보안 엔드포인트에서 ID 지속성 구성

목차

소개

이 문서에서는 Cisco Secure Endpoint Identity Persistence 기능을 검토하는 방법에 대해 설명합니다.

ID 지속성이란 무엇입니까?

ID 지속성은 가상 환경 또는 컴퓨터가 다시 이미징될 때 일관된 이벤트 로그를 유지할 수 있는 기능입니다. 새 가상 세션이 시작되거나 컴퓨터가 다시 이미지화될 때마다 새 커넥터 레코드가 생성되지 않도록 MAC 주소 또는 호스트 이름에 커넥터를 바인딩할 수 있습니다. 이 기능은 비영구적 VM

및 랩 환경을 위해 특별히 설계되었으며 기존 워크스테이션 및 서버 설정에서 활성화해서는 안 됩니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Endpoints 포털 액세스
- Cisco TAC에 문의하여 조직에서 ID 지속성 기능을 활성화해야 합니다.
- ID 지속성은 Windows 운영 체제(OS)에서만 지원됩니다.

Id 지속성이 언제 필요합니까?

ID 지속성은 초기 커넥터 등록 시 보안 엔드포인트를 식별하는 데 도움이 되는 보안 엔드포인트의 기능으로, 특정 커넥터에 대한 MAC 주소 또는 호스트 이름과 같은 ID 매개변수를 기반으로 이전에 알려진 항목과 매칭합니다. 이 기능의 구현은 올바른 라이센스 수를 유지하는 데 도움이 될 뿐만 아니라 가장 중요한 것은 비영구 시스템에서 기록 데이터를 제대로 추적할 수 있도록 합니다.

가상 엔드포인트 구축

가상 구축에서 ID 지속성을 위해 가장 많이 사용되는 용도는 비영구적 VDI(Virtual Desktop Infrastructure) 구축입니다. VDI 호스트 데스크톱 환경은 최종 사용자의 요청 또는 필요에 따라 구축됩니다. 여기에는 VMware, Citrix, AWS AMI Golden Image Deployment 등과 같은 여러 벤더가 포함됩니다.

'스테이트풀 VDI'라고도 하는 영구 VDI는 각 개별 사용자의 데스크탑을 고유하게 사용자 지정하고 한 세션에서 다른 세션으로 '지속'하는 설정입니다. 이러한 유형의 가상 구축은 ID 지속성 기능이 필요하지 않습니다. 이러한 시스템은 정기적으로 다시 이미징되지 않기 때문입니다.

Secure Endpoint의 성능과 상호 작용할 수 있는 모든 소프트웨어와 마찬가지로, 기능을 최대화하고 영향을 최소화하기 위해 Virtual Desktop 애플리케이션도 가능한 제외 항목을 평가해야 합니다.

참조: https://docs.vmware.com/en/VMware-Horizon/2103/horizon-architecture-planning/GUID-AED54AE0-76A5-479B-8CD6-3331A85526D2.html

물리적 엔드포인트 구축

보안 엔드포인트 물리적 시스템에 ID 지속성 구축을 적용할 수 있는 시나리오는 두 가지입니다.

- Secure Endpoint 커넥터가 미리 설치된 골든 이미지로 물리적 엔드포인트를 배포하거나 이미지로 다시 설치할 경우 Goldenimage Flag를 활성화해야 합니다. ID 지속성은 다시 이미지화된 시스템의 인스턴스에서 중복을 방지하는 데 사용할 수 있지만 필수는 아닙니다.

- 골든 이미지로 물리적 엔드포인트를 배포하거나 이미지로 다시 설치한 후 나중에 보안 엔드포인트 커넥터를 설치할 경우 ID 지속성을 사용하여 이미지로 다시 설치된 시스템의 인스턴스에서 중복을 방지할 수 있지만 반드시 필요한 것은 아닙니다.

ID 지속성 프로세스 개요

1. 커넥터는 policy.xml 파일의 토큰과 함께 다운로드되며, 이를 클라우드 측의 해당 정책에 다시 연결합니다.
2. 커넥터가 설치되어 있으며 토큰을 local.xml에 저장하고 커넥터는 포털에 문제의 토큰과 함께 POST 요청을 수행합니다.
3. 클라우드는 다음과 같은 운영 순서를 거칩니다.
   a. 컴퓨터가 ID 동기화 정책 컨피그레이션에 대한 정책을 확인합니다. 이 기능이 없으면 정상적으로 등록이 수행됩니다.
   b. 정책 설정에 따라 등록은 기존 데이터베이스에서 호스트 이름 또는 MAC 주소를 확인합니다.
      비즈니스 전반:설정에 따라 호스트 이름 또는 MAC에서 모든 정책이 일치하는지 점검됩니다. 일치하는 개체 GUID가 기록되어 최종 클라이언트 컴퓨터로 다시 전송됩니다. 그런 다음 클라이언트 시스템은 UUID를 가정하고 이전에 매치한 호스트의 그룹/정책 설정을 가정합니다. 이는 설치된 정책/그룹 설정을 재정의합니다.
      전체 정책: 토큰 클라우드 측의 정책과 일치하며 해당 정책 내에서만 호스트 이름 또는 MAC 주소가 동일한 기존 객체를 찾습니다. 존재하는 경우 UUID를 가정합니다. 해당 정책에 연결된 기존 객체가 없는 경우 새 객체가 생성됩니다. 참고: 동일한 호스트 이름에 대해 다른 그룹/정책과 연결된 중복 항목이 존재할 수 있습니다.
   c. 토큰이 누락되어 그룹/정책에 일치시킬 수 없는 경우(이전에 등록된 경우, 잘못된 구축 사례 등) 커넥터가 비즈니스 탭에 설정된 기본 커넥터 그룹/정책에 속합니다. 그룹/정책의 설정에 따라 일치(회사 전반), 해당 정책(정책 전반) 또는 없음(없음)에 대한 모든 정책을 검토하려고 시도합니다. 이를 염두에 두고, 일반적으로 토큰 문제 발생 시 시스템이 올바르게 다시 동기화되도록 기본 그룹을 원하는 ID 동기화 설정이 포함된 그룹으로 설정하는 것이 좋습니다.

조직 내 중복 항목 파악

외부에서 사용 가능한 GitHub 스크립트

중복 UUID 찾기: https://github.com/CiscoSecurity/amp-04-find-duplicate-guids

중복 항목을 만드는 이유

중복된 항목이 사용자 측에서 발견될 수 있는 몇 가지 일반적인 경우가 있습니다.

1. VDI 풀이 진행되는 동안 다음 단계를 수행한 경우:

- 비영구 VM/VDI에 대한 초기 구축은 ID 지속성이 비활성화된 상태에서 수행됩니다(예: 골든 이미지 사용).
- 정책은 ID 지속성이 활성화되도록 클라우드에서 업데이트되며, 낮에는 엔드포인트에서 업데이트됩니다.
- 시스템은 새로 고침/리이미징됩니다(동일한 골든 이미지 사용). 그런 다음 ID 지속성 없이 원래 정책을 엔드포인트에 다시 배치합니다.
- 정책에 로컬에서 ID 지속성이 없으므로 등록 서버가 이전 레코드를 확인하지 않습니다.
- 이 플로우는 Duplicates(중복)가 됩니다.

2. 사용자가 한 그룹의 정책에 ID 지속성이 활성화된 원본 골든 이미지를 배포한 다음 보안 엔드포인트 포털에서 다른 그룹으로 엔드포인트를 이동합니다. 그런 다음 'moved-to' 그룹에 원래 레코드를 저장했다가 VM이 다시 이미징/재구축되면 원래 그룹에 새 복사본을 만듭니다.

참고: 이는 중복을 일으킬 수 있는 시나리오의 전체 목록이 아니라 가장 일반적인 시나리오 중 일부입니다.

잘못된 ID 지속성 구축과 관련된 일반적인 문제/증상

잘못된 ID 지속성 구현으로 인해 다음 문제/증상이 발생할 수 있습니다.

- 커넥터 시트 수가 잘못되었습니다.
- 잘못된 보고 결과
- 디바이스 전파 흔적 분석 데이터 불일치
- 감사 로그 내에서 시스템 이름 스왑
- 커넥터는 콘솔에서 무작위로 등록 및 등록 취소
- 커넥터가 클라우드에 제대로 보고되지 않음
- UUID 복제
- 시스템 이름 중복
- 데이터 불일치
- 재구성 후 시스템이 기본 비즈니스 그룹/정책에 등록됩니다.

- 정책에서 ID 지속성을 활성화하여 수동으로 구축.

- 정책에서 ID 지속성이 이미 활성화된 상태에서 명령줄 스위치를 통해 엔드포인트를 수동으로 배포한 다음 나중에 엔드포인트를 제거하고 다른 그룹/정책의 패키지로 다시 설치하려고 하면 엔드포인트가 자동으로 원래 정책으로 다시 전환됩니다.

- 자체 정책 스위치를 보여주는 SFC 로그의 출력(1~10초)

```
(167656, +0 ms) Dec 14 11:37:17 [1308]: Util::VerifyOsVersion: ret 0
(167656, +0 ms) Dec 14 11:37:17 [1308]: ERROR: ETWEnableConfiguration::IsETWEnabled: ETW not initialize
(167656, +0 ms) Dec 14 11:37:17 [1308]: UiPublisher::PublishPolicyInfo: Name -UTMB-WinServer-Protect Se
(167656, +0 ms) Dec 14 11:37:17 [1308]: UiPublisher::PublishLastPolicyUpdateTime: Publish Last Policy U
(167656, +0 ms) Dec 14 11:37:17 [1308]: UiPublisher::PublishAgentVersion: Agent Version 7.5.7.21234
(167656, +0 ms) Dec 14 11:37:17 [1308]: HeartBeat::PolicyNotifyCallback: EXIT
(167656, +0 ms) Dec 14 11:37:17 [1308]: AmpkitRegistrationHandler::PolicyCallback: EXIT (0)
.
.
.
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitRegistrationHandler::UpdateConfiguration: Enter
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitRegistrationHandler::UpdateConfiguration: Aborting - not
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitRegistrationHandler::ConnectionStateChanged: Starting Pro
(173125, +0 ms) Dec 14 11:37:22 [4704]: UIPipe::SendPolicyReloaded sending policy reloaded to UI. ui.da
(173125, +0 ms) Dec 14 11:37:22 [4704]: PipeSend: sending message to user interface: 28, id: 0
(173125, +0 ms) Dec 14 11:37:22 [4704]: UIPipe::SendStatus: notifying UI: No Product
(173125, +0 ms) Dec 14 11:37:22 [4704]: UIPipe::SendStatus: notifying UI: No Product
(173125, +0 ms) Dec 14 11:37:22 [4704]: UIPipe::SendStatus: notifying UI: No Product
(173125, +0 ms) Dec 14 11:37:22 [4704]: UIPipe::SendStatus : engine1 (0, 0), engine2 (0, 0)
(173125, +0 ms) Dec 14 11:37:22 [4704]: PipeSend: sending message to user interface: 1, id: 0
```

```
(173125, +0 ms) Dec 14 11:37:22 [4704]: UiStatusHandler::ConnectionStateChangedState: 0
(173125, +0 ms) Dec 14 11:37:22 [4704]: UiPublisher::PublishConnectionStatus: State 0
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpApiServer.cpp:AmpApiServer::PublishScanAvailable:223: Cloud
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitProxyHelper::LoadProxyFromConfig: Enter
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitProxyHelper::LoadProxyFromConfig proxy server is NULL
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitProxyHelper::LoadProxyFromConfig: Direct connection detec
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitProxyHelper::LoadProxyFromConfig: Exit(1)
(173125, +0 ms) Dec 14 11:37:22 [4704]: UiAgentGuidUpdater::ConnectionStateChanged
(173125, +0 ms) Dec 14 11:37:22 [4704]: UiAgentGuidUpdater::RefreshAgentGuidUi: Agent GUID: e1a756e2-65
(173125, +0 ms) Dec 14 11:37:22 [4704]: UiPublisher::PublishAgentGuid: Agent GUID did not change (e1a75
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitSubscriptionThread::NotificationWorker: Waiting on queue
```

다른 그룹에 속한 커넥터를 설치하려고 할 경우 다른 부작용이 발생합니다. 포털에서 커넥터가 올바른 그룹에 할당되었지만 원래 정책이 "잘못된"것임을 확인할 수 있습니다

이는 ID 지속성(ID 동기화)이 작동하는 방식 때문입니다.

ID SYNC가 없으면 커넥터가 완전히 제거되거나 재등록 명령줄 스위치를 사용하여 제거됩니다. 제거 시 새 만든 날짜 및 커넥터 GUID가 표시되거나 재등록 명령의 경우 새 커넥터 GUID만 표시됩니다. 그러나 ID SYNC를 사용하면 ID SYNC가 이전 GUID 및 날짜를 덮어씁니다. 그게 우리가 호스트를 '동기화'하는 방법입니다.

이 문제가 관찰된 경우 정책 변경을 통해 수정을 구현해야 합니다. 영향을 받는 엔드포인트를 원래 그룹/정책으로 다시 이동하고 정책이 동기화되는지 확인해야 합니다. 그런 다음 엔드포인트를 원하는 그룹/정책으로 다시 이동합니다

구축 모범 사례

snapvol 파일 구성

VDI 인프라에 애플리케이션 볼륨을 사용하는 경우 snapvol.cfg 컨피그레이션에 대해 이러한 컨피그레이션을 변경하는 것이 좋습니다

이러한 제외는 snapvol.cfg 파일에 구현해야 합니다.

