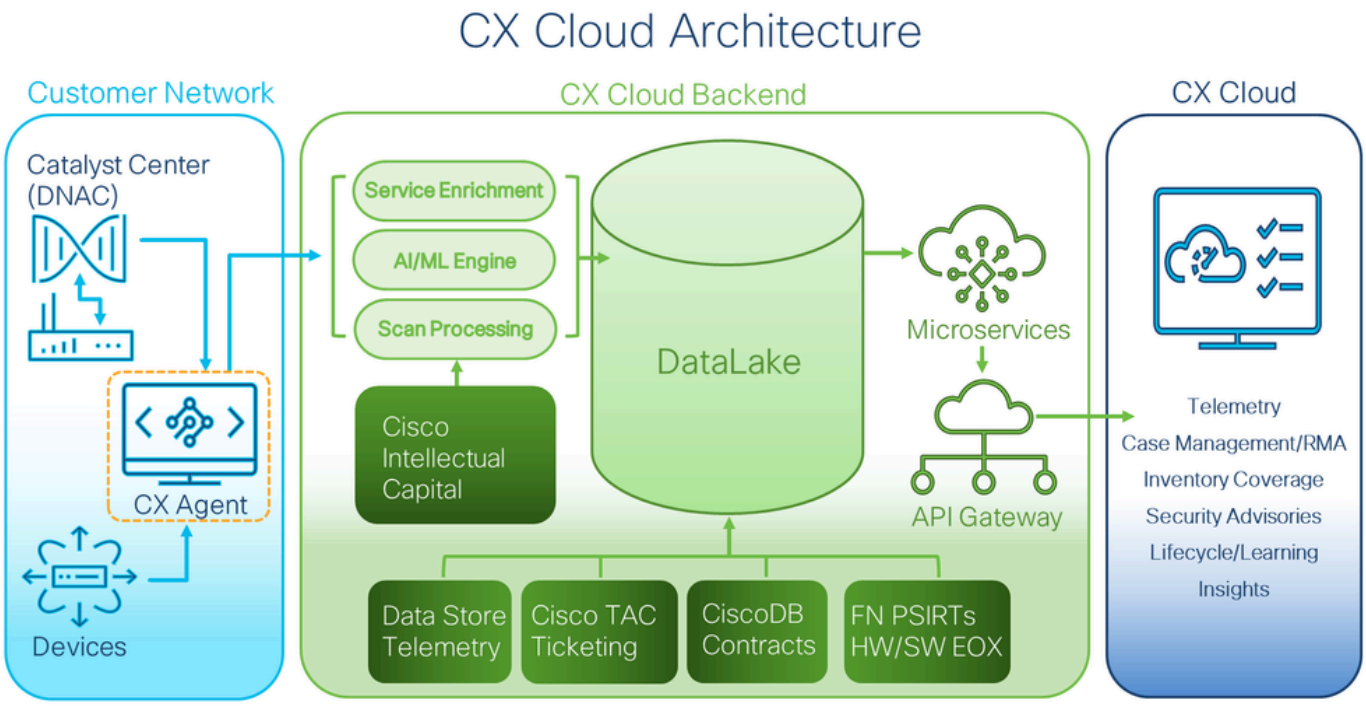
CX Cloud Agent 개요 v2.2

목차

소개

이 문서에서는 Cisco의 CX(Customer Experience) 클라우드 에이전트에 대해 설명합니다. Cisco(CX) Cloud Agent는 확장성이 뛰어난 플랫폼으로, 고객 네트워크 장치로부터 텔레메트리 데이터를 수집하여 고객에게 실행 가능한 통찰력을 제공합니다. CX Cloud Agent를 사용하면 AI(Artificial Intelligence)/ML(Machine Learning)에서 실행 중인 활성 구성 데이터를 CX Cloud에 표시되는 사전 대응적 및 예측 통찰력으로 변환할 수 있습니다.

이 설명서는 CX Cloud Agent v2.2 이상에 적용됩니다. 이전 버전에 액세스하려면 Cisco CX Cloud Agent 페이지를 참조하십시오.



CX 클라우드 아키텍처

참고: 이 가이드의 이미지(및 해당 내용)는 참조용으로만 제공됩니다. 실제 내용은 다를 수 있습니다.

사전 요구 사항

CX Cloud Agent는 가상 시스템(VM)으로 실행되며 OVA(Open Virtual Appliance) 또는 VHD(Virtual Hard Disk)로 다운로드할 수 있습니다.

구축 요건:

- 이러한 하이퍼바이저:
  - VMware ESXi 버전 5.5 이상
  - Oracle Virtual Box 5.2.30 이상
  - Windows 하이퍼바이저 버전 2012 - 2022
- 하이퍼바이저는 다음을 필요로 하는 VM을 호스팅할 수 있습니다.
  - 8코어 CPU
  - 16GB 메모리/RAM
  - 200GB 디스크 공간
- 지정된 미국 데이터 센터를 기본 데이터 영역으로 사용하여 CX 클라우드 데이터를 저장하는 고객의 경우, CX 클라우드 에이전트는 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 클라우드 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
- 지정된 아시아 태평양 데이터 센터를 기본 데이터 영역으로 사용하여 CX 클라우드 데이터를 저장하는 고객의 경우: CX 클라우드 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 영역으로 사용하는 고객의 경우, 초기 설정 과정에서 CX Cloud Agent를 CX Cloud에 등록하기 위해서만 FQDN: agent.us.csco.cloud에 대한 연결이 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.
- 다음 표는 CX Cloud Agent가 올바르게 작동하기 위해 열고 활성화해야 하는 포트 및 프로토콜에 대한 요약을 제공합니다.

					Required for both Cisco DNA Center and Other Assets collected by CX Cloud Agent support	
					Mandatory TCP/7 Echo (ICMP) port must be combined with one of the other two ports (for device discovery process)	
CX Cloud Agent Traffic					Mandatory for other assets collected by CX Cloud Agent support	

Source	Destination		Protocol	Port	Purpose	Type
	IP Address	Hostname				
Data Collection and Transfer						
Agent IP	Dynamic IPs Cisco DNA Center Server IP	For All regions, FQDN: cloudsso.cisco.com FQDN: api-cx.cisco.com QDN: agent.us.csco.cloud DNAC Servers Additionally, For Americas region, FQDN: ng.acs.agent.us.csco.cloud For EMEA region, FQDN: agent.emea.csco.cloud, and FQDN: ng.acs.agent.emea.csco.cloud For APJC region, FQDN: agent.apjc.csco.cloud, and FQDN: ng.acs.agent.apjc.csco.cloud	HTTPS	TCP/ 443	Data collection via DNAC servers, Data transfer to CX Cloud, including upgrade functionality	Outbound connection to DNAC servers + Outbound to Cisco AWS regional data centers
Agent IP	Customer Device		SNMP	UDP/161	Collect OIDs and MIBs for other assets collected by CX Cloud Agent	Outbound to LAN
Devices	Agent IP		SYSLOG	UDP/514	Stream Syslog messages from Device to Agent	Inbound from LAN
Agent IP	Customer Device		SSH	TCP/22	Collect CLI commands	Outbound to LAN
Agent IP	Customer Device		Echo	TCP/7	Check the device reachability	Outbound to LAN
Agent IP	Customer Device		Telnet	TCP/23	Collect CLI commands	Outbound to LAN
Agent Administration Access						
Support VM	Agent IP		SSH	TCP/22	Agent Maintenance	Inbound from LAN

기타 참고 사항:

- VM 환경에서 DHCP(Dynamic Host Configuration Protocol)를 활성화하면 IP가 자동으로 검색됩니다. 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 Cisco DNA Center 버전은 2.1.2.x~2.2.3.x, 2.3.3.x, 2.3.5.x와 Cisco Catalyst Center Virtual Appliance 및 Cisco DNA Center Virtual Appliance입니다
- 네트워크에 SSL 가로채기가 있는 경우 permit-list CX Cloud Agent의 IP 주소
- 직접 연결된 모든 자산의 경우 SSH 권한 레벨 15가 필요합니다
- 제공된 호스트 이름만 사용하십시오. 고정 IP 주소는 사용할 수 없습니다.

중요 도메인 액세스

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

CX 클라우드 에이전트 포털 관련 도메인

주요 도메인	기타 도메인
cisco.com	mixpanel.com
csco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com

	tiqcdn.com
	jquery.com

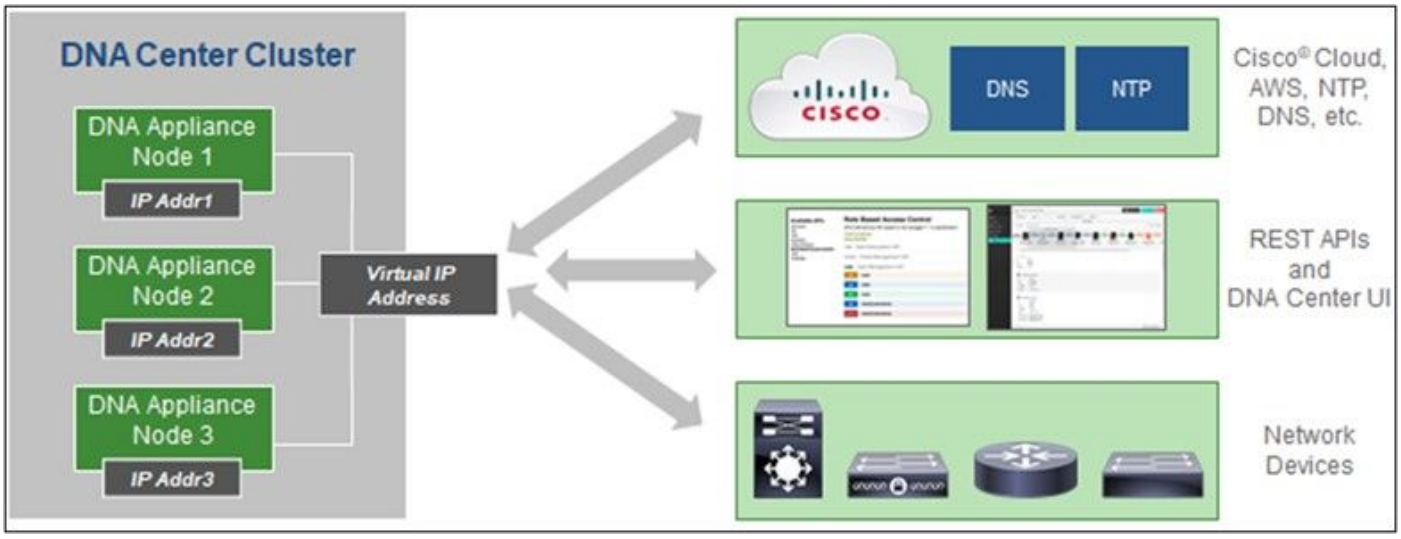
CX Cloud Agent OVA 전용 도메인

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 FQDN의 포트 443에서 활성화된 리디렉션으로 허용되어야 합니다.

Cisco DNA Center 지원 버전

지원되는 단일 노드 및 HA 클러스터 Cisco DNA Center 버전은 2.1.2.x~2.2.3.x, 2.3.3.x, 2.3.5.x와 Cisco Catalyst Center Virtual Appliance 및 Cisco DNA 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

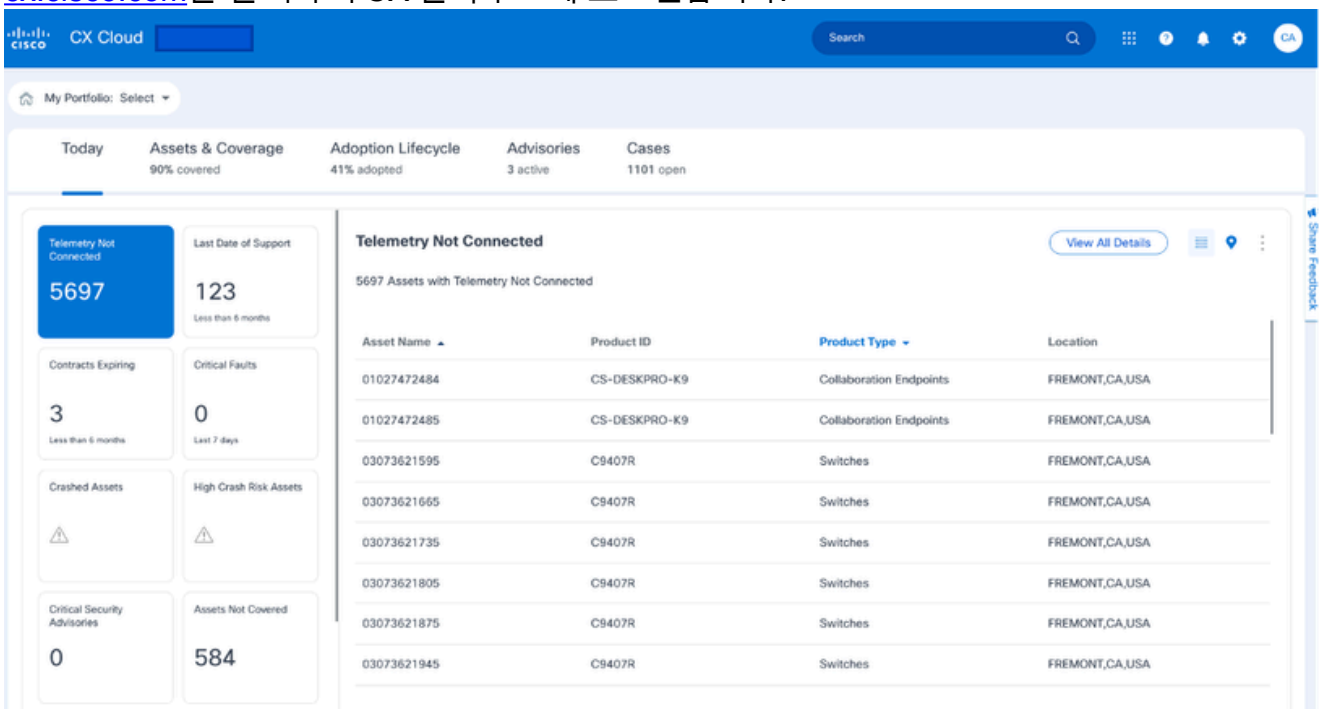
지원되는 제품 목록

CX Cloud Agent에서 지원하는 제품 목록을 보려면 지원되는 제품 목록을 참조하십시오.

데이터 소스 연결

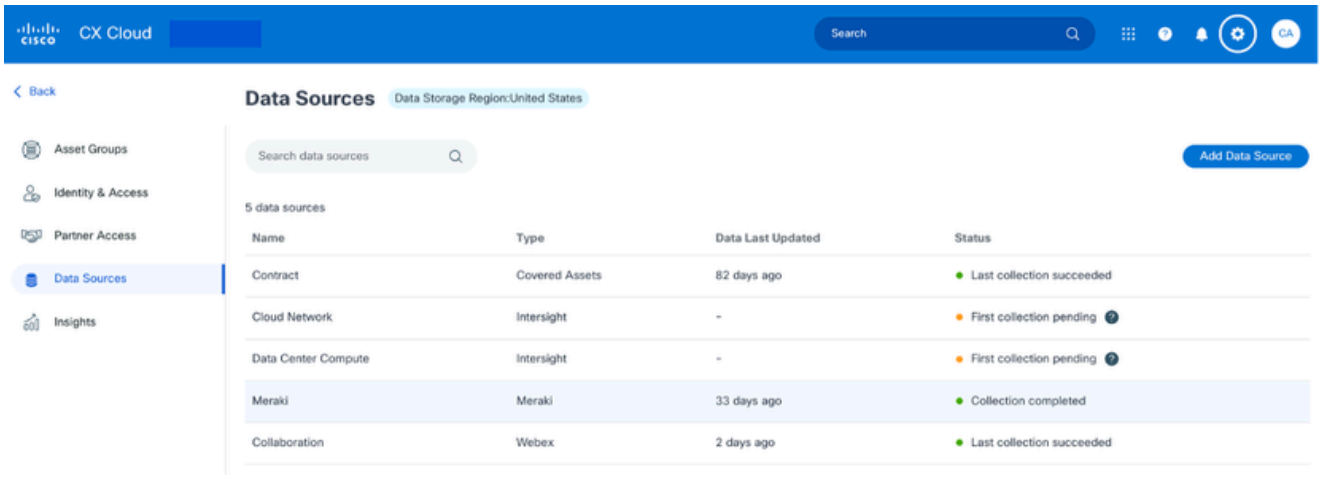
데이터 소스를 연결하려면 다음을 수행합니다.

1. cx.cisco.com을 클릭하여 CX 클라우드에 로그인합니다.



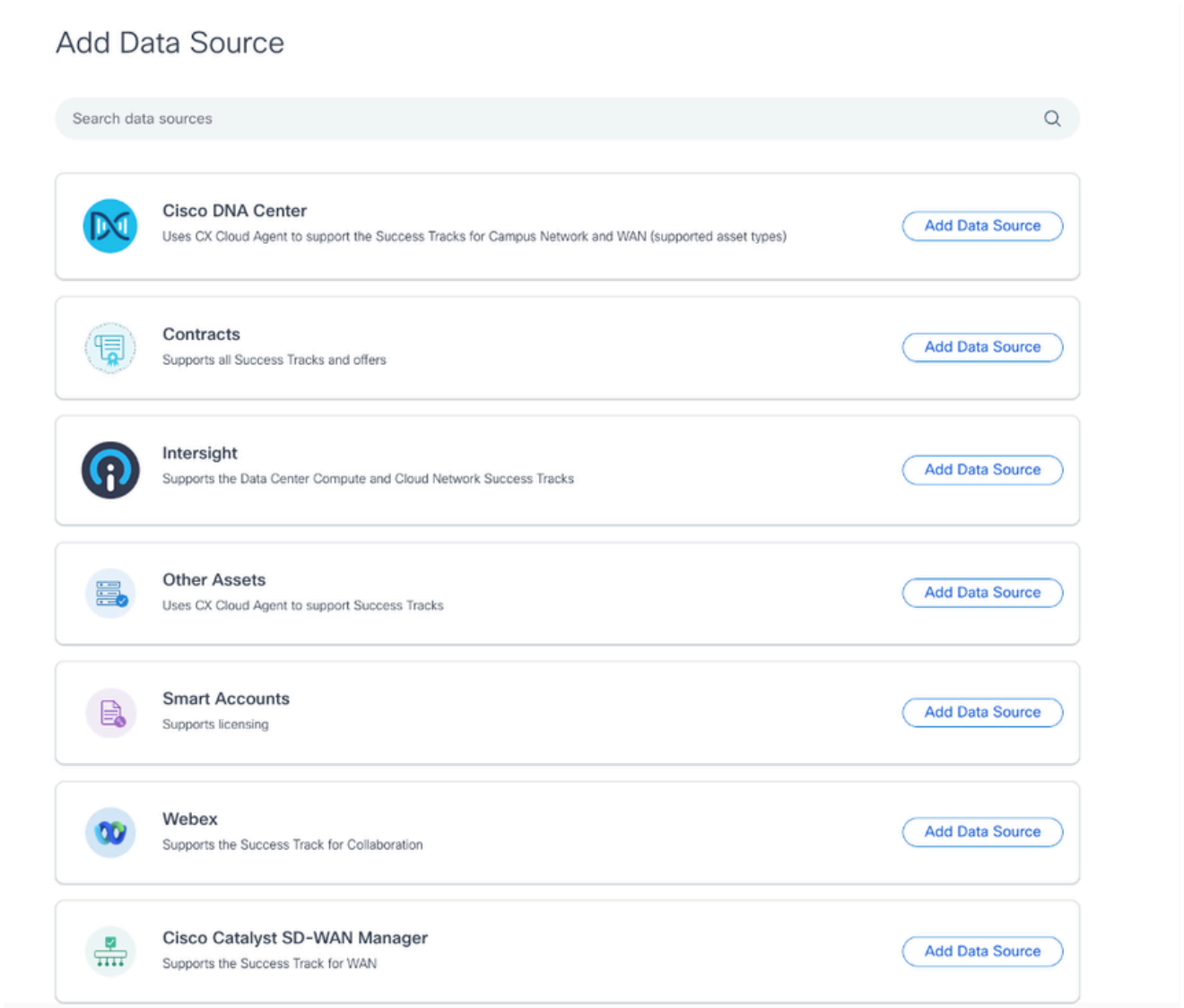
CX 클라우드 홈 페이지

2. Admin Settings(관리 설정) 아이콘을 선택합니다. 데이터 소스 창이 열립니다.



데이터 소스

3. 데이터 소스 추가를 클릭합니다. 데이터 소스 추가 창이 열립니다. 표시되는 옵션은 고객 서브스크립션에 따라 다를 수 있습니다.



데이터 원본 추가

4. 적용 가능한 데이터 소스를 선택하려면 데이터 소스 추가를 누릅니다. CX Cloud Agent가 이전에 설정되지 않은 경우 설정을 완료해야 하는 CX Cloud Agent 설정 창이 열립니다. 설정이

완료되면 연결이 계속됩니다. 계속하려면 다음 섹션 중 하나를 참조하십시오.

[CX 클라우드 에이전트 설정]

[Cisco DNA Center를 데이터 소스로 추가]

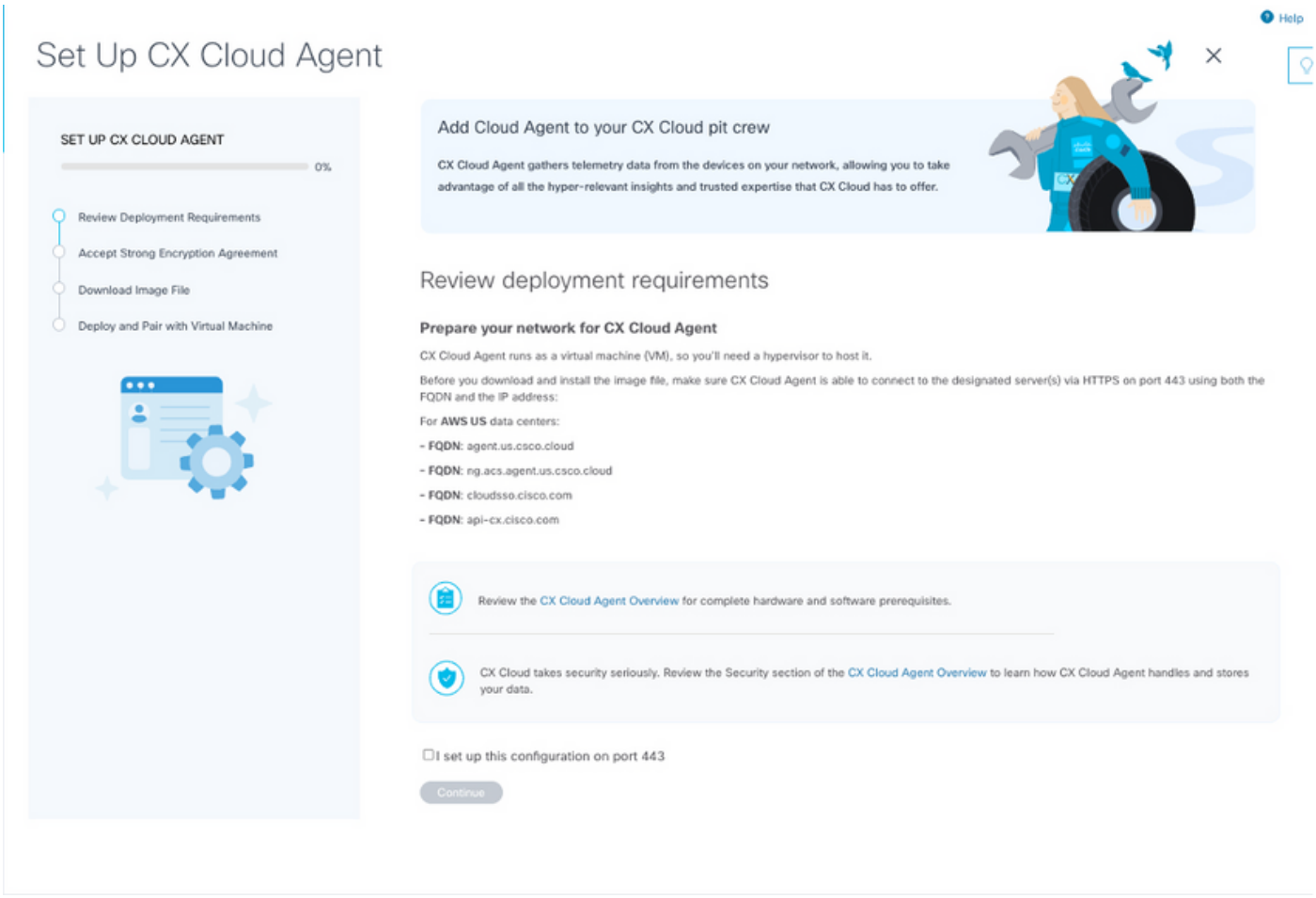
[기타 자산을 데이터 소스로 추가]

참고: Other Assets 옵션은 직접 디바이스 연결이 이전에 구성되지 않은 경우에만 사용할 수 있습니다.

CX 클라우드 에이전트 설정

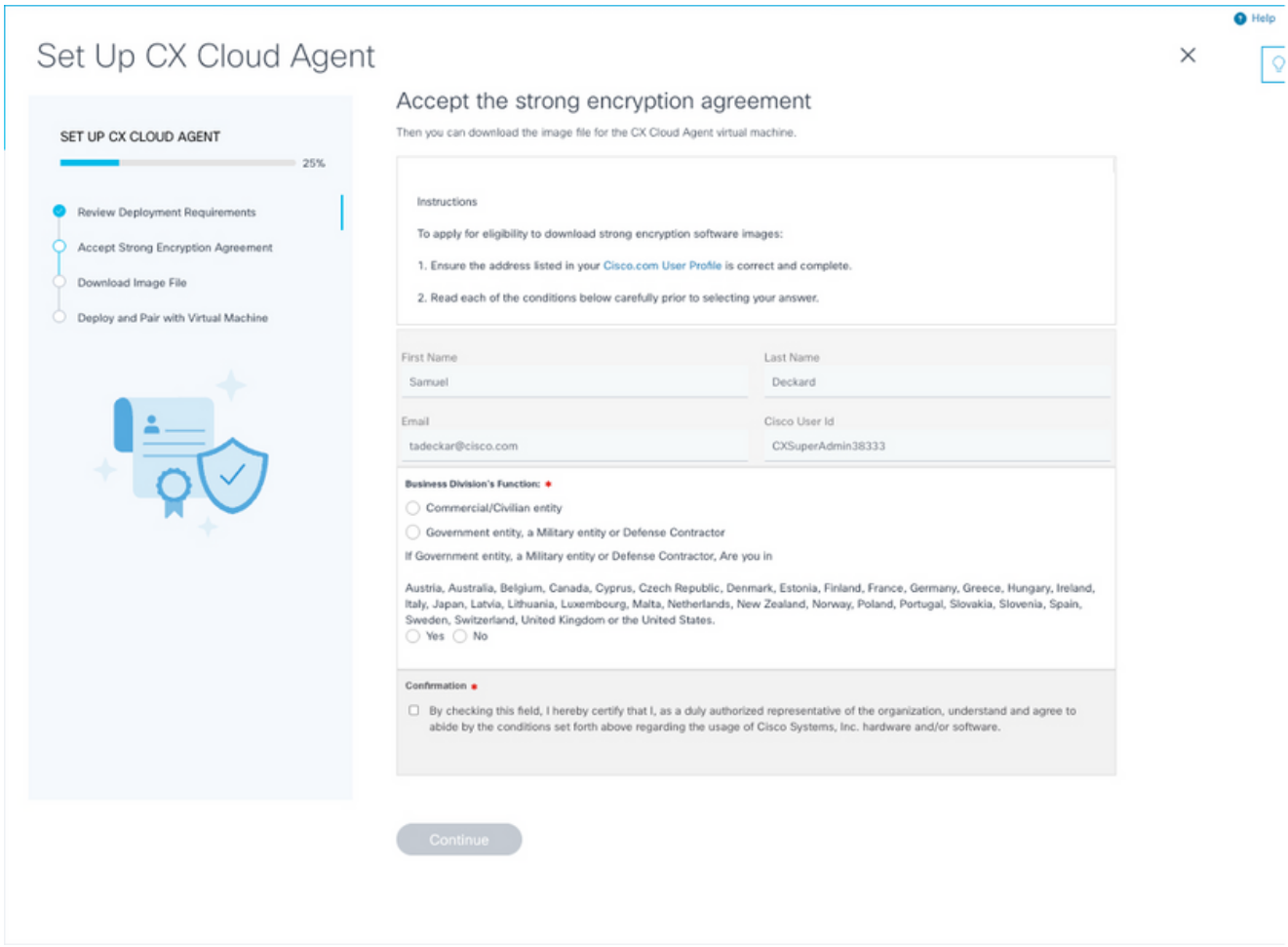
CX Cloud Agent 설정은 이전에 완료하지 않은 경우 데이터 소스 연결 시 프롬프트를 표시합니다.

CX 클라우드 에이전트를 설정하려면



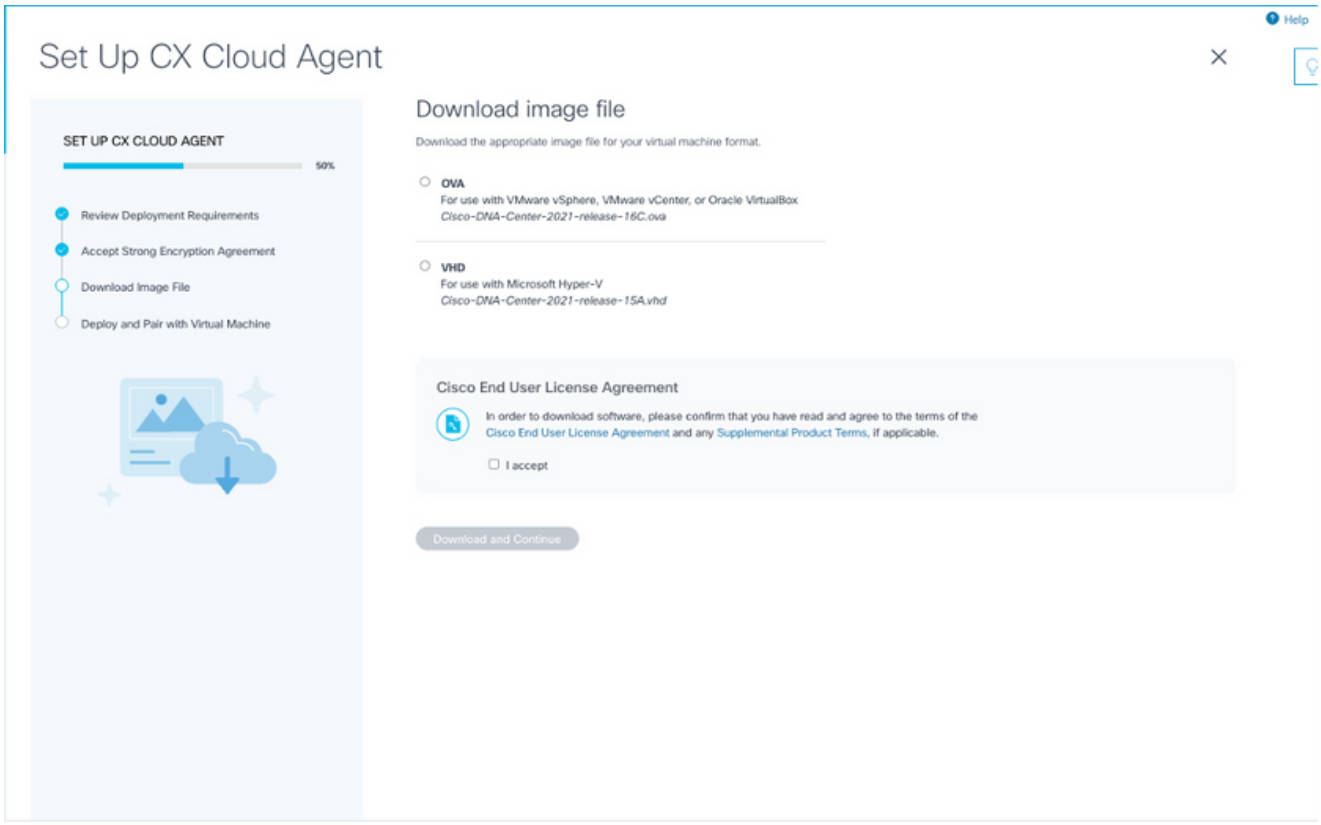
구축 요구 사항 검토

1. Review deployment requirements(구축 요구 사항 검토)를 검토하고 I set up this configuration on port 443(포트 443에서 이 컨피그레이션을 설정함) 확인란을 선택합니다.
2. Continue(계속)를 클릭합니다. Set Up CX Cloud Agent - Accept the strong encryption agreement(CX 클라우드 에이전트 설정 - 강력한 암호화 계약 동의) 창이 열립니다.



암호화 계약

3. First Name, Last Name, E-mail 및 Cisco User Id 필드에서 미리 입력된 정보를 확인합니다.
4. 적절한 비즈니스 부서의 기능을 선택합니다.
5. 사용 조건에 동의하려면 Confirmation(확인) 확인란을 선택합니다.
6. Continue(계속)를 클릭합니다. Set Up CX Cloud Agent - Download image file(CX 클라우드 에이전트 설정 - 이미지 파일 다운로드) 창이 열립니다.



이미지 다운로드

7. 설치에 필요한 이미지 파일을 다운로드하려면 적절한 파일 형식을 선택합니다.
8. Cisco End User License Agreement(Cisco 최종 사용자 라이센스 계약)에 동의하려면 동의함 확인란을 선택합니다.
9. 다운로드 및 계속을 클릭합니다. Set Up CX Cloud Agent - Deploy and pair with your virtual machine(CX 클라우드 에이전트 설정 - 구축 및 가상 머신과 페어링) 창이 열립니다.
10. 다음 섹션에서 필요한 페어링 코드를 얻으려면 네트워크 컨피그레이션을 참조하십시오.

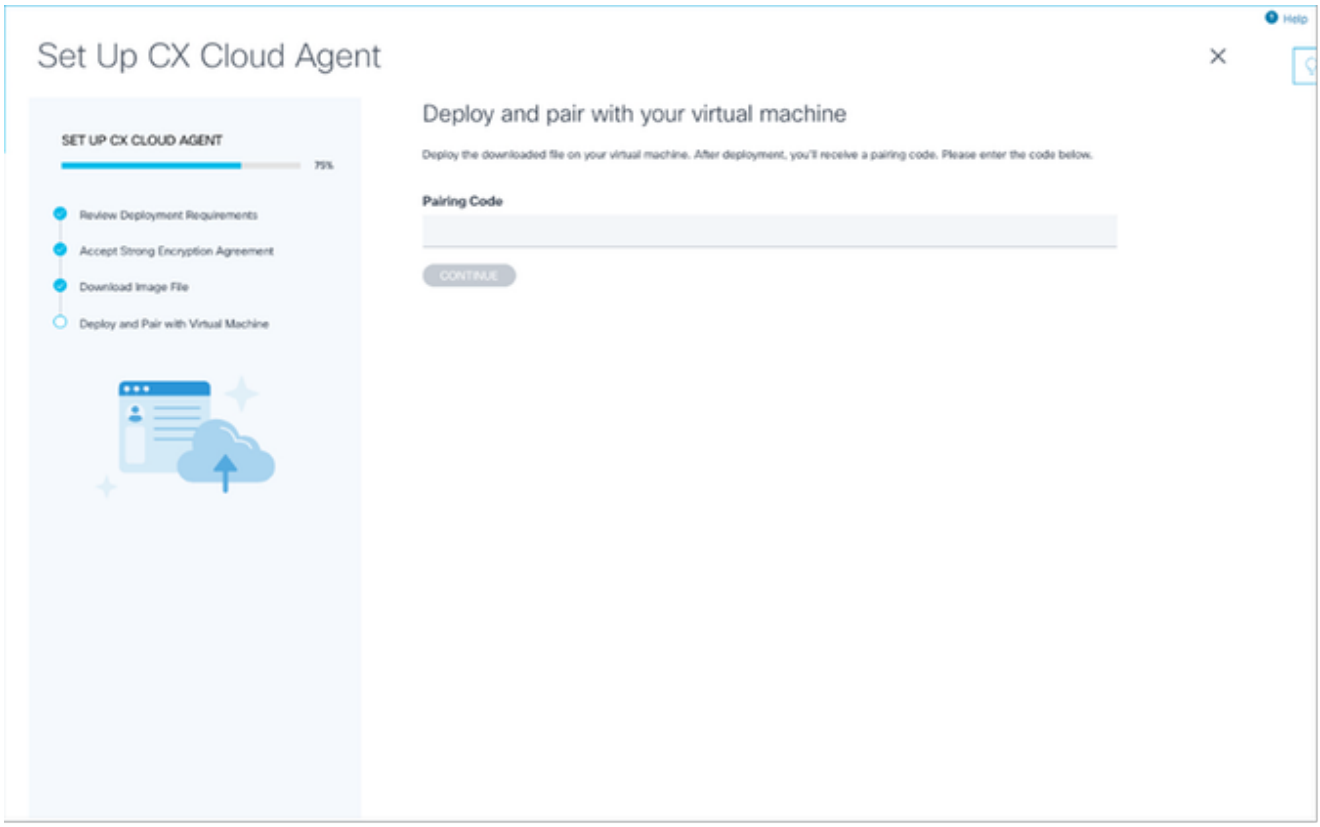
CX Cloud Agent를 CX Cloud에 연결

텔레메트리 수집을 시작하려면 CX Cloud Agent를 CX Cloud에 연결해야 합니다. 그러면 UI의 정보를 업데이트하여 현재 자산 및 통찰력을 표시할 수 있습니다. 이 섹션에서는 연결 및 문제 해결 지침을 완료하는 데 필요한 세부 정보를 제공합니다.

CX Cloud Agent를 CX Cloud에 연결하려면

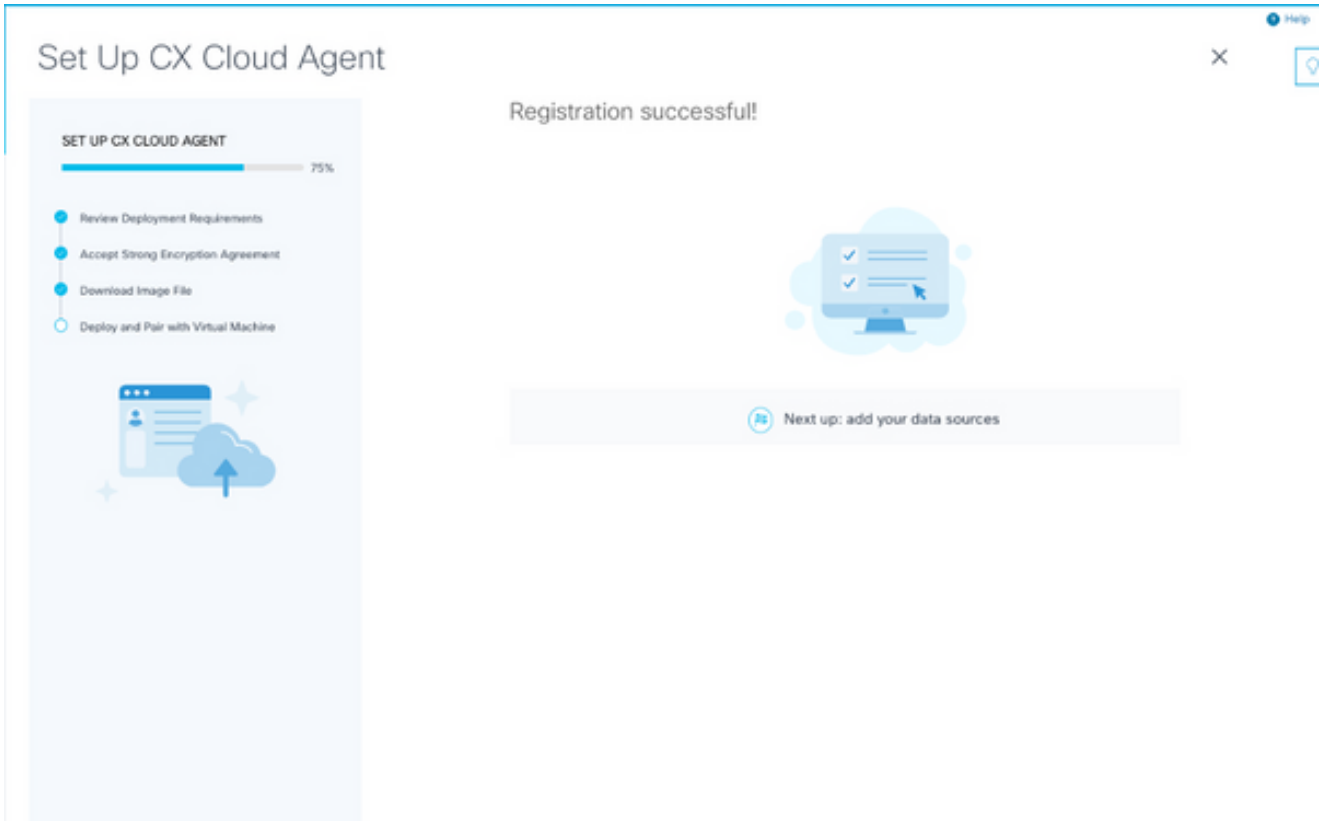
1. 에이전트를 통해 연결된 가상 머신의 콘솔 대화 상자 또는 CLI(Command Line Interface)에 제공된 페어링 코드를 입력합니다.

> 참고: 페어링 코드는 다운로드한 OVA 파일을 배포한 후에 수신됩니다.



