Konfigurieren der Persistenz der Identität in einem sicheren Endgerät

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Cisco Secure Endpoint Identity Persistence-Funktion nutzen.

Was ist Identity Persistence?

Identity Persistence ist eine Funktion, die es Ihnen ermöglicht, ein konsistentes Ereignisprotokoll in virtuellen Umgebungen oder bei Neuaufnahmen von Computern zu verwalten. Sie können einen Connector an eine MAC-Adresse oder einen Hostnamen binden, sodass nicht jedes Mal ein neuer Connector-Datensatz erstellt wird, wenn eine neue virtuelle Sitzung gestartet wird oder ein Computer neu abgebildet wird. Diese Funktion wurde speziell für nicht persistente VM- und Lab-Umgebungen entwickelt und darf nicht für herkömmliche Workstation- und Server-Konfigurationen aktiviert werden.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Zugriff auf das Cisco Secure Endpoints-Portal
- Wenden Sie sich an das Cisco TAC, damit dieses die Funktion für die permanente Identitätsverwaltung in Ihrem Unternehmen aktiviert.

- Identity Persistence wird nur unter Windows Operating System (OS) unterstützt

Wann benötigen Sie dauerhafte Identitäten?

Identity Persistence ist eine Funktion für sichere Endpunkte, die bei der Identifizierung sicherer Endpunkte bei der erstmaligen Connector-Registrierung hilft und diese anhand von Identitätsparametern wie MAC-Adresse oder Hostname für diesen spezifischen Connector mit zuvor bekannten Einträgen vergleicht. Die Implementierung dieser Funktion hilft nicht nur, die Anzahl der Lizenzen korrekt zu halten, sondern ermöglicht vor allem eine korrekte Nachverfolgung von Verlaufsdaten auf nicht-persistenten Systemen.

Bereitstellung virtueller Endgeräte

Die häufigste Methode zur Persistenz der Identität in virtuellen Bereitstellungen ist die Bereitstellung einer nicht persistenten virtuellen Desktop-Infrastruktur (VDI). VDI-Host-Desktop-Umgebungen werden auf Anfrage oder Bedarf des Endbenutzers bereitgestellt. Hierzu gehören Anbieter wie VMware, Citrix, AWS AMI Golden Image Deployment usw.

Persistente VDI, auch oft als "Stateful VDI" bezeichnet, ist eine Konfiguration, in der der Desktop jedes einzelnen Benutzers individuell anpassbar ist und von einer Sitzung zu einer anderen "erhalten bleibt". Für diese Art der virtuellen Bereitstellung ist die Funktionalität von Identity Persistence nicht erforderlich, da diese Systeme nicht dazu vorgesehen sind, regelmäßig ein neues Image zu erstellen.

Wie bei jeder Software, die möglicherweise mit der Leistung des sicheren Endgeräts interagieren kann, müssen Virtual Desktop-Anwendungen auf mögliche Ausnahmen hin überprüft werden, um die Funktionalität zu maximieren und die Auswirkungen zu minimieren.

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

Bereitstellung physischer Endgeräte

Es gibt zwei Szenarien für die Bereitstellung von Identity Persistency auf physischen Computern mit sicheren Endpunkten:

- Wenn Sie einen physischen Endpunkt mit einem Golden Image mit vorinstalliertem Secure Endpoint Connector bereitstellen oder ein neues Image erstellen, muss die Goldenimage-Markierung aktiviert sein. Identity Persistence kann verwendet werden, um Duplikate in Instanzen von erneut abgebildeten Systemen zu vermeiden, ist jedoch nicht erforderlich.

- Wenn Sie einen physischen Endpunkt mit einem Golden Image bereitstellen oder ein neues Image erstellen und später den Secure Endpoint Connector installieren, kann Identity Persistence verwendet werden, um Duplizierungen in Instanzen von erneut abgebildeten Computern zu vermeiden, ist jedoch nicht erforderlich.

Häufige Probleme/Symptome bei falscher Bereitstellung von Persistenz für die Identität

Eine falsche Implementierung der Identitätspersistenz kann folgende Probleme/Symptome verursachen:

- Falsche Anzahl von Steckerplätzen
- Falsche gemeldete Ergebnisse
- Device Trajectory-Datenkonflikt

- Systemnamensaustausch in Überwachungsprotokollen
- Steckverbinder werden nach dem Zufallsprinzip von der Konsole registriert und entfernt
- Connectors werden nicht ordnungsgemäß in der Cloud gemeldet
- UUID-Duplizierung
- Duplizierung von Computernamen
- Dateninkonsistenz
- Computer werden nach der Neuzusammensetzung als Standard-Geschäftsgruppe/Richtlinie registriert

- Manuelle Bereitstellung mit aktivierter Identitätspersistenz in der Richtlinie.

- Wenn Sie den Endpunkt manuell über den Befehlszeilen-Switch bereitstellen, wobei Identity Persistence bereits in der Richtlinie aktiviert ist, und dann später den Endpunkt deinstallieren und versuchen, ihn mit einem Paket aus einer anderen Gruppe/Richtlinie neu zu installieren, wechselt der Endpunkt automatisch zur ursprünglichen Richtlinie zurück.

