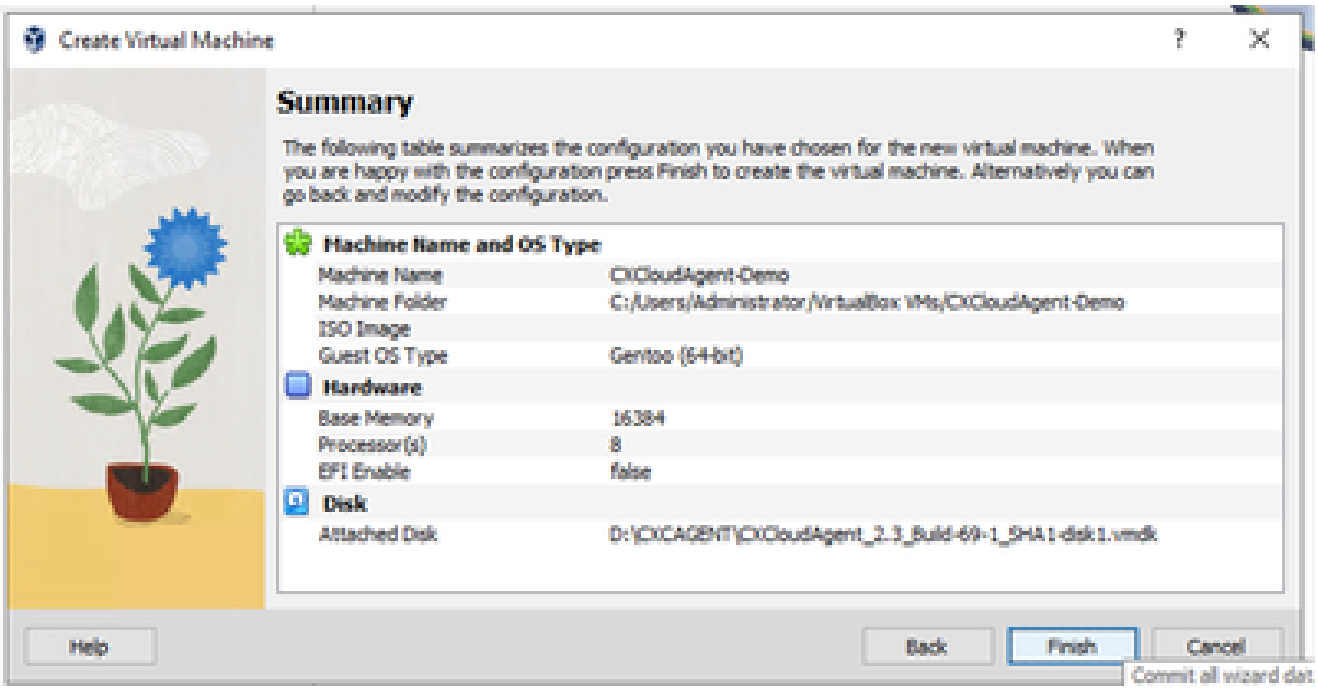
하드 디스크 선택기

12. 선택을 클릭합니다. 가상 하드 디스크 창이 열립니다. 표시된 옵션이 선택되었는지 확인합니다.



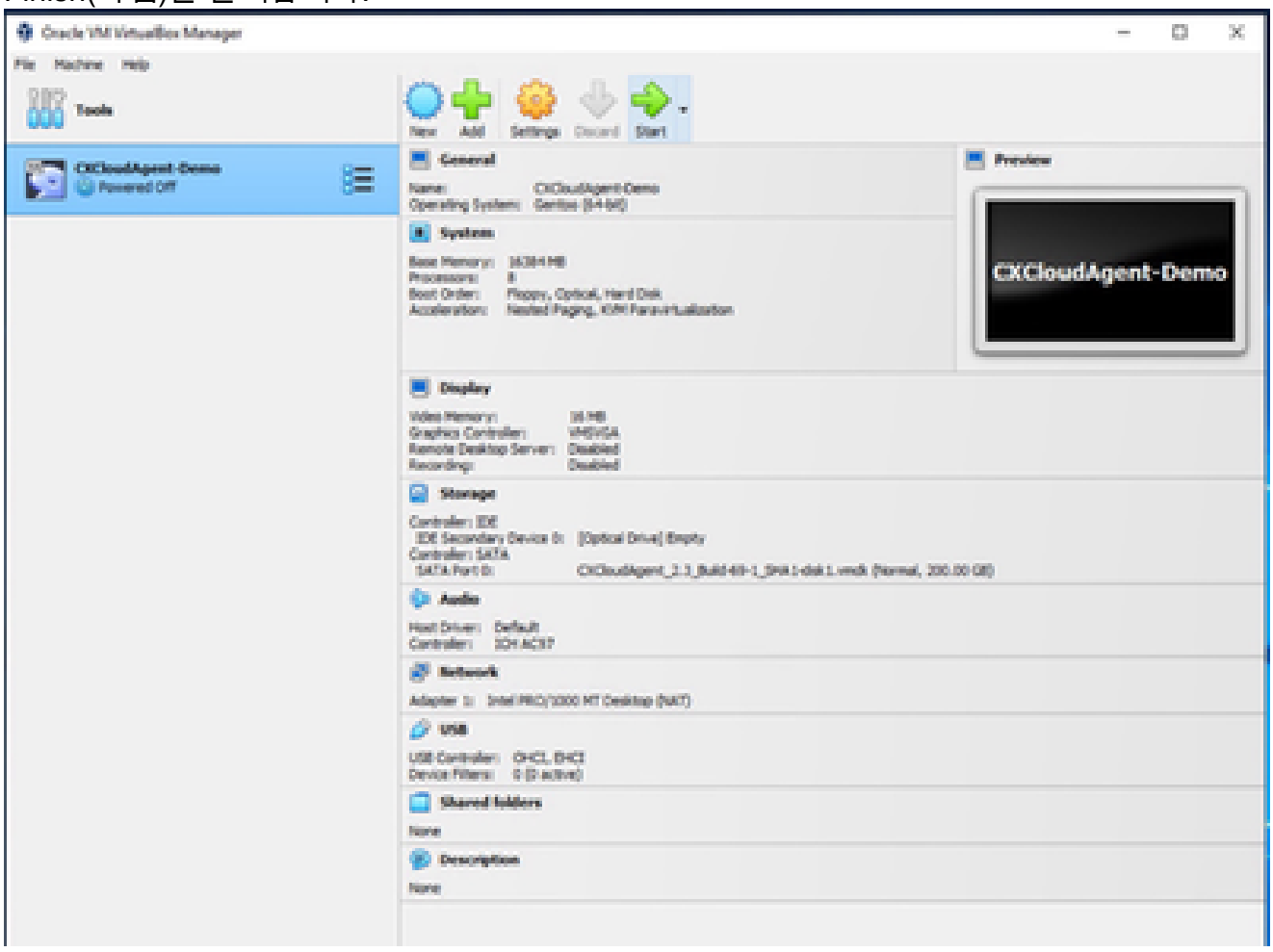
파일 선택

13. Next(다음)를 클릭합니다. 요약 창이 열립니다.



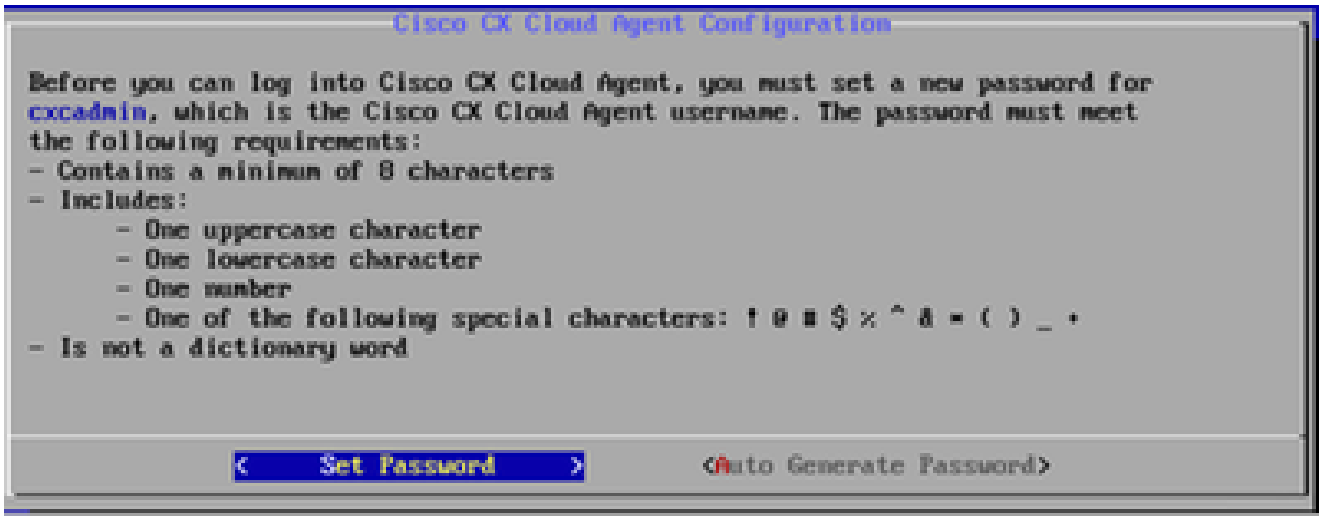
요약

14. Finish(마침)를 클릭합니다.



VM 콘솔 시작

15. 구축된 VM을 선택하고 시작을 클릭합니다. VM이 켜지고 설정에 대한 콘솔 화면이 표시됩니다.



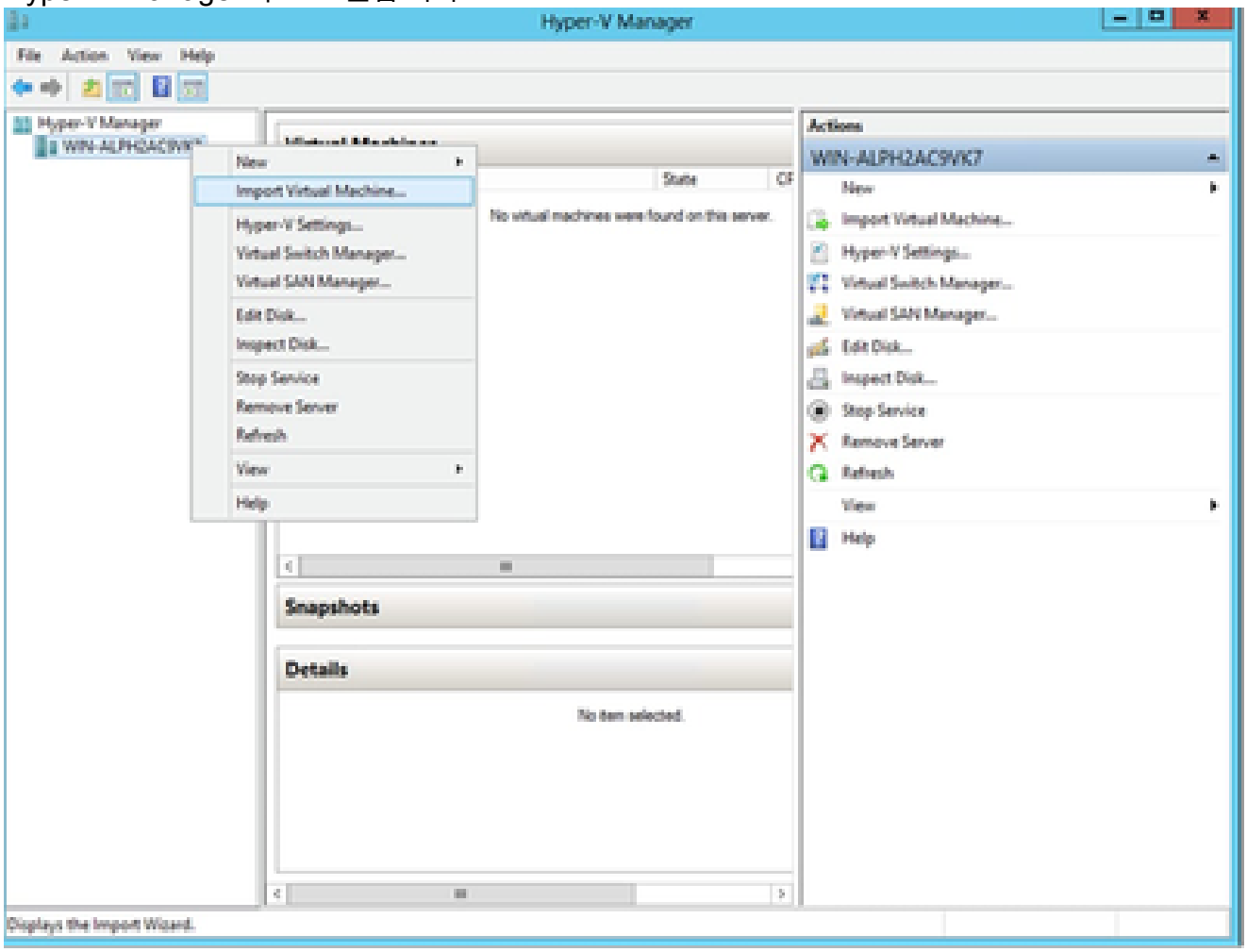
콘솔 열기

16. 다음 단계를 진행하려면 Network Configuration(네트워크 컨피그레이션)으로 이동합니다.

Microsoft Hyper-V 설치

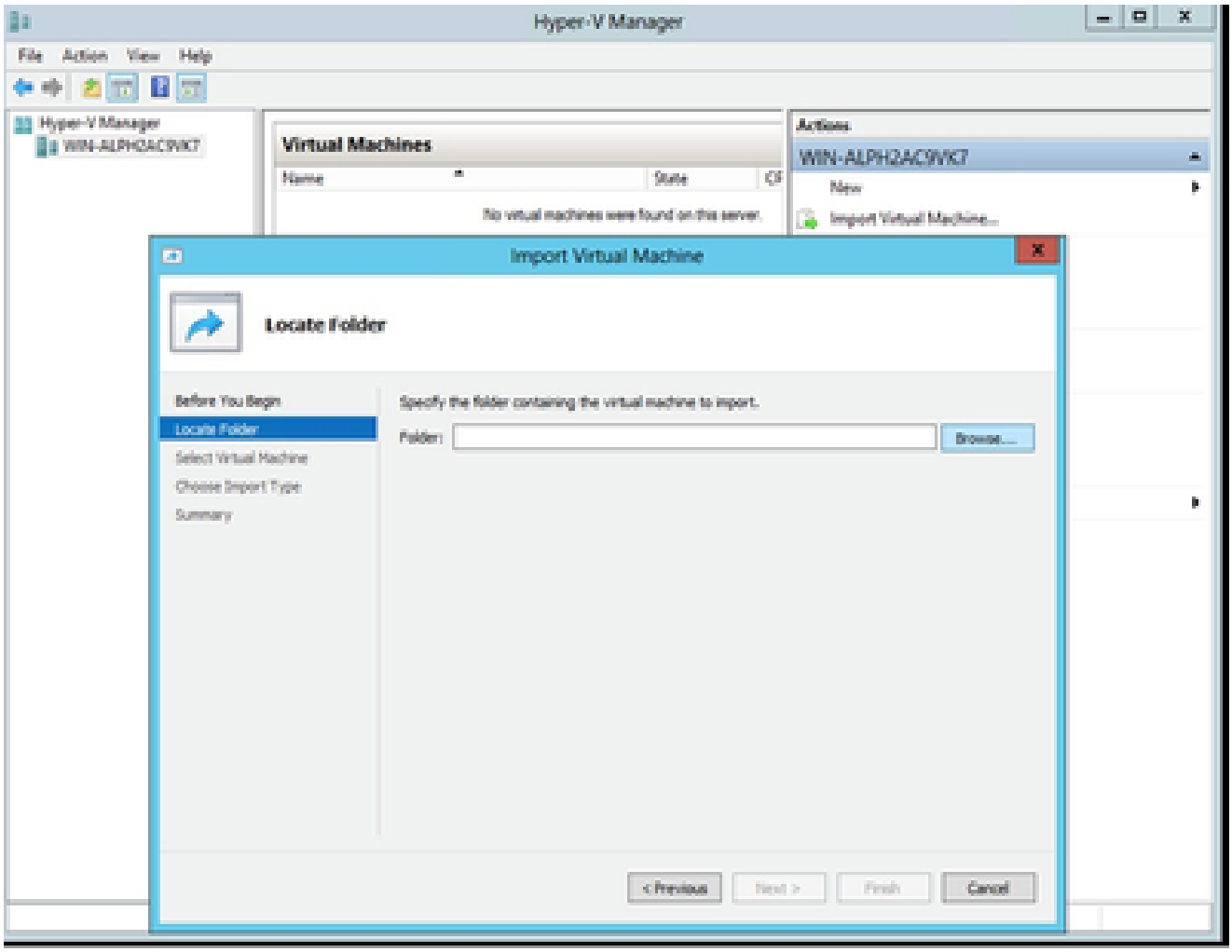
이 클라이언트는 Microsoft Hyper-V 설치를 통해 CX Agent OVA를 구축합니다.