페어링 코드

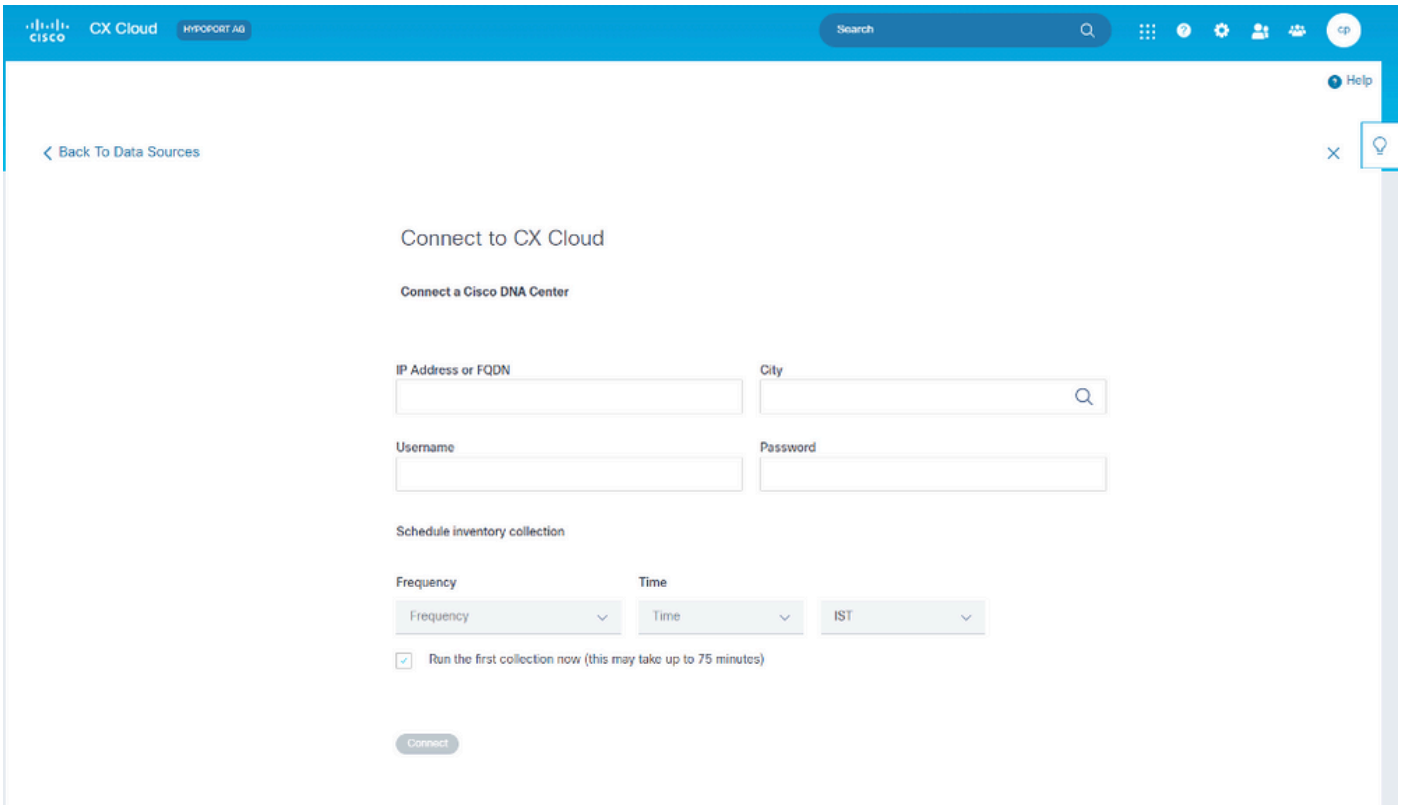
2. CX 클라우드 에이전트를 등록하려면 Continue(계속)를 클릭합니다. CX Cloud Agent 설정 - 등록 성공 창이 잠시 열리고 자동으로 데이터 소스 추가 페이지로 이동합니다.



등록 성공

Cisco DNA Center를 데이터 소스로 추가

데이터 소스 연결 창에서 Cisco DNA Center를 선택하면(데이터 소스 연결 섹션의 데이터 소스 연결 이미지 참조) 다음 창이 열립니다.



CX 클라우드에 연결

Cisco DNA Center를 데이터 소스로 추가하려면

1. Cisco DNA Center IP 주소 또는 가상 IP 주소 또는 FQDN, 시(Cisco DNA Center의 위치), 사용자 이름 및 비밀번호를 입력합니다.

   참고: 개별 클러스터 노드 IP를 사용하지 마십시오.

2. CX Cloud Agent에서 네트워크 검사를 수행하고 연결된 디바이스에 대한 정보를 업데이트하는 빈도를 지정하려면 빈도와 시간을 입력하여 인벤토리 수집을 예약합니다.

   참고: 첫 번째 인벤토리 수집에는 최대 75분이 소요될 수 있습니다.

3. 연결을 클릭합니다. 확인 메시지가 Cisco DNA Center IP 주소와 함께 표시됩니다.

연결 성공

4. Add Another Cisco DNA Center(다른 Cisco DNA 센터 추가), Done(완료) 또는 Back to Data Sources(데이터 소스로 돌아가기)를 클릭하여 데이터 소스 창으로 돌아갑니다.

기타 자산을 데이터 소스로 추가

개요

텔레메트리 수집은 Cisco DNA Center에서 관리하지 않는 장치까지 확장되어 고객이 텔레메트리 기반의 통찰력과 분석을 보고 상호 작용하면서 더 광범위한 장치를 사용할 수 있게 되었습니다. 초기 CX Cloud Agent 설정 후 사용자는 CX Cloud Agent를 구성하여 CX Cloud에서 모니터링하는 인프라 내의 20개의 추가 Cisco DNA Center에 연결할 수 있습니다. 또한 사용자는 CX Cloud Agent를 직접 연결된 최대 10,000개의 디바이스를 보유한 환경의 다른 하드웨어 자산에 직접 연결할 수 있습니다.

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

참고:
시드 파일 또는 IP 범위를 사용할 수 있습니다. 초기 설정 후에는 이 선택을 변경할 수 없습니다.

참고:
초기 시드 파일은 다른 시드 파일로 바꿀 수 있으며 초기 IP 범위는 새 IP 범위로 편집할 수 있습니다.

데이터 소스 연결 창에서 기타 에셋을 선택하면 다음 창이 열립니다.

CX 클라우드에 대한 연결 구성

다른 자산을 데이터 소스로 추가하려면

- 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 Cloud Agent는 SNMPV2c 및 SNMP V3를 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 SNMPV3는 보안 및 원격 컨피그레이션 모델 측면에서 차이가 있습니다. SNMPV3는 SHA 암호화를 지원하는 고급 암호화 보안 시스템을 사용하여 메시지를 인증하고 개인 정보를 보호합니다. 보안 위험과 위협으로부터 보호하기 위해 모든 공용 및 인터넷 연결 네트워크에서 SNMPv3를 사용하는 것이 좋습니다. CX 클라우드에서는 SNMPv3를 기본적으로 지원하지 않는 구형 레거시 디바이스를 제외하고 SNMPv2c가 아닌 SNMPv3를 구성하는 것이 좋습니다. 사용자가 두 버전의 SNMP를 모두 구성한 경우, CX Cloud 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 정보, 즉 SSH(또는 텔넷)를 지정해야 합니다. SSHv2를 사용해야 합니다. 단, 적절한 기본 제공 지원이 없는 개별 레거시 자산의 경우는 예외입니다. SSHv1 프로토콜에는 기본 취약성이 포함되어 있습니다. SSHv1에 의존

할 경우 이러한 취약성으로 인해 추가 보안, 텔레메트리 데이터 및 기본 자산이 손상될 수 있습니다. 텔넷도 안전하지 않습니다. 텔넷을 통해 제출된 자격 증명 정보(사용자 이름 및 비밀번호)는 암호화되지 않으므로 보안상의 문제가 발생할 수 있습니다.

시드 파일을 사용하여 디바이스 추가

시드 파일 정보

시드 파일은 쉼표로 구분된 값(csv) 파일이며 각 행은 시스템 데이터 레코드를 나타냅니다. 시드 파일에서 모든 시드 파일 레코드는 CX Cloud Agent에서 텔레메트리를 수집해야 하는 고유한 디바이스에 해당합니다. 가져오는 시드 파일의 각 디바이스 항목에 대한 모든 오류 또는 정보 메시지는 작업 로그 세부사항의 일부로 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 Cloud Agent는 디바이스에 연결을 시도하지만 PID 또는 일련 번호를 확인할 수 없는 경우 Assets(에셋) 페이지에 표시하기 위해 각 디바이스를 처리하지 못할 수 있습니다.세미콜론으로 시작하는 시드 파일의 모든 행은 무시됩니다. 시드 파일의 헤더 행은 세미콜론으로 시작하며 고객 시드 파일을 생성하는 동안 그대로 유지하거나(권장 옵션) 삭제할 수 있습니다.

열 헤더를 비롯한 샘플 시드 파일의 형식은 어떤 식으로든 변경되지 않는 것이 중요합니다. 제공된 링크를 클릭하여 시드 파일을 PDF 형식으로 봅니다. 이 PDF는 참조용이며 .csv 형식으로 저장해야 하는 시드 파일을 만드는 데 사용할 수 있습니다.

시드 파일을 .csv 형식으로 만드는 데 사용할 수 있는 시드 파일을 보려면 이 링크를 클릭합니다.

참고: 이 PDF는 참조 전용이며 .csv 형식으로 저장해야 하는 시드 파일을 만드는 데 사용할 수 있습니다.

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 Cloud Agent에 필요하며 고객 네트워크 내의 디바이스 검색에 사용됩니다. 값은 snmpv2c 또는 snmpv3이 될 수 있지만 보안 고려 사항으로 인해 snmpv3이 권장됩니다.
C	snmpRo: col#=3이	특정 디바이스에 대해 SNMPv2의 레거시 변형

Seed File(시드 파일) 열	열 헤더/식별자	열의 목적
	'snmpv2c'로 선택된 경우 필수	을 선택한 경우 디바이스 SNMP 컬렉션에 대한 snmpRO(읽기 전용) 자격 증명을 지정해야 합니다. 그렇지 않으면 항목을 비워 둘 수 있습니다.
D	snmpv3UserName : col#=3이 'snmpv3'로 선택된 경우 필수	특정 디바이스와 통신하도록 SNMPv3을 선택한 경우 해당 로그인 사용자 이름을 제공해야 합니다.
E	snmpv3AuthAlgorithm: 값은 MD5 또는 SHA일 수 있습니다.	SNMPv3 프로토콜은 MD5 또는 SHA 알고리즘을 통한 인증을 허용합니다. 디바이스가 보안 인증으로 구성된 경우 각 인증 알고리즘을 제공해야 합니다. 참고: MD5는 안전하지 않은 것으로 간주되며 이를 지원하는 모든 디바이스에서 SHA를 사용해야 합니다.
F	snmpv3AuthPassword : 비밀번호	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. 참고: DES에서 사용하는 56비트 키는 너무 짧아 암호화 보안을 제공할 수 없으며 3DES는 이를 지원하는 모든 디바이스에서 사용해야 합니다.
H	snmpv3PrivPassword : 비밀번호	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 Cloud Agent에서 SNMP 데이터 세트를 수집하는 동안 참조로 전송됩니다. 고객이 EngineID를 수동으로 구성하는 경우 해당 EngineID를 제공해

Seed File(시드 파일) 열	열 헤더/식별자	열의 목적
		야 합니다.
제이	cliProtocol: 값은 'telnet', 'sshv1', 'sshv2'가 될 수 있습니다. 비어 있으면 기본적으로 'sshv2'로 설정됩니다.	CLI는 디바이스와 직접 상호 작용하기 위한 것입니다. CX Cloud Agent는 특정 디바이스의 CLI 수집에 이 프로토콜을 사용합니다. 이 CLI 수집 데이터는 CX 클라우드 내의 Assets 및 기타 Insights 보고에 사용됩니다. SSHv2가 권장됩니다. 다른 네트워크 보안 수단이 없고 그 자체로는 SSHv1 및 텔넷 프로토콜이 적절한 전송 보안을 제공하지 않습니다.
케이	cliPort : CLI 프로토콜 포트 번호	CLI 프로토콜을 선택한 경우 해당 포트 번호를 제공해야 합니다. 예를 들어, SSH의 경우 22, 텔넷의 경우 23입니다.
L	cliUser : CLI 사용자 이름 (CLI 사용자 이름/비밀번호 또는 둘 다 제공할 수 있지만 두 열(col#=12 및 col#=13)은 모두 비워둘 수 없습니다.)	디바이스의 각 CLI 사용자 이름을 제공해야 합니다. 이는 CLI 수집 중에 디바이스에 연결할 때 CX Cloud Agent에서 사용됩니다.
M	cliPassword : CLI 사용자 비밀번호(CLI 사용자 이름/비밀번호 또는 둘 다 제공할 수 있지만 두 열(col#=12 및 col#=13)은 모두 비워둘 수 없습니다.)	디바이스의 각 CLI 비밀번호를 제공해야 합니다. 이는 CLI 수집 중에 디바이스에 연결할 때 CX Cloud Agent에서 사용됩니다.
네트워킹	cliEnable사용자	디바이스에 "enable"이 구성된 경우 디바이스의 enableUsername 값을 제공해야 합니다.
O	cliEnable비밀번호	디바이스에 "enable"이 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

Seed File(시드 파일) 열	열 헤더/식별자	열의 목적
R	향후 지원(입력 필요 없음)	향후 사용을 위해 예약됨
초	향후 지원(입력 필요 없음)	향후 사용을 위해 예약됨

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. 디바이스 계측 제한으로 인해 이러한 디바이스 텔레메트리를 처리할 수 없습니다.

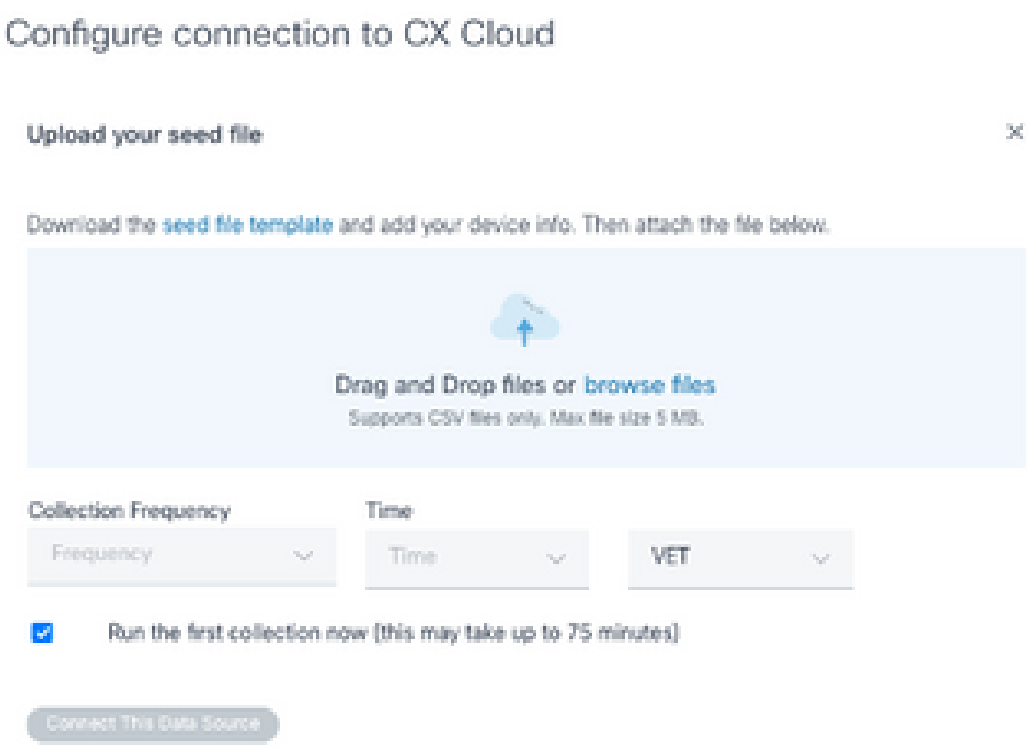
- Campus Success Track에 속하지 않은 디바이스의 CX Cloud Assets 페이지에서 텔레메트리 특성이 부정확하거나 누락될 수 있습니다.
- 시드 파일 또는 IP 범위 컬렉션의 디바이스도 Cisco DNA Center 인벤토리의 일부인 경우 디바이스는 Cisco DNA Center 항목에 대해 한 번만 보고됩니다. 시드 파일/IP 범위 항목은 중복을 방지하기 위해 수집되거나 처리되지 않습니다.

새 시드 파일을 사용하여 디바이스 추가

새 시드 파일을 사용하여 디바이스를 추가하려면

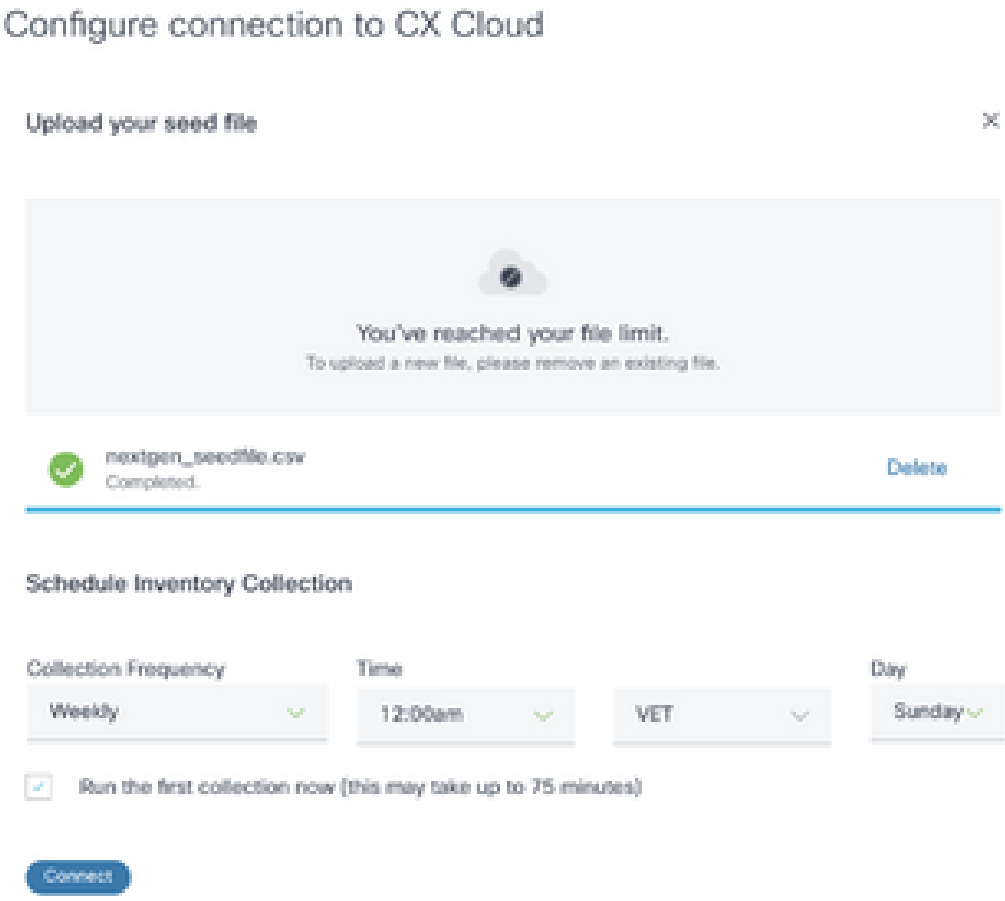
1. 이 문서에 포함된 링크를 사용하거나(시드 파일 정보 참조) CX 클라우드에 대한 연결 구성 창의 링크를 통해 시드 파일 템플릿(PDF)을 다운로드합니다.

   참고: 초기 시드 파일을 다운로드한 후 Configure Connection to CX Cloud(CX 클라우드에 연결 구성) 창의 링크를 더 이상 사용할 수 없습니다.



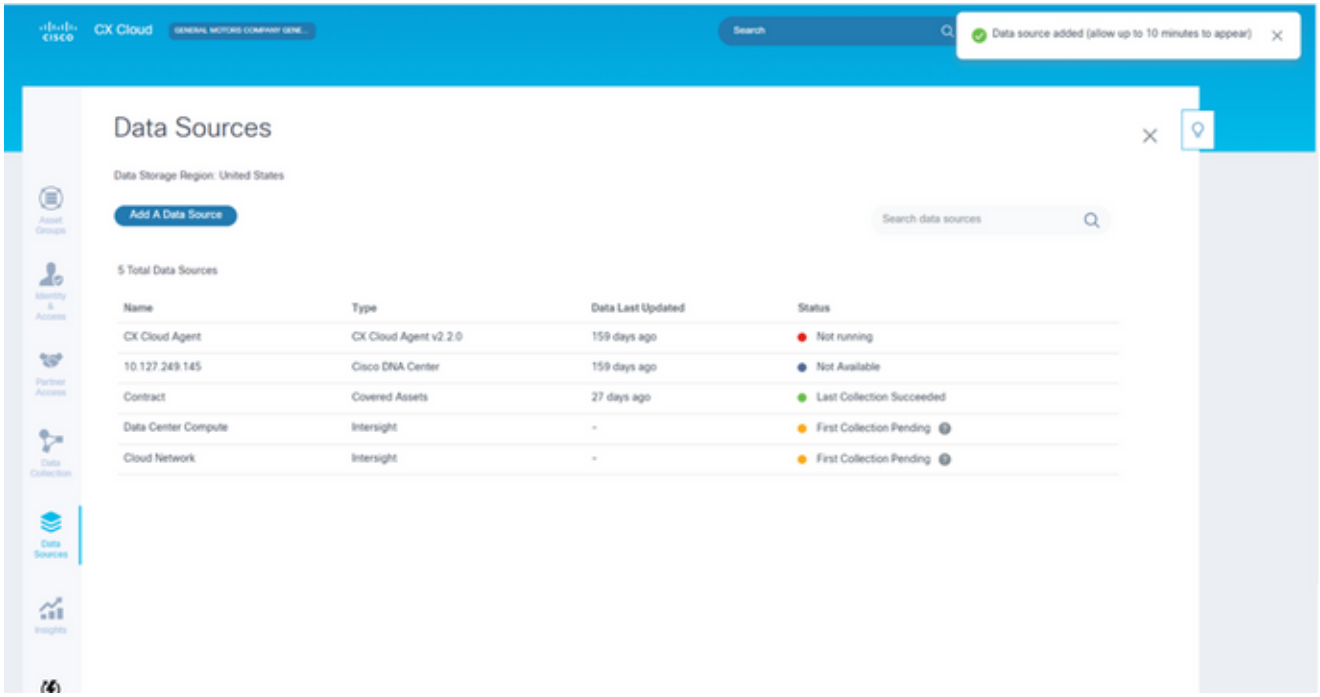
CX 클라우드에 연결 구성 창

2. Excel 스프레드시트(또는 원하는 스프레드시트)를 열고 템플릿에 표시된 대로 머리글을 입력합니다.
3. 데이터를 수동으로 입력하거나 파일로 데이터를 가져옵니다.
4. 완료되면 템플릿을 .csv 파일로 저장하여 파일을 CX Cloud Agent로 가져옵니다.



시드 파일 업로드 창

5. Upload your seed file(시드 파일 업로드) 창에서 새로 생성된 .csv 파일을 드래그 앤 드롭하거나 browse files(파일 찾아보기)를 클릭하고 .csv 파일로 이동합니다.
6. Schedule Inventory Collection(인벤토리 수집 예약) 섹션을 완료하고 Connect(연결)를 클릭합니다. 데이터 소스 창이 열리고 확인 메시지가 표시됩니다.
7. 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 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.



확인 메시지

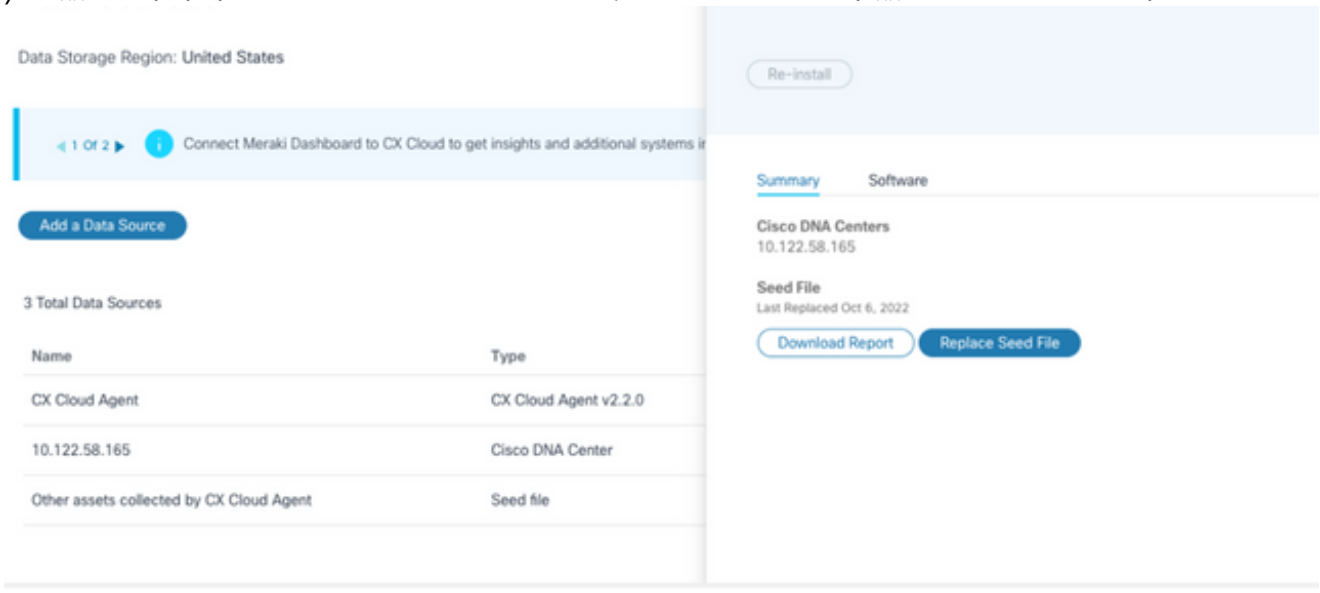
수정된 시드 파일을 사용하여 디바이스 추가

현재 시드 파일을 사용하여 디바이스를 추가, 수정 또는 삭제하려면

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

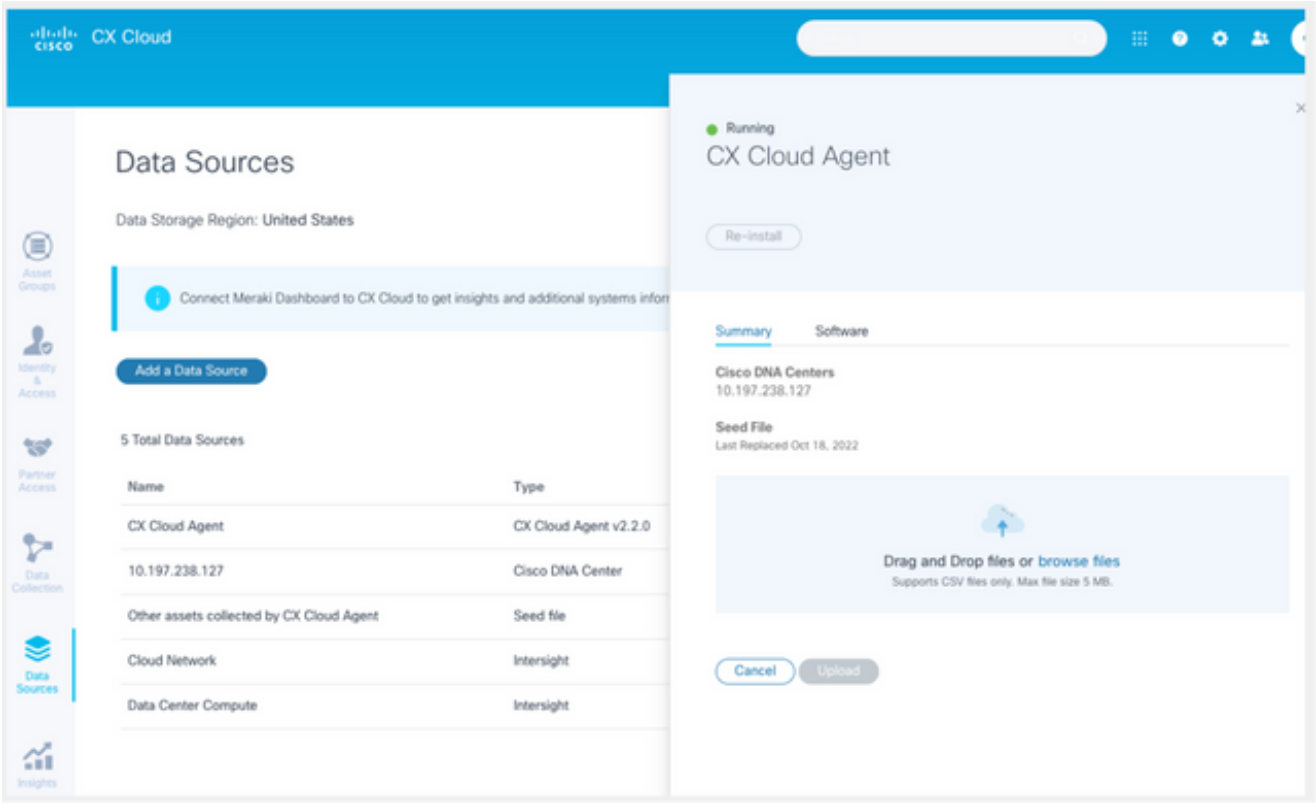
> 참고: 시드 파일에 에셋을 추가하려면 이전에 생성한 시드 파일에 에셋을 추가하고 파일을 다시 로드합니다. 새 시드 파일을 업로드하면 현재 시드 파일이 대체되므로 이 작업이 필요합니다. 최신 업로드된 시드 파일만 검색 및 수집에 사용됩니다.

2. Data Sources(데이터 소스) 페이지에서 Type of CX Cloud Agent(CX 클라우드 에이전트 유형)가 있는 데이터 소스를 선택합니다. 요약 및 소프트웨어 탭이 있는 세부 정보 창이 열립니다.



세부 정보 창

3. 선택한 데이터 소스에 대한 모든 에셋에 대한 보고서를 생성하려면 보고서 다운로드를 클릭합니다. 이 보고서는 디바이스 IP 주소, 일련 번호, 연결 가능성, 명령 유형, 명령 상태, 명령 오류(해당되는 경우)에 대한 정보를 제공합니다.
4. 시드 파일 교체를 클릭합니다. CX Cloud Agent 창이 열립니다.



CX Cloud Agent 창

5. 수정된 시드 파일을 창으로 끌어다 놓거나 해당 파일을 찾아 창에 추가합니다.
6. Upload를 클릭합니다.

IP 범위를 사용하여 디바이스 추가

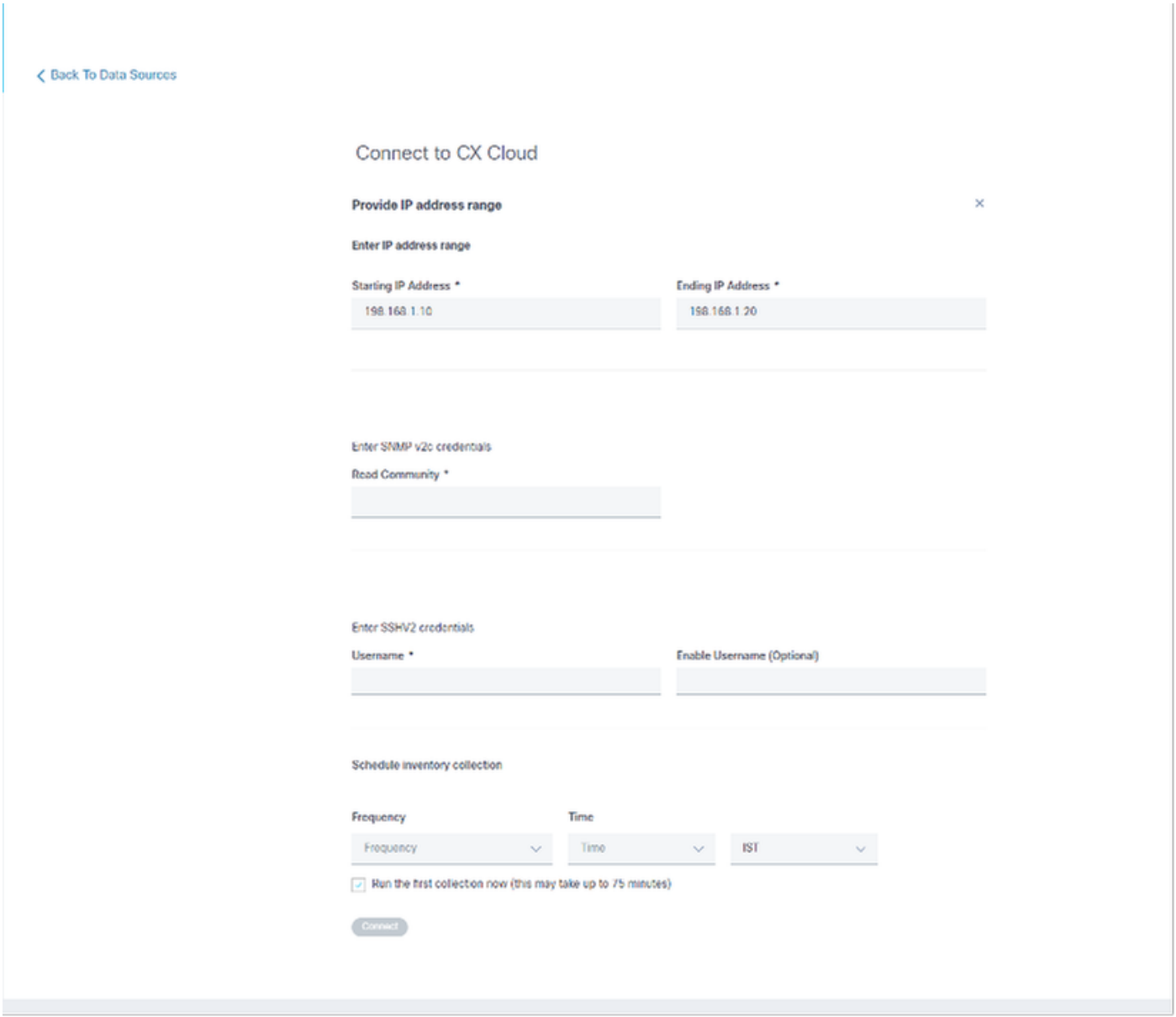
IP 범위를 통해 사용자는 하드웨어 자산을 식별하고, IP 주소를 기반으로 해당 디바이스에서 텔레메트리를 수집할 수 있습니다. 텔레메트리 수집을 위한 디바이스는 단일 네트워크 레벨 IP 범위를 지정하여 고유하게 식별할 수 있으며, 이는 SNMP 프로토콜을 사용하여 CX Cloud Agent에서 스캔해야 합니다. 직접 연결된 디바이스를 식별하기 위해 IP 범위를 선택하는 경우, 참조되는 IP 주소는 가능한 한 제한적이어야 하며, 필요한 모든 자산에 대한 커버리지를 허용해야 합니다.

- 특정 IP를 제공하거나, 범위를 생성하기 위해 IP의 옥텟을 대체하는 데 와일드카드를 사용할 수 있습니다
- 설정 과정에서 확인된 IP 범위에 특정 IP 주소가 포함되지 않은 경우 CX Cloud Agent는 해당 IP 주소가 있는 디바이스와의 통신을 시도하지 않으며 해당 디바이스로부터 텔레메트리를 수집하지도 않습니다
- *.*.*.*를 입력하면 CX Cloud Agent에서 모든 IP에 사용자 제공 자격 증명을 사용할 수 있습니다. 예: 172.16.*.*는 172.16.0.0/16 서브넷의 모든 디바이스에 자격 증명을 사용할 수 있도록 허용합니다

- 네트워크 또는 IB(Installed Base)에 변경 사항이 있을 경우 IP 범위를 수정할 수 있습니다. IP 범위 수정 섹션을 참조하십시오.

CX Cloud 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 삭제되는 경우(내부 또는 외부), 고객은 항상 IP 주소 범위 수정(IP 범위 수정 섹션 참조)을 클릭하고 새로 추가된 디바이스를 CX Cloud Agent 컬렉션 인벤토리에 포함하도록 온디맨드 디바이스 검색을 시작하는 데 필요한 단계를 완료해야 합니다.



Initial IP address range(초기 IP 주소 범위) 창

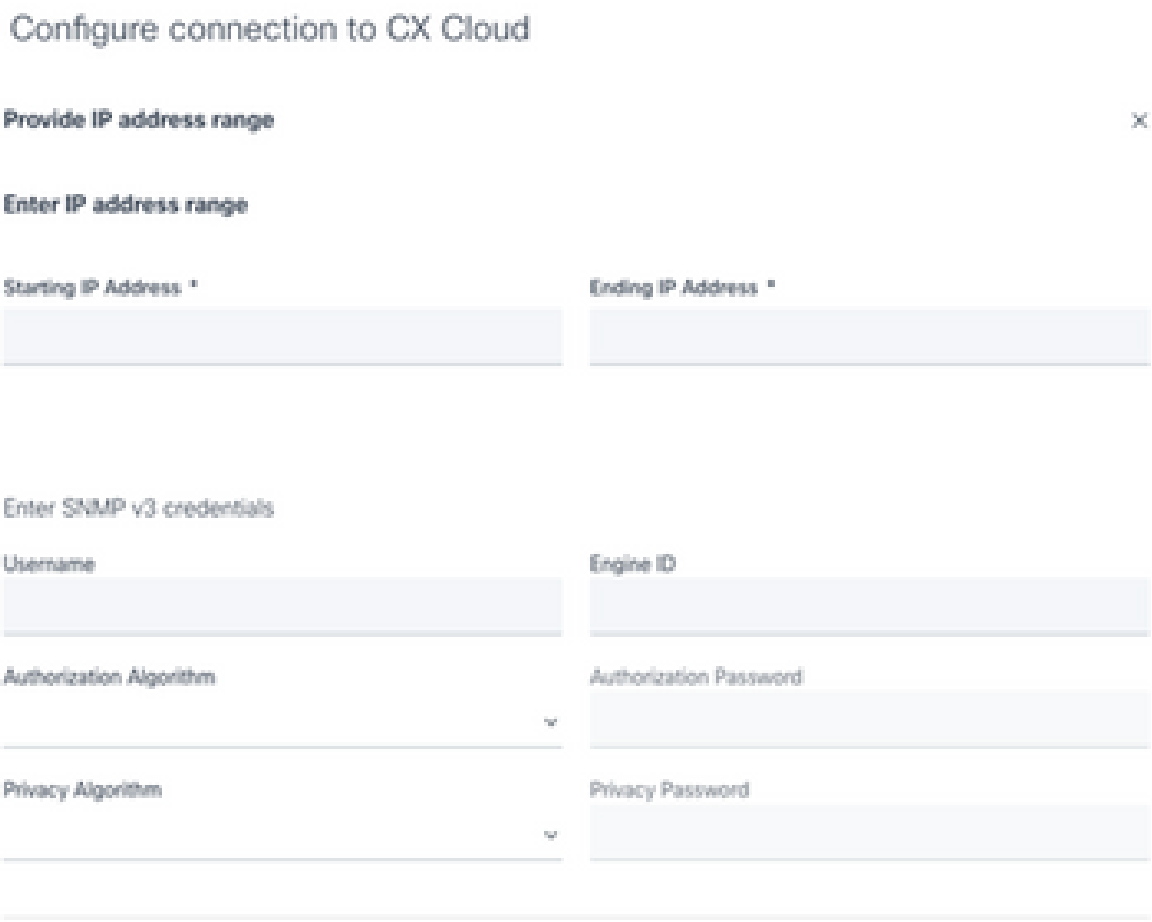
IP 범위를 사용하여 디바이스를 추가하려면 사용자가 컨피그레이션 UI를 통해 적용 가능한 모든 자격 증명을 지정해야 합니다. 표시되는 필드는 이전 창에서 선택한 프로토콜에 따라 달라집니다.

SNMPv2c와 SNMPv3을 둘 다 선택하거나 SSHv2와 SSHv1을 둘 다 선택하는 등 동일한 프로토콜에 대해 여러 항목을 선택한 경우, CX Cloud Agent는 개별 디바이스 기능을 기반으로 프로토콜 선택 사항을 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.

