# Configurar Persistência de Identidade em Ponto de Extremidade Seguro

## Contents



## Introdução

Este documento descreve como examinar o recurso Cisco Secure Endpoint Identity Persistence.

## O que é persistência de identidade?

A Persistência de identidade é um recurso que permite manter um registro de eventos consistente em ambientes virtuais ou quando os computadores são recriados. Você pode vincular um Conector a um endereço MAC ou nome de host para que um novo registro de conector não seja criado toda vez que uma nova sessão virtual for iniciada ou uma imagem do computador for recriada. Esse recurso foi projetado especificamente para ambientes VM e Lab não persistentes e não deve ser ativado para configurações tradicionais de estação de trabalho e servidor.

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso ao portal Cisco Secure Endpoints
- Você precisa entrar em contato com o Cisco TAC para que ele habilite o recurso de persistência de identidade na sua organização.
- A Persistência de Identidade só tem suporte no Sistema Operacional Windows

## Quando Você Precisa De Persistência De Identidade?

A Persistência de identidade é uma funcionalidade em endpoints seguros que ajuda na identificação de endpoints seguros no momento do registro inicial do conector e os compara com entradas conhecidas anteriormente com base em parâmetros de identidade, como endereço MAC ou nome de host para esse conector específico. A implementação desse recurso não só ajuda a manter uma contagem de licenças correta, mas também, e o mais importante, permite o rastreamento adequado de dados históricos em sistemas não persistentes.

### Implantação de endpoint virtual

O uso mais comum da persistência de identidade em implantações virtuais é a implantação da infraestrutura de desktop virtual (VDI) não persistente. Os ambientes de desktop do host VDI são implantados mediante solicitações ou necessidades do usuário final. Isso inclui fornecedores diferentes, como VMware, Citrix, AWS AMI Golden Image Deployment, etc.

O VDI persistente, também chamado de "VDI com informações de estado", é uma configuração em que o desktop de cada usuário individual é exclusivamente personalizável e "persiste" de uma sessão para outra. Esse tipo de Implantação virtual não precisa da funcionalidade da Persistência de identidade, pois essas máquinas não devem ter imagens criadas novamente regularmente.

Como ocorre com todos os softwares que poderiam interagir com o desempenho do Secure Endpoint, os aplicativos de desktop virtual precisam ser avaliados quanto a possíveis exclusões para maximizar a funcionalidade e minimizar o impacto.

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

### Implantação de endpoint físico

Há dois cenários que podem ser aplicados para a implantação da persistência de identidade em máquinas físicas de endpoints seguros:

- Quando você implanta ou recria um endpoint físico com uma imagem dourada com o conector Secure Endpoint pré-instalado, o Sinalizador Goldenimage deve ser ativado. A persistência de identidade pode ser usada para evitar duplicação em instâncias de máquinas com nova imagem, mas não é necessária.

- Quando você implanta ou recria um endpoint físico com uma imagem de ouro e instala posteriormente o conector Secure Endpoint, a Persistência de identidade pode ser usada para evitar duplicação em instâncias de máquinas com nova imagem, mas não é necessária.

# Problemas comuns/sintomas com implantação de persistência de identidade incorreta

A implementação incorreta da persistência de identidade pode causar estes problemas/sintomas:

- Contagem de assento do conector incorreta
- Resultados Incorretos Relatados
- Incompatibilidade de dados da trajetória do dispositivo
- Trocas de nome de máquina dentro dos logs de auditoria
- Os conectores registram e cancelam o registro aleatoriamente do console

- Os conectores não se reportam corretamente à nuvem
- Duplicação de UUID
- Duplicação do nome da máquina
- Inconsistência de dados
- As máquinas são registradas na política/grupo comercial padrão após a recomposição

- Implantação manual com a Persistência de identidade habilitada na política.

- Se você implantar o ponto de extremidade manualmente por meio da opção de linha de comando com a Persistência de Identidade já habilitada na política e, em seguida, desinstalar o ponto de extremidade e tentar reinstalar com o pacote de um Grupo/Política diferente, o ponto de extremidade voltará automaticamente para a política original.

- Saída de logs SFC mostrando que o switch de política está ativado sozinho em 1-10seg

```
(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
```

O outro efeito colateral é tentar instalar um conector que pertence a um grupo diferente. Você verá no portal que o conector está atribuído ao grupo correto, mas com a política **"errada"** original

Isso se deve ao fato de como a persistência de identidade (ID SYNC) funciona.

Sem ID SYNC uma vez que o conector é completamente desinstalado ou usando a opção de linha de comando de registro novamente. Você deve ver a nova Data de criação e o GUID do conector em caso de desinstalação ou apenas o novo GUID do conector em caso de comando de novo registro. No entanto, com a

ID SYNC, não é possível que a ID SYNC seja substituída pela antiga GUID e DATE. É assim que "sincronizamos" o host.

Se esse problema for observado, a correção deverá ser implementada por meio da alteração de política. Você precisará mover os pontos de extremidade afetados de volta para o Grupo/Política original e verificar se a política está sincronizada. Em seguida, mova o(s) endpoint(s) de volta para o Grupo/Política desejado

# Práticas recomendadas de implantação

## Configurar arquivo snapvol

Caso você use Volumes de Aplicativos para sua Infraestrutura de VDI, é recomendável fazer essas alterações de configuração na configuração do **snapvol.cfg**

Essas exclusões devem ser implementadas no **arquivo snapvol.cfg**:

Caminhos:

- 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

Chaves do Registro:

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

Em sistemas x64, adicione estes:

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

Referências:

- 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

## Criação de imagem dourada

Siga as diretrizes de práticas recomendadas do documento do Fornecedor (VMware, Citrix, AWS, Azure e assim por diante) ao criar uma Imagem Dourada a ser usada no processo de Clonagem de VDI.

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

Como você identificou o VMware, o processo de composição do AWS reinicia o Clonado (VMs filho) várias vezes antes da finalização da configuração da VM, o que causa problemas com o processo de registro do Secure Endpoint, pois nesse momento o Clonado (VMs filho) não tem os nomes de host finais/corretos atribuídos e isso faz com que o Clonado (VMs filho) use o nome de host Golden Image e registre na Secure Endpoint Cloud. Isso interrompe o processo de clonagem e pode causar problemas.

Isso não é um problema com o processo do conector de endpoint seguro, mas sim com a incompatibilidade com o processo de clonagem e o registro de endpoint seguro. Para evitar esse problema, identificamos algumas alterações a serem implementadas no processo de clonagem que ajudam a resolver esses problemas.

Essas são as alterações que precisam ser implementadas na VM Golden Image antes que a imagem seja congelada para clonagem

1. Use sempre o indicador **Goldenimage** na Imagem Dourada no momento da instalação do Ponto Final Seguro.

2. Implementar scripts que ajudam a ATIVAR o serviço de Ponto de Extremidade somente quando tivermos um nome de host final implementado nas VMs Clonadas (Filhas). Consulte a seção Problemas de Duplicação do VMware Horizon para obter mais detalhes.

### Sinalizador de Substituição de Imagem Dourada

Quando você usa o instalador, o sinalizador a ser usado para imagens douradas é **/goldenimage 1**.

O flag de imagem de ouro impede que o conector seja iniciado e registrado na imagem base e, assim, no próximo início da imagem, o conector estará no estado funcional em que foi configurado pela política atribuída a ele.

Para obter informações sobre outros Sinalizadores, você pode usar o, consulte este artigo.

Instale o como uma imagem dourada. Essa é a opção típica usada com o sinalizador e é o único uso esperado. Ignora o registro inicial do Conector e a Inicialização na instalação.

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

### Etapas da criação da imagem dourada

É uma prática recomendada instalar o conector por último para a preparação da **Imagem Dourada**.

1. Prepare a imagem do Windows de acordo com os seus requisitos; instale todos os softwares e configurações necessários para a imagem do Windows, exceto o conector.
2. Instale o conector Cisco Secure Endpoint.
3. Use o sinalizador/**goldenimage 1** para indicar ao instalador que esta é uma implantação de imagem

dourada.

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

4. Implemente a lógica do script (se necessário) conforme descrito aqui.
5. Conclua a instalação.
6. Congele sua imagem dourada.

Depois que a Golden Image tiver aplicativos instalados, o sistema preparado e o Secure Endpoint tiver sido instalado com o sinalizador/goldenimageflag, o host estará pronto para ser congelado e distribuído. Depois que o host clonado é inicializado, o Secure Endpoint é iniciado e registrado na nuvem. Nenhuma outra ação é necessária com relação à configuração do conector, a menos que haja alterações que você queira fazer na política ou no host. Se forem feitas alterações após a conclusão do registro da imagem de ouro, esse processo deverá ser reiniciado.

### Planejamento de política do portal

Estas são algumas das práticas recomendadas que devem ser seguidas ao implementar a persistência de identidade no Secure Endpoint Portal:

1. É altamente recomendável usar políticas/grupos separados para endpoints com Persistência de Identidade habilitada para segregação mais fácil.