1. Hyper-V Manager에 로그인합니다.



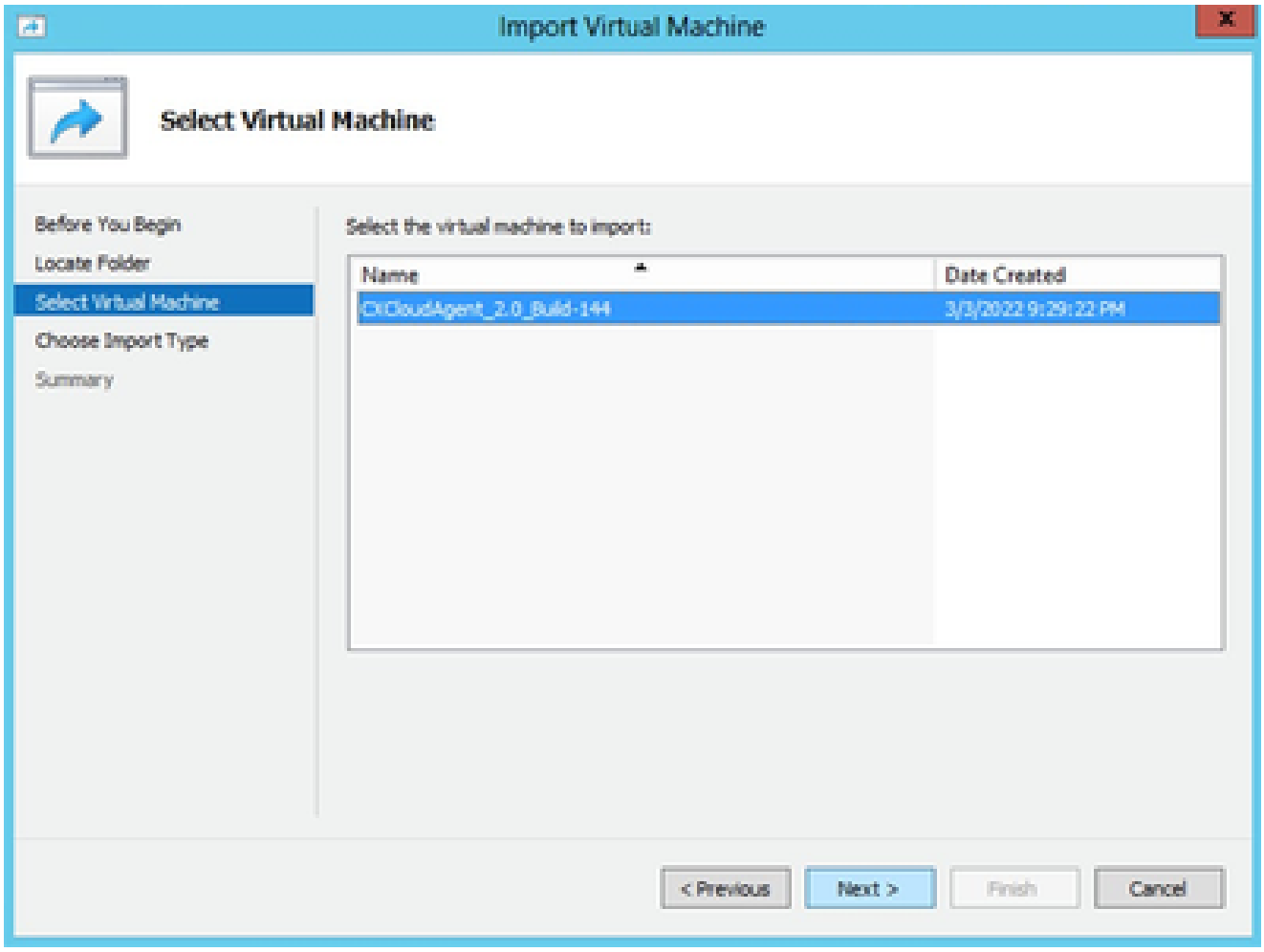
Hyper V 관리자

2. 대상 VM을 선택하고 마우스 오른쪽 버튼을 클릭하여 메뉴를 연 다음 Import Virtual Machine을 선택합니다.



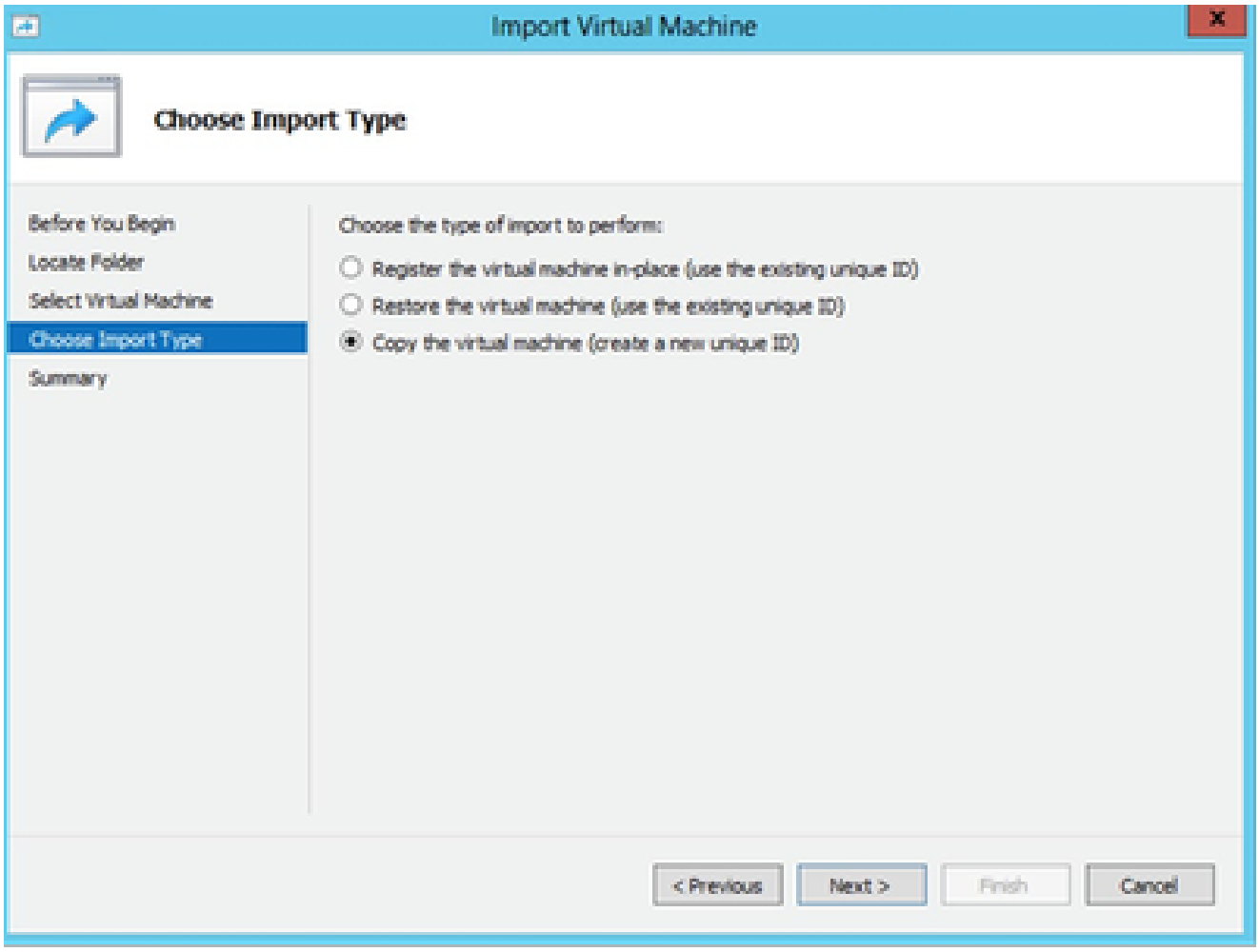
가져올 폴더

3. 다운로드 폴더를 찾아 선택하고 Next(다음)를 클릭합니다.