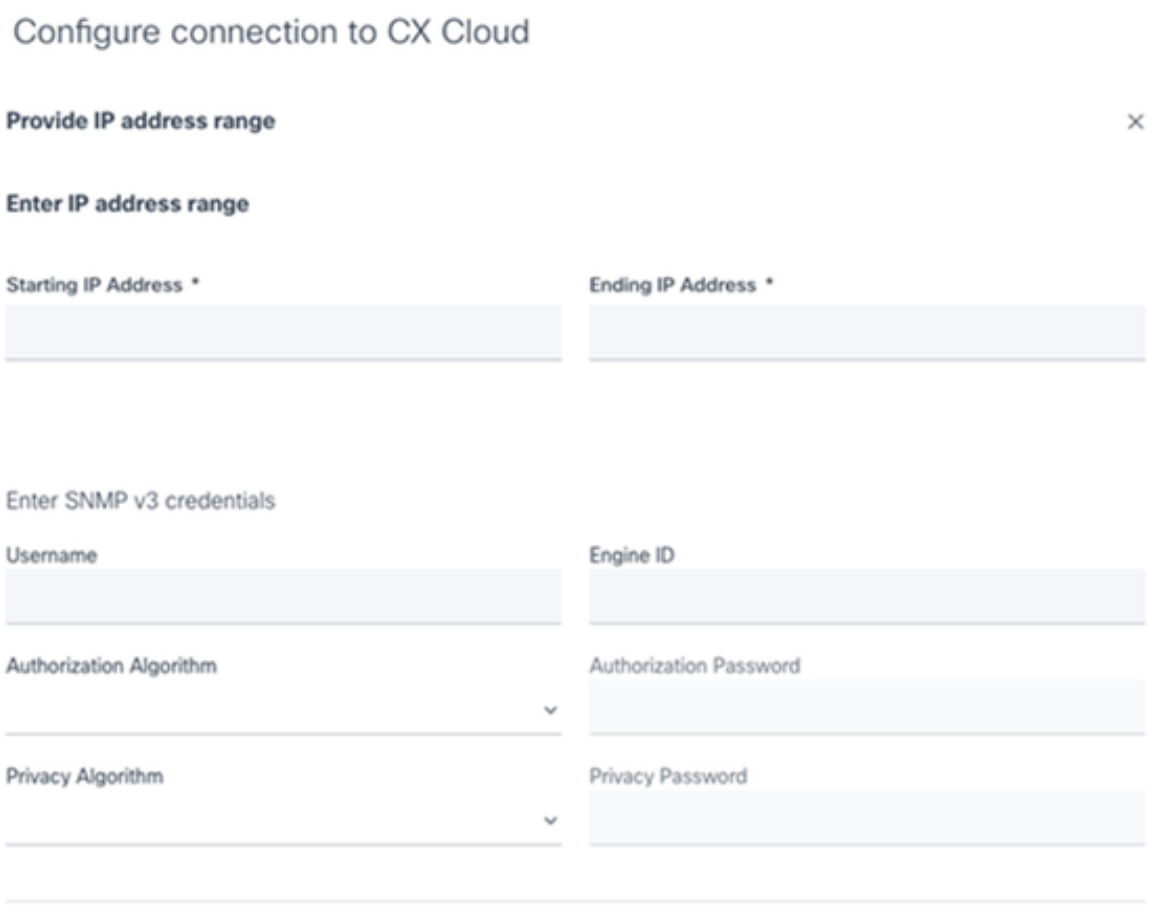
IP 범위를 사용하여 디바이스를 추가하려면

1. CX 클라우드에 대한 연결 구성 창에서 IP 주소 범위 제공 옵션을 선택합니다.

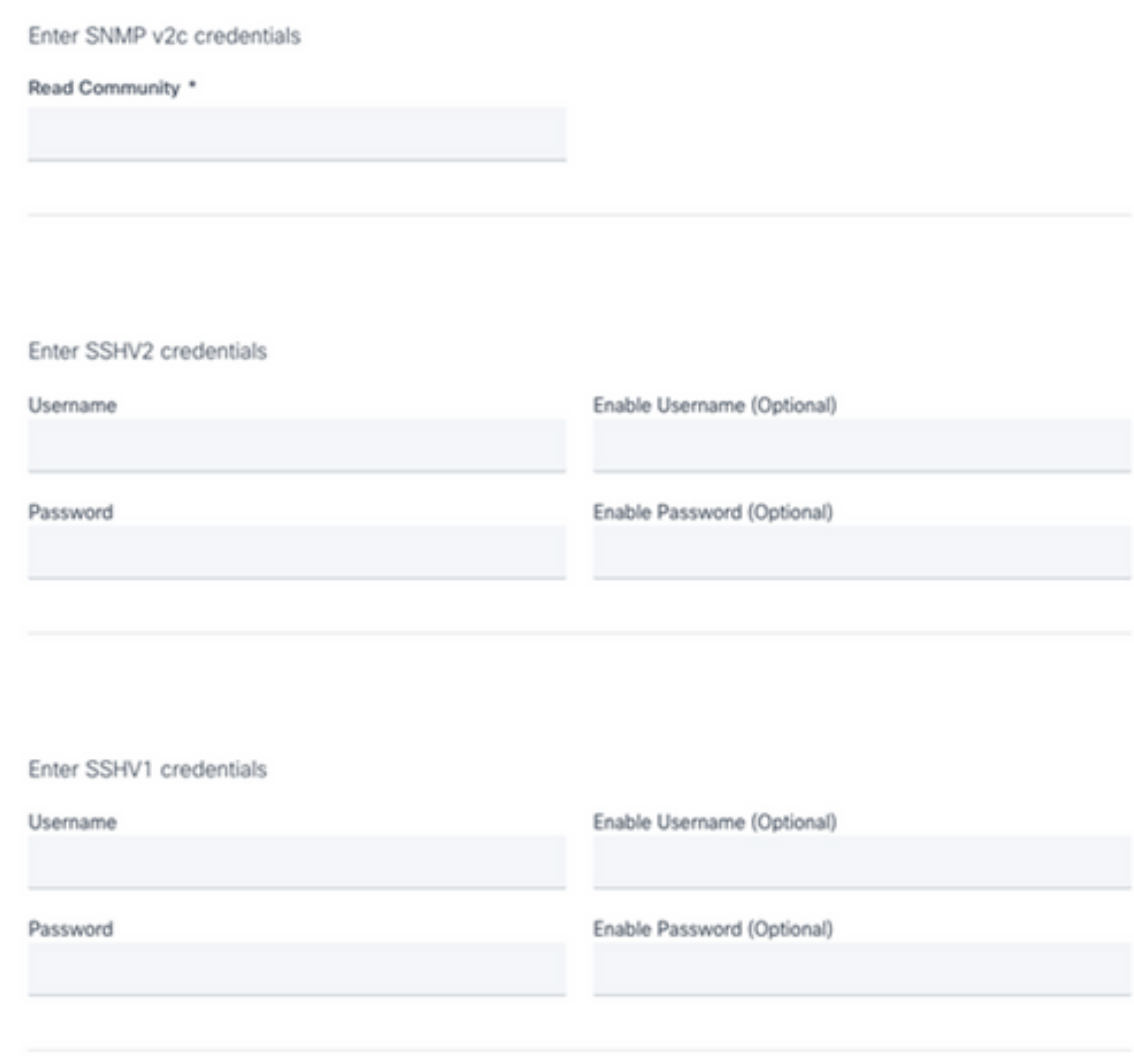


IP 주소를 사용하여 장치 추가 양식

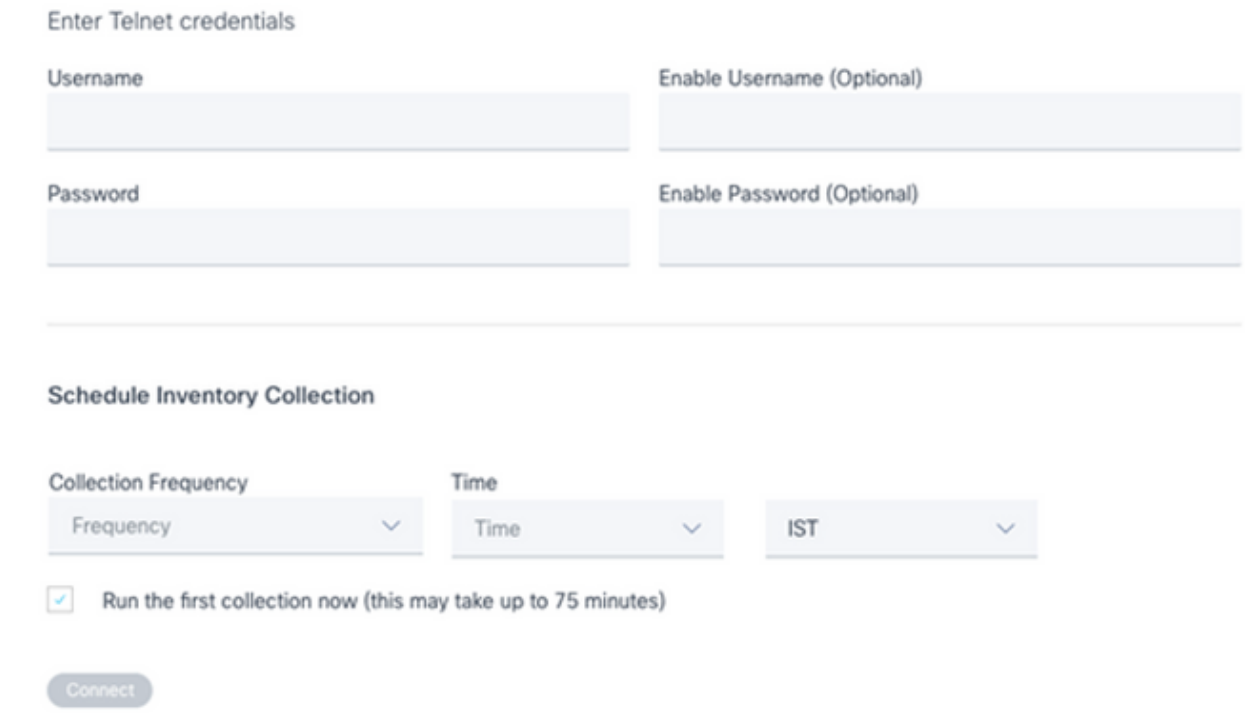
2. 관련 정보가 포함된 양식을 작성합니다.
3. 여러 연결 옵션을 선택할 수 있습니다. 다음 화면에는 옵션에 대한 컨피그레이션 자격 증명이 표시됩니다. 각 연결 옵션의 자격 증명 필드에 대한 설명은 시드 파일 정보를 참조하십시오.


Configure connection to CX Cloud
Provide IP address range
Enter IP address range
Starting IP Address *
Ending IP Address *
Enter SNMP v3 credentials
Username
Engine ID
Authorization Algorithm
Authorization Password
Privacy Algorithm
Privacy Password

SNMP v3 자격 증명

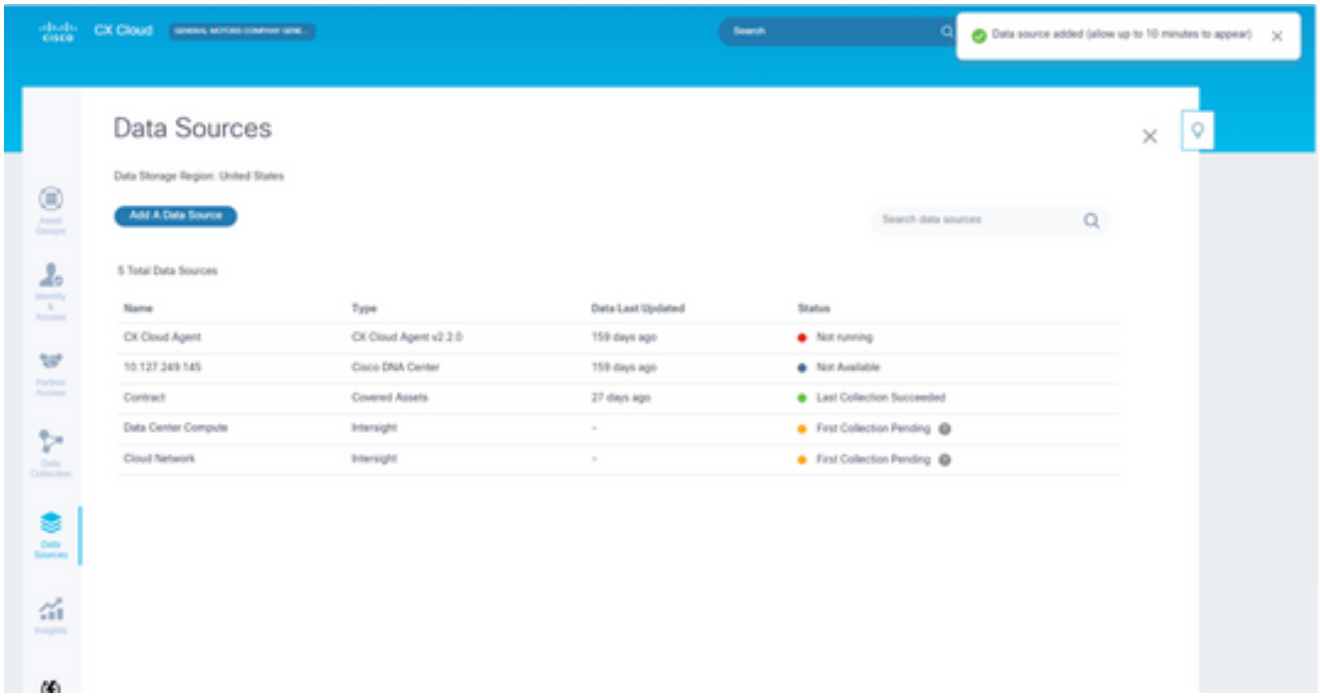


SNMP v2, SSHV2 및 SSHV1 자격 증명



텔넷 자격 증명 및 네트워크 검사 예약

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

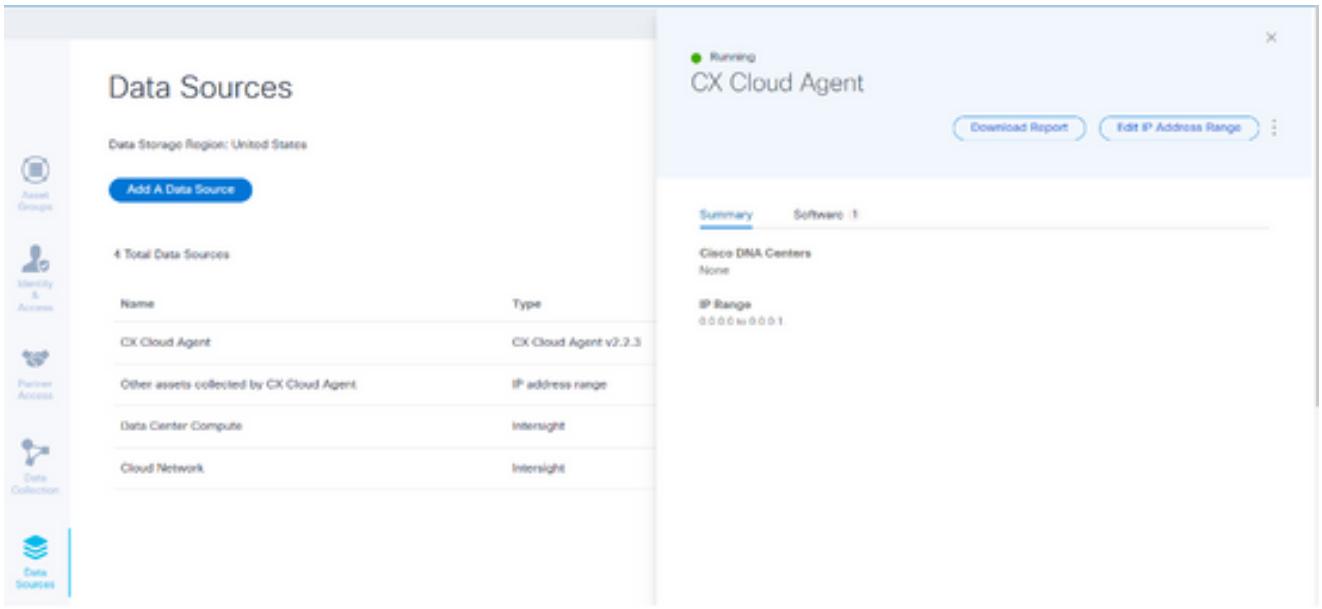


확인

IP 범위 수정

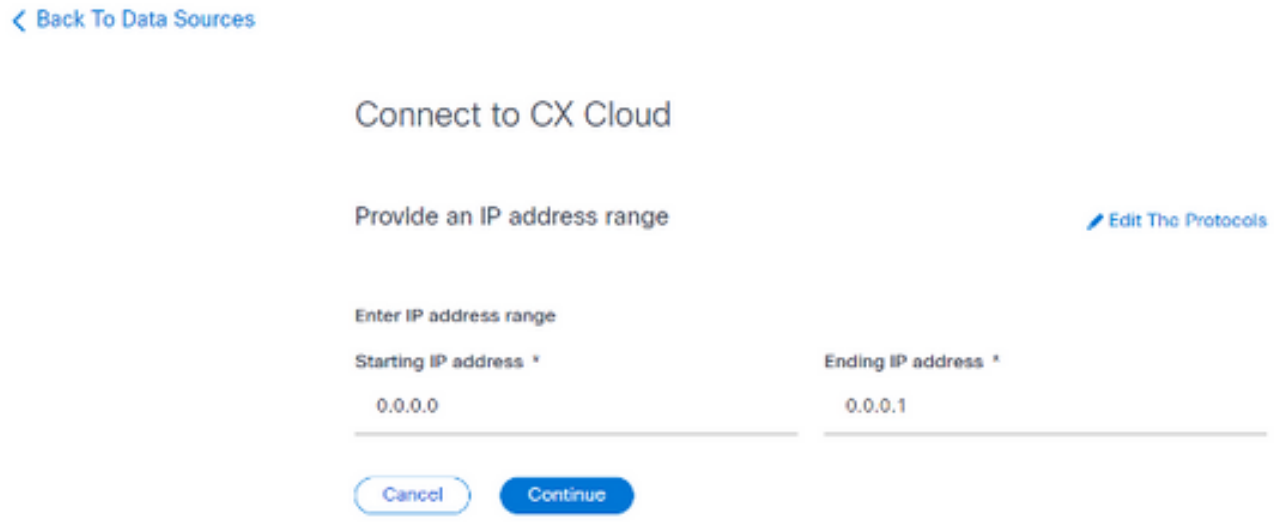
IP 범위를 수정하려면

1. 데이터 소스 창으로 이동합니다.



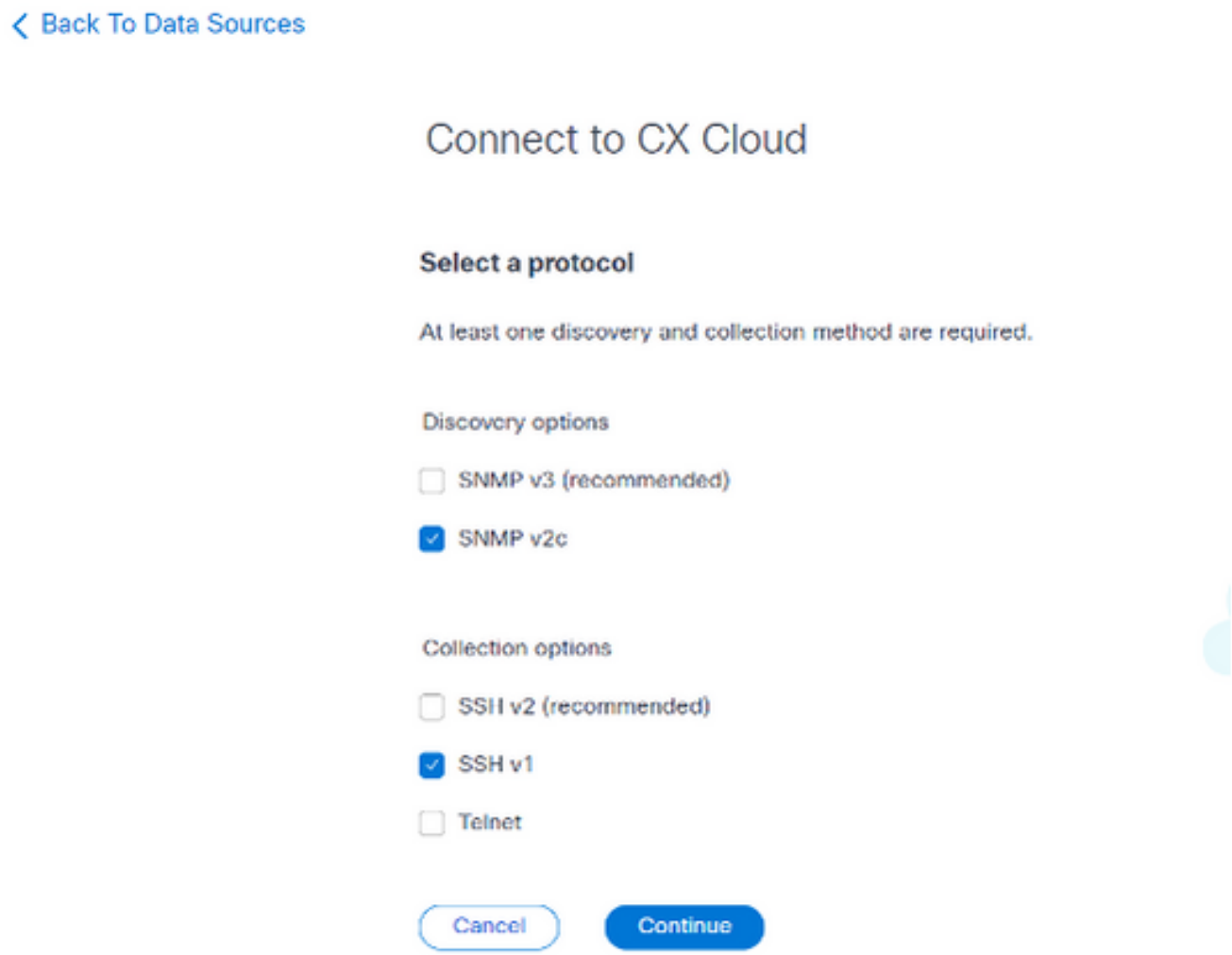
데이터 소스

2. 데이터 소스에서 IP 범위를 수정해야 하는 CX 클라우드 에이전트를 클릭합니다. 세부내용 창이 열립니다.
3. Edit IP Address Range(IP 주소 범위 수정)를 클릭합니다. Connect to CX Cloud(CX 클라우드에 연결) 창이 열립니다.



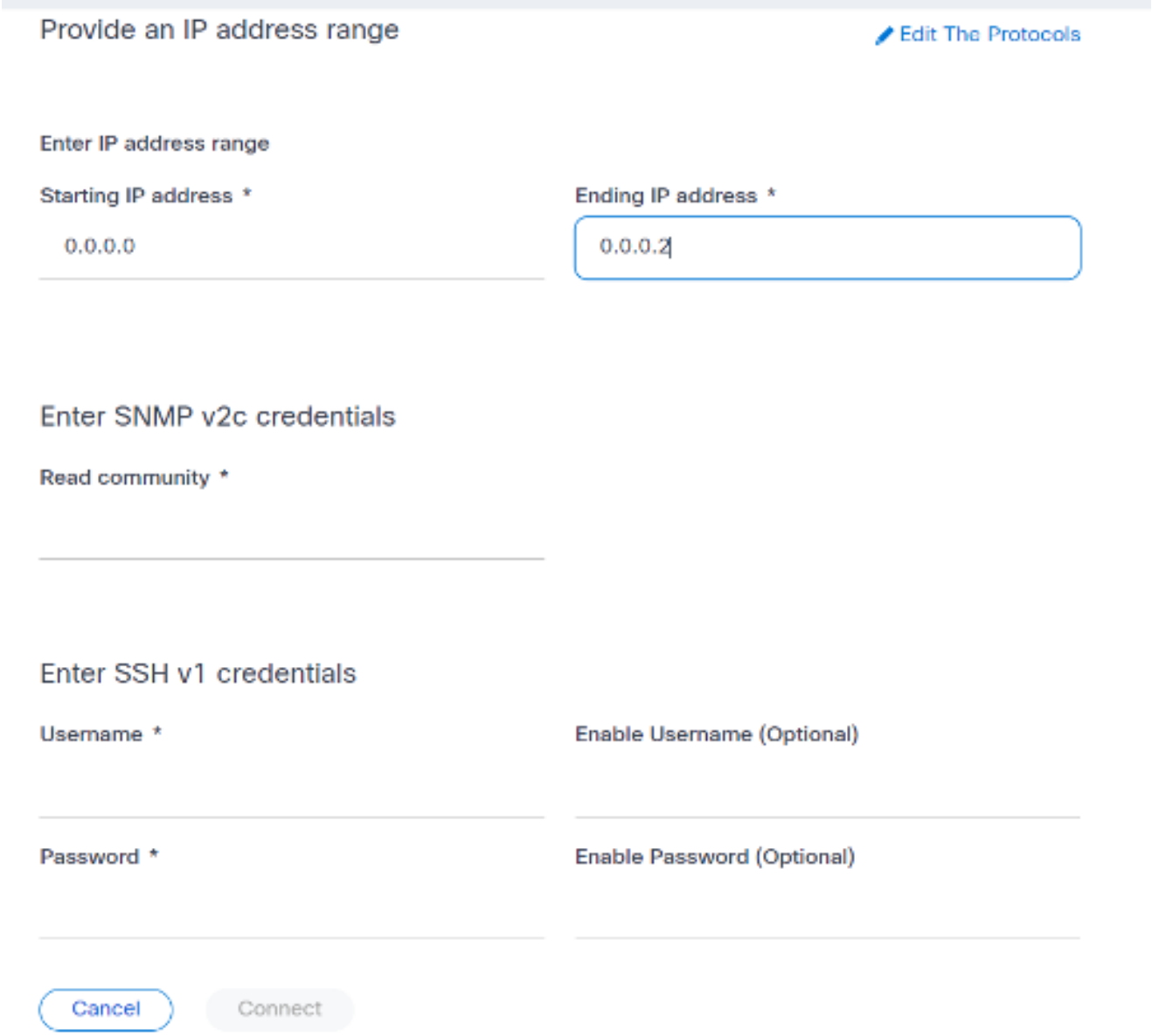
IP 범위 제공

4. Starting IP address(시작 IP 주소) 및 Ending IP address(종료 IP 주소) 필드에서 새 IP를 업데이트합니다.
5. Edit the Protocols 링크를 클릭합니다. Connect to CX Cloud - Select a protocol 창이 열립니다.



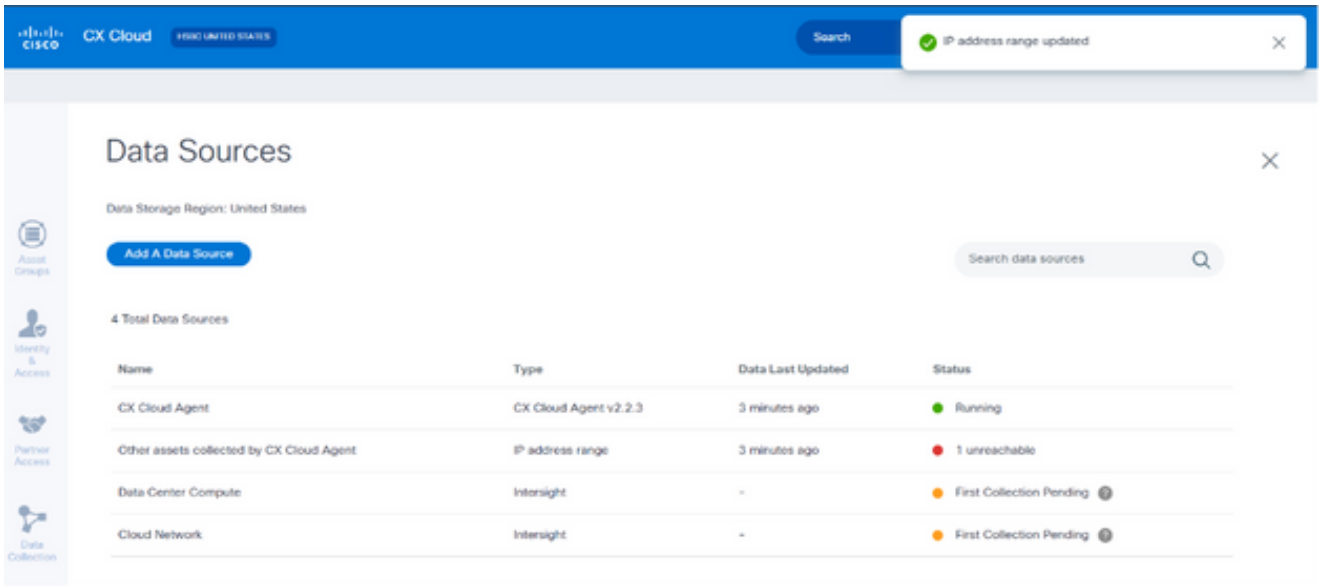
프로토콜 선택

6. 적절한 확인란을 클릭하여 해당 프로토콜을 선택합니다.
7. Continue(계속)를 클릭합니다. Provide an IP address range(IP 주소 범위 제공) 창이 열립니다.



자격 증명 입력

8. 컨피그레이션 자격 증명을 입력합니다.
9. 연결을 클릭합니다. 데이터 소스 창이 열리고 확인 메시지가 표시됩니다.



확인

참고: 확인 메시지는 편집된 범위의 디바이스에 연결할 수 있는지, 자격 증명이 수락되었는지 확인하지 않습니다.

여러 컨트롤러에서 검색된 디바이스 정보

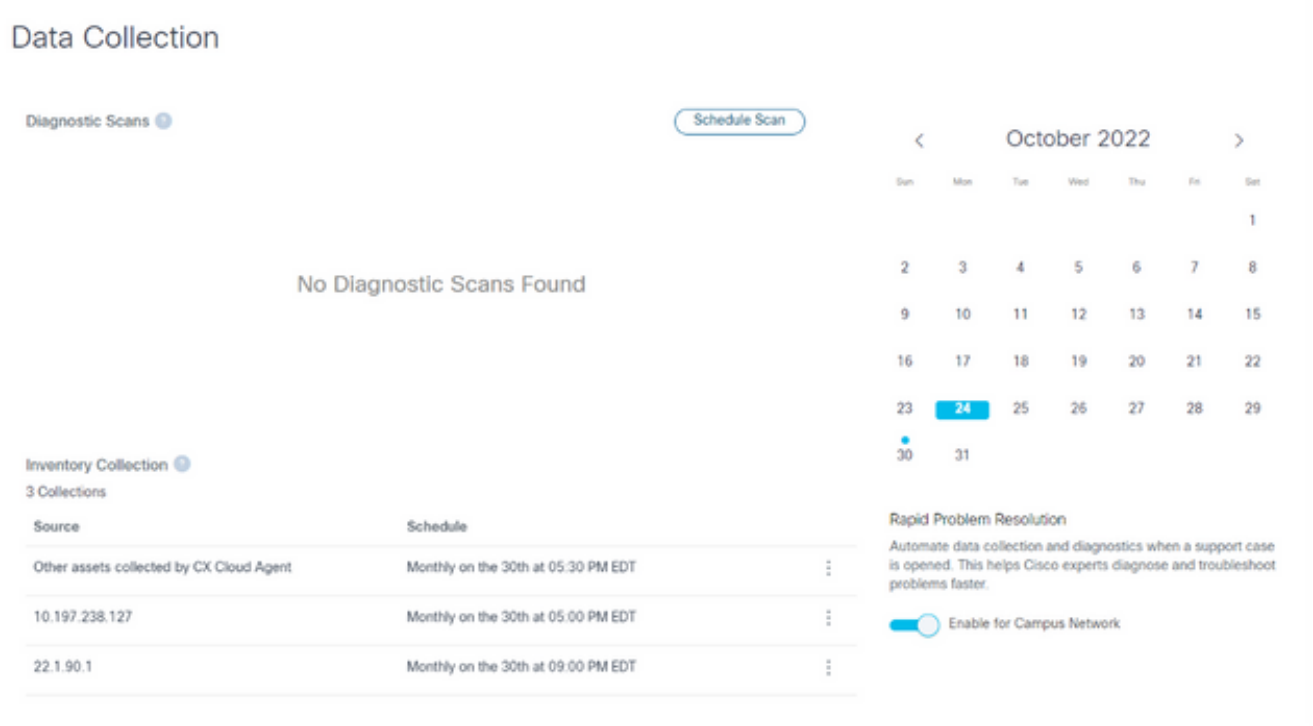
Cisco DNA Center에서 일부 디바이스를 검색하고 CX Cloud Agent에 직접 디바이스를 연결하여 해당 디바이스에서 중복 데이터를 수집할 수 있습니다. 중복 데이터를 수집하고 하나의 컨트롤러로 디바이스를 관리하지 않으려면 CX Cloud Agent에서 디바이스를 관리하는 우선 순위를 결정해야 합니다.

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

진단 검사 예약

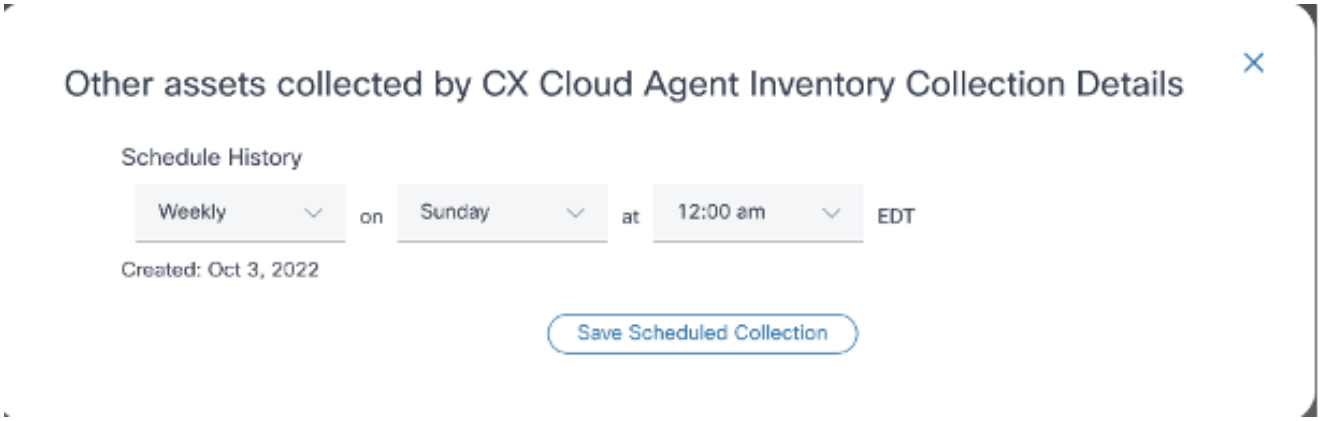
진단 스캔을 예약하려면

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



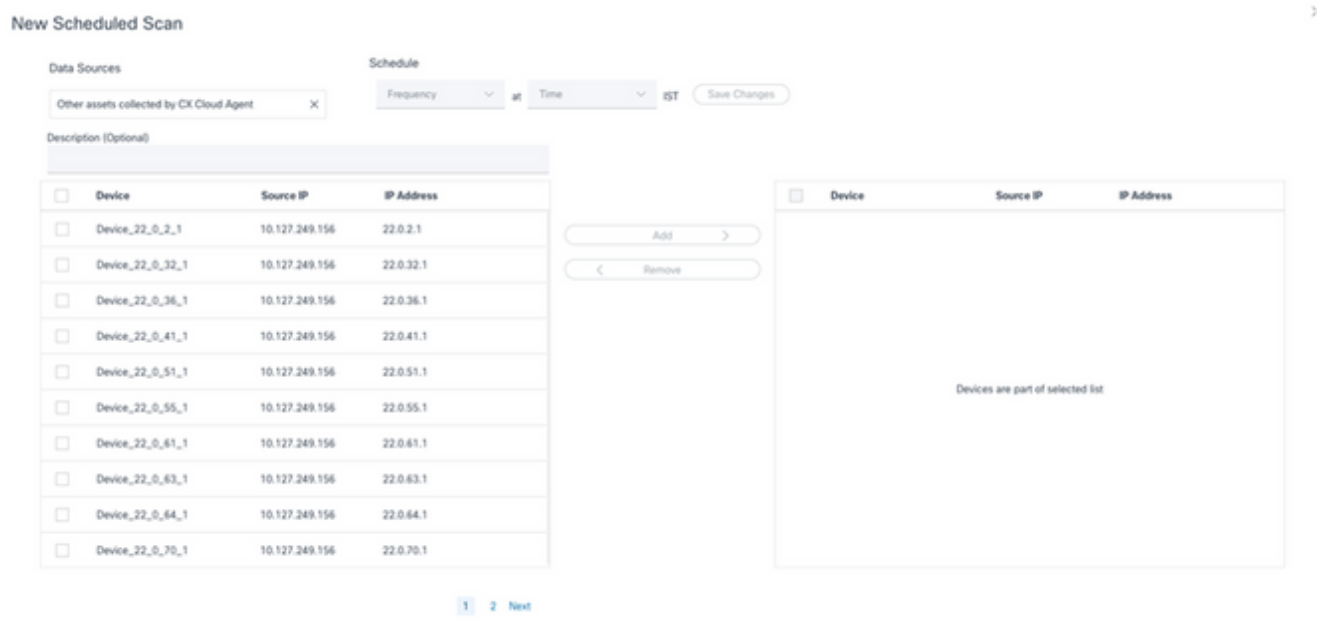
데이터 수집

4. 이 스캔에 대한 일정을 구성합니다.



스캔 일정 구성

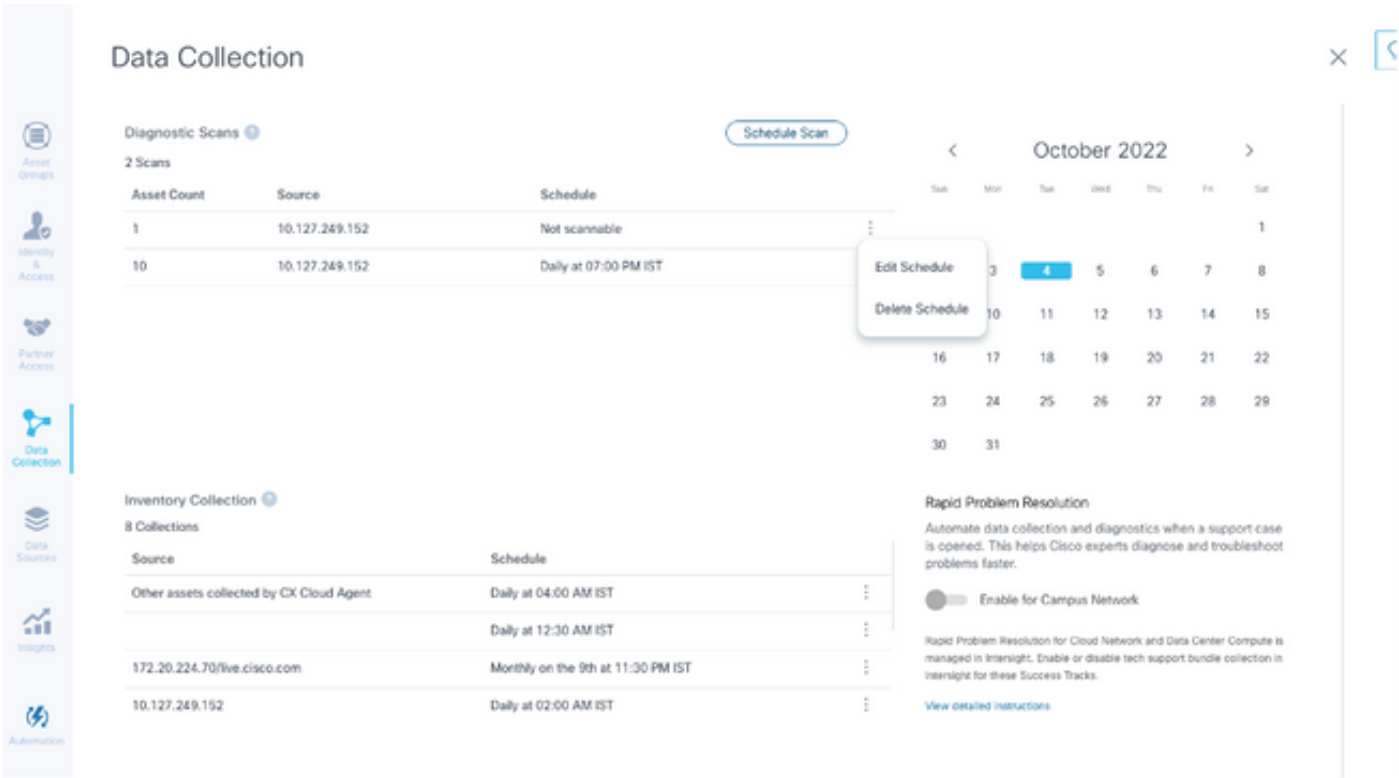
5. Devices(디바이스) 목록에서 스캔할 모든 디바이스를 선택하고 Add(추가)를 클릭합니다.



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

구축 및 네트워크 설정

CX Cloud Agent를 구축하려면 다음 옵션 중 하나를 선택합니다.

- VMware vSphere/vCenter Thick Client ESXi 5.5/6.0을 선택하려면 Thick Client로 이동합니다
- VMware vSphere/vCenter Web Client ESXi 6.0을 선택하려면 Web Client 또는 vSphere Center로 이동합니다
- Oracle Virtual Box 5.2.30을 선택하려면 Oracle VM으로 이동합니다.
- Microsoft Hyper-V를 선택하려면 Hyper-V로 이동하십시오.

