Identity Persistence in Secure Endpoint configureren

Inhoud

Inleiding

Dit document beschrijft hoe u de functie Cisco Secure Endpoint Identity Persistence kunt gebruiken.

Wat is Identity Persistence?

Identity Persistence is een functie waarmee u een consistent gebeurtenissenlogboek kunt bijhouden in virtuele omgevingen of wanneer computers een nieuwe image krijgen. U kunt een Connector koppelen aan een MAC-adres of hostnaam, zodat er geen nieuwe connector-record wordt gemaakt telkens wanneer een nieuwe virtuele sessie wordt gestart of een computer opnieuw wordt weergegeven. Deze voorziening is specifiek ontworpen voor niet-persistente VM- en Lab-omgevingen en mag niet worden ingeschakeld voor traditionele werkstations- en serverinstellingen.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot het Cisco Secure Endpoints-portal
- U moet contact opnemen met Cisco TAC om ze de functie Identity Persistence in uw organisatie te laten inschakelen.
- Identity Persistence wordt alleen ondersteund op Windows-besturingssysteem

Wanneer heb je identiteitsvolharding nodig?

Identity Persistence is functionaliteit op beveiligde endpoints die helpt bij de identificatie van beveiligde endpoints ten tijde van de initiële registratie van de connector en deze aanpast aan eerder bekende vermeldingen op basis van identiteitsparameters zoals MAC-adres of Hostname voor die specifieke connector. De implementatie van deze functie helpt niet alleen om een correct aantal licenties te behouden, maar maakt het vooral mogelijk om historische gegevens van niet-persistente systemen correct te volgen.

Virtuele endpointimplementatie

Het meest gebruikelijke gebruik voor Identity Persistence in virtuele implementaties is niet-persistente virtuele desktopinfrastructuur (VDI). VDI-host desktopomgevingen worden geïmplementeerd op verzoek of behoefte van de eindgebruiker. Hieronder vallen verschillende leveranciers zoals VMware, Citrix, AWS AMI Golden Image Implementation, enzovoort.

Persistente VDI, ook wel 'Stateful VDI' genoemd, is een setup waarbij het bureaublad van elke individuele gebruiker uniek aanpasbaar is en van de ene sessie tot de andere 'blijft'. Voor dit type virtuele implementatie is de functionaliteit van Identity Persistence niet nodig, aangezien deze machines niet bedoeld zijn om regelmatig opnieuw te worden geimaged.

Net als bij alle software die mogelijk kan interageren met de prestaties van het Secure Endpoint, moeten virtuele desktoptoepassingen worden geëvalueerd op mogelijke uitsluitingen om de functionaliteit te maximaliseren en de impact te minimaliseren.

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

Physical Endpoint-implementatie

Er zijn twee scenario's die van toepassing kunnen zijn op de implementatie van Identity Persistence op Secure Endpoints fysieke machines:

- Wanneer u een fysiek eindpunt met een gouden beeld met de vooraf geïnstalleerde Secure Endpoint-connector implementeert of opnieuw image maakt, moet de Goldenimage Flag zijn ingeschakeld. Identity Persistence kan worden gebruikt om duplicatie te voorkomen in het geval van machines met een nieuwe afbeelding, maar is niet vereist.

- Wanneer u een fysiek eindpunt met een gouden beeld implementeert of opnieuw image maakt en later de Secure Endpoint-connector installeert, kan Identity Persistence worden gebruikt om duplicatie te voorkomen in gevallen van opnieuw gebeeldhouwde machines, maar is dit niet vereist.

Veelvoorkomende problemen/symptomen met onjuiste implementatie van identiteitspersistentie

Onjuiste implementatie van Identity Persistence kan deze problemen/symptomen veroorzaken:

- Onjuist aantal aansluitpunten
- Onjuiste gerapporteerde resultaten
- Gegevensmismatch op apparaattraject
- Swaps van machinenamen binnen controlelogboeken
- Connectors registreren en willekeurig uit de console verwijderen
- Connectors rapporteren niet correct aan de cloud

- UID-duplicatie
- Duplicatie van machinenaam
- Gegevensinconsistentie
- Machines registreren om standaard Business Group / beleid na hersamenstelling

- Handmatig implementeren met Identity Persistence ingeschakeld in het beleid.

- Als u het eindpunt handmatig via de opdrachtregel implementeert en Identity Persistence al in het beleid is ingeschakeld, en vervolgens het eindpunt later verwijdert en probeert opnieuw te installeren met het switch uit verschillende groep/beleid, zal het eindpunt automatisch switches naar het oorspronkelijke beleid.

- Uitvoer van SFC-logboeken die de switch van het beleid op het eigen tonen met in 1-10sec

```
(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 initialized
(167656, +0 ms) Dec 14 11:37:17 [1308]: UiPublisher::PublishPolicyInfo: Name -UTMB-WinServer-Protect Ser
(167656, +0 ms) Dec 14 11:37:17 [1308]: UiPublisher::PublishLastPolicyUpdateTime: Publish Last Policy Up
(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 r
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitRegistrationHandler::ConnectionStateChanged: Starting Prox
(173125, +0 ms) Dec 14 11:37:22 [4704]: UIPipe::SendPolicyReloaded sending policy reloaded to UI. ui.dat
(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 c
(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 detect
(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: e1a756e2-65a
(173125, +0 ms) Dec 14 11:37:22 [4704]: UiPublisher::PublishAgentGuid: Agent GUID did not change (e1a756
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitSubscriptionThread::NotificationWorker: Waiting on queue
```

De andere bijwerking als u probeert te installeren connector die tot verschillende groep behoort. U ziet in het portal dat de connector is toegewezen aan de juiste groep maar met **"verkeerde"** originele beleid

Dit komt doordat Identity Persistence (ID SYNC) in feite werkt.

Zonder ID SYNC wanneer de connector volledig is verwijderd of met de switch re-register opdrachtregel. U dient de nieuwe gemaakte datum en connector GUID te zien indien de installatie ongedaan wordt gemaakt of alleen de nieuwe connector GUID indien de opdracht opnieuw wordt geregistreerd. Met ID SYNC is dat echter niet mogelijk. ID SYNC overschrijft met de oude GUID en DATUM. Dat is hoe we de host 'synchroniseren'.

Indien deze kwestie wordt waargenomen, moet de correctie worden geïmplementeerd door middel van de beleidswijziging. U moet de betrokken eindpunten terugbrengen naar de oorspronkelijke groep/het oorspronkelijke beleid en ervoor zorgen dat het beleid gesynchroniseerd wordt. Verplaats de eindpunten vervolgens terug naar de gewenste groep/beleid

Best practices voor implementatie

Snapvol-bestand configureren

Indien u App Volumes gebruikt voor uw VDI-infrastructuur, is het aan te raden dat u deze configuratiewijzigingen aanbrengt in uw **snapvol.cfg-**configuratie

Deze uitsluitingen moeten worden geïmplementeerd in het **bestand snapvol.cfg**:

Paden:

- 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

Registratiesleutels:

- HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Immunet Protect
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\CiscoAMP
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CiscoAMPCEFWDriver
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CiscoAMPELAMDriver
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CiscoAMPHeurDriver
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CiscoOrbital
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CiscoSAM
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CiscoSCMS
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ImmunetProtectDriver
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ImmunetSelfProtectDriver
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Trufos

Op x64 systemen, voeg deze toe:

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Immunet Protect
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Im Protect

Referenties:

- 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

Gouden afbeelding maken

Volg de richtlijnen voor best practices uit het document van de leverancier (VMware, Citrix, AWS, Azure, enzovoort.) wanneer u een Golden Image maakt voor het VDI-kloningproces.

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

Aangezien u de VMware hebt geïdentificeerd, start het AWS-samenstellingsproces de gekloonde (Child VM's) meerdere malen opnieuw op voordat de VM-configuratie is voltooid, wat problemen oplevert met het registratieproces voor het beveiligde endpoint, aangezien de gekloonde (Child VM's) op dit moment niet de definitieve/juiste hostnamen hebben toegewezen en de gekloonde (Child VM's) de Golden Image Hostname en de registers van de Secure Endpoint Cloud gebruiken. Dit doorbreekt het kloneringsproces en veroorzaakt problemen.

Dit is geen probleem met het Secure Endpoint-verbindingsproces, maar is incompatibel met het kloonproces en de registratie van Secure Endpoint. Om dit probleem te voorkomen hebben we een aantal wijzigingen vastgesteld die in het kloneringsproces moeten worden aangebracht en die ertoe bijdragen dat deze problemen worden opgelost.

Dit zijn de wijzigingen die op de Golden Image VM moeten worden geïmplementeerd voordat het beeld wordt bevroren om te klonen

1. Gebruik altijd de vlag van **Goldenafbeelding** op de Gouden Afbeelding ten tijde van de installatie van Secure Endpoint.

2. Voer scripts uit die helpen de Endpoint service alleen in te schakelen wanneer we een definitieve hostnaam hebben geïmplementeerd op de gekloonde (Child VM's). Raadpleeg het gedeelte Problemen met VMware Horizon-duplicatie voor meer informatie.

Vlag voor Golden Image negeren

Wanneer u het installatieprogramma gebruikt, is de vlag voor gouden afbeeldingen **/goudafbeelding 1**.

De gouden beeldvlag voorkomt dat de connector start en registreert op het basisbeeld; en zo is de connector bij het volgende begin van het beeld in de functionele staat waarin hij is ingesteld door het beleid dat eraan is toegewezen.

Voor meer informatie over andere vlaggen, zie dit artikel.