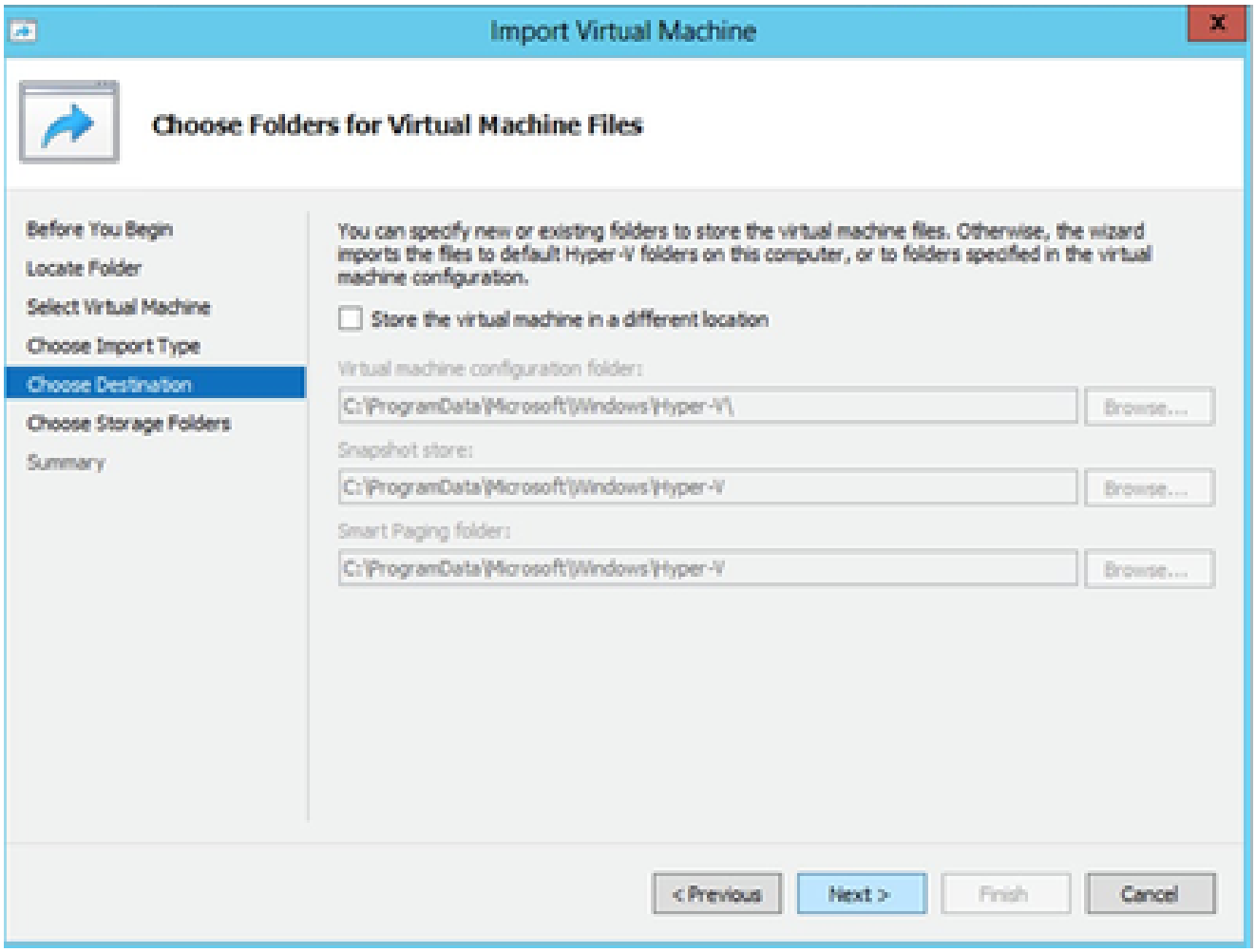
VM 선택

4. VM을 선택하고 Next(다음)를 클릭합니다.



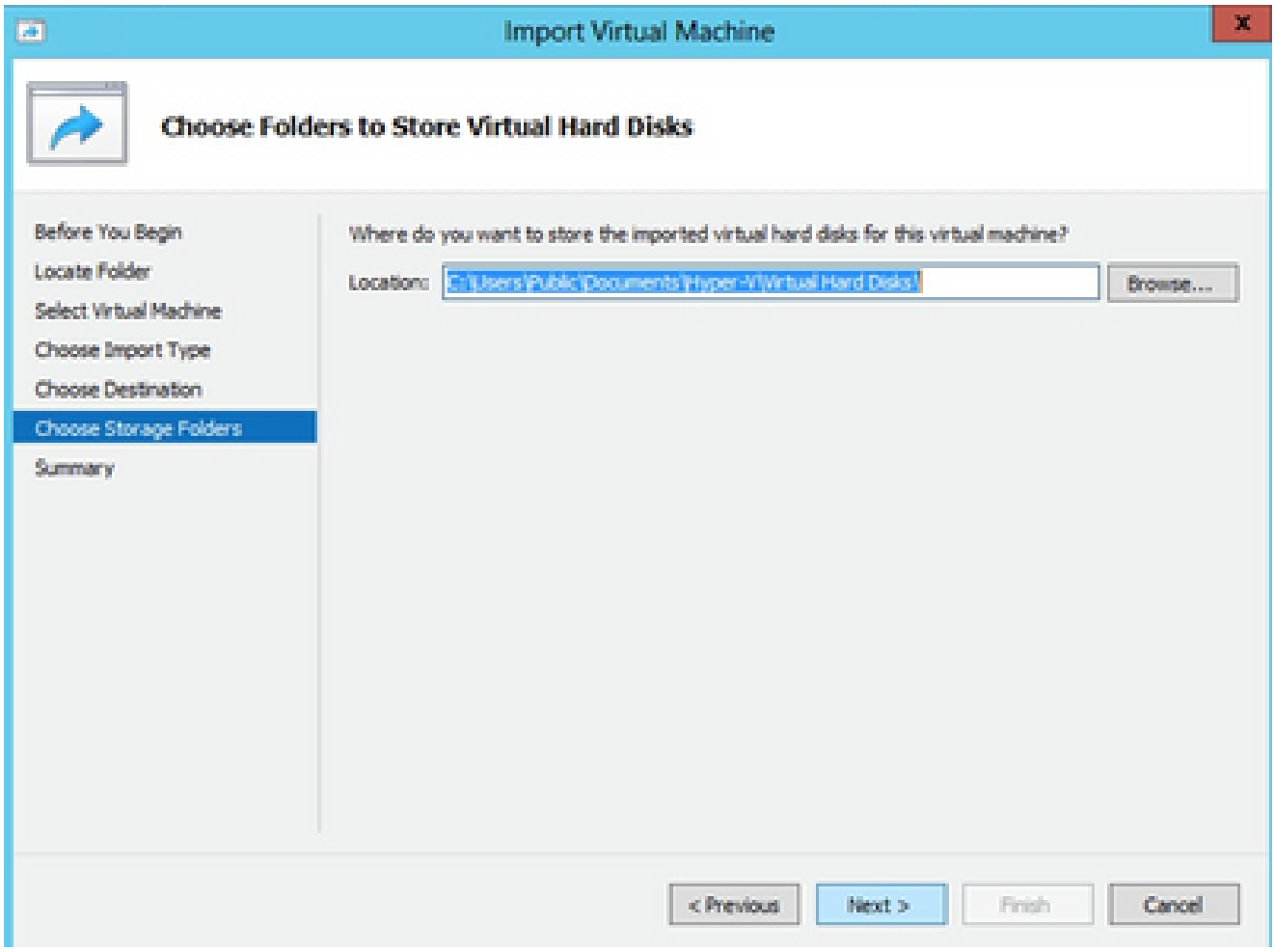
가져오기 유형

5. Copy the virtual machine (create a new unique ID)(가상 머신 복사(새 고유 ID 생성)) 라디오 버튼을 선택하고 Next(다음)를 클릭합니다.



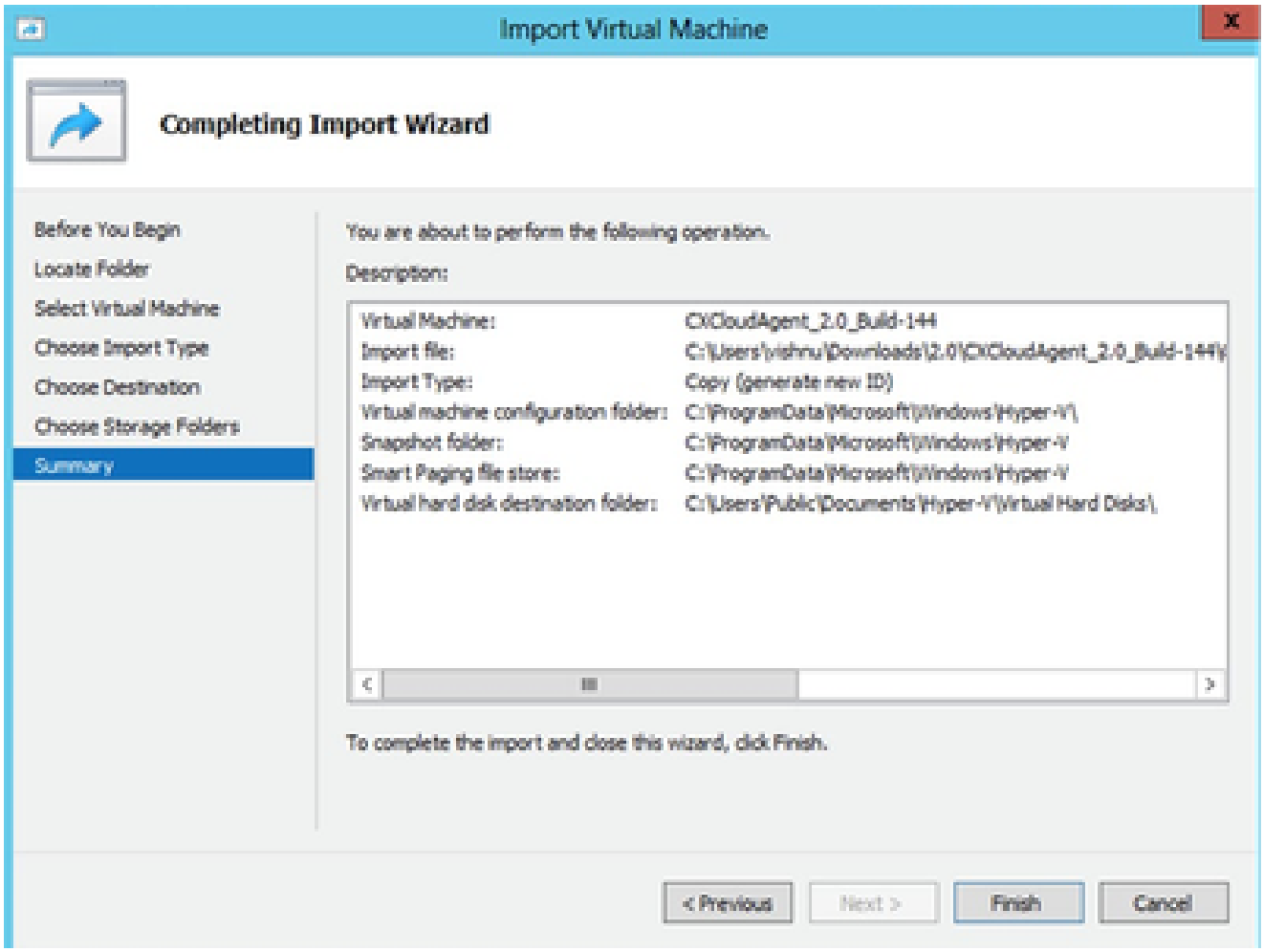
가상 컴퓨터 파일의 폴더 선택

6. VM 파일의 폴더를 찾아 선택합니다. 기본 경로를 사용하는 것이 좋습니다.
7. Next(다음)를 클릭합니다.



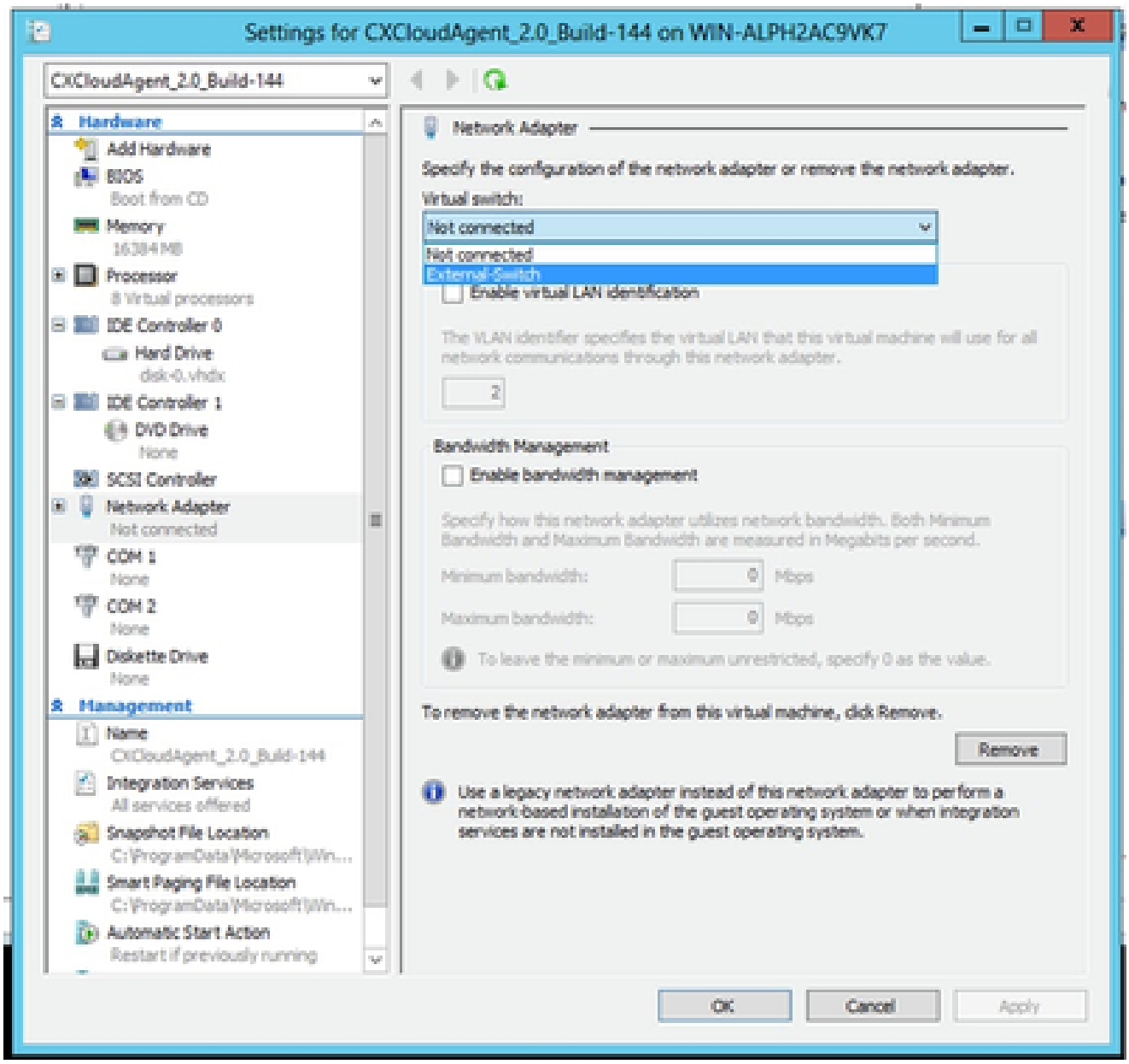
가상 하드 디스크를 저장할 폴더

8. VM 하드 디스크를 저장할 폴더를 찾아 선택합니다. 기본 경로를 사용하는 것이 좋습니다.
9. Next(다음)를 클릭합니다. VM 요약이 표시됩니다.



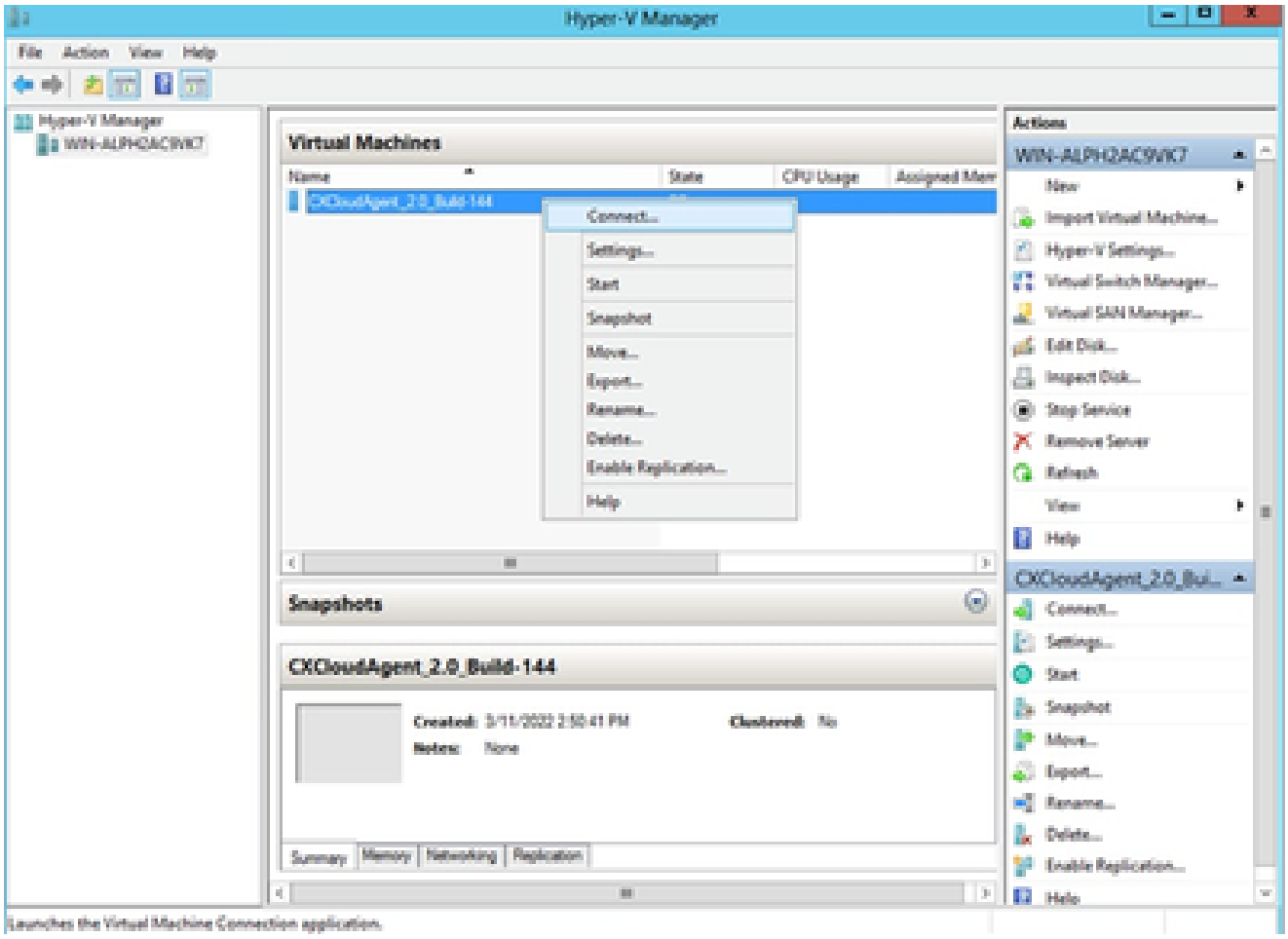
요약

10. 모든 입력을 확인하고 Finish(마침)를 클릭합니다.
11. 가져오기가 성공적으로 완료되면 Hyper-V에 새 VM이 생성됩니다. VM 설정을 엽니다.



가상 스위치

12. 왼쪽 패널에서 Network Adaptor(네트워크 어댑터)를 선택하고 드롭다운 목록에서 사용 가능한 Virtual Switch(가상 스위치)를 선택합니다.

