Configuración de la persistencia de identidad en un terminal seguro

Contenido

Introducción

Este documento describe cómo revisar la función Cisco Secure Endpoint Identity Persistence.

¿Qué es la persistencia de identidad?

La persistencia de identidad es una función que permite mantener un registro de eventos coherente en entornos virtuales o cuando se vuelven a crear imágenes de los equipos. Puede

enlazar un conector a una dirección MAC o nombre de host de modo que no se cree un nuevo registro de conector cada vez que se inicie una nueva sesión virtual o se vuelva a crear una imagen de un equipo. Esta función está diseñada específicamente para entornos de laboratorio y VM no persistentes y no debe habilitarse para las configuraciones de servidor y estación de trabajo tradicionales.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso al portal de terminales seguros de Cisco
- Debe ponerse en contacto con el TAC de Cisco para que habilite la función Persistencia de identidad en su organización.
- La persistencia de identidad solo se admite en el sistema operativo (SO) de Windows

¿Cuándo Necesita Persistencia De Identidad?

Identity Persistence es una funcionalidad en los terminales seguros que ayuda en la identificación de los terminales seguros en el momento del registro inicial del conector y los compara con entradas conocidas anteriormente basadas en parámetros de identidad como la dirección MAC o el nombre de host para ese conector específico. La implementación de esta función no solo ayuda a mantener un recuento de licencias correcto, sino que, lo que es más importante, permite un seguimiento adecuado de los datos históricos de los sistemas no persistentes.

Implementación de terminales virtuales

El uso más común de la persistencia de la identidad en las implementaciones virtuales es la implementación de infraestructuras de escritorio virtual (VDI) no persistentes. Los entornos de escritorio host de VDI se implementan a petición o necesidad del usuario final. Esto incluye diferentes proveedores como VMware, Citrix, AWS AMI, Golden Image Deployment, etc.

La VDI persistente, también denominada "VDI stateful", es una configuración en la que el escritorio de cada usuario individual se puede personalizar de forma exclusiva y "persiste" de una sesión a otra. Este tipo de implementación virtual no necesita la funcionalidad de Identity Persistence, ya que estas máquinas no se deben volver a crear imágenes con regularidad.

Al igual que con todo el software que podría interactuar con el rendimiento del terminal seguro, las aplicaciones de escritorio virtual deben evaluarse para detectar posibles exclusiones con el fin de maximizar la funcionalidad y minimizar el impacto.

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

Implementación de terminales físicos

Existen dos situaciones que se pueden aplicar para la implementación de la Persistencia de identidad en equipos físicos de terminales seguros:

- Al implementar o recrear imágenes de un terminal físico con una imagen dorada con el conector de terminal seguro preinstalado, se debe habilitar Goldenimage Flag. La persistencia de identidad se puede utilizar para evitar la duplicación en los casos de máquinas recreadas, pero no es necesaria.

- Al implementar o recrear imágenes de un terminal físico con una imagen dorada e instalar posteriormente el conector de terminal seguro, se puede utilizar Identity Persistence para evitar la duplicación en los casos de equipos en los que se han vuelto a crear imágenes, pero no es necesario.

Visión General del Proceso de Persistencia de Identidad

1. El conector se descarga con un token en el archivo policy.xml, que lo vincula de nuevo a la política en cuestión en el lado de la nube.
2. El conector está instalado, almacenando el token en local.xml, y el conector realiza una solicitud POST al portal con el token en cuestión.
3. El lado de la nube sigue este orden de operaciones:
   a. El equipo comprueba la configuración de directiva de sincronización de identificadores en la directiva. Sin esto, el registro ocurre como normal.
   b. Dependiendo de la configuración de la política, el registro comprueba la base de datos existente para el nombre de host o la dirección MAC.
      En toda la empresa:En función de la configuración, se comprueba si todas las políticas coinciden en el nombre de host o MAC. El GUID del objeto coincidente se registra y se devuelve al equipo cliente final. El equipo cliente asume entonces el UUID y asume cualquier configuración de grupo/política del host previamente coincidente. Esto reemplaza la configuración de grupo o directiva instalada.
      En la directiva: el token coincide con la política en el lado de la nube y busca un objeto existente con el mismo nombre de host o dirección MAC DENTRO de esa política solamente. Si existe uno, se asume el UUID. Si no hay un objeto existente vinculado a esa directiva, se crea un nuevo objeto. Nota: pueden existir duplicados para el mismo nombre de host vinculado a otros grupos/políticas.
   c. Si no se puede hacer una coincidencia con un grupo/política debido a un token faltante (anteriormente registrado, mala práctica de implementación, etc.), el conector cae en el grupo/política de conector predeterminado establecido en la ficha de negocio. Basándose en la configuración del grupo o la directiva, intenta revisar todas las directivas para buscar una coincidencia (en toda la empresa), sólo esa directiva en cuestión (en toda la directiva) o ninguna en absoluto (ninguna). Teniendo esto en cuenta, generalmente se recomienda colocar el grupo predeterminado para que contenga la configuración de sincronización de ID deseada para que las máquinas vuelvan a sincronizarse correctamente en caso de un problema de token.

Identificación de duplicados en su organización

Scripts de GitHub disponibles externamente

Busque los UUID duplicados: https://github.com/CiscoSecurity/amp-04-find-duplicate-guids

Motivos por los que se crean duplicados

Hay algunos casos comunes que pueden causar que se vean duplicados por su parte:

1. Si se han seguido estos pasos mientras el conjunto VDI:

- La implementación inicial en una VM/VDI no persistente se realiza con la persistencia de identidad desactivada (utilice una imagen dorada, por ejemplo).
- La política se actualiza en la nube para tener habilitada la función Persistencia de identidad, que a lo largo del día la actualiza en el terminal.
- Las máquinas se actualizan o se vuelven a crear (utilizan la misma imagen dorada), que vuelve a colocar la política original en el terminal sin la persistencia de identidad.
- La política localmente no tiene Persistencia de Identidad, por lo que el servidor de registro no verifica los registros anteriores.
- Este flujo produce duplicados.