Installeer het als een gouden beeld. Dit is de typische optie die met de vlag wordt gebruikt en is het enige verwachte gebruik. Hiermee wordt de eerste registratie van de connector en het opstarten bij installatie overgeslagen.

```
C:\> CiscoInstaller_goldenimage.exe /R /S /goldenimage 1 [other flags hereâ€¦]
```

Stappen voor het maken van Golden Image

Het is best practice om de connector als laatste te installeren voor de voorbereiding van de **Golden Image**.

1. Bereid het Windows-beeld voor op uw wensen; installeer al uw vereiste software, configuraties voor de Windows-afbeelding, met uitzondering van de -aansluiting.
2. Installeer de Cisco Secure Endpoint-connector.

3. Gebruik de vlag/goldenimage **1** om de installateur erop te wijzen dat het om een golden image-implementatie gaat.

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

4. Voer de Script Logic (indien nodig) uit zoals hier beschreven.
5. Volledige installatie.
6. Zet je gouden beeld stil.

Nadat Golden Image applicaties heeft geïnstalleerd, is het systeem voorbereid en Secure Endpoint is geïnstalleerd met de / goldenimageflag, is de host klaar om te worden bevroren en gedistribueerd. Zodra de gekloonde host opstart, start Secure Endpoint en registreert deze bij de cloud. Geen verdere actie wordt vereist met betrekking tot het configureren van de connector tenzij er veranderingen zijn die u wilt aanbrengen in het beleid of de host. Als er wijzigingen worden aangebracht nadat de registratie van de gouden afbeelding is voltooid, moet dit proces opnieuw worden gestart.

Portal en beleidsplanning

Dit zijn enkele van de best practices die moeten worden gevolgd wanneer u Identity Persistence implementeert op Secure Endpoint Portal:

1. Het is sterk aanbevolen om afzonderlijke beleidsregels/groepen te gebruiken voor endpoints die compatibel zijn met Identity Persistence voor een eenvoudiger segregatie.

2. Als u van plan bent Endpoint Isolation te gebruiken en de **Move Computer to Group** te implementeren **na een compromitterende** actie. De doelgroep moet ook Identity Persistence enabled hebben en mag alleen worden gebruikt voor VDI-computers.

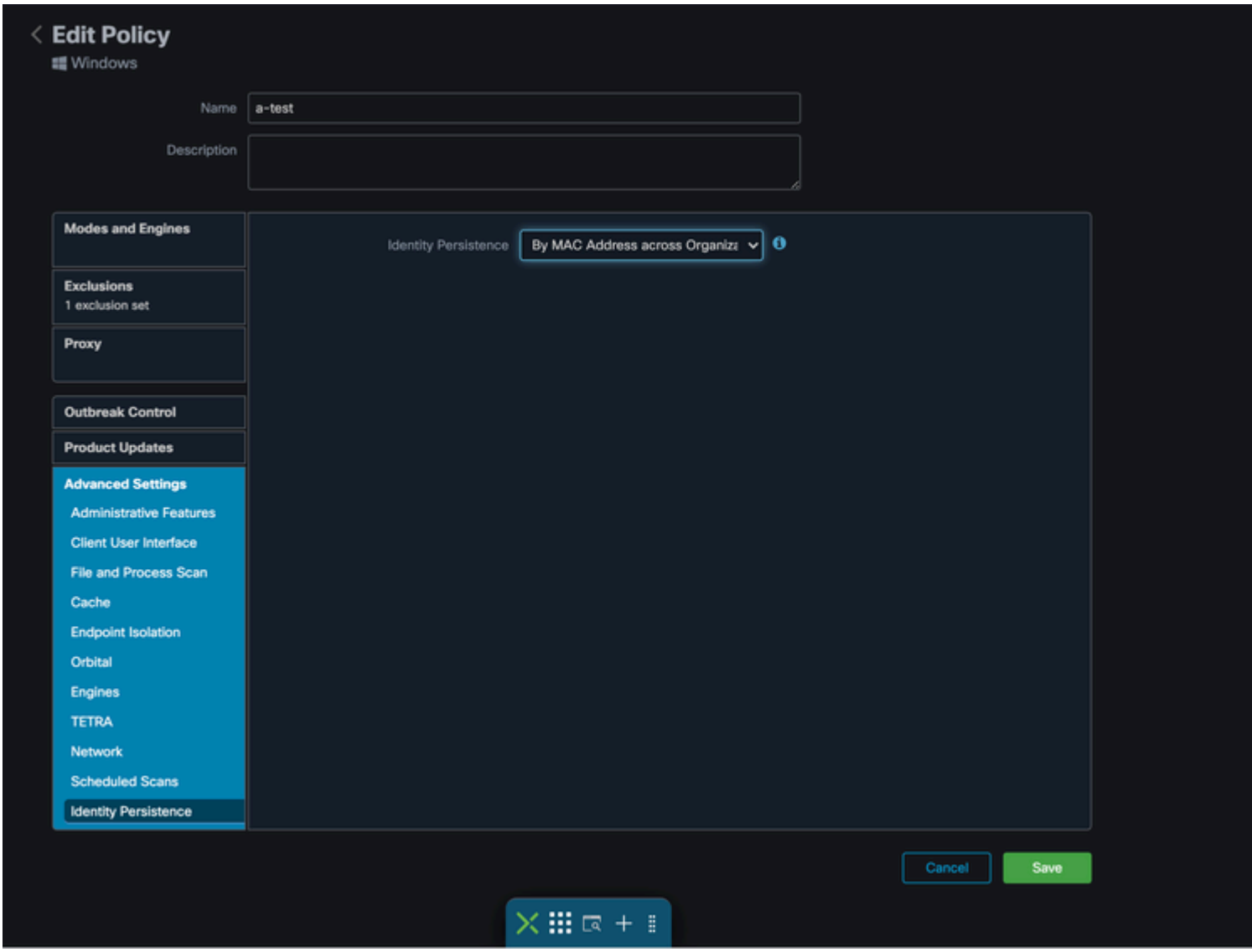
3. Het wordt niet aanbevolen om **Identity Persistence** in te schakelen op de standaardgroep/het standaardbeleid voor uw organisatie-instellingen, tenzij Identity Persistence is ingeschakeld voor alle beleidsgebieden met Overal in de organisatie als instellingenbereik.

Configuratie

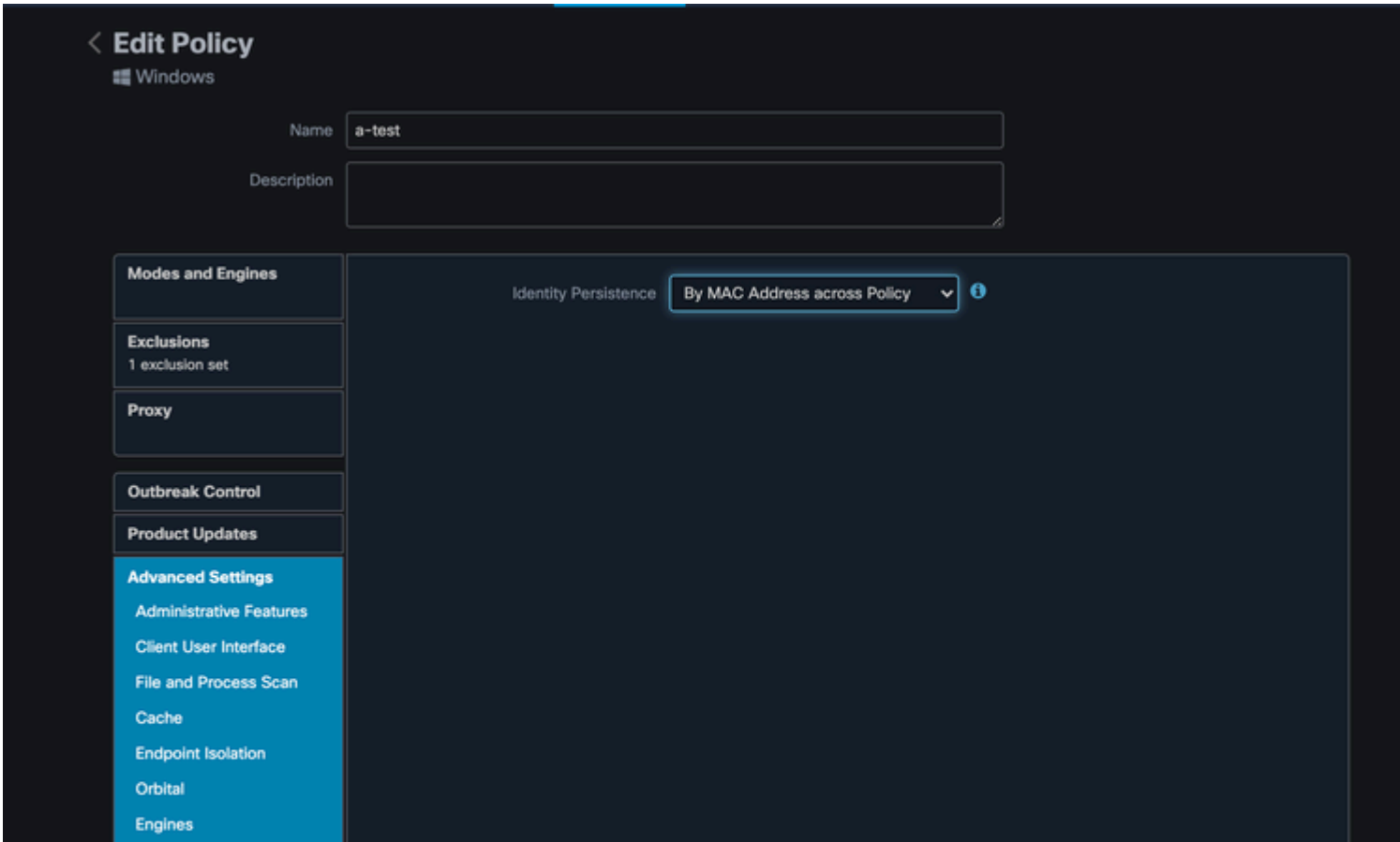
Volg deze stappen om de Secure Endpoint-connector met Identity Persistence te implementeren:

Stap 1. Pas de gewenste instelling voor Identity Persistence toe op uw beleid:

- Navigeer in het Secure Endpoint portal naar **Management > Policy**.
- Selecteer het gewenste beleid waarop u Identity Persistence wilt inschakelen en **klik** vervolgens **op Bewerken**.
- Navigeer naar **het** tabblad **Geavanceerde** instellingen en klik onderaan op het tabblad **Identity Persistence**.
- Selecteer de vervolgkeuzelijst Identity Persistence en kies de optie die het meest zinvol is voor uw omgeving. Raadpleeg de afbeelding.