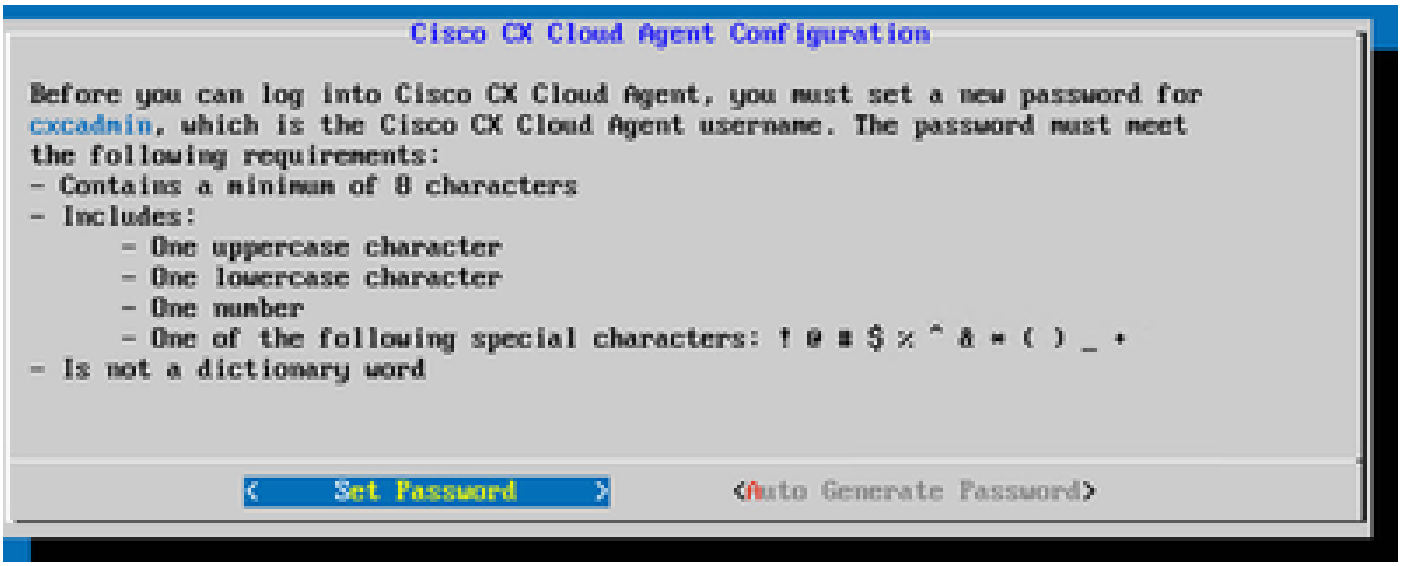


VM 시작

13. Connect(연결)를 선택하여 VM을 시작합니다.
14. 다음 단계를 진행하려면 Network Configuration(네트워크 컨피그레이션)으로 이동합니다.

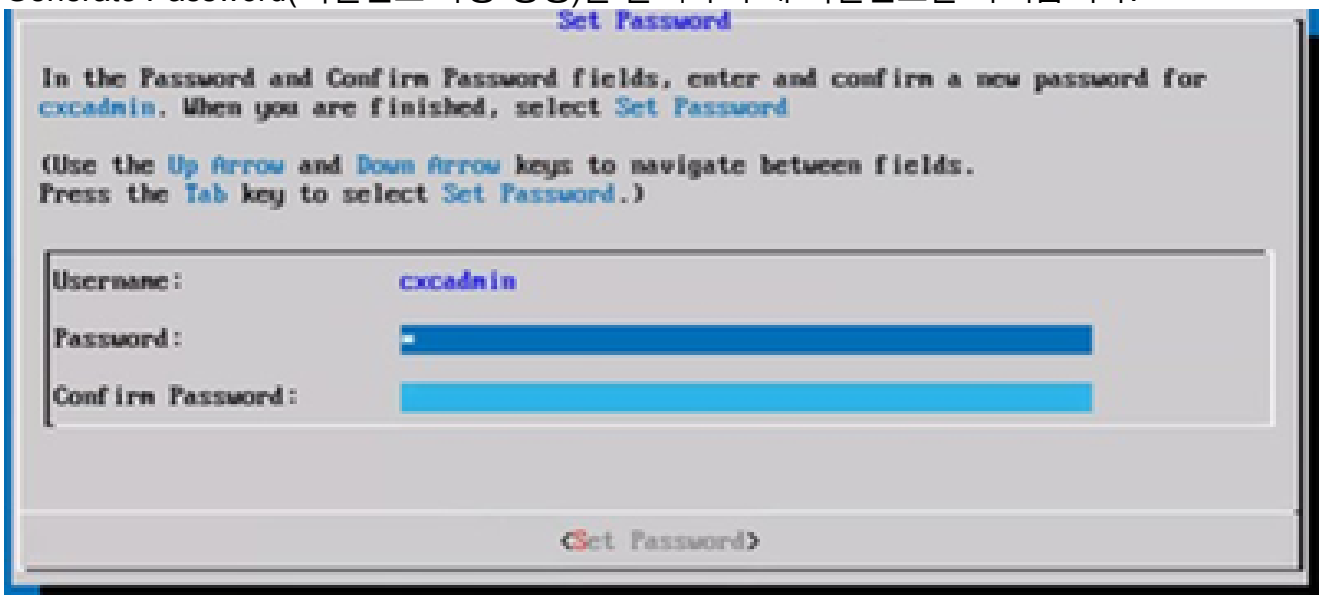
네트워크 설정

cxcadmin 사용자 이름에 대한 CX 클라우드 에이전트 비밀번호를 설정하려면



비밀번호 설정

1. Set Password(비밀번호 설정)를 클릭하여 cxcadmin에 대한 새 비밀번호를 추가하거나 Auto Generate Password(비밀번호 자동 생성)를 클릭하여 새 비밀번호를 가져옵니다.



새 비밀번호

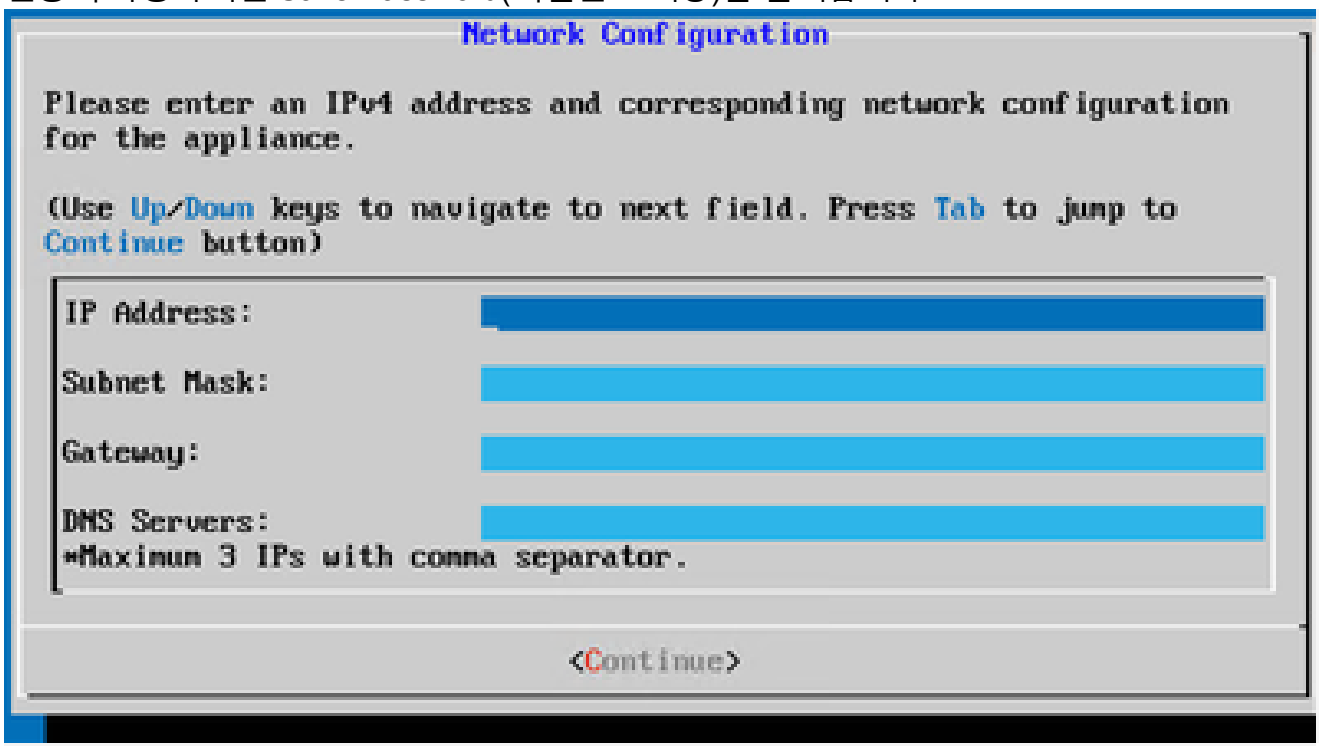
2. Set Password(비밀번호 설정)를 선택한 경우 cxcadmin의 비밀번호를 입력하고 확인합니다. Set Password(비밀번호 설정)를 클릭하고 3단계로 이동합니다.
또는

Auto Generate Password(비밀번호 자동 생성)를 선택한 경우 생성된 비밀번호를 복사하여 나중에 사용할 수 있도록 저장합니다. Save Password(비밀번호 저장)를 클릭하고 4단계로 이동합니다.

자동 생성 비밀번호

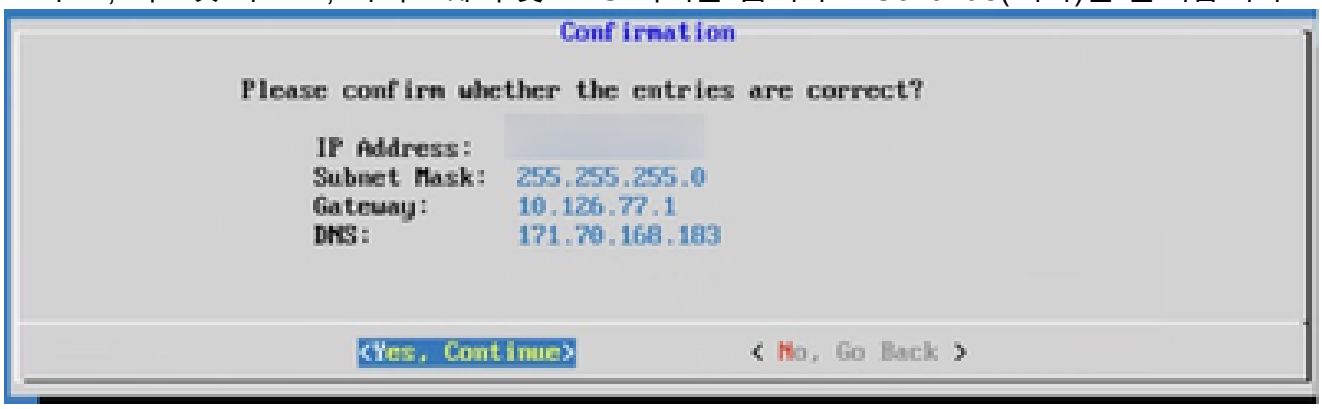
비밀번호 저장

3. 인증에 사용하려면 Save Password(비밀번호 저장)를 클릭합니다.



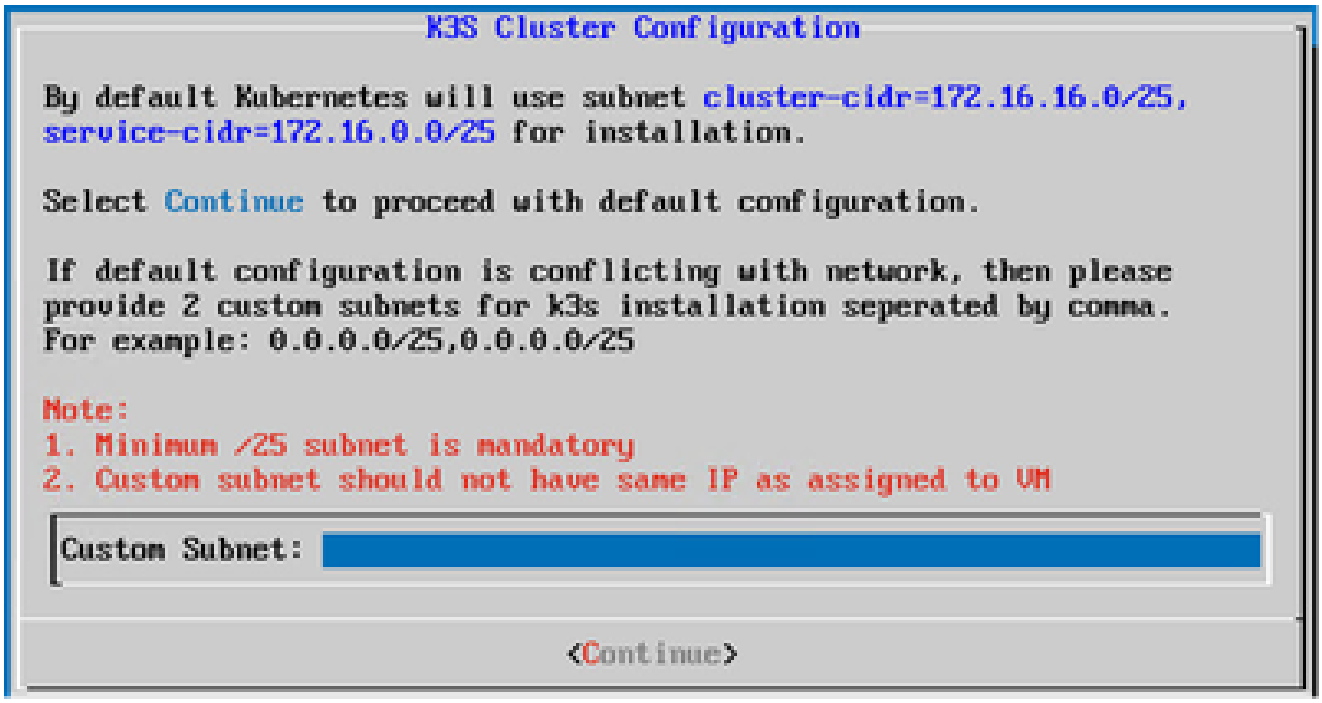
네트워크 설정

4. IP 주소, 서브넷 마스크, 게이트웨이 및 DNS 서버를 입력하고 Continue(계속)를 클릭합니다.



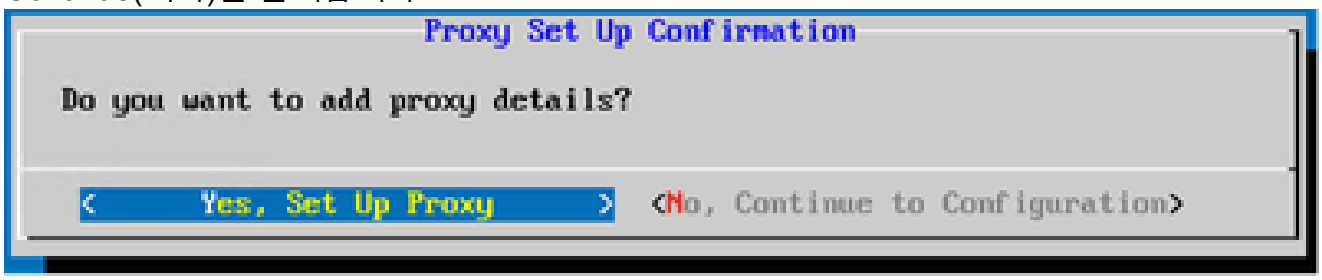
확인

5. 항목을 확인하고 Yes, Continue(예, 계속합니다)를 클릭합니다.