OVA 구축

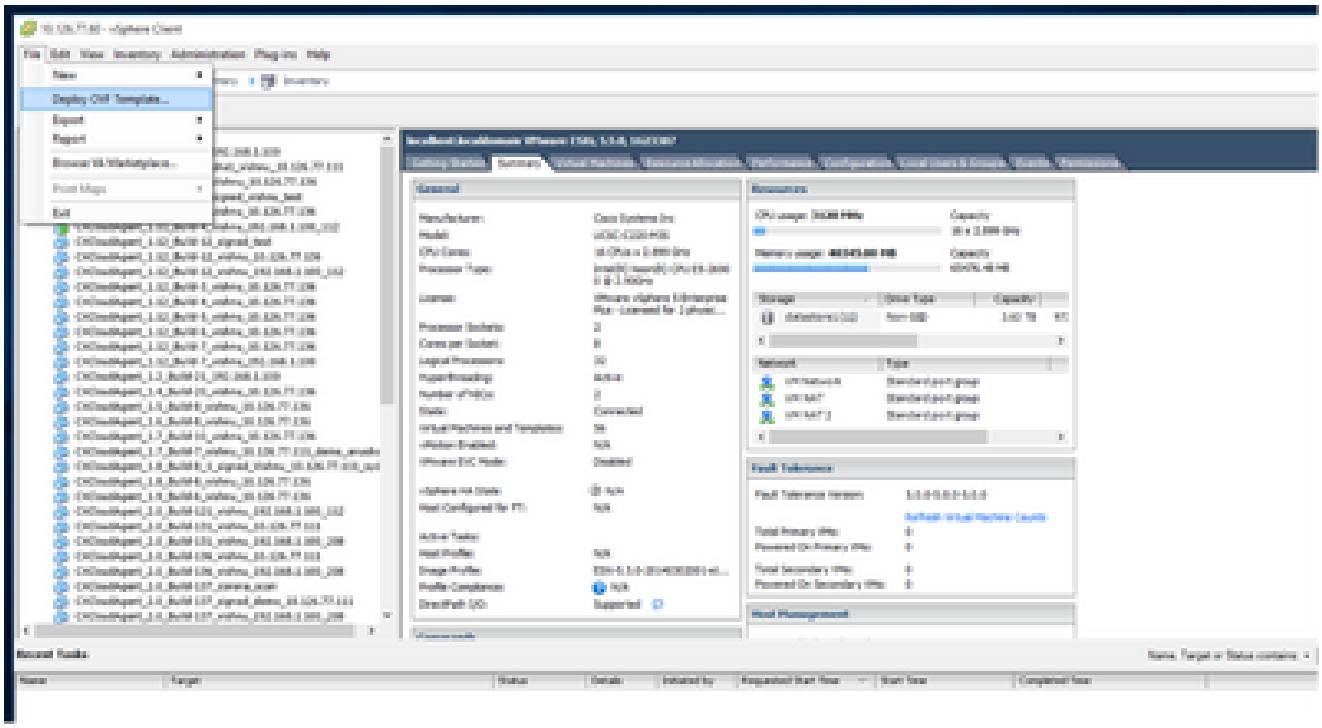
Thick Client ESXi 5.5/6.0 설치

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

1. 이미지를 다운로드한 후 VMware vSphere Client를 시작하고 로그인합니다.

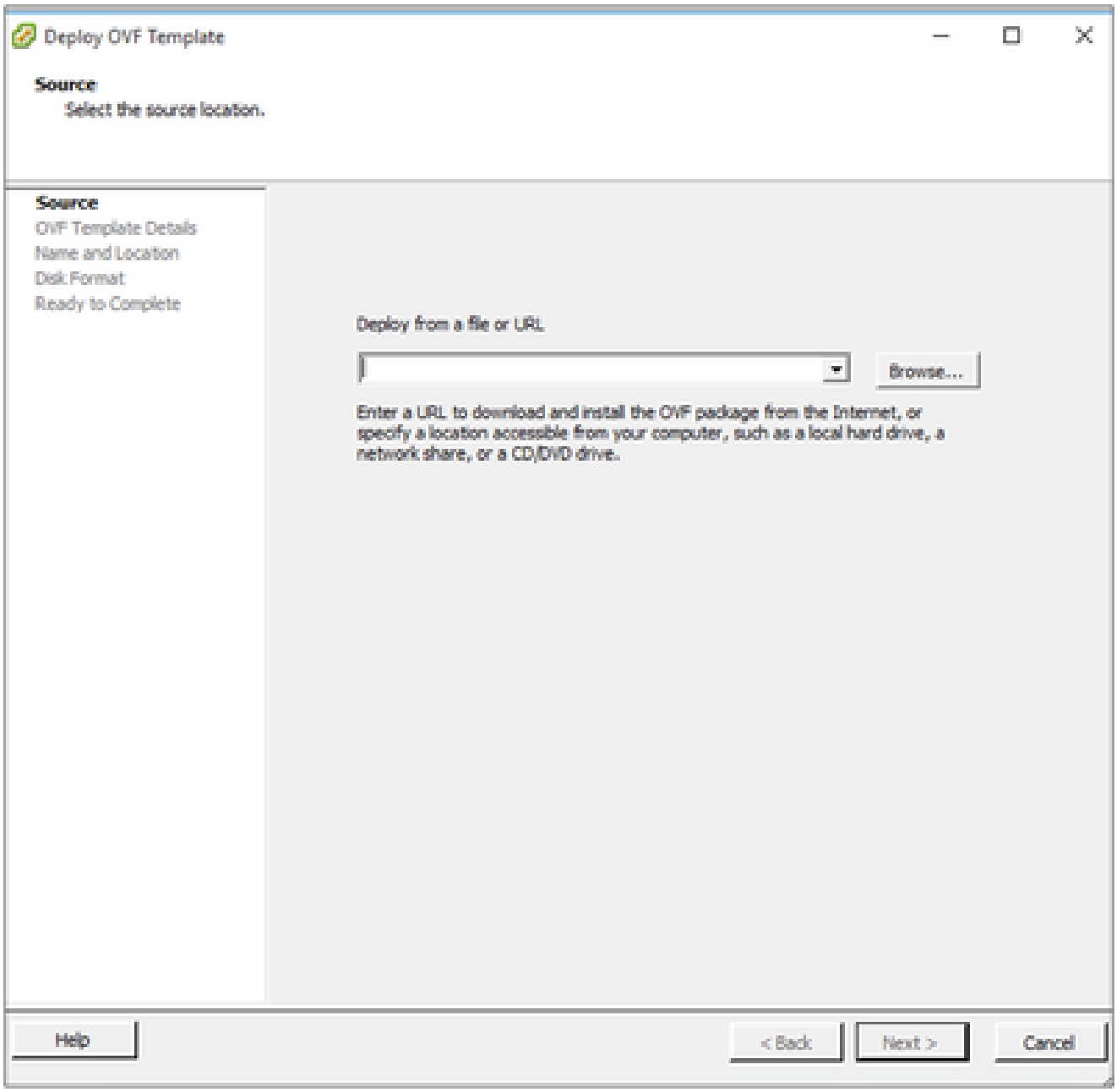
로그인

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



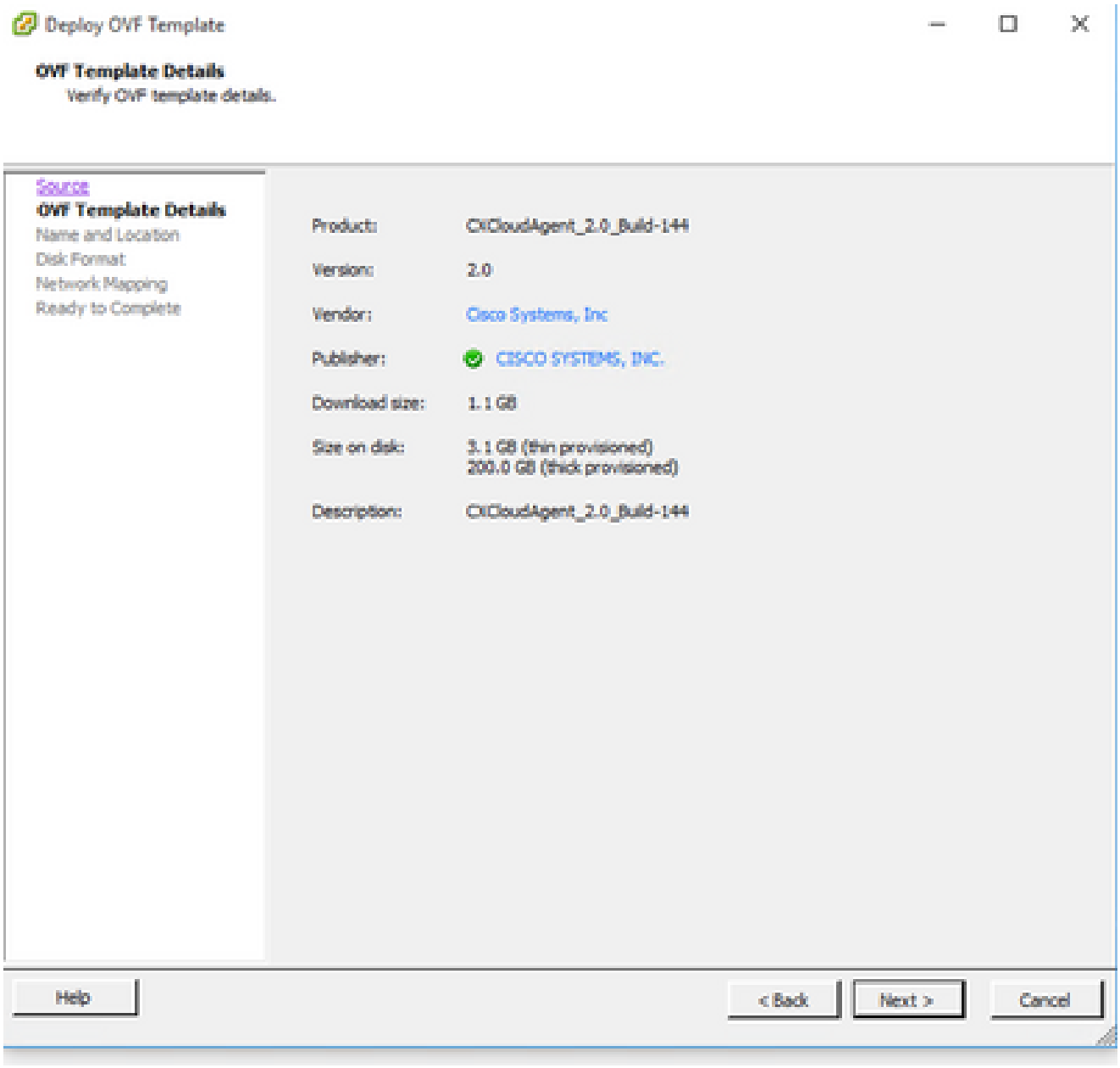
vSphere Client

3. OVA 파일을 찾아 선택하고 Next(다음)를 클릭합니다.



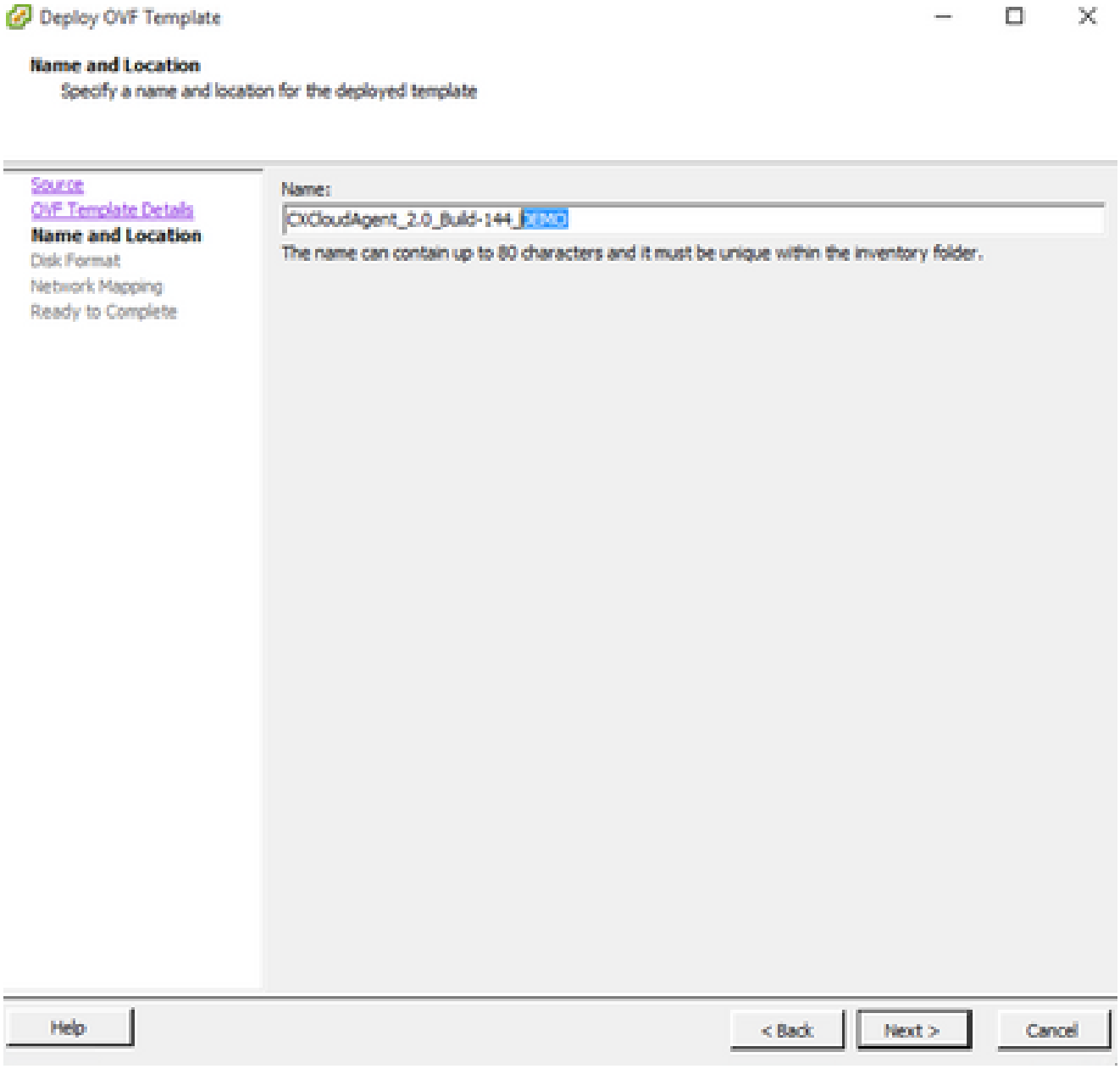
OVA 경로

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



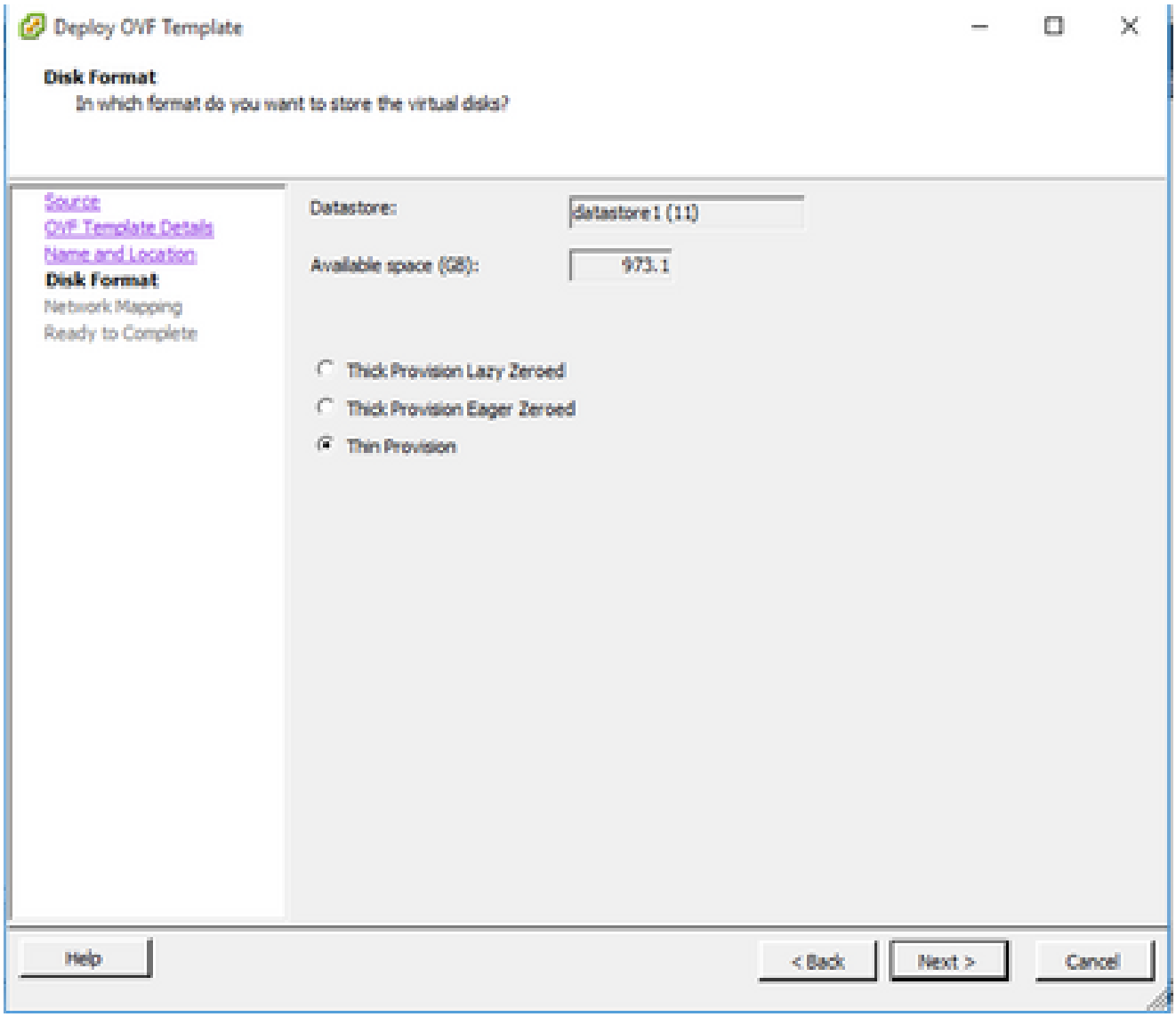
템플릿 세부 정보

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



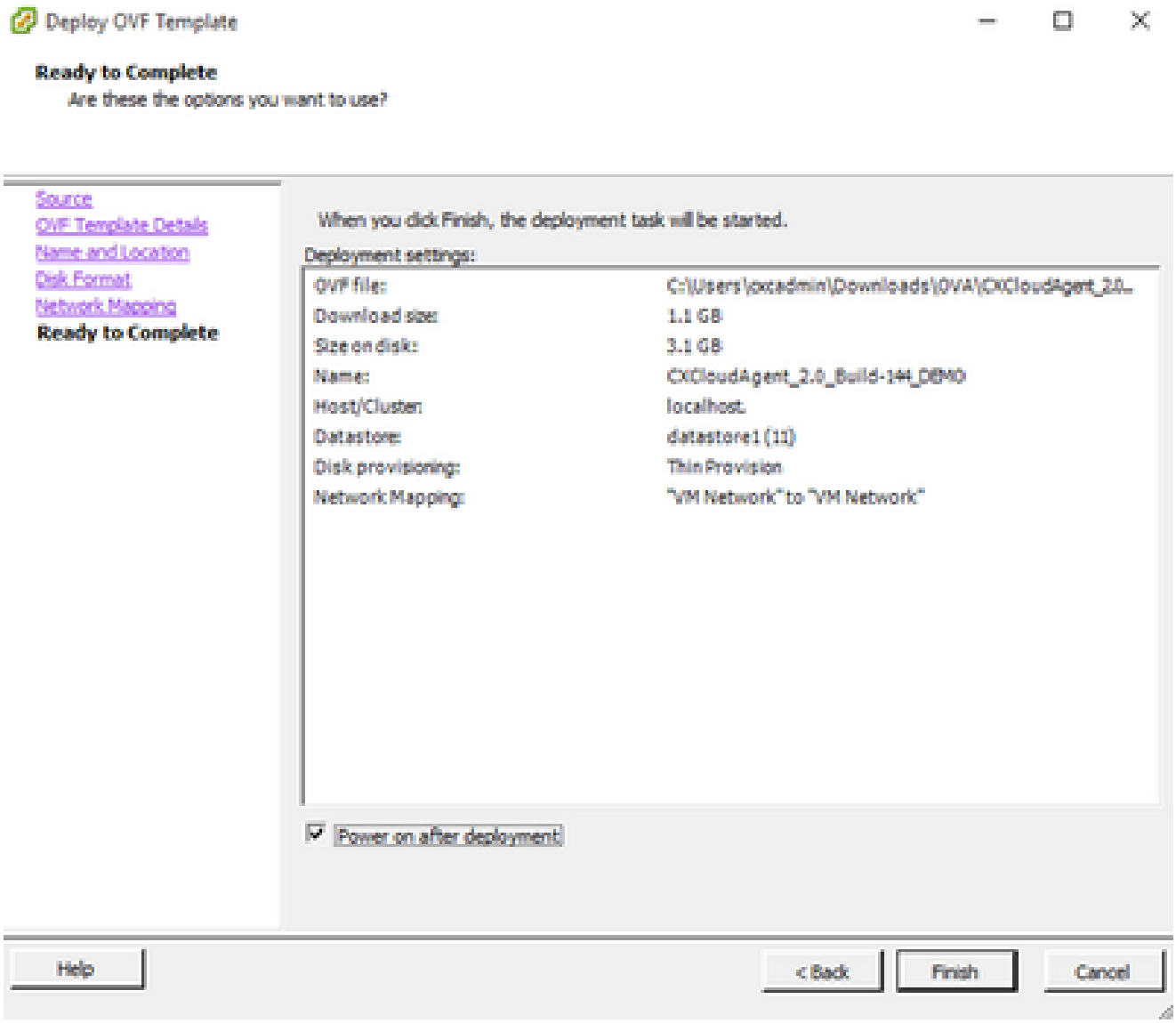
이름 및 위치

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



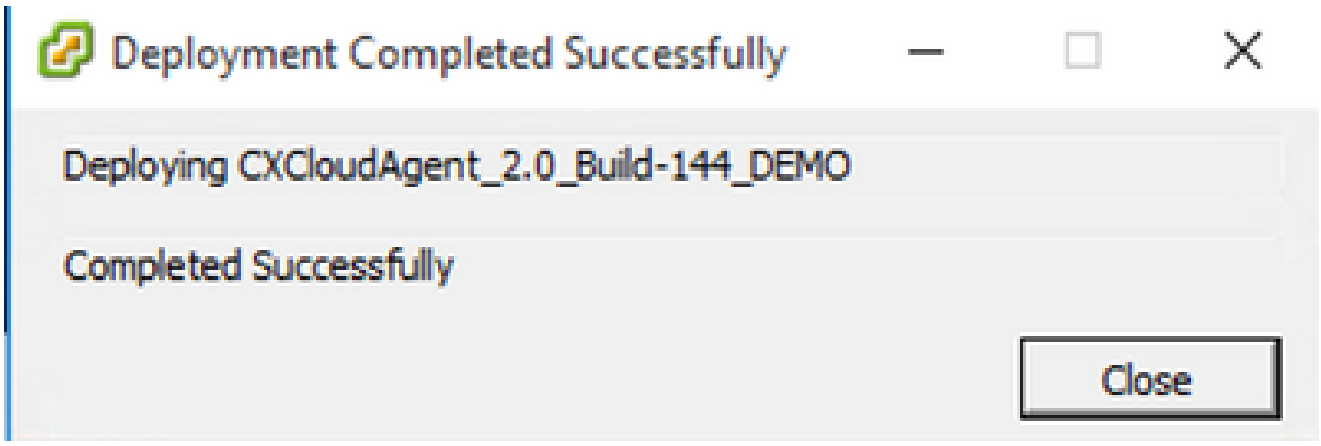
디스크 형식

7. Power on after deployment(구축 후 전원 켜기) 확인란을 선택하고 닫아



완료 준비

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



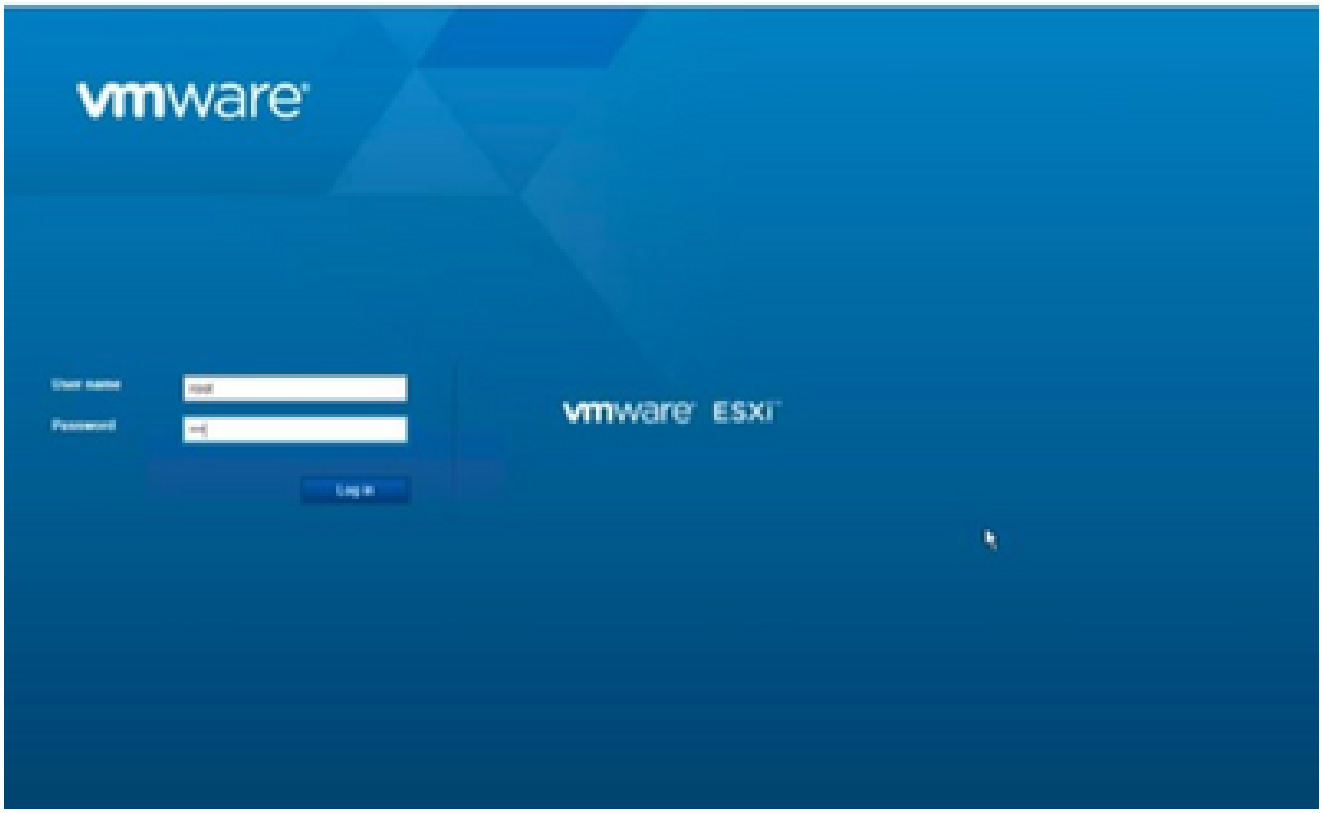
구축 완료

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

Web Client ESXi 6.0 설치

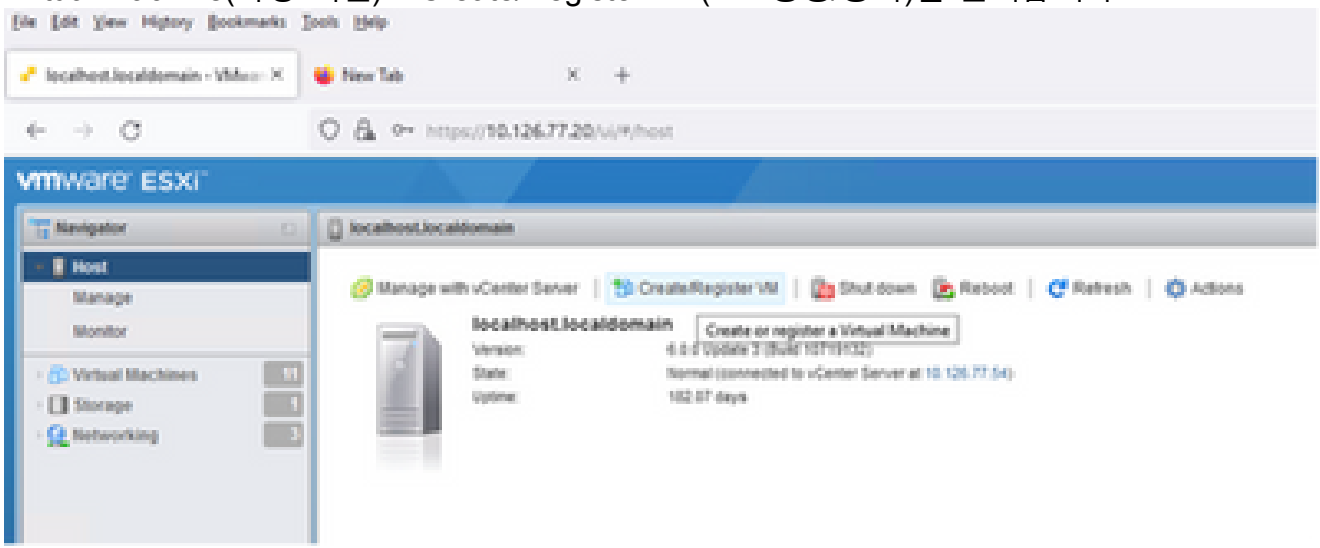
이 클라이언트는 vSphere 웹을 사용하여 CX 클라우드 에이전트 OVA를 구축합니다.

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



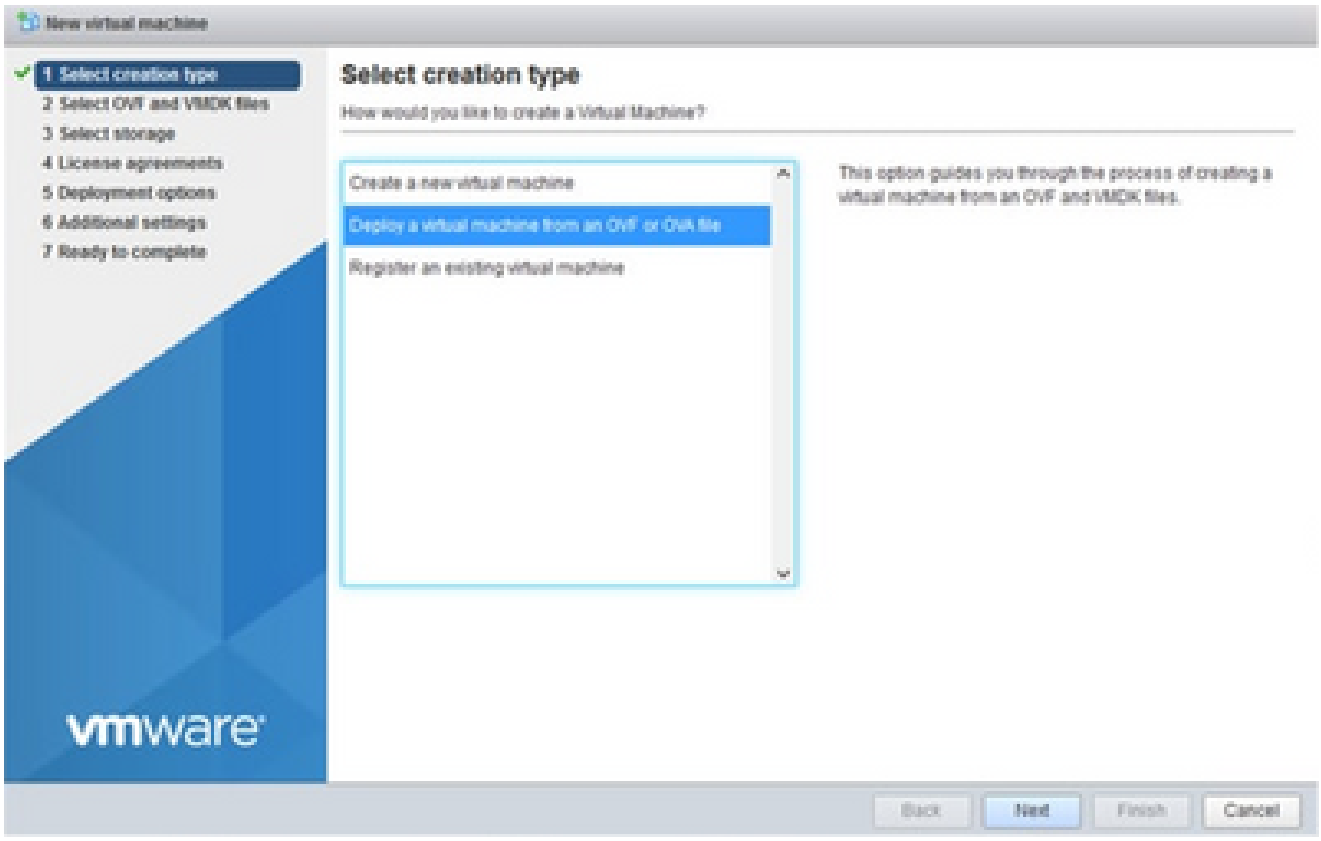
VMware ESXi 로그인

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



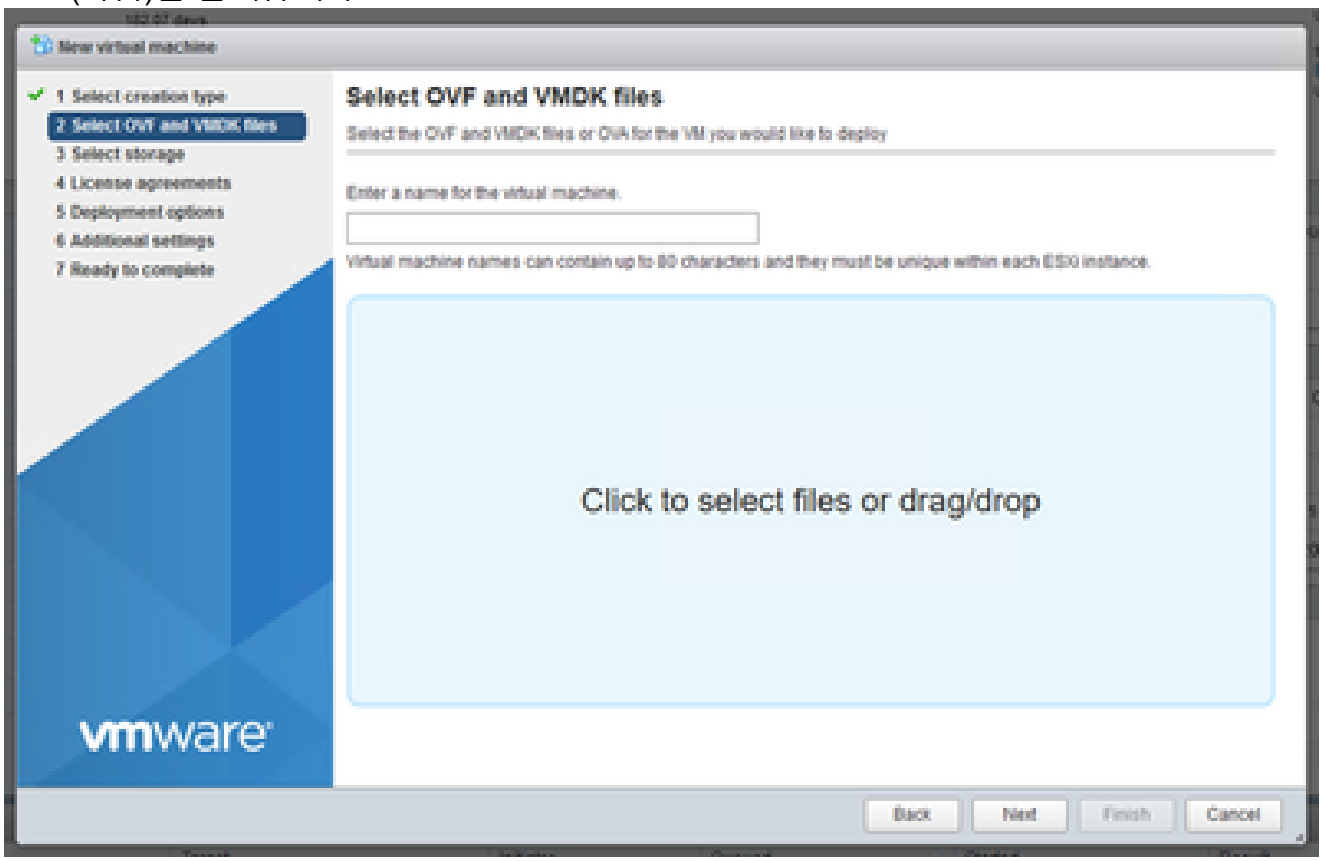
VM 생성

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



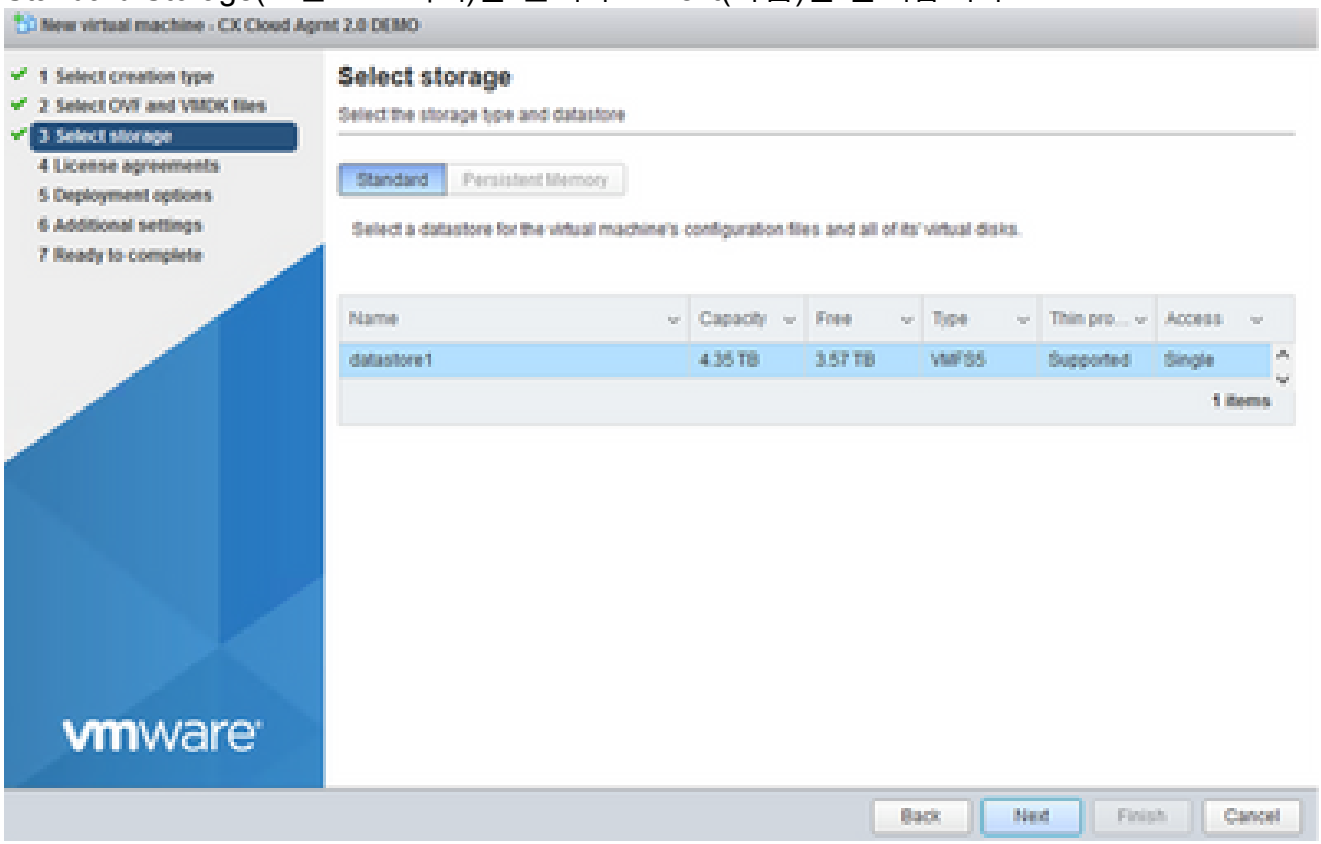
생성 유형 선택

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



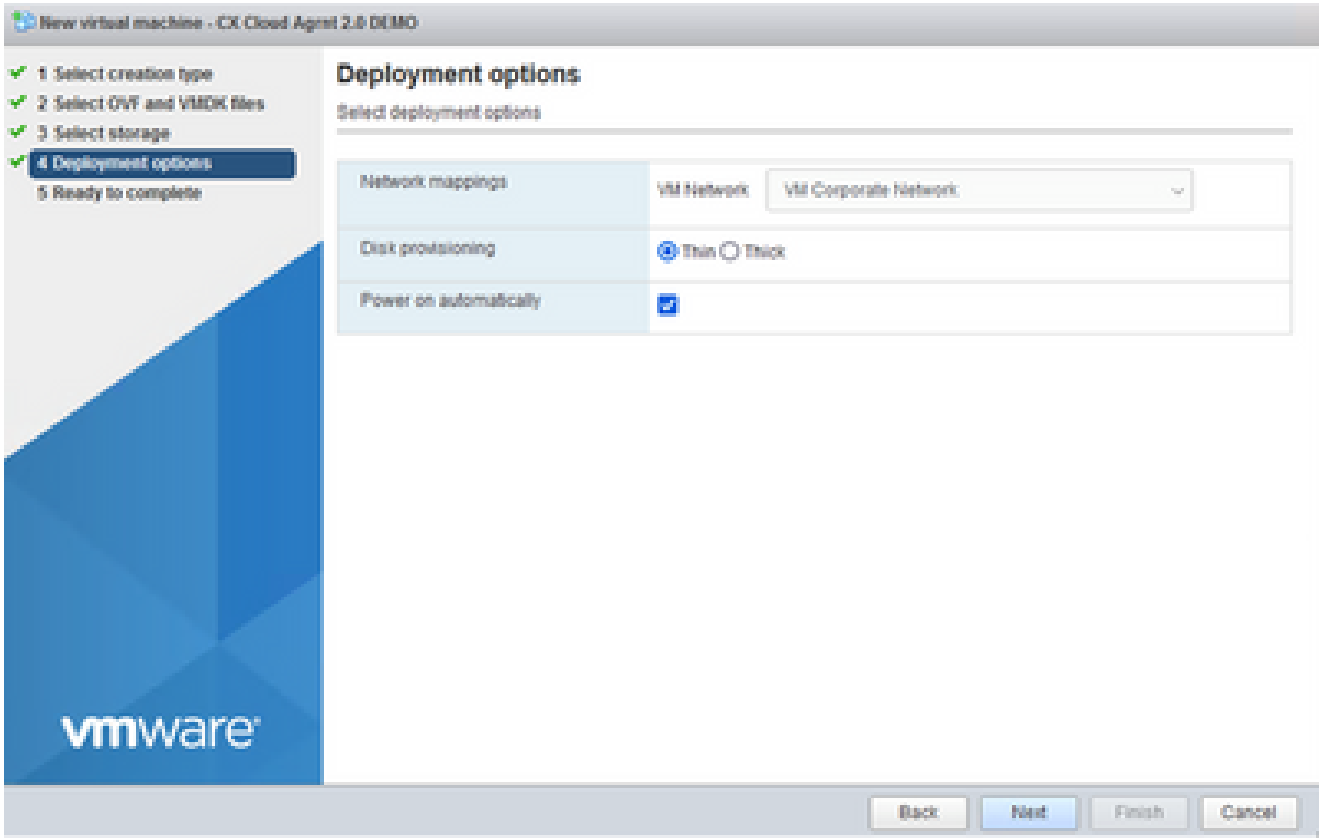
OVA 선택

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



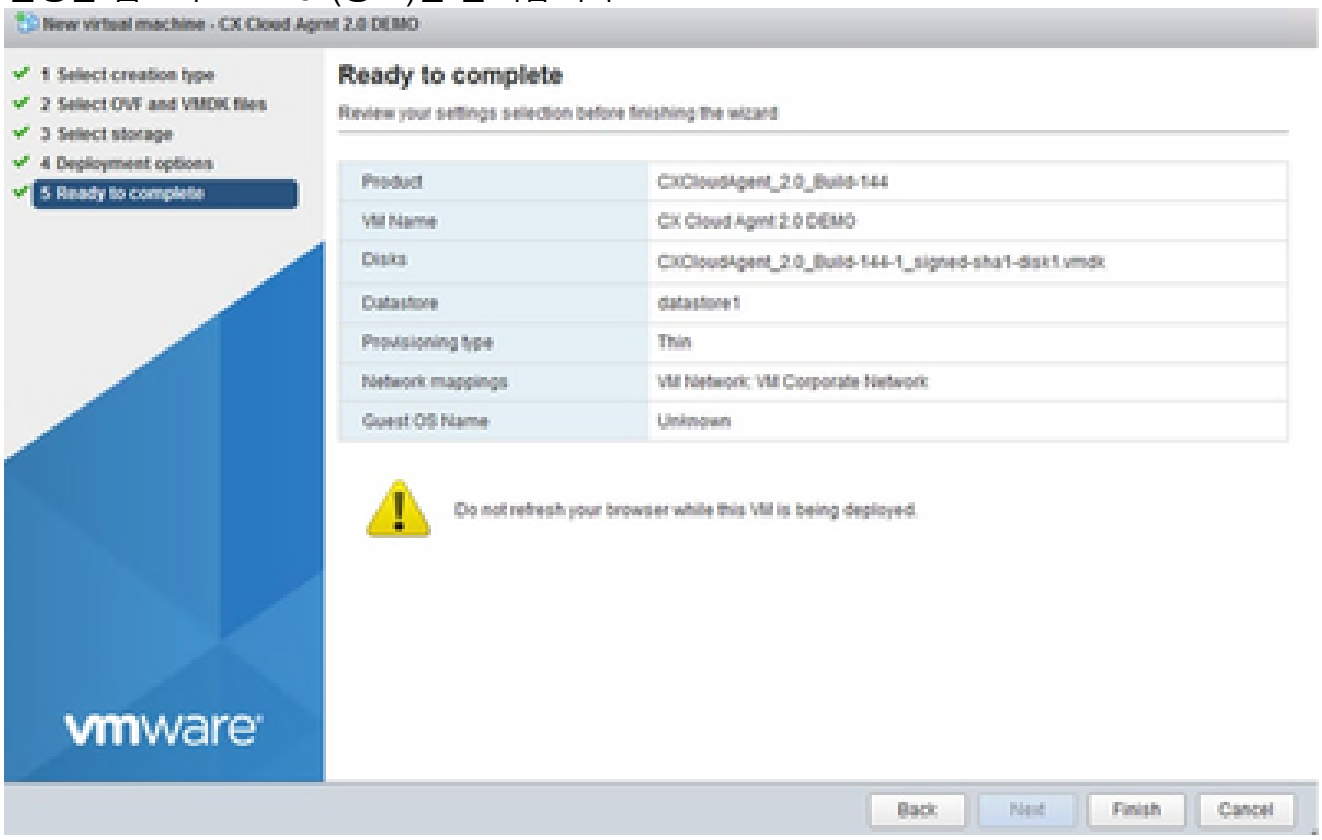
스토리지 선택

7. 적절한 구축 옵션을 선택하고 다음을 클릭합니다. 다음 단계.