경로:

- C:\Program Files\Cisco\AMP
- C:\ProgramData\Cisco
- C:\Windows\System32\drivers
- C:\Windows\System32\drivers\ImmunetNetworkMonitor.sys
- C:\Windows\System32\drivers\immunetprotect.sys
- C:\Windows\System32\drivers\immunetselfprotect.sys
- C:\Windows\System32\drivers\ImmunetUtilDriver.sys
- C:\Windows\System32\drivers\trufos.sys

레지스트리 키:

- HKEY_LOCAL_MACHINE\SOFTWARE\Immunet 보호

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Immunet 보호
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\CiscoAMP을 참조하십시오.
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CiscoAMPCEFWDriver을 참조하십시오.
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CiscoAMPELAMDriver을 참조하십시오.
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CiscoAMPHeurDriver을 참조하십시오.
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CiscoOrbital을 참조하십시오.
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CiscoSAM을 참조하십시오.
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CiscoSCMS을 참조하십시오.
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ImmunetProtectDriver을 참조하십시오.
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ImmunetSelfProtectDriver을 참조하십시오.
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Trufos을 참조하십시오.

x64 시스템에서 다음을 추가합니다.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Immunet 보호
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstal 보호

참조:

- https://docs.vmware.com/en/VMware-App-Volumes/index.html
- https://docs.vmware.com/en/VMware-App-Volumes/2103/app-volumes-admin-guide/GUID-0B588F2C-4054-4C5B-B491-F55BDA33A028.html

포털 정책 계획

다음은 Secure Endpoint Portal에서 ID 지속성을 구현할 때 따라야 할 모범 사례입니다.

1. 더 쉬운 분리를 위해 ID 지속성 엔드포인트에 대해 별도의 정책/그룹을 사용하는 것이 좋습니다.

2. Endpoint Isolation(엔드포인트 격리)을 사용하고 Move Computer to Group on Compromise(보안 침해 시 컴퓨터를 그룹으로 이동) 작업을 구현하려는 경우 또한 대상 그룹에는 ID 지속성이 활성화되어 있어야 하며 VDI 컴퓨터에만 사용해야 합니다.

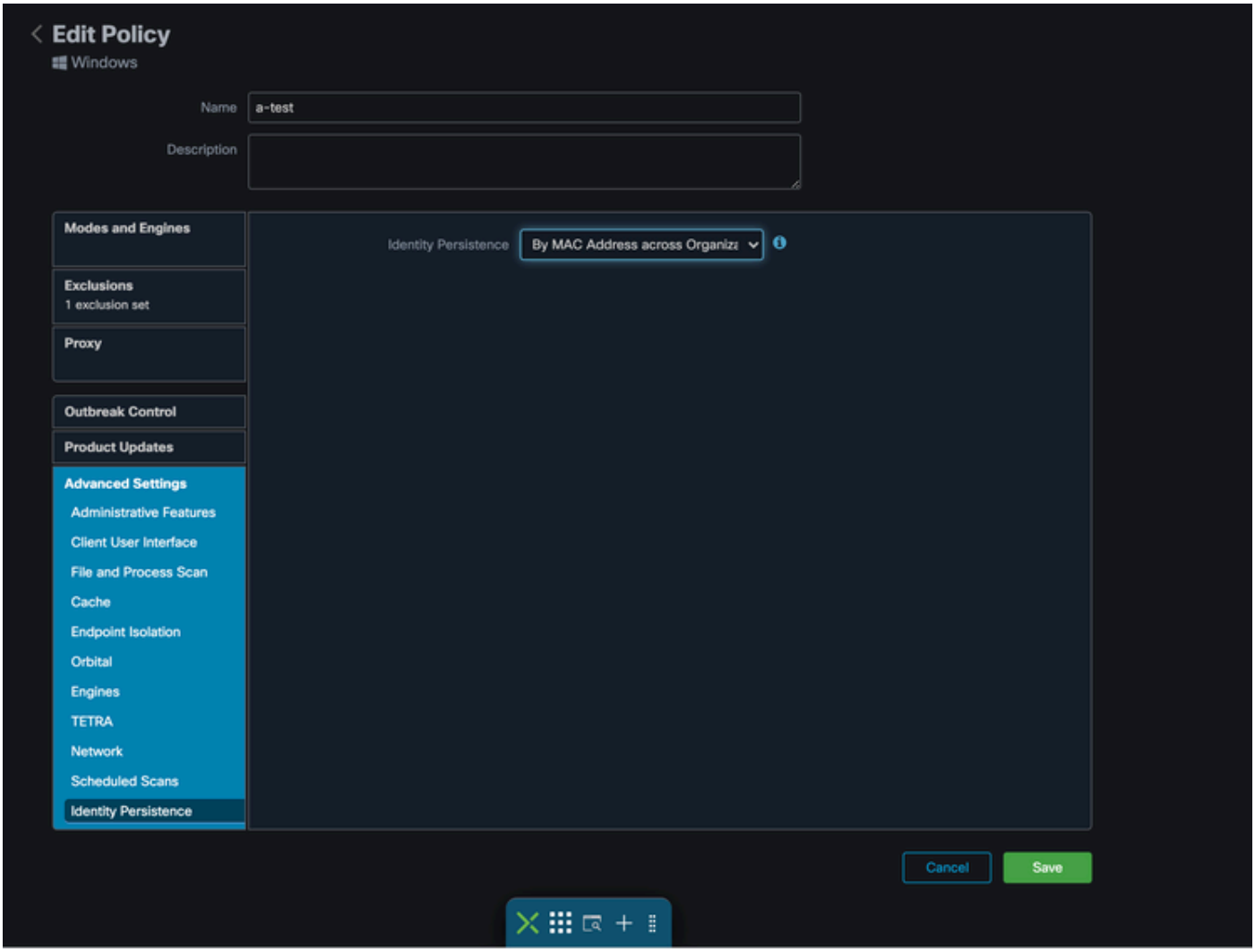
3. 조직 간의 설정 범위로 모든 정책에 대해 ID 지속성을 활성화하지 않은 경우 조직 설정의 기본 그룹/정책에서 ID 지속성을 활성화하지 않는 것이 좋습니다.

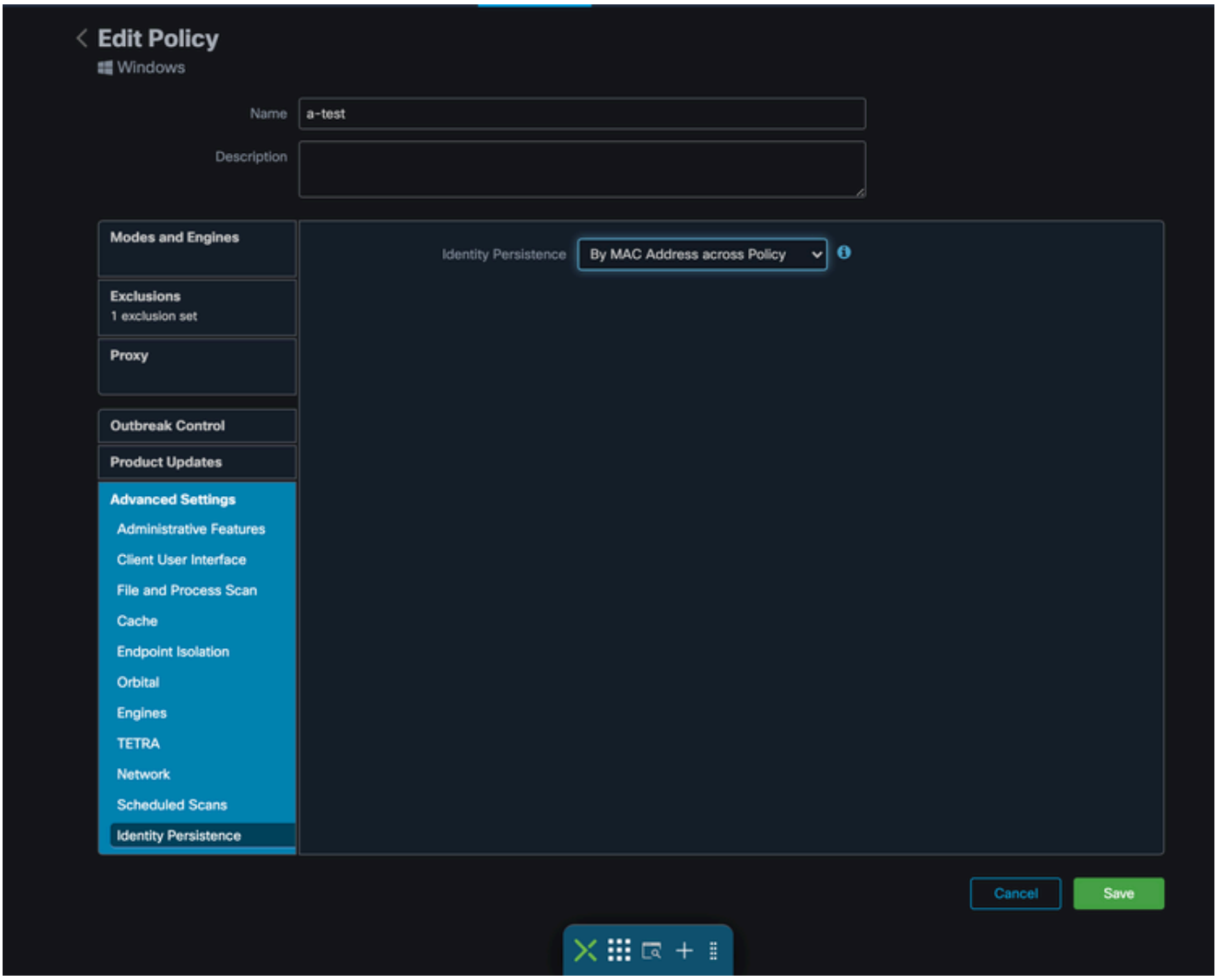
설정

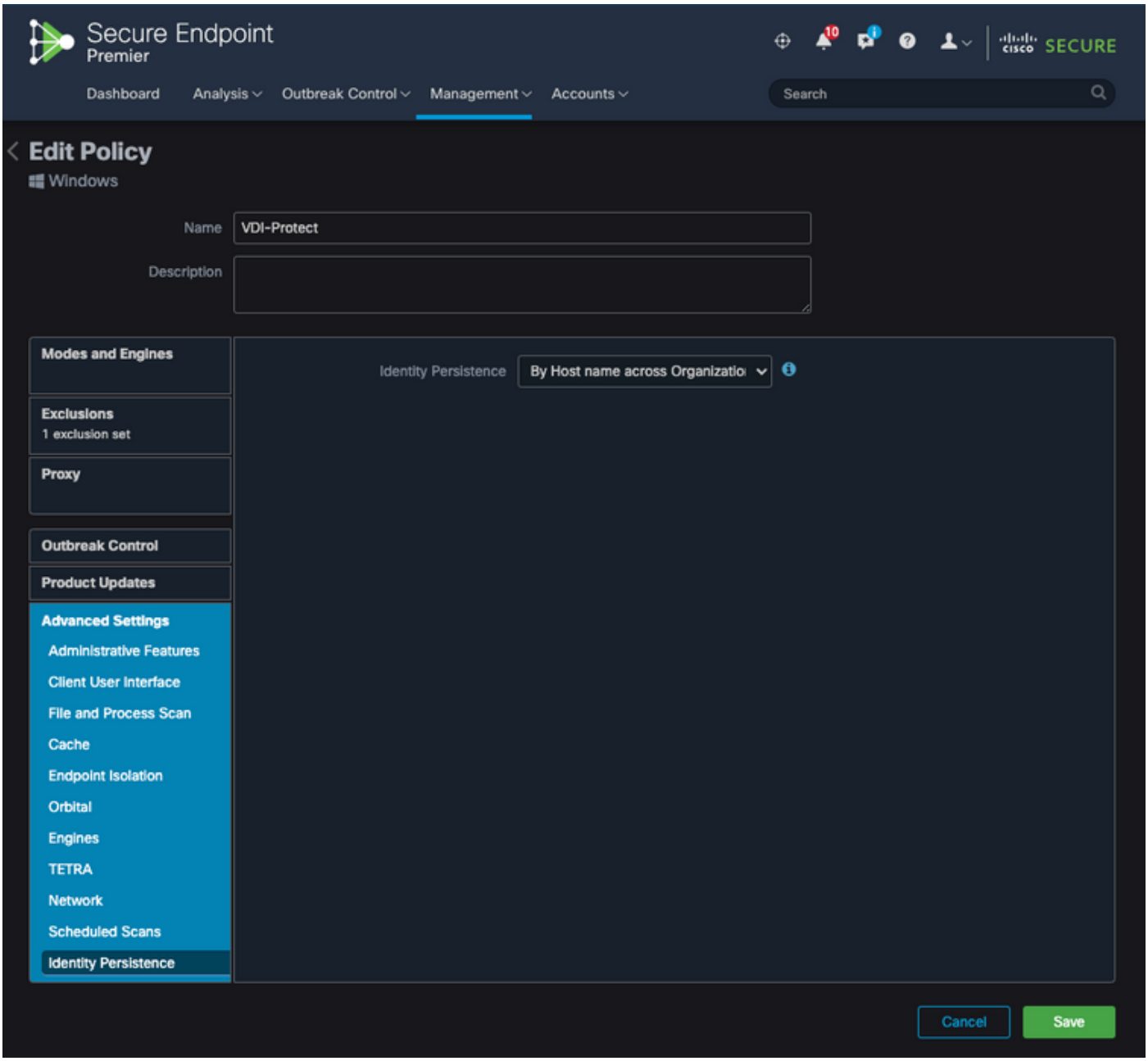
ID 지속성을 가진 보안 엔드포인트 커넥터를 구축하려면 다음 단계를 수행합니다.