- Ausgabe aus SFC-Protokollen mit eigenem Policy-Switch 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
```

Der andere Nebeneffekt, wenn Sie versuchen, einen Connector zu installieren, der zu einer anderen Gruppe gehört. Sie sehen im Portal, dass der Connector der richtigen Gruppe zugewiesen ist, aber mit der "**falschen"** ursprünglichen Richtlinie.

Das liegt daran, wie Identity Persistence (ID SYNC) funktioniert.

Ohne ID SYNC, sobald der Connector vollständig deinstalliert wurde, oder mit dem Befehlszeilenschalter zur Neuregistrierung. Im Falle einer Deinstallation sollten Sie die neue GUID für das Erstellungsdatum und den Connector sehen oder im Falle eines Befehls zur erneuten Registrierung nur die neue GUID für den Connector. Bei ID SYNC ist dies jedoch nicht möglich, da ID SYNC mit der alten GUID und DATE überschrieben wird. So "synchronisieren" wir den Host.

Wenn dieses Problem festgestellt wird, muss die Behebung durch die Richtlinienänderung implementiert werden. Sie müssen die betroffenen Endpunkte zurück zur ursprünglichen Gruppe/Richtlinie verschieben und sicherstellen, dass die Richtlinie synchronisiert wird. Verschieben Sie dann die Endpunkte zurück zur gewünschten Gruppe/Richtlinie.

Best Practices für die Bereitstellung

Snapvol-Datei konfigurieren

Falls Sie App-Volumes für Ihre VDI-Infrastruktur verwenden, sollten Sie diese Konfigurationsänderungen an Ihrer **snapvol.cfg**-Konfiguration vornehmen

Diese Ausschlüsse müssen in der **Datei snapvol.cfg** implementiert werden:

Pfade

- 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

Registrierungsschlüssel:

- HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Immunet schützen
- 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

Fügen Sie auf x64-Systemen Folgendes hinzu:

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

Referenzen:

- 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

Erstellung von goldenen Bildern

Befolgen Sie die Best Practices-Richtlinien aus dem Dokument des Anbieters (VMware, Citrix, AWS, Azure usw.), wenn Sie ein Golden Image für den VDI-Klonprozess erstellen.

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

Da Sie die VMware identifiziert haben, startet der AWS-Zusammenstellungsprozess die geklonten (untergeordneten VMs) vor Abschluss der VM-Konfiguration mehrmals neu. Dies führt zu Problemen mit dem Registrierungsprozess für sichere Endpunkte, da den geklonten (untergeordneten VMs) derzeit nicht die endgültigen/korrekten Hostnamen zugewiesen sind, und die geklonten (untergeordneten VMs) den Golden Image-Hostnamen verwenden und sich in der sicheren Endpoint-Cloud registrieren. Dies unterbricht den Klonprozess und würde zu Problemen führen.

Dies ist kein Problem mit dem Connector-Prozess für sichere Endpunkte, sondern mit dem Klonprozess und der Registrierung sicherer Endpunkte unvereinbar. Um dieses Problem zu vermeiden, haben wir einige Änderungen im Klonprozess identifiziert, die zur Lösung dieser Probleme beitragen.

Dies sind die Änderungen, die auf dem virtuellen System für Golden Image implementiert werden müssen, bevor das Image für den Clone eingefroren wird.

1. Verwenden Sie zum Zeitpunkt der Installation von Secure Endpoint immer die **Goldenimage**-Markierung auf dem Golden Image.

2. Implementieren Sie Skripte, die den Endpunktdienst nur aktivieren, wenn auf den geklonten (untergeordneten VMs) ein endgültiger Hostname implementiert ist. Weitere Informationen finden Sie im Abschnitt VMware Horizon Duplication Issues (VMware-Horizon-Duplizierungsprobleme).

Markierung zum Überschreiben des goldenen Bilds

Wenn Sie das Installationsprogramm verwenden, wird das Flag für goldene Images /**goldenimage 1** verwendet.

Das goldene Image-Flag verhindert, dass der Connector gestartet und im Basis-Image registriert wird. Beim nächsten Start des Images befindet sich der Connector also im funktionalen Zustand, in dem er durch die ihm zugewiesene Richtlinie konfiguriert wurde.

Für Informationen über andere Flags, können Sie verwenden, bitte lesen Sie diesen Artikel.

Als goldenes Bild installieren. Dies ist die typische Option, die mit dem Flag verwendet wird, und die einzige erwartete Verwendung. Überspringt die anfängliche Connector-Registrierung und den Startvorgang bei der Installation.

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

Schritte zur Erstellung von goldenen Bildern

Es ist empfehlenswert, den Steckverbinder zuletzt für die Vorbereitung des **Golden Image** zu installieren.

1. Bereiten Sie das Windows-Abbild entsprechend Ihren Anforderungen vor, installieren Sie die gesamte erforderliche Software und die Konfigurationen für das Windows-Abbild mit Ausnahme des Connectors.
2. Installieren Sie den Cisco Secure Endpoint-Connector.
3. Verwenden Sie das **Flag /goldenimage 1**, um dem Installationsprogramm zu signalisieren, dass es sich um eine Bereitstellung eines goldenen Images handelt.

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

4. Implementieren Sie die Skriptlogik (falls erforderlich) wie hier beschrieben.
5. Vollständige Installation.
6. Lassen Sie Ihr goldenes Bild stehen.

Nachdem Anwendungen auf dem Golden Image installiert wurden, das System vorbereitet wurde und Secure Endpoint mit der/**goldenimageflag** installiert wurde, kann der Host eingefroren und verteilt werden. Nach dem Start des geklonten Hosts startet Secure Endpoint und registriert sich bei der Cloud. Für die Konfiguration des Connectors sind keine weiteren Maßnahmen erforderlich, es sei denn, Sie möchten Änderungen an der Richtlinie oder dem Host vornehmen. Wenn Änderungen nach der Registrierung des Golden Images vorgenommen werden, muss dieser Prozess neu gestartet werden.

Portalrichtlinienplanung

Dies sind einige der Best Practices, die bei der Implementierung von Identity Persistence auf Secure Endpoint Portal befolgt werden müssen:

1. Es wird dringend empfohlen, separate Richtlinien/Gruppen für Endgeräte mit aktivierter Identity Persistence zu verwenden, um die Segregation zu vereinfachen.

2. Wenn Sie die Endpunktisolierung verwenden und den Befehl **Computer nach** Kompromittierung **in Gruppe verschieben** implementieren möchten. Für die Zielgruppe muss außerdem "Identity Persistence" aktiviert sein und darf nur für VDI-Computer verwendet werden.

3. Es wird nicht empfohlen, **Identity Persistence** auf der Standardgruppe/Policy in Ihren Organisationseinstellungen zu aktivieren, es sei denn, Identity Persistence wurde für alle Richtlinien mit Across Organization als Einstellungsbereich aktiviert.