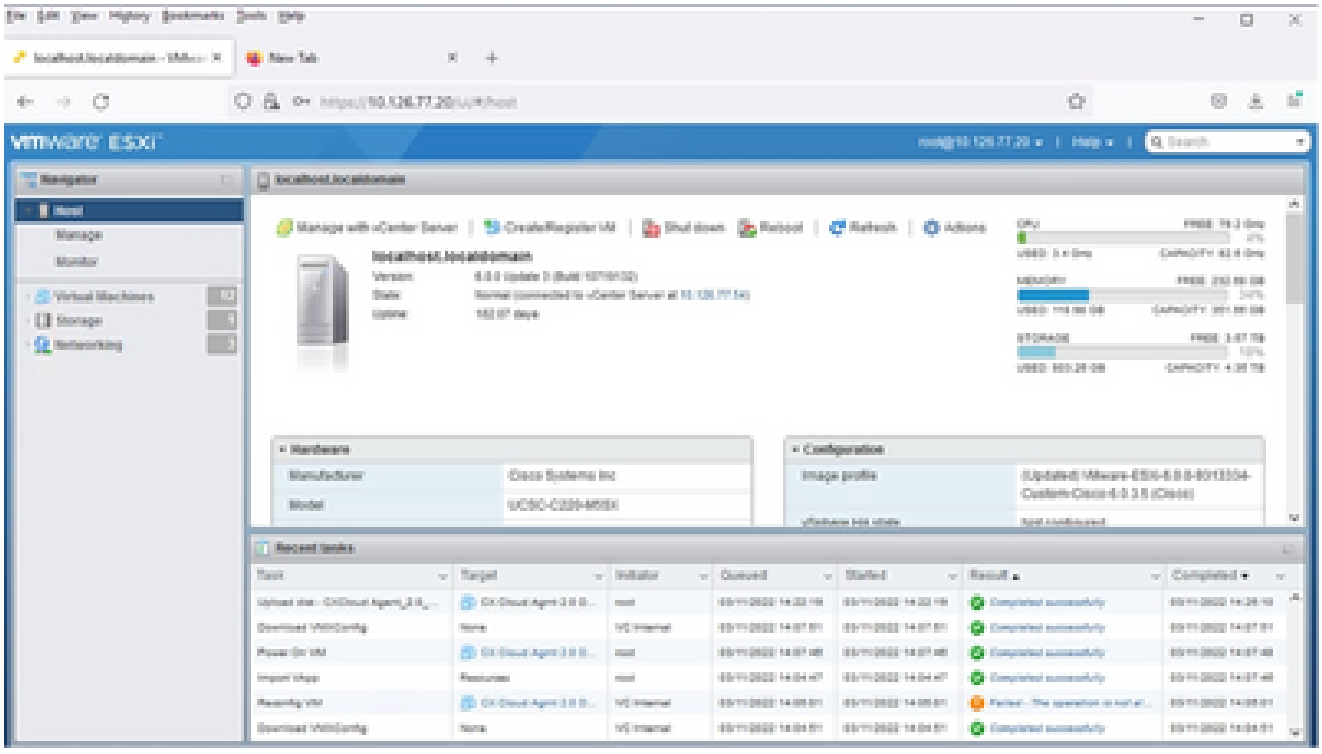


구축 옵션

8. 설정을 검토하고 Finish(종료)를 클릭합니다.

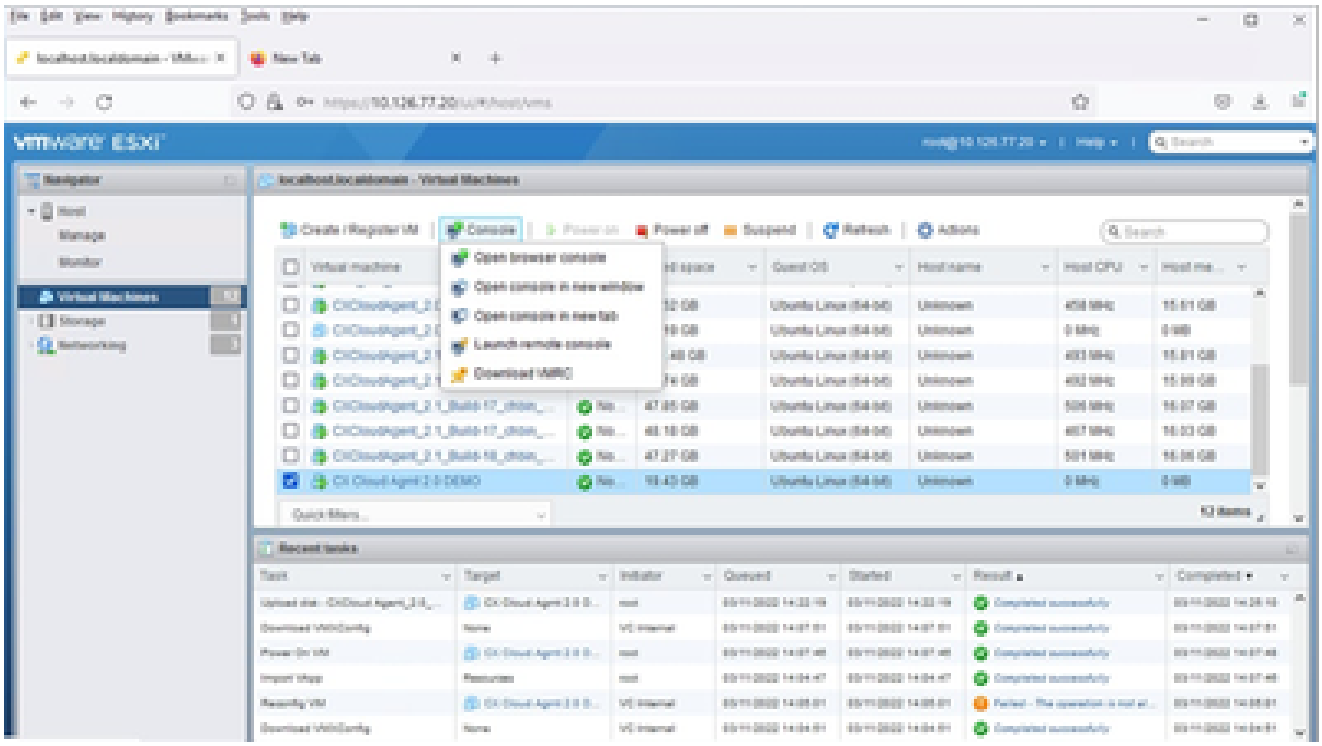


완료 준비



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.

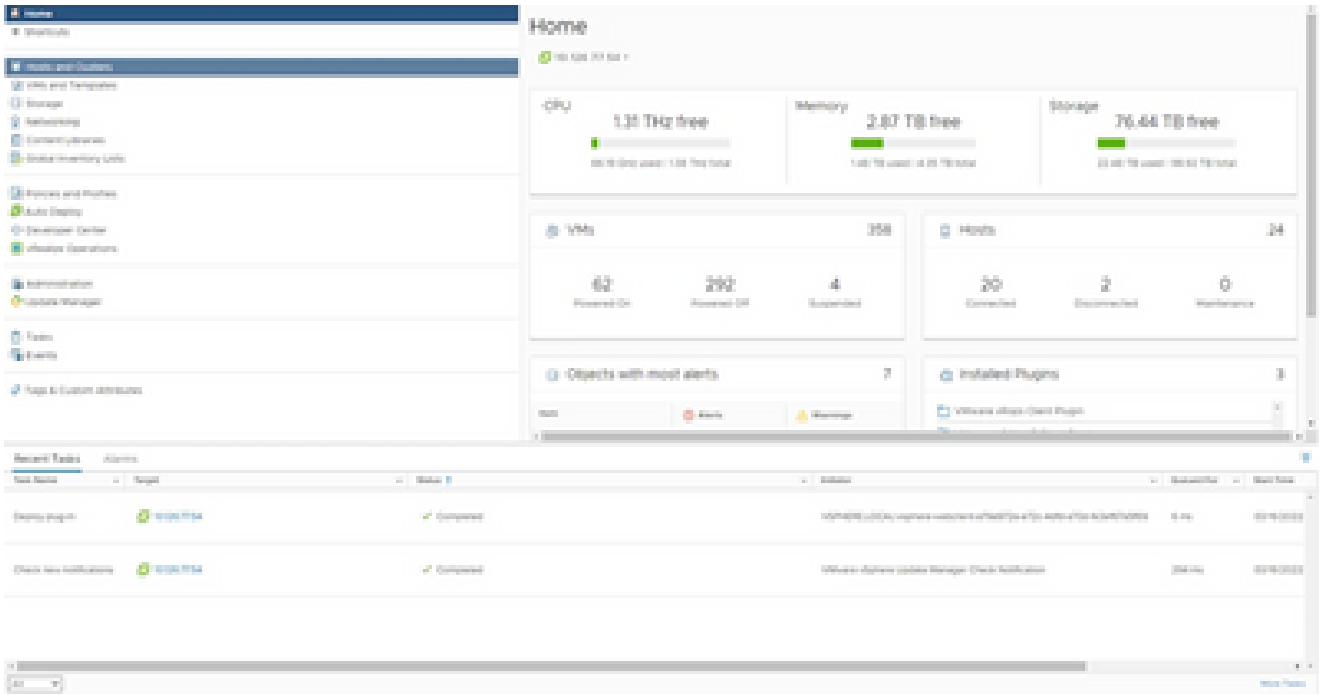
Web Client vCenter 설치

다음을 수행합니다.

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

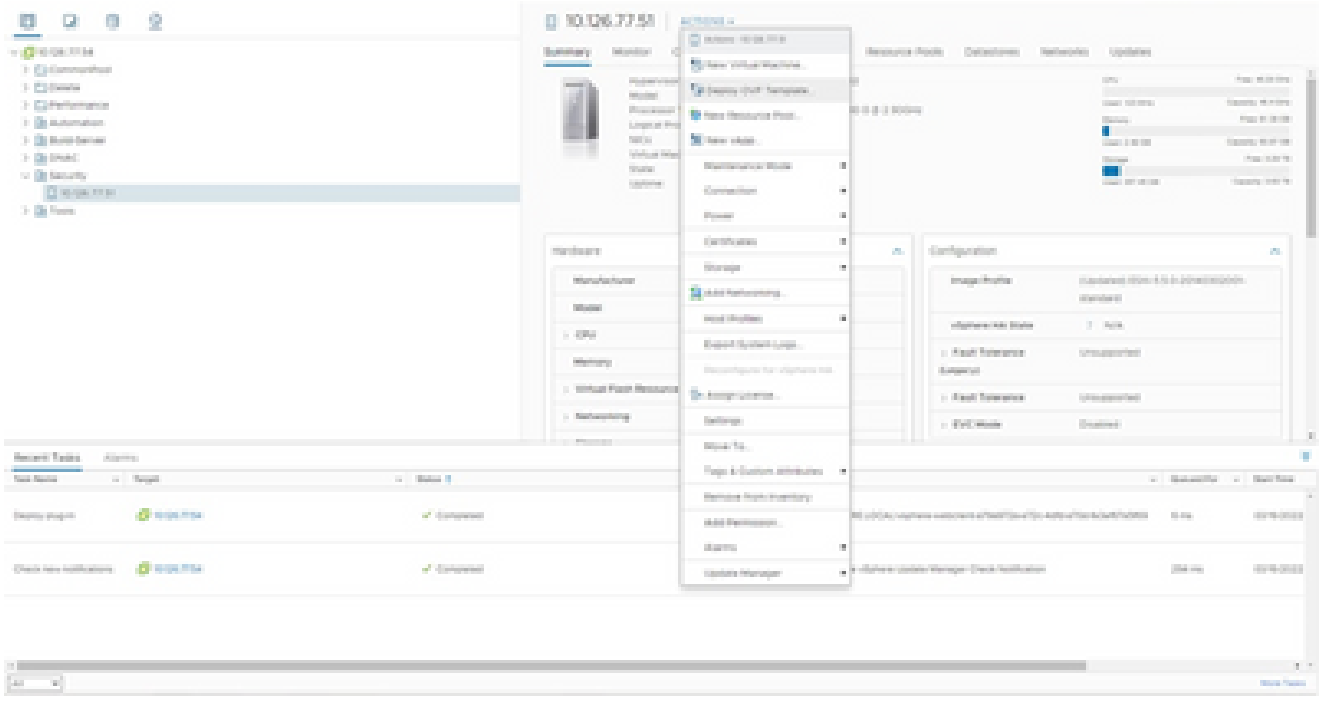
로그인

2. 홈 페이지에서 호스트 및 클러스터를 누릅니다.

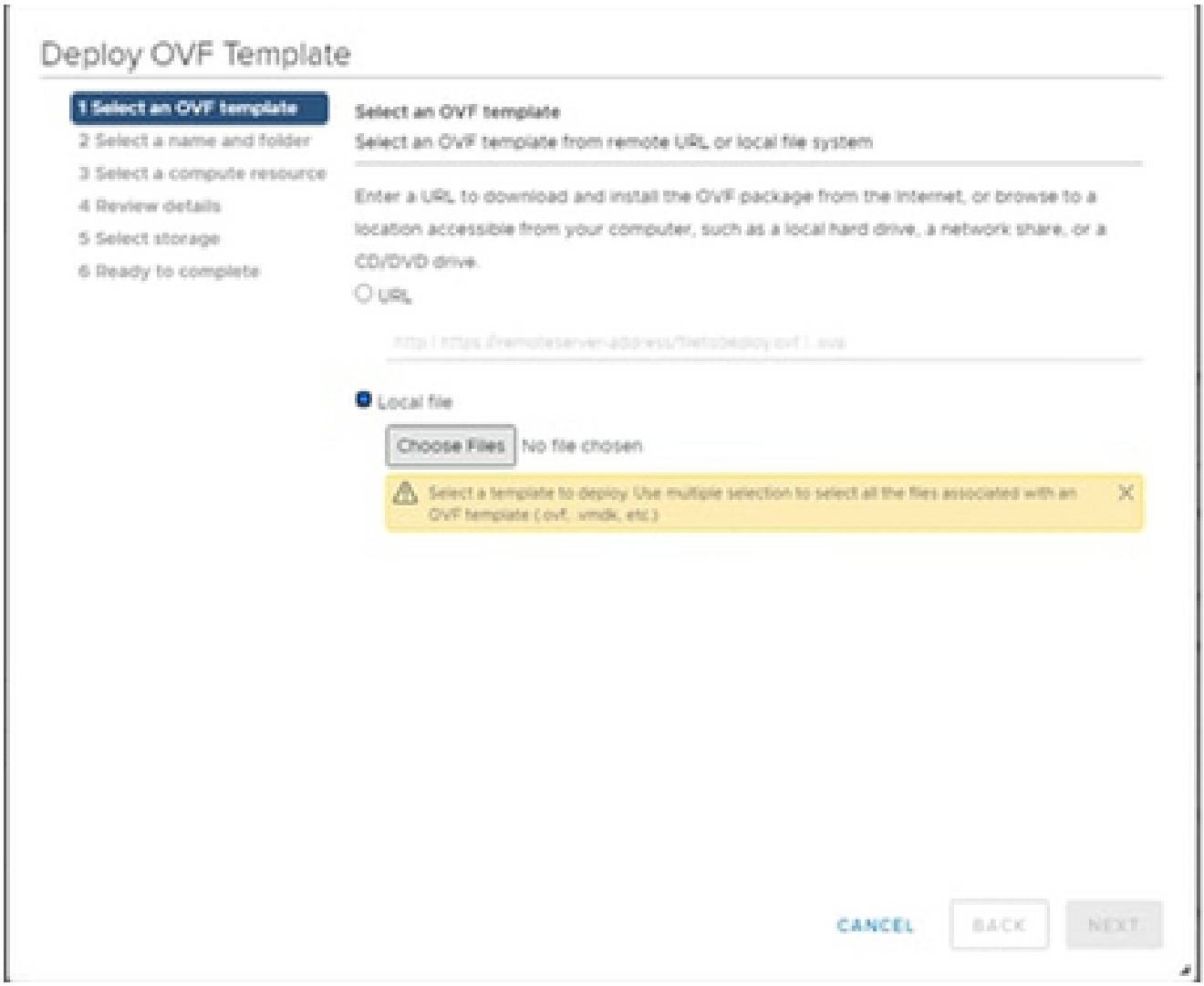


홈 페이지

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

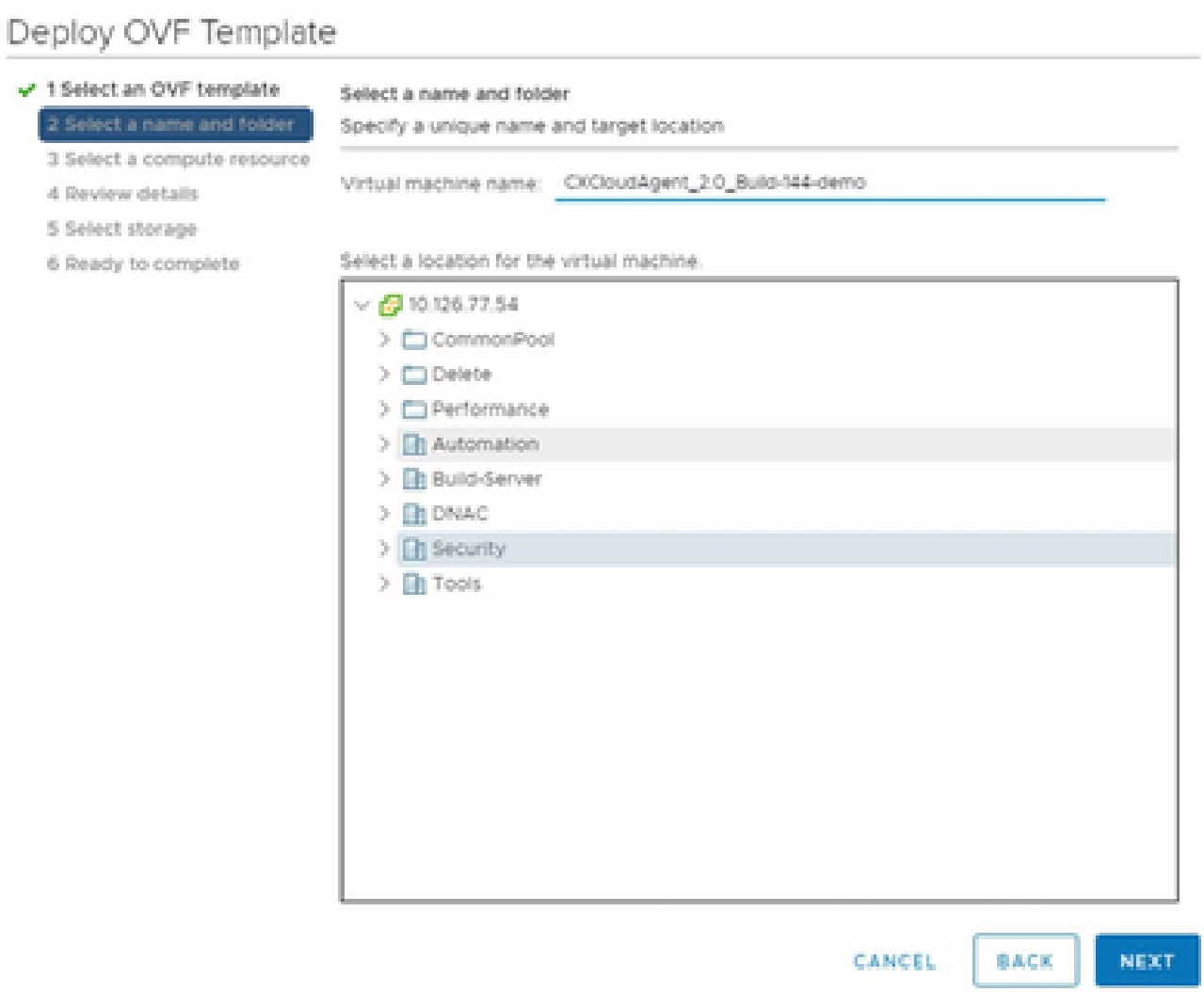


작업



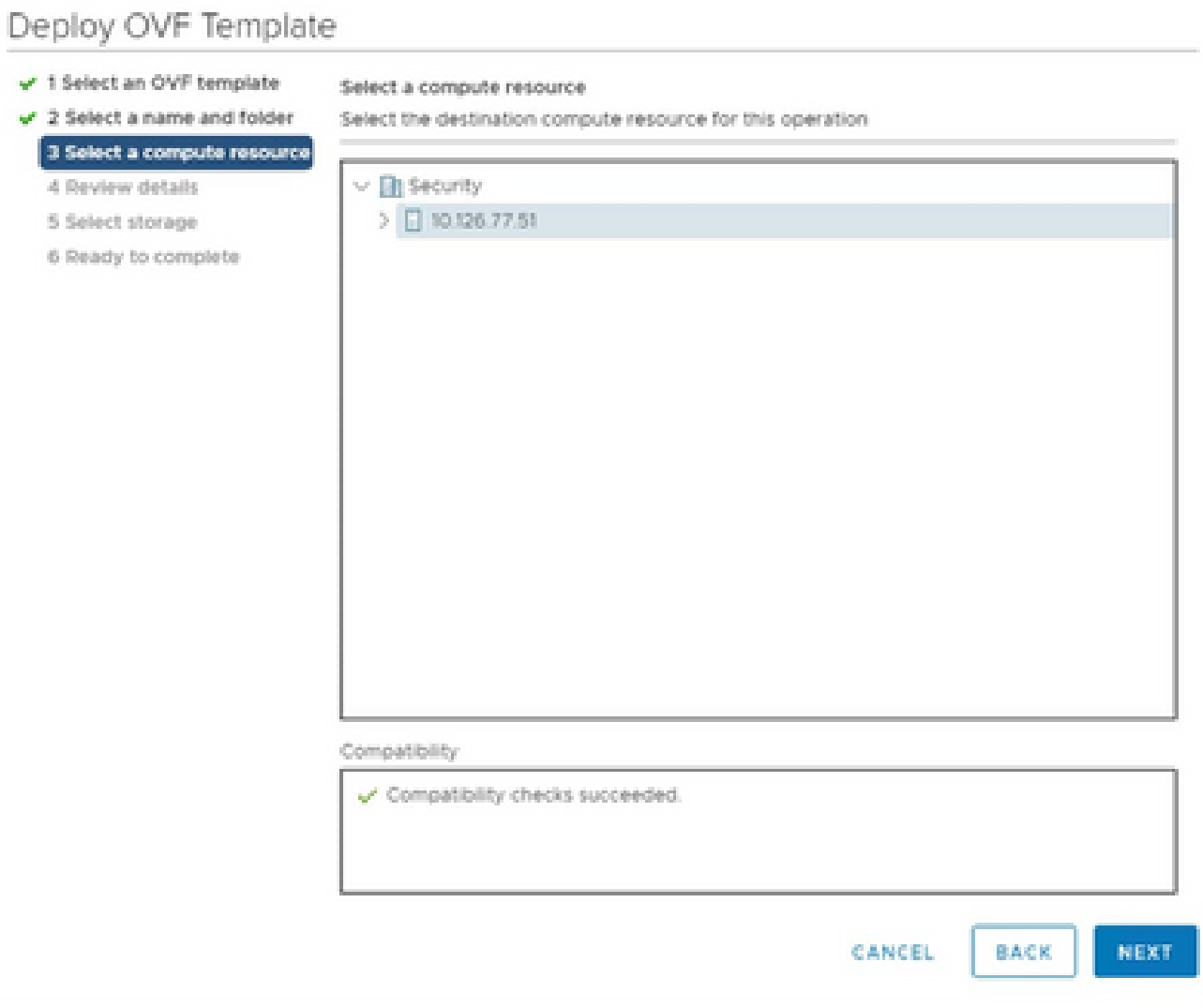
템플릿 선택

4. URL을 직접 추가하거나 OVA 파일을 찾아 선택하고 Next(다음)를 클릭합니다.
5. 고유한 이름을 입력하고 필요한 경우 위치를 찾습니다.
6. Next(다음)를 클릭합니다.



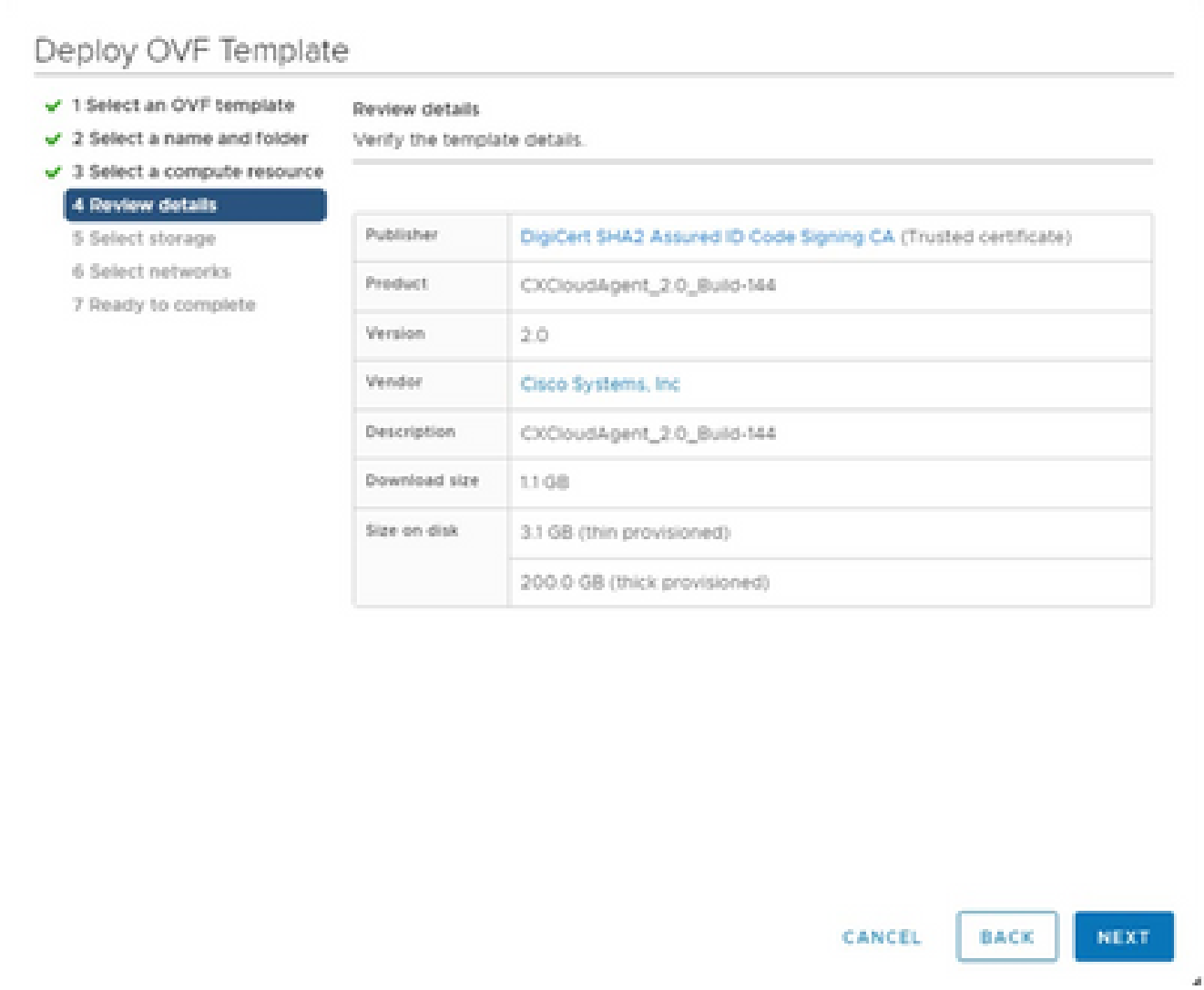
이름 및 폴더

7. 컴퓨팅 리소스를 선택하고 다음을 누릅니다.



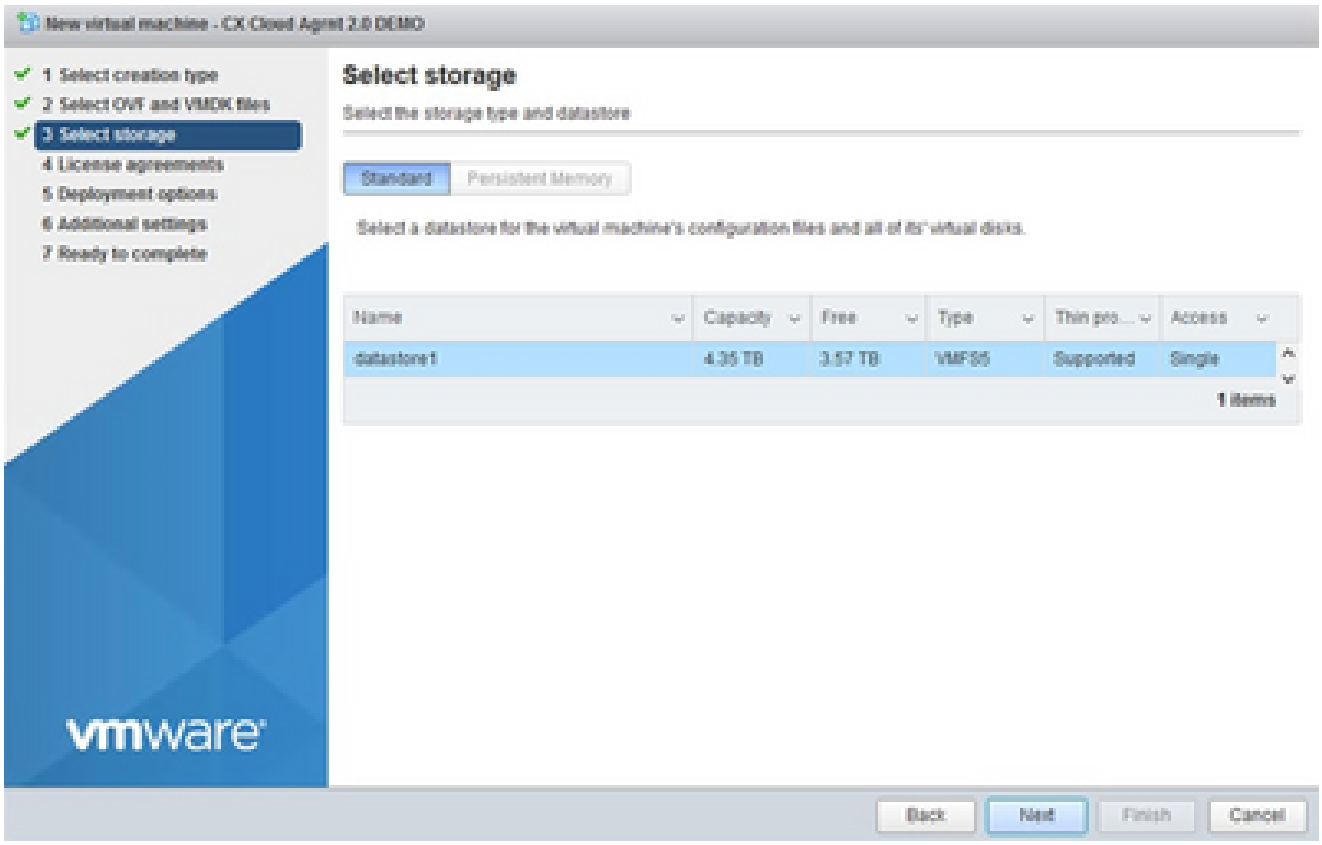
컴퓨터 리소스 선택

8. 세부 정보를 검토하고 Next(다음)를 클릭합니다.



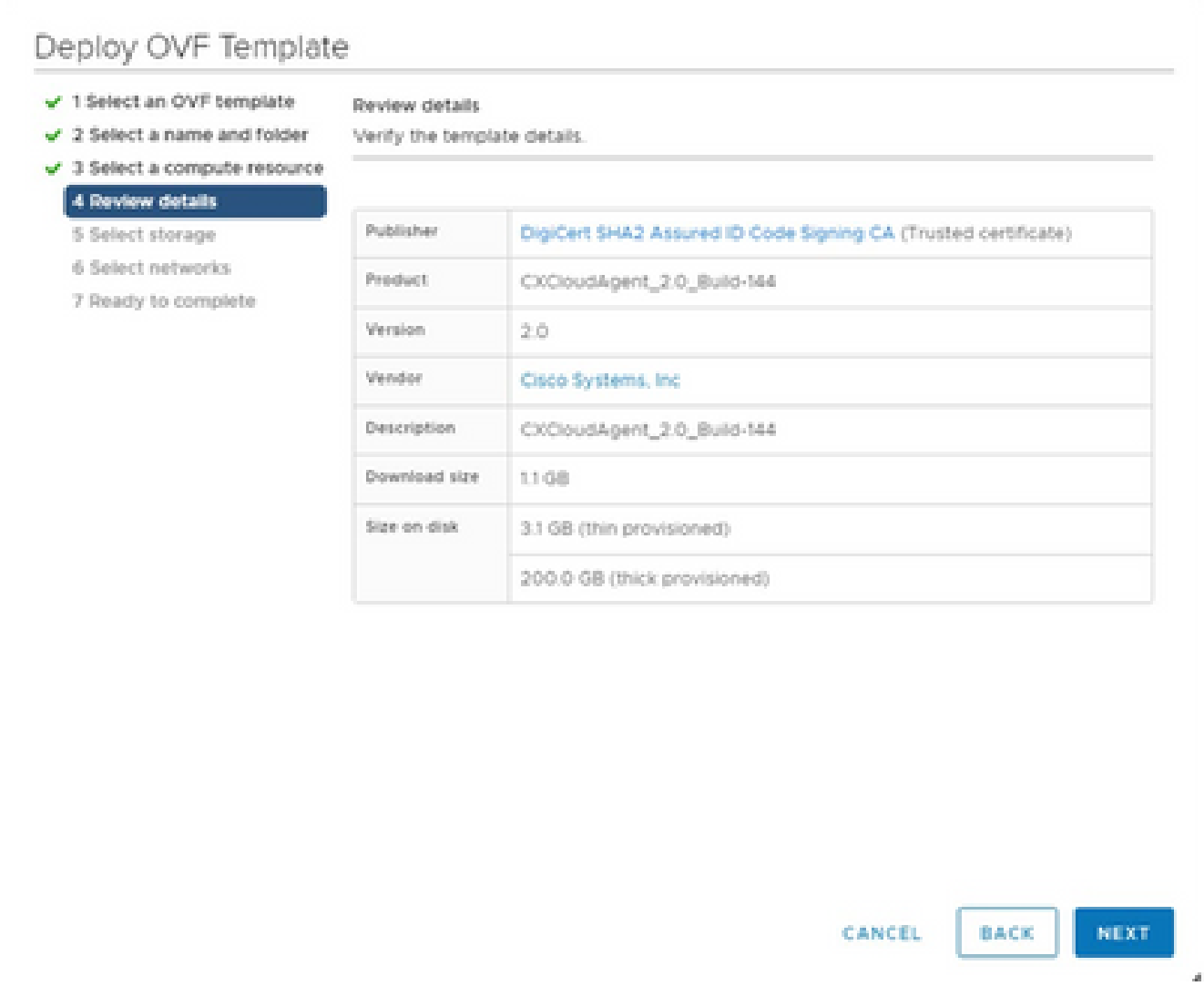
세부 사항 검토

9. 가상 디스크 형식을 선택하고 Next(다음)를 클릭합니다.