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 Organiza
Cancel
Save

Test - 123

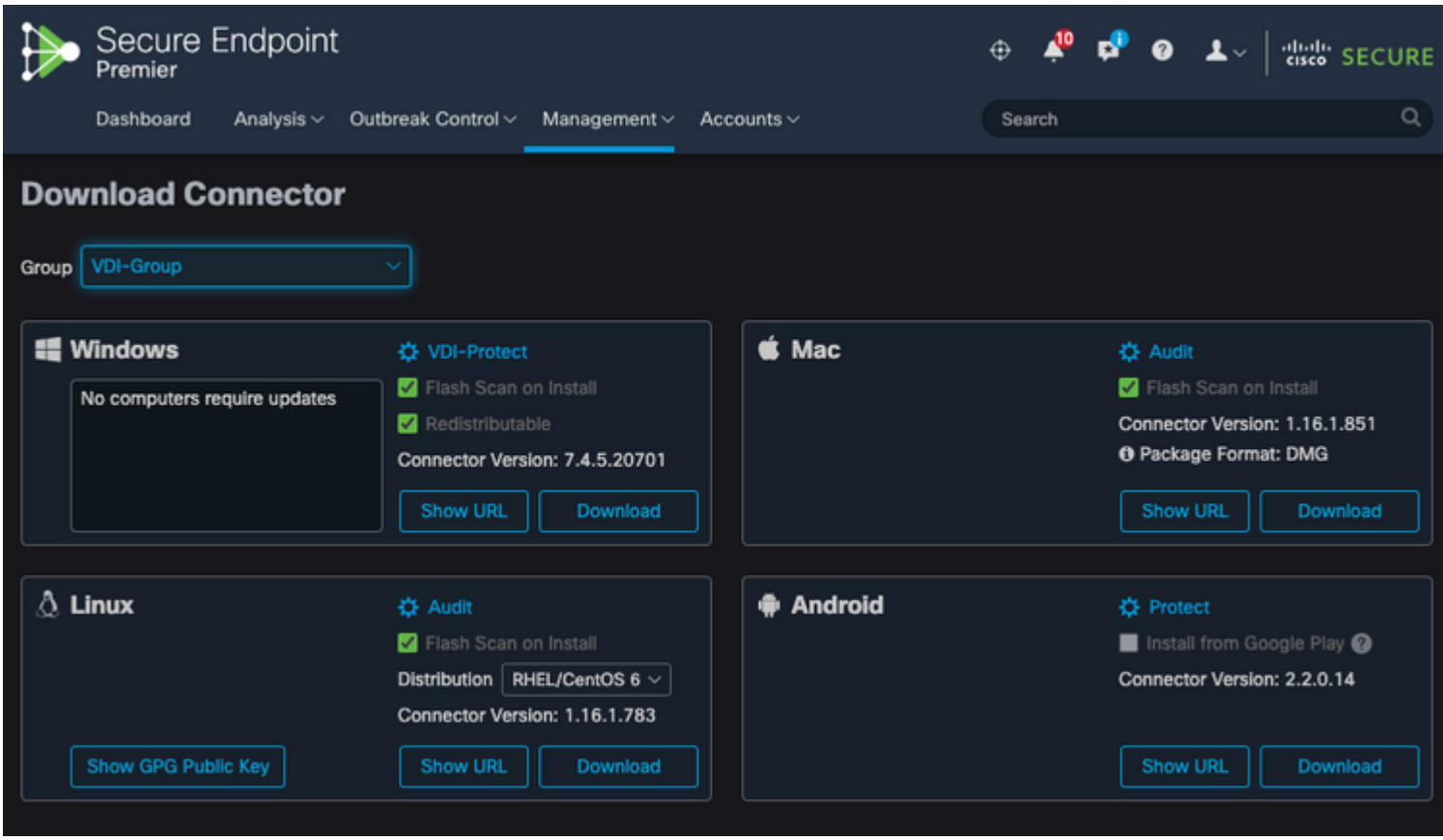

Edit Policy
Windows
Name
a-test
Description
Modes and Engines
Exclusions
1 exclusion set
Proxy
Outbreak Control
Product Updates
Advanced Settings
Administrative Features
Client User Interface
File and Process Scan
Cache
Endpoint Isolation
Orbital
Engines
Identity Persistence
By MAC Address across Policy

- Door MAC-adres over bedrijven: Nieuwe of vernieuwde installaties zoeken naar het meest recente Connectorrecord dat hetzelfde MAC-adres heeft om eerdere historische gegevens te synchroniseren met de nieuwe registratie. Deze instelling doorkijkt alle bedrijfsgegevens, ongeacht de instellingen voor Identity Persistence in ander beleid en de Connector kan zijn beleid bijwerken om de vorige installatie weer te geven als het verschilt van de nieuwe.
- Door MAC-adres over beleid: Nieuwe of vernieuwde installaties zoeken naar het meest recente Connector-record dat hetzelfde MAC-adres heeft om eerdere historische gegevens te synchroniseren met de nieuwe registratie. Deze instelling kijkt alleen door de records die zijn gekoppeld aan het beleid dat in de implementatie wordt gebruikt. Als de Connector niet eerder in dit beleid was geïnstalleerd maar eerder actief was in een ander beleid, kan dit duplicaten creëren.
- Door Hostname over Bedrijven: Nieuwe of vernieuwde installaties zoeken naar het meest recente Connector record dat dezelfde Hostname heeft om eerdere historische gegevens te synchroniseren met de nieuwe registratie. Deze instelling doorkijkt alle bedrijfsgegevens, ongeacht de instellingen voor Identity Persistence in ander beleid en de Connector kan zijn beleid bijwerken om de vorige installatie weer te geven als het verschilt van de nieuwe. Hostname bevat FQDN, zodat er duplicaten kunnen optreden als de connector regelmatig tussen netwerken beweegt (zoals een laptop).
- Door Hostname over het beleid: Nieuwe of vernieuwde installaties zoeken naar het meest recente Connector record dat dezelfde Hostname heeft om eerdere historische gegevens te synchroniseren met de nieuwe registratie. Deze instelling doorkijkt alleen de records die gekoppeld zijn aan het beleid dat voor de implementatie wordt gebruikt. Als de Connector niet eerder in dit beleid was geïnstalleerd maar eerder actief was in een ander beleid, kan dit duplicaten creëren. Hostname bevat FQDN, zodat duplicaten ook kunnen optreden als de connector regelmatig tussen netwerken beweegt (zoals een laptop).

N.B.: Als u Identity Persistence wilt gebruiken, raadt Cisco u aan **Hostname te** gebruiken **via het bedrijfsnetwerk of het beleid**. Een machine heeft één hostnaam, maar kan meer dan één MAC-adres hebben en veel VM's klonen de MAC-adressen.

Stap 2. Download de Secure Endpoint Connector.

- Navigeer **naar Beheer > Download Connector**.
- Selecteer de groep voor het beleid dat u in Stap 1 hebt bewerkt.
- **Klik op Downloaden** voor de Windows Connector zoals in de afbeelding.



Stap 3. Connector op endpoints implementeren.

- U kunt nu de gedownloade connector gebruiken om Secure Endpoint (met Identity Persistence nu ingeschakeld) handmatig op uw endpoints te installeren.
- Anders kunt u de connector ook inzetten met een gouden afbeelding (zie afbeelding)

Opmerking: u moet het herverdelbare installatieprogramma selecteren. Dit is een ~57 MB (grootte kan variëren met nieuwere versies) bestand dat zowel de 32- en 64-bits installateurs bevat. Als u de connector op meerdere computers wilt installeren, kunt u dit bestand op een netwerkaandeel plaatsen of het naar alle computers dienovereenkomstig duwen. Het installatieprogramma bevat een bestand policy.xml dat wordt gebruikt als configuratiebestand voor de installatie.

Problemen met VMware Horizon-duplicatie

Met VMware Horizon konden we vaststellen dat de Child VM-machines bij het maken ervan meerdere malen opnieuw worden opgestart als onderdeel van het Horizon Compose-proces. Dit veroorzaakt problemen omdat de Secure Endpoint-services ingeschakeld worden wanneer de Child VM's niet klaar zijn (ze hebben niet de definitieve/juiste NetBios-naam toegewezen). Dit veroorzaakt verdere problemen met Secure Endpoint die verwarrend worden en vandaar de procesonderbrekingen. Na verder onderzoek kwam het Engineering Team met een oplossing voor deze incompatibiliteit met het Horizon-proces, waarbij de bijgevoegde scripts op de Golden Image VM moeten worden geïmplementeerd en het post-synchronisatiescript Functionality for VMware Horizon: [https://docs.vmware.com/en/VMware-Horizon/2103/published-desktops-applications.pdf.](https://docs.vmware.com/en/VMware-Horizon/2103/published-desktops-applications.pdf)

Dit zou waarschijnlijk het probleem zijn met elke andere leverancier, net als Citrix, AWS, en zo verder en dus kan deze oplossing ook voor hen werken.