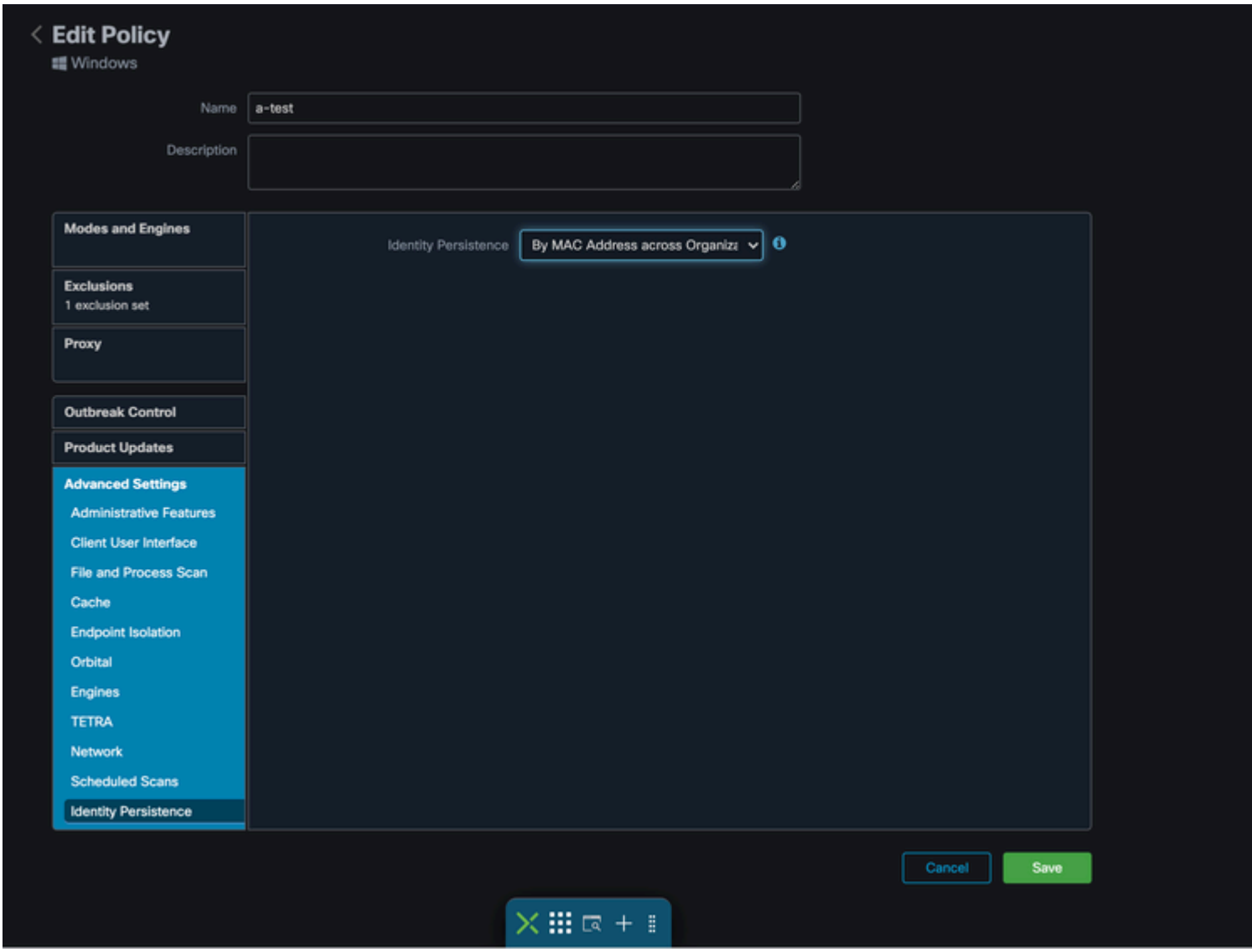
Konfiguration

Führen Sie die folgenden Schritte aus, um den Secure Endpoint Connector mit Identity Persistency bereitzustellen:

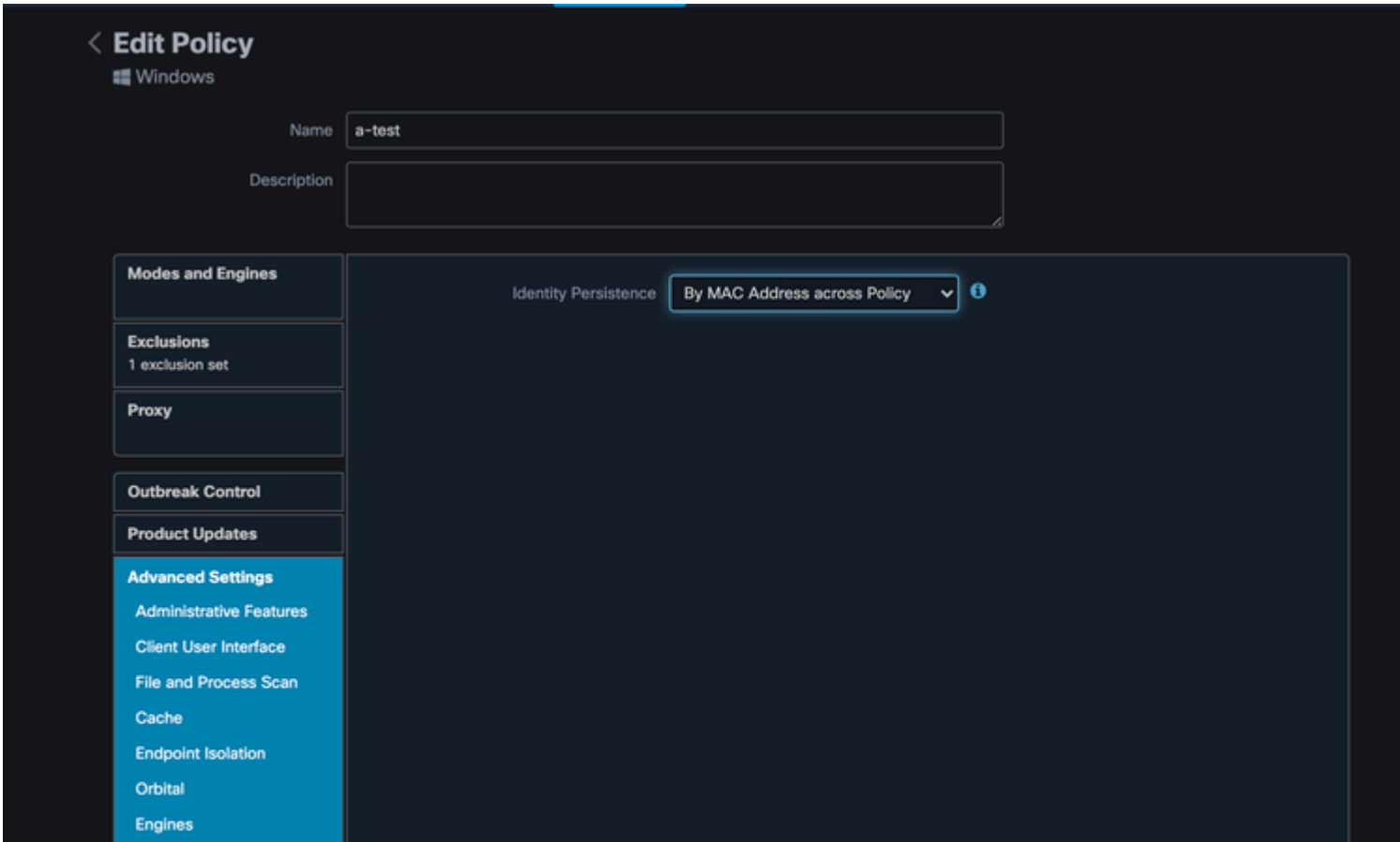
Schritt 1: Wenden Sie die gewünschte Einstellung für die Persistenz der Identität auf Ihre Richtlinien an:

- Navigieren Sie im Secure Endpoint-Portal zu **Management > Policies (Verwaltung > Richtlinien)**.
- Wählen Sie die gewünschte Richtlinie aus, für die Identity Persistence aktiviert werden soll, und **klicken Sie** dann **auf Edit**.
- Navigieren Sie zu **der** Registerkarte **Erweiterte Einstellungen**, und klicken Sie dann unten auf die Registerkarte **Identitätspersistenz**.
- Wählen Sie das Dropdown-Menü Identity Persistence (Identitätspersistenz) und anschließend die für

Ihre Umgebung am sinnvollsten Option aus. Siehe dieses Bild.


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

- Nach MAC-Adresse im gesamten Unternehmen: Neue oder aktualisierte Installationen suchen nach dem neuesten Connector-Datensatz mit derselben MAC-Adresse, um frühere Verlaufsdaten mit der neuen Registrierung zu synchronisieren. Diese Einstellung durchsucht alle Geschäftsunterlagen

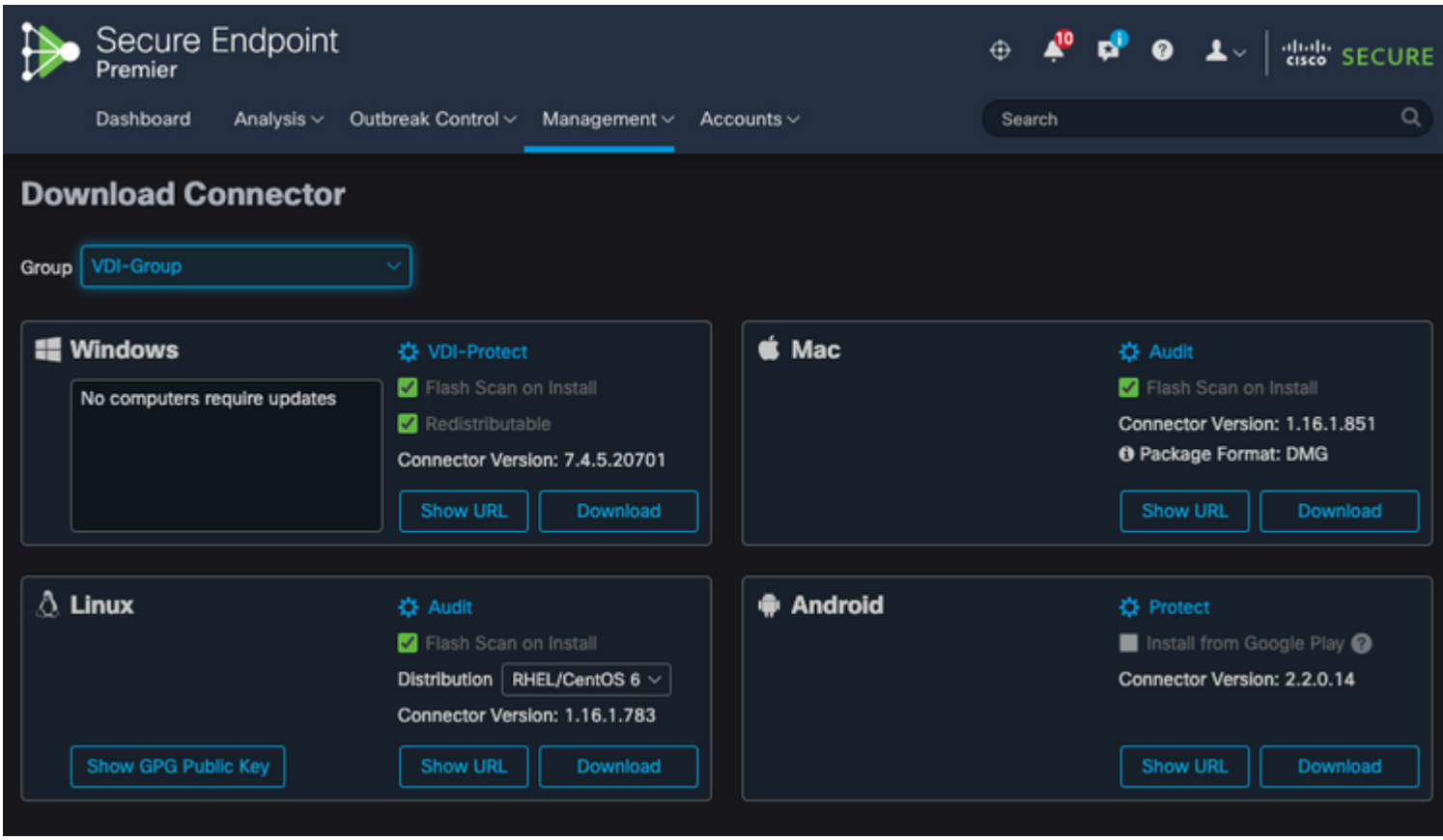
  für alle Richtlinien in der Organisation, für die die Identitätssynchronisierung auf einen anderen Wert als None festgelegt ist. Der Connector kann seine Richtlinie so aktualisieren, dass sie die vorherige Installation widerspiegelt, wenn sie sich von der neuen unterscheidet.

- By MAC Address across Policy (Nach MAC-Adresse über Richtlinie): Neue oder aktualisierte Installationen suchen nach dem neuesten Connector-Datensatz mit derselben MAC-Adresse, um frühere Verlaufsdaten mit der neuen Registrierung zu synchronisieren. Diese Einstellung durchsucht nur die Datensätze, die der bei der Bereitstellung verwendeten Richtlinie zugeordnet sind. Wenn der Connector zuvor nicht in dieser Richtlinie installiert, aber in einer anderen bereits aktiv war, können Duplikate erstellt werden.
- Nach Hostname in allen Geschäftsbereichen: Neue oder aktualisierte Installationen suchen nach dem neuesten Connector-Datensatz mit demselben Hostnamen, um frühere Verlaufsdaten mit der neuen Registrierung zu synchronisieren. Diese Einstellung durchsucht alle Geschäftsdatensätze, unabhängig von den Einstellungen für die Persistenz der Identität in anderen Richtlinien, und Connector kann seine Richtlinie aktualisieren, um die vorherige Installation wiederzugeben, wenn sie sich von der neuen unterscheidet. Der Hostname enthält FQDN, sodass Duplikate auftreten können, wenn sich der Connector regelmäßig zwischen Netzwerken bewegt (z. B. auf einem Laptop).
- Nach Hostname in allen Richtlinien: Neue oder aktualisierte Installationen suchen nach dem neuesten Connector-Datensatz mit demselben Hostnamen, um frühere Verlaufsdaten mit der neuen Registrierung zu synchronisieren. Diese Einstellung durchsucht nur die Datensätze, die der für die Bereitstellung verwendeten Richtlinie zugeordnet sind. Wenn der Connector zuvor nicht in dieser Richtlinie installiert, aber in einer anderen bereits aktiv war, können Duplikate erstellt werden. Der Hostname enthält FQDN, sodass es auch zu Duplikaten kommen kann, wenn sich der Connector regelmäßig zwischen Netzwerken bewegt (z. B. auf einem Laptop).

Hinweis: Wenn Sie Identity Persistence verwenden möchten, empfiehlt Cisco, **By Hostname (Nach Hostname)** für **alle geschäftlichen oder richtlinienbasierten Anwendungen** zu verwenden. Ein System hat einen Hostnamen, kann aber mehrere MAC-Adressen haben, und viele VMs klonen die MAC-Adressen.

Schritt 2: Laden Sie den Secure Endpoint Connector herunter.

- Navigieren Sie **zuManagement > Download Connector**.
- Wählen Sie die Gruppe für die Richtlinie aus, die Sie in Schritt 1 bearbeitet haben.
- **Klicken Sie** für den Windows Connector auf **Herunterladen**, wie im Bild dargestellt.



Schritt 3: Bereitstellung von Connector für Endgeräte

- Sie können den heruntergeladenen Connector jetzt verwenden, um Secure Endpoint (mit aktivierter Identity Persistence) manuell auf Ihren Endgeräten zu installieren.
- Andernfalls können Sie den Connector auch mithilfe eines goldenen Images bereitstellen (siehe Abbildung).

Hinweis: Sie müssen das verteilbare Installationsprogramm auswählen. Dies ist eine Datei mit ca. 57 MB (Größe kann mit neueren Versionen variieren), die sowohl die 32- als auch die 64-Bit-Installationsprogramme enthält. Um den Connector auf mehreren Computern zu installieren, können Sie diese Datei in eine Netzwerkfreigabe einfügen oder sie an alle Computer übertragen. Das Installationsprogramm enthält eine Datei policy.xml, die als Konfigurationsdatei für die Installation verwendet wird.

VMware Horizon-Duplizierungsprobleme

Mit VMware Horizon konnten wir feststellen, dass die untergeordneten VM-Systeme bei ihrer Erstellung im Rahmen des Horizon-Erstellungsprozesses mehrmals neu gestartet werden. Dies führt zu Problemen, wenn die Secure Endpoint Services aktiviert werden, wenn die untergeordneten VMs nicht bereit sind (ihnen wurde nicht der endgültige/richtige NetBios-Name zugewiesen). Dies führt zu weiteren Problemen mit Secure Endpoint, die zu Verwirrung führen und die Prozesse unterbrechen. Nach weiteren Untersuchungen hat das Engineering Team eine Lösung für diese Inkompatibilität mit dem Horizon-Prozess gefunden, die die Implementierung der angehängten Skripte auf der Golden Image VM und die Verwendung der Post-Synchronisations-Skript-Funktionalität für VMware Horizon umfasst: https://docs.vmware.com/en/VMware-Horizon/2103/published-desktops-applications.pdf.

Dies ist höchstwahrscheinlich bei allen anderen Anbietern der Fall, z. B. Citrix, AWS usw., weshalb diese Lösung auch für sie geeignet ist.

Keine Konfiguration/Änderungen mehr erforderlich

- Sie müssen Secure Endpoint nicht mehr deinstallieren und erneut installieren, wenn Sie nach der ersten Bereitstellung Änderungen am Golden Image vornehmen möchten.
- Der Dienst für sichere Endgeräte muss nicht auf **verzögerter Start** festgelegt **werden**.

Skriptmethodik

Hier sind die Beispielskripte, die verwendet werden können.

- **VMWareHorizonAMPSetup.bat:** Dieses Skript muss implementiert werden, sobald AMP wie zuvor beschrieben mit den Flags installiert wurde, wie weiter oben beschrieben. Mit diesem Skript wurde der Secure Endpoint-Dienst in Manueller Start geändert, und der Hostname für das Golden Image wird als Umgebungsvariable gespeichert, auf die im nächsten Schritt verwiesen werden kann.