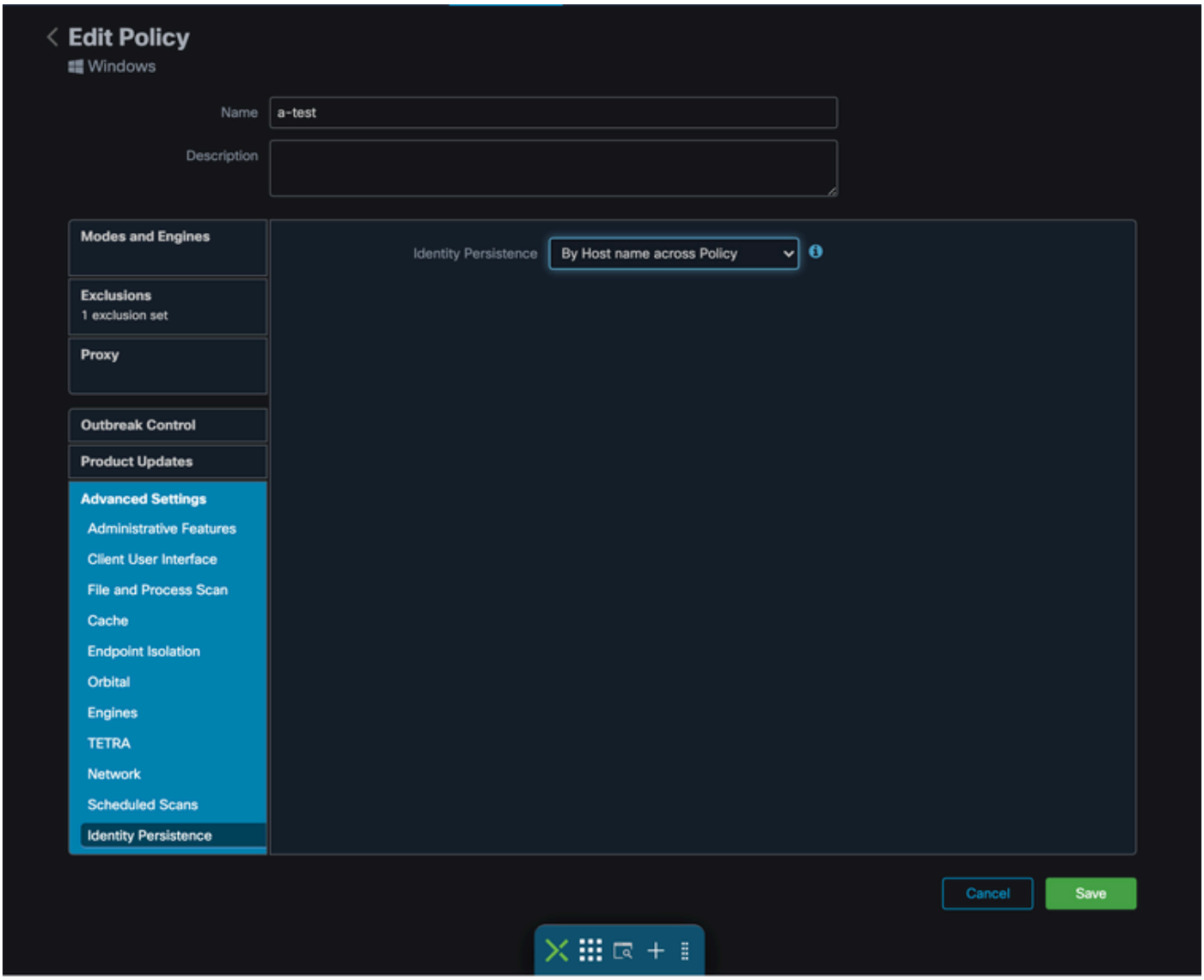
1단계. 원하는 ID 지속성 설정을 정책에 적용합니다.

- Secure Endpoint(보안 엔드포인트) 포털에서 Management(관리) > Policies(정책)로 이동합니다.
- ID 지속성을 활성화할 원하는 정책을 선택한 다음 Edit(수정)를 클릭합니다.
- Advanced Settings(고급 설정) 탭으로 이동한 다음 하단의 Identity Persistence(ID 지속성) 탭을 클릭합니다.
- Identity Persistence(ID 지속성) 드롭다운을 선택하고 환경에 가장 적합한 옵션을 선택합니다. 이 이미지를 참조하십시오.




Edit Policy
Windows
Name
a-test
Description
Modes and Engines
Exclusions
1 exclusion set
Proxy
Outbreak Control
Product Updates
Advanced Settings
Administrative Features
Client User Interface
File and Process Scan
Cache
Endpoint Isolation
Orbital
Engines
TETRA
Network
Scheduled Scans
Identity Persistence
Identity Persistence
By MAC Address across Policy
Cancel
Save


Secure Endpoint
Premier
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
SECURE
Edit Policy
Windows
Name
VDI-Protect
Description
Modes and Engines
Exclusions
1 exclusion set
Proxy
Outbreak Control
Product Updates
Advanced Settings
Administrative Features
Client User Interface
File and Process Scan
Cache
Endpoint Isolation
Orbital
Engines
TETRA
Network
Scheduled Scans
Identity Persistence
Identity Persistence
By Host name across Organizatio
Cancel
Save



5가지 옵션 중에서 선택할 수 있습니다.

- Feature가 활성화되지 않았습니다. 어떤 상황에서도 커넥터 UUID는 새 커넥터 설치와 동기화되지 않습니다. 새로 설치할 때마다 새 시스템 객체가 생성됩니다.
- By MAC Address across Business(비즈니스 전반에 걸쳐 MAC 주소 기준): 이전 기록 데이터를 새 등록과 동기화하기 위해 신규 또는 새로 고친 설치에서 동일한 MAC 주소를 가진 최신 커넥터 레코드를 찾습니다. 이 설정은 모든 비즈니스 레코드를 검사합니다

  Identity Synchronization(ID 동기화)이 None(없음) 이외의 값으로 설정된 조직의 모든 정책 전반에 걸쳐 적용됩니다. 커넥터는 이전 설치가 새 설치와 다를 경우 이전 설치를 반영하도록 정책을 업데이트할 수 있습니다.

- By MAC Address across Policy(정책 전반의 MAC 주소 기준): 이전 기록 데이터를 새 등록과 동기화하기 위해 신규 또는 새로 고친 설치에서 동일한 MAC 주소를 가진 최신 커넥터 레코드를 찾습니다. 이 설정은 배포에 사용된 정책과 연결된 레코드만 살펴봅니다. 커넥터가 이전에 이 정책에 설치되지 않았지만 이전에 다른 정책에서 활성화된 경우 중복 항목을 생성할 수 있습니다.
- By Hostname across Business(비즈니스 전반에 걸쳐 호스트 이름별): 이전 기록 데이터를 새 등록과 동기화하기 위해 새로 설치하거나 새로 고친 설치에서 동일한 호스트 이름을 가진 가

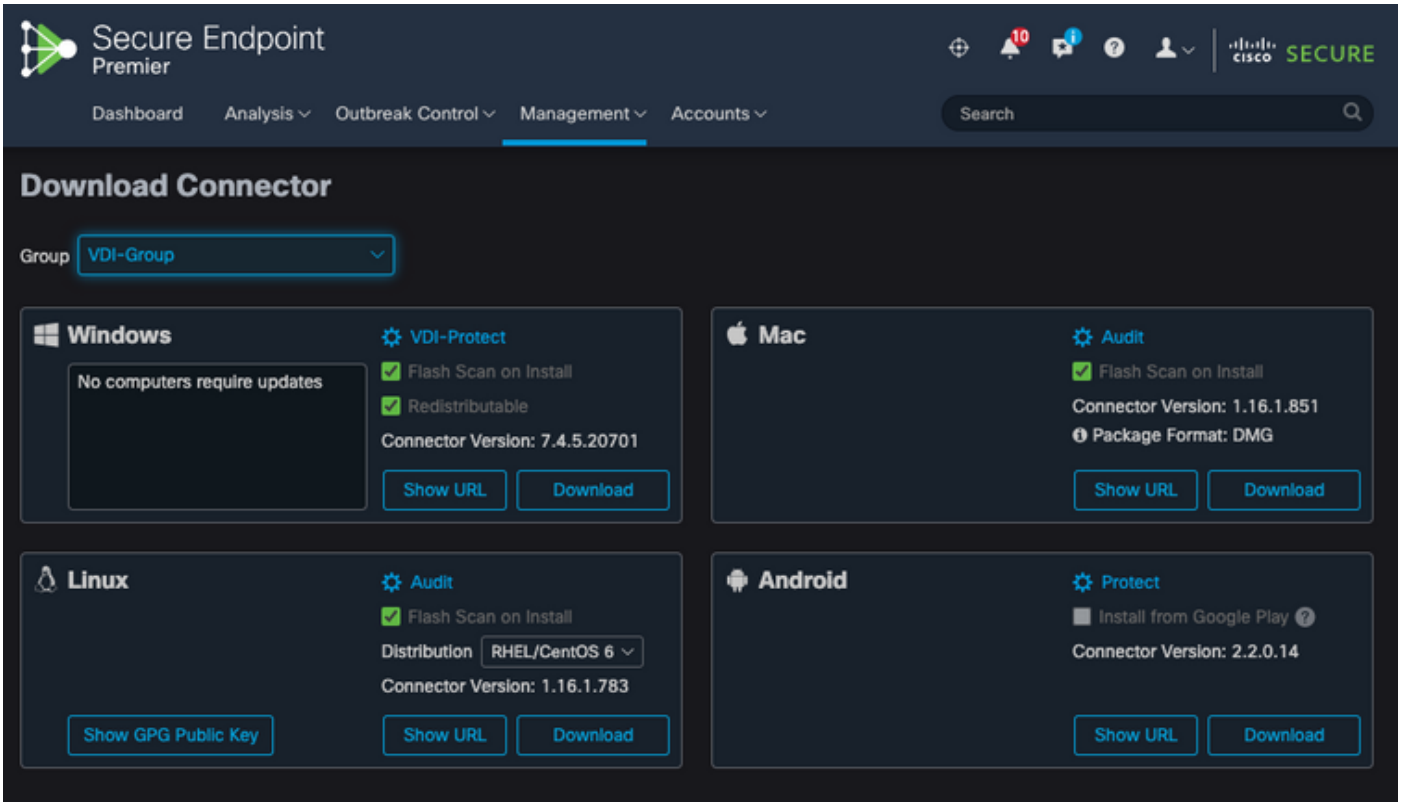
장 최근의 커넥터 레코드를 찾습니다. 이 설정은 다른 정책의 ID 지속성 설정과 상관없이 모든 비즈니스 레코드를 검사하며, 새 설정과 다를 경우 커넥터가 이전 설치를 반영하도록 정책을 업데이트할 수 있습니다. 호스트 이름에는 FQDN이 포함되어 있으므로 커넥터가 정기적으로 네트워크 간에 이동하는 경우(예: 랩톱) 중복이 발생할 수 있습니다.

- By Hostname across Policy(정책 전반의 호스트 이름별): 이전 기록 데이터를 새 등록과 동기화하기 위해 새 설치 또는 새로 고친 설치에서 동일한 호스트 이름을 가진 가장 최근의 커넥터 레코드를 찾습니다. 이 설정은 배포에 사용된 정책과 연결된 레코드만 살펴봅니다. 커넥터가 이전에 이 정책에 설치되지 않았지만 이전에 다른 정책에서 활성화된 경우 중복 항목을 생성할 수 있습니다. 호스트 이름에는 FQDN이 포함되어 있으므로 커넥터가 정기적으로 네트워크 간에 이동하는 경우에도 중복이 발생할 수 있습니다(예: 랩톱).

참고: Identity Persistence(ID 지속성)를 사용하도록 선택한 경우 Cisco에서는 By Hostname(호스트 이름별)을 Business(비즈니스) 또는 Policy(정책) 전체에서 사용하도록 권장합니다. 하나의 시스템에는 하나의 호스트 이름이 있지만 둘 이상의 MAC 주소가 있을 수 있으며 여러 VM이 MAC 주소를 복제할 수 있습니다.

2단계. Secure Endpoint Connector를 다운로드합니다.

- Management(관리) > Download Connector(커넥터 다운로드)로 이동합니다.
- 1단계에서 편집한 정책의 그룹을 선택합니다.
- 이미지에 표시된 대로 Windows 커넥터에 대한 다운로드를 클릭합니다.



3단계. 엔드포인트에 Connector를 구축합니다.

- 이제 다운로드한 커넥터를 사용하여 엔드포인트에 보안 엔드포인트(ID 지속성이 활성화된 상태)를 수동으로 설치할 수 있습니다.

- 그렇지 않으면 골든 이미지를 사용하여 커넥터를 구축할 수도 있습니다(이미지 참조)

참고: 재배포 가능 설치 관리자를 선택해야 합니다. 이 파일은 32비트 및 64비트 설치 프로그램이 모두 포함된 ~57MB(최신 버전에 따라 크기가 다를 수 있음) 파일입니다. 여러 컴퓨터에 Connector를 설치하려면 이 파일을 네트워크 공유에 두거나 모든 컴퓨터에 푸시할 수 있습니다. 설치 프로그램에는 설치를 위한 컨피그레이션 파일로 사용되는 policy.xml 파일이 포함되어 있습니다.

골든 이미지 생성

VDI 복제 프로세스에 사용할 골든 이미지를 만들 때는 공급업체 문서(VMware, Citrix, AWS, Azure 등)의 모범 사례 지침을 따르십시오.

예를 들어, VMware Golden Image Process: https://docs.vmware.com/en/VMware-Horizon/2106/virtual-desktops/GUID-D9C46AEF-1C41-4711-BF9E-84362EBE6ABF.html.

VMware를 식별했듯이, AWS 작성 프로세스는 VM 컨피그레이션을 완료하기 전에 복제된(자식 VM)을 여러 번 다시 시작하므로, 현재 복제된(자식 VM)에 최종/올바른 호스트 이름이 할당되지 않아 복제된(자식 VM)이 골든 이미지 호스트 이름을 사용하고 보안 엔드포인트 클라우드에 등록하기 때문에 보안 엔드포인트 등록 프로세스에 문제가 발생합니다. 이로 인해 복제 프로세스가 중단되고 문제가 발생합니다.

이는 보안 엔드포인트 커넥터 프로세스에서는 문제가 되지 않지만 복제 프로세스 및 보안 엔드포인트 등록에서는 호환되지 않습니다. 이 문제를 방지하기 위해 복제 프로세스에서 구현할 몇 가지 변경 사항을 식별했으며, 이는 이러한 문제를 해결하는 데 도움이 됩니다.

이미지가 복제되도록 고정되기 전에 Golden Image VM에 구현해야 하는 변경 사항입니다

1. 보안 엔드포인트를 설치할 때 골든 이미지에 Goldenimage 플래그를 항상 사용합니다.

2. Golden Image Setup Script 및 Golden Image Startup Script 섹션을 구현하여 복제된(하위 VM)에 최종 호스트 이름이 구현된 경우에만 엔드포인트 서비스를 켜는 데 도움이 되는 스크립트를 찾습니다. 자세한 내용은 VMware Horizon 복제 문제 섹션을 참조하십시오.

골든 이미지 재정의 플래그

설치 프로그램을 사용할 때 골든 이미지에 사용할 플래그는 /goldenimage 1입니다.