2. El usuario implementa la imagen dorada original con la opción Persistencia de identidad habilitada en la directiva en un grupo y, a continuación, mueve un extremo a otro grupo desde el portal de extremos seguros. A continuación, tiene el registro original en el grupo "movido a", pero crea nuevas copias en el grupo original cuando se vuelven a crear imágenes de las VM o se vuelven a implementar.

 Nota: Esta no es una lista exhaustiva de escenarios que podrían causar duplicados, sino algunos de los más comunes.

Problemas y síntomas comunes con una implementación incorrecta de persistencia de identidad

La implementación incorrecta de Persistencia de identidad puede causar estos problemas/síntomas:

- Recuento de asientos del conector incorrecto
- Resultados informados incorrectos
- Discordancia de datos de trayectoria del dispositivo
- Intercambios de nombre de equipo en registros de auditoría
- Los conectores se registran y anulan el registro aleatoriamente desde la consola
- Los conectores no informan correctamente a la nube
- Duplicación de UUID
- Duplicación de nombre de máquina
- Incoherencia de datos
- Las máquinas se registran en Grupo de trabajo/Política predeterminada después de la recomposición

- Implementación manual con la función Persistencia de identidad habilitada en la directiva.

- Si implementa el terminal manualmente a través del switch de línea de comandos con la

Persistencia de identidad ya habilitada en la política y luego desinstala el terminal e intenta reinstalar con un paquete de otro grupo/política, el terminal volverá automáticamente a la política original.

- Salida de los registros de SFC que muestran el switch de políticas por sí solo con en 1-10 segundos

```
(167656, +0 ms) Dec 14 11:37:17 [1308]: Util::VerifyOsVersion: ret 0
(167656, +0 ms) Dec 14 11:37:17 [1308]: ERROR: ETWEnableConfiguration::IsETWEnabled: ETW not initialize
(167656, +0 ms) Dec 14 11:37:17 [1308]: UiPublisher::PublishPolicyInfo: Name -UTMB-WinServer-Protect Se
(167656, +0 ms) Dec 14 11:37:17 [1308]: UiPublisher::PublishLastPolicyUpdateTime: Publish Last Policy U
(167656, +0 ms) Dec 14 11:37:17 [1308]: UiPublisher::PublishAgentVersion: Agent Version 7.5.7.21234
(167656, +0 ms) Dec 14 11:37:17 [1308]: HeartBeat::PolicyNotifyCallback: EXIT
(167656, +0 ms) Dec 14 11:37:17 [1308]: AmpkitRegistrationHandler::PolicyCallback: EXIT (0)
.
.
.
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitRegistrationHandler::UpdateConfiguration: Enter
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitRegistrationHandler::UpdateConfiguration: Aborting - not
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitRegistrationHandler::ConnectionStateChanged: Starting Pro
(173125, +0 ms) Dec 14 11:37:22 [4704]: UIPipe::SendPolicyReloaded sending policy reloaded to UI. ui.da
(173125, +0 ms) Dec 14 11:37:22 [4704]: PipeSend: sending message to user interface: 28, id: 0
(173125, +0 ms) Dec 14 11:37:22 [4704]: UIPipe::SendStatus: notifying UI: No Product
(173125, +0 ms) Dec 14 11:37:22 [4704]: UIPipe::SendStatus: notifying UI: No Product
(173125, +0 ms) Dec 14 11:37:22 [4704]: UIPipe::SendStatus: notifying UI: No Product
(173125, +0 ms) Dec 14 11:37:22 [4704]: UIPipe::SendStatus : engine1 (0, 0), engine2 (0, 0)
(173125, +0 ms) Dec 14 11:37:22 [4704]: PipeSend: sending message to user interface: 1, id: 0
(173125, +0 ms) Dec 14 11:37:22 [4704]: UiStatusHandler::ConnectionStateChangedState: 0
(173125, +0 ms) Dec 14 11:37:22 [4704]: UiPublisher::PublishConnectionStatus: State 0
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpApiServer.cpp:AmpApiServer::PublishScanAvailable:223: Cloud
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitProxyHelper::LoadProxyFromConfig: Enter
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitProxyHelper::LoadProxyFromConfig proxy server is NULL
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitProxyHelper::LoadProxyFromConfig: Direct connection detec
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitProxyHelper::LoadProxyFromConfig: Exit(1)
(173125, +0 ms) Dec 14 11:37:22 [4704]: UiAgentGuidUpdater::ConnectionStateChanged
(173125, +0 ms) Dec 14 11:37:22 [4704]: UiAgentGuidUpdater::RefreshAgentGuidUi: Agent GUID: e1a756e2-65
(173125, +0 ms) Dec 14 11:37:22 [4704]: UiPublisher::PublishAgentGuid: Agent GUID did not change (e1a75
(173125, +0 ms) Dec 14 11:37:22 [4704]: AmpkitSubscriptionThread::NotificationWorker: Waiting on queue
```

El otro efecto secundario si intenta instalar un conector que pertenece a un grupo diferente. Verá en el portal que el conector está asignado al grupo correcto pero con la política original "incorrecta"

Esto se debe a cómo funciona la Persistencia de identidad (ID SYNC).