Geen configuratie/wijzigingen meer nodig

- U hoeft Secure Endpoint niet langer te verwijderen en opnieuw te installeren als u na de eerste implementatie wijzigingen in het Golden Image wilt aanbrengen.
- U hoeft de Secure Endpoint Service niet in te stellen op **Timer-start**.

Script-methodologie

Hier zijn de voorbeeldscripts die gebruikt kunnen worden.

- **VMWareHorizonAMPSetup.bat:** Dit script moet worden geïmplementeerd zodra het AMP is geïnstalleerd zoals eerder beschreven met de vlaggen zoals eerder gedocumenteerd. In dit script wordt de Secure Endpoint-service gewijzigd in Manual Start en wordt de Hostnaam Golden Image opgeslagen als een Omgevingsvariabele die in de volgende stap kan worden geraadpleegd.

```
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%
```

- **VMWareHorizonAMPStartup.bat:** Dit script is een logische controle waarbij we de hostnaam op de gekloonde (kind) VMs vergelijken met de naam die in de vorige stap is opgeslagen, om er zeker van te zijn dat we weten wanneer de gekloonde (kind) VM een hostnaam krijgt die iets anders is dan de Golden Image VM (die de definitieve hostnaam voor de machine zou zijn) en dan ga je verder en start de Secure Endpoint Service en wijzig die automatisch is. U verwijdert ook de Omgevingsvariabele uit het eerder genoemde script. Dit wordt normaal gesproken geïmplementeerd met behulp van de mechanismen die beschikbaar zijn bij de implementatieoplossing zoals VMware. Op VMware kunt u post-synchronisatieparameters gebruiken: https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-E177899E-023D-4E61-B058-AFE3822158AA.html Evenzo kunt u voor AWS Startup Scripts op een vergelijkbare manier gebruiken: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-windows-user-data.html.

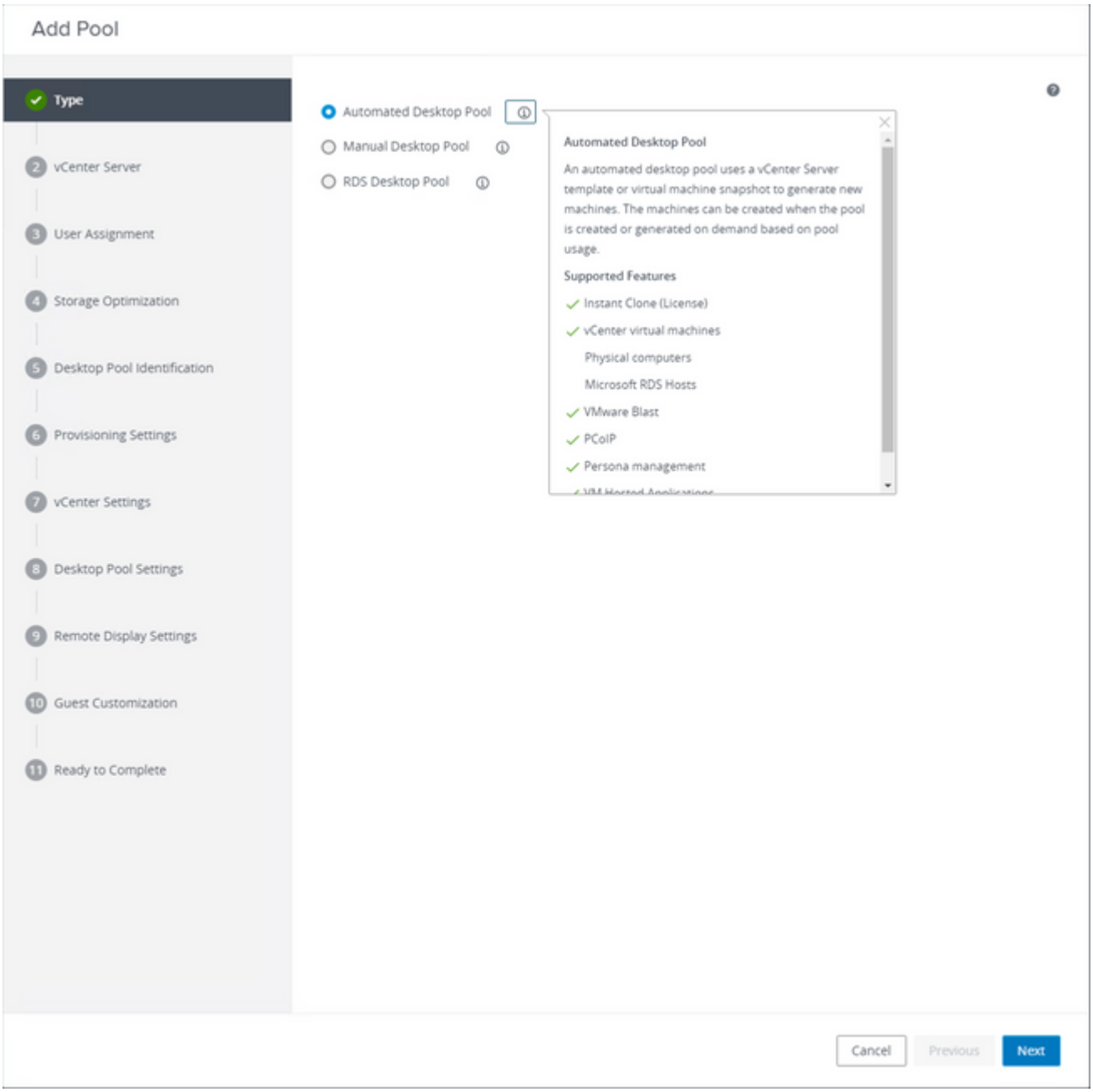
```
echo "Current hostname: %COMPUTERNAME% vs %AMP_GOLD_HOST%"

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


:same
rem Do nothing as we are still the golden image name
echo "No changes to the AMP service"
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

goto exit

:exit
```