골든 이미지 플래그는 커넥터가 시작되어 기본 이미지에 등록되지 않도록 합니다. 따라서 이미지의 다음 시작에서 커넥터는 지정된 정책에 의해 구성되었던 기능 상태에 있습니다.

다른 Flags에 대한 자세한 내용은 이 문서를 참조하십시오.

설치 프로그램을 사용할 때 골든 이미지에 사용할 새 플래그는 /goldenimage [1|0]입니다

0 - 기본값 - 이 값은 골든 이미지 옵션을 트리거하지 않으며, 설치 프로그램이 옵션 없이 실행된 것처럼 작동합니다. 초기 커넥터 등록 및 설치 시 시작을 건너뛰지 마십시오.

```
C:\> CiscoInstaller_goldenimage.exe /R /S /goldenimage 0 [other options…]
```

1 - 골든 이미지로 설치합니다. 이는 플래그와 함께 사용되는 일반적인 옵션이며 유일한 예상 사용량입니다. 설치 시 초기 커넥터 등록 및 시작을 건너뜁니다.

```
C:\> CiscoInstaller_goldenimage.exe /R /S /goldenimage 1 [other flags here…]
```

골든 이미지 생성 단계

골든 이미지 준비를 위해 커넥터를 마지막으로 설치하는 것이 가장 좋습니다.

1. Windows 이미지를 요구 사항에 맞게 준비하고 커넥터를 제외한 모든 필수 소프트웨어 및 Windows 이미지 구성을 설치합니다.
2. Cisco Secure Endpoint 커넥터를 설치합니다.

이/goldenimage 1 플래그를 사용하여 설치 관리자에게 골든 이미지 구축임을 나타냅니다.

```
C:\> CiscoInstaller_goldenimage.exe /R /S /goldenimage 1
```

3. 여기 설명된 대로 스크립트 로직 구현(필요한 경우)

4. 설치 완료

5. 골든 이미지 동결

Golden Image(골든 이미지)에 애플리케이션이 설치된 후 시스템이 준비되고 보안 엔드포인트가 /goldenimageflag와 함께 설치되면 호스트를 고정하고 배포할 준비가 됩니다. 복제된 호스트가 부팅되면 Secure Endpoint가 시작되고 클라우드에 등록됩니다. 정책 또는 호스트를 변경하려는 경우가 아니면 커넥터 구성과 관련하여 추가 작업이 필요하지 않습니다. 골든 이미지 등록이 완료된 후 변경 사항이 있는 경우 이 프로세스를 다시 시작해야 합니다. 이 플래그는 커넥터가 시작되어 기본 이미지에 등록되는 것을 방지합니다. 이미지의 다음 시작에서 커넥터는 할당된 정책에 의해 구성되었던 기능 상태가 됩니다.

참고: VM을 고정할 수 있기 전에 Golden Image가 Secure EndpointCloud에 등록되면 Golden Image VM에서 Secure Endpoint를 제거하고 다시 설치한 다음 다시 VM을 고정하여 등록 및 중복 커넥터 문제를 방지하는 것이 좋습니다. 이 제거 프로세스의 일부로 Secure Endpoint에 대한 레지스트리 값을 수정하는 것은 권장되지 않습니다.

골든 이미지 업데이트

등록되지 않은 커넥터를 유지하기 위해 골든 이미지를 업데이트해야 하는 경우 두 가지 옵션이 있습니다.

권장 프로세스

1. 커넥터를 제거합니다.
2. 호스트 업데이트/업그레이드를 설치합니다.
3. 골든 이미지 플래그를 사용하여 골든 이미지 프로세스 후에 커넥터를 다시 설치합니다.
4. 프로세스를 따르는 경우 호스트가 커넥터를 시작하면 안 됩니다.
5. 이미지를 고정합니다.
6. 클론을 생성하기 전에 골든 이미지가 포털에 등록되지 않았는지 확인하여 원치 않는 중복 호스트를 방지합니다.

대체 프로세스

1. 호스트가 인터넷에 연결되어 있지 않은지 확인하여 커넥터가 등록되지 않도록 합니다.
2. 커넥터 서비스를 중지합니다.
3. 업데이트를 설치합니다.
4. 업데이트가 완료되면 이미지 고정
5. 중복 호스트가 발생하지 않도록 하려면 커넥터의 등록을 방지해야 합니다. 연결을 제거하면 클라우드에 등록하기 위해 연결이 차단됩니다. 또한 중지되는 커넥터는 다음 재부팅 시까지 이 상태를 유지하므로 클론이 고유한 호스트로 등록할 수 있습니다.
6. 클론을 생성하기 전에 골든 이미지가 포털에 등록되지 않았는지 확인하여 원치 않는 중복 호스트를 방지합니다.

골든 이미지 코드

이 섹션은 Golden Image Process를 지원하고 ID 지속성을 구현할 때 커넥터 중복을 방지하는 데 도움이 되는 코드 조각으로 구성되어 있습니다.

골든 이미지 설정 스크립트

설치 스크립트 설명

첫 번째 스크립트인 'Setup'은 복제 전에 골든 이미지에서 실행됩니다. 한 번만 수동으로 실행해야 합니다. 주요 목적은 다음 스크립트가 복제된 가상 머신에서 올바르게 작동할 수 있도록 하는 초기 컨피그레이션을 설정하는 것입니다. 이러한 컨피그레이션에는 다음이 포함됩니다.

- 자동 시작을 방지하기 위해 Cisco Secure Endpoint Service 시작을 수동으로 변경합니다.
- 최고 권한을 가진 시스템 시작 시 다음 스크립트(시작)를 실행하는 예약 작업 생성
- 골든 이미지의 호스트 이름을 저장하는 "AMP_GOLD_HOST"라는 시스템 환경 변수를 생성합니다. 이는 Startup 스크립트에서 변경 사항을 되돌려야 하는지 확인하는 데 사용됩니다

설치 스크립트 코드

```
rem Turn AMP to manual start
sc config CiscoAMP start=demand
```

```
rem Add host name to a system variable that we can check on startup
setx -m AMP_GOLD_HOST %COMPUTERNAME%

rem Add the startup script to the startup scripts
rem /rp password when there is a password
schtasks /create /tn "Startamp" /tr "C:\Users\XXXXXX\Desktop\VMWareHorizonAMPStartup.bat" /sc onstart /
```

설치 스크립트 코드는 매우 간단합니다.

행 2: 악성코드 차단 서비스의 시작 유형을 manual로 변경합니다.

행 5: "AMP_GOLD_HOST"라는 새 환경 변수를 만들고 현재 컴퓨터의 호스트 이름을 저장합니다.

행 9: "Startamp"라는 이름의 예약된 작업을 만듭니다. 이 작업은 시스템 시작 중에 비밀번호 없이 가장 높은 권한으로 지정된 'Startamp' 스크립트를 실행합니다.

골든 이미지 시작 스크립트

시작 스크립트 설명

두 번째 스크립트인 'Startup'은 복제된 가상 머신의 각 시스템 시작에서 실행됩니다. 주요 목적은 현재 시스템의 호스트 이름이 '골든 이미지'인지 확인하는 것입니다.

- 현재 시스템이 골든 이미지이면 작업이 수행되지 않고 스크립트가 종료됩니다. 예약된 작업을 유지 관리하므로 보안 끝점은 시스템 시작 시 계속 실행됩니다.
- 현재 시스템이 '골든' 이미지가 아닌 경우 첫 번째 스크립트에서 변경한 내용이 재설정됩니다.
  - Cisco Secure Endpoint Service 시작 컨피그레이션을 자동으로 변경합니다.
  - Cisco Secure Endpoint Service 시작
  - "AMP_GOLD_HOST" 환경 변수를 제거합니다.
  - 시작 스크립트를 실행하는 예약 작업을 삭제하고 스크립트 자체를 삭제합니다.

시작 스크립트 코드

```
echo "Current hostname: %COMPUTERNAME% vs %AMP_GOLD_HOST%"

if "%COMPUTERNAME%" == "%AMP_GOLD_HOST%" ( goto same ) else ( goto notsame )

:same
rem Do nothing as we are still the golden image name
goto exit

:notsame
rem Turn AMP to autostart
sc config CiscoAMP start=auto

rem Turn on AMP
sc start CiscoAMP

rem Remove environment variable
REG delete "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" /F /V AMP_GOLD_HOST
```

```
schtasks /delete /tn Startamp

goto exit
:exit
```

행 2: 현재 호스트 이름을 저장된 "AMP_GOLD_HOST" 값과 비교합니다. 동일한 경우 스크립트는 "same" 레이블로 이동하고, 그렇지 않으면 "notsame" 레이블로 이동합니다.

행 4-6: "동일한" 레이블에 도달하면 스크립트는 여전히 골든 이미지이므로 아무 작업도 수행하지 않고 "종료" 레이블로 진행합니다.

행 8-16: "notsame" 레이블에 도달하면 스크립트는 다음 작업을 수행합니다.

- 악성코드 차단 서비스의 시작 유형을 automatic으로 변경합니다.
- 악성코드 차단 서비스를 시작합니다.
- "AMP_GOLD_HOST" 환경 변수를 제거합니다.
- "Startamp"라는 예약된 작업을 삭제합니다.

참고: 이 문서에 포함된 스크립트는 TAC에서 공식적으로 지원하지 않습니다.

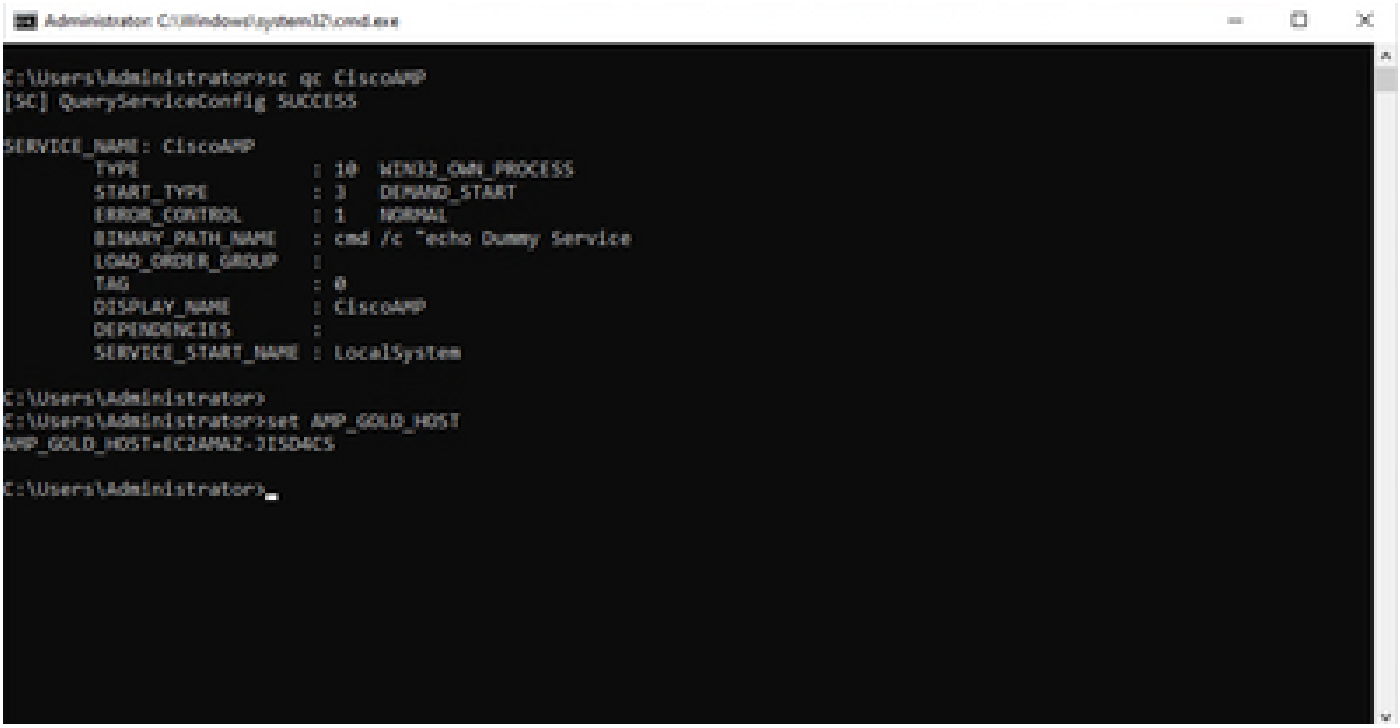
참고: 이 두 스크립트는 복제된 가상 머신 환경에서 Cisco AMP 서비스를 시작할 수 있게 해줍니다. Golden 이미지를 올바르게 구성하고 시작 스크립트를 사용하면 Cisco Secure Endpoint가 올바른 컨피그레이션으로 복제된 모든 가상 머신에서 실행되도록 할 수 있습니다.