Sin ID SYNC una vez que el conector se haya desinstalado completamente o mediante el switch de línea de comandos re-register. Debería ver la nueva fecha de creación y el GUID del conector en caso de desinstalación o solo el nuevo GUID del conector en caso de volver a registrar el comando. Sin embargo, con ID SYNC que no es posible, ID SYNC se sobrescribe con el GUID y la FECHA antiguos. Así es como "sincronizamos" el host.

Si se observa este problema, la solución debe implementarse a través del cambio de política.

Deberá mover los terminales afectados de nuevo al grupo o la directiva original y asegurarse de que la directiva se sincroniza. A continuación, vuelva a colocar los terminales en el grupo o la política que desee

Prácticas recomendadas de implementación

Configurar archivo snapvol

En caso de que utilice App Volumes para su infraestructura VDI, se recomienda que realice estos cambios de configuración en su configuración de snapvol.cfg

Estas exclusiones deben implementarse en el archivo snapvol.cfg:

Rutas:

- 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

Claves del Registro:

- HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Immunet de protección
- 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

En sistemas x64, agregue lo siguiente:

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Immunet de protección
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstal de protección

Referencias:

- 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

Planificación de políticas del portal

Estas son algunas de las prácticas recomendadas que deben seguirse al implementar la persistencia de identidad en Secure Endpoint Portal:

1. Se recomienda encarecidamente utilizar políticas o grupos independientes para los terminales de persistencia de identidad para facilitar la segregación.

2. Si tiene pensado utilizar el aislamiento de terminales e implementar la acción Mover equipo a grupo si se pone en riesgo. El grupo de destino también debe tener habilitada la Persistencia de identidad y sólo se debe utilizar para equipos VDI.

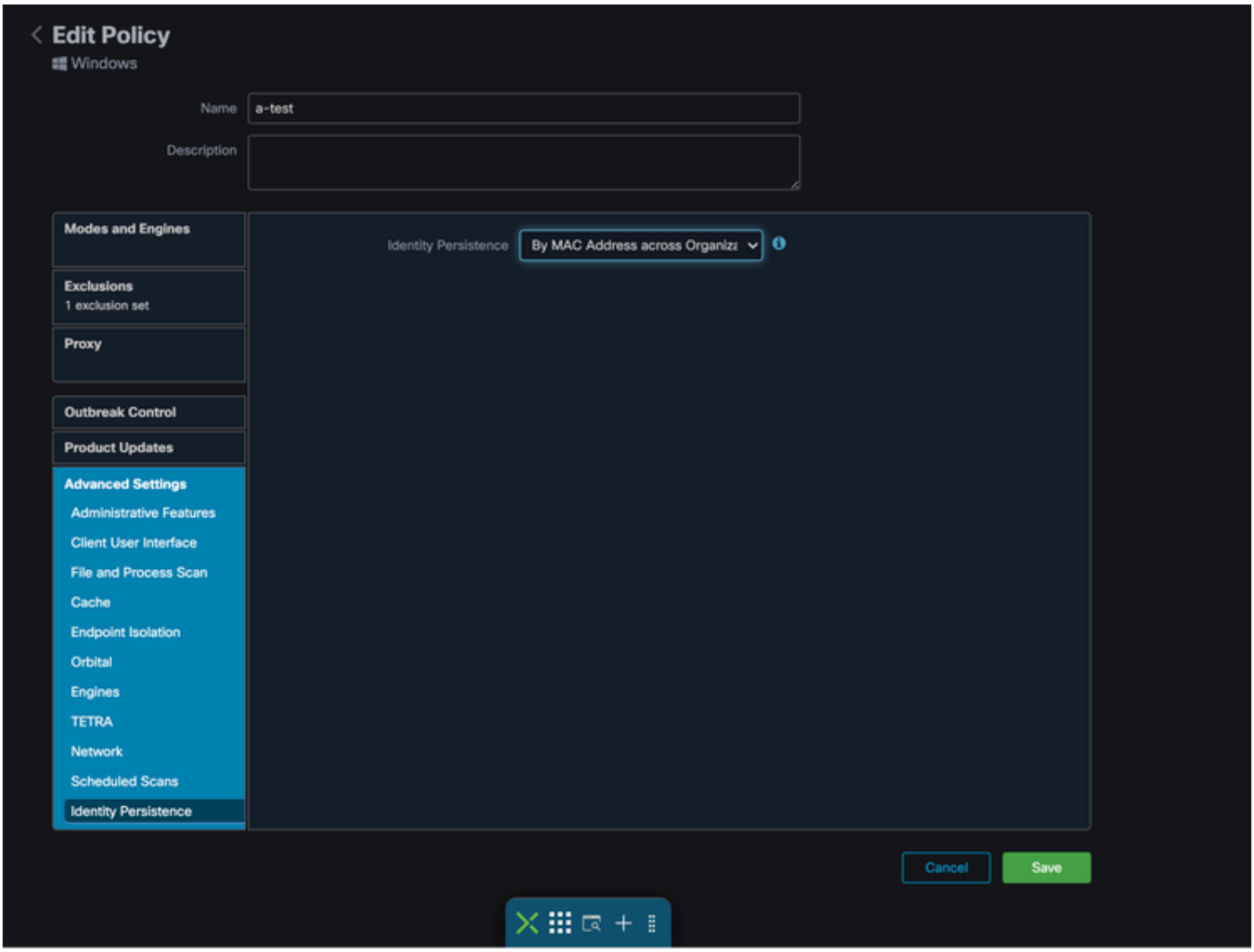
3. No se recomienda habilitar Persistencia de identidad en el grupo o la política predeterminados de la configuración de la organización, a menos que se haya habilitado Persistencia de identidad en todas las políticas con Toda la organización como ámbito de configuración.