Opmerking: de scripts in dit document worden niet officieel ondersteund door TAC

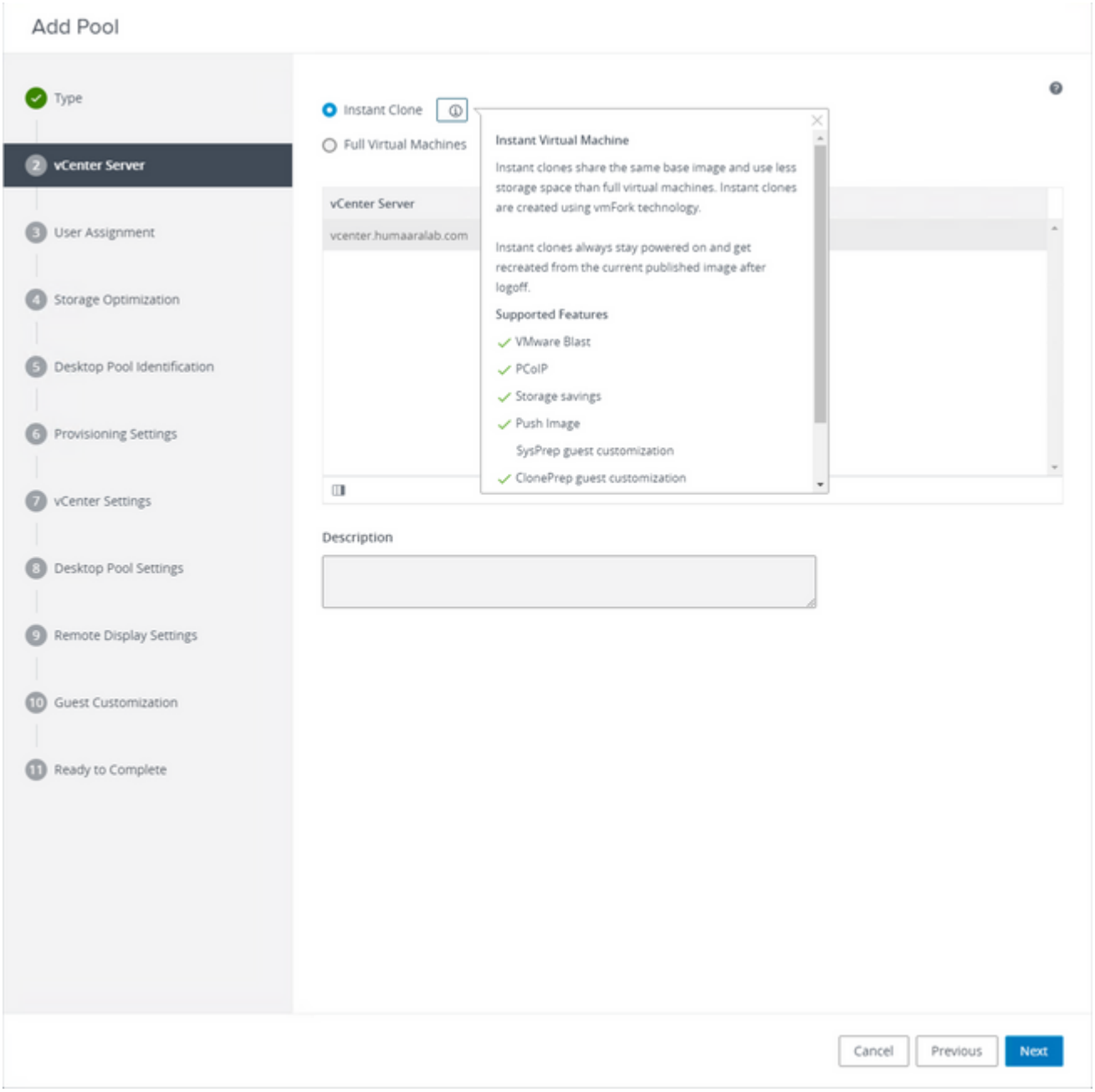
Configuratie VMware Horizon

1. Golden Image VM wordt voorbereid en alle vereiste toepassingen voor de eerste inzet van de pool worden op de VM geïnstalleerd.
2. Secure Endpoint wordt met deze opdrachtregelsyntaxis geïnstalleerd om de goldenimage-vlag op te nemen. Bijvoorbeeld, **<ampinstaller.exe> /R /S /goldenimage 1**.Houd er rekening mee dat de Golden Image Flag ervoor zorgt dat de Secure Endpoint service niet wordt uitgevoerd tot een reboot die van cruciaal belang is voor dit proces om correct te werken. Raadpleeg https://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-endpoints/118587-technote-fireamp-00.html
3. Voer na de beveiligde eindpuntinstallatie eerst het script **VMWareHorizonAMPSetup.bat** op de Golden Image VM uit. In essentie verandert dit script de AMP Service naar **Handmatig starten** en maakt een Omgeving Variabele die de Golden Image Hostname opslaat voor later gebruik.
4. U moet de **VMWareHorizonAMPStartup.bat** kopiëren naar een universeel pad op de Golden Image VM zoals "**C:\ProgramData"** aangezien dit in de latere stappen zou worden gebruikt.
5. De Golden Image VM kan nu worden uitgeschakeld en het samenstellingsproces kan worden gestart op VMware Horizon.
6. Dit is de stapsgewijze informatie over hoe het eruit ziet vanuit het perspectief van VMware Horizon:



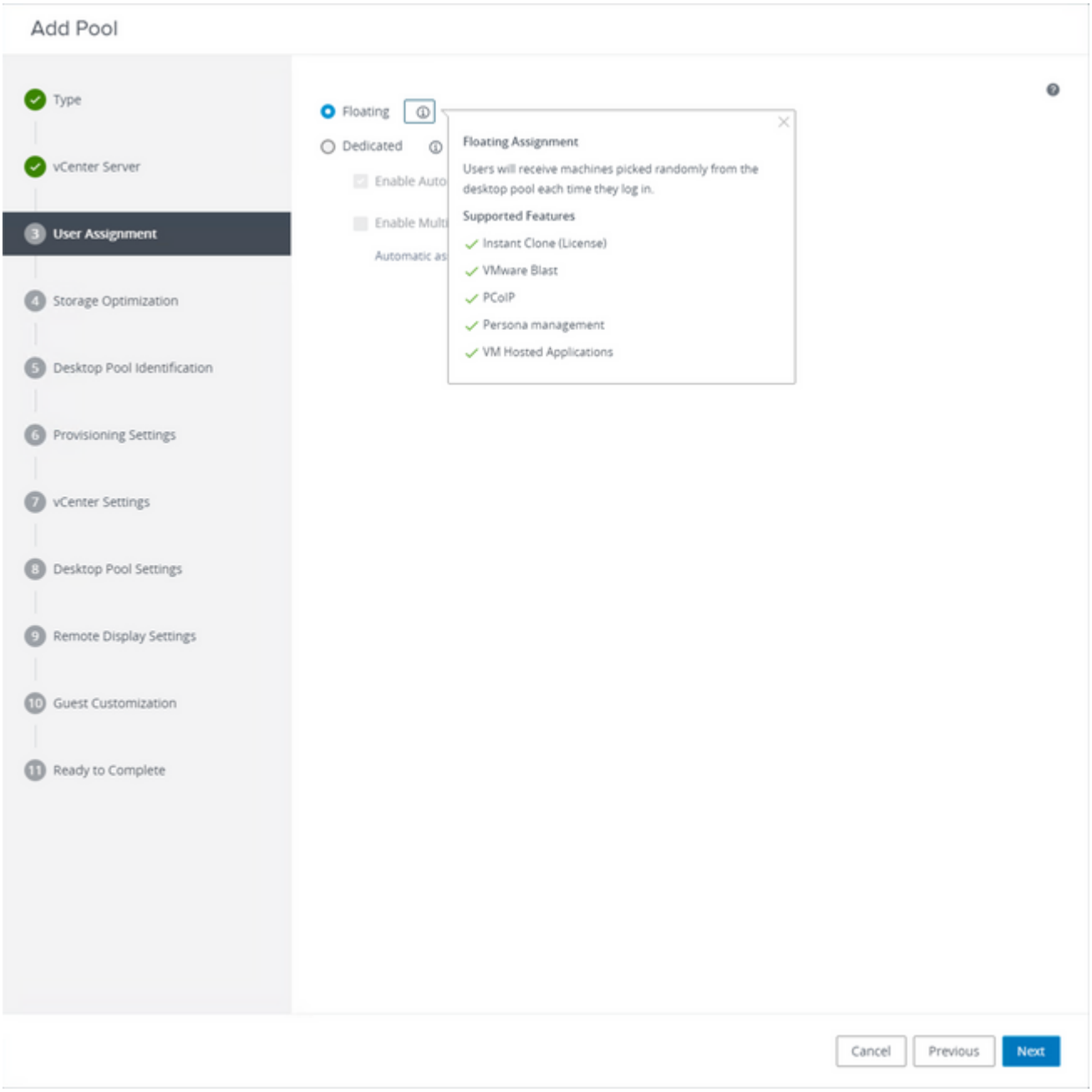
"Geautomatiseerde desktoppool" selecteren