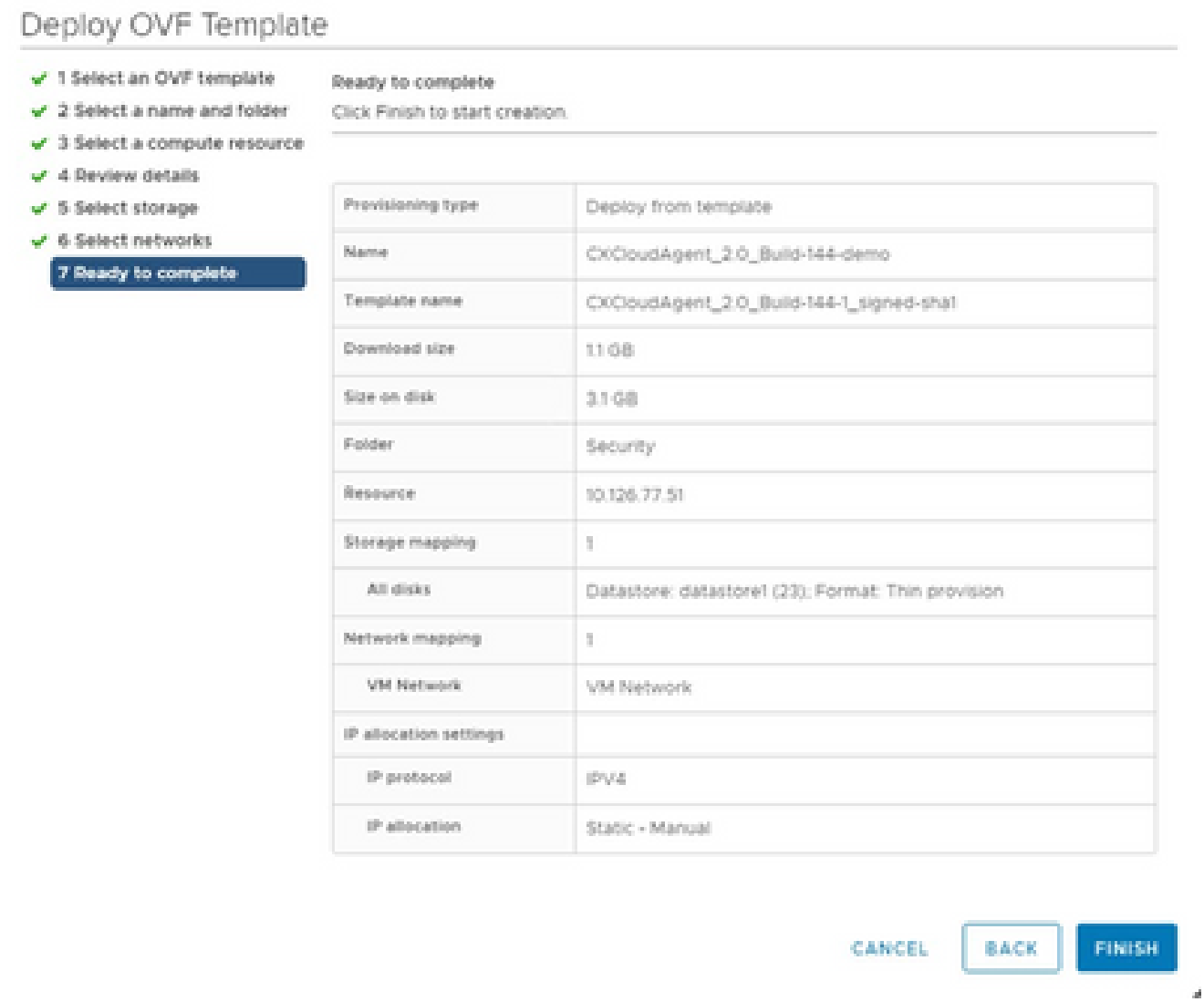
스토리지 선택

10. Next(다음)를 클릭합니다.



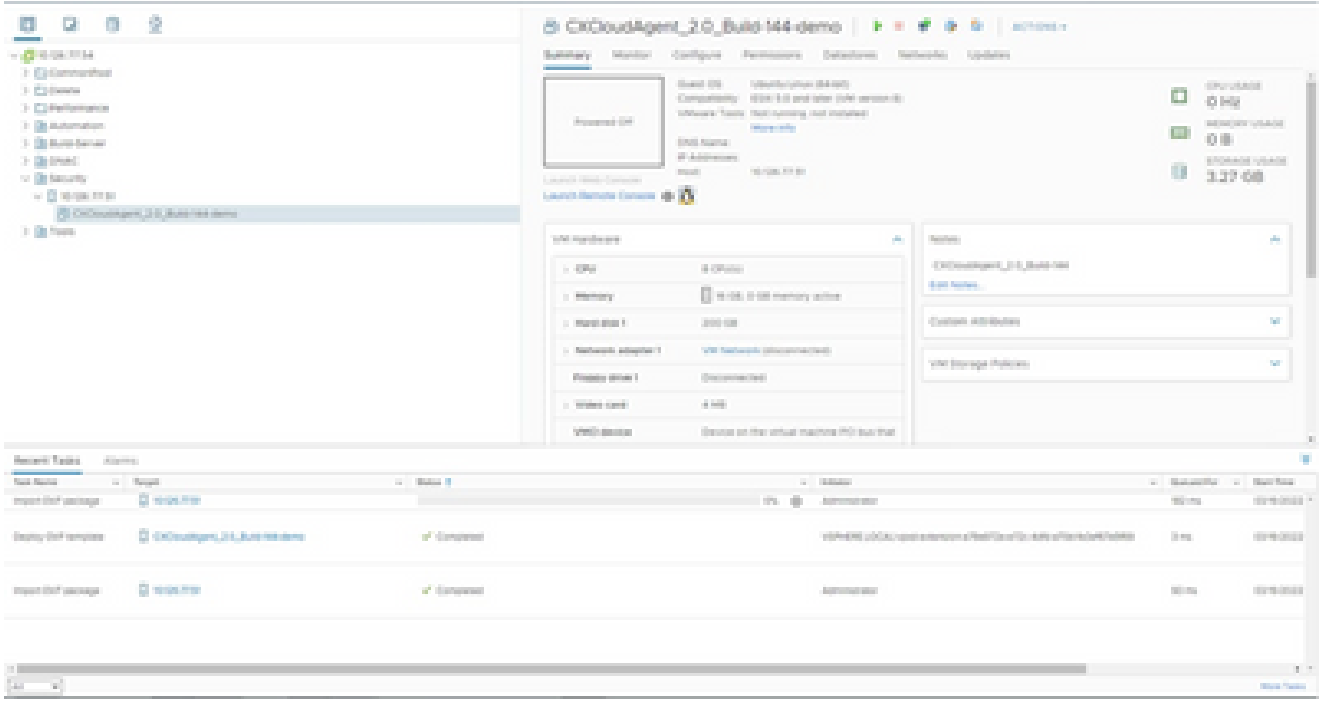
네트워크 선택

11. Finish(마침)를 클릭합니다.



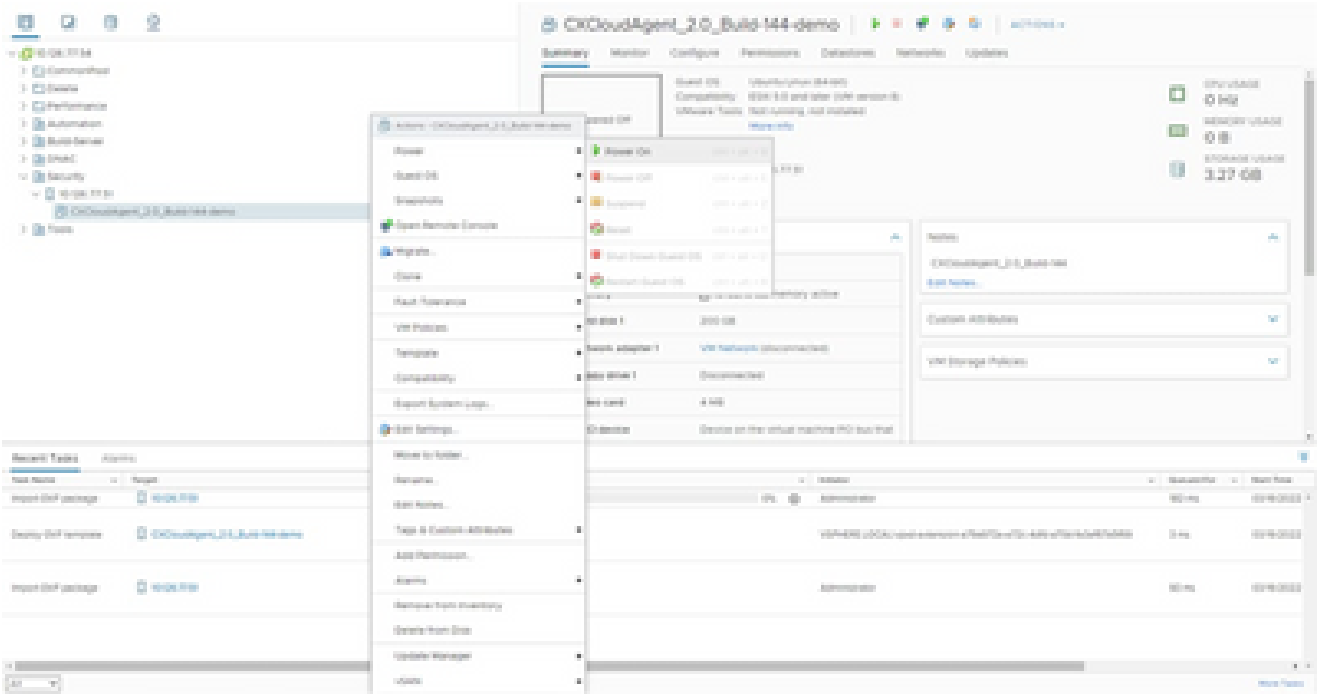
완료 준비

12. 상태를 보려면 새로 추가된 VM의 이름을 클릭합니다.



VM 추가됨

13. 설치가 완료되면 VM의 전원을 켜고 콘솔을 엽니다.



콘솔 열기

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

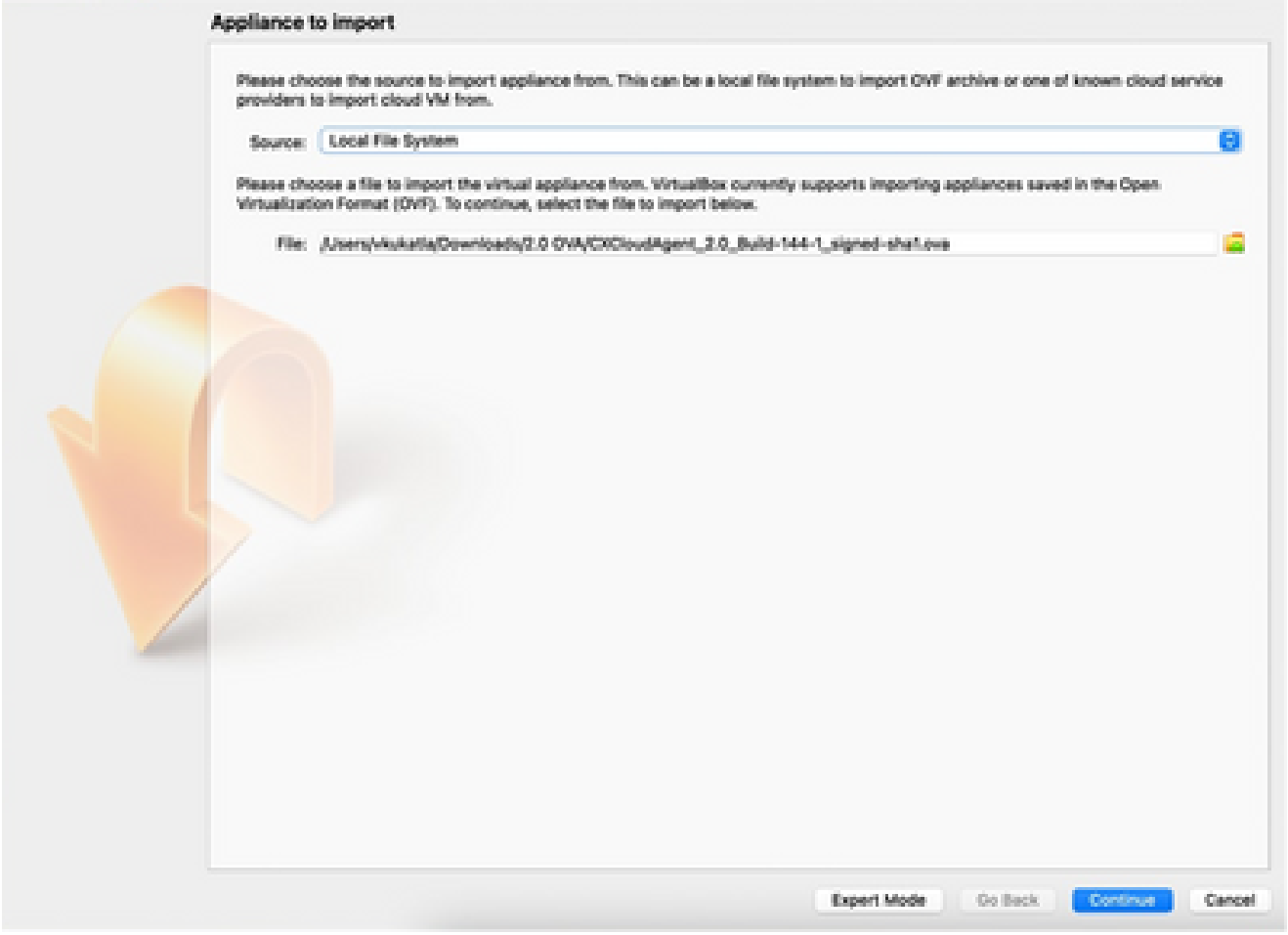
Oracle Virtual Box 5.2.30 설치

이 클라이언트는 Oracle Virtual Box를 통해 CX Cloud Agent OVA를 구축합니다.

1. Oracle VM UI를 열고 File > Import Appliance를 선택합니다.

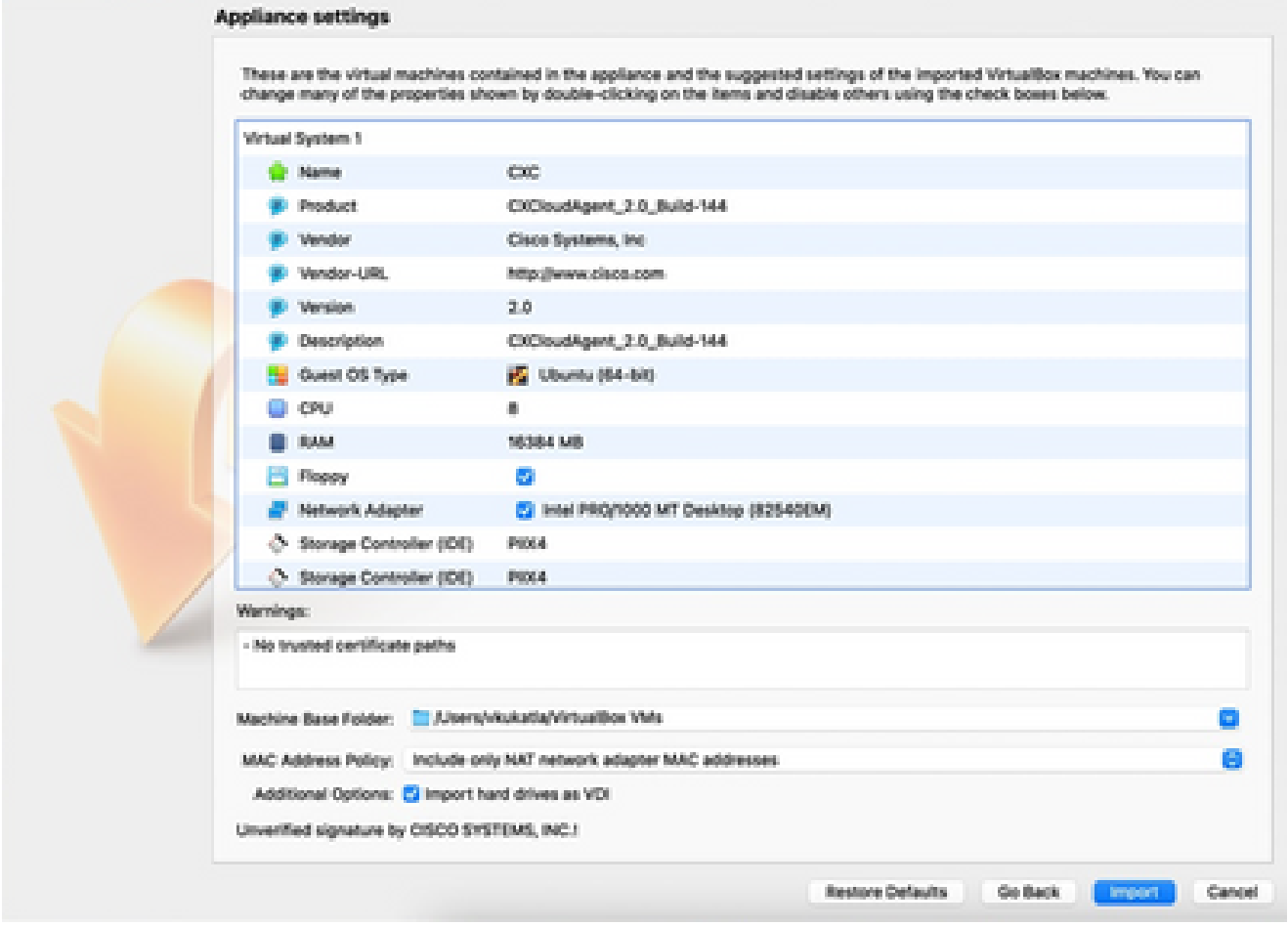
Oracle VM

2. OVA 파일을 찾아 가져옵니다.



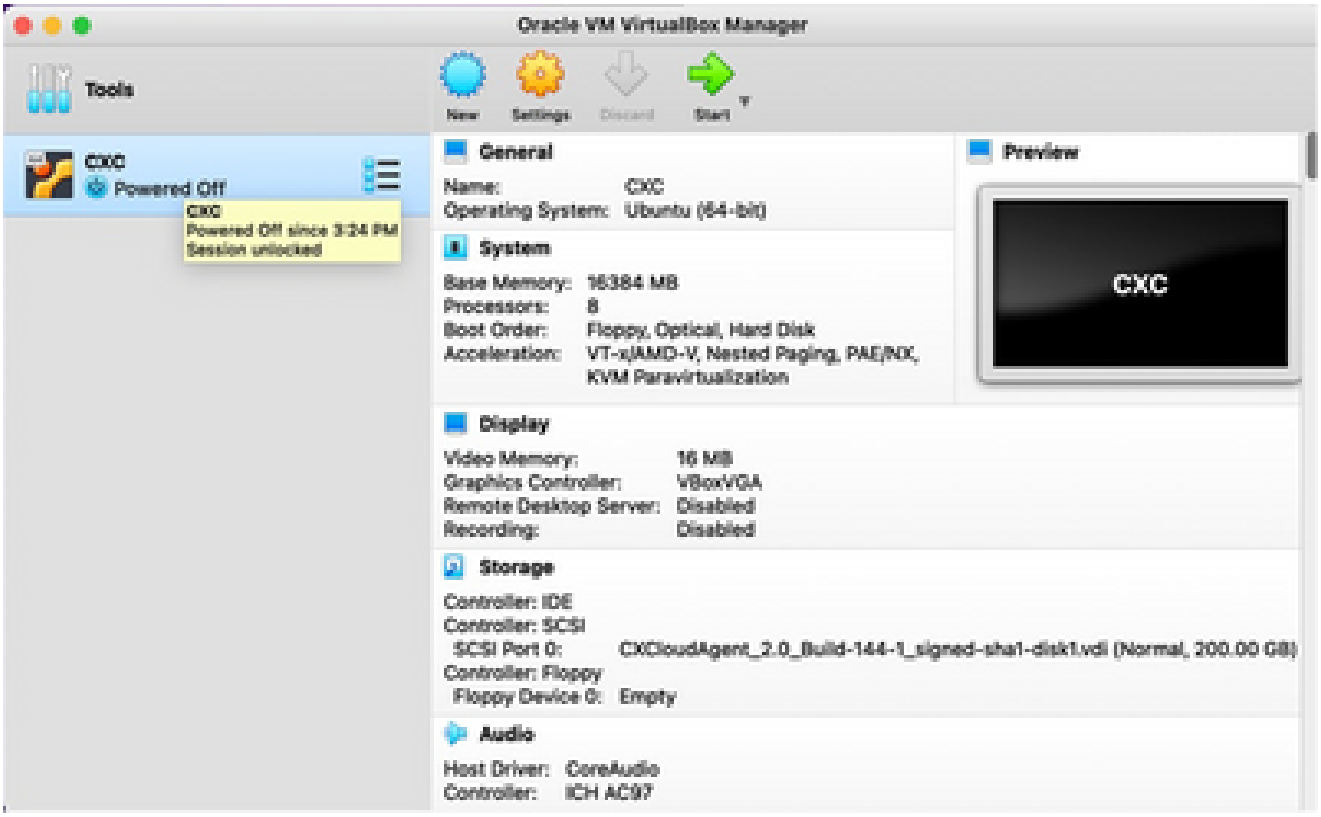
파일 선택

3. Import(가져오기)를 클릭합니다.

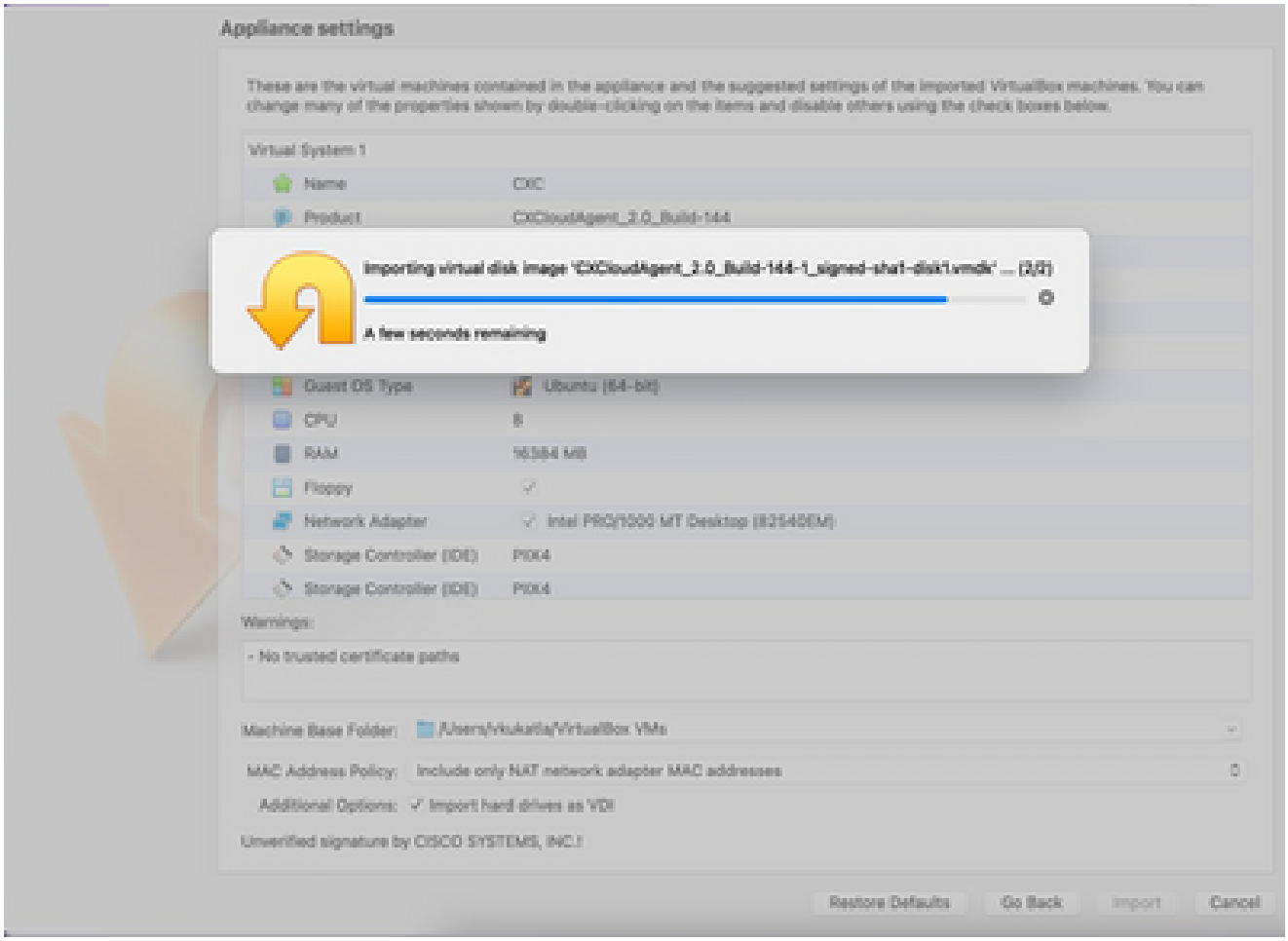


파일 가져오기

4. 방금 구축한 VM을 선택하고 시작을 클릭합니다.

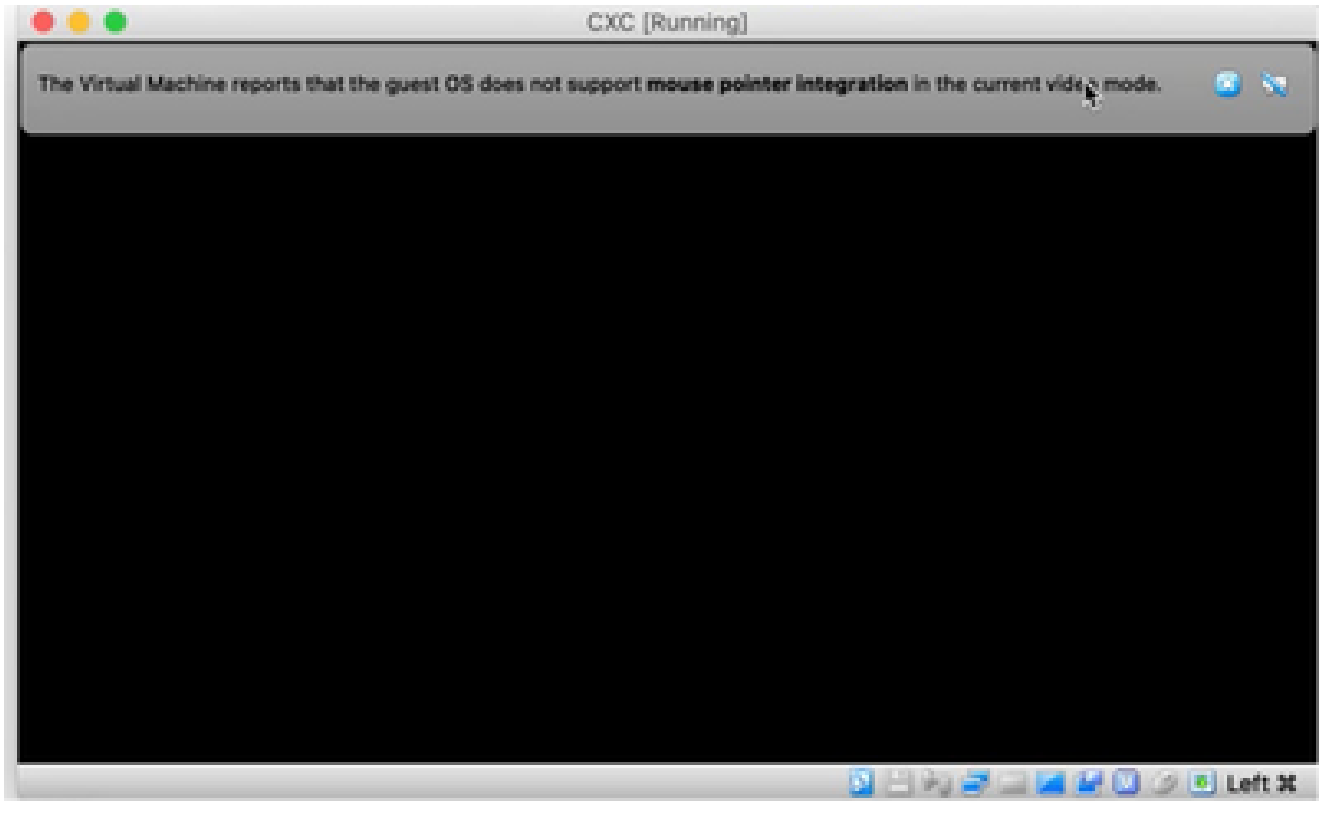


VM 콘솔 시작



가져오기 진행 중

5. VM 전원을 켭니다. 콘솔이 표시됩니다.



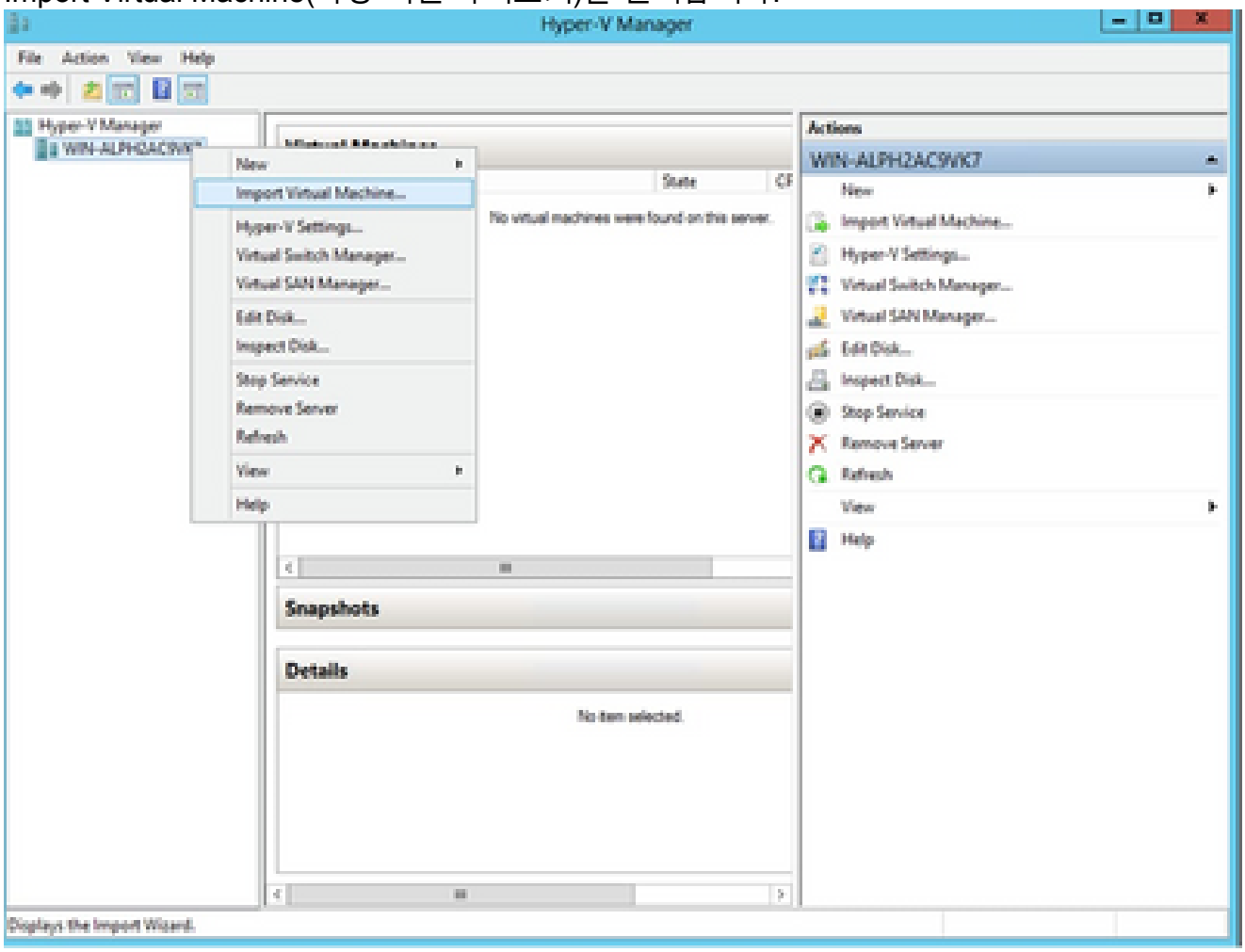
콘솔 열기

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

Microsoft Hyper-V 설치

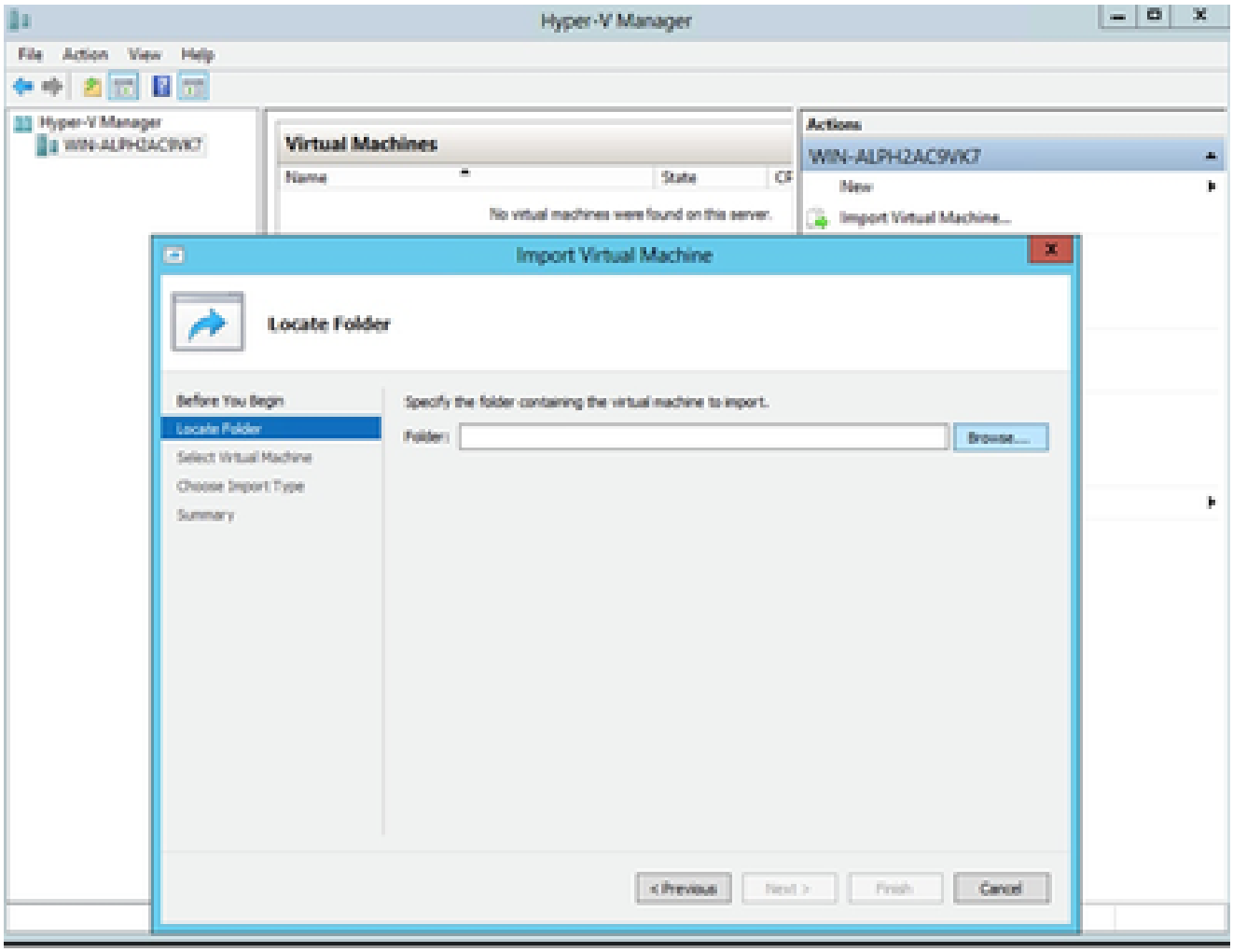
다음을 수행합니다.

1. Import Virtual Machine(가상 머신 가져오기)을 선택합니다.



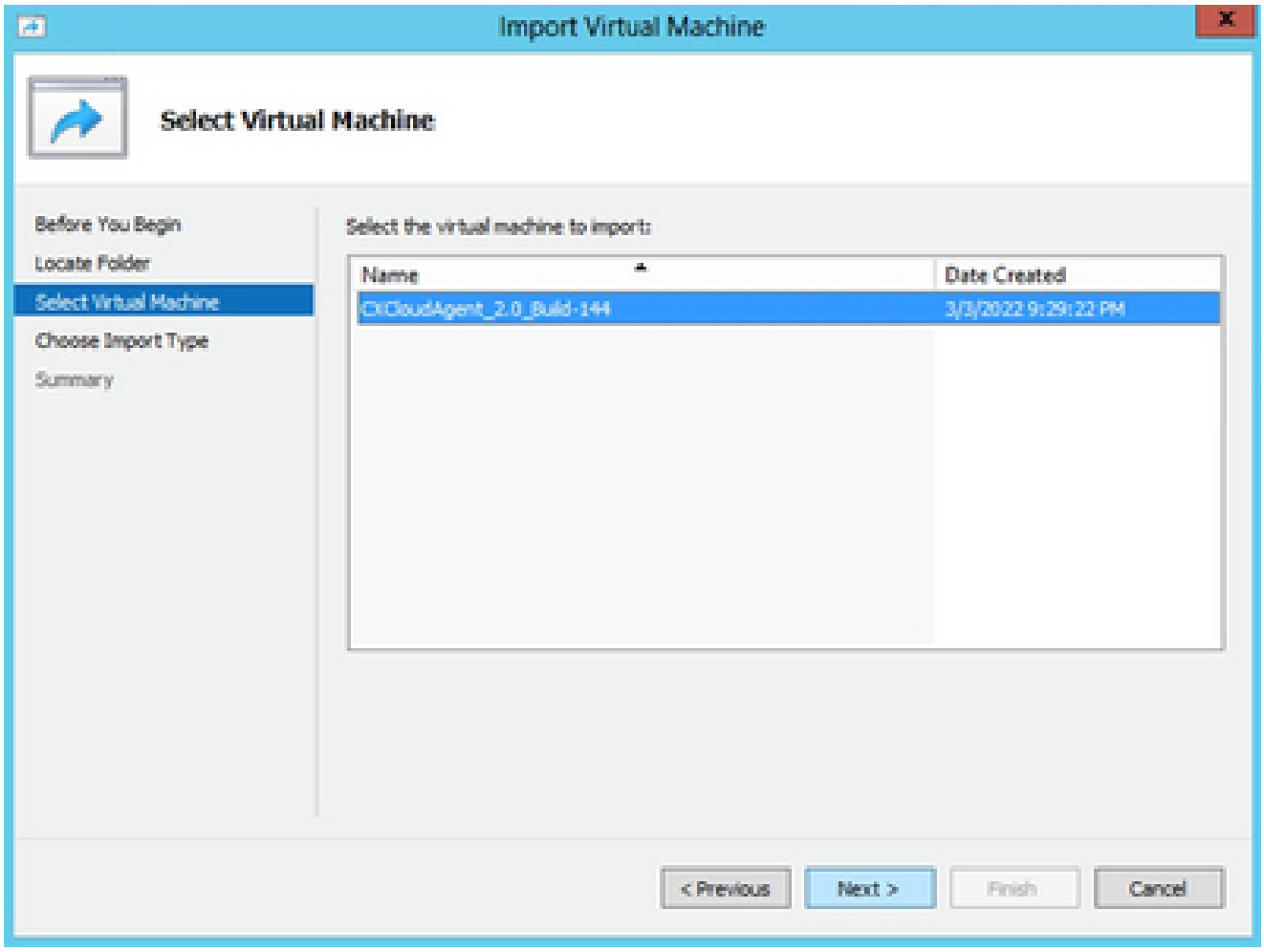
Hyper V 관리자

2. 다운로드 폴더를 찾아 선택합니다
3. Next(다음)를 클릭합니다.