Configuración

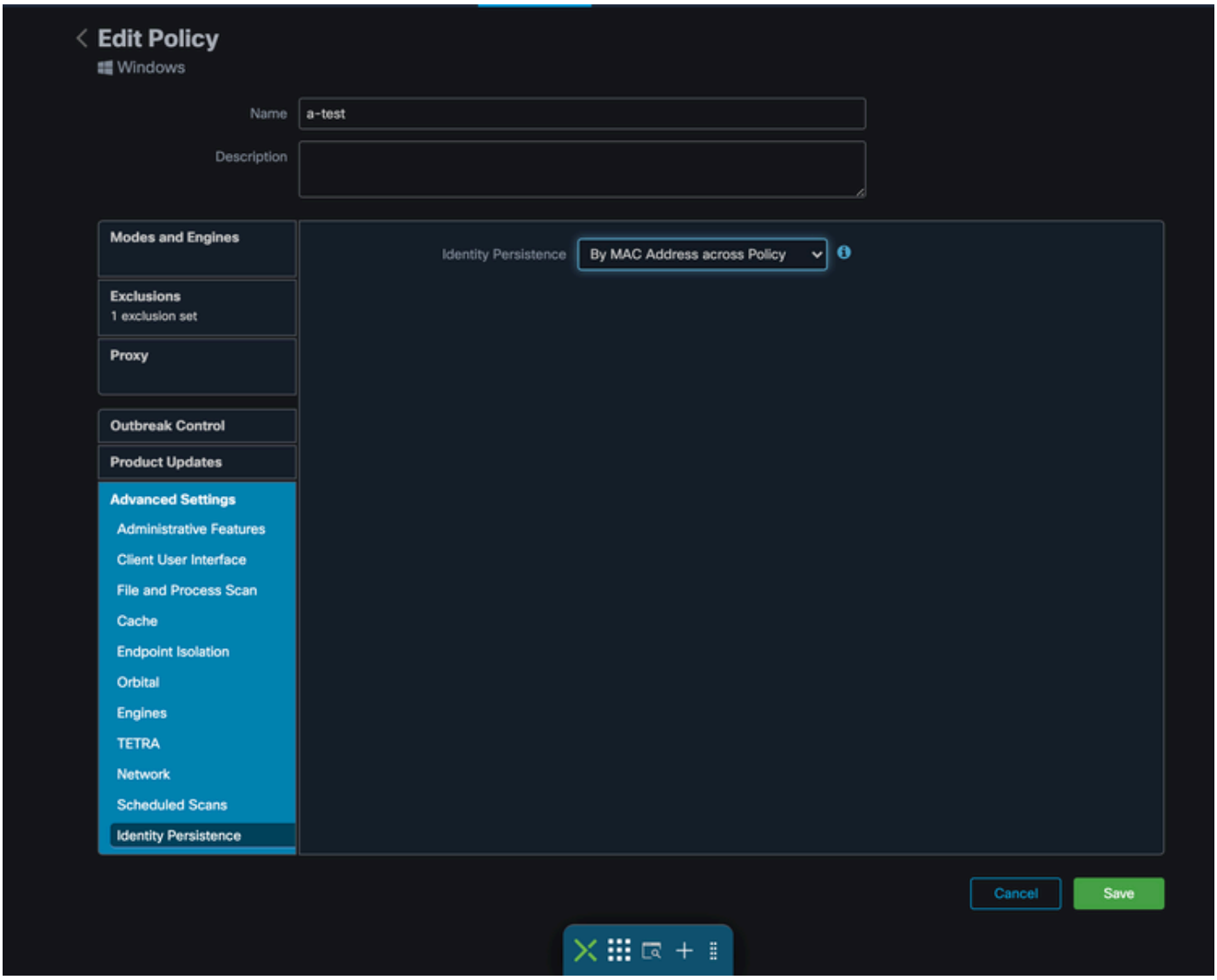
Siga estos pasos para implementar el conector de terminal seguro con Persistencia de identidad:

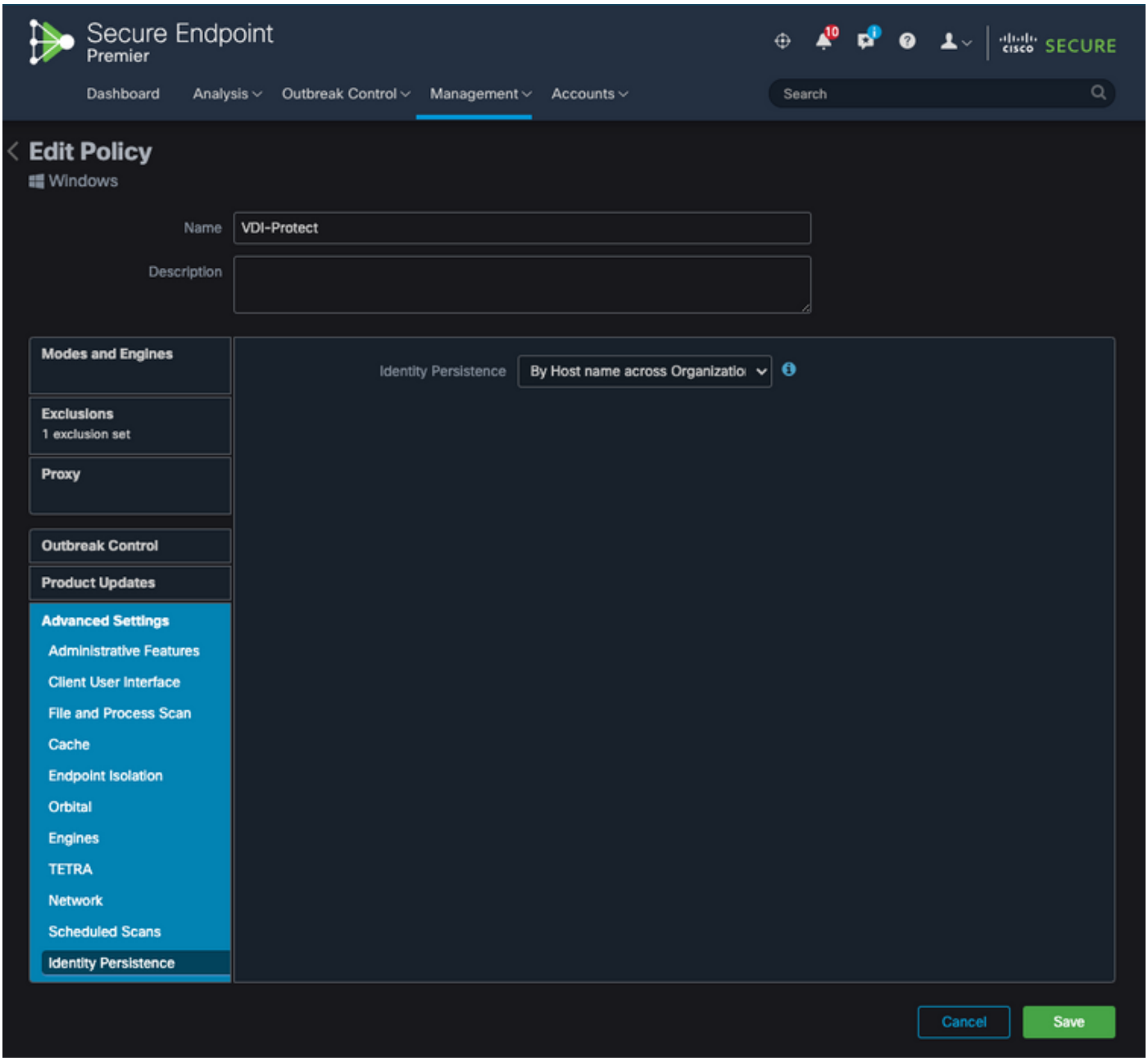
Paso 1. Aplique la configuración de Persistencia de identidad deseada a las políticas:

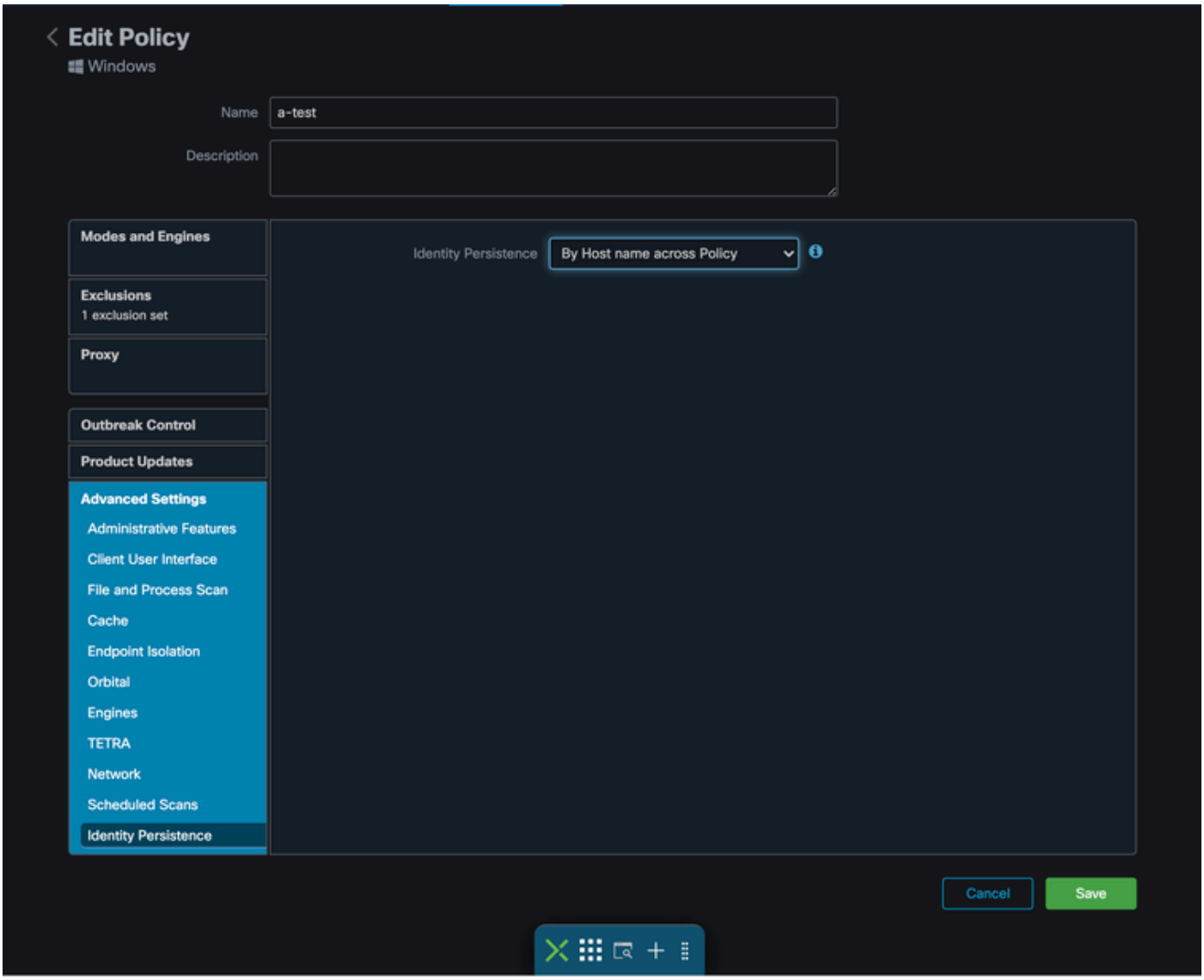
- En el portal de terminales seguros, navegue hasta Administración > Políticas.
- Seleccione la política deseada en la que desea habilitar la Persistencia de identidad y, a continuación, haga clic en Editar.
- Navegue hasta la pestañaConfiguración avanzada y luego haga clic en la pestaña Persistencia de identidad en la parte inferior.
- Seleccione la lista desplegable Persistencia de identidad y elija la opción que mejor se adapte a su entorno. Consulte esta imagen.