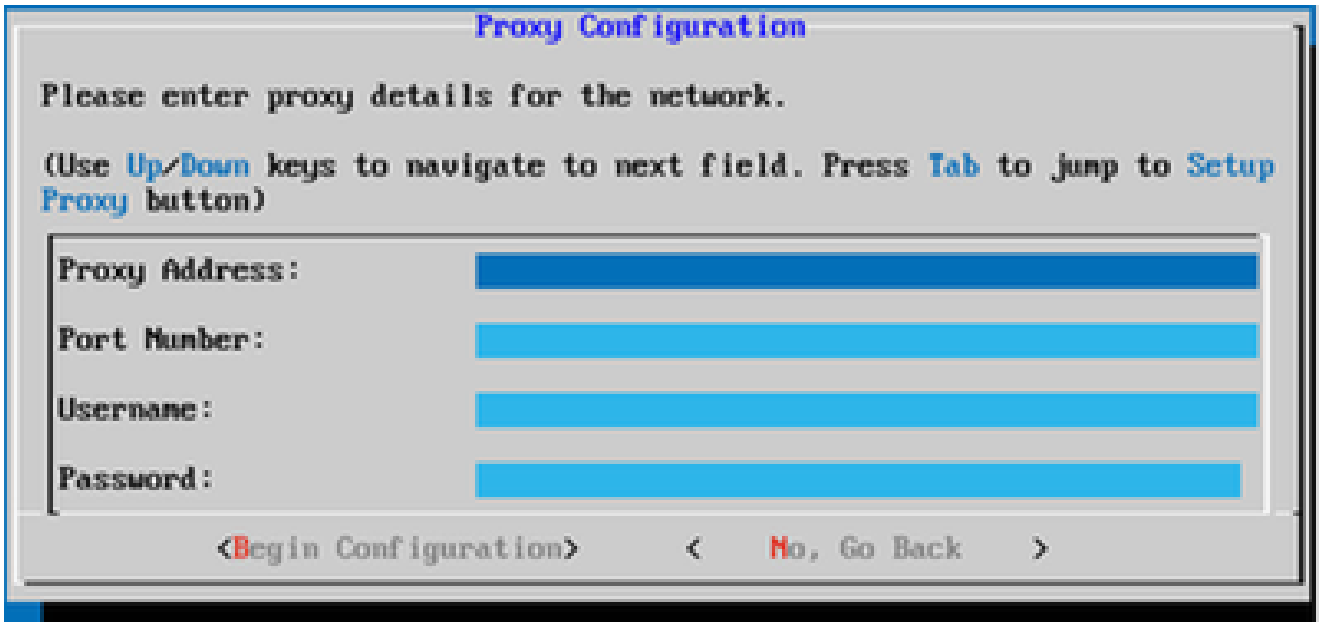
사용자 지정 서브넷

6. K3S 클러스터 컨피그레이션에 대한 사용자 지정 서브넷 IP를 입력합니다(고객의 기본 서브넷이 해당 디바이스 네트워크와 충돌할 경우 다른 사용자 지정 서브넷을 선택합니다).
7. Continue(계속)를 클릭합니다.



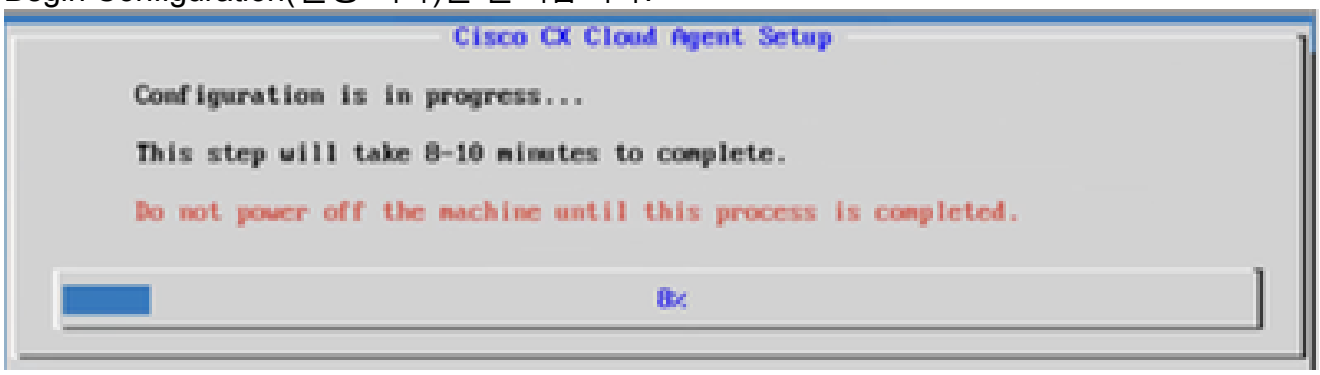
프록시 설정

8. Yes, Set Up Proxy(예, 프록시 설정)를 클릭하여 프록시 세부 정보를 설정하거나 No, Continue to Configuration(아니요, 컨피그레이션 계속)을 클릭하여 11단계로 직접 진행합니다.

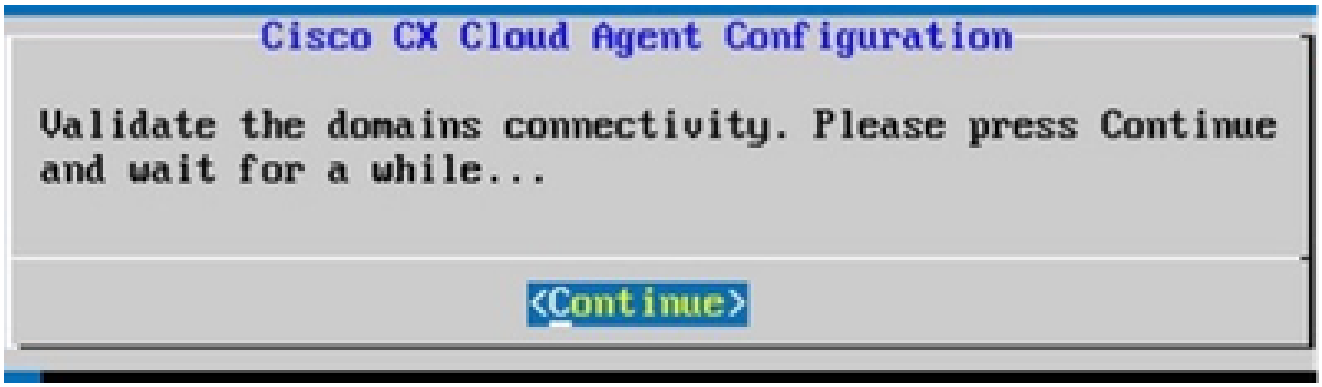


프록시 구성

9. 프록시 주소, 포트 번호, 사용자 이름 및 비밀번호를 입력합니다.
10. Begin Configuration(설정 시작)을 클릭합니다.

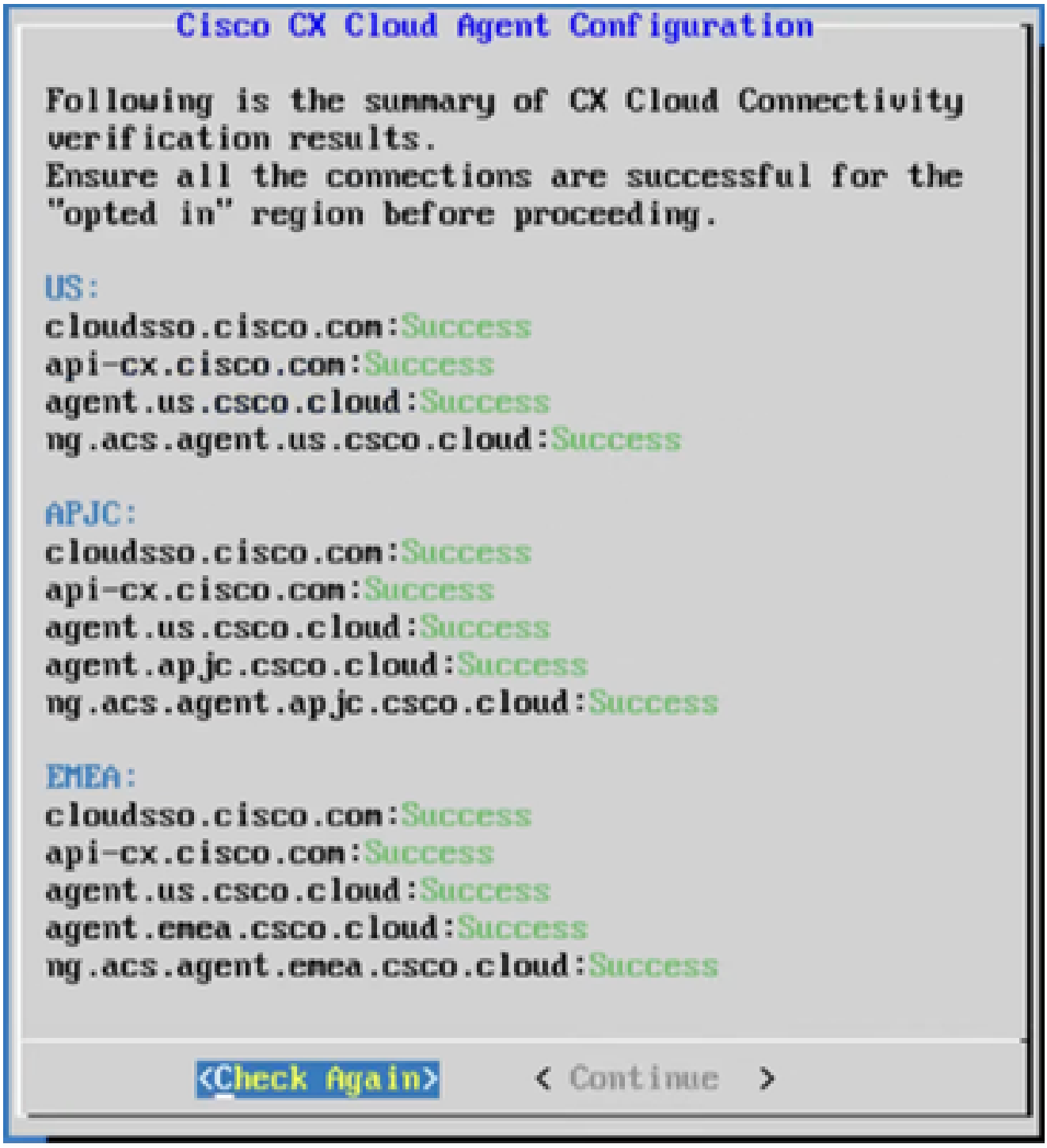


CX 클라우드 에이전트 설정



CX 클라우드 에이전트 컨피그레이션

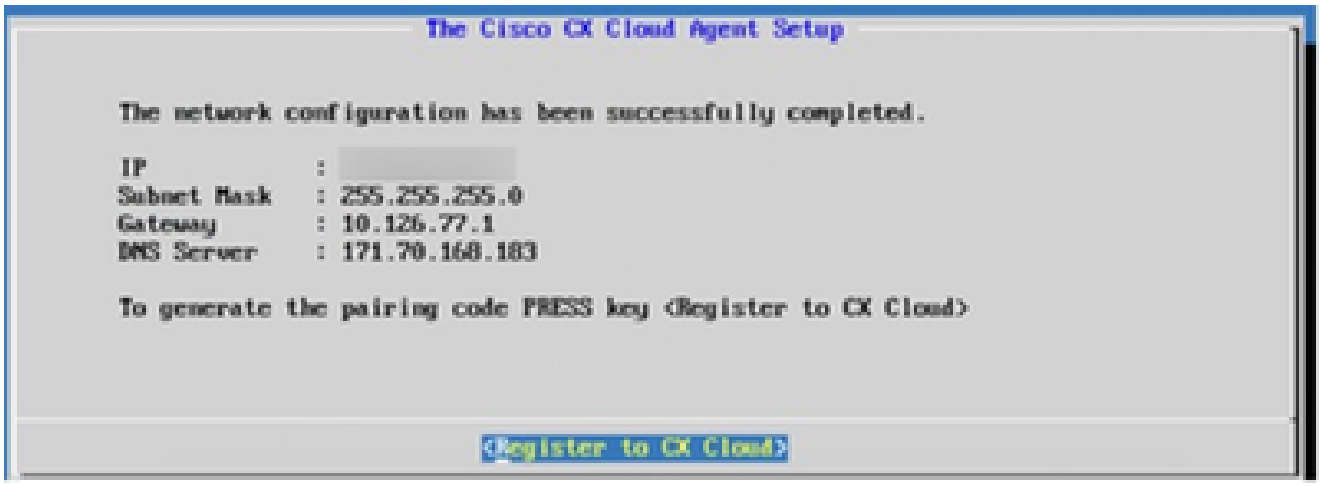
11. Continue(계속)를 클릭합니다.



컨피그레이션 계속

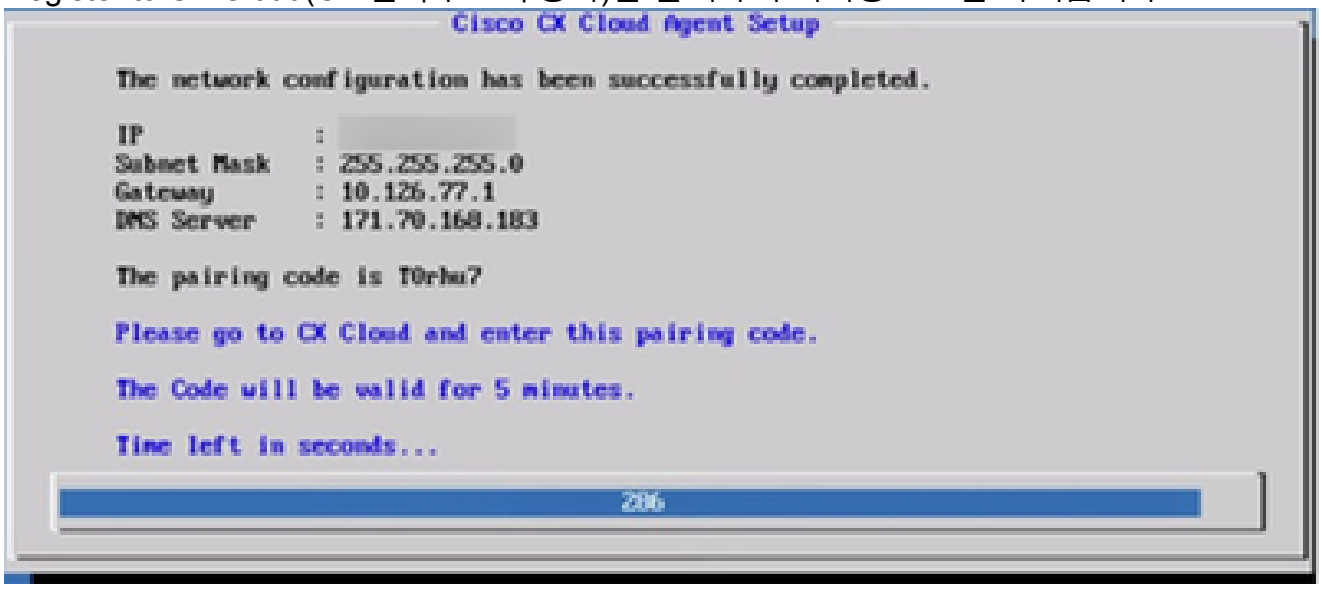
12. Continue(계속)를 클릭하여 성공적인 도메인 도달 구성을 진행합니다. 컨피그레이션을 완료하는 데 몇 분 정도 걸릴 수 있습니다.