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



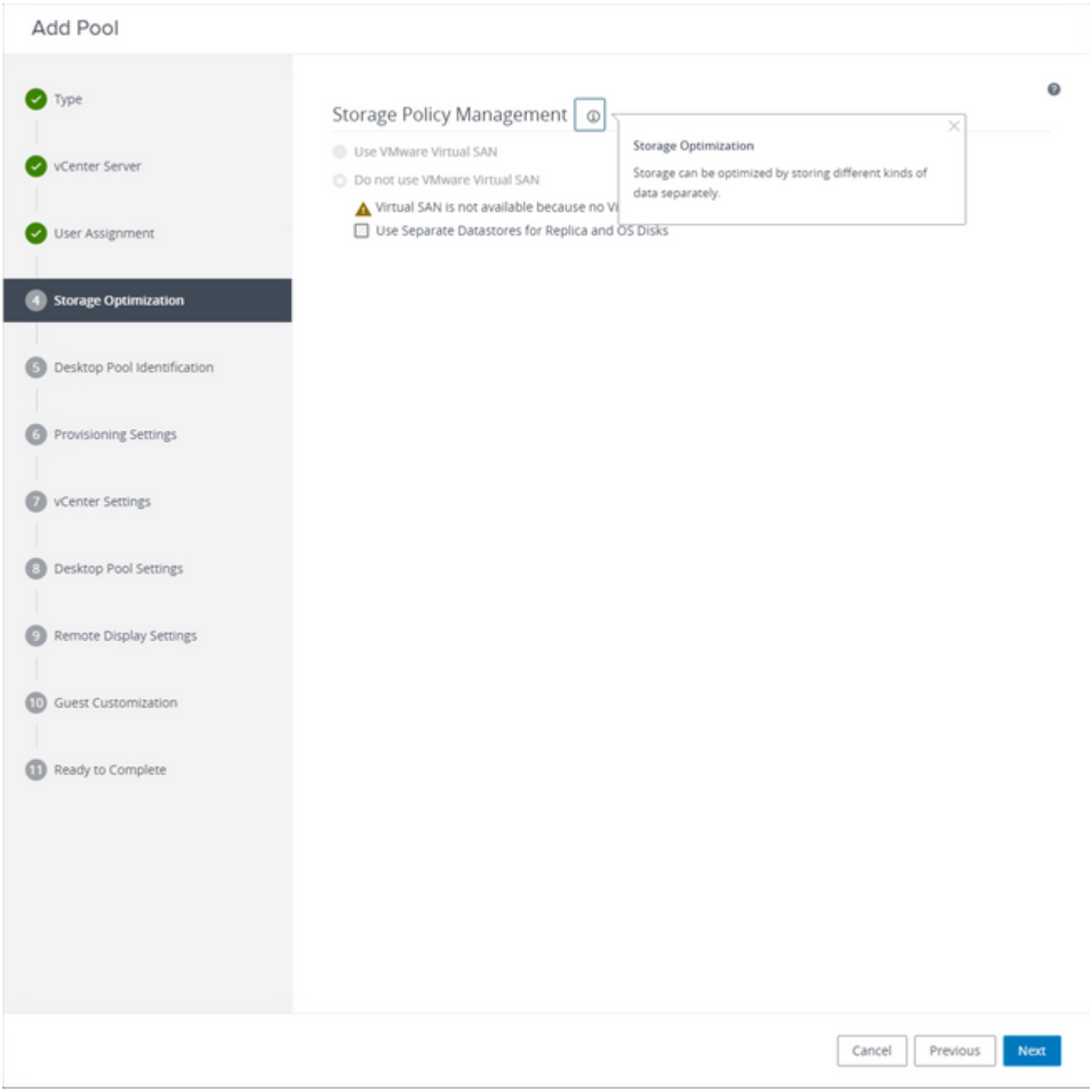
"Onmiddellijke klonen" selecteren

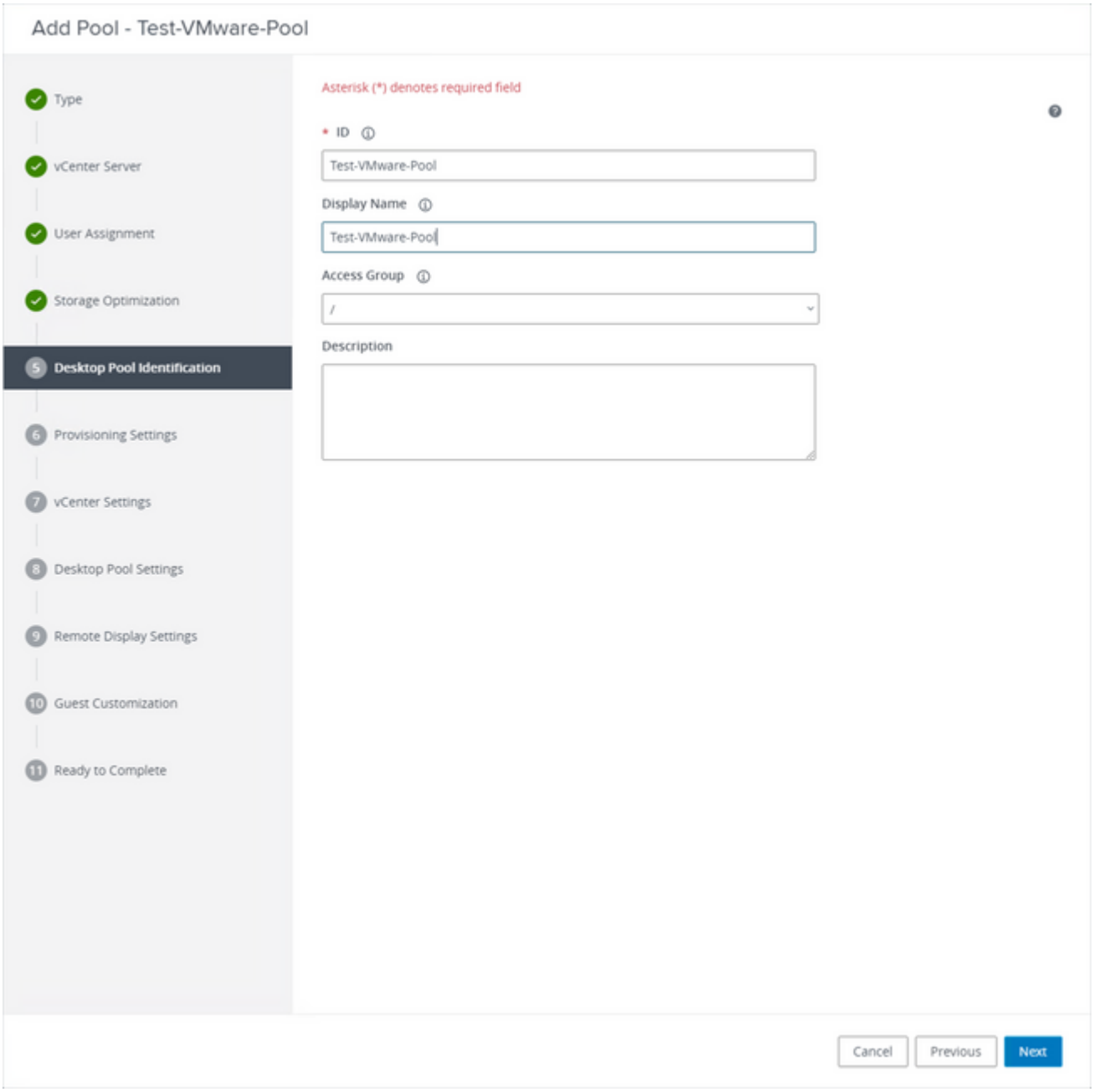
Raadpleeg: https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-D7C0150E-18CE-4012-944D-4E9AF5B28347.html