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 Organiz
Cancel
Save

Prueba - 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
TETRA
Network
Scheduled Scans
Identity Persistence
Identity Persistence
By MAC Address across Policy
Cancel
Save


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



Puede elegir entre cinco opciones.

- Tenga en cuenta que la función no está activada. Los UUID del conector no están sincronizados con los nuevos conectores instalados bajo ninguna circunstancia. Cada nueva instalación genera un nuevo objeto de equipo.
- Por dirección MAC en la empresa: las instalaciones nuevas o actualizadas buscan el registro del conector más reciente que tenga la misma dirección MAC para sincronizar los datos históricos anteriores con el nuevo registro. Esta configuración busca en todos los registros empresariales

  en todas las directivas de la organización que tienen la sincronización de identidad establecida en un valor distinto de Ninguno. El conector puede actualizar su directiva para reflejar la instalación anterior si difiere de la nueva.

- Por dirección MAC en la política: las instalaciones nuevas o actualizadas buscan el registro del conector más reciente que tenga la misma dirección MAC para sincronizar los datos históricos anteriores con el nuevo registro. Esta configuración sólo busca en los registros asociados a la directiva utilizada en la implementación. Si el conector no estaba instalado previamente en esta directiva pero estaba activo anteriormente en otra, puede crear

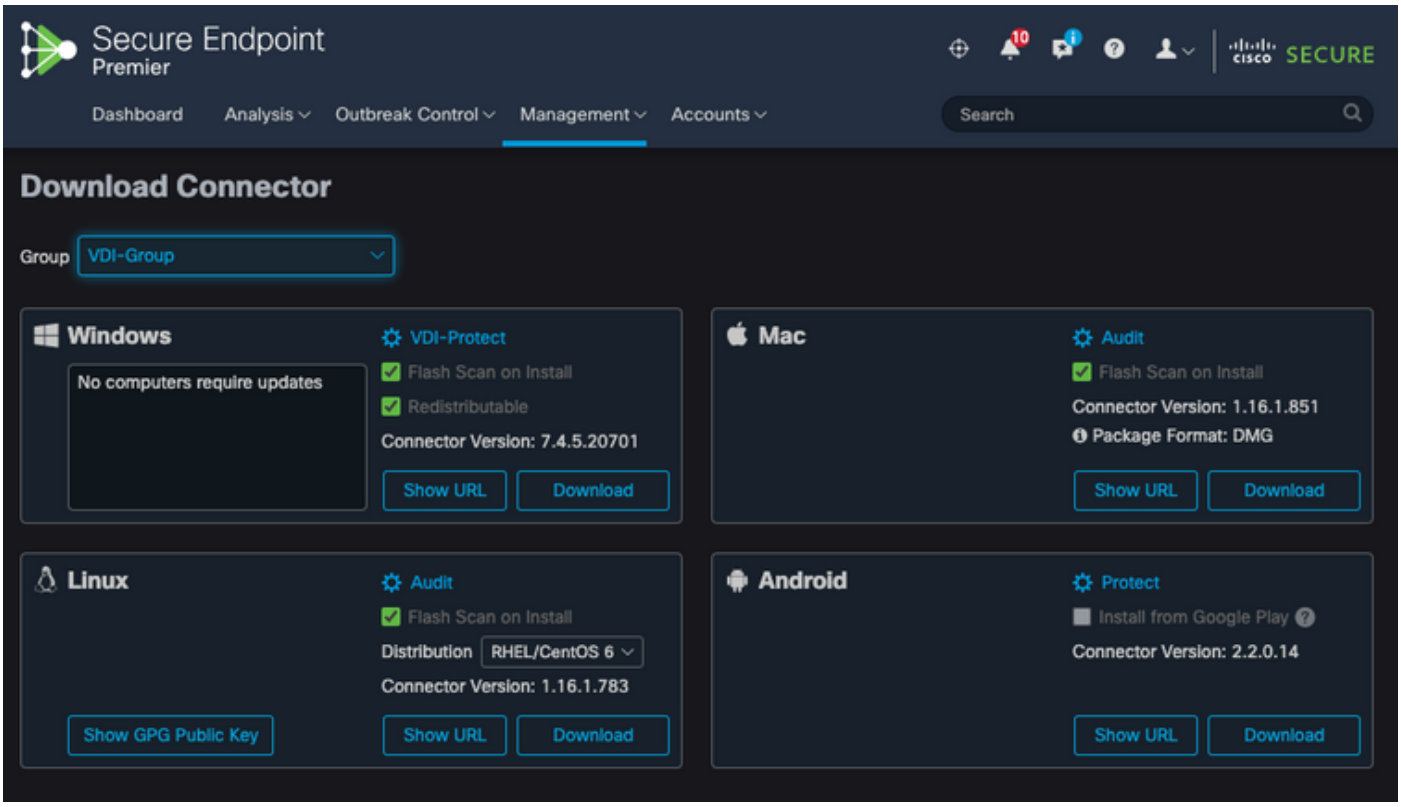
duplicados.