참고: 도메인에 연결할 수 없는 경우, 고객은 방화벽을 변경하여 도메인에 연결할 수 있도록 함으로써 도메인 연결 문제를 해결해야 합니다. 도메인 연결 문제가 해결되면 Check Again(다시 확인)을 클릭합니다.



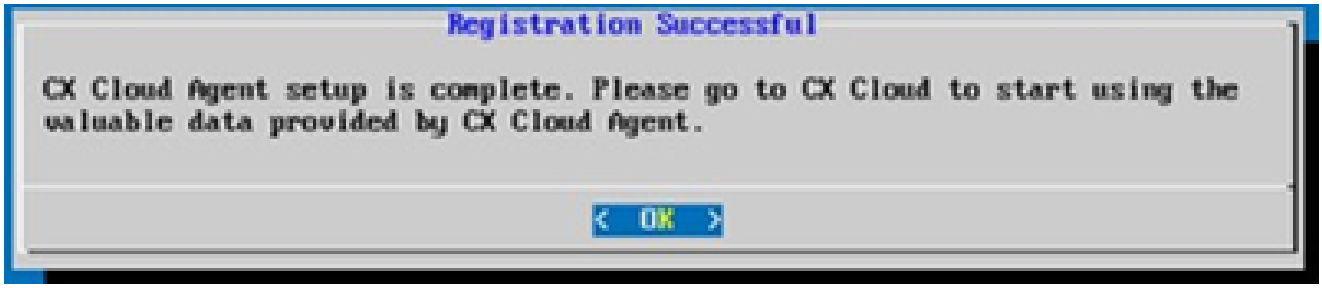
CX Cloud에 등록

13. Register to CX Cloud(CX 클라우드에 등록)를 클릭하여 페어링 코드를 가져옵니다.



페어링 코드

14. 페어링 코드를 복사하고 CX Cloud로 돌아가 설정을 계속합니다.



등록 성공

참고: 페어링 코드가 만료되면 Register to CX Cloud(CX Cloud에 등록)를 클릭하여 새 페어링 코드를 생성합니다(13단계).

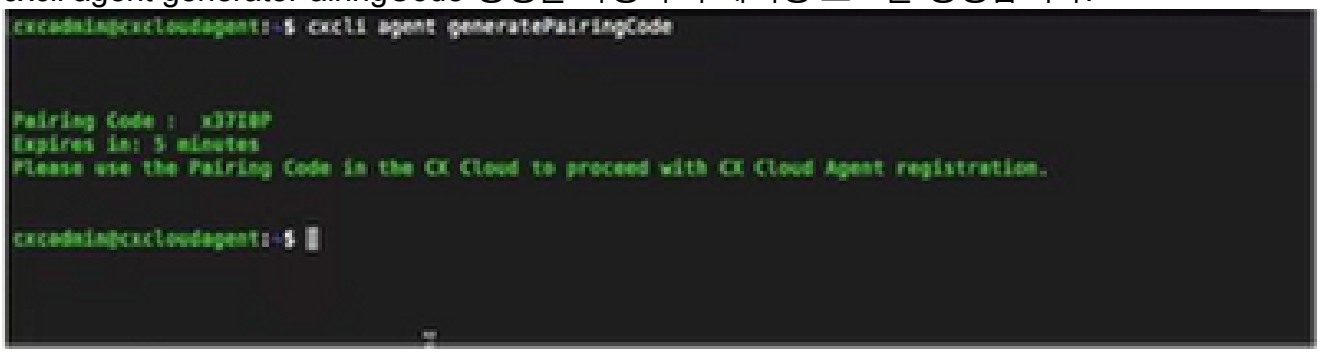
15. 확인을 클릭합니다.

CLI를 사용하여 페어링 코드를 생성하기 위한 대안적인 접근법

사용자는 CLI 옵션을 사용하여 페어링 코드를 생성할 수도 있습니다.

CLI를 사용하여 페어링 코드를 생성하려면

1. cxcadmin 사용자 자격 증명을 사용하여 SSH를 통해 클라우드 에이전트에 로그인합니다.
2. cxcli agent generatePairingCode 명령을 사용하여 페어링 코드를 생성합니다.



페어링 코드 CLI 생성

3. 페어링 코드를 복사하고 CX Cloud로 돌아가 설정을 계속합니다.

CX 클라우드 에이전트에 Syslog를 전달하도록 디바이스 구성

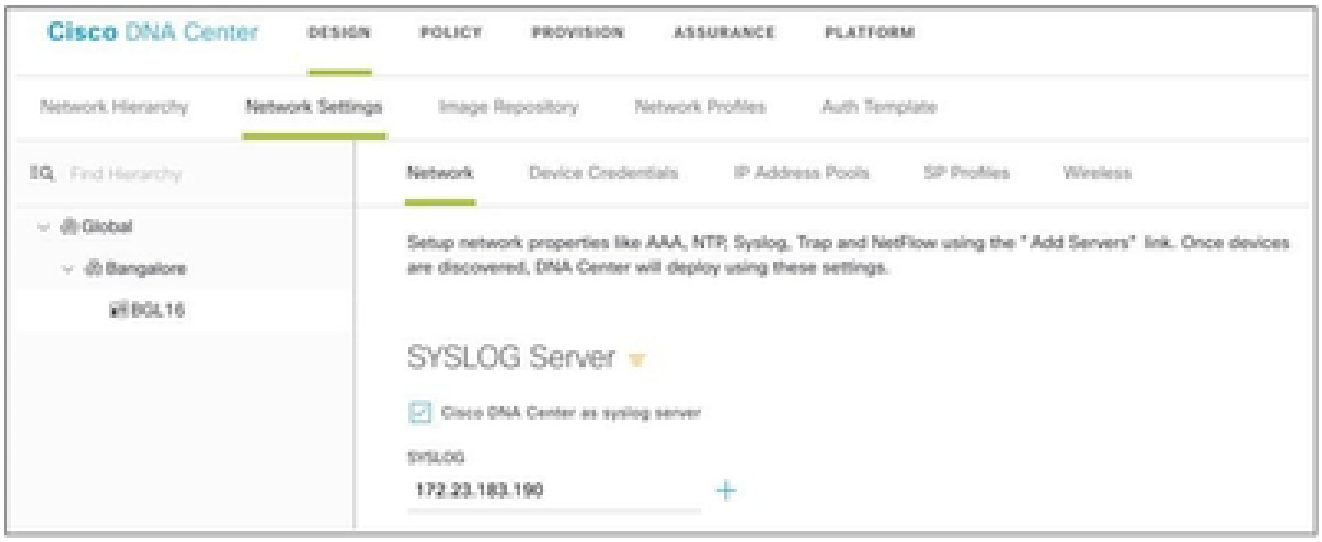
사전 요구 사항

지원되는 Cisco Catalyst Center 버전은 2.1.2.0~2.2.3.5, 2.3.3.4~2.3.3.6, 2.3.5.0, Cisco Catalyst Center Virtual Appliance입니다

Syslog 전달 설정 구성

Cisco Catalyst Center에서 CX Agent에 대한 Syslog 전달을 구성하려면 다음 단계를 수행합니다.

1. Cisco Catalyst Center를 시작합니다.
2. Design(설계)> Network Settings(네트워크 설정) > Network(네트워크)로 이동합니다.
3. 각 사이트에 대해 CX 에이전트 IP를 Syslog 서버로 추가합니다.



Syslog 서버

참고: 구성이 완료되면 해당 사이트와 연결된 모든 디바이스는 CX Agent에 대해 심각도가 높은 syslog를 전송하도록 구성됩니다. 디바이스에서 CX Cloud Agent로 syslog 전달을 활성화하려면 디바이스를 사이트에 연결해야 합니다. syslog 서버 설정이 업데이트되면 해당 사이트와 연결된 모든 디바이스가 자동으로 기본 위험 레벨로 설정됩니다.

Syslog를 CX 에이전트로 전달하도록 기타 자산(직접 디바이스 수집) 구성

CX 클라우드의 장애 관리 기능을 사용하려면 CX 에이전트에 Syslog 메시지를 전송하도록 디바이스를 구성해야 합니다.

참고: CX Agent는 Campus Success Track Level 2 자산의 syslog 정보만 CX 클라우드에 보고합니다. 다른 자산은 syslog가 CX Agent로 구성되어 CX 클라우드에 보고된 syslog 데이터가 없는 것이 방지됩니다.

전달 기능이 있는 기존 Syslog 서버

syslog 서버 소프트웨어에 대한 컨피그레이션 지침을 수행하고 CX 에이전트 IP 주소를 새 대상으로 추가합니다.

참고: syslog를 전달할 때 원래 syslog 메시지의 소스 IP 주소가 유지되는지 확인합니다.

전달 기능이 없거나 Syslog 서버가 없는 기존 Syslog 서버

CX 에이전트 IP 주소로 syslog를 직접 전송하도록 각 디바이스를 구성합니다. 특정 컨피그레이션 단계는 이 설명서를 참조하십시오.

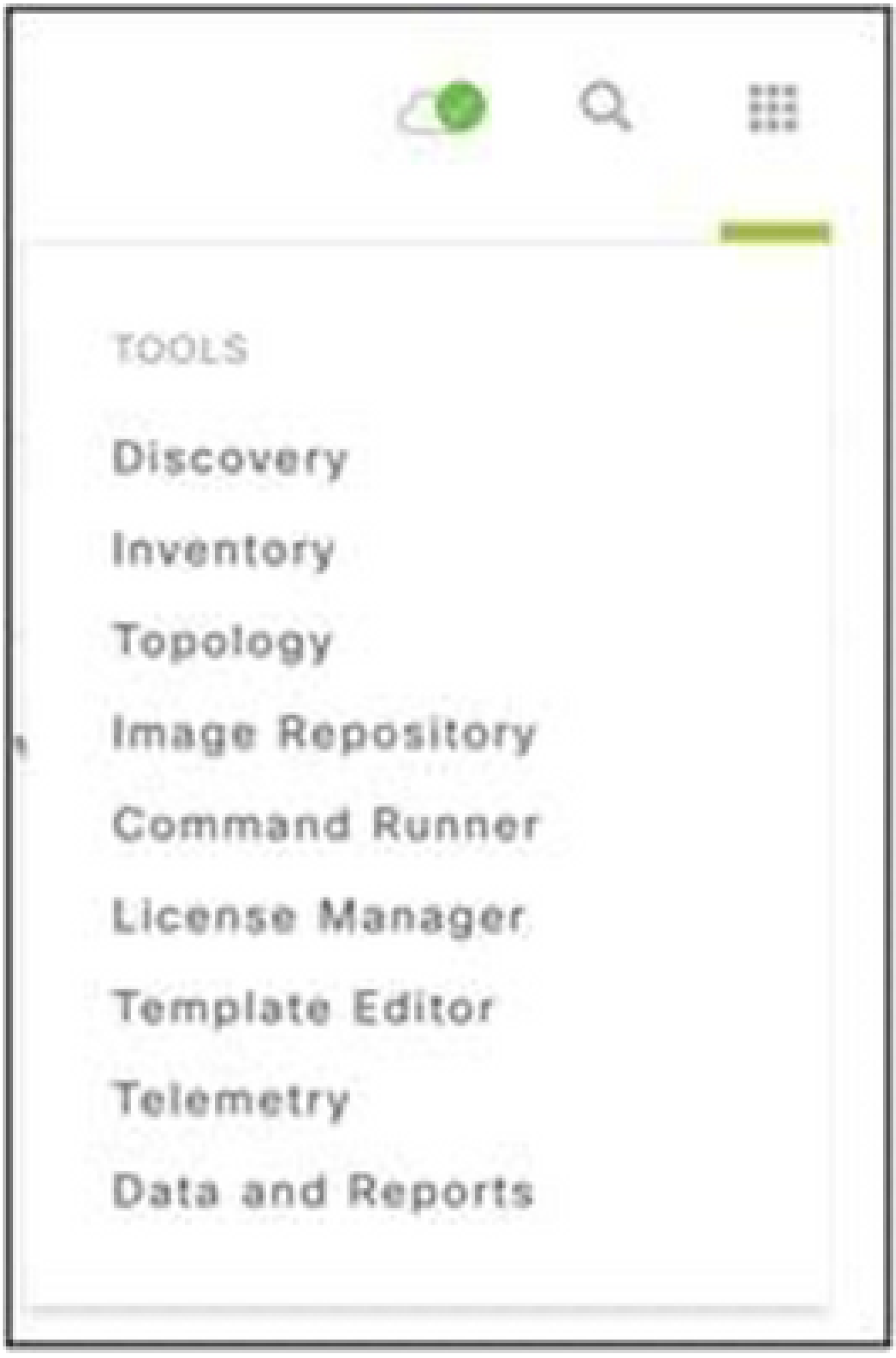
Cisco IOS® XE 컨피그레이션 가이드

AireOS Wireless Controller 컨피그레이션 가이드

Cisco Catalyst Center에 대한 정보 레벨 Syslog 설정 활성화

Syslog 정보 레벨을 표시하려면 다음 단계를 수행합니다.

1. Tools>Telemetry로 이동합니다.


TOOLS
Discovery
Inventory
Topology
Image Repository
Command Runner
License Manager
Template Editor
Telemetry
Data and Reports

도구 메뉴

2. 사이트 뷰를 선택 및 확장하고 사이트 계층에서 사이트를 선택합니다.

사이트 보기

3. 필수 사이트를 선택하고 Device name(디바이스 이름) 확인란을 사용하여 모든 디바이스를 선택합니다.

4. Actions(작업) 드롭다운에서 Optimal Visibility(최적 가시성)를 선택합니다.

작업

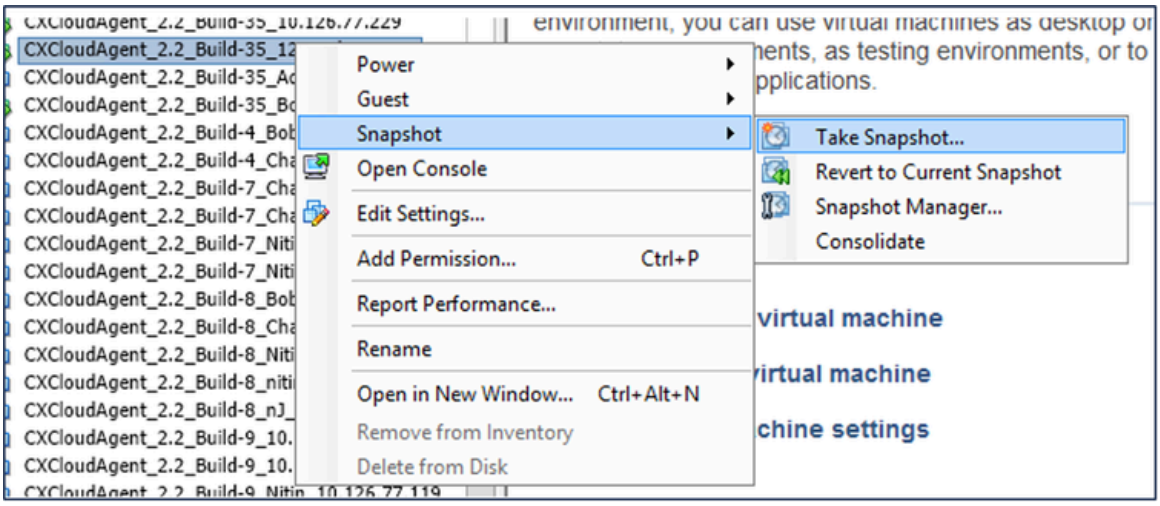
CX 클라우드 VM 백업 및 복원

스냅샷 기능을 사용하여 특정 시점에 CX 에이전트 VM의 상태와 데이터를 보존하는 것이 좋습니다. 이 기능은 스냅샷이 생성된 특정 시간까지 CX 클라우드 VM을 쉽게 복원할 수 있도록 합니다.