2. Se você planeja usar o Isolamento de Ponto Final e implementar a ação **Mover Computador para Grupo mediante comprometimento**. O grupo de destino também deve ter a Persistência de identidade habilitada e deve ser usado somente para computadores VDI.

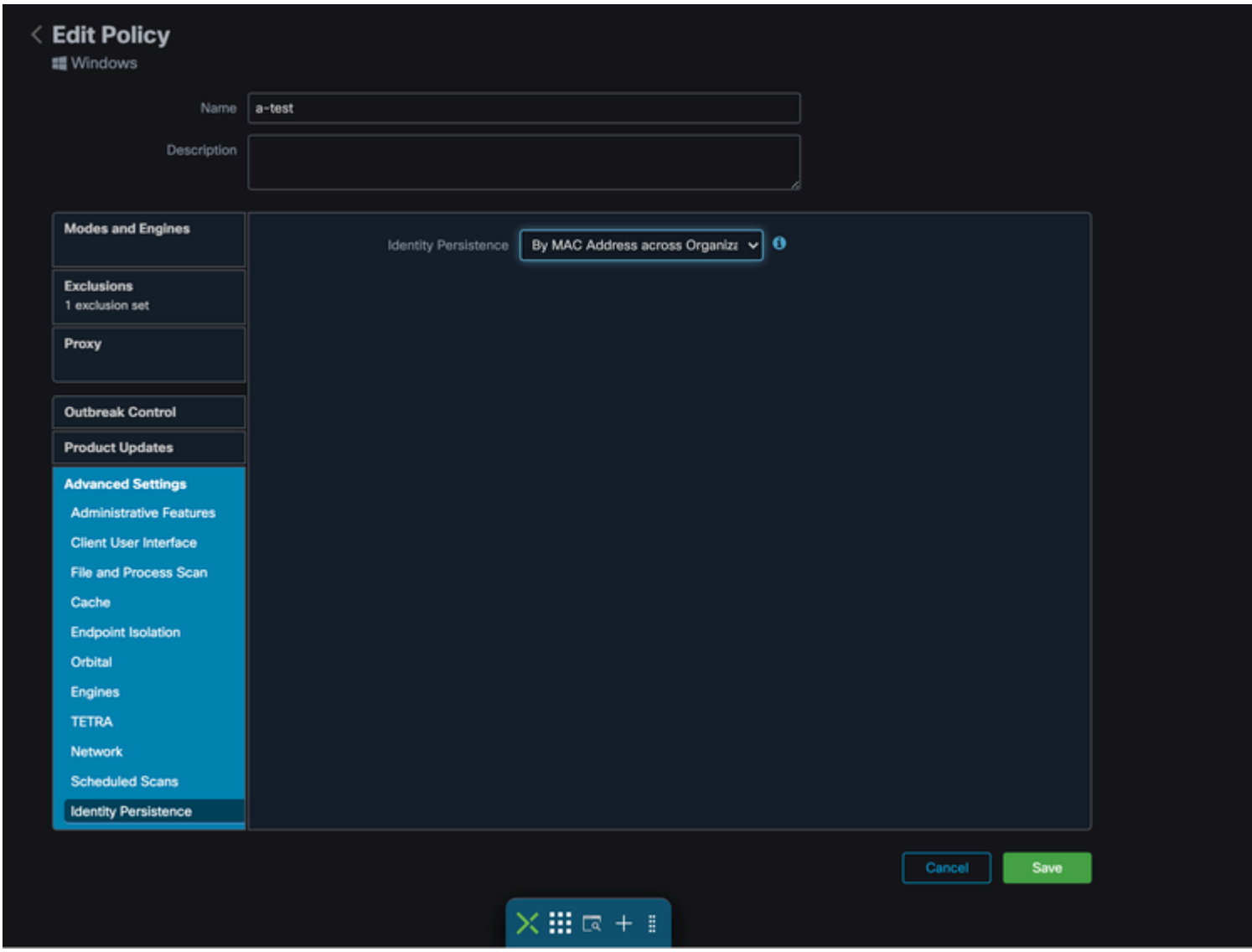
3. Não é recomendável habilitar a **Persistência de Identidade** no Grupo/Política Padrão nas configurações da organização, a menos que a Persistência de Identidade tenha sido habilitada em Todas as políticas com o escopo de configurações em Toda a Organização.

## Configuração

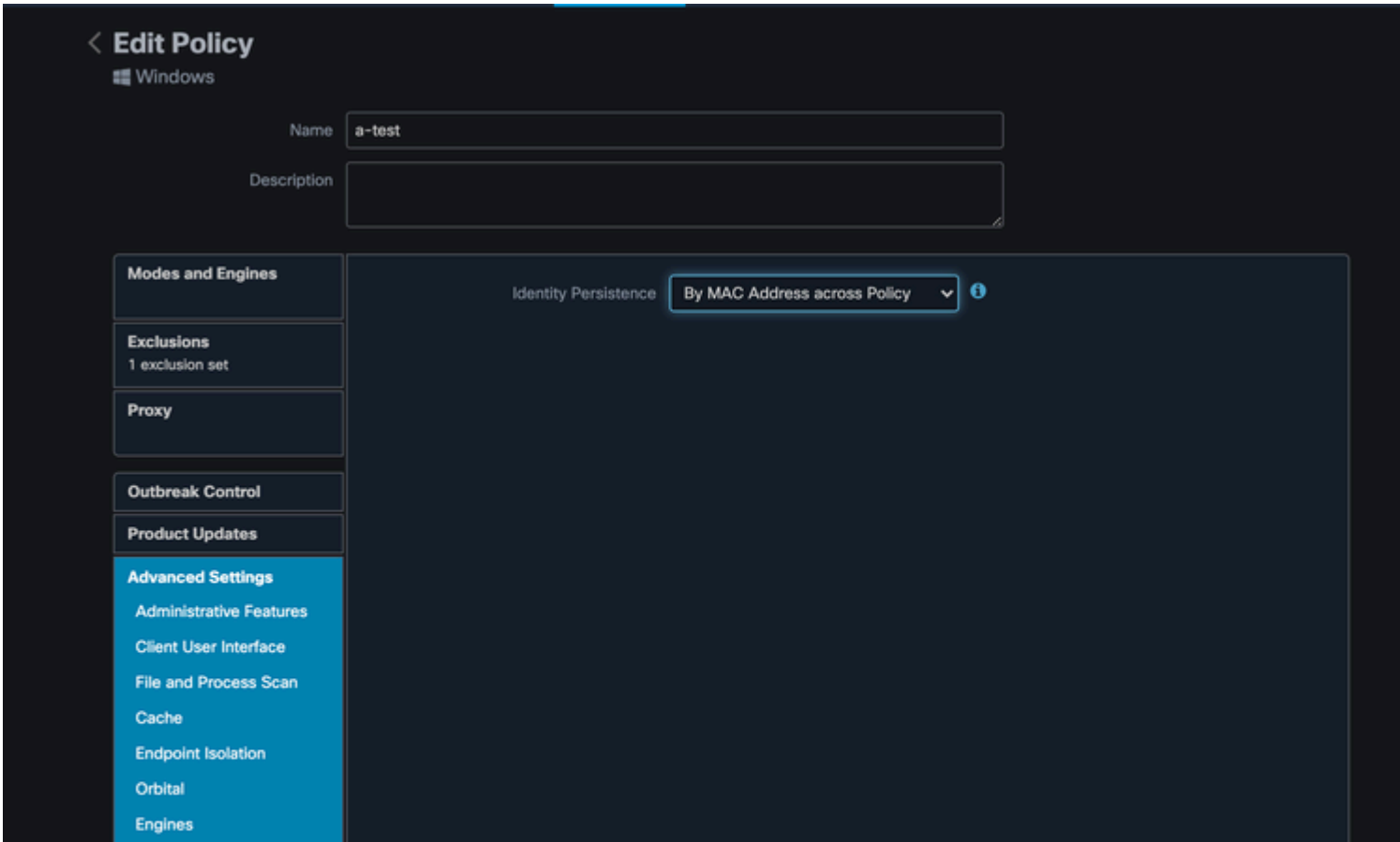
Siga estas etapas para implantar o conector de Ponto Final Seguro com Persistência de Identidade:

Etapa 1. Aplique a definição de Persistência de Identidade desejada às suas políticas:

- No portal Secure Endpoint, navegue até **Management > Policies**.
- Selecione a política desejada na qual deseja habilitar a Persistência de identidade e **clique emEditar**.
- Navegue até **a guiaConfigurações avançadas** e clique na guia **Persistência de identidade** na parte inferior.
- Selecione a lista suspensa Persistência de identidade e escolha a opção que faça mais sentido para o seu ambiente. Consulte esta imagem.