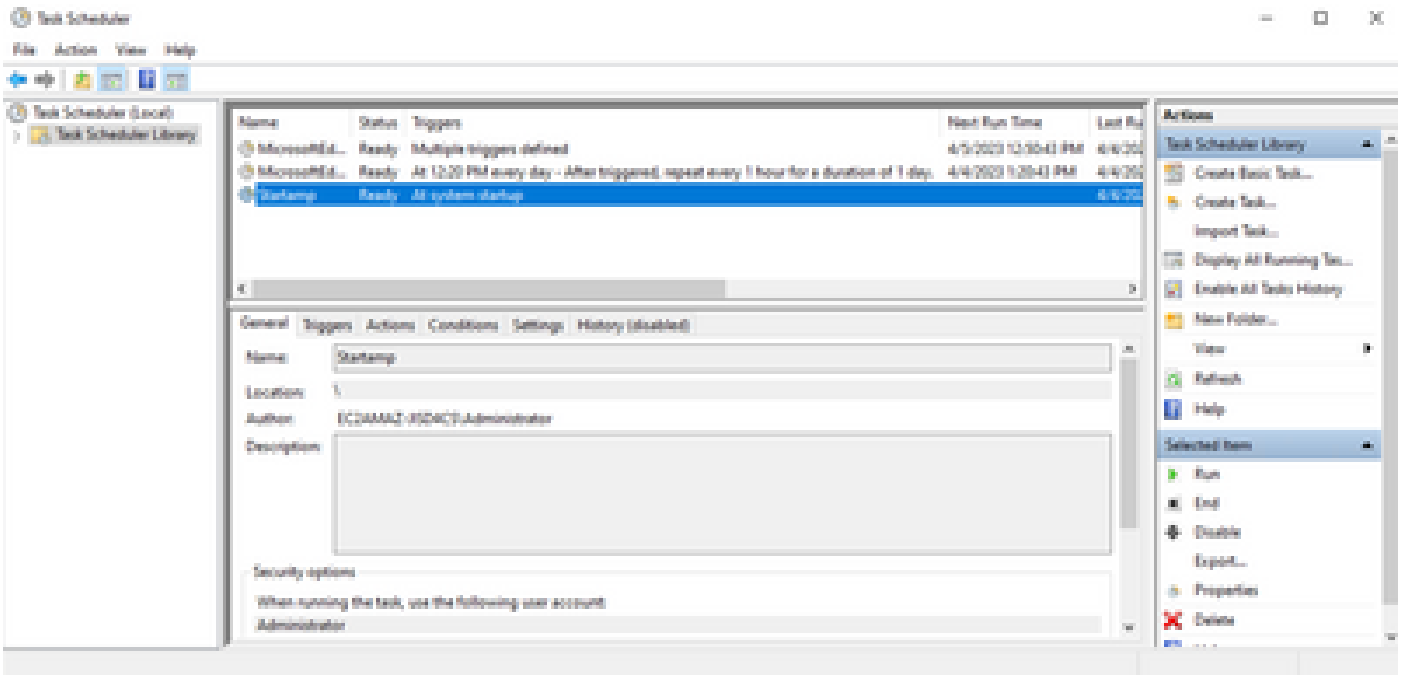
AWS Workspace 프로세스

이 솔루션은 복제 전에 골든 이미지에서 실행되는 '설치' 스크립트와 시스템 시작 중에 복제된 각 가상 머신에서 실행되는 '시작' 스크립트로 구성됩니다. 이러한 스크립트의 주요 목적은 수동 작업을 줄이면서 서비스의 올바른 구성을 보장하는 것입니다. 이 두 스크립트를 사용하면 복제된 가상 머신 환경에서 Cisco Secure Endpoint Service를 시작할 수 있습니다. Golden 이미지를 올바르게 구성하고 시작 스크립트를 사용하면 Cisco Secure Endpoint 커넥터가 올바른 컨피그레이션으로 복제된 모든 가상 머신에서 실행되도록 할 수 있습니다

AWS Workspace에서 골든 이미지를 구현하는 데 필요한 스크립트 코드는 골든 이미지 설정 스크립트 코드 및 골든 이미지 시작 스크립트 코드 섹션을 참조하십시오.

설치 스크립트를 실행한 후 컨피그레이션 변경 사항이 성공적으로 구축되었는지 확인할 수 있습니다.





골든 이미지에 대해 이 작업을 수행했으므로 모든 새 인스턴스는 이 컨피그레이션을 갖게 되며 시작 시 시작 스크립트를 실행합니다.

VMware Horizon 중복 문제

VMware Horizon을 사용하면 Horizon 작성 프로세스의 일부로 하위 VM 시스템을 생성할 때 여러 번 재부팅하는 것을 확인할 수 있습니다. 이렇게 하면 하위 VM이 준비되지 않은 경우(최종/올바른 NetBios 이름이 할당되지 않은 경우) 보안 엔드포인트 서비스가 활성화될 때 문제가 발생합니다. 이로 인해 보안 엔드포인트에서 혼동이 발생하여 프로세스가 중단되는 문제가 추가로 발생합니다. 이 문제를 방지하기 위해 Horizon Process와의 비호환성을 위한 솔루션을 마련했습니다. 여기에는 Golden Image VM에 첨부된 스크립트를 구현하고 VMware Horizon의 동기화 후 스크립트 기능

(https://docs.vmware.com/en/VMware-Horizon/2103/published-desktops-applications.pdf)을 사용하는 것이 포함됩니다.

더 이상 구성/변경 필요 없음

- 첫 번째 구축 후 골든 이미지를 변경하려면 Secure Endpoint를 더 이상 제거하고 다시 설치할 필요가 없습니다.
- Secure Endpoint Service(보안 엔드포인트 서비스)를 Delayed Start(지연된 시작)로 설정할 필요가 없습니다.

스크립트 방법론

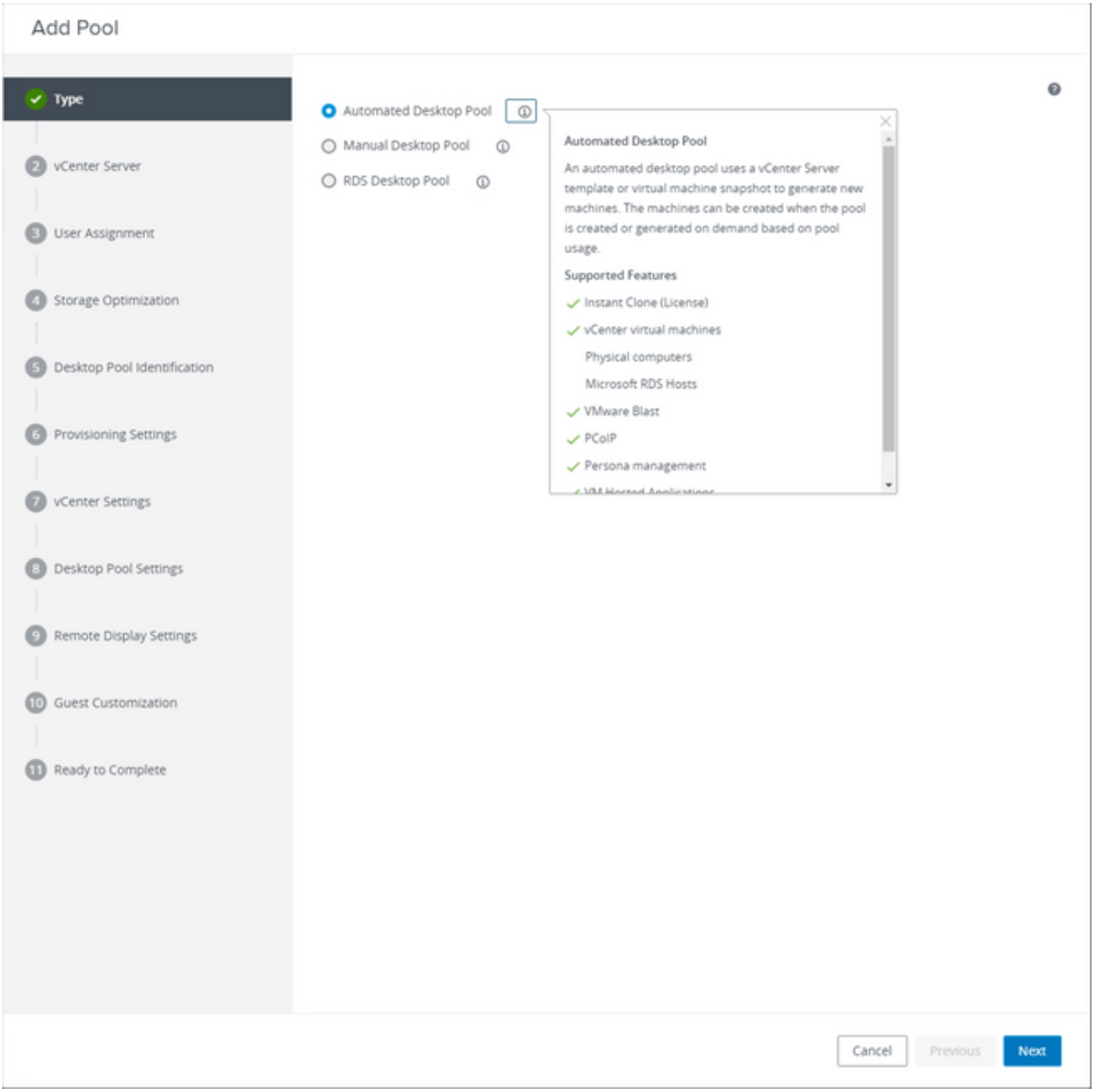
스크립트의 예는 아래에서 확인할 수 있습니다.

- 골든 이미지 설정 스크립트: 이 스크립트는 앞에서 설명한 것처럼 보안 엔드포인트 커넥터를 설치하고 앞서 설명한 플래그와 함께 구현해야 합니다. 이 스크립트는 보안 엔드포인트 서비스를 수동 시작으로 수정하고 골든 이미지 호스트 이름을 다음 단계에서 참조할 수 있도록 환경 변수로 저장합니다.

- Golden Image Startup Script(골든 이미지 시작 스크립트): 이 스크립트는 복제된(자식) VM의 호스트 이름을 이전 단계에서 저장된 호스트 이름과 일치시키는 논리적 검사로서, 복제된(자식) VM이 Golden Image VM(시스템의 최종 호스트 이름)이 아닌 다른 호스트 이름을 갖게 된 경우를 식별한 다음 Secure Endpoint Service를 시작하고 이를 Automatic으로 변경합니다. 앞서 언급한 스크립트에서도 환경 변수를 제거합니다. 이는 일반적으로 VMware와 같은 구축 솔루션에서 제공되는 메커니즘을 사용하여 구현됩니다. VMware에서는 사후 동기화 매개 변수 https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-E177899E-023D-4E61-B058-AFE3822158AA.html 을 사용할 수 있습니다. AWS의 경우에도 마찬가지로 https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-windows-user-data.html과 같은 방법으로 시작 스크립트를 사용할 수 있습니다.

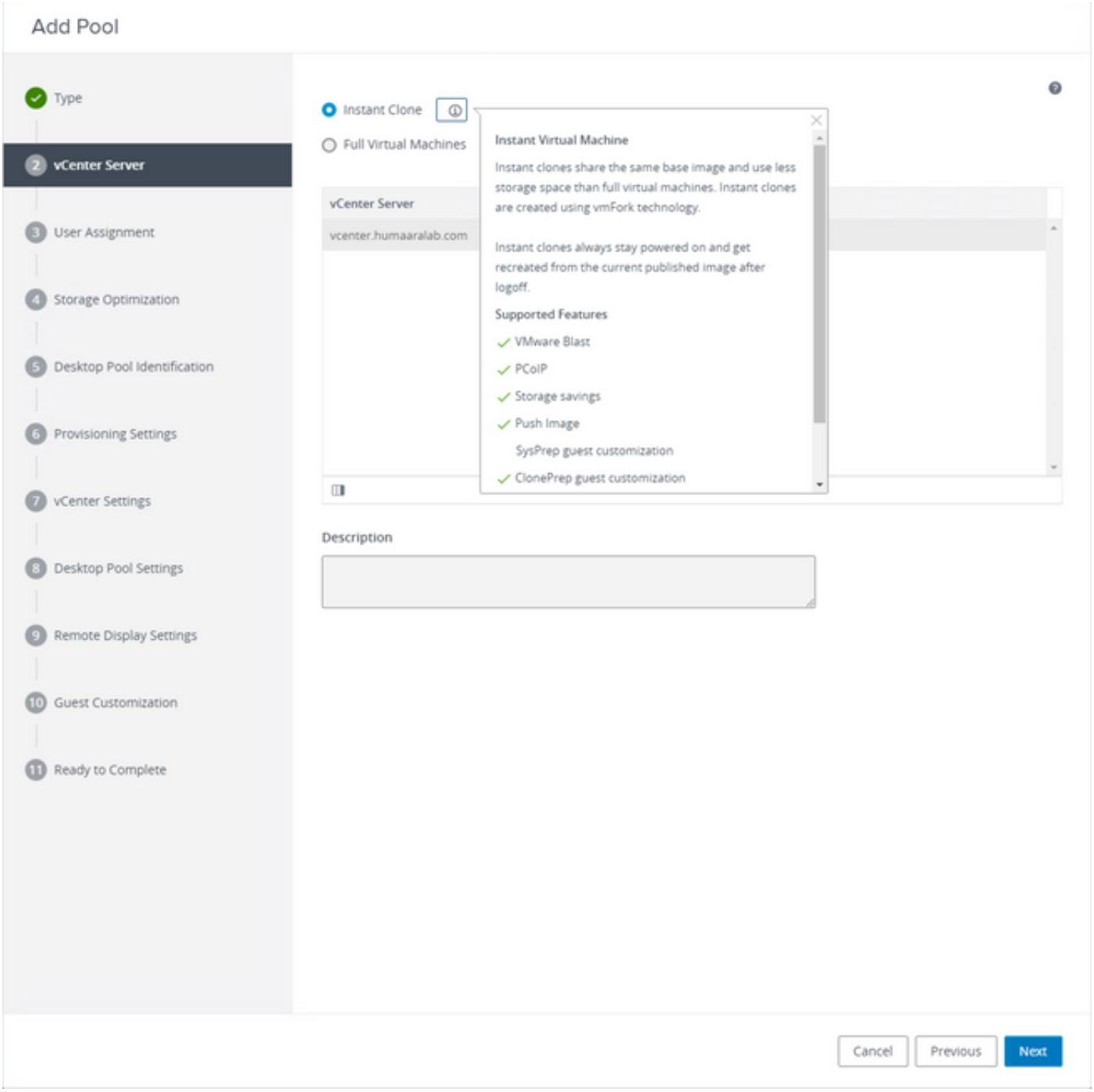
VMware Horizon 컨피그레이션

1. Golden Image VM이 준비되고 풀의 초기 구축에 필요한 모든 애플리케이션이 VM에 설치됩니다.
2. goldenimage 플래그를 포함하기 위해 보안 엔드포인트가 이 명령줄 구문으로 설치됩니다. 예: <ampinstaller.exe> /R /S /goldenimage 1. 골든 이미지 플래그는 이 프로세스가 올바르게 작동하는 데 중요한 재부팅이 있을 때까지 보안 엔드포인트 서비스가 실행되지 않도록 합니다. https://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-endpoints/118587-technote-fireamp-00.html을 참조하십시오.
3. 보안 엔드포인트 설치 후 먼저 Golden Image VM에서 VMWareHorizonAMPSetup.bat 스크립트를 실행합니다. 기본적으로 이 스크립트는 Secure Endpoint Service를 Manual Start(수동 시작)로 변경하고 나중에 사용할 수 있도록 골든 이미지 호스트 이름을 저장하는 환경 변수를 생성합니다.
4. VMWareHorizonAMPStartup.bat를 Golden Image VM의 범용 경로에 복사해야 합니다. 예를 들면 "C:\ProgramData"와 같습니다. 이 작업은 이후 단계에서 사용됩니다.
5. 이제 골든 이미지 VM을 종료하여 VMware Horizon에서 구성 프로세스를 시작할 수 있습니다.
6. VMware Horizon의 관점에서 본 단계별 정보는 다음과 같습니다.