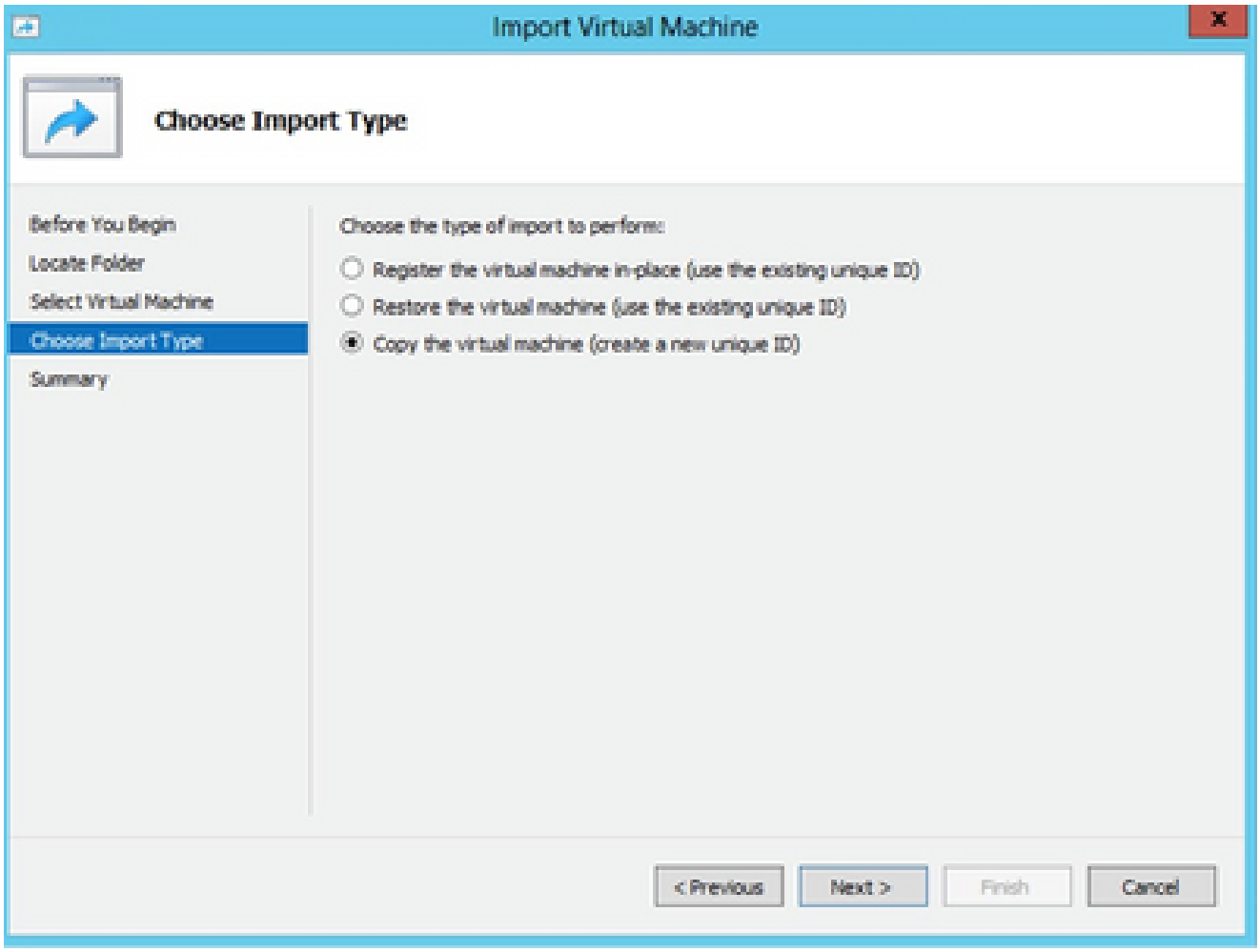
가져올 폴더

4. VM을 선택하고 Next(다음)를 클릭합니다.



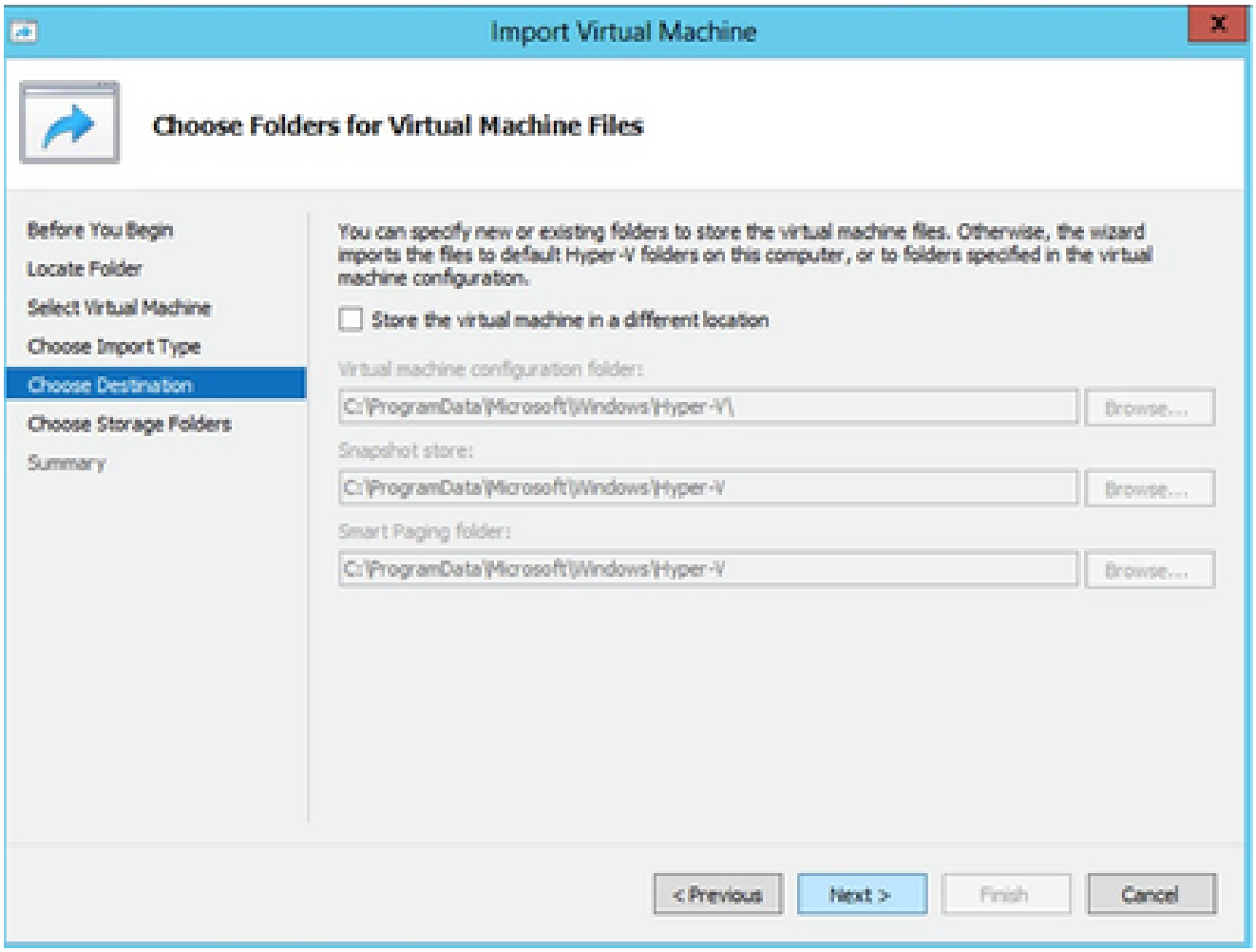
VM 선택

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



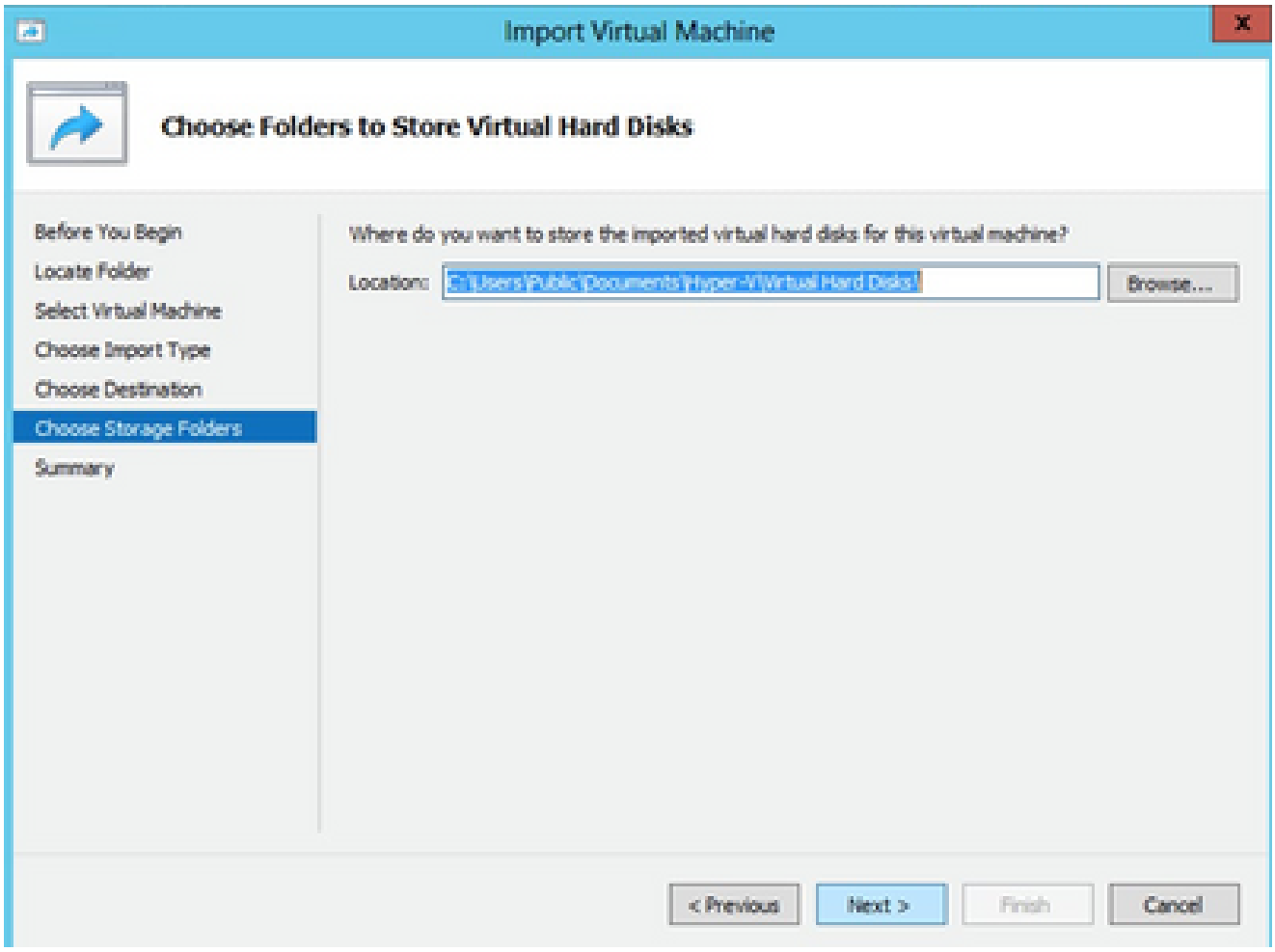
가져오기 유형

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



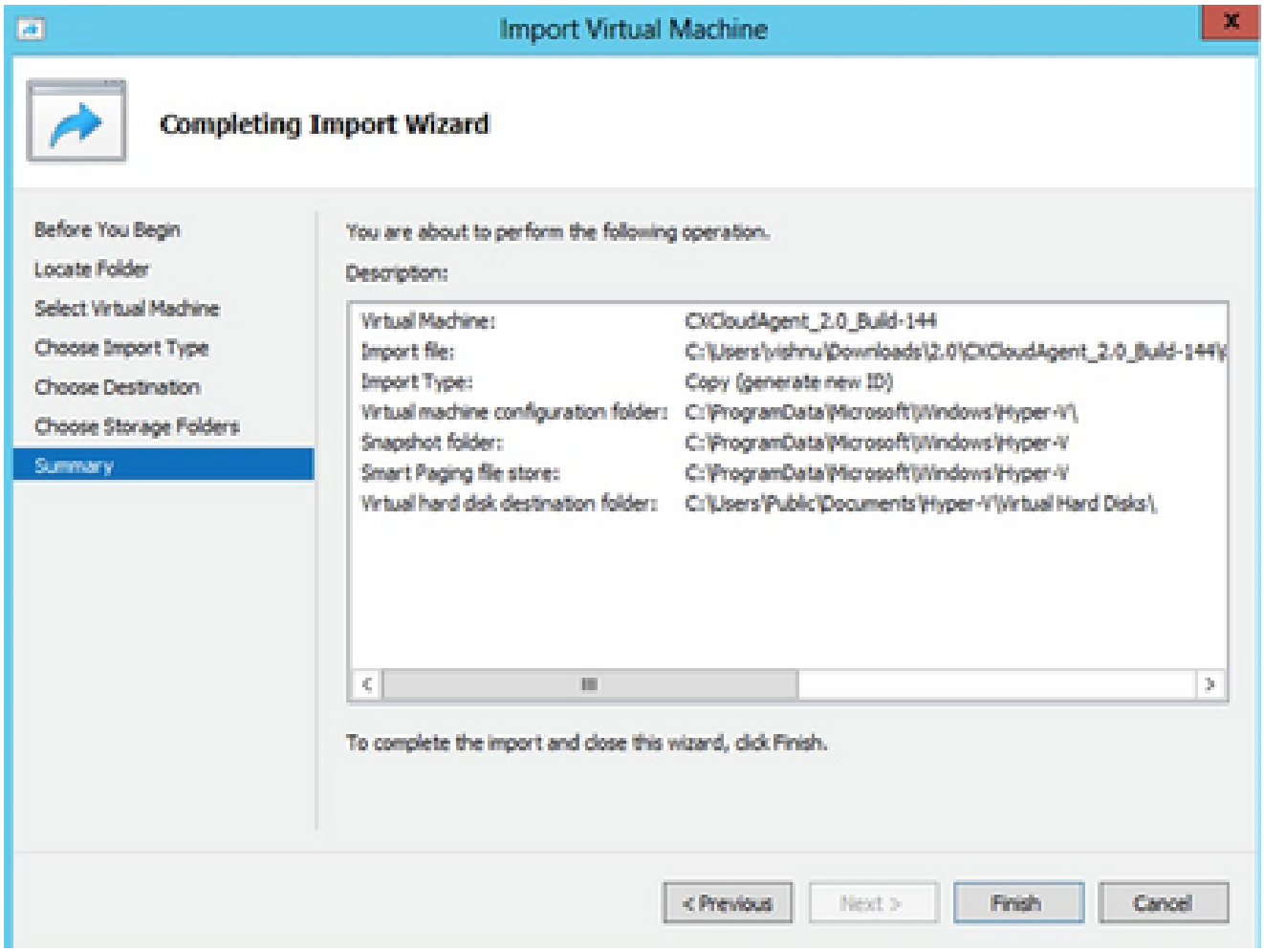
가상 컴퓨터 파일의 폴더 선택

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



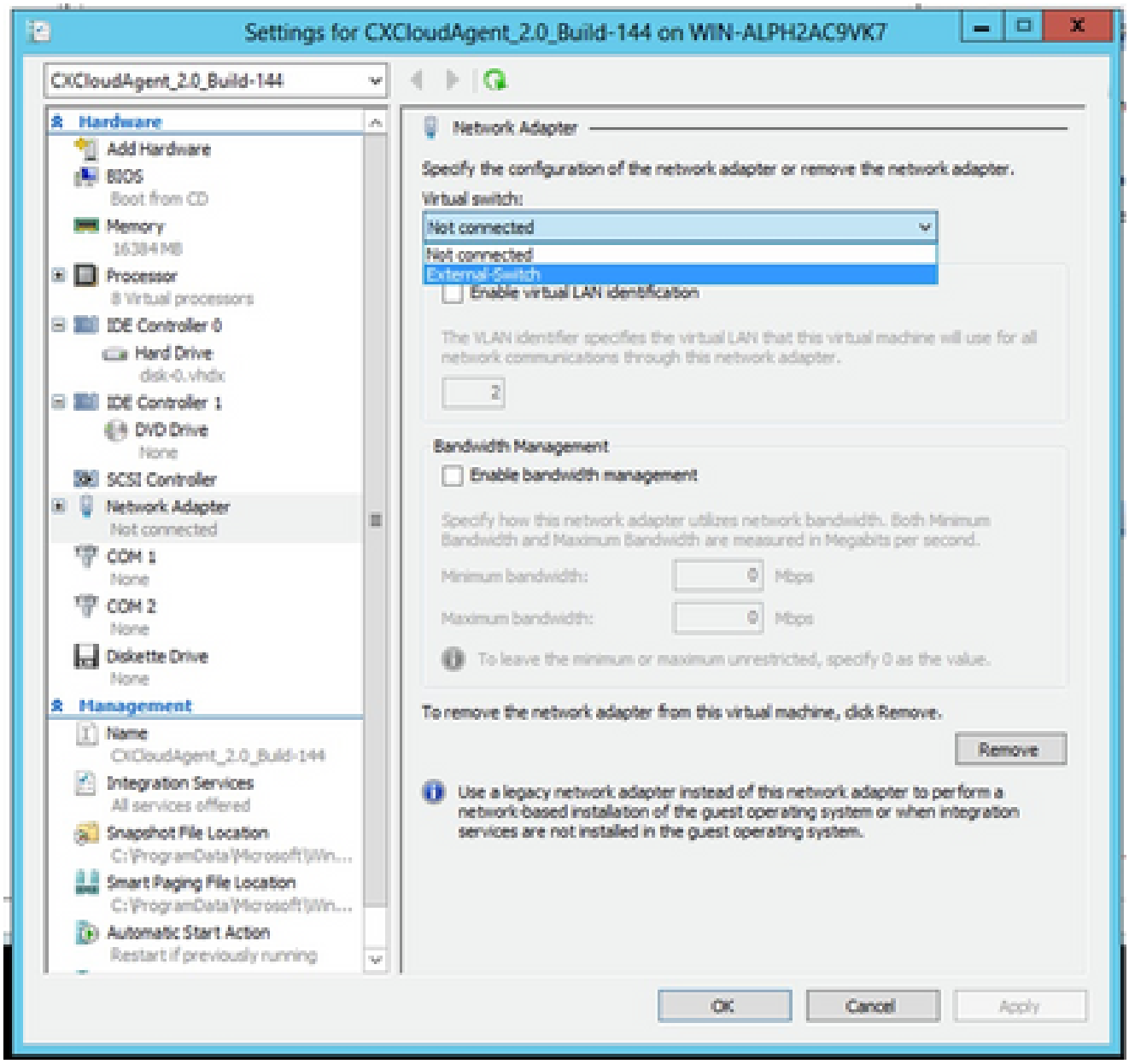
가상 하드 디스크를 저장할 폴더

10. VM 요약이 표시됩니다. 모든 입력을 확인하고 Finish(마침)를 클릭합니다.



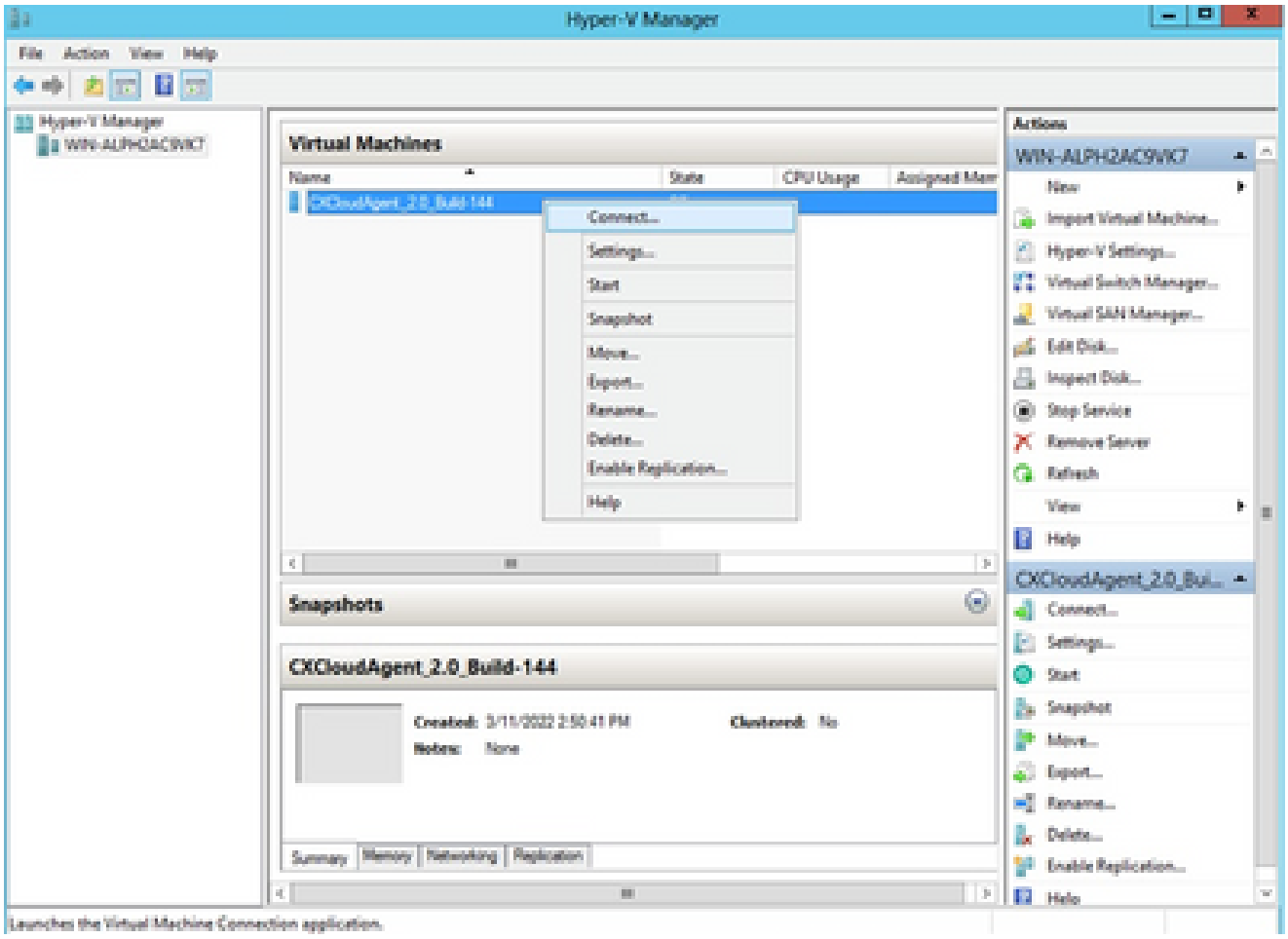
요약

11. 가져오기가 성공적으로 완료되면 Hyper-V에 새 VM이 생성됩니다. VM 설정을 엽니다.
12. 왼쪽 창에서 네트워크 어댑터를 선택하고 드롭다운에서 사용 가능한 가상 스위치를 선택합니다.



가상 스위치

13. Connect(연결)를 선택하여 VM을 시작합니다.

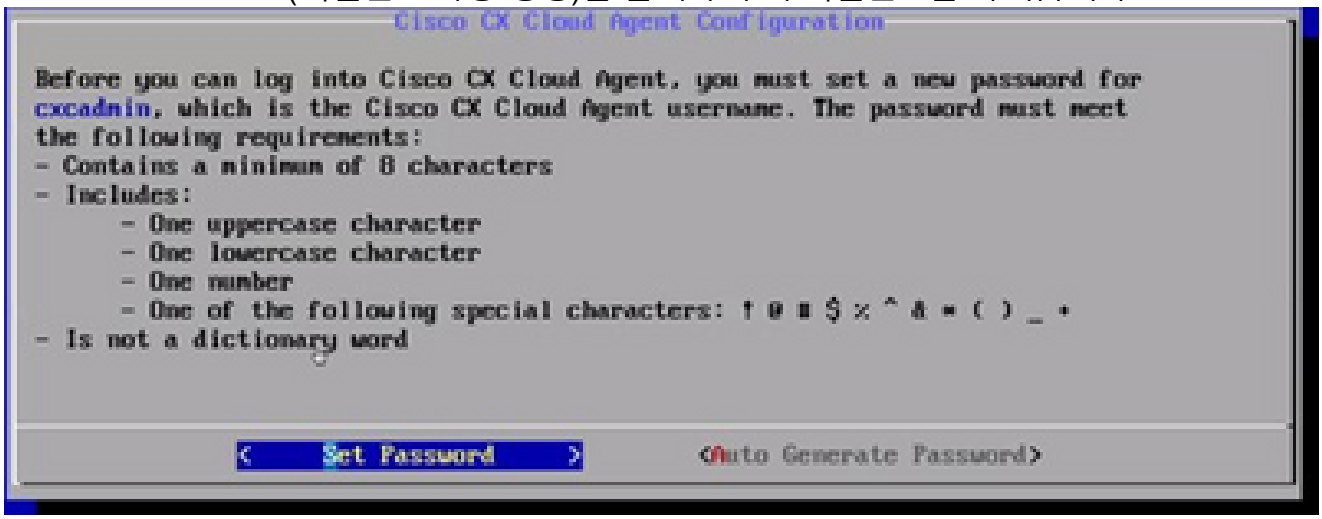


VM 시작

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

네트워크 설정

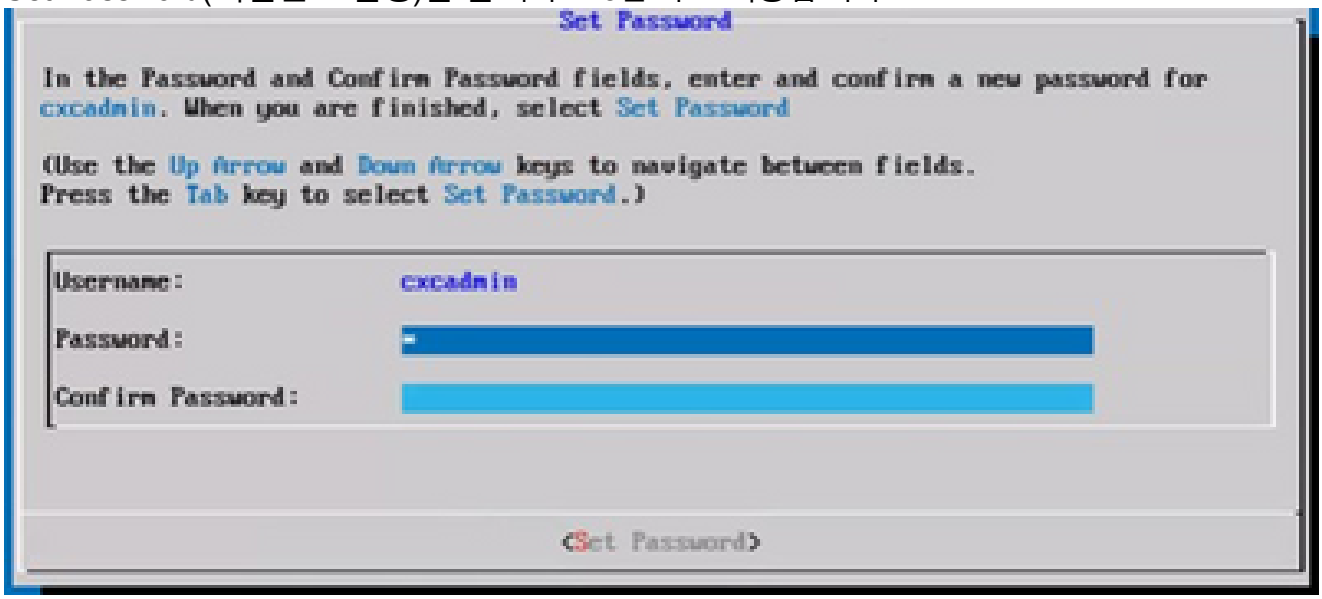
1. Set Password(비밀번호 설정)를 클릭하여 cxcadmin에 대한 새 비밀번호를 추가하거나 Auto Generate Password(비밀번호 자동 생성)를 클릭하여 새 비밀번호를 가져옵니다.



비밀번호 설정

2. Set Password(비밀번호 설정)를 선택한 경우 cxcadmin의 비밀번호를 입력하고 확인합니다.

Set Password(비밀번호 설정)를 클릭하고 3단계로 이동합니다.



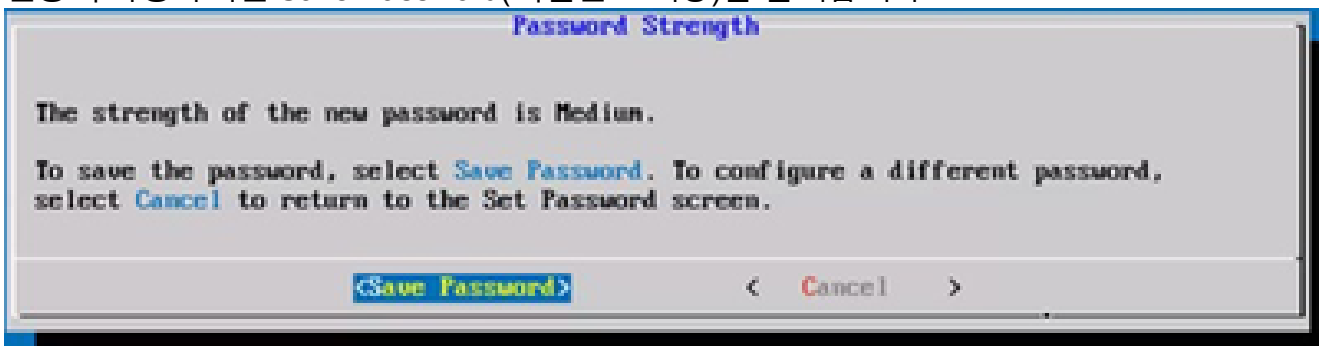
새 비밀번호

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.

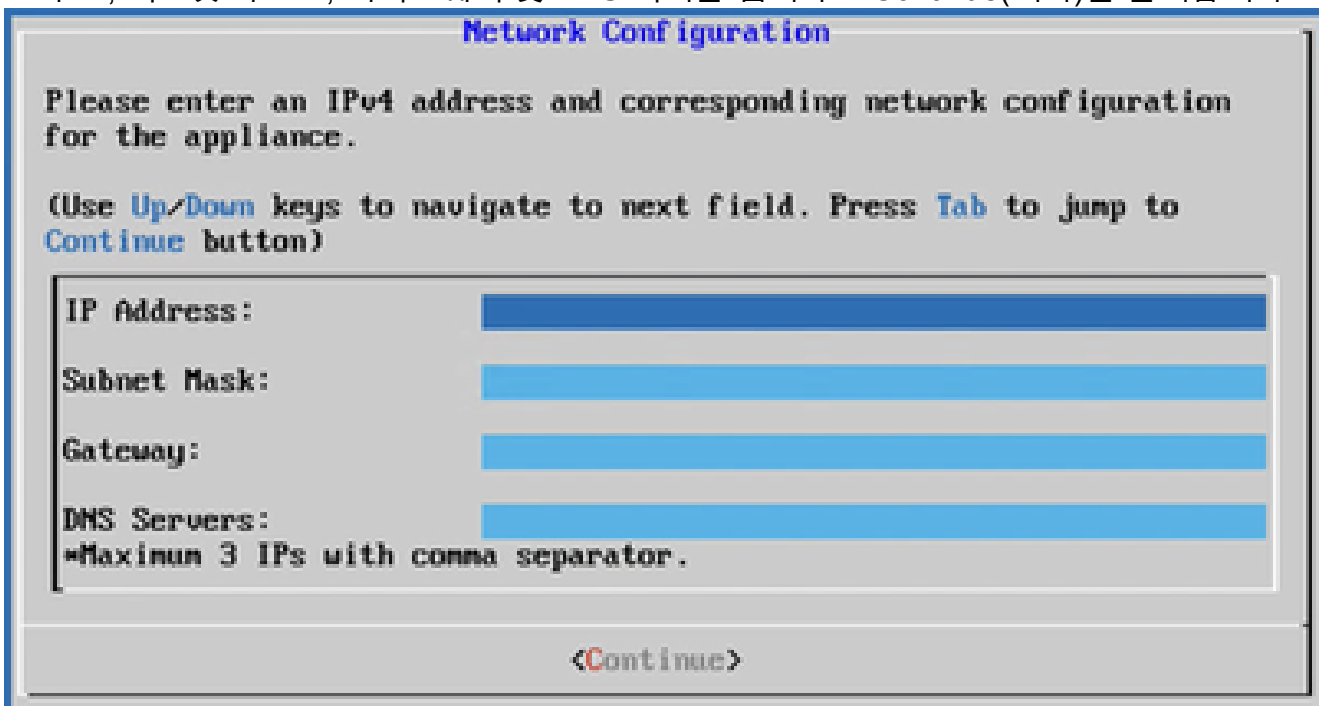
자동 생성 비밀번호

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



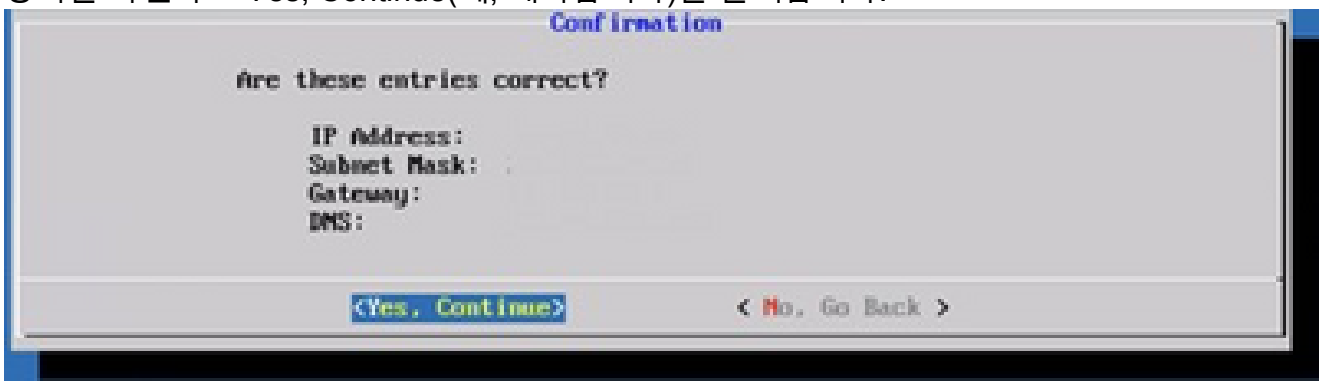
비밀번호 저장

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



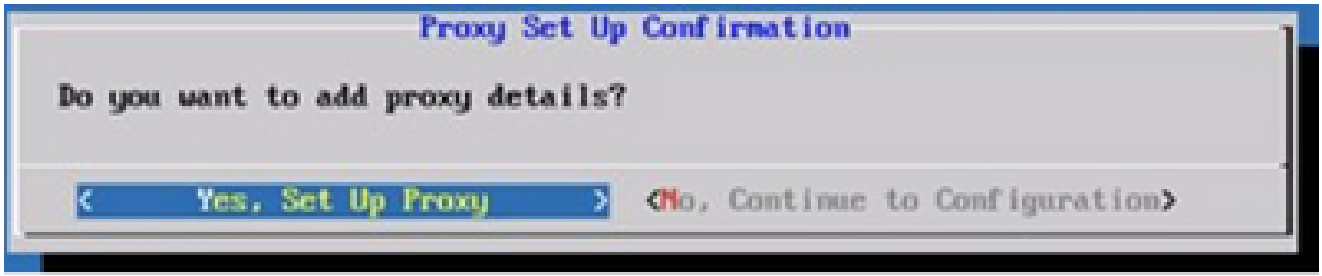
네트워크 설정

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



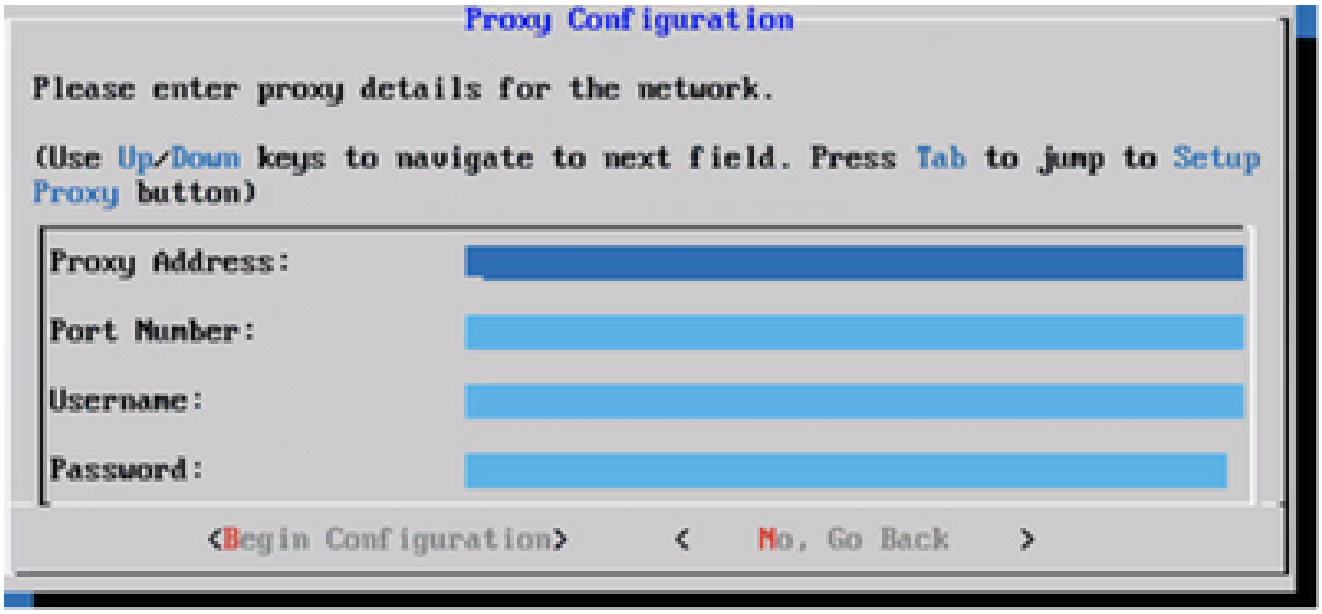
설정

6. 프록시 세부 정보를 설정하려면 Yes(예), Set Up Proxy(프록시 설정)를 클릭하거나 No(아니요), Continue to Configuration(컨피그레이션 계속)을 클릭하여 컨피그레이션을 완료한 후 8단계로 이동합니다.



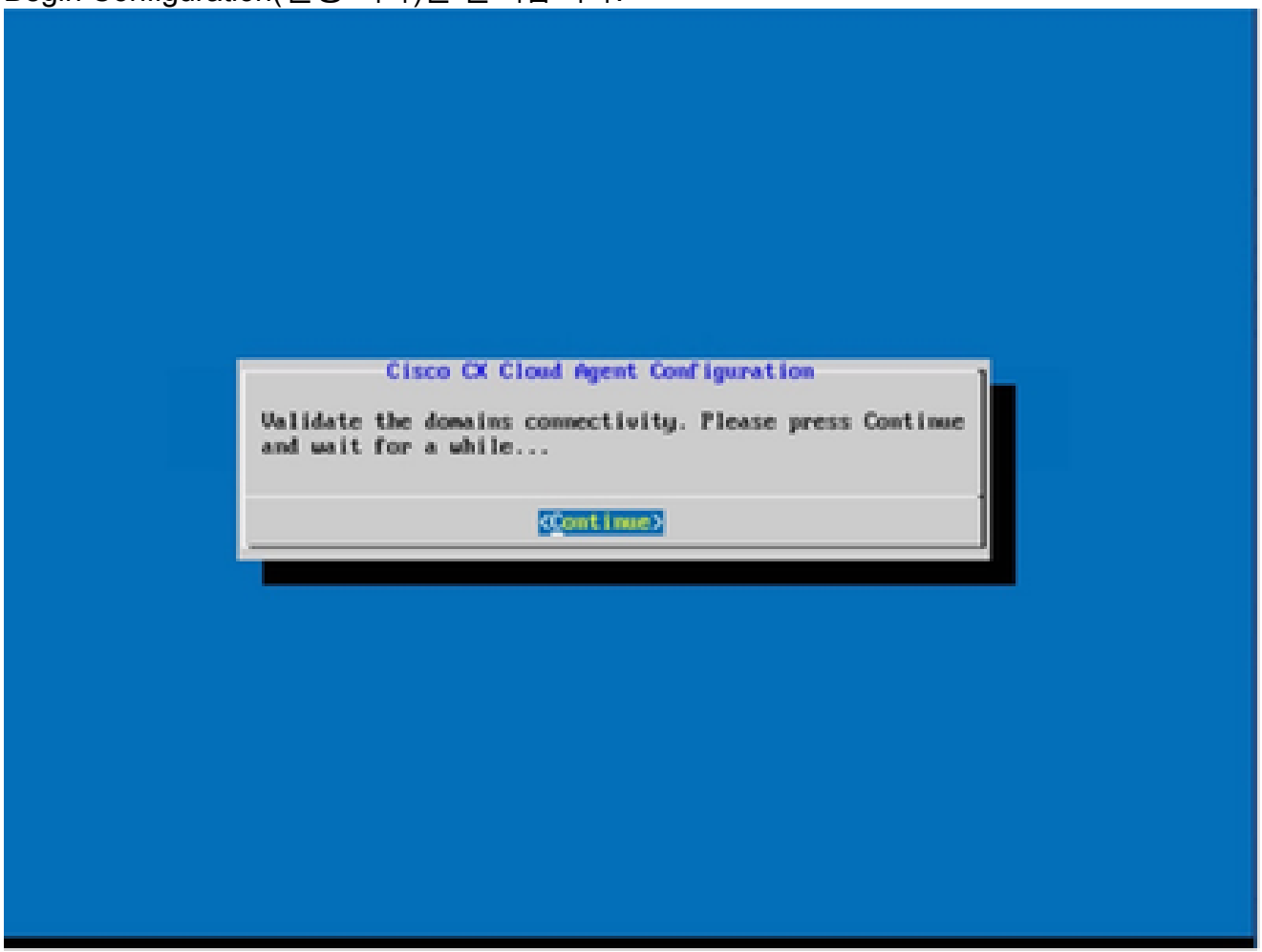
프록시 설정

7. 프록시 주소, 포트 번호, 사용자 이름 및 비밀번호를 입력합니다.