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

*Teste - 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

- Por endereço MAC na empresa: instalações novas ou atualizadas buscam o registro de conector mais recente que tenha o mesmo endereço MAC para sincronizar dados históricos anteriores com o novo registro. Esta configuração examina todos os registros comerciais

  em todas as políticas na organização que têm a Sincronização de Identidade definida com um valor diferente de Nenhum. O Conector pode atualizar sua política para refletir a instalação anterior se ela for diferente da nova.

- Por endereço MAC na política: instalações novas ou atualizadas buscam o registro de conector mais recente que tenha o mesmo endereço MAC para sincronizar dados históricos anteriores com o novo registro. Essa configuração procura apenas os registros associados à política usada na implantação. Se o Conector não tiver sido instalado anteriormente nesta diretiva, mas tiver estado ativo anteriormente em outra diretiva, ele poderá criar duplicatas.
- Por nome de host entre empresas: instalações novas ou atualizadas procuram o registro de conector mais recente que tenha o mesmo nome de host para sincronizar dados históricos anteriores com o novo registro. Essa configuração procura todos os registros de negócios, independentemente das configurações de Persistência de Identidade em outras políticas, e o Conector pode atualizar sua política para refletir a instalação anterior se ela for diferente da nova. O nome de host inclui o FQDN para que possam ocorrer duplicatas se o conector se mover regularmente entre as redes (como um laptop).
- Por nome de host na política: instalações novas ou atualizadas procuram o registro de conector mais recente que tem o mesmo nome de host para sincronizar dados históricos anteriores com o novo registro. Essa configuração procura apenas os registros associados à política usada para a implantação. Se o Conector não tiver sido instalado anteriormente nesta diretiva, mas tiver estado ativo anteriormente em outra diretiva, ele poderá criar duplicatas. O nome de host inclui o FQDN, de modo que as duplicatas também podem ocorrer se o conector se mover regularmente entre as redes (como um laptop).

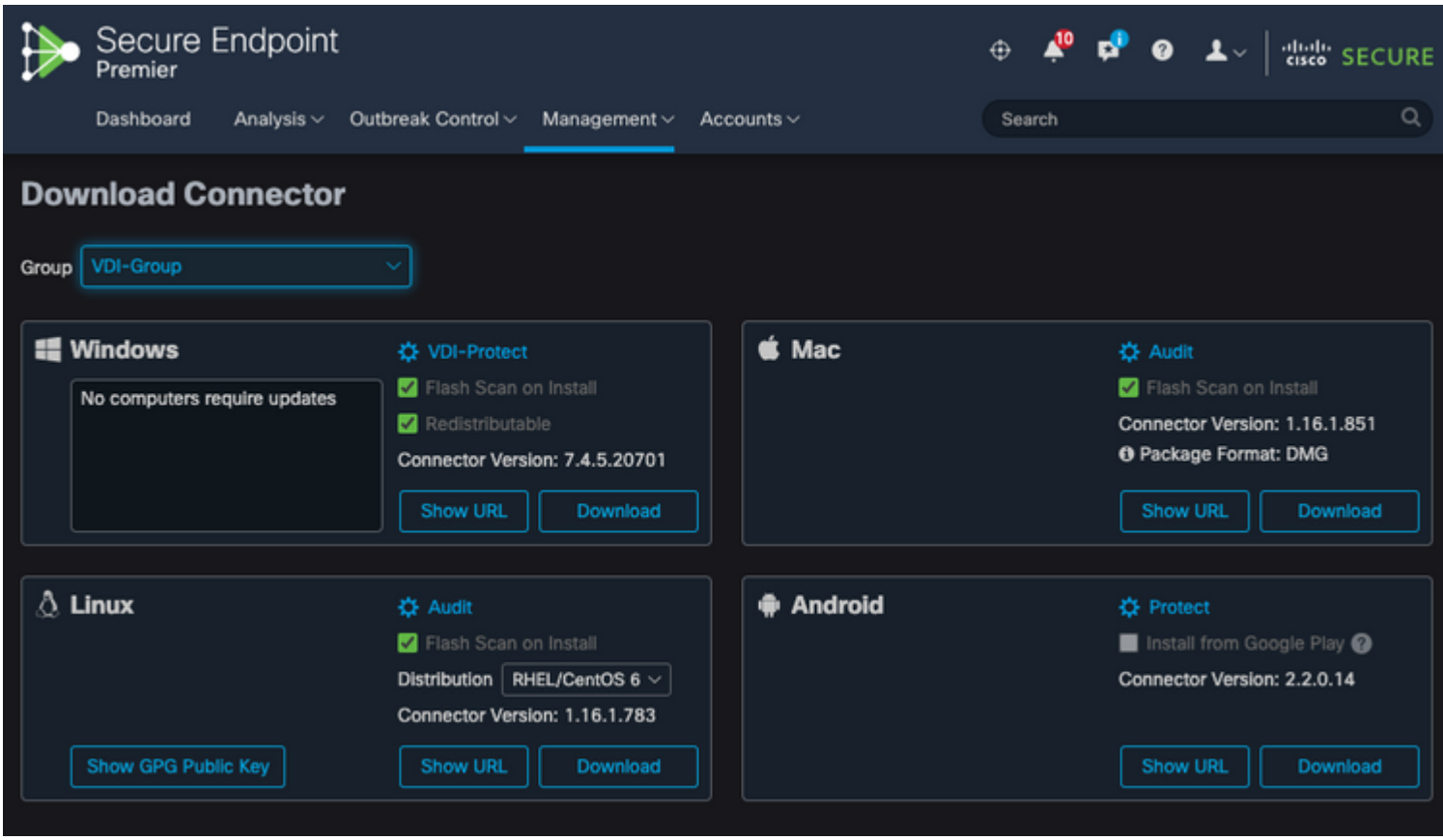
---

**Observação**: se você optar por usar a Persistência de identidade, a Cisco sugere que você use **Por nome de host na empresa ou na política**. Uma máquina tem um nome de host, mas pode ter mais de um endereço MAC e muitas VMs clonam os endereços MAC.

---

Etapa 2. Baixe o conector de endpoint seguro.

- Navegue **para Gerenciamento > Conector de Download**.
- Selecione o grupo para a política editada na Etapa 1.
- **Clique em Download** para o Conector do Windows conforme mostrado na imagem.




Etapa 3. Implante o Conector nos endpoints.

- Agora você pode usar o conector baixado para instalar o Secure Endpoint (com a Persistência de identidade agora habilitada) manualmente em seus endpoints.
- Caso contrário, você também pode implantar o conector usando uma imagem dourada (consulte a imagem)

---

**Observação**: você precisa selecionar o instalador redistribuível. Esse é um arquivo de ~57 MB (o tamanho pode variar com as versões mais recentes) que contém os instaladores de 32 e 64 bits. Para instalar o conector em vários computadores, você pode colocar esse arquivo em um compartilhamento de rede ou enviá-lo para todos os computadores de acordo. O instalador contém um arquivo policy.xml que é usado como arquivo de configuração para a instalação.

---

# Problemas de duplicação do VMware Horizon

Com o VMware Horizon, pudemos identificar que as máquinas VMs filhas, quando estão sendo criadas, são reinicializadas várias vezes como parte do processo de composição do Horizon. Isso causa problemas, pois os serviços de Ponto de Extremidade Seguro são habilitados quando as VMs Filho não estão prontas (elas não têm o Nome NetBios final/correto atribuído). Isso causa mais problemas com o Secure Endpoint sendo confundido e, portanto, o processo é interrompido. Após uma investigação mais aprofundada, a equipe de engenharia apresentou uma solução para essa incompatibilidade com o Horizon Process, que envolve a implementação dos scripts anexados na Golden Image VM e o uso da funcionalidade de script pós-sincronização para o 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)

Isso provavelmente seria o problema de qualquer outro fornecedor, como Citrix, AWS e assim por diante, e, portanto, essa solução também pode funcionar para eles.

## Configurações/alterações não mais necessárias

- Não será mais necessário desinstalar e reinstalar o Secure Endpoint se você quiser fazer alterações na Golden Image após a primeira implantação.
- Não há necessidade de definir o Secure Endpoint Service como **Delayed Start**.

## Metodologia de script

Aqui estão os scripts de exemplo que podem ser usados.