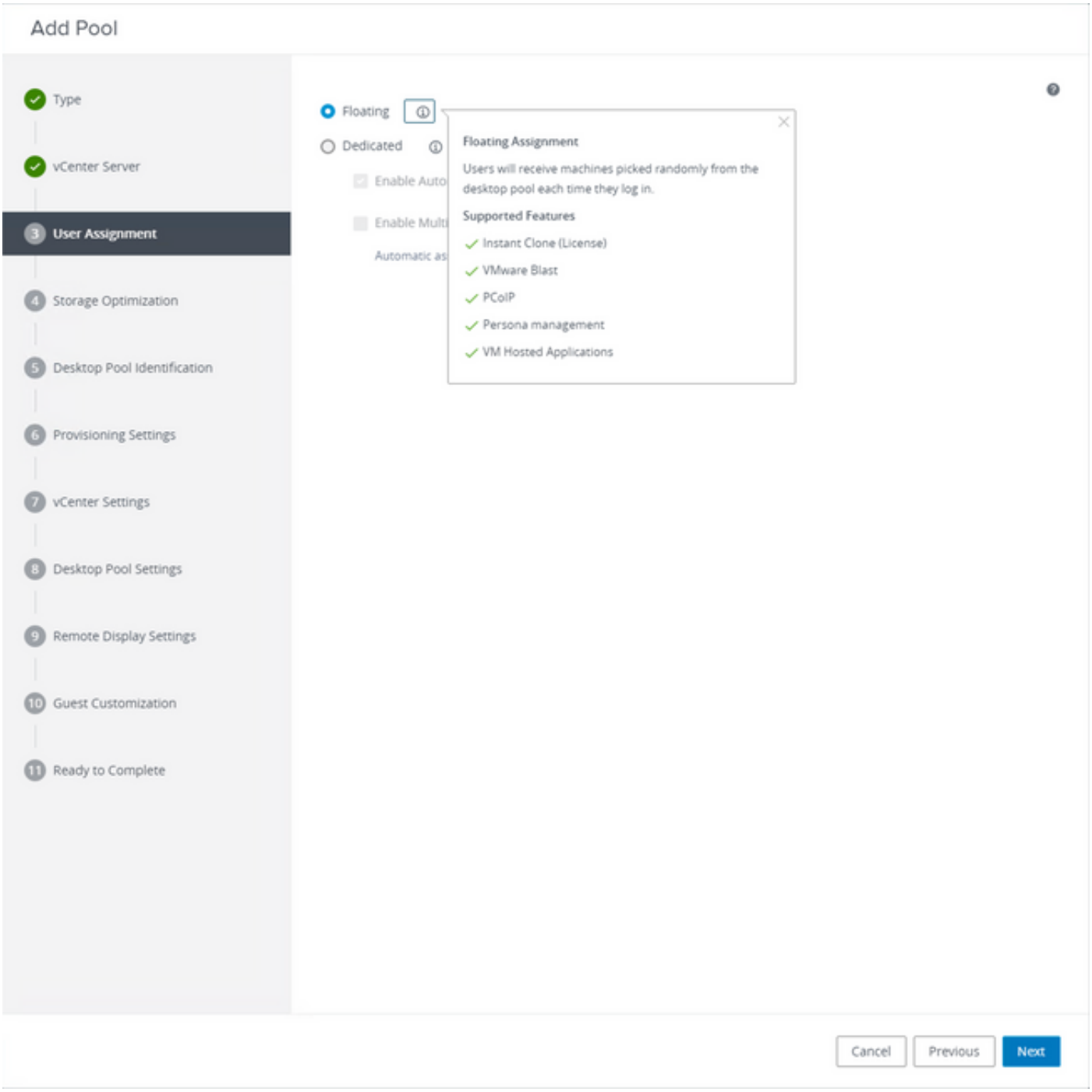
"Automated Desktop Pool(자동 데스크톱 풀)" 선택

참조: https://docs.vmware.com/en/VMware-Horizon/2106/virtual-desktops/GUID-6C3AB7F3-0BCF-4423-8418-30CA19CFC8FC.html



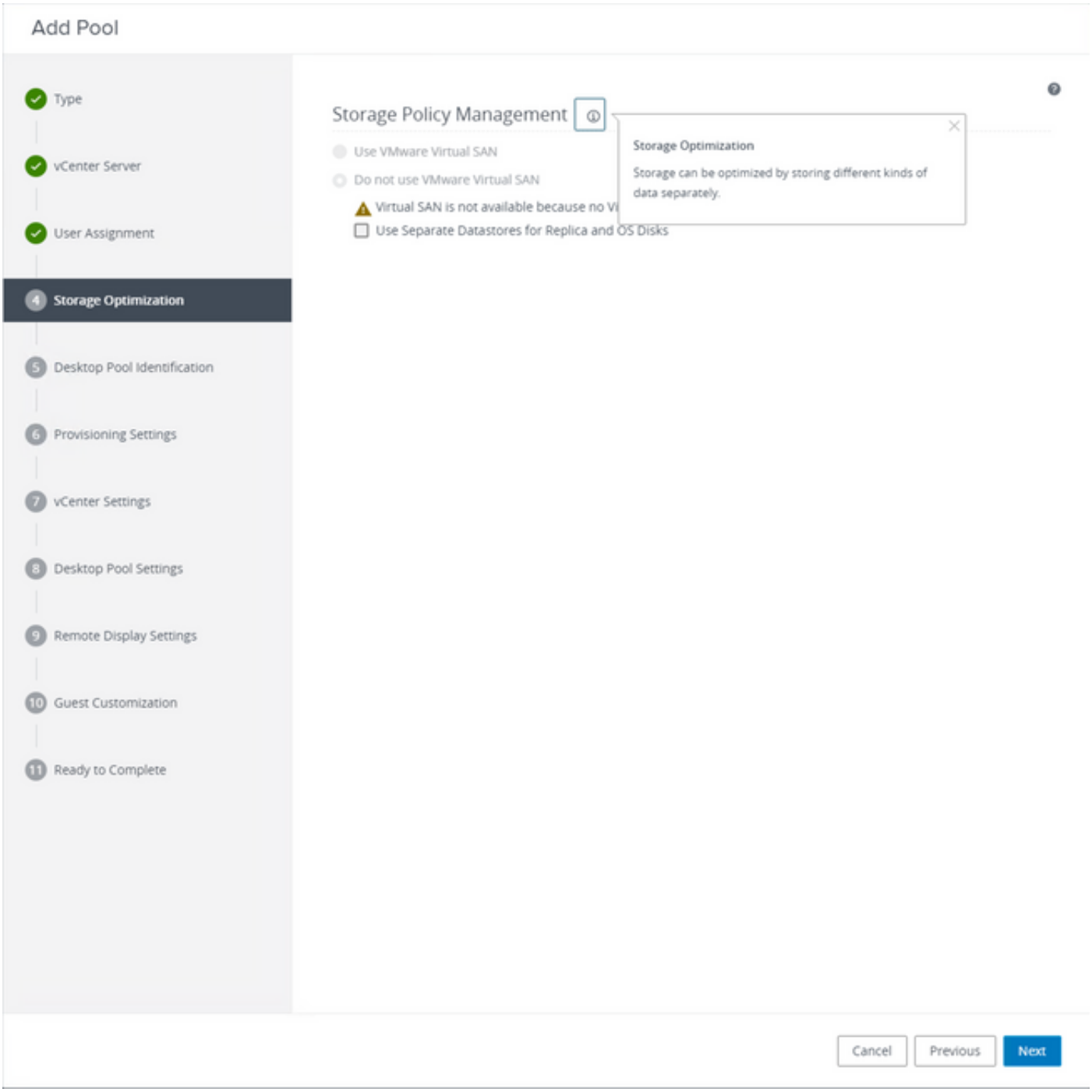
"Instant Clones" 선택

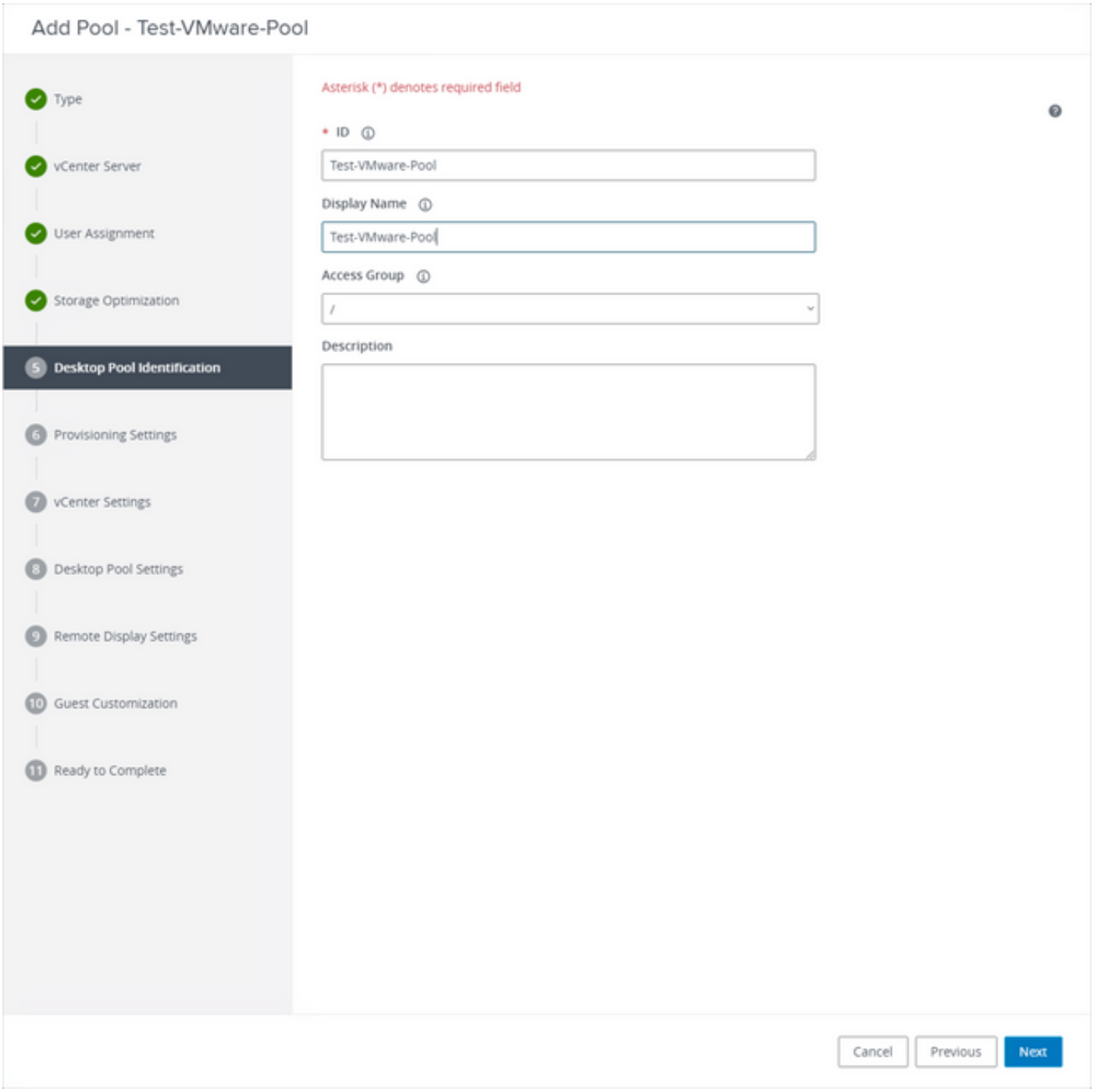
참조: https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-D7C0150E-18CE-4012-944D-4E9AF5B28347.html



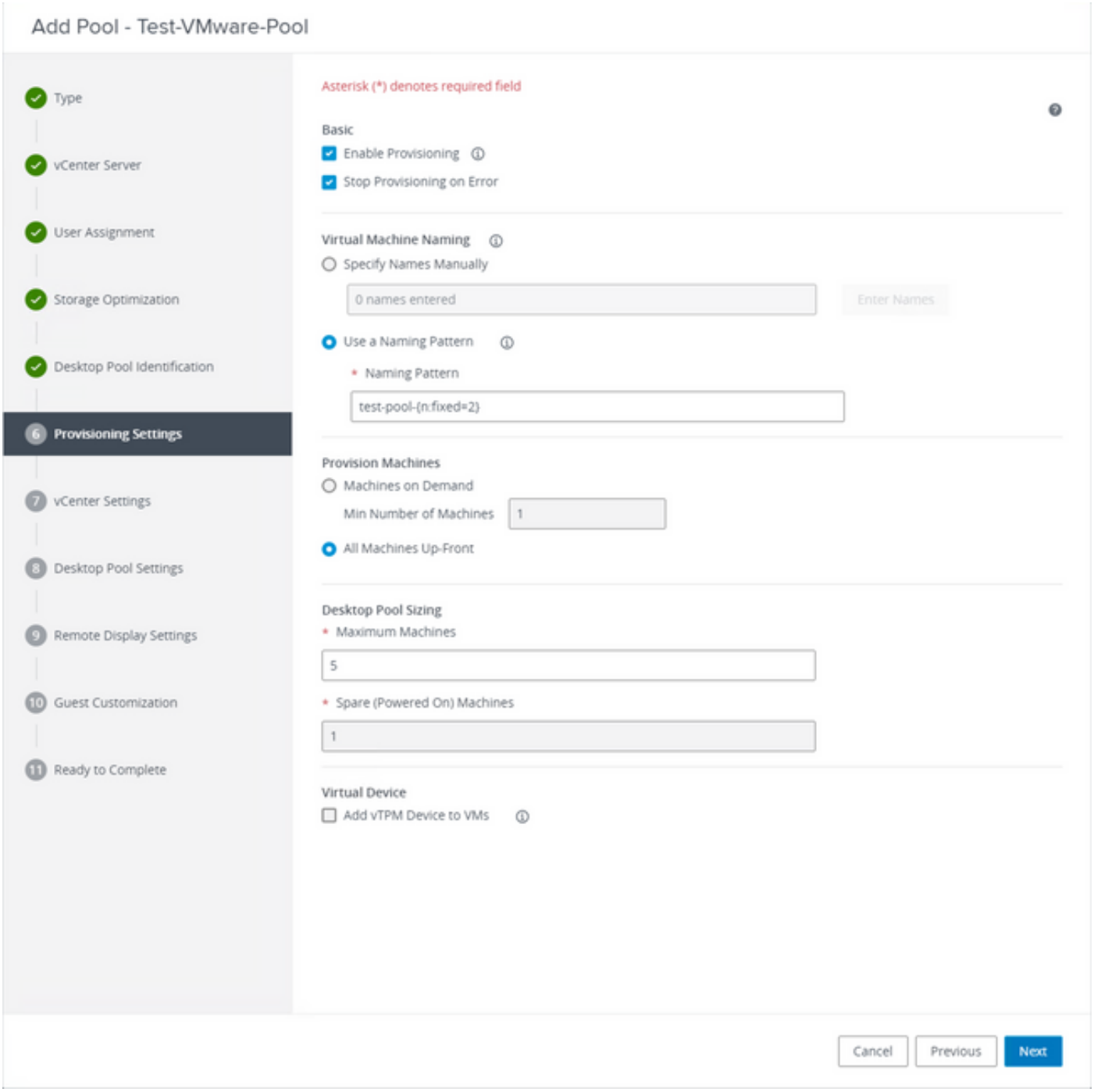
"부동" 유형 선택

참조: https://docs.vmware.com/en/VMware-Horizon-Cloud-Service-on-IBM-Cloud/21.1/horizoncloudhosted.deploy/GUID-34C260C7-A63E-452E-88E9-6AB63DEBB416.html