- Por nombre de host en la empresa: las instalaciones nuevas o actualizadas buscan el registro del conector más reciente que tenga el mismo nombre de host para sincronizar los datos históricos anteriores con el nuevo registro. Esta configuración busca en todos los registros comerciales, independientemente de la configuración de Persistencia de identidad en otras directivas, y el conector puede actualizar su directiva para reflejar la instalación anterior si difiere de la nueva. El nombre de host incluye FQDN para que se puedan producir duplicados si el conector se mueve con regularidad entre redes (como un portátil).
- Por nombre de host en la política: las instalaciones nuevas o actualizadas buscan el registro del conector más reciente que tenga el mismo nombre de host para sincronizar los datos históricos anteriores con el nuevo registro. Esta configuración sólo busca en los registros asociados a la directiva utilizada para la implementación. Si el conector no estaba instalado previamente en esta directiva pero estaba activo anteriormente en otra, puede crear duplicados. El nombre de host incluye FQDN para que también se puedan producir duplicados si el conector se mueve con regularidad entre redes (como un portátil).

Nota: Si decide utilizar Persistencia de identidad, Cisco sugiere que utilice Por nombre de host en la empresa o la política. Una máquina tiene un nombre de host pero puede tener más de una dirección MAC y muchas VM clonan las direcciones MAC.

Paso 2. Descargue Secure Endpoint Connector.

- Vaya a Administración > Conector de descarga.
- Seleccione el grupo para la directiva que editó en el paso 1.
- Haga clic en Descargar para el conector de Windows como se muestra en la imagen.



Paso 3. Implemente el conector en los terminales.

- Ahora puede utilizar el conector descargado para instalar Secure Endpoint (con Identity Persistence ahora activado) manualmente en los terminales.
- De lo contrario, también puede implementar el conector mediante una imagen dorada (consulte la imagen)

Nota: Debe seleccionar el instalador redistribuible. Se trata de un archivo de ~57 MB (el tamaño puede variar con las versiones más recientes) que contiene los instaladores de 32 y 64 bits. Para instalar el conector en varios equipos, puede colocar este archivo en un recurso compartido de red o enviarlo a todos los equipos según corresponda. El instalador contiene un archivo policy.xml que se utiliza como archivo de configuración para la instalación.

Creación de imágenes doradas

Siga las directrices de prácticas recomendadas del documento del proveedor (VMware, Citrix, AWS, Azure, etc.) cuando cree una imagen dorada para utilizarla en el proceso de clonación de VDI.

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

Como ha identificado el proceso de composición VMware, AWS reinicia las VM clonadas (VM secundarias) varias veces antes de finalizar la configuración de VM, esto provoca problemas con el proceso de registro de terminales seguros, ya que en este momento las VM clonadas (VM secundarias) no tienen asignados los nombres de host finales/correctos y esto hace que las VM clonadas (VM secundarias) utilicen el nombre de host de la imagen dorada y se registren en la nube de terminales seguros. Esto interrumpe el proceso de clonación y causa problemas.

Esto no es un problema con el proceso de conector de Secure Endpoint, pero es incompatible con el proceso de clonación y el registro de Secure Endpoint. Para evitar este problema, hemos identificado algunos cambios que se implementarán en el proceso de clonación que ayudan a resolver estos problemas.

Estos son los cambios que deben implementarse en la máquina virtual Golden Image antes de congelar la imagen para clonarla

1. Utilice siempre el indicador Goldenimage en Golden Image en el momento de la instalación de Secure Endpoint.

2. Implemente la sección Golden Image Setup Script y Golden Image Startup Script para encontrar los scripts que ayudarían a activar el servicio de terminales solo cuando tengamos un nombre de host final implementado en Cloned (Child VM). Consulte la sección Problemas de Duplicación de VMware Horizon para obtener más detalles.

Indicador de anulación de imagen dorada

Cuando utilice el instalador, el indicador que debe utilizar para las imágenes doradas es /goldenimage 1.

El indicador de imagen dorado impide que el conector se inicie y registre en la imagen base; por lo tanto, en el siguiente inicio de la imagen, el conector se encuentra en el estado funcional en el que fue configurado por la política que se le asignó.

Para obtener información sobre otras marcas, puede utilizar, consulte este artículo.

Cuando utilice el instalador, el nuevo indicador que se utilizará para las imágenes doradas es /goldenimage [1|0]

0 - Valor predeterminado - este valor no activará la opción de imagen dorada, y funciona como si el instalador se ejecutara sin la opción en absoluto. No omita el registro inicial del conector ni el inicio durante la instalación.

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

1 -Instalar como una imagen dorada. Esta es la opción típica utilizada con el indicador y es el único uso esperado. Omite el registro inicial del conector y el inicio durante la instalación.

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

Pasos para la creación de imágenes doradas

Se recomienda instalar el conector en último lugar para la preparación de la imagen dorada.

1. Prepare la imagen de Windows según sus necesidades; instale todo el software y las configuraciones necesarios para la imagen de Windows, excepto el conector.
2. Instale el conector de Cisco Secure Endpoint.

Utilice el indicador/goldenimage 1para indicar al instalador que se trata de una implementación de imagen dorada.