- **VMWareHorizonAMPSetup.bat:** este script deve ser implementado assim que o AMP for instalado, conforme descrito anteriormente com os sinalizadores documentados anteriormente. Este script modificou o serviço Secure Endpoint para Início manual e salva o nome de host Golden Image como uma Variável de ambiente para referência na próxima etapa.

```
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:** Este script é uma verificação lógica em que combinamos o nome de host nas VMs Clonadas (Filhas) com o armazenado na etapa anterior para garantir que identificamos quando a VM Clonada (Filha) recebe um nome de host que seja qualquer coisa diferente da VM Golden Image (que seria o nome de host final para a máquina) e, em seguida, você inicia o Secure Endpoint Service e o altera para Automático. Você também remove a Variável de ambiente do script mencionado anteriormente. Isso normalmente é implementado com o uso dos mecanismos disponíveis na solução de implantação, como o VMware. No VMware, você pode usar os parâmetros de pós-sincronização: https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-E177899E-023D-4E61-B058-AFE3822158AA.html Da mesma forma para o AWS, você pode usar os Scripts de inicialização da mesma maneira: 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
```

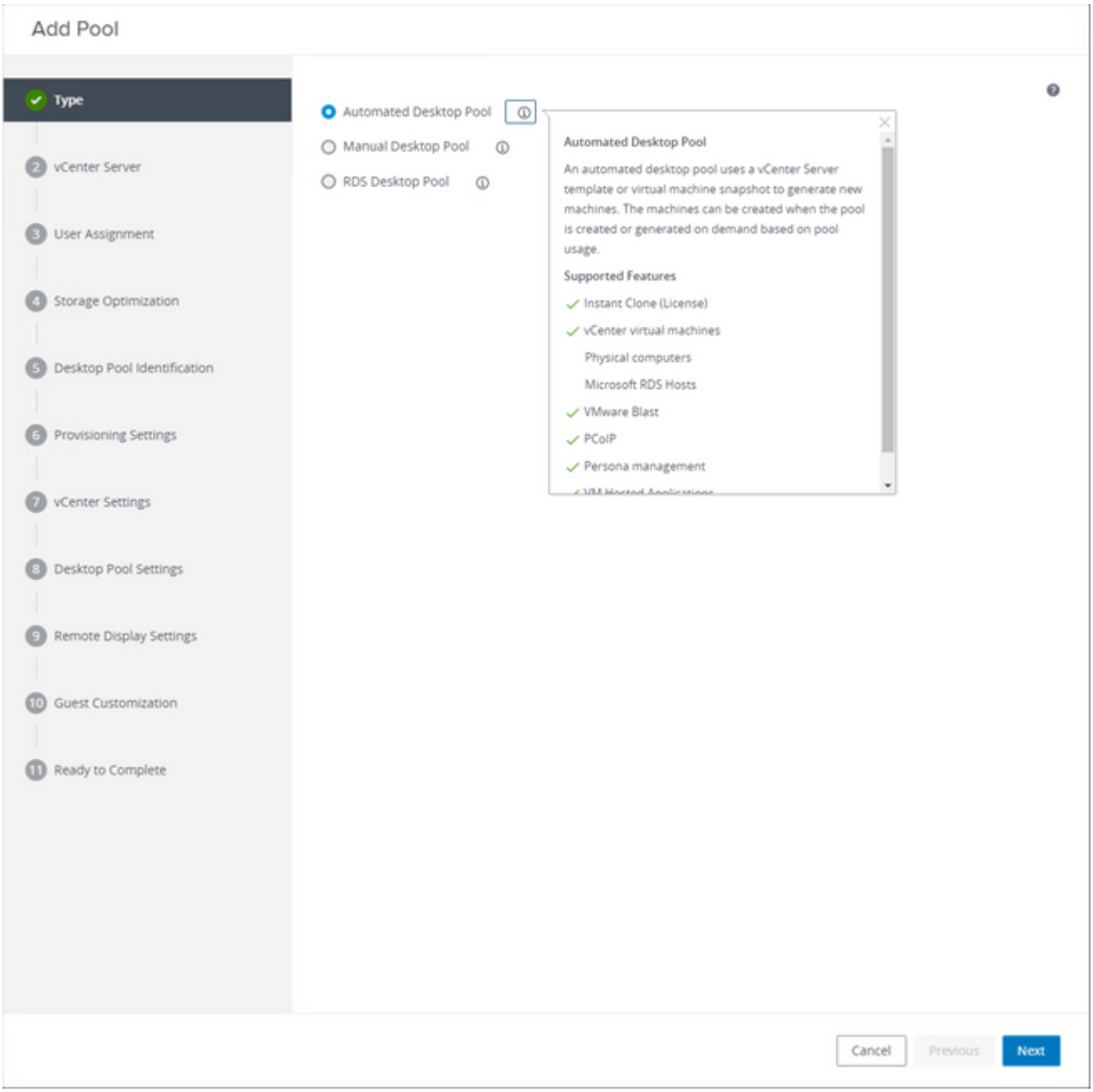
---

**Observação**: observe que os scripts contidos neste documento não são oficialmente suportados pelo TAC

---

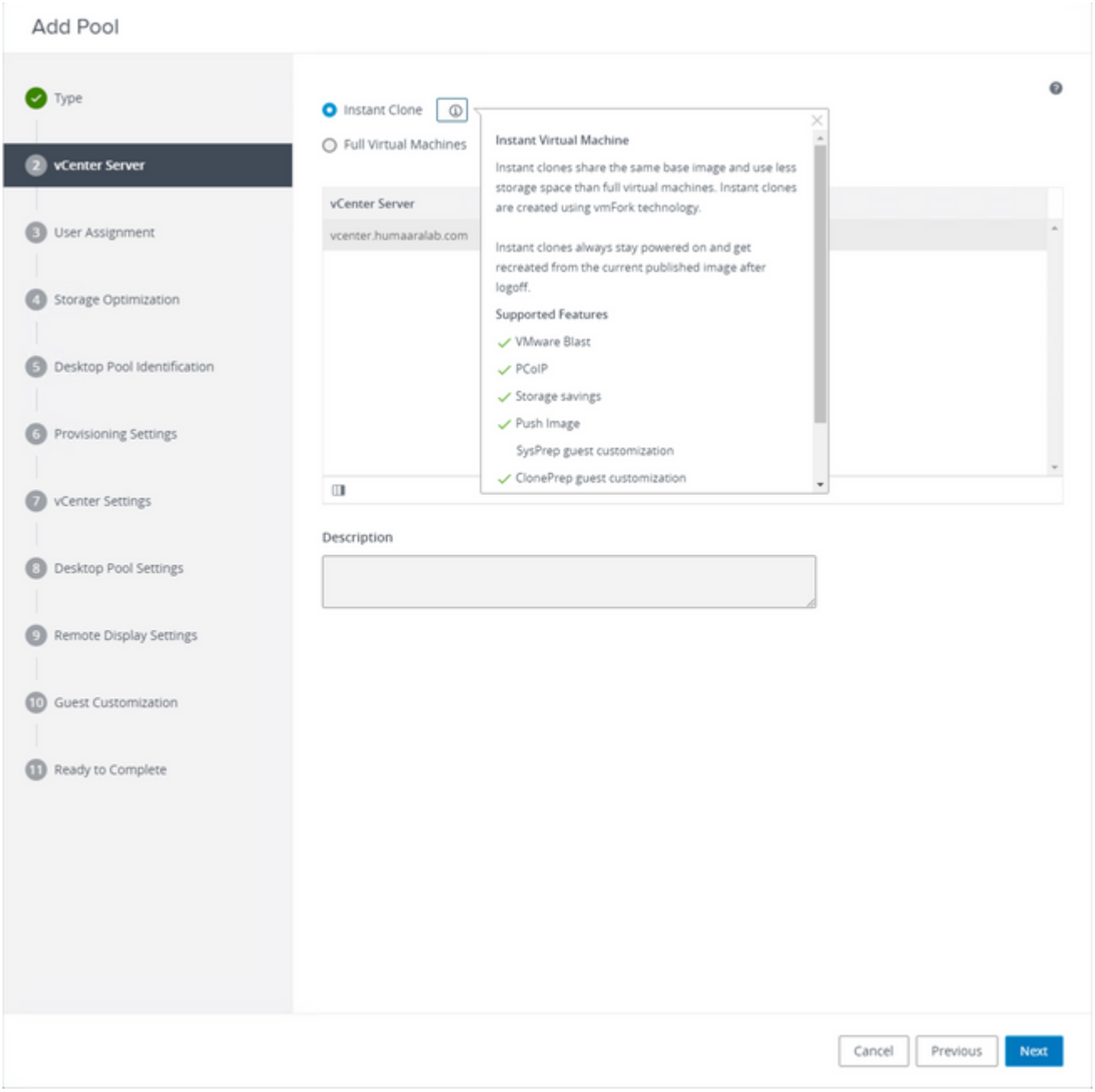
# Configuração do VMware Horizon

1. A VM Golden Image é preparada e todos os aplicativos necessários para a implantação inicial do pool são instalados na VM.
2. O Secure Endpoint é instalado com essa Sintaxe de Linha de Comando para incluir a Flag goldenimage. Por exemplo, **<ampinstaller.exe> /R /S /goldenimage 1**.Observe que o Sinalizador Golden Image garante que o serviço Secure Endpoint não seja executado até uma reinicialização, o que é crítico para que esse processo funcione corretamente. Consulte https://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-endpoints/118587-technote-fireamp-00.html
3. Após a instalação do Secure Endpoint, execute o script **VMWareHorizonAMPSetup.bat** na máquina virtual Golden Image primeiro. Essencialmente, esse script altera o Serviço AMP para **Início manual** e cria uma Variável de ambiente que armazena o nome de host Golden Image para uso posterior.
4. Você precisa copiar o **VMWareHorizonAMPStartup.bat** para um caminho universal na máquina virtual Golden Image como "**C:\ProgramData"** pois isso seria usado nas etapas posteriores.
5. A Golden Image VM agora pode ser desativada e o processo de composição pode ser iniciado no VMware Horizon.
6. Estas são as informações passo a passo sobre sua aparência do ponto de vista do VMware Horizon:



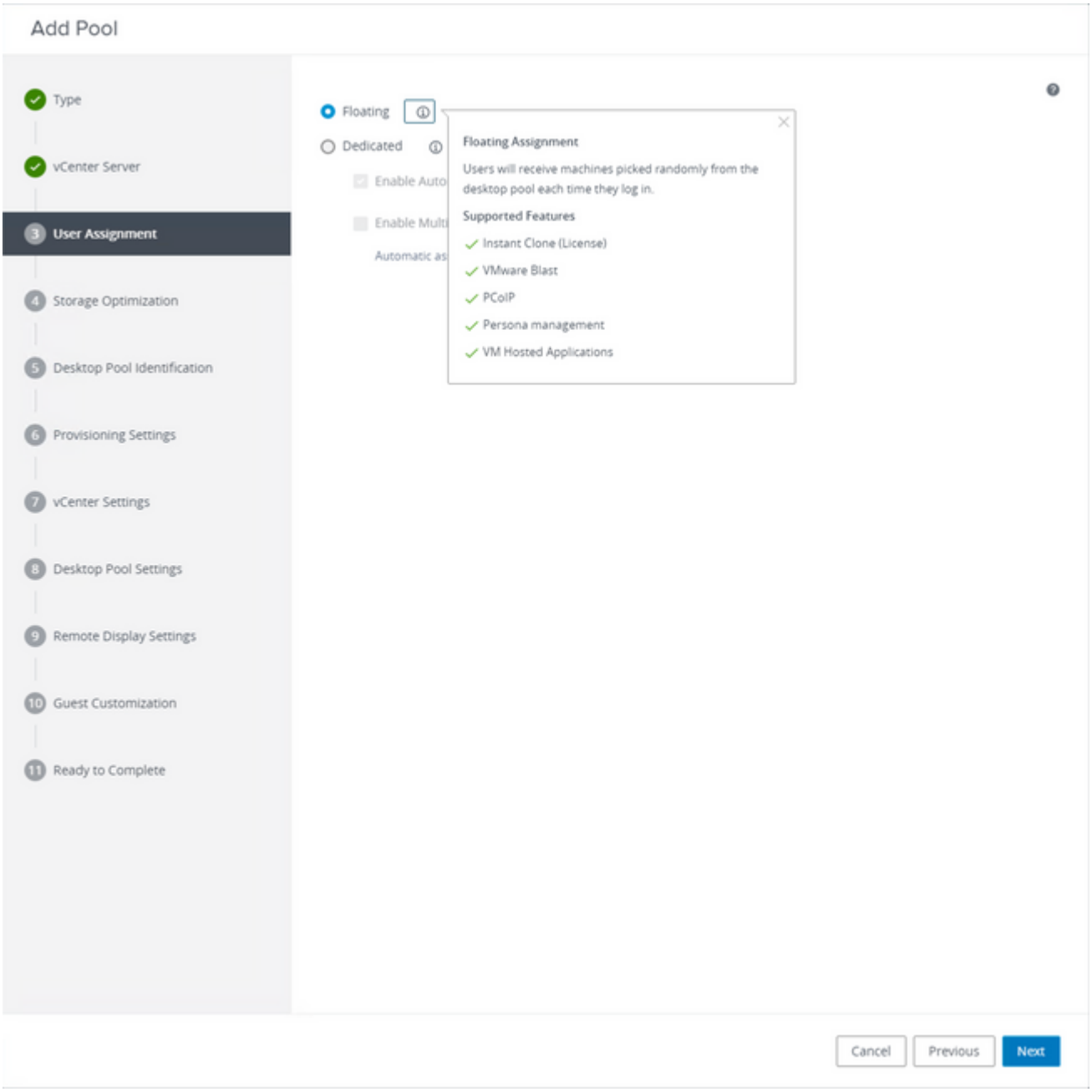

*Selecionando "Pool de desktops automatizado"*

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



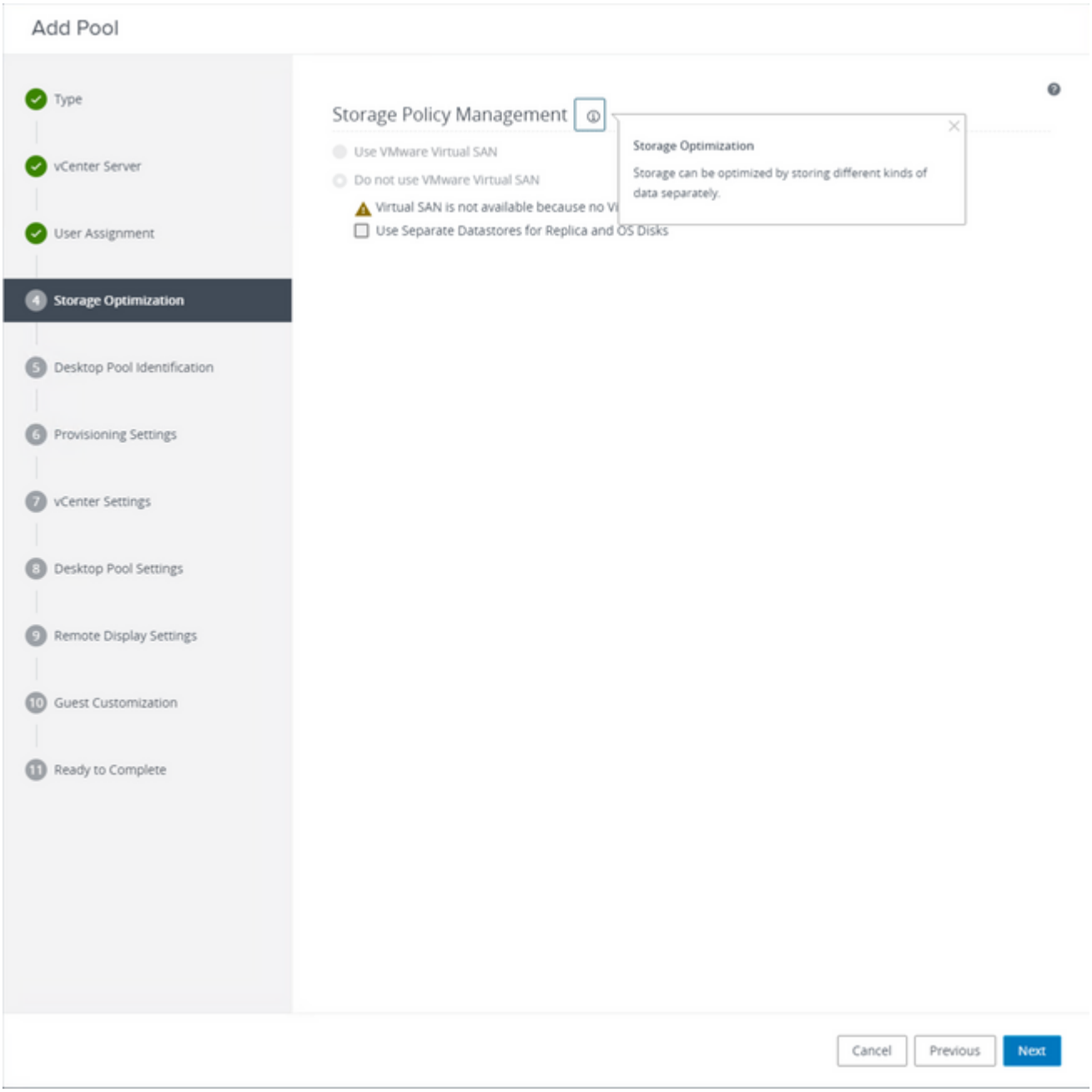

*Seleção de "clones instantâneos"*

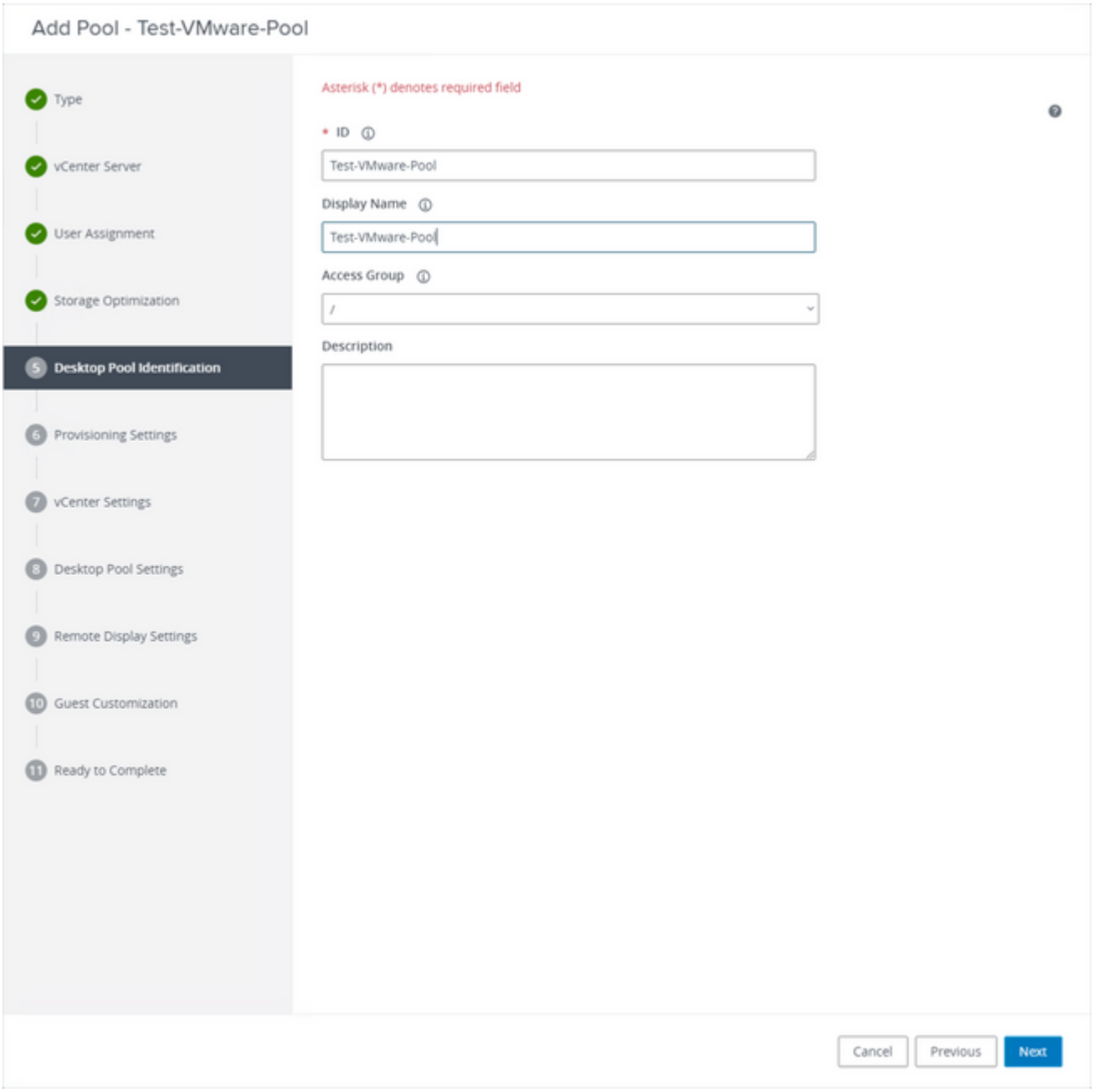
Consulte: https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-D7C0150E-18CE-4012-944D-4E9AF5B28347.html