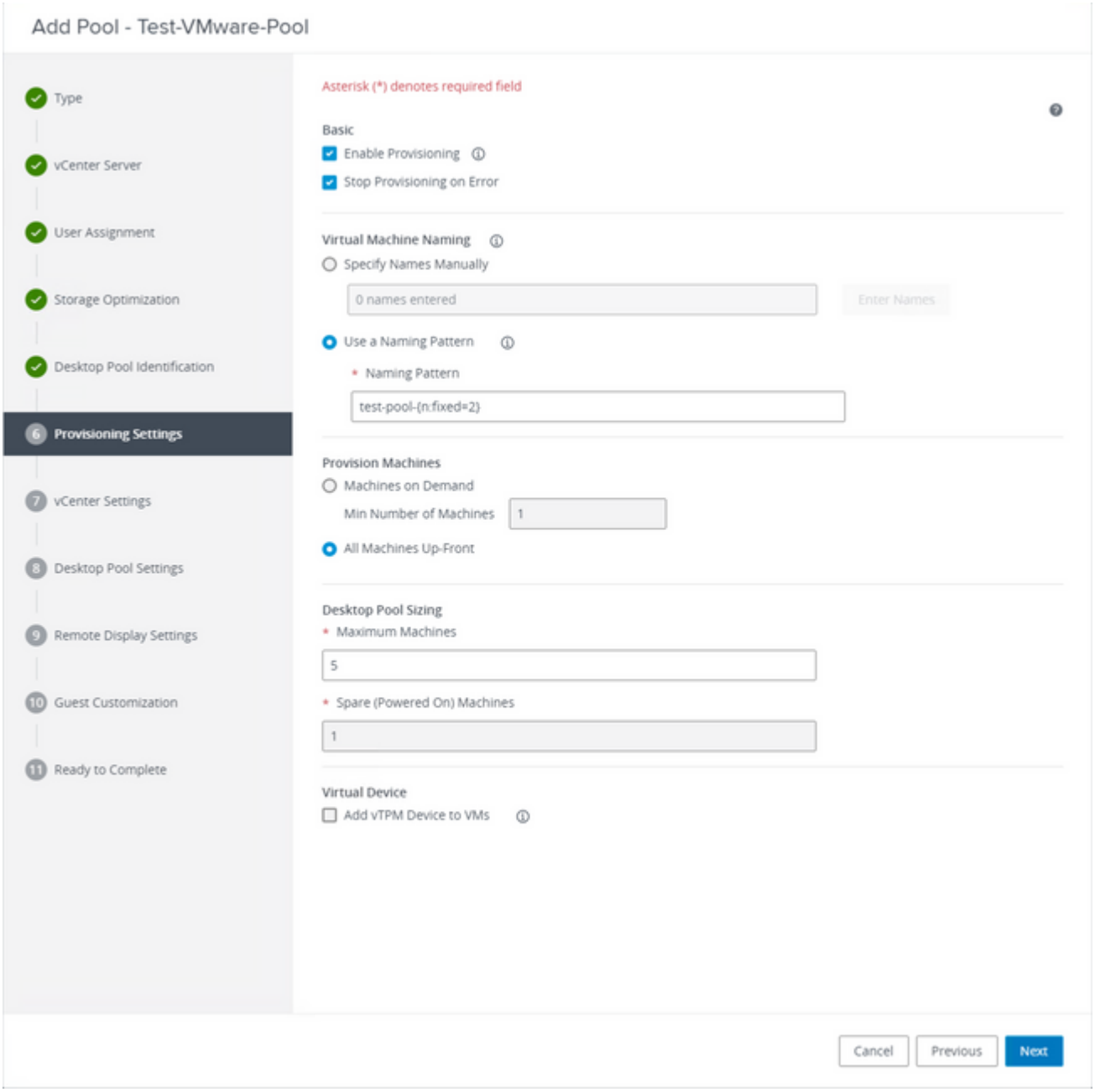
Het type "Zwevend" selecteren

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

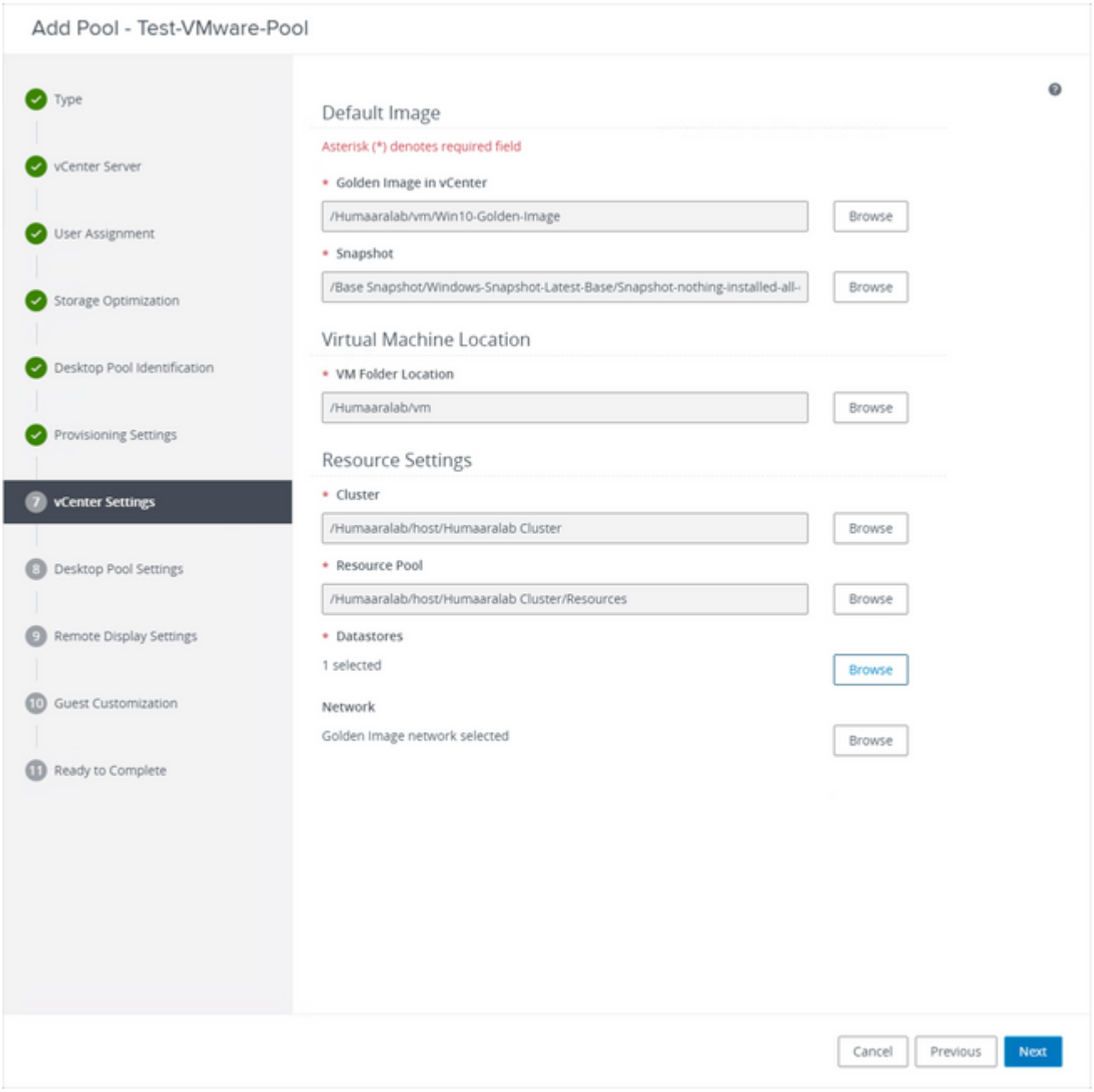

Add Pool
Type
vCenter Server
User Assignment
4 Storage Optimization
5 Desktop Pool Identification
6 Provisioning Settings
7 vCenter Settings
8 Desktop Pool Settings
9 Remote Display Settings
10 Guest Customization
11 Ready to Complete
Storage Policy Management
Use VMware Virtual SAN
Do not use VMware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



Namen van desktopgroepen

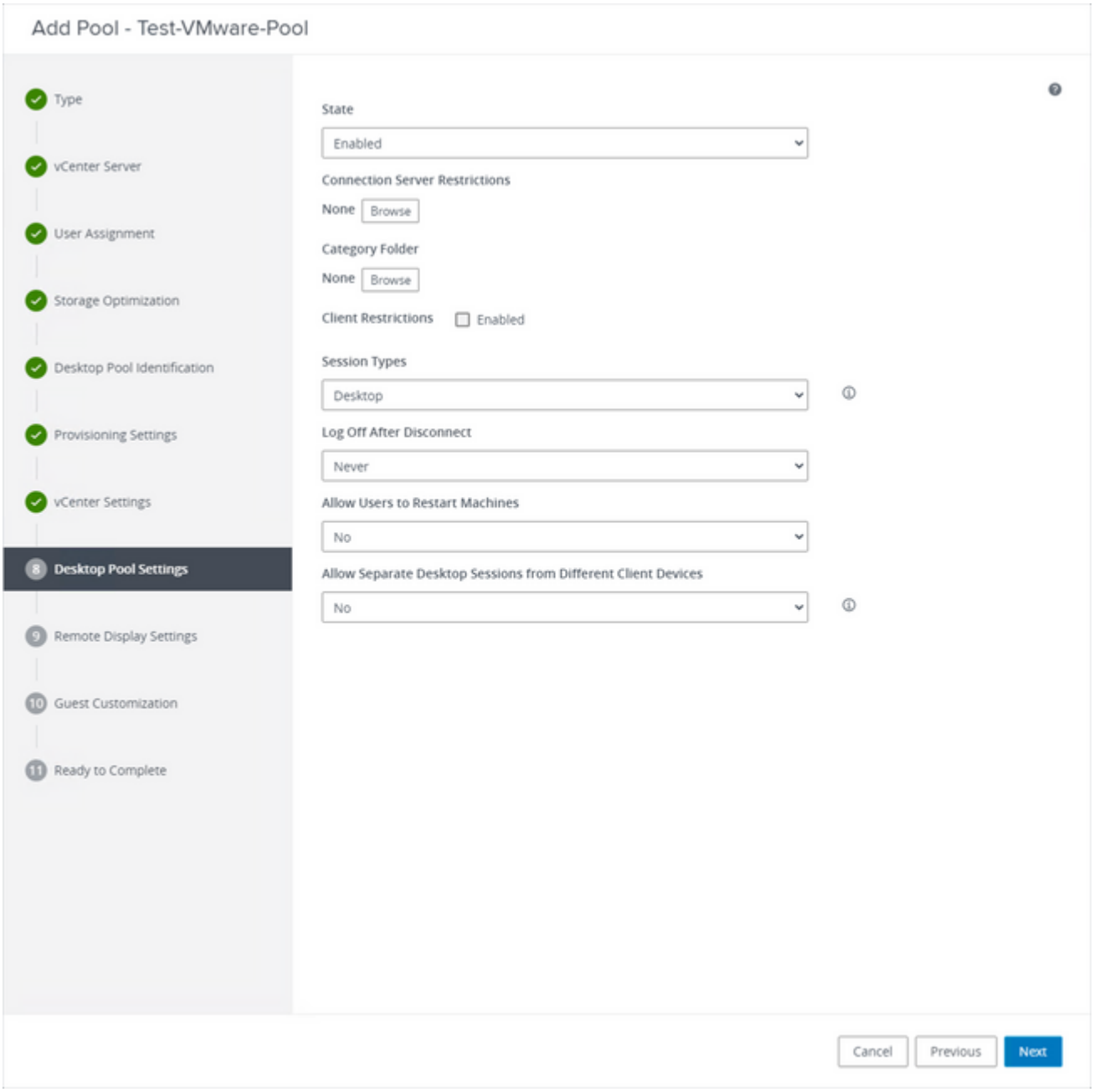


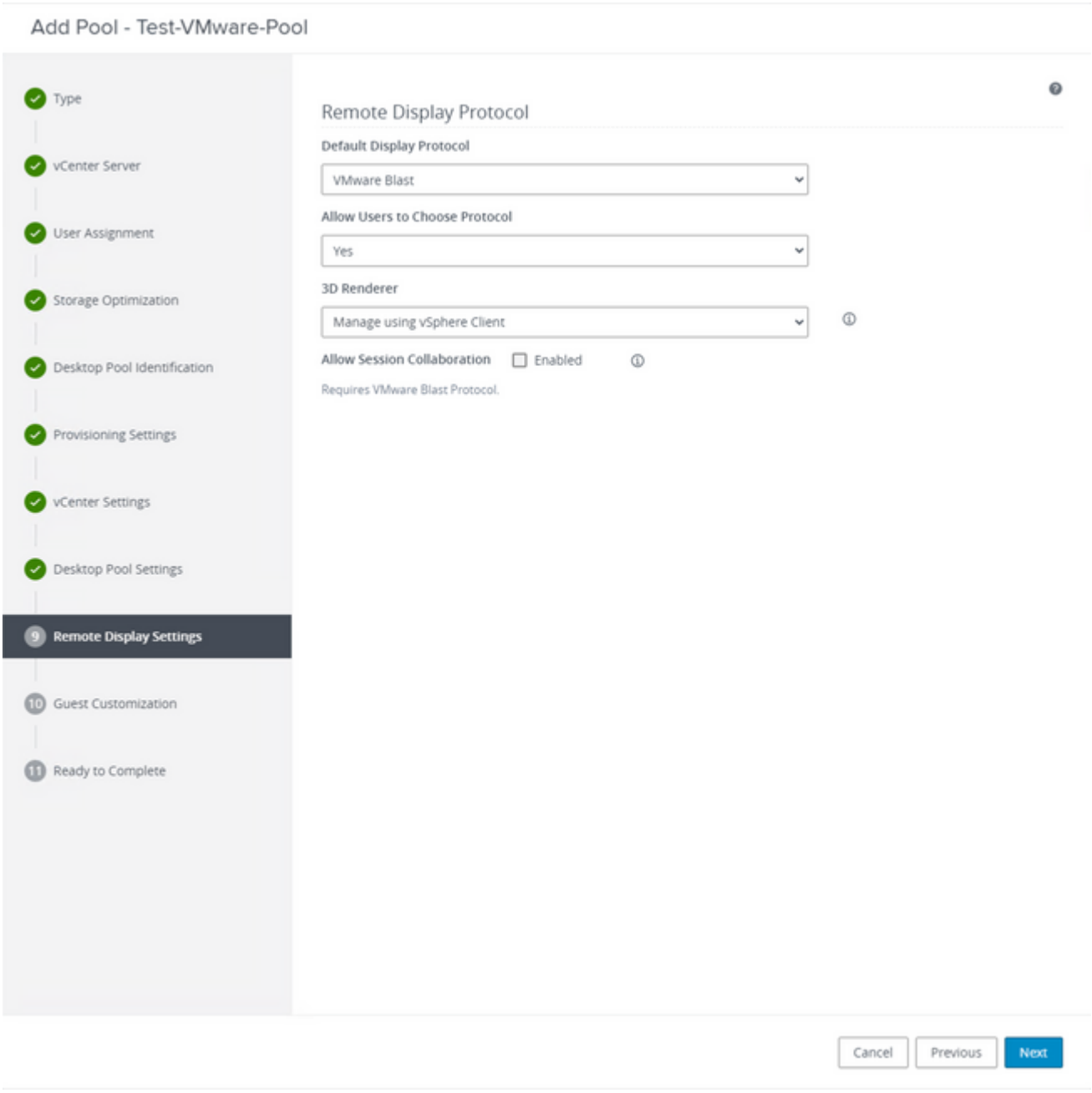
VMware Horizon Naming Pattern: https://docs.vmware.com/en/VMware-Horizon/2103/virtual-desktops/GUID-26AD6C7D-553A-46CB-B8B3-DA3F6958CD9C.html