```
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:** Mit diesem Skript wird logisch überprüft, ob der Hostname auf den geklonten (untergeordneten) VMs mit dem im vorherigen Schritt gespeicherten übereinstimmt, um sicherzustellen, dass der geklonte (untergeordnete) VM einen Hostnamen erhält, der nicht dem Golden Image VM entspricht (dies wäre der endgültige Hostname für die Maschine). Anschließend starten Sie Secure Endpoint Zeigen Sie auf "Service", und ändern Sie dies in "Automatisch". Sie entfernen auch die Umgebungsvariable aus dem zuvor erwähnten Skript. Dies wird in der Regel mithilfe der von der Bereitstellungslösung wie VMware verfügbaren Mechanismen implementiert. Auf VMware können Sie nach der Synchronisierung folgende Parameter verwenden: https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-E177899E-023D-4E61-B058-AFE3822158AA.html Ähnlich für AWS können Sie Startup Scripts auf ähnliche Weise verwenden: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-windows-user-data.html.

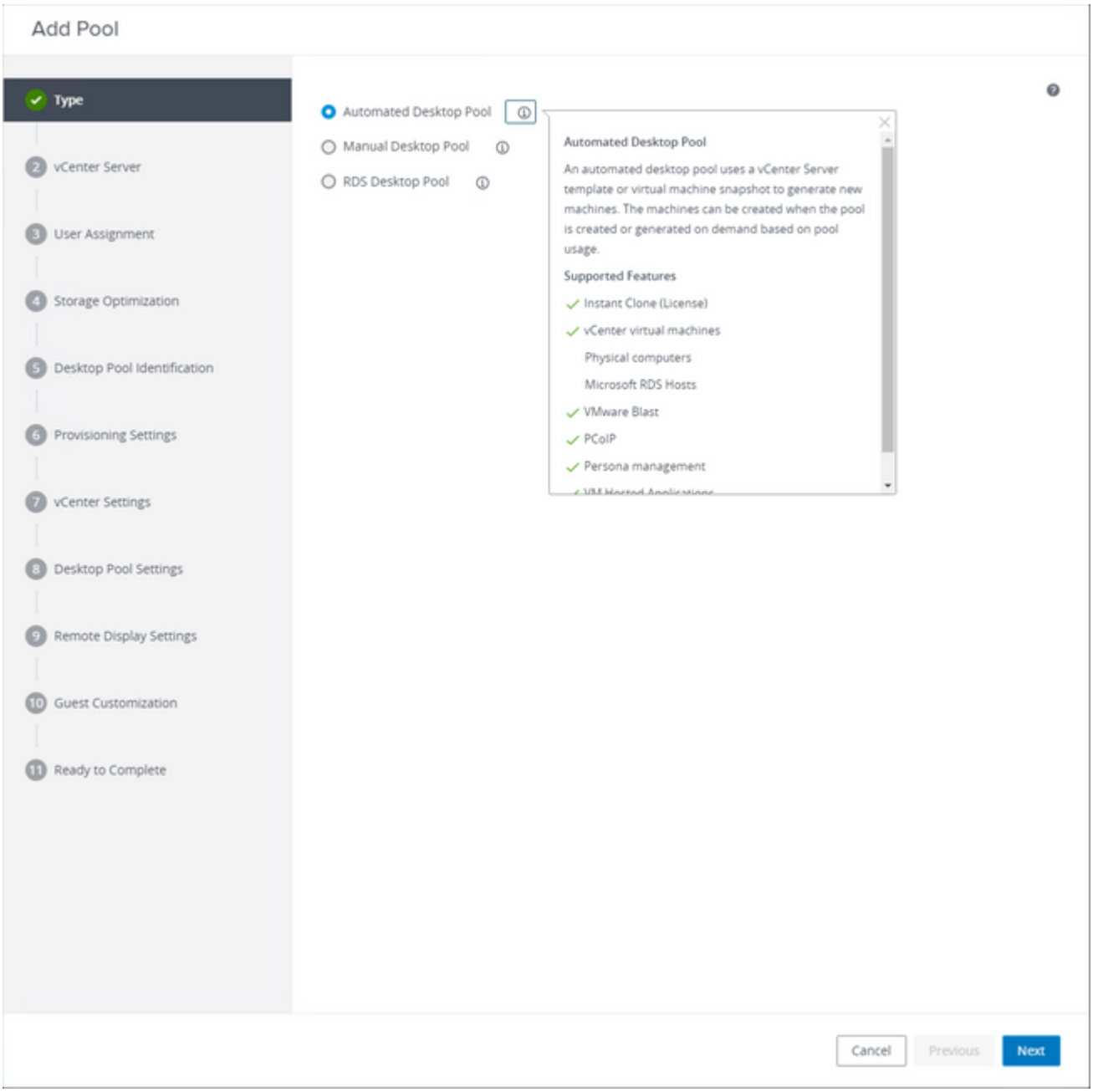
```
echo "Current hostname: %COMPUTERNAME% vs %AMP_GOLD_HOST%"

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
```

Hinweis: Beachten Sie, dass die in diesem Dokument enthaltenen Skripte nicht offiziell vom TAC unterstützt werden.