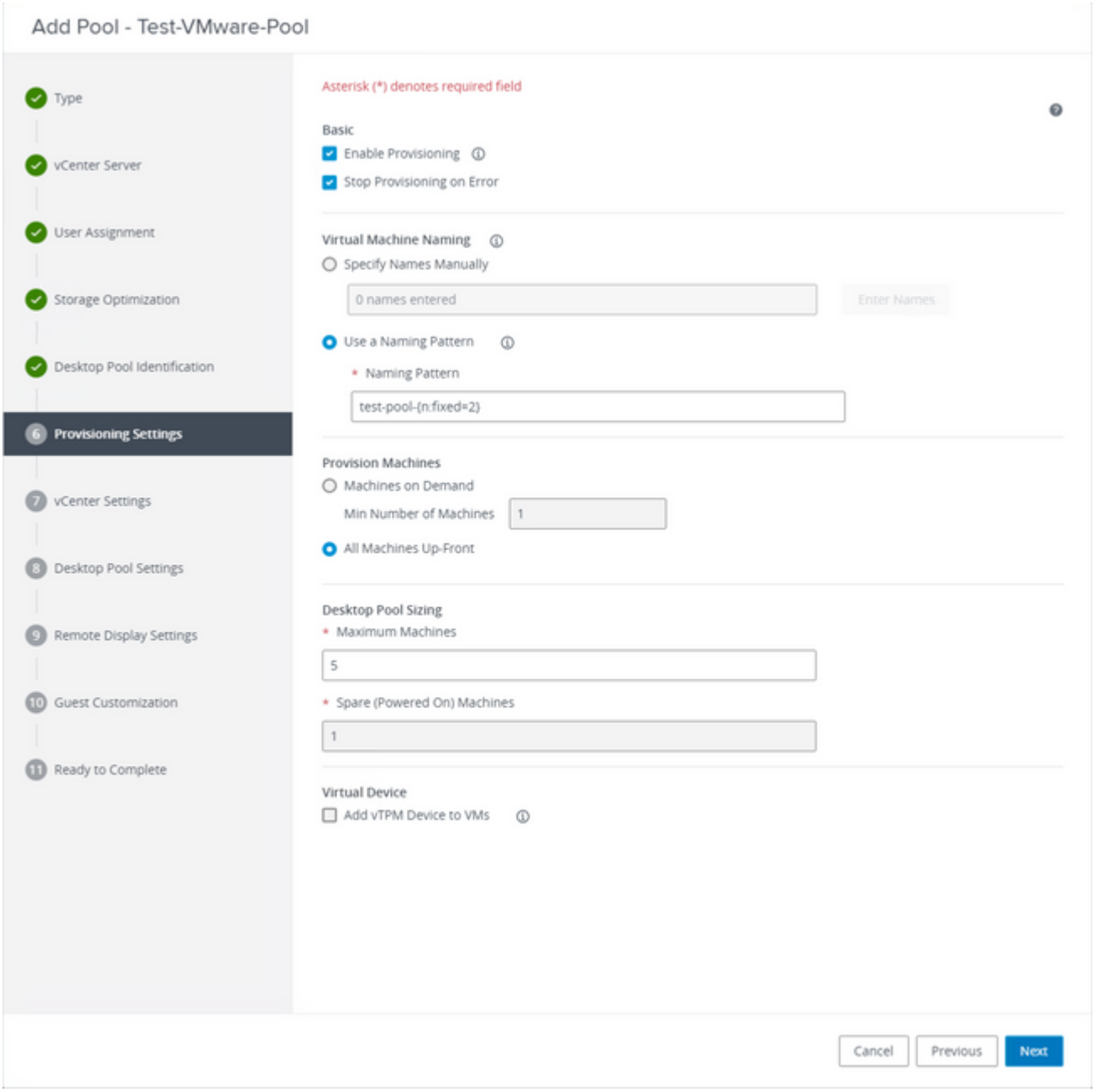

*Seleção do tipo "Flutuante"*

Consulte: 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




*Nomes de Pool de Área de Trabalho*