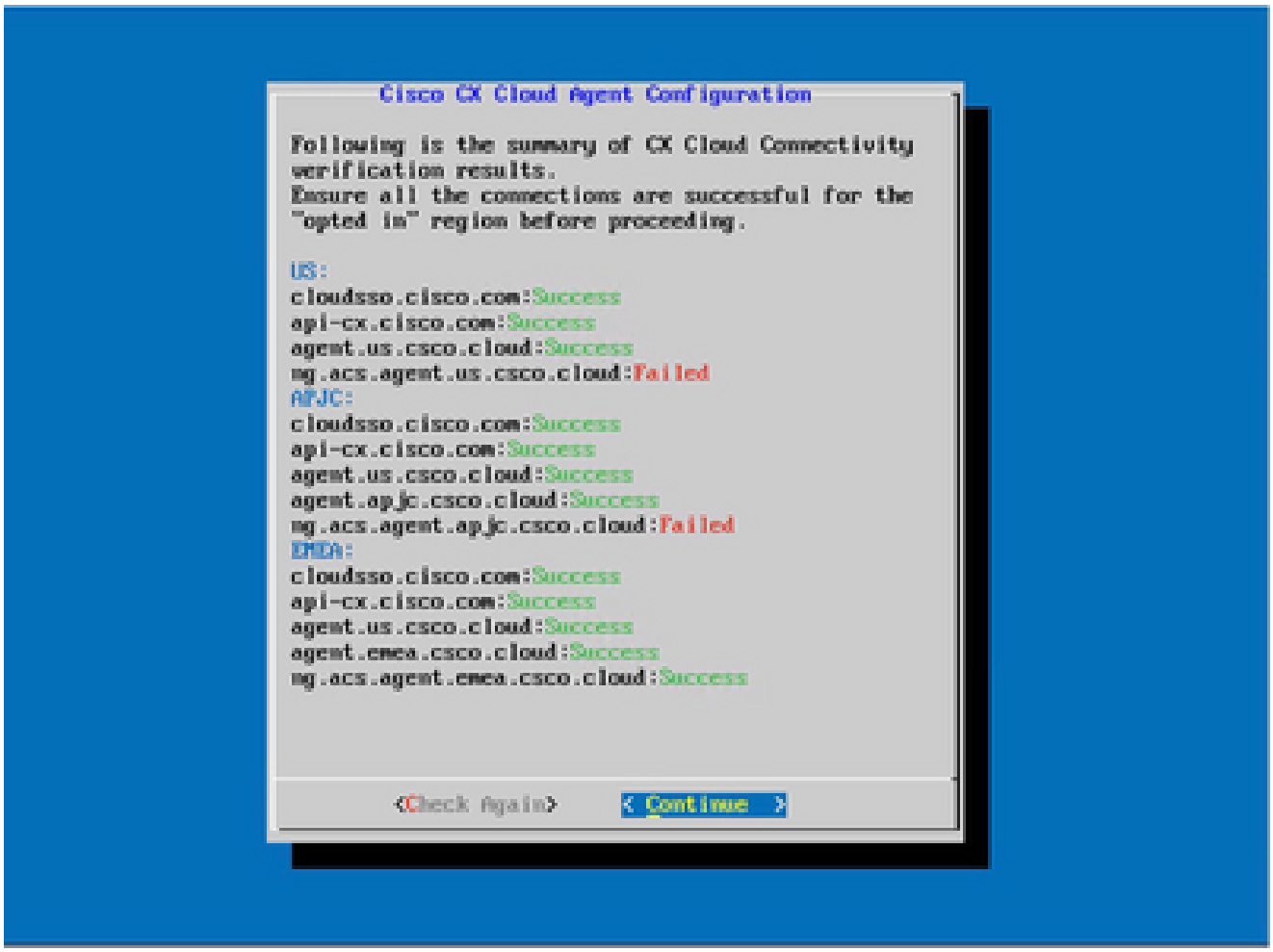
프록시 구성

8. Begin Configuration(설정 시작)을 클릭합니다.



구성 시작

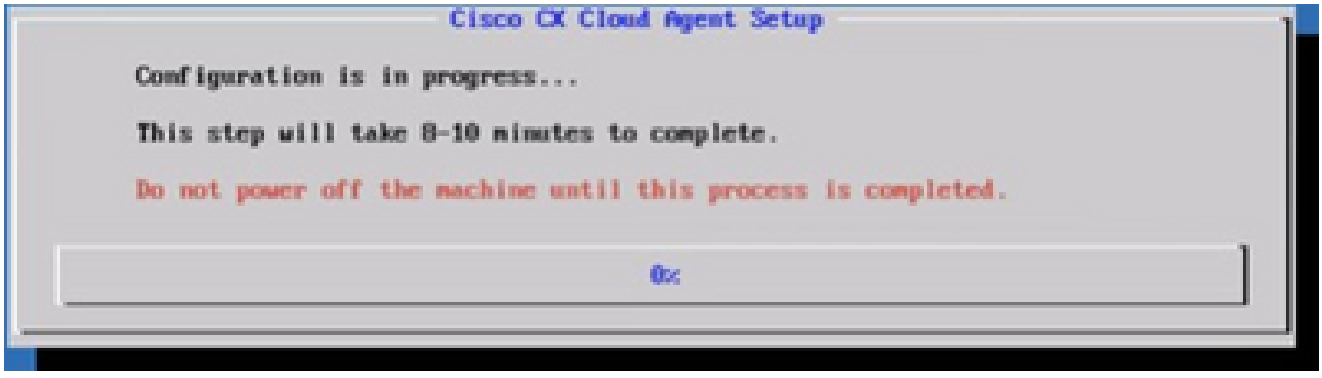
9. Continue(계속)를 클릭합니다.



컨피그레이션 계속

10. 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.

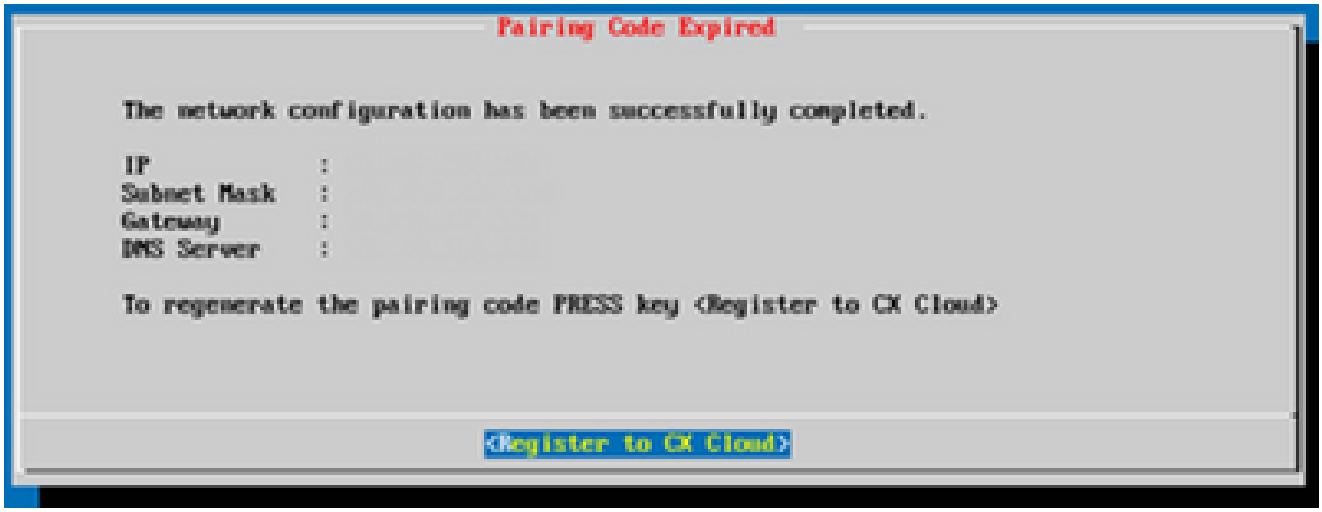


설정 진행 중

11. 페어링 코드를 복사하고 CX Cloud로 돌아가 설정을 계속합니다.

페어링 코드

12. 페어링 코드가 만료되면 CX Cloud에 등록을 클릭하여 코드를 다시 가져옵니다.



코드가 만료됨

13. OK(확인)를 클릭합니다.

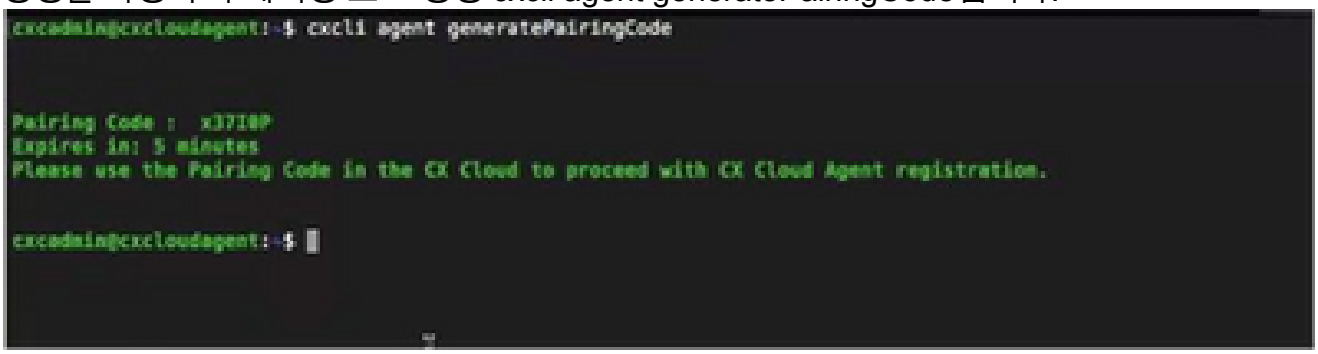
등록 성공

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. 명령을 사용하여 페어링 코드 생성 cxcli agent generatePairingCode입니다.



페어링 코드 CLI 생성

3. 페어링 코드를 복사하고 CX Cloud로 돌아가 설정을 계속합니다.

CX 클라우드 에이전트에 Syslog를 전달하도록 Cisco DNA Center 구성

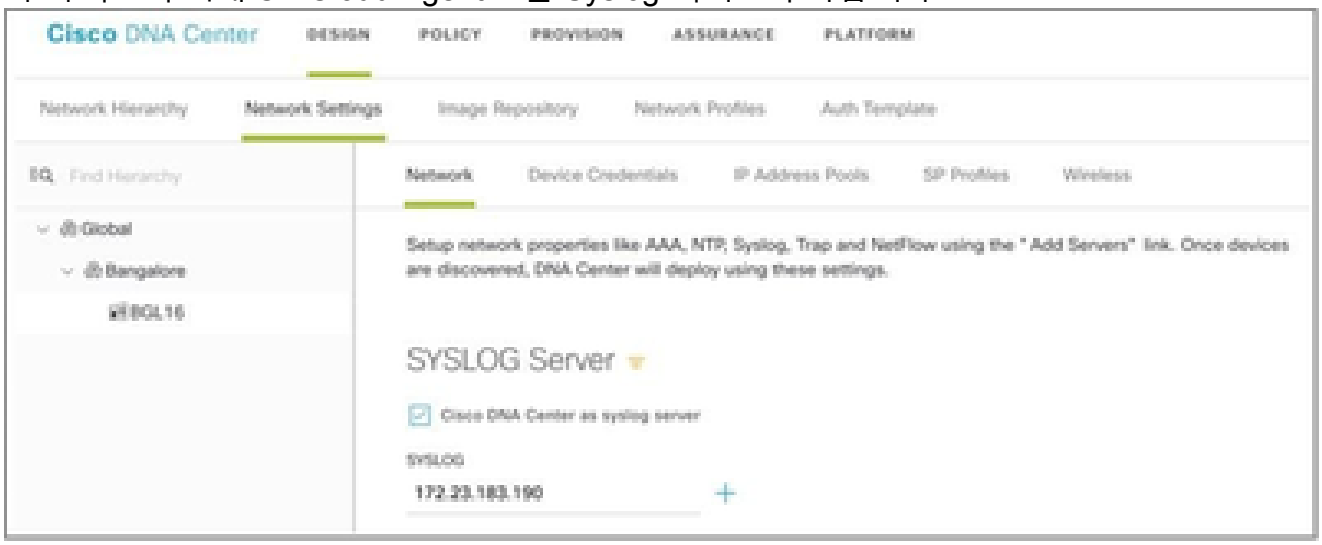
사전 요구 사항

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

Syslog 전달 설정 구성

Cisco DNA Center에서 CX Cloud Agent로 Syslog 전달을 구성하려면 다음 단계를 수행합니다.

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



Syslog 서버

참고:
구성이 완료되면 해당 사이트와 연결된 모든 디바이스는 CX Cloud Agent에 수준이 중요한

---

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 클라우드 에이전트로 전달하도록 기타 자산 구성

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

참고: Campus Success Track Level 2 디바이스만 syslog를 전달하도록 다른 자산을 구성할 수 있습니다.

전달 기능이 있는 기존 Syslog 서버

syslog 서버 소프트웨어에 대한 컨피그레이션 지침을 수행하고 CX 클라우드 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 클라우드 에이전트 IP 주소로 직접 syslog를 전송하도록 각 디바이스를 구성합니다. 특정 컨피그레이션 단계는 다음 설명서를 참조하십시오.

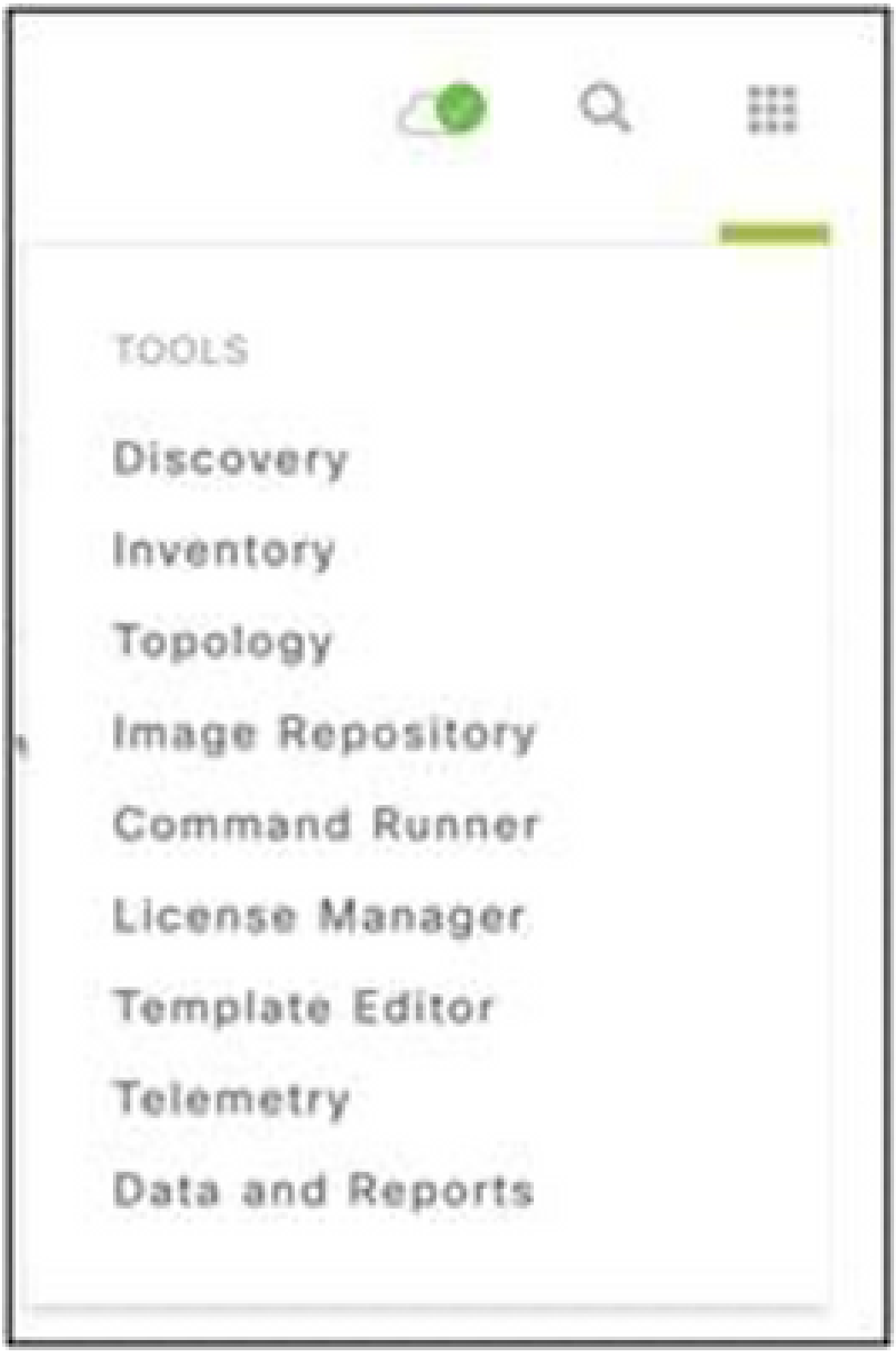
IOS-XE 컨피그레이션 가이드

AireOS Wireless Controller 컨피그레이션 가이드

정보 레벨 Syslog 설정 활성화

Syslog 정보 레벨을 표시하려면 다음 단계를 수행하십시오.

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 계층 구조에서 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

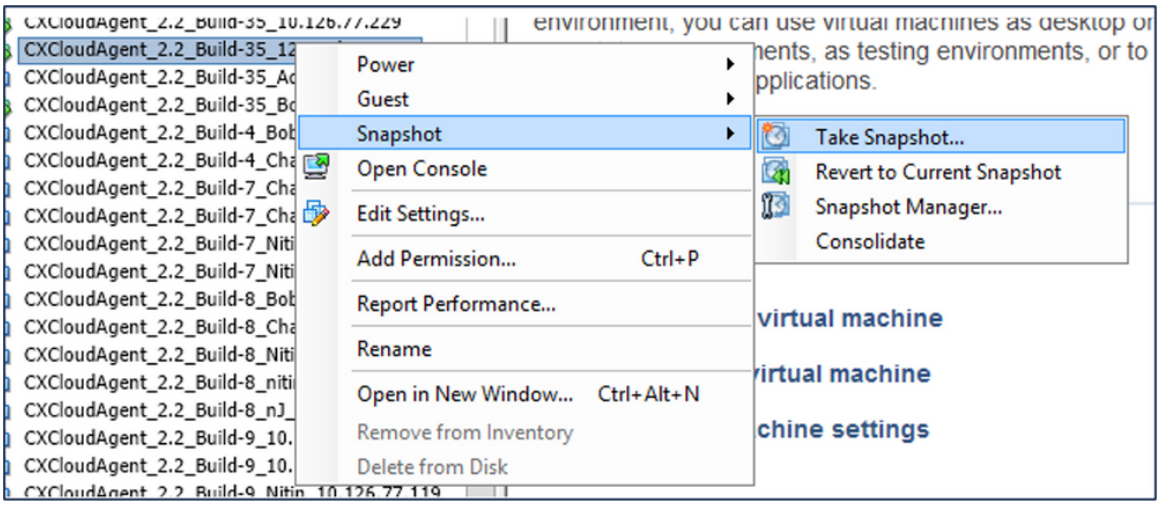
CX 클라우드 VM 백업 및 복원

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

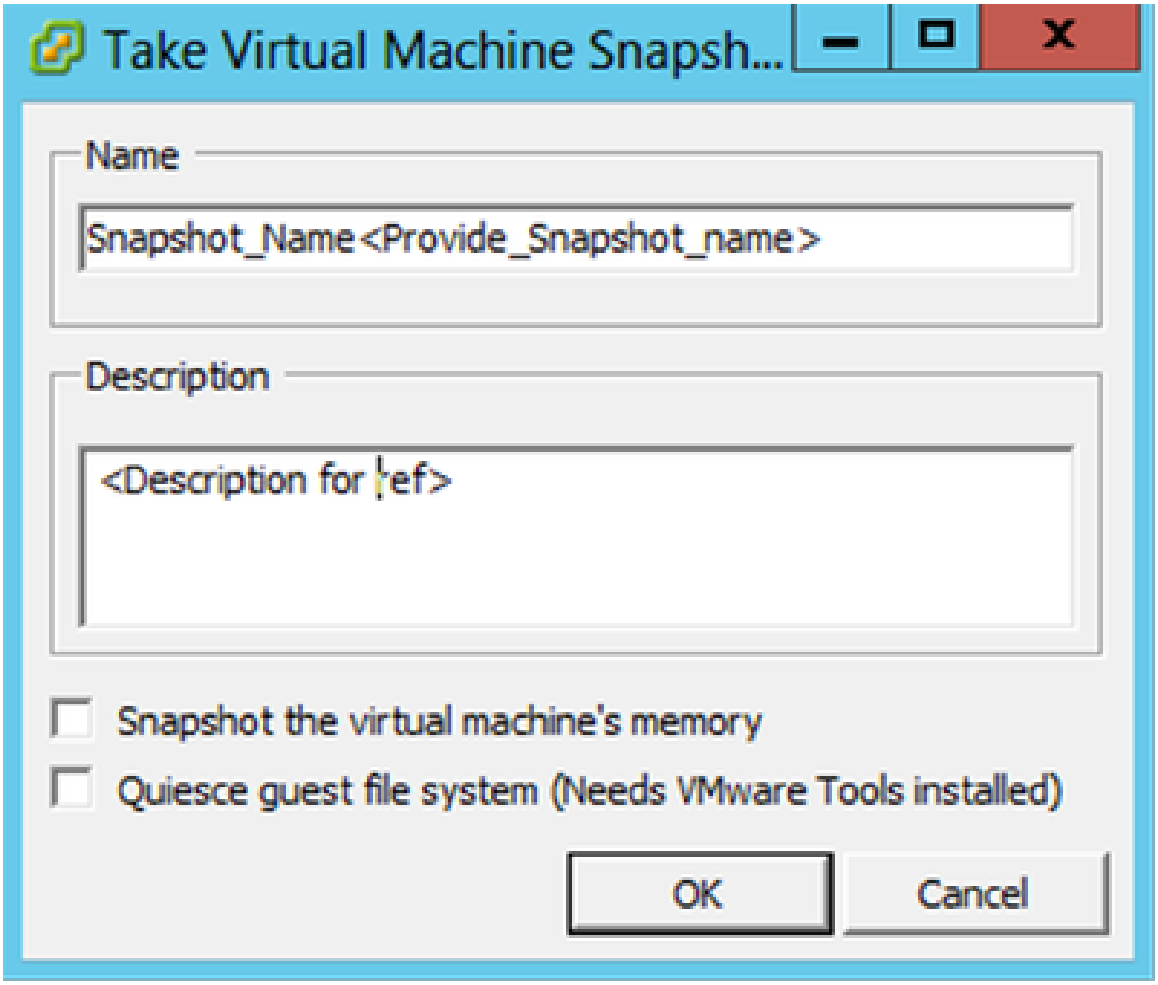
백업

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

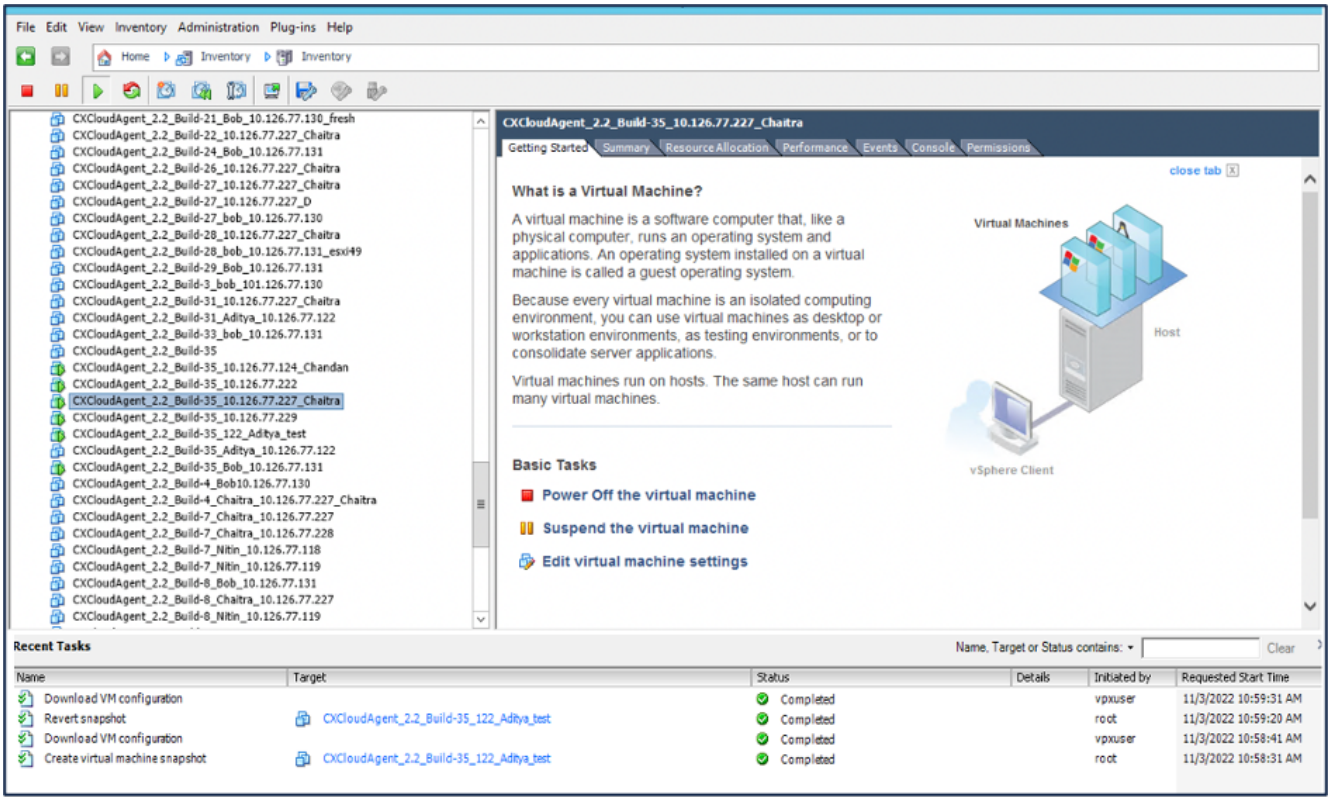


가상 컴퓨터 스냅숏 만들기

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.

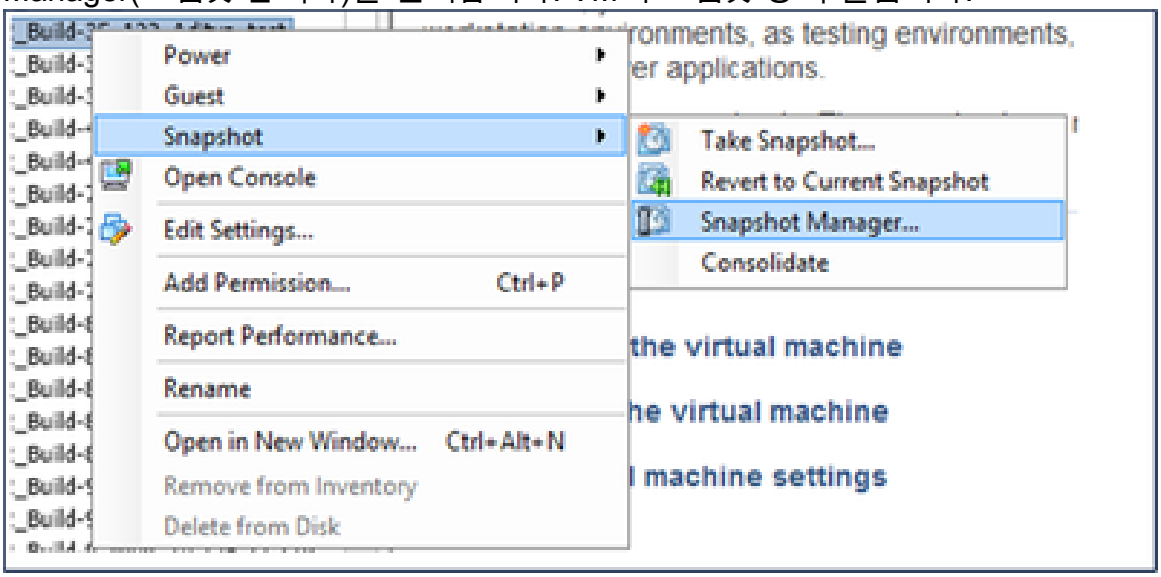


최근 작업

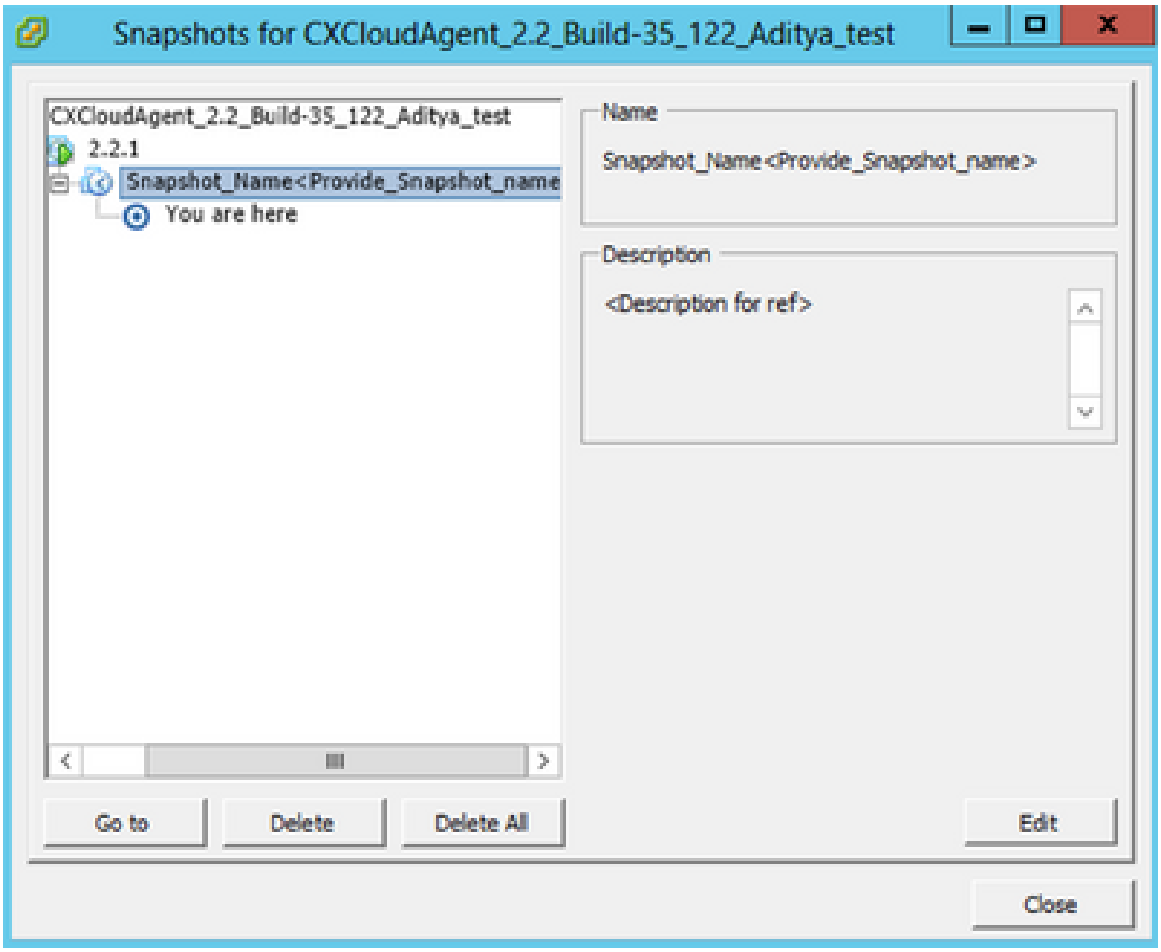
복원

CX 클라우드 VM을 복원하려면

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

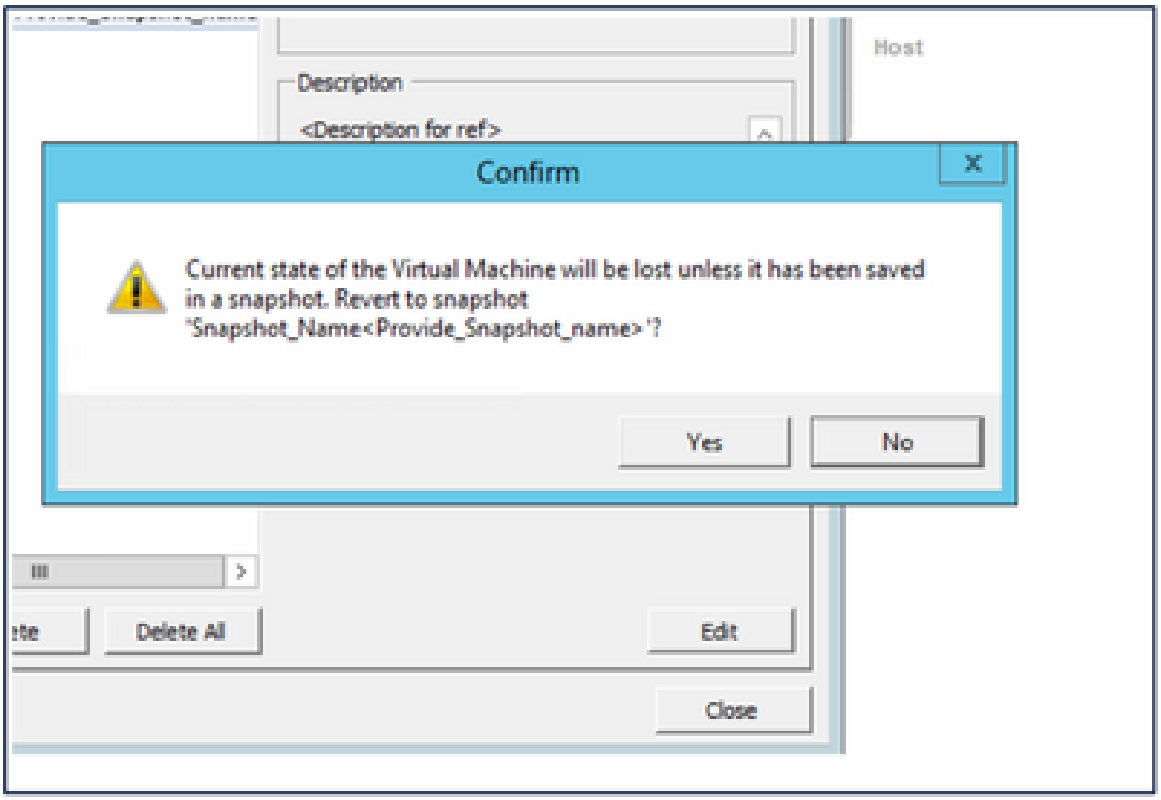


VM 선택 창



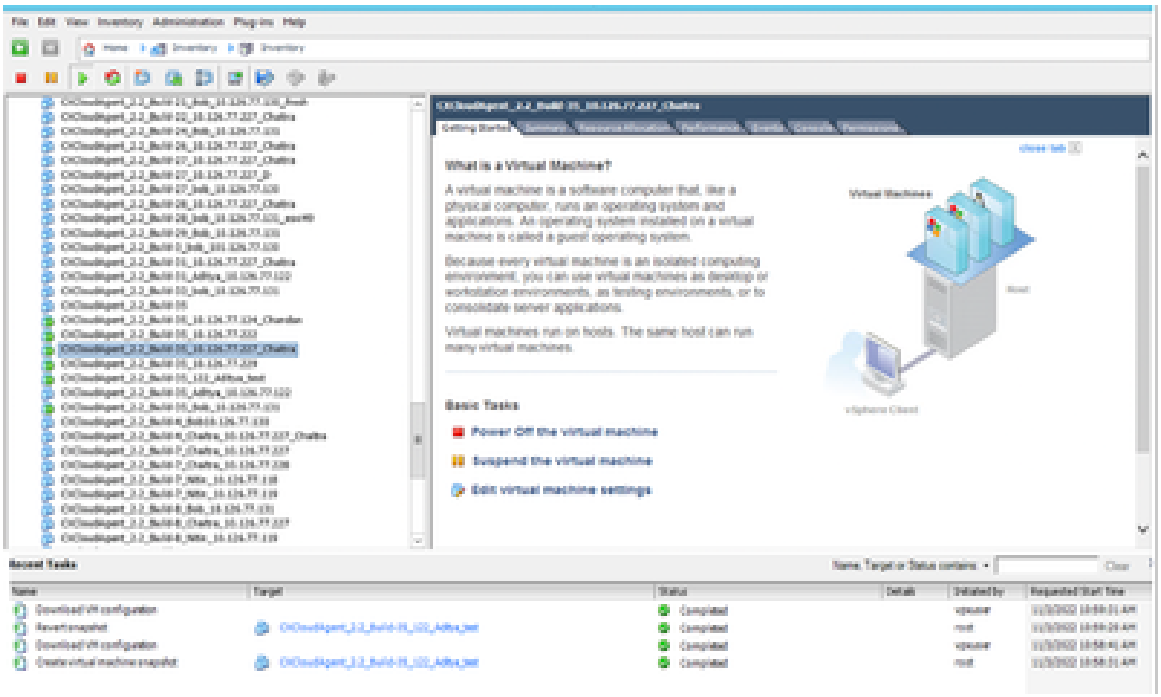
스냅샷 창

2. 이동을 클릭합니다. 확인 창이 열립니다.



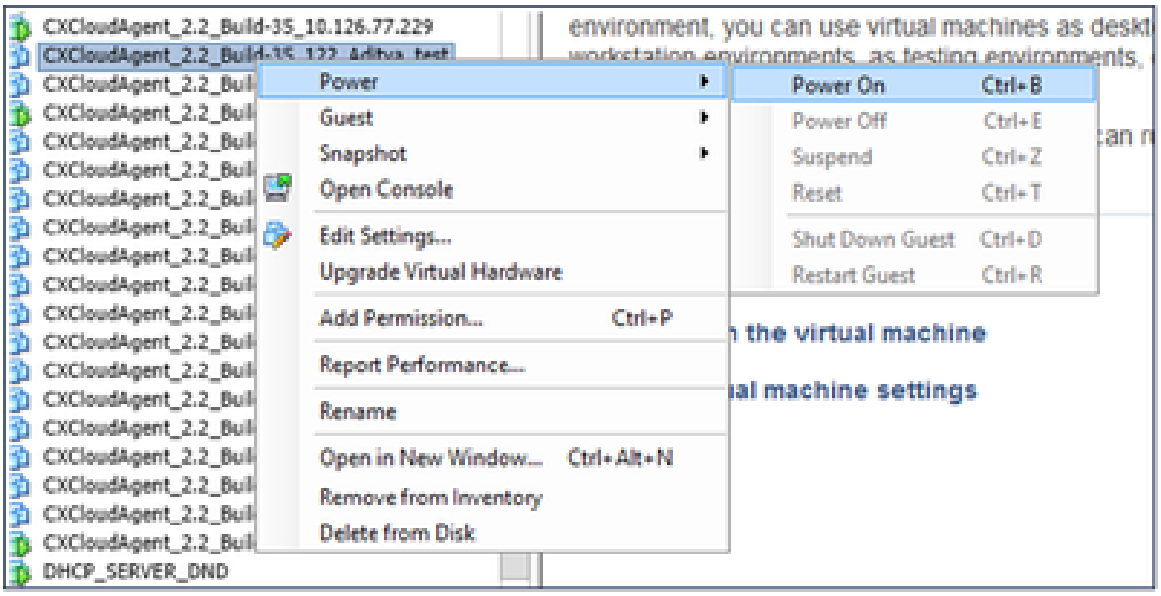
창 확인

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 Cloud Agent는 고객에게 엔드 투 엔드 보안을 보장합니다. CX Cloud와 CX Cloud Agent 간의 연결은 TLS로 보호됩니다. Cloud Agent의 기본 SSH 사용자는 기본 작업만 수행하도록 제한됩니다
.

물리적 보안

보안 VMware 서버 회사에 CX 클라우드 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 클라우드 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 만들 수 있습니다. cxcroot 사용자는 루트 권한을 얻을 수 있습니다.

네트워크 보안

CX 클라우드 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 사용자는 CX 클라우드 에이전트를 인증하고 CX 클라우드 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(https://swims.cisco.com/abraxas/decrypt)에서만 해독할 수 있는 RSA/ECB/PKCS1v1_5 암호화된 비밀번호를 표시합니다. 권한이 부여된 담당자만 이 포털에 액세스할 수 있습니다. cxcroot 사용자는 이 암호 해독된 암호를 사용하여 루트 권한을 얻을 수 있습니다. 암호는 2일 동안만 유효합니다. cxcadmin 사용자는 계정을 다시 만들고 SWIM 포털 게시물 암호 만료에서 암호를 얻어야 합니다.

강화

CX Cloud Agent 어플라이언스는 Center of Internet Security 강화 표준을 따릅니다.

데이터 보안

CX Cloud Agent 어플라이언스는 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 형

태로도 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 DNA Center 인벤토리, 진단 브리지, Intersight, 컴플라이언스 인사이트, 결함 및 CX 클라우드 에이전트가 수집한 기타 모든 텔레메트리 소스에 대한 적용 가능성에 따라 명령을 분류합니다.

자산 텔레메트리 내의 민감한 정보는 클라우드로 전송되기 전에 마스킹됩니다. CX 클라우드 에이전트는 CX 클라우드 에이전트에 직접 텔레메트리를 전송하는 수집된 모든 자산에 대해 민감한 데이터를 마스킹합니다. 여기에는 비밀번호, 키, 커뮤니티 문자열, 사용자 이름 등이 포함됩니다. 컨트롤러는 이 정보를 CX Cloud 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 DNA 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 Cloud Agent에서 수집한 기타 자산)에 설명된 대로 데이터 소스를 지정하여 어떤 자산의 텔레메트리 CX Cloud 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 생성

	한 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 클라우드 에이전트 애플리케이션 명령을 실행할 수 있으며 어플라이언스에 대한 권한이 가장 적음. cxcroot 사용자 및 해당 암호화된 비밀번호는 cxcadmin 사용자를 사용하여 생성됨 · cxcroot: cxcadmin은 "remoteaccount" 유틸리티를 사용하여 이 사용자를 만들 수 있습니다. 사용자는 이 계정으로 루트 권한을 얻을 수 있습니다.
cxcadmin 비밀번호 정책	·비밀번호는 SHA-256을 사용하여 단방향으로 해시되며 안전하게 저장됩니다 · 대문자, 소문자, 숫자 및 특수 문자 중 3개를 포함하는 8자 이상
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	· 대문자, 소문자, 숫자 및 특수 문자 중 세 가지를 포함하는 8자 이상 · 5회 로그인 실패 시 30분 동안 차단. 비밀번호는 90일 후에 만료
포트	수신 포트 열기 – 514(Syslog) 및 22(ssh)
데이터 보안	·저장된 고객 정보가 없습니다 ·저장된 디바이스 데이터가 없습니다 ·Cisco DNA Center 서버 인증서가 암호화되어 데이터베이스에 저장됩니다

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.