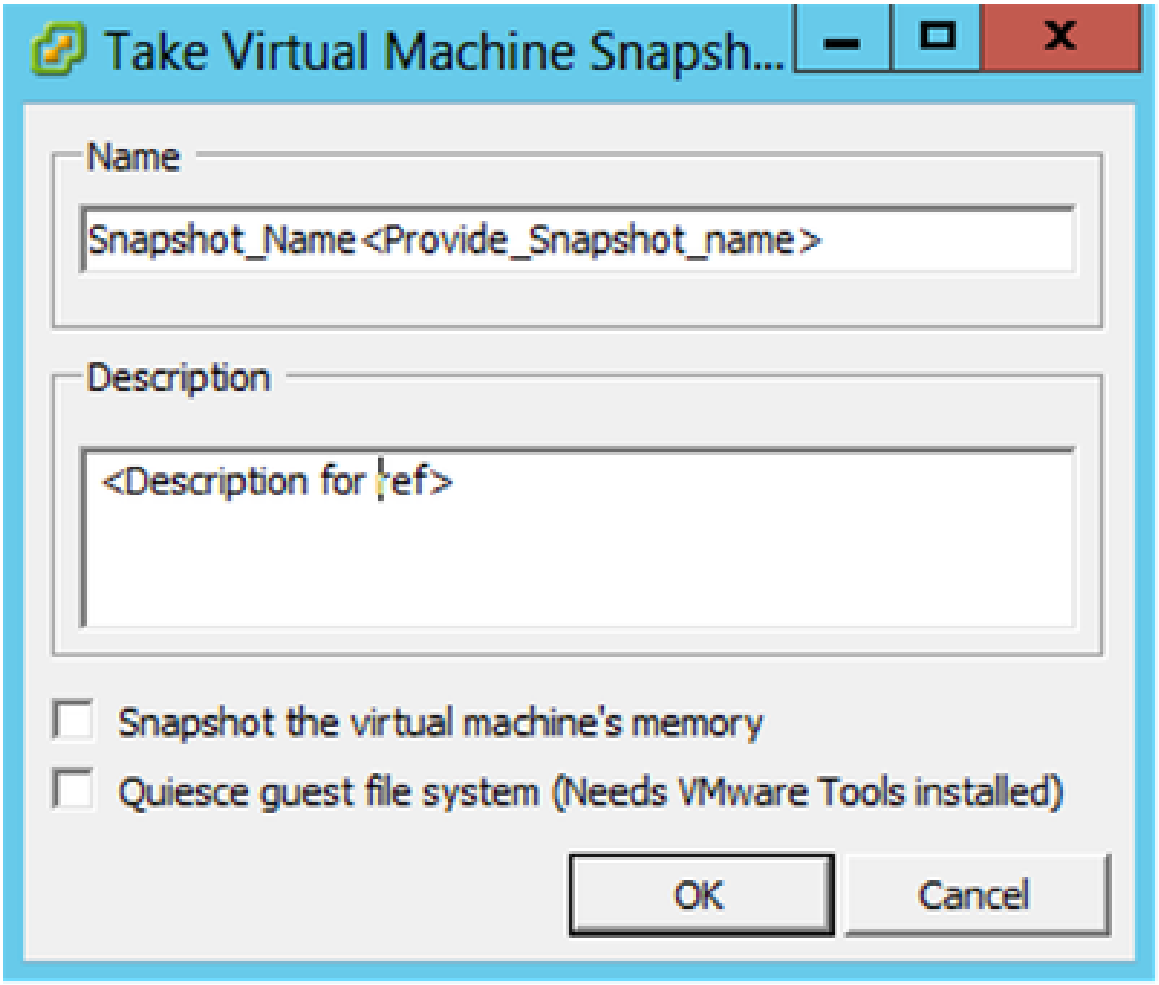
CX 클라우드 VM 백업

CX 클라우드 VM을 백업하려면

1. VM을 마우스 오른쪽 버튼으로 클릭하고 Snapshot(스냅샷) > Take Snapshot(스냅샷 생성)을 선택합니다. Take Virtual Machine Snapshot(가상 머신 스냅샷 가져오기) 창이 열립니다.



VM 선택

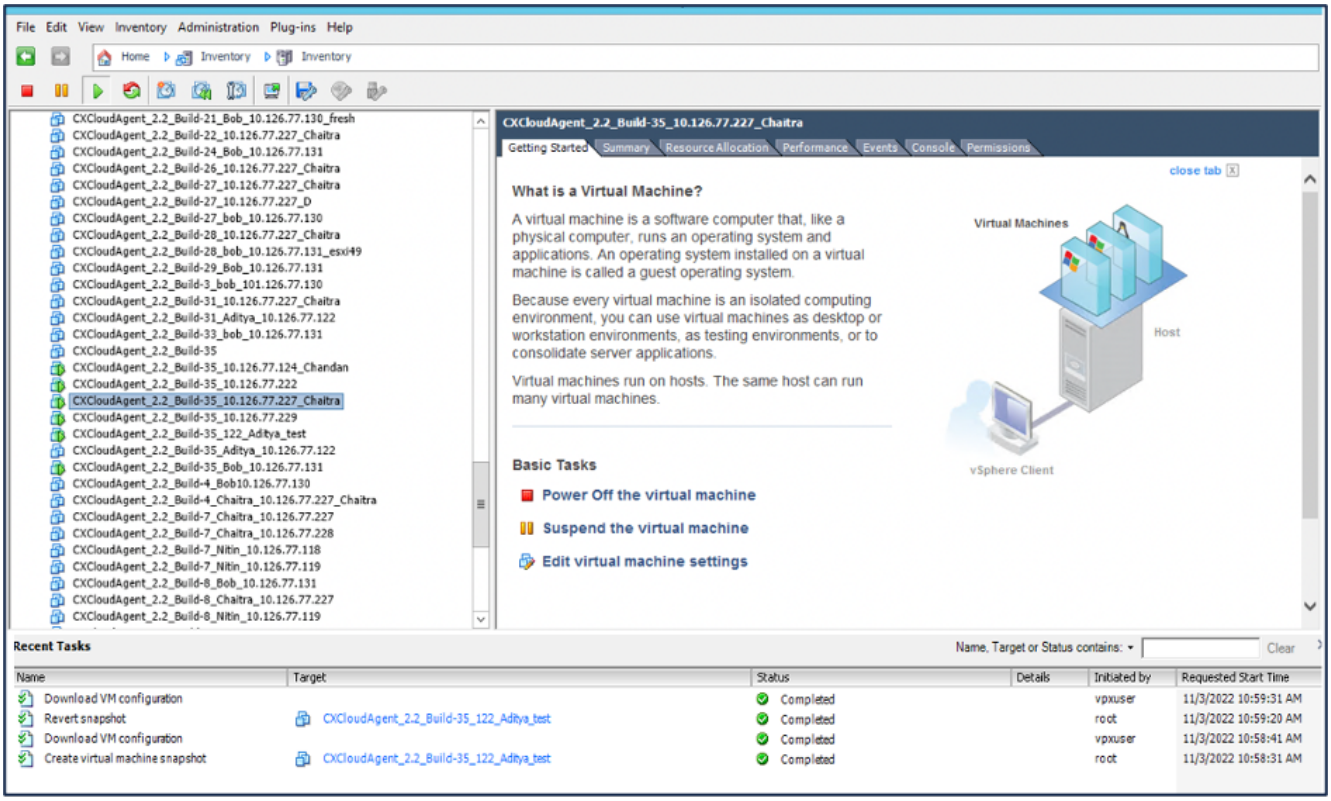


가상 컴퓨터 스냅숏 만들기

2. 이름과 설명을 입력합니다.

참고: Snapshot the virtual machine's memory(가상 머신의 메모리 스냅샷) 확인란의 선택이 취소되었는지 확인합니다.

3. 확인을 클릭합니다. Create virtual machine snapshot(가상 머신 스냅샷 생성) 상태가 Recent Tasks(최근 작업) 목록에 Completed(완료됨)로 표시됩니다.