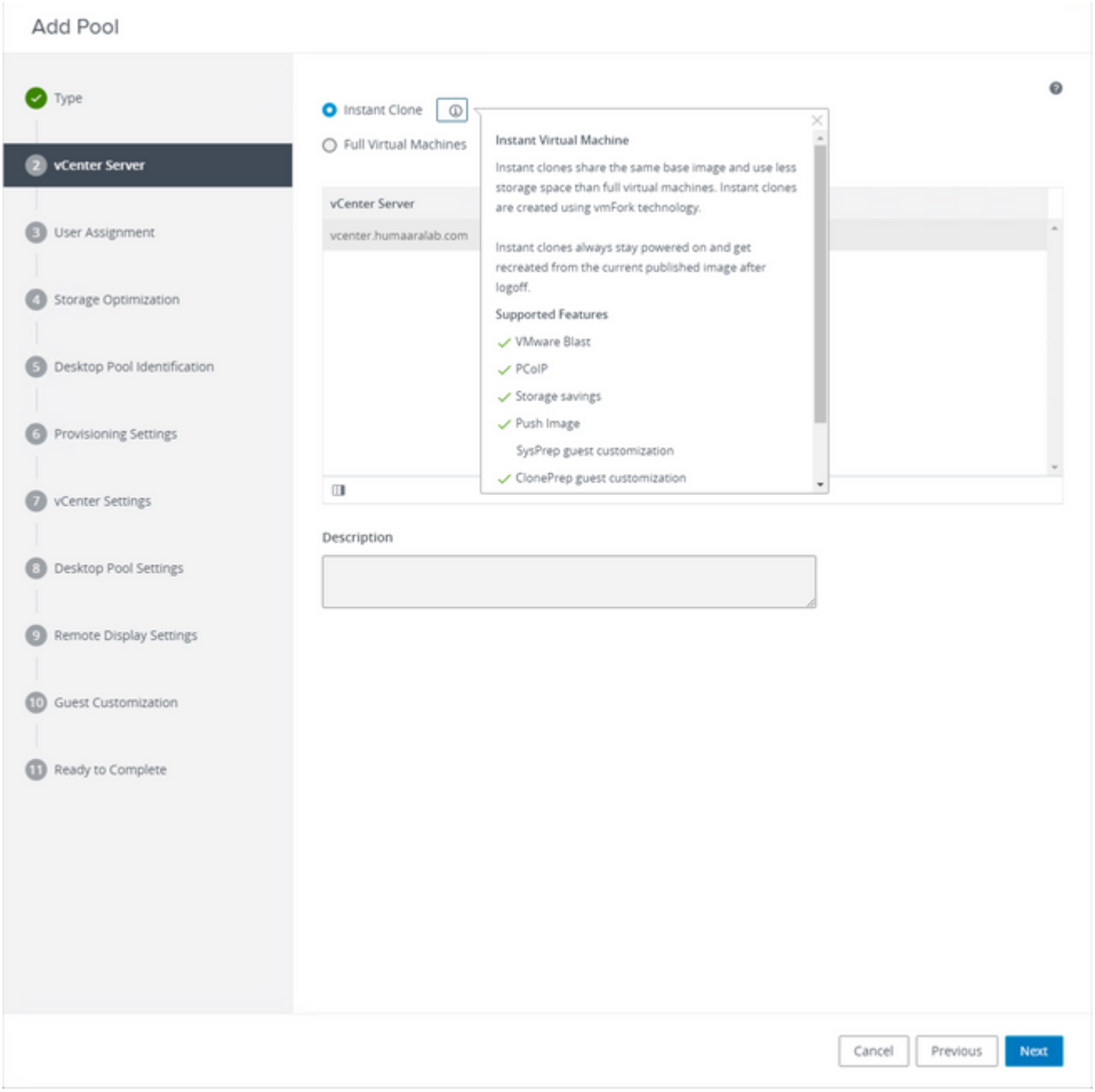
Konfiguration von VMware Horizon

1. Die Golden Image VM ist vorbereitet, und alle für die anfängliche Bereitstellung des Pools erforderlichen Anwendungen sind auf der VM installiert.
2. Secure Endpoint wird mit dieser Befehlszeilensyntax installiert, um das goldenimage-Flag einzuschließen. Beispiel: <**ampinstaller.exe**> **/R /S /goldenimage 1.**Beachten Sie, dass das Flag "Golden Image" sicherstellt, dass der Secure Endpoint-Dienst erst nach einem Neustart ausgeführt wird, der für das ordnungsgemäße Funktionieren dieses Prozesses von entscheidender Bedeutung ist. Siehe https://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-endpoints/118587-technote-fireamp-00.html
3. Führen Sie nach der Installation des sicheren Endpunkts zuerst das Skript **VMWareHorizonAMPSetup.bat** auf der Golden Image VM aus. Im Wesentlichen ändert dieses Skript den AMP-Dienst in **Manueller Start** und erstellt eine Umgebungsvariable, die den Hostnamen des Golden Image für die spätere Verwendung speichert.
4. Sie müssen die **VMWareHorizonAMPStartup.bat** auf einen universellen Pfad auf der Golden Image VM wie "**C:\ProgramData**" kopieren, da dies in den späteren Schritten verwendet wird.
5. Die Golden Image VM kann nun heruntergefahren und der Kompositionsprozess auf VMware Horizon initiiert werden.
6. Dies sind die aus VMware Horizon-Sicht wichtigsten Informationen:



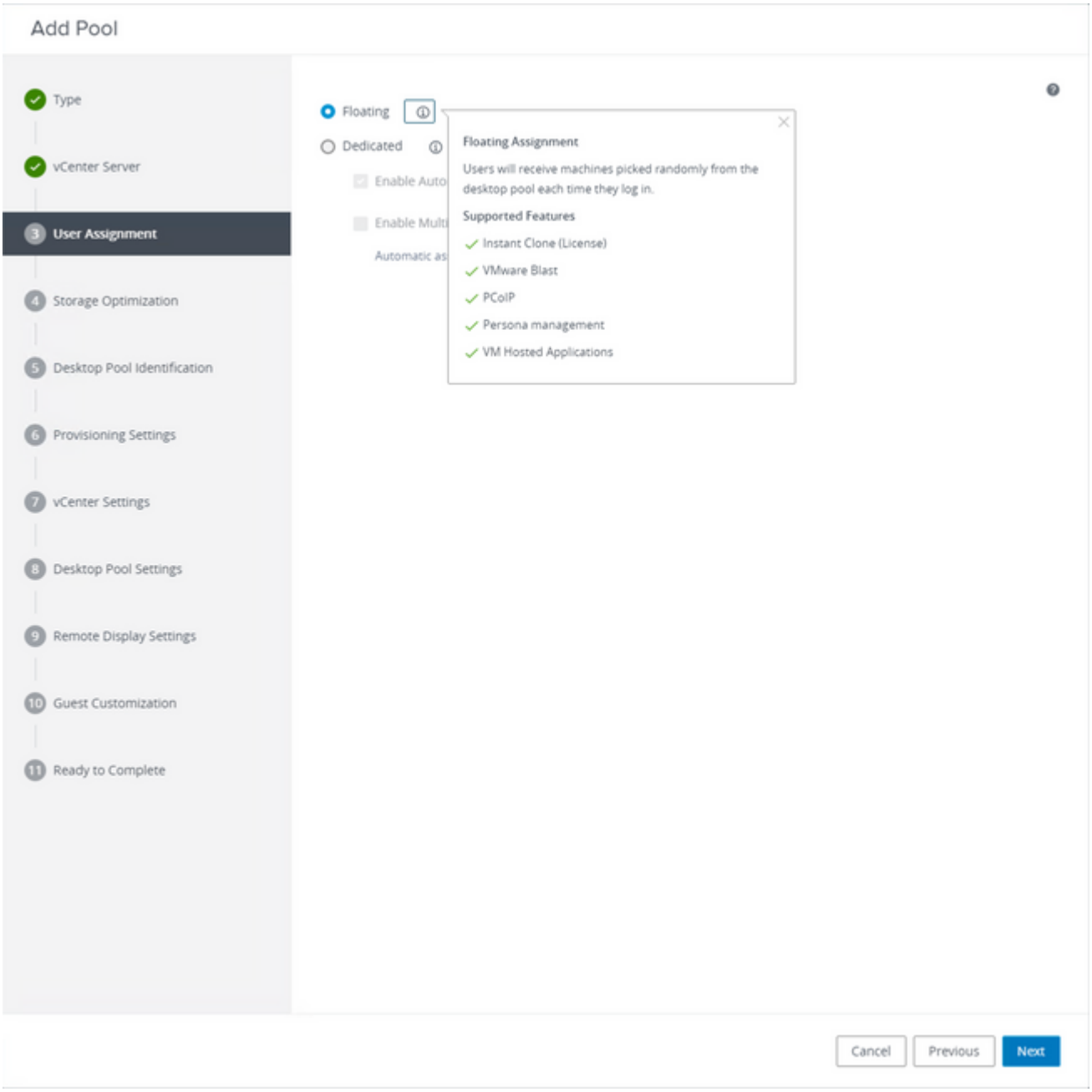
Auswählen von "Automatisierter Desktop-Pool"

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



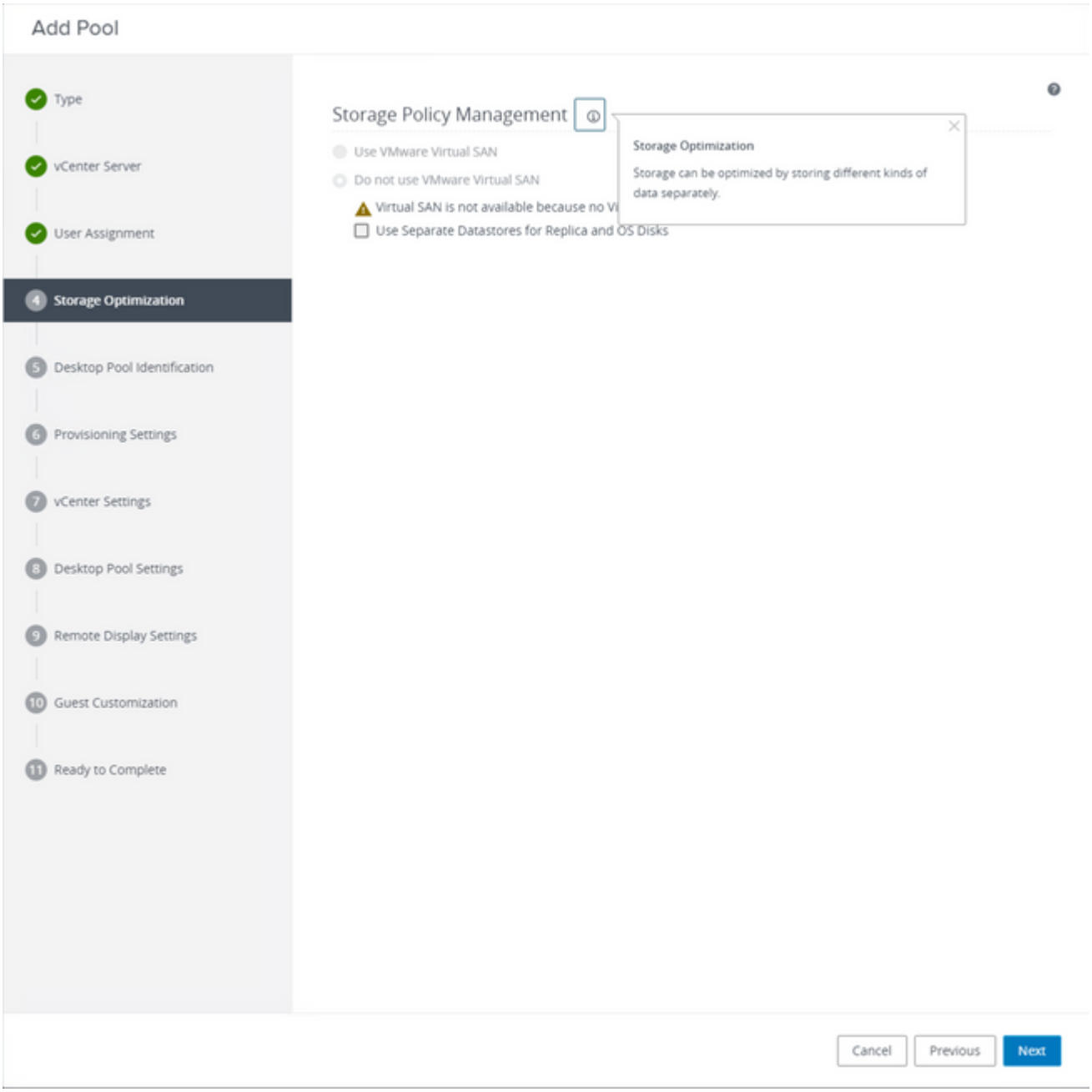
Auswählen von "Instant Clones"