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

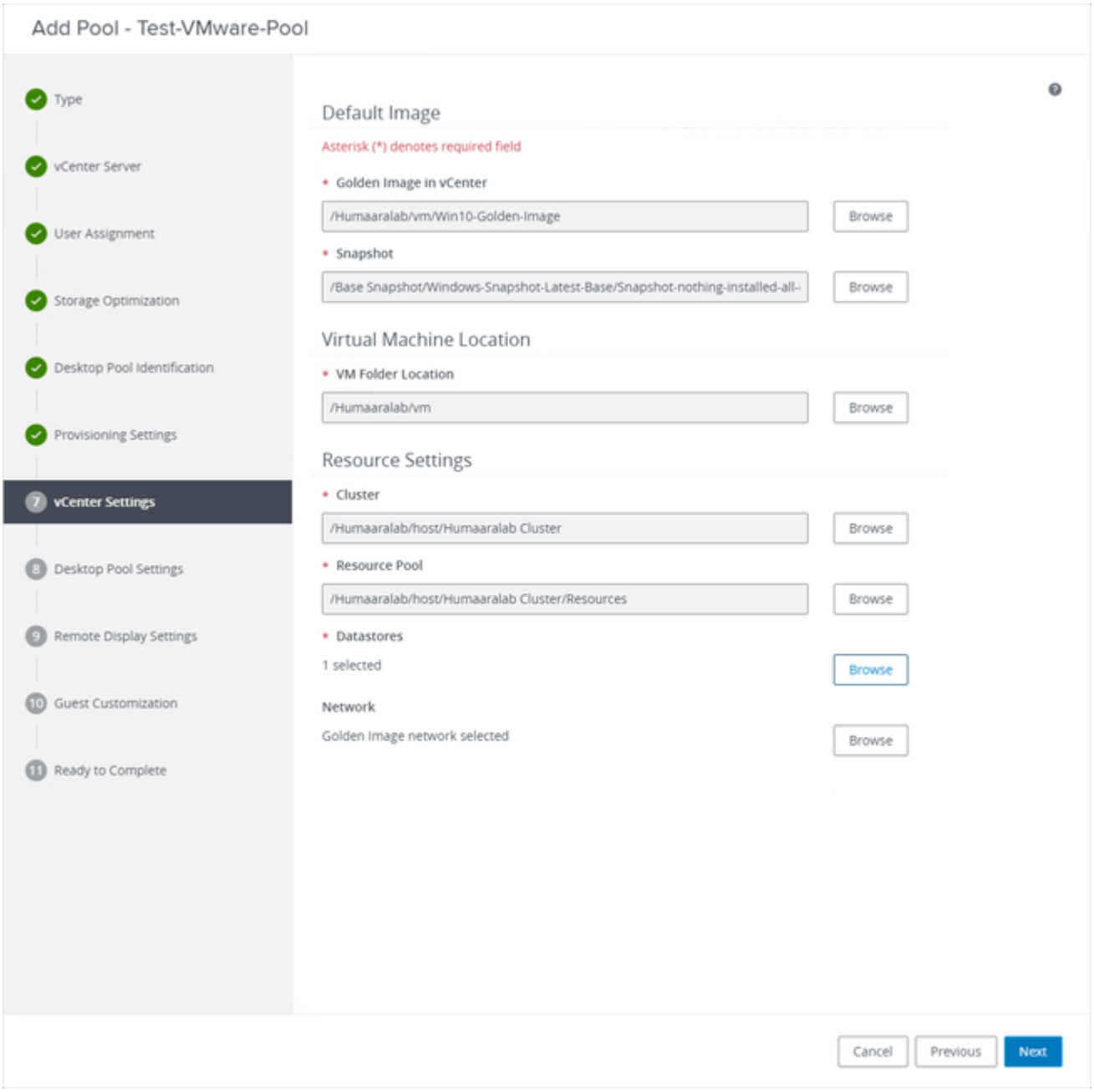
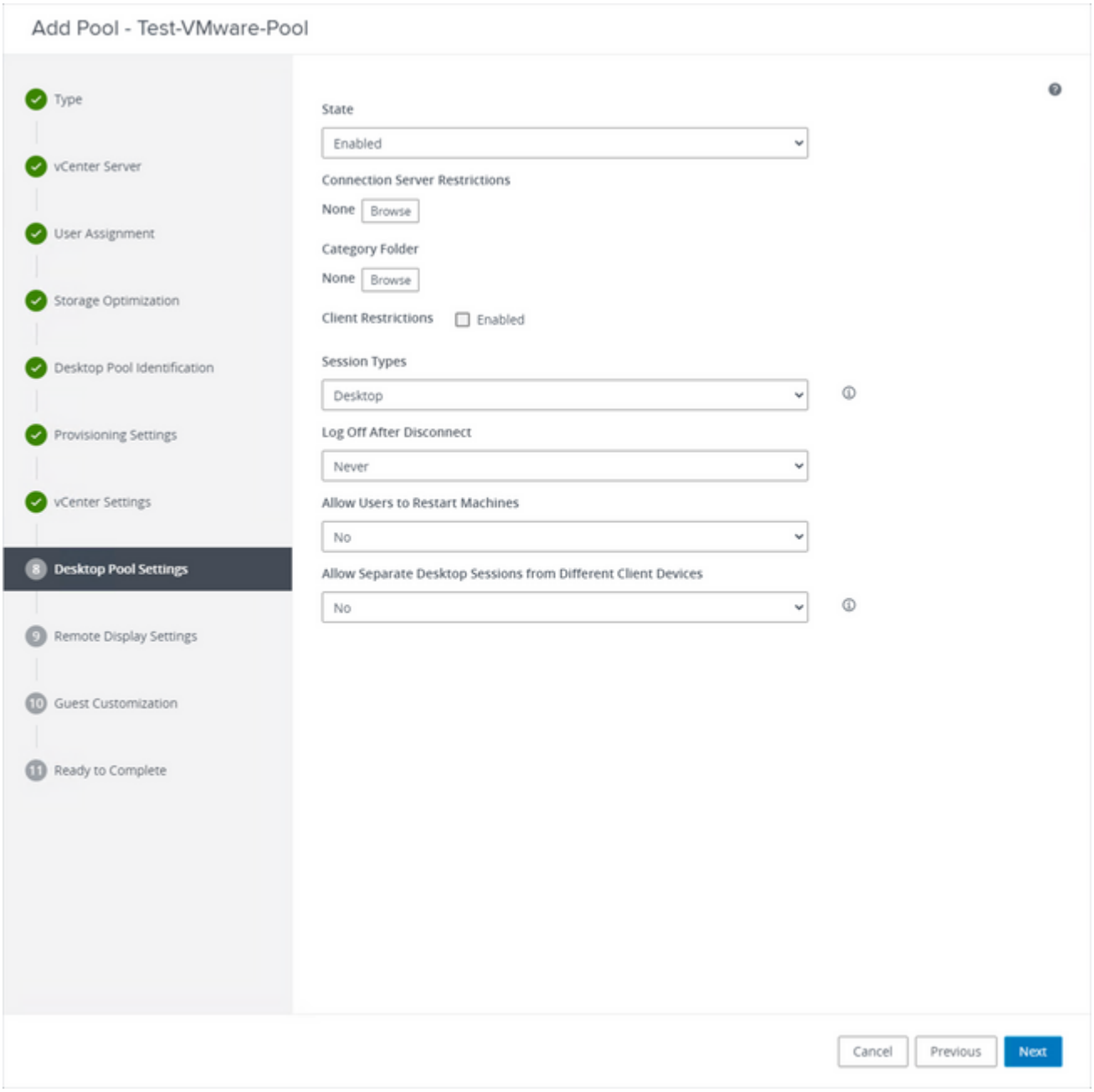
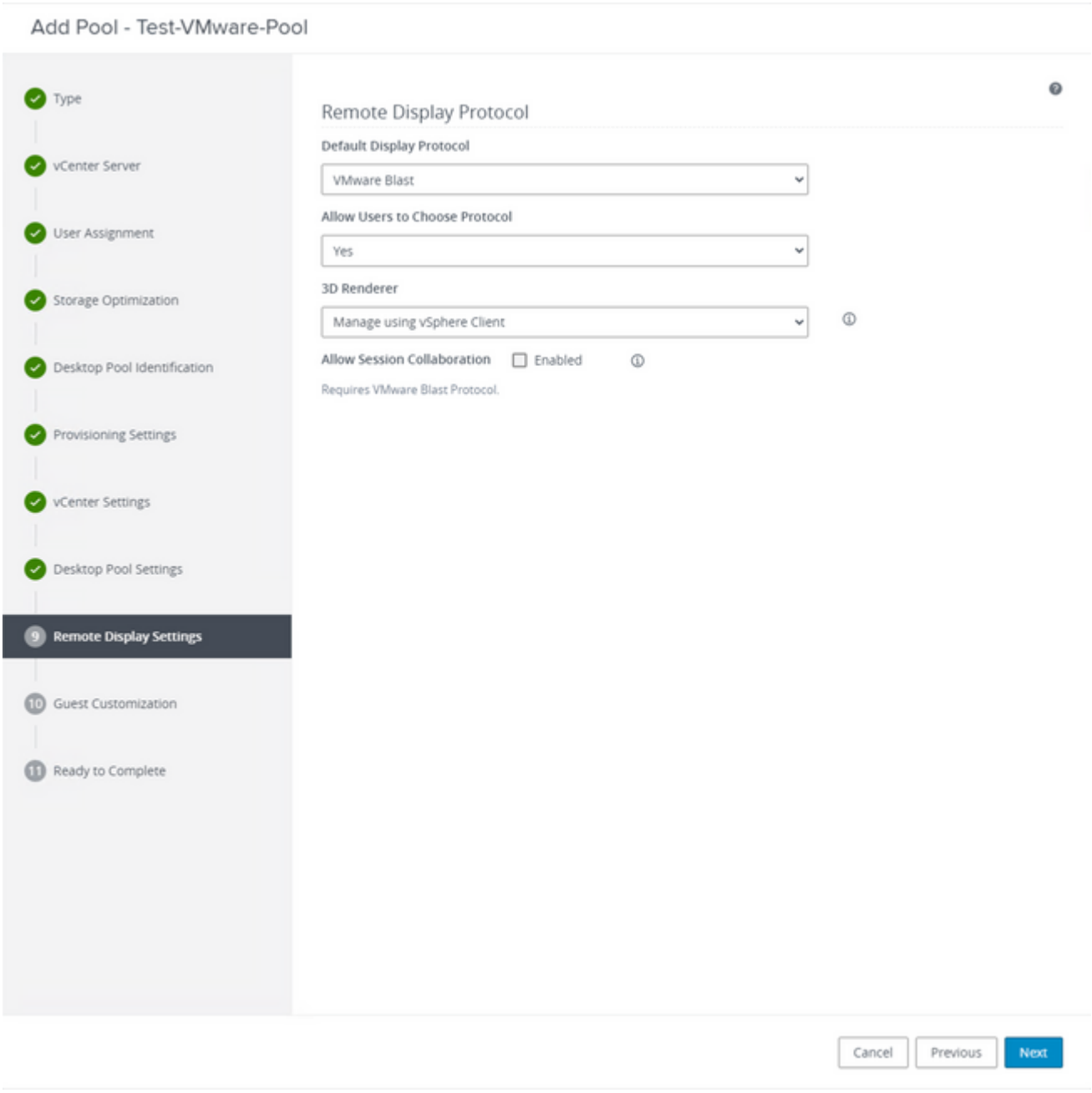
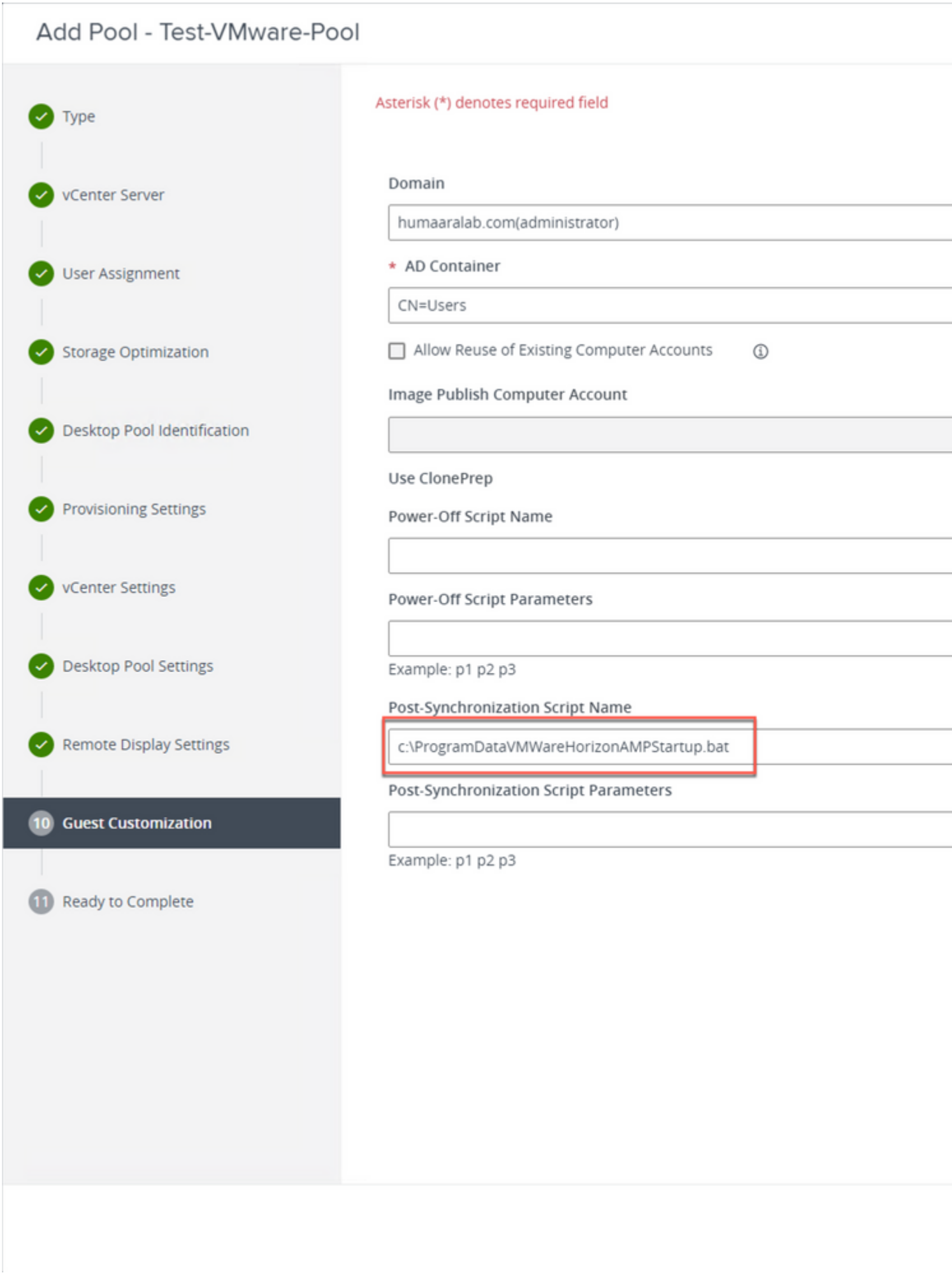