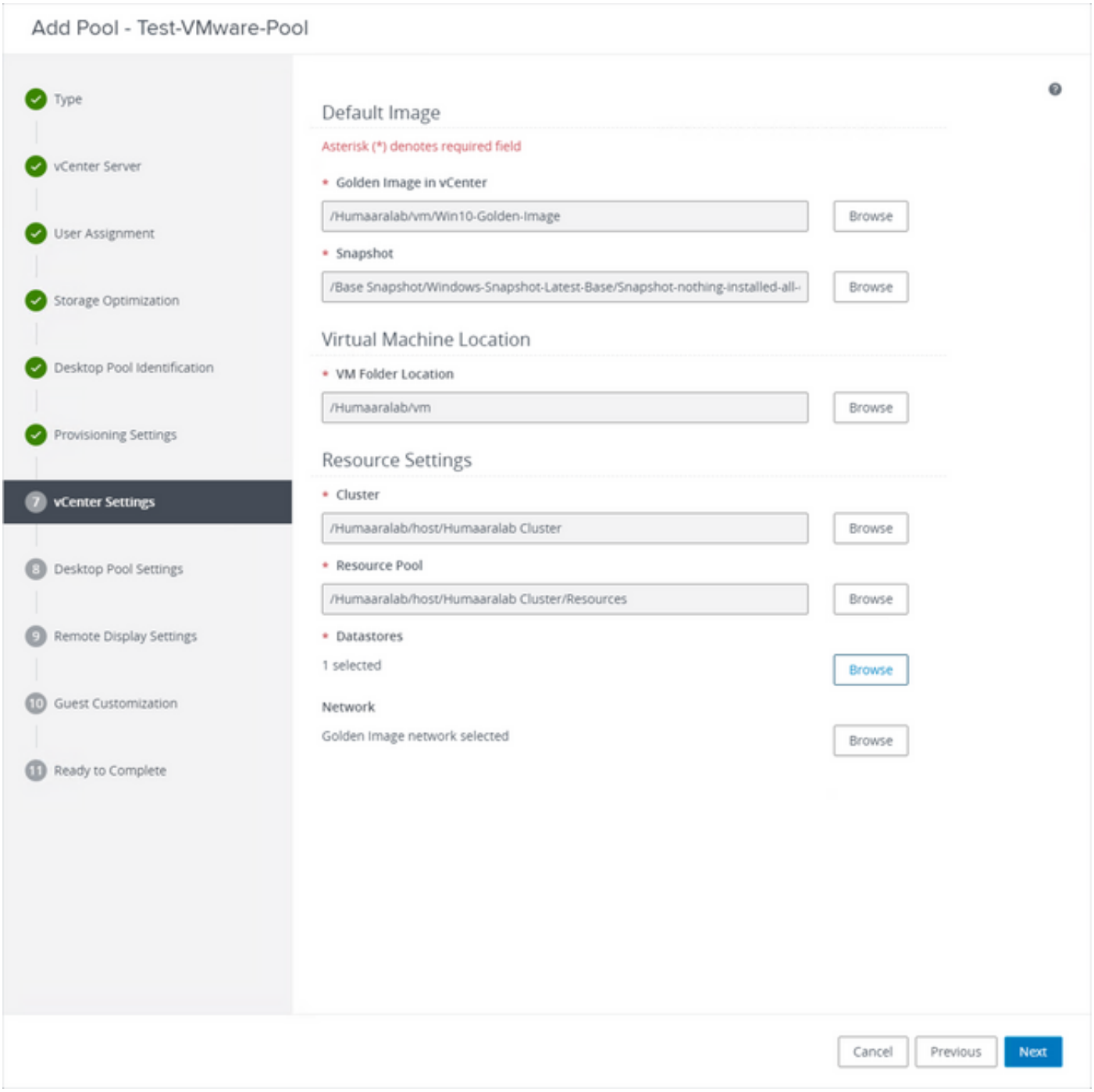

Add Pool
Type
vCenter Server
User Assignment
4 Storage Optimization
5 Desktop Pool Identification
6 Provisioning Settings
7 vCenter Settings
8 Desktop Pool Settings
9 Remote Display Settings
10 Guest Customization
11 Ready to Complete
Storage Policy Management
Use VMware Virtual SAN
Do not use VMware Virtual SAN
Virtual SAN is not available because no V
Use Separate Datastores for Replica and OS Disks
Storage Optimization
Storage can be optimized by storing different kinds of data separately.
Cancel
Previous
Next


Add Pool - Test-VMware-Pool
Type
vCenter Server
User Assignment
Storage Optimization
5 Desktop Pool Identification
6 Provisioning Settings
7 vCenter Settings
8 Desktop Pool Settings
9 Remote Display Settings
10 Guest Customization
11 Ready to Complete
Asterisk (*) denotes required field
* ID
Test-VMware-Pool
Display Name
Test-VMware-Pool
Access Group
/
Description
Cancel
Previous
Next

데스크톱 풀 이름

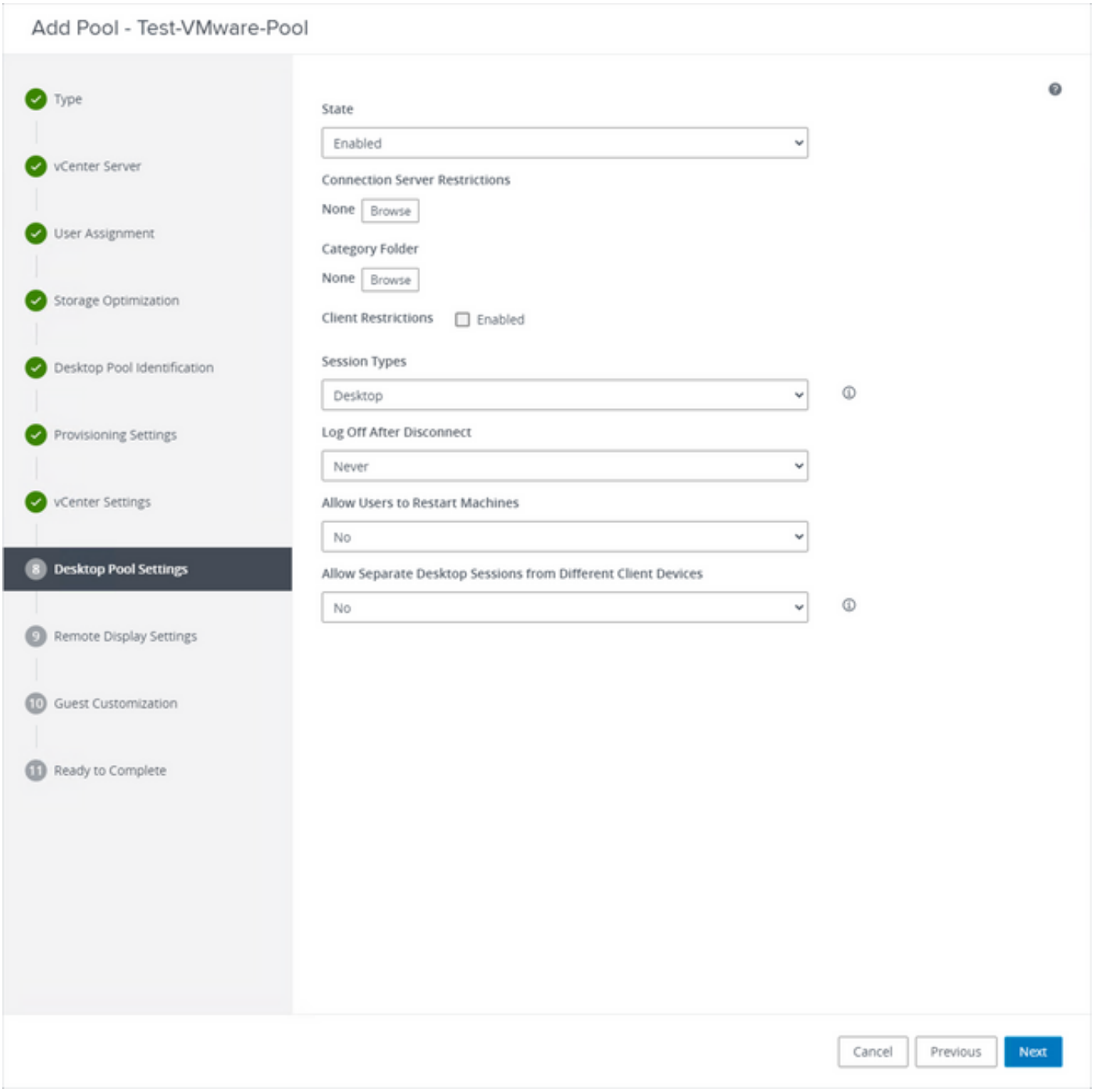


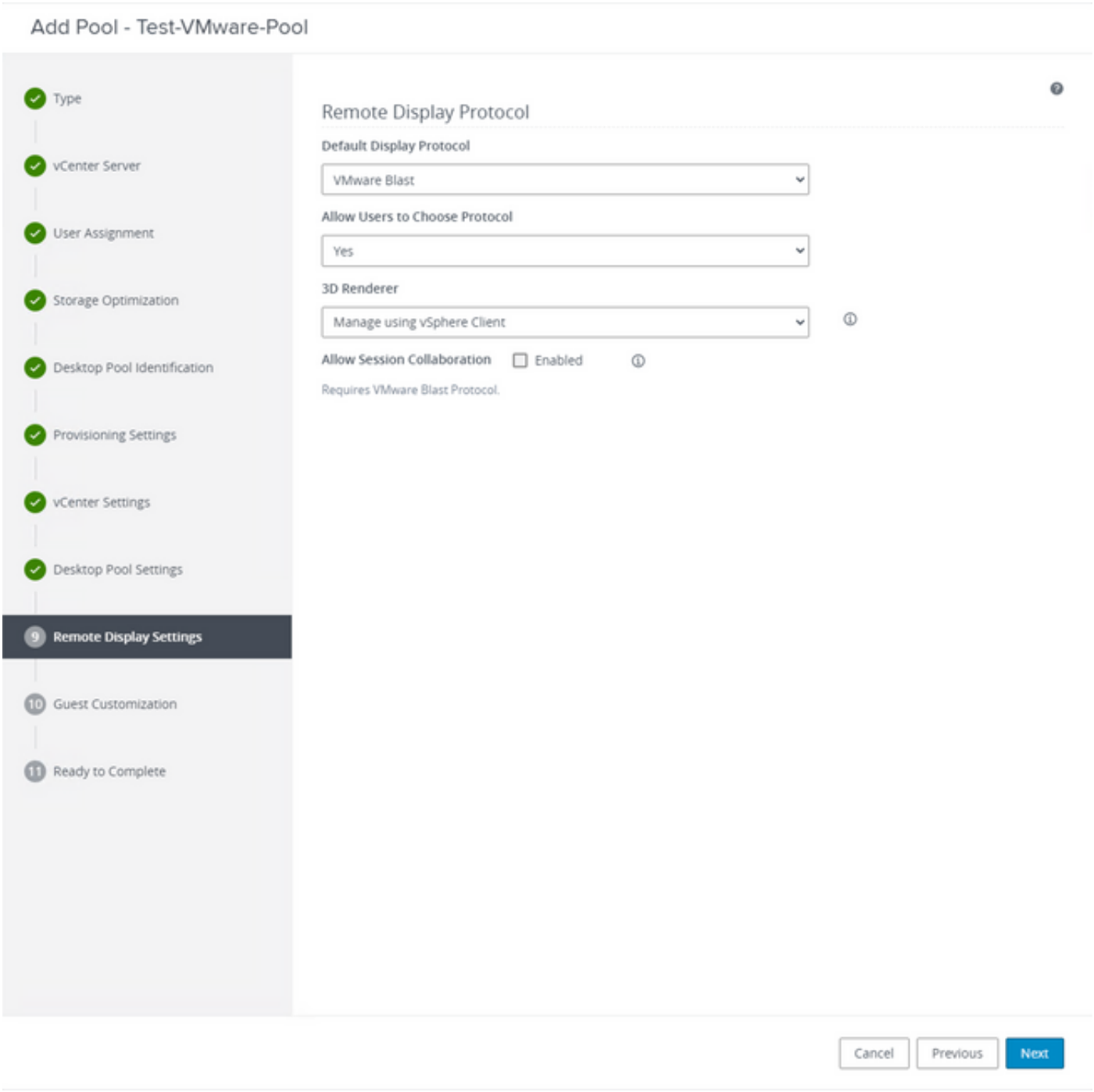
VMware Horizon 이름 지정 패턴: https://docs.vmware.com/en/VMware-Horizon/2103/virtual-desktops/GUID-26AD6C7D-553A-46CB-B8B3-DA3F6958CD9C.html