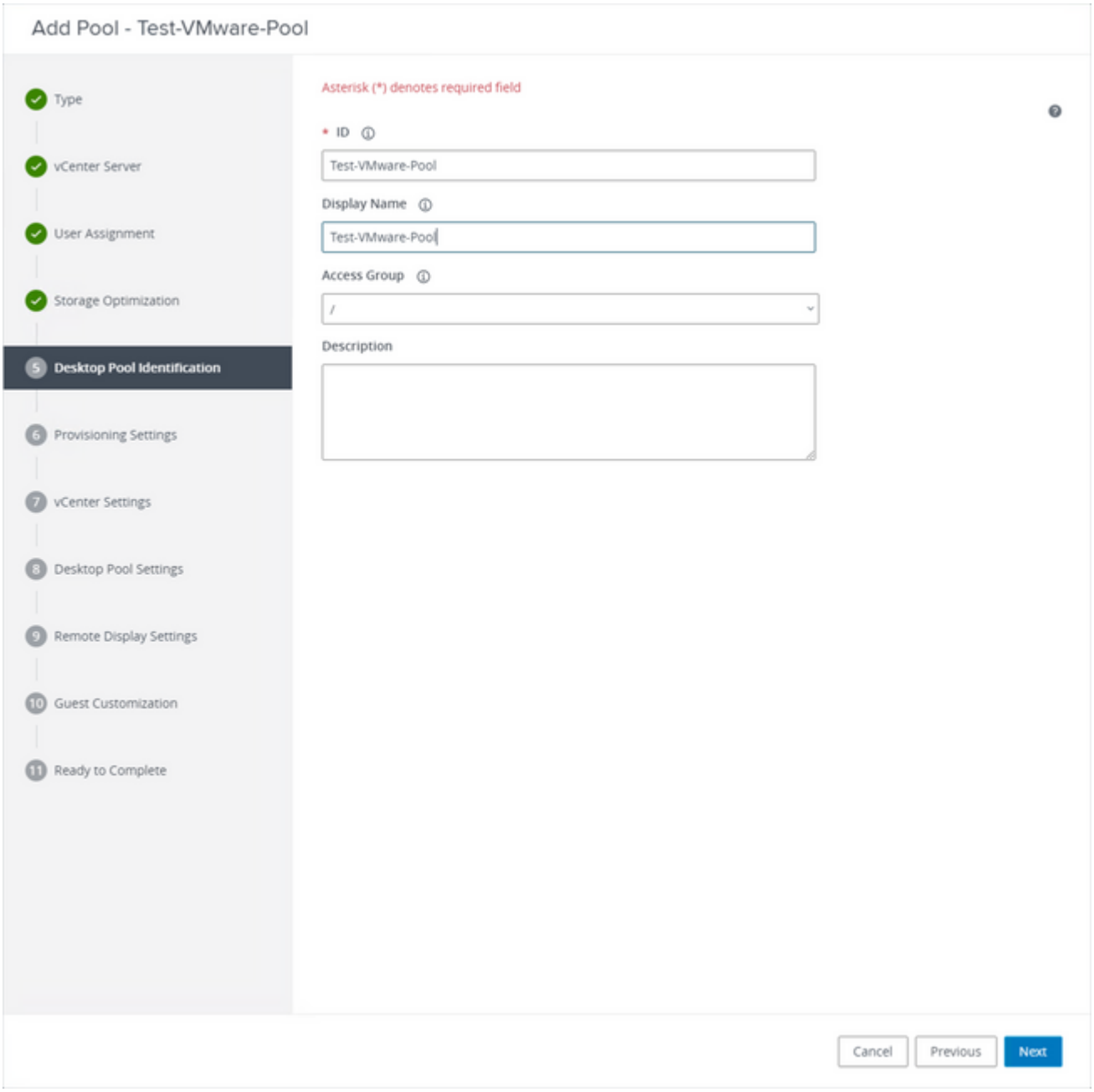
Siehe: https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-D7C0150E-18CE-4012-944D-4E9AF5B28347.html



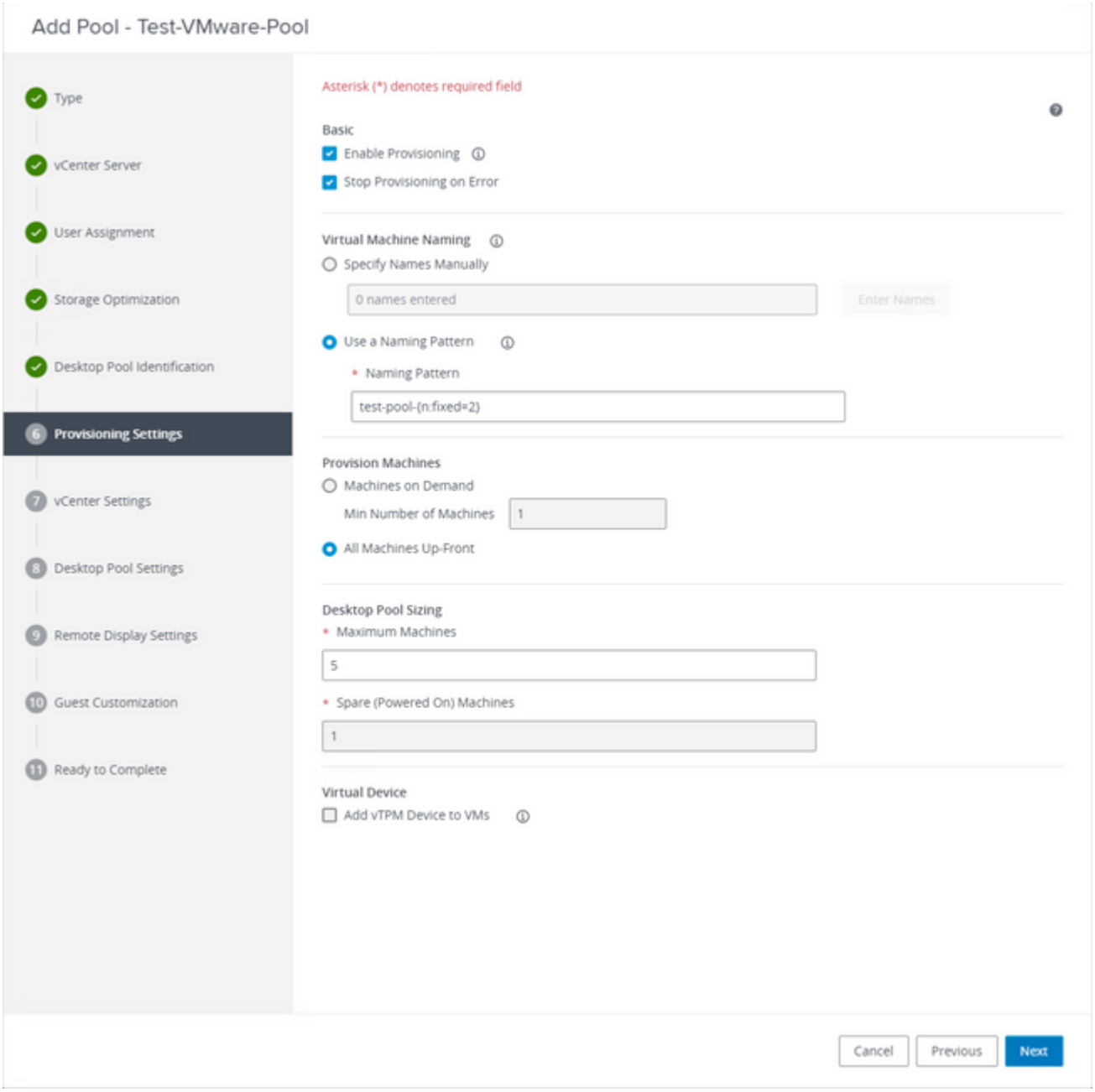
Auswählen des Typs "Floating"