Imagem dourada: essa é a VM real da imagem dourada.

Instantâneo: esta é a imagem que você deseja usar para implantar a VM filha. Este é o valor que é atualizado quando você atualiza a Imagem Dourada com qualquer alteração. Rest são algumas das configurações específicas do VMware Environment.


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. Como mencionado anteriormente, a Etapa 10. do assistente é onde você define o **caminho do script**.

2. O conector é instalado, armazenando o token em local.xml, e o conector faz uma solicitação POST ao portal com o token em questão.
3. O lado da nuvem passa por essa ordem de operações:

   a. O computador verifica a política quanto à configuração da política de sincronização de ID. Sem isso, o registro ocorre normalmente.
   b. Dependendo das configurações da política, o Registro verifica o nome do host ou o endereço MAC no banco de dados existente.
      Entre empresas:Todas as políticas são verificadas quanto a uma correspondência no nome do host ou no MAC, dependendo da configuração. O GUID do objeto correspondente é anotado e enviado de volta à máquina cliente final. A máquina cliente assume então o UUID e assume qualquer configuração de grupo/política do host correspondente anteriormente. Isso substitui as configurações de política/grupo instaladas.
      Entre políticas:O token corresponde à política no lado da nuvem e procura um objeto existente com o mesmo nome de host ou endereço MAC DENTRO dessa política apenas. Se existir algum, ele assume o UUID. Se não houver um objeto existente vinculado a essa política, um novo objeto será criado. Observação: podem existir duplicatas para o mesmo nome de host vinculado a outros grupos/políticas.
   c. Se não for possível fazer uma correspondência com um grupo/política devido a um token ausente (registrado anteriormente, prática de implantação incorreta etc.), o conector se enquadra no grupo/política de conector padrão definido na guia comercial. Com base na configuração do grupo/política, ele tenta revisar todas as políticas de uma correspondência (em toda a empresa), somente aquela política em questão (em toda a política) ou nenhuma (nenhuma). Com isso em mente, geralmente é aconselhável colocar seu grupo padrão para ser um que contenha suas configurações de sincronização de ID desejadas para que as máquinas sejam sincronizadas novamente corretamente no caso de um problema de token.

## Identifique duplicatas em sua organização

### Scripts GitHub disponíveis externamente

Localize os UUIDs duplicados: https://github.com/CiscoSecurity/amp-04-find-duplicate-guids

Remova os UUIDs antigos/obsoletos: https://github.com/CiscoSecurity/amp-04-delete-stale-guids

## Motivos pelos quais as duplicatas são criadas

Há algumas instâncias comuns que podem fazer com que as duplicatas sejam vistas no seu lado:

1. Se estas etapas foram seguidas enquanto o Pool de VDI:

- A implantação inicial em uma VM/VDI não persistente é feita com a persistência de identidade desativada (use uma imagem dourada, por exemplo).
- A política é atualizada na nuvem para ter a Persistência de Identidade habilitada, que, durante o dia, a atualiza no endpoint.
- As máquinas são atualizadas/recriadas (use a mesma imagem dourada), que coloca a política original de volta no endpoint sem a Persistência de identidade.
- A política localmente não tem Persistência de Identidade, portanto o servidor de registro não verifica registros anteriores.
- Esse fluxo resulta em Duplicatas.

2. O usuário implanta a gold image original com a persistência de identidade ativada na política em um grupo e, em seguida, move um endpoint para outro grupo no portal de endpoints seguros. Em seguida, ele

tem o registro original no grupo â€˜movido paraâ€™, mas cria novas cópias no grupo original quando as VMs são recriadas/reimplantadas.

---

> **Observação**: esta não é uma lista completa de cenários que podem causar duplicatas, mas algumas das mais comuns.

---

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.