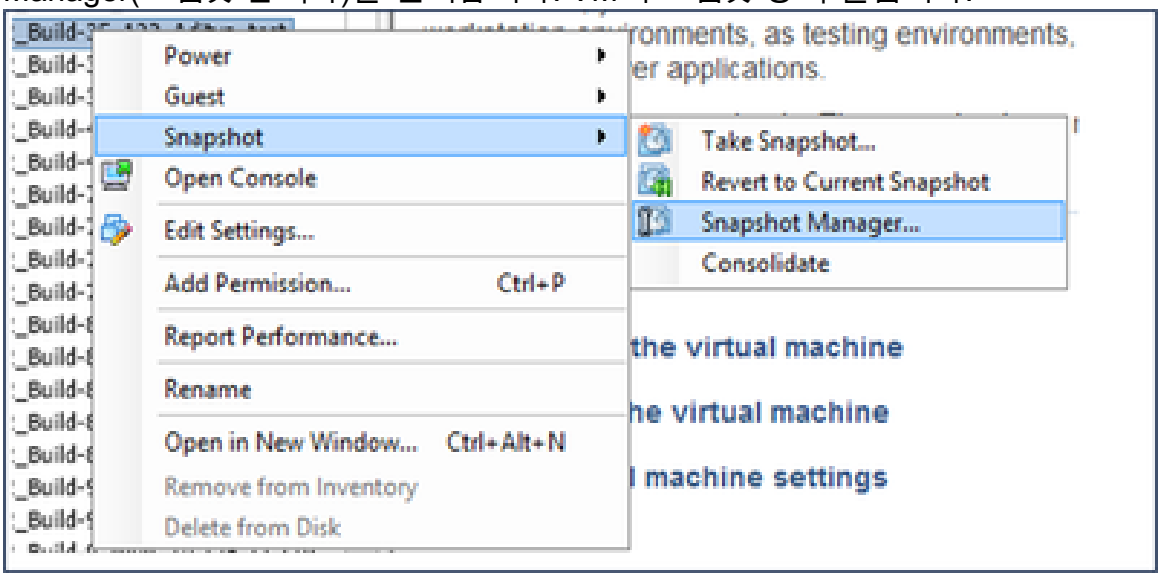


최근 작업

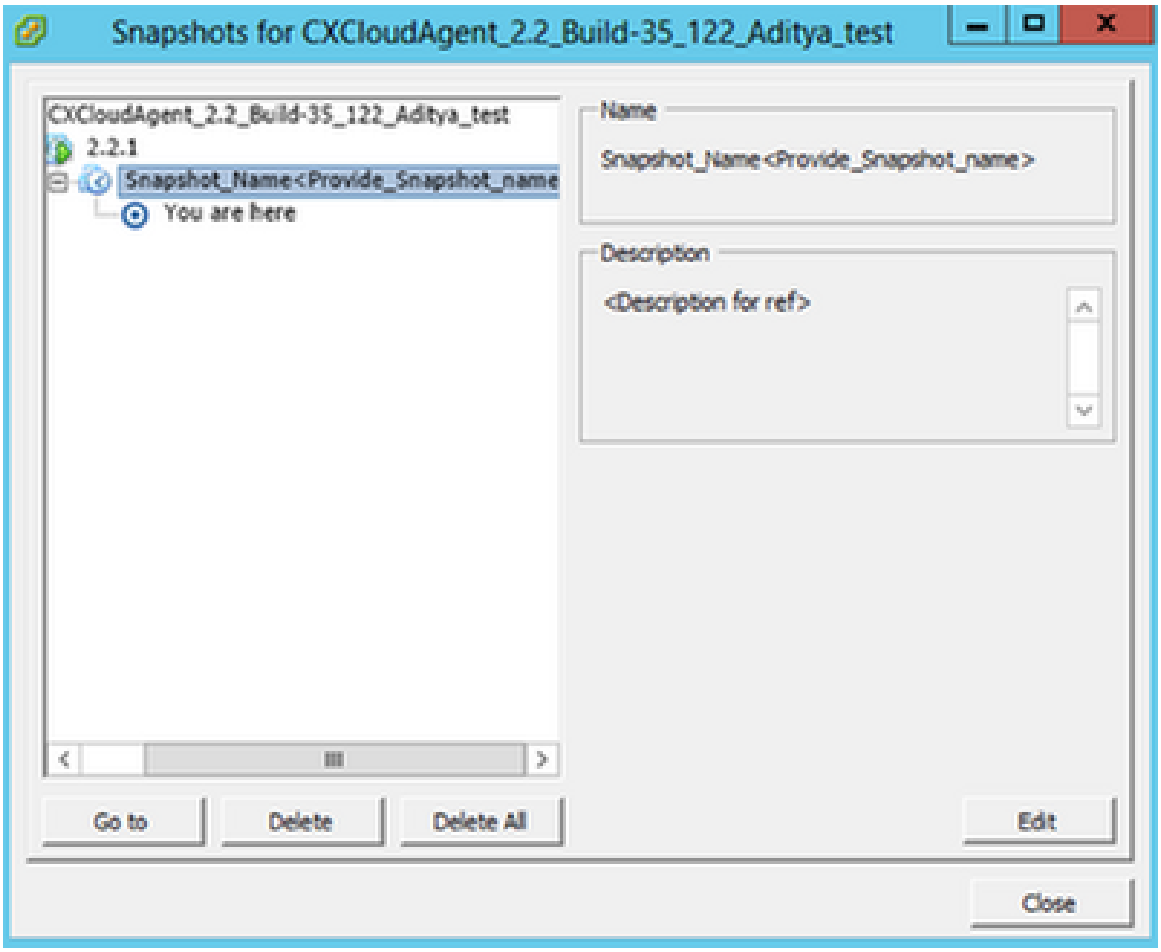
CX 클라우드 VM 복원

CX 클라우드 VM을 복원하려면

1. VM을 마우스 오른쪽 버튼으로 클릭하고 Snapshot(스냅샷) > Snapshot Manager(스냅샷 관리자)를 선택합니다. VM의 스냅샷 창이 열립니다.

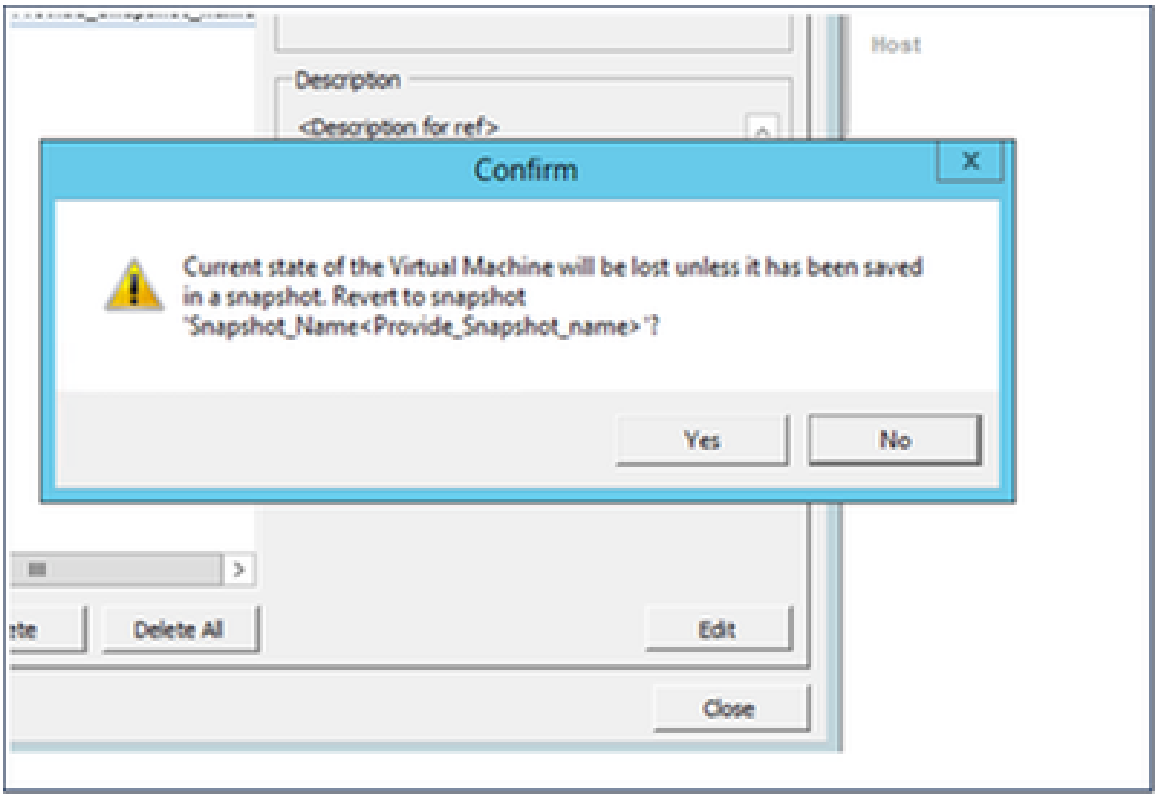


VM 선택 창



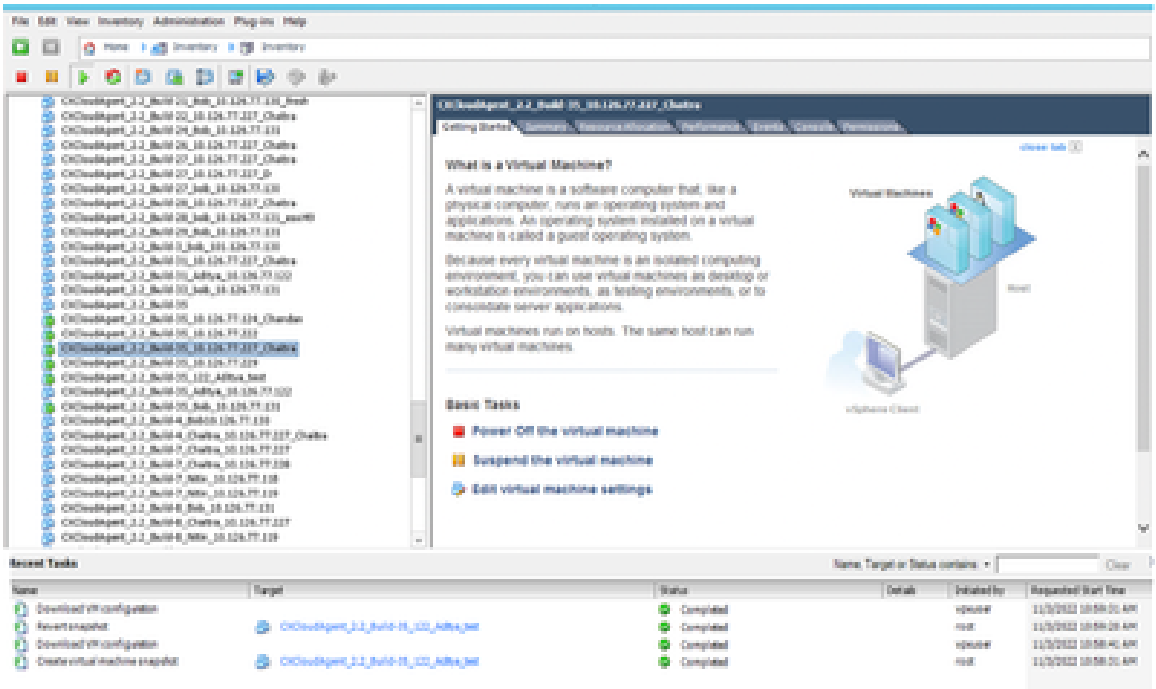
스냅샷 창

2. 이동을 클릭합니다. 확인 창이 열립니다.



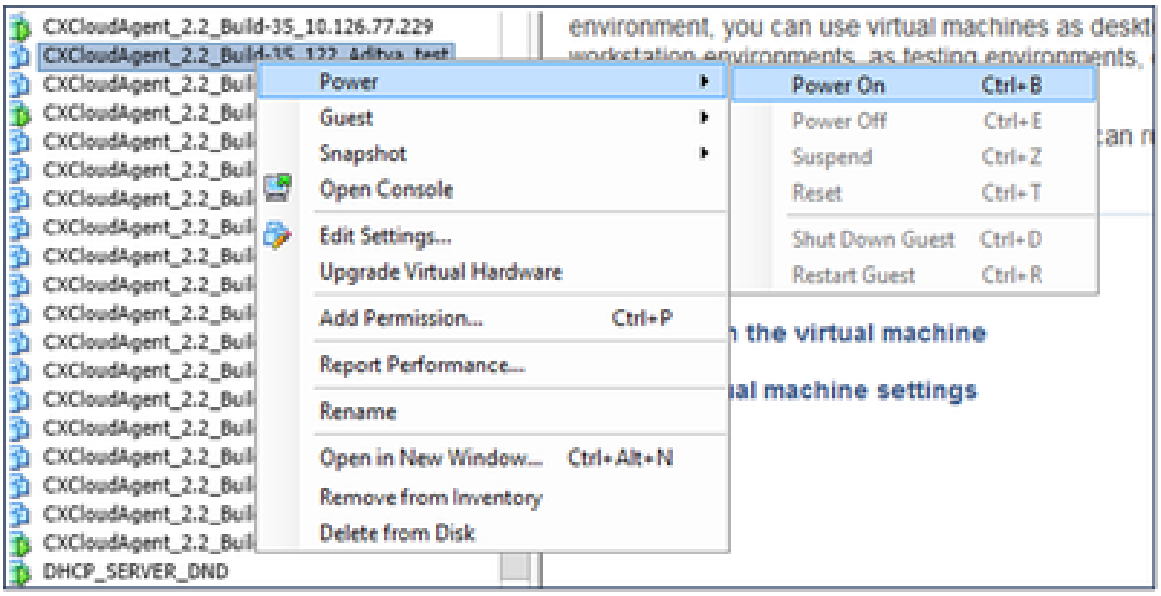
창 확인

3. Yes(예)를 클릭합니다. 스냅샷 되돌리기 상태가 최근 작업 목록에 완료됨으로 표시됩니다.



최근 작업

4. VM을 마우스 오른쪽 버튼으로 클릭하고 Power(전원) > Power On(전원 켜기)을 선택하여 VM의 전원을 켭니다.



보안

CX Agent 는 고객에게 완벽한 보안을 보장합니다. CX Cloud와 CX Agent 간의 연결은 TLS로 보호됩니다. Cloud Agent의 기본 SSH 사용자는 기본 작업만 수행하도록 제한됩니다.

물리적 보안

보안 VMware 서버 회사에 CX 에이전트 OVA 이미지를 구축합니다. OVA는 Cisco Software Download Center를 통해 안전하게 공유됩니다. 부트 로더(단일 사용자 모드) 비밀번호는 무작위로 고유한 비밀번호로 설정됩니다. 이 부트로더(단일 사용자 모드) 비밀번호를 설정하려면 이 FAQ를 참조해야 합니다.

계정 보안

구축 과정에서 cxcadmin 사용자 계정이 생성됩니다. 사용자는 초기 컨피그레이션 중에 비밀번호를 설정해야 합니다. cxcadmin 사용자/자격 증명은 CX 에이전트 API에 액세스하고 SSH를 통해 어플라이언스에 연결하는 데 사용됩니다.

cxcadmin 사용자는 최소 권한으로 액세스를 제한합니다. cxcadmin 비밀번호는 보안 정책을 따르며 만료 기간이 90일인 단방향 해시됩니다. cxcadmin 사용자는 remoteaccount라는 유틸리티를 사용하여 cxcroot 사용자를 생성할 수 있습니다. cxcroot 사용자는 루트 권한을 얻을 수 있습니다.

네트워크 보안

CX 에이전트 VM은 cxcadmin 사용자 자격 증명과 함께 SSH를 사용하여 액세스할 수 있습니다. 수신 포트는 22(ssh), 514(Syslog)로 제한됩니다.

인증

비밀번호 기반 인증: 어플라이언스는 단일 사용자(cxcadmin)를 유지 관리하므로 사용자가 CX 에이전트를 인증하고 CX 에이전트와 통신할 수 있습니다.

- ssh를 사용하는 어플라이언스에 대한 루트 권한 작업.

cxcadmin 사용자는 remoteaccount라는 유틸리티를 사용하여 cxcroot 사용자를 생성할 수 있습니다. 이 유틸리티는 SWIM 포털(DECRYPT Request Form)에서만 해독할 수 있는 RSA/ECB/PKCS1v1_5 암호화된 비밀번호를 표시합니다. 승인된 담당자만이 포털에 액세스할 수 있습니다. cxcroot 사용자는 이 암호 해독된 암호를 사용하여 루트 권한을 얻을 수 있습니다. 암호는 2일 동안만 유효합니다. cxcadmin 사용자는 계정을 다시 생성하고 SWIM 포털 게시물 비밀번호 만료에서 비밀번호를 가져와야 합니다.

강화

CX Agent 어플라이언스는 Center of Internet Security 강화 표준을 따릅니다.

데이터 보안

CX Agent Appliance는 고객 개인 정보를 저장하지 않습니다. 디바이스 자격 증명 애플리케이션(포드 중 하나로 실행)은 암호화된 서버 자격 증명을 보안 데이터베이스 내에 저장합니다. 수집된 데이터는 어플라이언스 내에서 처리되는 경우를 제외하고 어떤 형태로도 저장되지 않습니다. 텔레메트리 데이터는 수집이 완료된 후 가능한 한 빨리 CX 클라우드에 업로드되며 업로드가 성공했음을 확인한 후 로컬 스토리지에서 즉시 삭제됩니다.

데이터 전송

등록 패키지에는 Iot Core와의 보안 연결을 설정하는 데 필요한 고유한 X.509 디바이스 인증서 및 키가 포함되어 있습니다. 이 에이전트를 사용하면 MQTT(Message Queuing Telemetry Transport) over TLS(Transport Layer Security) v1.2를 사용하여 보안 연결이 설정됩니다

기록 및 모니터링

로그에는 PII(개인 식별 정보) 데이터 형식이 포함되어 있지 않습니다. 감사 로그는 CX Cloud Agent Appliance에서 수행되는 모든 보안 관련 작업을 캡처합니다.

Cisco Telemetry 명령

CX Cloud는 Cisco Telemetry 명령에 나열된 API 및 명령을 사용하여 자산 텔레메트리를 검색합니다. 이 문서에서는 Cisco Catalyst Center 인벤토리, 진단 브리지, Intersight, 컴플라이언스 인사이트, 결함 및 CX Agent에서 수집한 기타 모든 텔레메트리 소스에 대한 적용 가능성에 따라 명령을 분류합니다.

자산 텔레메트리 내의 민감한 정보는 클라우드로 전송되기 전에 마스킹됩니다. CX Agent는 CX Agent에 직접 텔레메트리를 전송하는 수집된 모든 자산에 대해 민감한 데이터를 마스킹합니다. 여기에는 비밀번호, 키, 커뮤니티 문자열, 사용자 이름 등이 포함됩니다. 컨트롤러는 이 정보를 CX Agent에 전송하기 전에 모든 컨트롤러 관리 자산에 대한 데이터 마스킹을 제공합니다. 경우에 따라 컨트롤러 관리 자산 텔레메트리를 더 익명화할 수 있습니다. 텔레메트리 익명화에 대한 자세한 내용은 해당 제품 지원 문서를 참조하십시오(예: Cisco Catalyst Center Administrator Guide의 Anonymize Data 섹션).

텔레메트리 명령 목록을 사용자 지정할 수 없고 데이터 마스킹 규칙을 수정할 수 없지만, 고객은 컨트롤러 관리 디바이스에 대한 제품 지원 설명서 또는 이 문서의 Connecting Data Sources 섹션(CX Agent에서 수집한 기타 자산)에 설명된 대로 데이터 소스를 지정하여 어떤 자산의 텔레메트리 CX 클라우드 액세스를 제어할 수 있습니다.

보안 요약

보안 기능	설명
부트 로더 비밀번호	부트 로더(단일 사용자 모드) 비밀번호는 무작위로 고유한 비밀번호로 설정됩니다. 사용자는 FAQ를 참조하여 부트로더(단일 사용자 모드) 비밀번호를 설정해야 합니다.
사용자 액세스	SSH: ·cxcadmin 사용자를 사용하여 어플라이언스에 액세스하려면 설치 중에 생성한 인증서가 필요합니다. · cxcroot 사용자를 사용하여 어플라이언스에 액세스하려면 공인 담당자가 SWIM 포털을 사용하여 자격 증명을 해독해야 합니다.
사용자 계정	·cxcadmin: 기본 사용자 계정이 생성됨; 사용자는 cxcli를 사용하여 CX Agent 애플리케이션 명령을 실행할 수 있으며 어플라이언스에 대한 권한이 가장 적습니다. cxcroot 사용자 및 해당 암호화된 비밀번호는 cxcadmin 사용자를 사용하여 생성됩니다. ·cxcroot: cxcadmin은 유틸리티 remoteaccount를 사용하여 이 사용자를 생성할 수 있습니다. 사용자는 이 계정으로 루트 권한을 얻을 수 있습니다.
cxcadmin 비밀번호 정책	·비밀번호는 SHA-256을 사용하여 단방향으로 해시되며 안전하게 저장됩니다. · 최소 8자 - 다음 범주 중 3개 포함: 대문자, 소문자, 숫자 및 특수 문자
cxcroot 비밀번호 정책	· cxcroot 암호는 RSA/ECB/PKCS1v1_5 암호화됨 ·생성된 암호는 SWIM 포털에서 해독해야 합니다. · cxcroot 사용자 및 비밀번호는 2일간 유효하며 cxcadmin 사용자를 사용하여 재생성할 수 있습니다.
ssh 로그인 비밀번호 정책	· 다음 범주 중 3개를 포함하는 8자 이상: 대문자, 소문자, 숫자 및 특수 문자 · 5회 로그인 실패 시 30분 동안 차단 비밀번호는 90일 후에 만료됩니다.

포트	수신 포트 열기 – 514(Syslog) 및 22(ssh)
데이터 보안	·저장된 고객 정보가 없습니다. ·저장된 디바이스 데이터가 없습니다. · Cisco Catalyst Center 서버 자격 증명을 암호화하여 데이터베이스에 저장합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.