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

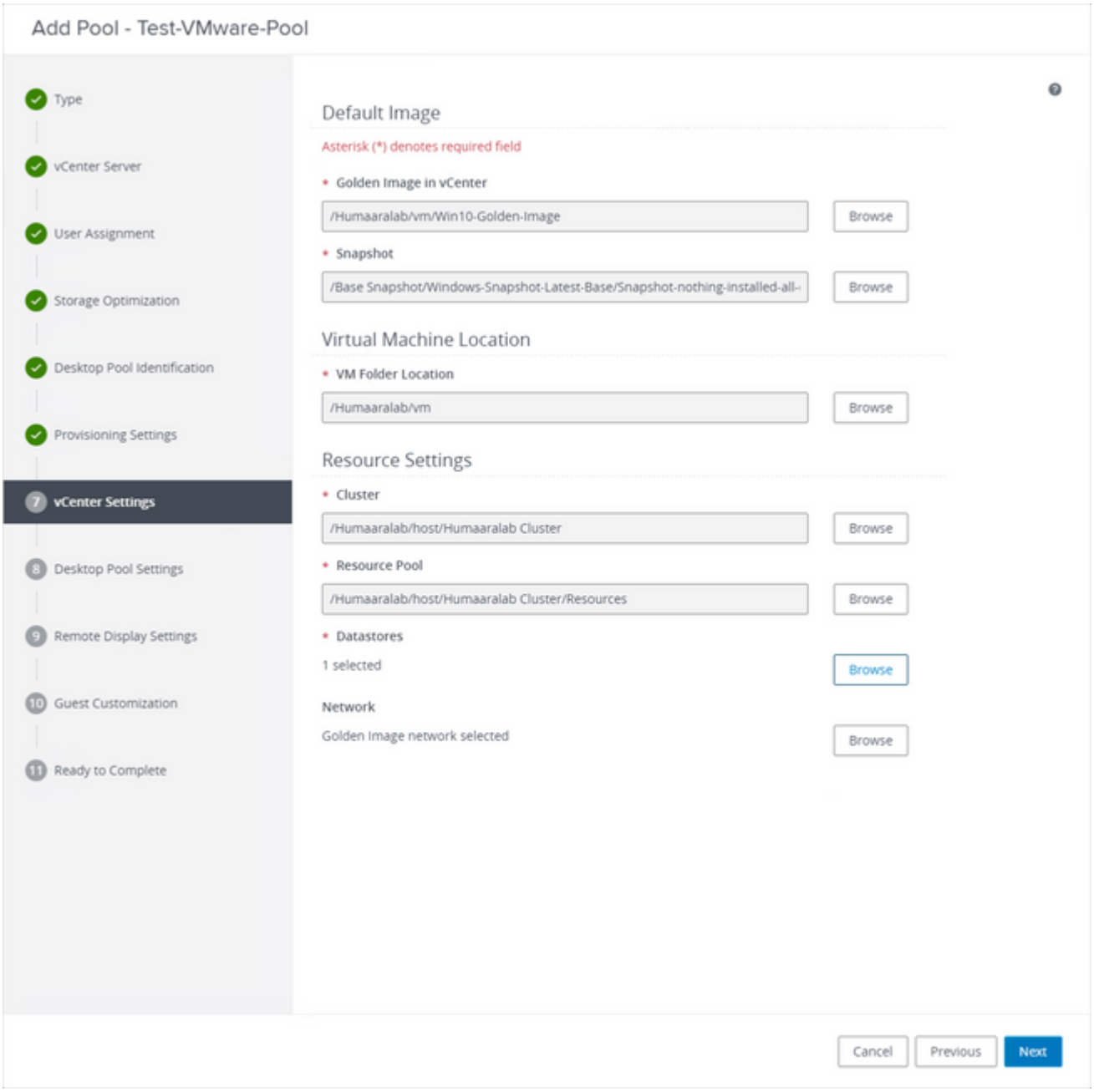

Add Pool
Type
vCenter Server
User Assignment
4 Storage Optimization
5 Desktop Pool Identification
6 Provisioning Settings
7 vCenter Settings
8 Desktop Pool Settings
9 Remote Display Settings
10 Guest Customization
11 Ready to Complete
Storage Policy Management
Use VMware Virtual SAN
Do not use VMware 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 von Desktop-Pools

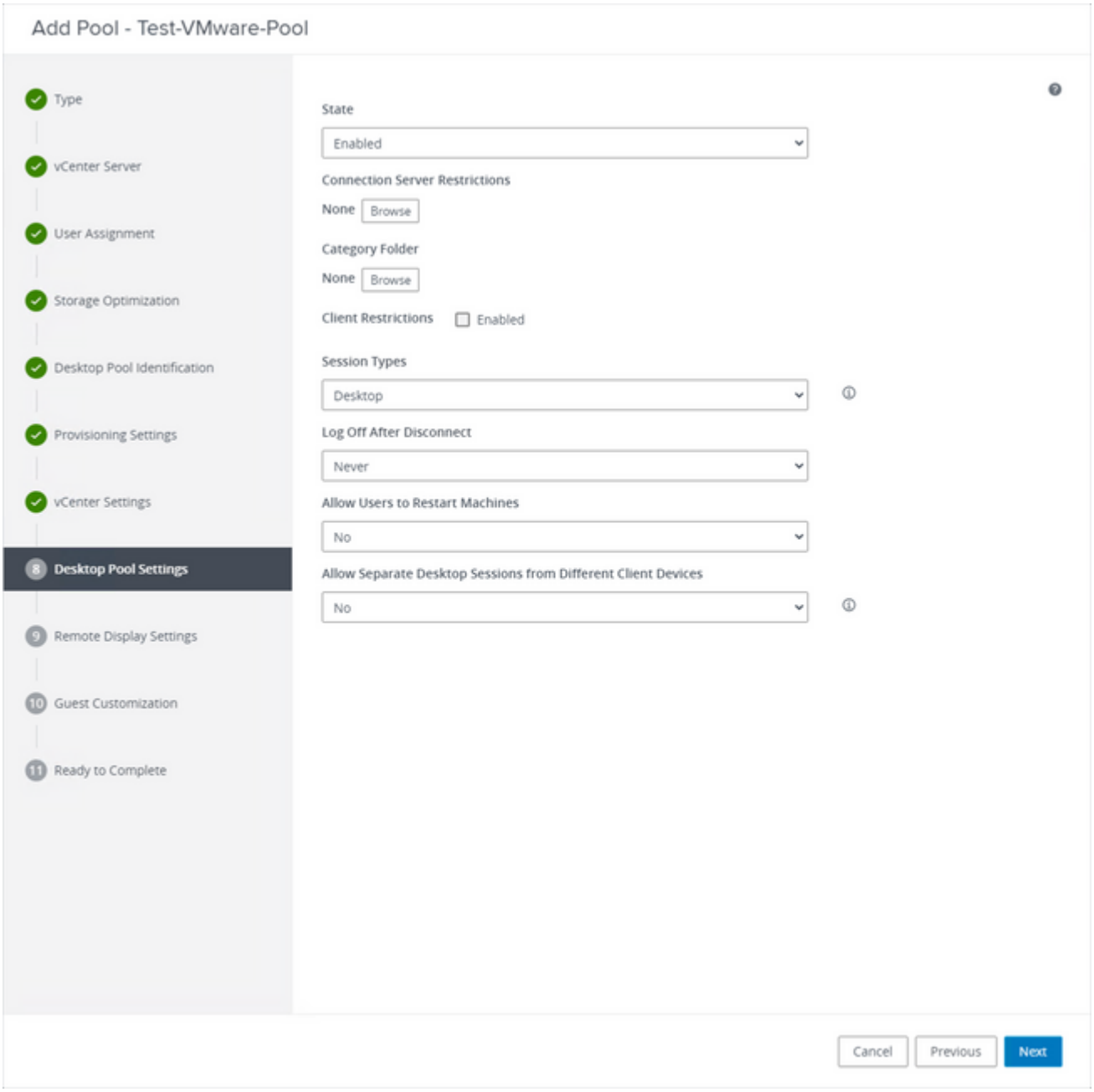


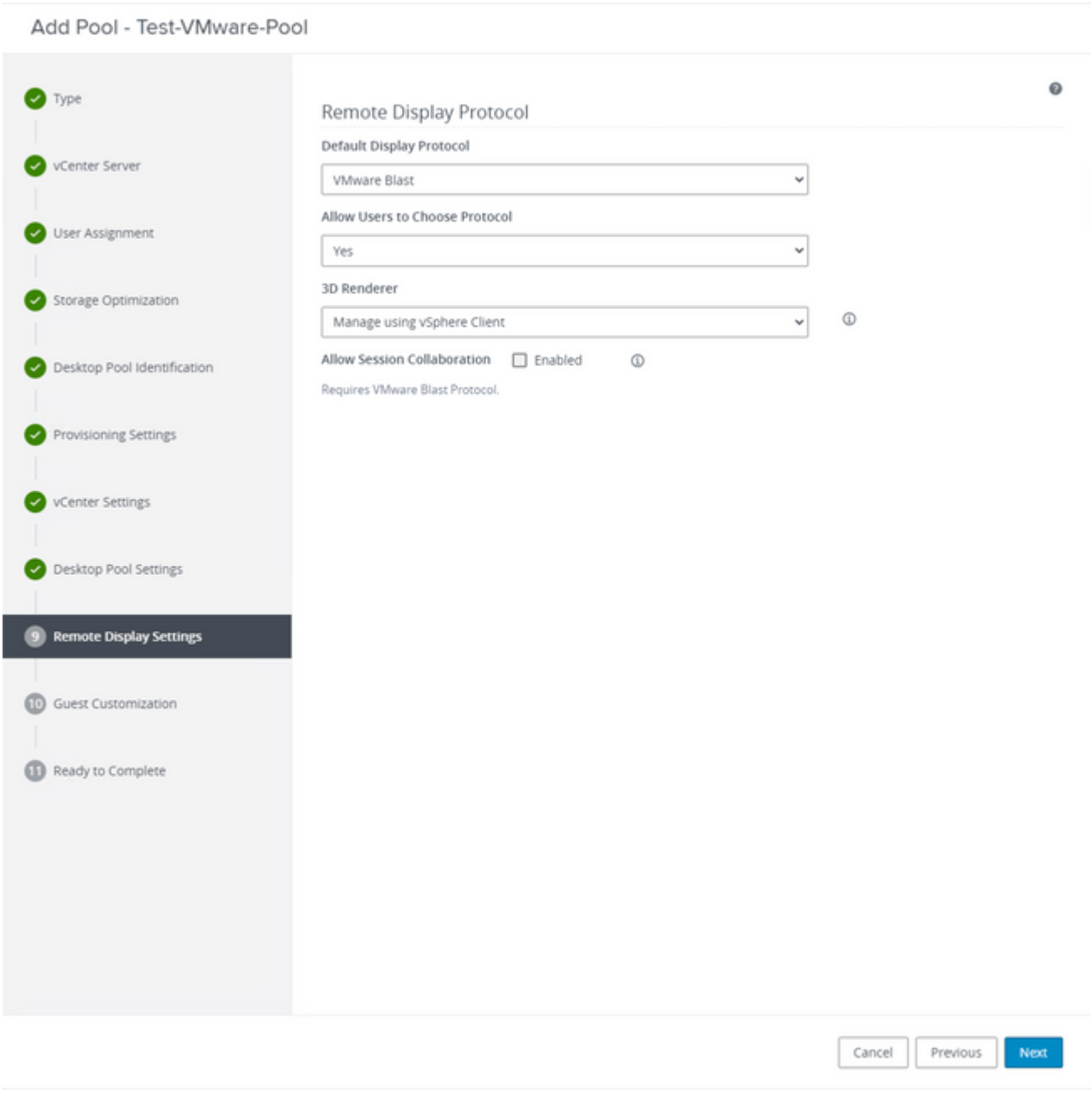
VMware Horizon Naming Pattern: https://docs.vmware.com/en/VMware-Horizon/2103/virtual-desktops/GUID-26AD6C7D-553A-46CB-B8B3-DA3F6958CD9C.html