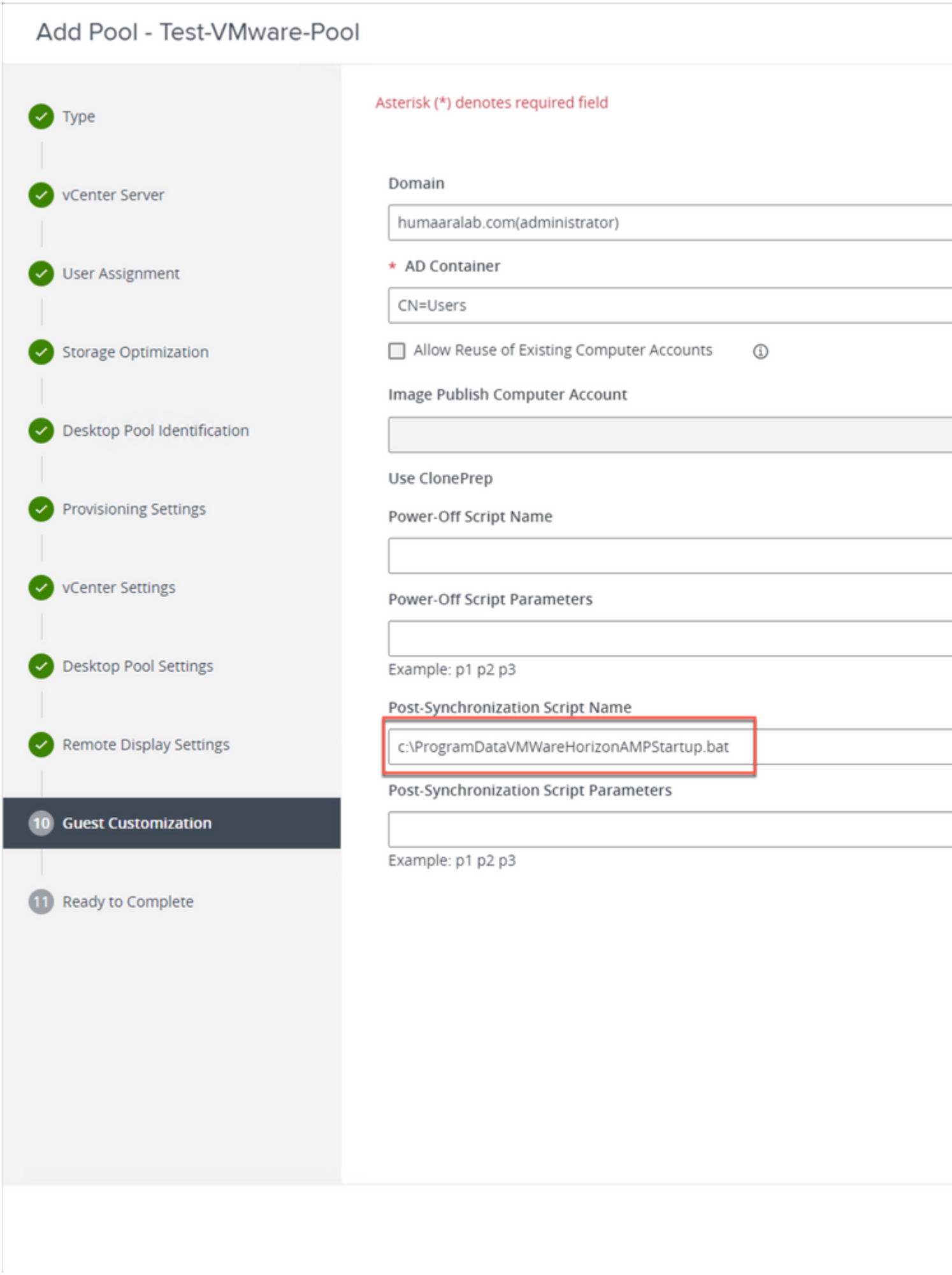


Golden Image: Dit is de eigenlijke Golden Image VM.

Snapshot: Dit is het beeld dat u wilt gebruiken om de onderliggende VM te implementeren. Dit is de waarde die wordt bijgewerkt wanneer u de Gouden Afbeelding met om het even welke veranderingen bijwerkt. Rest zijn enkele van de VMware Environment specifieke instellingen.


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. Zoals eerder vermeld, Stap 10. In de wizard staat waar u het **scriptpad** instelt.

2. De connector is geïnstalleerd, slaat het token op in local.xml en de connector doet een POST-verzoek aan het portal met het token in kwestie.
3. De cloudzijde doorloopt deze volgorde van bewerkingen:

a. De computer controleert het beleid voor de configuratie van het ID-synchronisatiebeleid. Zonder dit, treedt de registratie als normaal voor.
b. Afhankelijk van de beleidsinstellingen controleert Registratie de bestaande database op de hostnaam of het MAC-adres.
Voor alle bedrijven:Al het beleid wordt gecontroleerd op een overeenkomst op Hostname of MAC, afhankelijk van de instelling. Overeenkomende object GUID wordt genoteerd en teruggestuurd naar de eindclient machine. De client machine gaat dan uit van de UUID en veronderstelt alle groepen/beleidsinstellingen van de eerder gematchte host. Hiermee worden de geïnstalleerde beleids-/groepsinstellingen overschreven.
Over het gehele beleid:Token past het beleid aan de kant van de cloud aan en zoekt alleen binnen dat beleid naar een bestaand object met dezelfde hostnaam of hetzelfde MAC-adres. Als er een bestaat, gaat het uit van de UUID. Als er geen bestaand object aan dat beleid is gekoppeld, wordt er een nieuw object aangemaakt. Opmerking: er kunnen duplicaten bestaan voor dezelfde hostnaam die gekoppeld is aan andere groepen/beleid.
c. Als een overeenkomst niet aan een groep/beleid kan worden gemaakt toe te schrijven aan een ontbrekend teken (eerder geregistreerd, slechte plaatsingspraktijk, etc.) valt de connector aan de standaard die connectorgroep/het beleid onder het bedrijfs tabblad wordt geplaatst. Gebaseerd op de instelling van de groep/het beleid, probeert het alle beleid voor een match (over de business), alleen dat beleid in kwestie (over het beleid heen), of helemaal geen (niets) te herzien. Met dit in gedachten, is het over het algemeen geadviseerd om uw standaardgroep te plaatsen om één te zijn die hun gewenste ID synchronisatie-instellingen bevat zodat machines correct terug synchroniseren in het geval van een token probleem.

Identificeer duplicaten in uw organisatie

Extern beschikbare GitHub-scripts

Vind de Duplicate UUIDâ€™s: https://github.com/CiscoSecurity/amp-04-find-duplicate-guids

Verwijder de oude UUIDâ€™s van Stale/Old: https://github.com/CiscoSecurity/amp-04-delete-stale-guids

Redenen waarom duplicaten worden gemaakt

Er zijn een paar veel voorkomende gevallen die ervoor kunnen zorgen dat je dubbel ziet:

1. Als deze stappen zijn gevolgd tijdens de VDI-pool:

- De eerste implementatie op een niet-persistente VM/VDI vindt plaats terwijl Identity Persistence uitgeschakeld is (gebruik bijvoorbeeld een gouden afbeelding).
- Het beleid wordt in de cloud bijgewerkt om Identity Persistence ingeschakeld te hebben, die het overdag op het eindpunt bijwerkt.
- Machines worden vernieuwd/opnieuw weergegeven (gebruik dezelfde gouden afbeelding), die vervolgens het oorspronkelijke beleid weer op het eindpunt plaatst zonder Identity Persistence.
- Het beleid heeft lokaal geen Identity Persistence, dus de registratieserver controleert niet op eerdere records.
- Deze stroom resulteert in Duplicaten.

2. Gebruiker implementeert het originele gouden beeld met Identity Persistence ingeschakeld in het beleid in de ene groep en verplaatst vervolgens een eindpunt naar een andere groep van het Secure Endpoints-portaal.

Vervolgens heeft het de originele opname in de groep â€˜verhuisd-naarâ€™, maar maakt het nieuwe kopieën in de oorspronkelijke groep wanneer de VM's opnieuw worden geimaged/opnieuw worden ingezet.

> **Opmerking**: dit is geen uitputtende lijst van scenario's die duplicaten kunnen veroorzaken, maar enkele van de meest voorkomende.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.