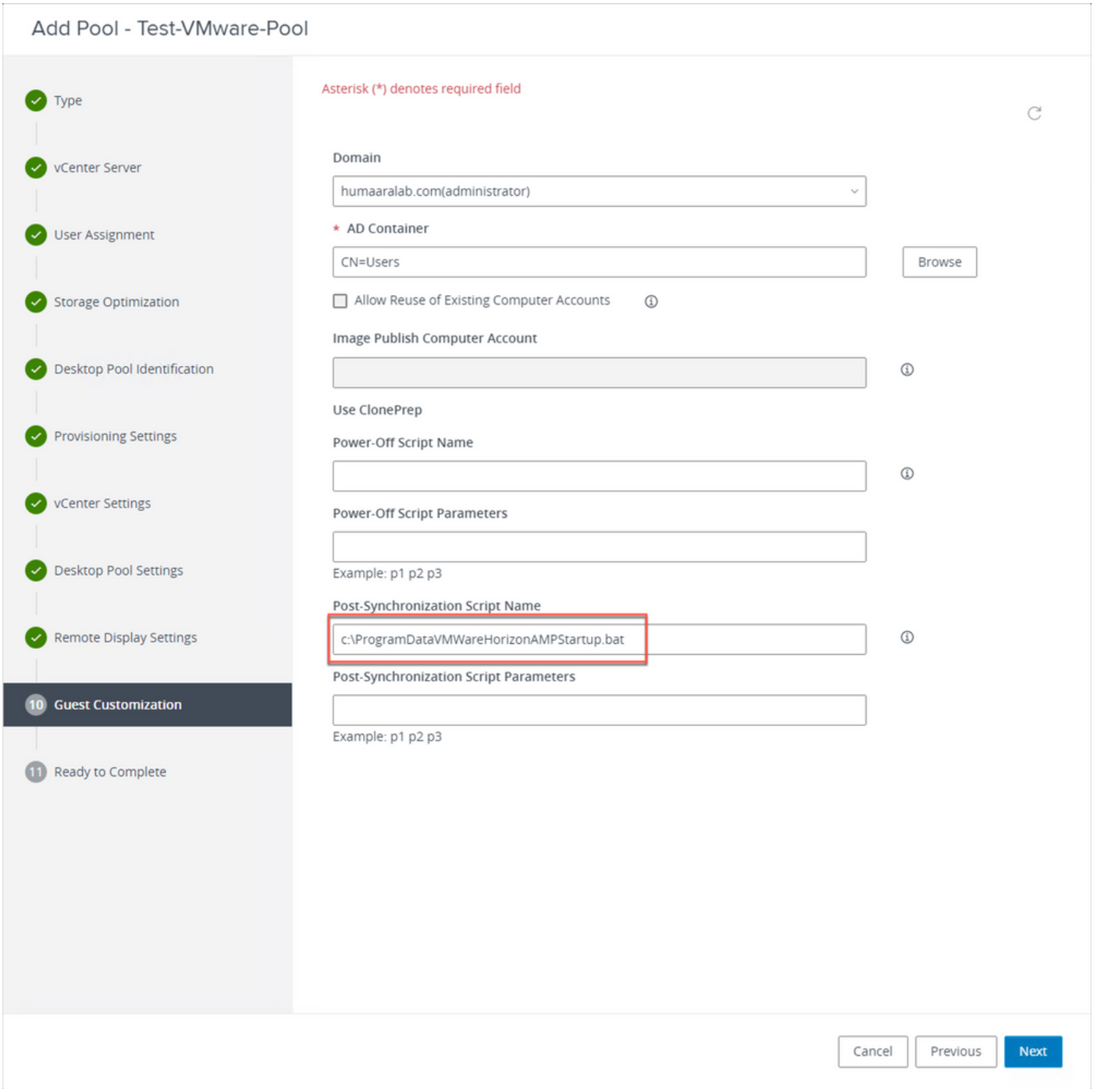


Golden Image(골든 이미지): 실제 골든 이미지 VM입니다.

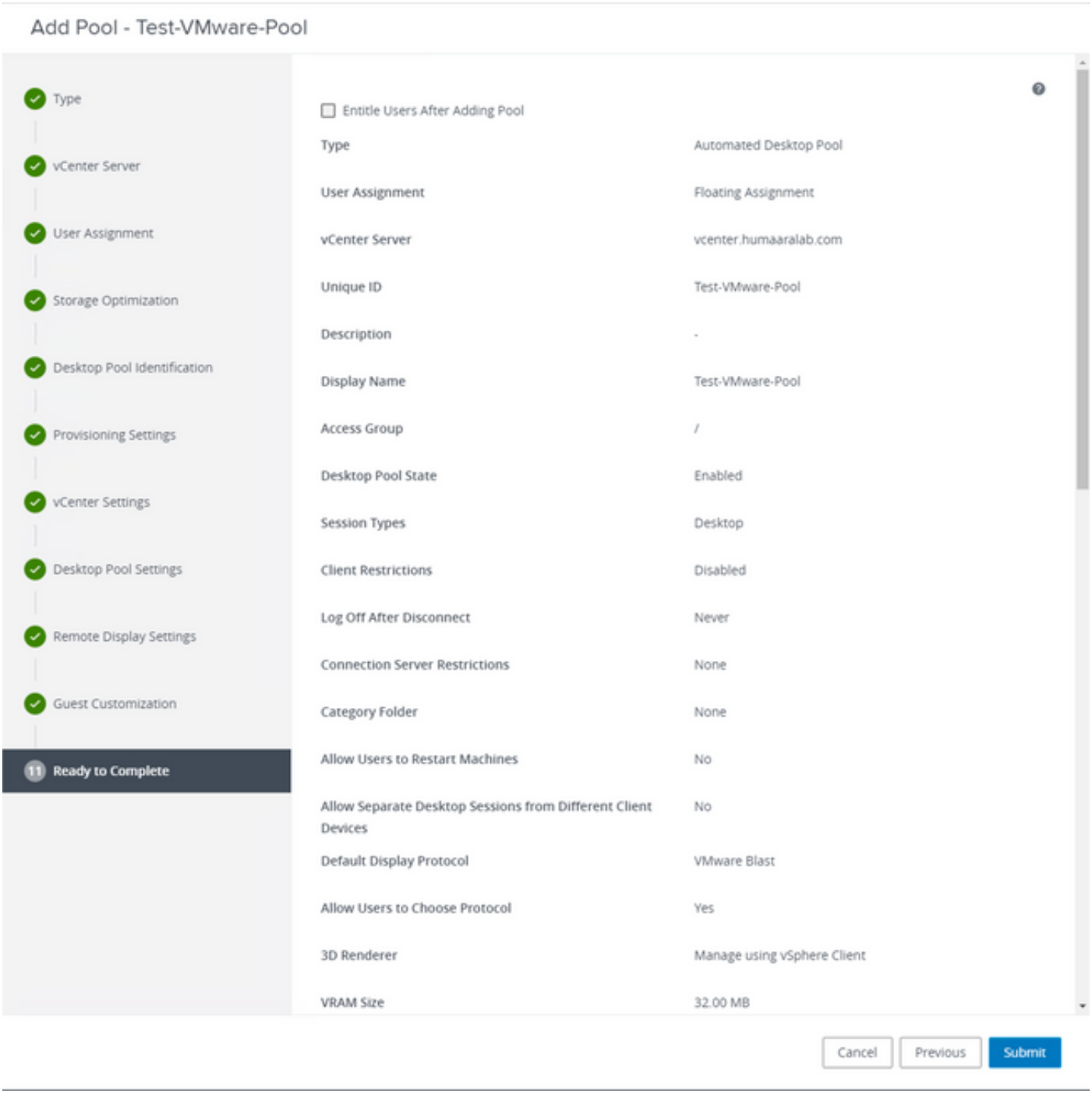
스냅샷: 하위 VM을 구축하기 위해 사용할 이미지입니다. 골든 이미지를 변경 사항으로 업데이트할 때 업데이트되는 값입니다. 나머지는 VMware 환경별 설정 중 일부입니다.


Add Pool - Test-VMware-Pool
Type
vCenter Server
User Assignment
Storage Optimization
Desktop Pool Identification
Provisioning Settings
vCenter Settings
8 Desktop Pool Settings
9 Remote Display Settings
10 Guest Customization
11 Ready to Complete
State
Enabled
Connection Server Restrictions
None
Browse
Category Folder
None
Browse
Client Restrictions
Enabled
Session Types
Desktop
Log Off After Disconnect
Never
Allow Users to Restart Machines
No
Allow Separate Desktop Sessions from Different Client Devices
No
Cancel
Previous
Next


Add Pool - Test-VMware-Pool
Type
vCenter Server
User Assignment
Storage Optimization
Desktop Pool Identification
Provisioning Settings
vCenter Settings
Desktop Pool Settings
9 Remote Display Settings
10 Guest Customization
11 Ready to Complete
Remote Display Protocol
Default Display Protocol
VMware Blast
Allow Users to Choose Protocol
Yes
3D Renderer
Manage using vSphere Client
Allow Session Collaboration
Enabled
Requires VMware Blast Protocol.
Cancel
Previous
Next



7. 앞서 설명한 대로 10단계 마법사에서 스크립트 경로를 설정합니다.



8. 완료 및 제출되면 VMware Horizon이 구성을 시작하고 하위 VM이 생성됩니다.

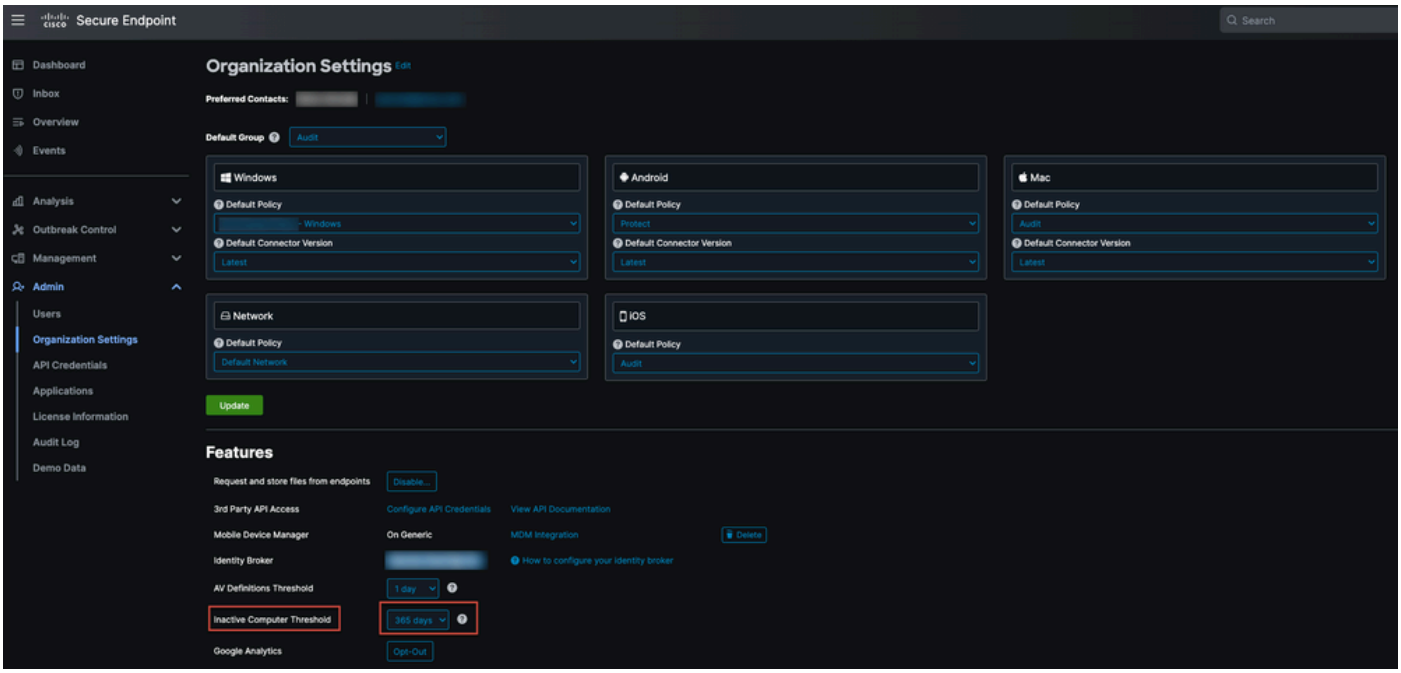
✎ 참고: 이 단계에 대한 자세한 내용은 VMware 설명서를 참조하되, 이 단계는 쉽게 설명할 수 있습니다.

중복 항목 제거

커넥터 중복 엔트리를 제거하는 몇 가지 방법이 있습니다.

1. Secure Endpoint Portal에서 자동 제거 기능을 사용하여 중복(비활성) 항목을 제거합니다.

Admin(관리) > Organization Settings(조직 설정)에서 이 설정을 찾을 수 있습니다



Inactive Computer Threshold(비활성 컴퓨터 임계값)를 사용하면 Cisco 클라우드를 체크 인하지 않고 커넥터가 Computer Management(컴퓨터 관리) 페이지 목록에서 제거되기 전까지 얼마나 많은 날짜를 지정할 수 있습니다. 기본 설정은 90일입니다. 비활성 컴퓨터는 목록에서만 제거되고 해당 컴퓨터에서 생성되는 모든 이벤트는 Secure Endpoint 조직에 남아 있습니다. 커넥터가 다시 체크 인하면 컴퓨터가 목록에 다시 나타납니다.

2. 사용 가능한 오케스트레이션 워크플로 활용: https://ciscosecurity.github.io/sxo-05-security-workflows/workflows/secure-endpoint/0056-remove-inactive-endpoints

3. 외부에서 사용 가능한 스크립트를 사용하여 부실/기존 UUID를 제거합니다. https://github.com/CiscoSecurity/amp-04-delete-stale-guids

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.