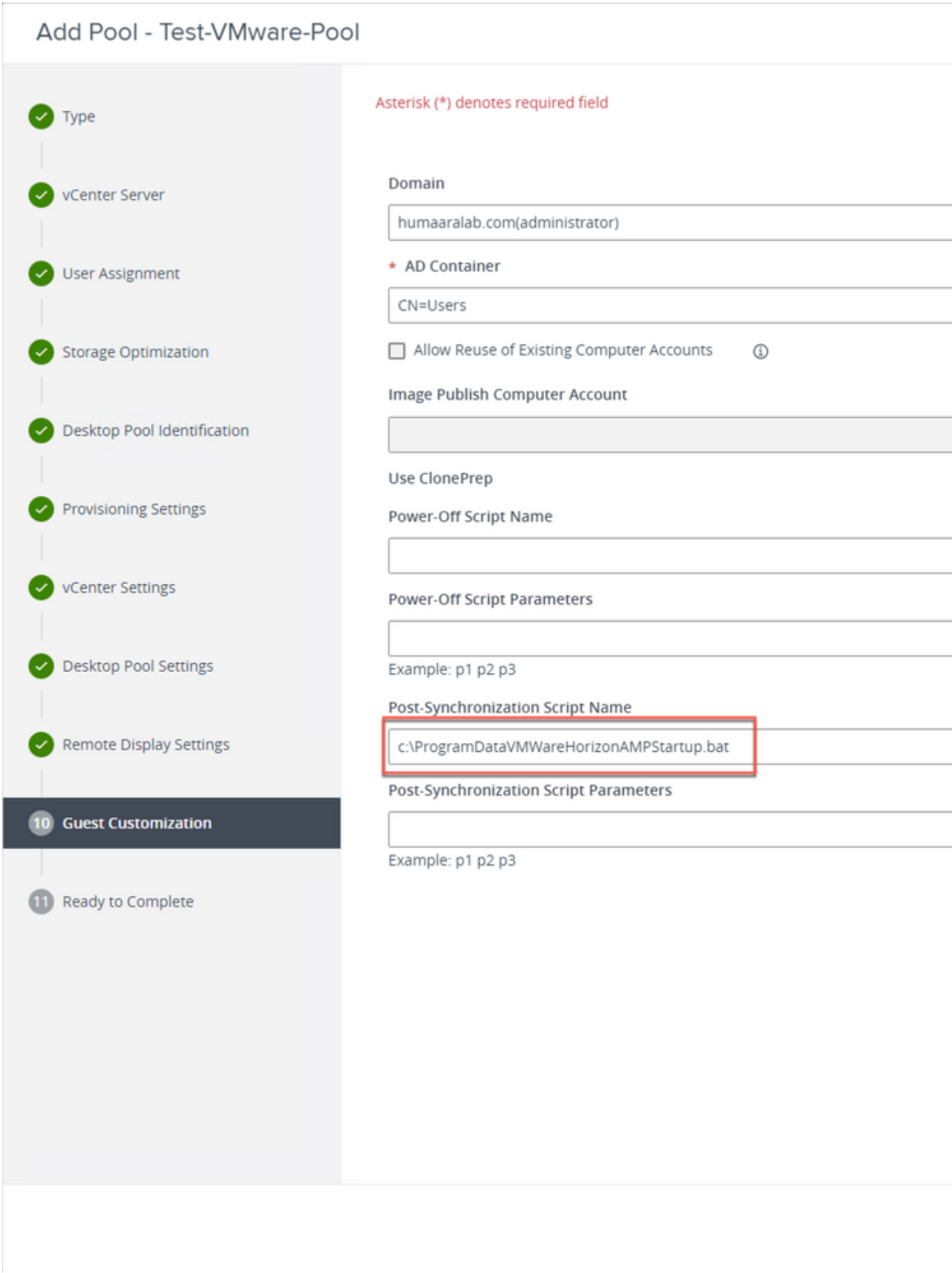


Golden Image: Dies ist die eigentliche Golden Image VM.

Snapshot: Dies ist das Image, das Sie verwenden möchten, um die untergeordnete VM bereitzustellen. Dies ist der Wert, der aktualisiert wird, wenn Sie das Goldene Bild mit Änderungen aktualisieren. Rest sind einige der VMware Environment-spezifischen Einstellungen.


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. Wie bereits erwähnt, wird in Schritt 10. im Assistenten der **Skriptpfad** festgelegt.

: Weitere Informationen zu diesen Schritten finden Sie im VMware-Leitfaden. Diese sind jedoch selbsterklärend.

Übersicht über den Persistenzprozess für Identität

1. Der Connector wird mit einem Token in der Datei policy.xml heruntergeladen, der ihn mit der betreffenden Cloud-Richtlinie verknüpft.
2. Der Connector wird installiert und speichert das Token in local.xml, und der Connector sendet eine POST-Anforderung an das Portal mit dem fraglichen Token.
3. Auf der Cloud-Seite wird diese Reihenfolge durchlaufen:
   antwort: Der Computer überprüft die Richtlinie auf die Konfiguration der ID-Synchronisierungsrichtlinie. Andernfalls erfolgt die Registrierung normal.
   b. Abhängig von den Richtlinieneinstellungen überprüft die Registrierung die vorhandene Datenbank auf den Hostnamen oder die MAC-Adresse.
   Unternehmensübergreifend:Alle Richtlinien werden je nach Einstellung auf Übereinstimmung bei Hostname oder MAC geprüft. Die übereinstimmende Objekt-GUID wird notiert und an den Endclient-Computer zurückgesendet. Der Client-Computer übernimmt dann die UUID und alle Gruppen-/Richtlinieneinstellungen des zuvor zugeordneten Hosts. Damit werden die installierten Richtlinien-/Gruppeneinstellungen überschrieben.
   Richtlinienübergreifend:Das Token stimmt mit der Cloud-Richtlinie überein und sucht innerhalb dieser Richtlinie nur nach einem vorhandenen Objekt mit demselben Hostnamen oder derselben MAC-Adresse. Wenn eine vorhanden ist, wird von der UUID ausgegangen. Wenn kein vorhandenes Objekt mit dieser Richtlinie verknüpft ist, wird ein neues Objekt erstellt. Hinweis: Für denselben Hostnamen, der mit anderen Gruppen/Richtlinien verknüpft ist, können Duplikate vorhanden sein.
   c. Wenn eine Übereinstimmung mit einer Gruppe/Richtlinie aufgrund eines fehlenden Tokens (zuvor registriert, schlechte Bereitstellungspraxis usw.) nicht hergestellt werden kann, fällt der Connector unter die Standardkonnektorgruppe/Richtlinie, die auf der Registerkarte "Business" festgelegt wurde. Basierend auf der Einstellung der Gruppe/Richtlinie wird versucht, alle Richtlinien für eine Übereinstimmung (über das Unternehmen hinweg), nur die betreffende Richtlinie (über die Richtlinie hinweg) oder gar keine (keine) zu überprüfen. In diesem Zusammenhang wird generell empfohlen, die Standardgruppe so zu konfigurieren, dass sie die gewünschten ID-Synchronisierungseinstellungen enthält, damit Computer im Falle eines Tokenproblems ordnungsgemäß zurücksynchronisiert werden können.

Identifizieren von Duplikaten in Ihrer Organisation

Extern verfügbare GitHub-Skripte

Suchen Sie nach doppelten UUIDs: https://github.com/CiscoSecurity/amp-04-find-duplicate-guids

Entfernen Sie veraltete/alte UUIDs: https://github.com/CiscoSecurity/amp-04-delete-stale-guids

Gründe für die Erstellung von Duplikaten

Es gibt einige häufige Fälle, die dazu führen können, dass Duplikate auf Ihrem Ende zu sehen:

1. Wenn diese Schritte während des VDI-Pools ausgeführt wurden:

- Die Erstbereitstellung auf einer nicht persistenten VM/VDI erfolgt mit deaktivierter Identity Persistence (z. B. "Golden Image" verwenden).
- Die Richtlinie wird in der Cloud aktualisiert, sodass Identity Persistence aktiviert wird, wodurch sie tagsüber auf dem Endgerät aktualisiert wird.

- Computer werden aktualisiert/mit einem Image versehen (dasselbe "golden image" verwenden), wodurch die ursprüngliche Richtlinie ohne "Identity Persistence" wieder auf den Endpunkt übertragen wird.
- Die Richtlinie verfügt lokal nicht über Identitätspersistenz, sodass der Registrierungsserver nicht nach vorherigen Datensätzen sucht.
- Dieser Fluss führt zu Duplikaten.

2. Der Benutzer stellt das ursprüngliche Golden Image mit aktivierter Identitätspersistenz in der Richtlinie in einer Gruppe bereit und verschiebt dann einen Endpunkt aus dem Portal für sichere Endpunkte in eine andere Gruppe. Der ursprüngliche Datensatz befindet sich dann in der verschobenen Gruppe, erstellt jedoch neue Kopien in der ursprünglichen Gruppe, wenn die VMs neu erstellt/bereitgestellt werden.

> **Hinweis**: Dies ist keine erschöpfende Liste von Szenarien, die zu Duplikaten führen können, sondern einige der gebräuchlichsten.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.