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

3. Implemente la lógica de script (si es necesario) como se describe aquí

4. Completar instalación

5. Congele su imagen dorada

Una vez que se han instalado las aplicaciones de Golden Image, el sistema está preparado y Secure Endpoint se ha instalado con/goldenimageflag, el host está listo para congelarse y distribuirse. Una vez que arranca el host clonado, se inicia Secure Endpoint y se registra en la nube. No se requiere ninguna otra acción con respecto a la configuración del conector a menos que haya cambios que desee hacer en la política o el host. Si se realizan cambios después de que la imagen dorada haya completado el registro, este proceso debe reiniciarse. El indicador impide que el conector se inicie y registre en la imagen base. En el siguiente inicio de la imagen, el conector estará en el estado funcional para el que fue configurado por la política que se le asignó.

Nota: Si la imagen dorada se registra en Secure EndpointCloud antes de que pueda inmovilizar la máquina virtual, se recomienda desinstalar y volver a instalar Secure Endpoint en la máquina virtual de la imagen dorada y, a continuación, inmovilizar la máquina virtual de nuevo para evitar problemas de registro y de conectores duplicados. No se recomienda modificar ningún valor del Registro para Secure Endpoint como parte de este proceso de desinstalación.

Actualizar la imagen dorada

Tiene dos opciones cuando necesita actualizar una imagen dorada para conservar un conector no registrado.

Proceso recomendado

1. Desinstale el conector.
2. Instale las actualizaciones del host.
3. Vuelva a instalar el conector después del proceso de imagen dorada utilizando los indicadores de imagen dorada.
4. El host no debe iniciar el conector si se sigue el proceso.
5. Congelar la imagen.
6. Antes de activar los clones, compruebe que la imagen dorada no se haya registrado en el portal para evitar hosts duplicados no deseados.

Proceso alternativo

1. Asegúrese de que el host no tiene conectividad a Internet para evitar que el conector se registre.
2. Detenga el servicio del conector.
3. Instalar actualizaciones.
4. Inmovilizar la imagen una vez que se hayan completado las actualizaciones
5. Es necesario evitar que el conector se registre para evitar que se produzcan hosts duplicados. Cuando se elimina la conectividad, esto impide que llegue a registrarse en la nube. Además, el conector que se detiene lo mantendrá en ese estado hasta el próximo reinicio, lo que permitirá que los clones se registren como hosts únicos.

6. Antes de activar los clones, compruebe que la imagen dorada no se haya registrado en el portal para evitar hosts duplicados no deseados.

Código de imagen dorado

Esta sección consta de fragmentos de código que pueden ayudar a admitir el proceso Golden Image y ayudarían a evitar duplicados de conectores al implementar Identity Persistence.

Guión de configuración de imagen dorada

Descripción del script de configuración

El primer script, 'Setup', se ejecuta en la imagen dorada antes de clonarla. Tiene que ser ejecutado manualmente solo una vez. Su objetivo principal es establecer configuraciones iniciales que permitan que el siguiente script funcione correctamente en las máquinas virtuales clonadas. Estas configuraciones incluyen:

- Cambiar el inicio del servicio Cisco Secure Endpoint a manual para evitar el inicio automático.
- Crear una tarea programada que ejecute el siguiente script (Inicio) al iniciar el sistema con los privilegios más altos.
- Creación de una variable de entorno del sistema denominada "AMP_GOLD_HOST" que almacena el nombre de host de la imagen dorada. El script de inicio lo utilizaría para comprobar si tenemos que revertir los cambios

Código de script de configuración

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

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

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

El código de la secuencia de comandos de configuración es bastante sencillo:

Línea 2: cambia el tipo de inicio del servicio de protección frente a malware a manual.

Línea 5: Crea una nueva variable de entorno denominada "AMP_GOLD_HOST" y guarda en ella el nombre de host del ordenador actual.

Línea 9: Crea una tarea programada denominada "Startamp" que ejecuta la secuencia de comandos 'Startup' especificada durante el inicio del sistema con los privilegios más altos, sin necesidad de una contraseña.

Guión de inicio de Golden Image

Descripción del script de inicio

El segundo script, 'Startup', se ejecuta en cada inicio del sistema en las máquinas virtuales clonadas. Su propósito principal es verificar si la máquina actual tiene el nombre de host de la 'Imagen Dorada':

- Si la máquina actual es la imagen dorada, no se realiza ninguna acción y el script finaliza. Secure Endpoint seguirá ejecutándose al iniciar el sistema, ya que mantenemos la tarea programada.
- Si la máquina actual NO es la imagen 'Golden', se restablecen los cambios realizados por el primer script:
  - Cambio de la configuración de inicio del servicio Cisco Secure Endpoint a automática.
  - Iniciando el servicio Cisco Secure Endpoint.
  - Quitando la variable de entorno "AMP_GOLD_HOST".
  - Eliminando la tarea programada que ejecuta la secuencia de inicio y eliminando la propia secuencia de comandos.

Código de script de inicio

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

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

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

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

rem Turn on AMP
sc start CiscoAMP

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

goto exit
:exit
```

Línea 2: compara el nombre de host actual con el valor "AMP_GOLD_HOST" almacenado; si son iguales, el script salta a la etiqueta "same"; de lo contrario, salta a la etiqueta "notsame".

Línea 4-6: Cuando se llega a la etiqueta "same", el script no hace nada, ya que sigue siendo la imagen dorada y procede a la etiqueta "exit".

Línea 8-16: Si se alcanza la etiqueta "notsame", el script realiza las siguientes acciones:

- Cambia el tipo de inicio del servicio de protección frente a malware a automático.
- Inicia el servicio de protección frente a malware.
- Elimina la variable de entorno "AMP_GOLD_HOST".
- Elimina la tarea programada denominada "Startamp"

Nota: Tenga en cuenta que los scripts contenidos en este documento no son oficialmente compatibles con TAC.

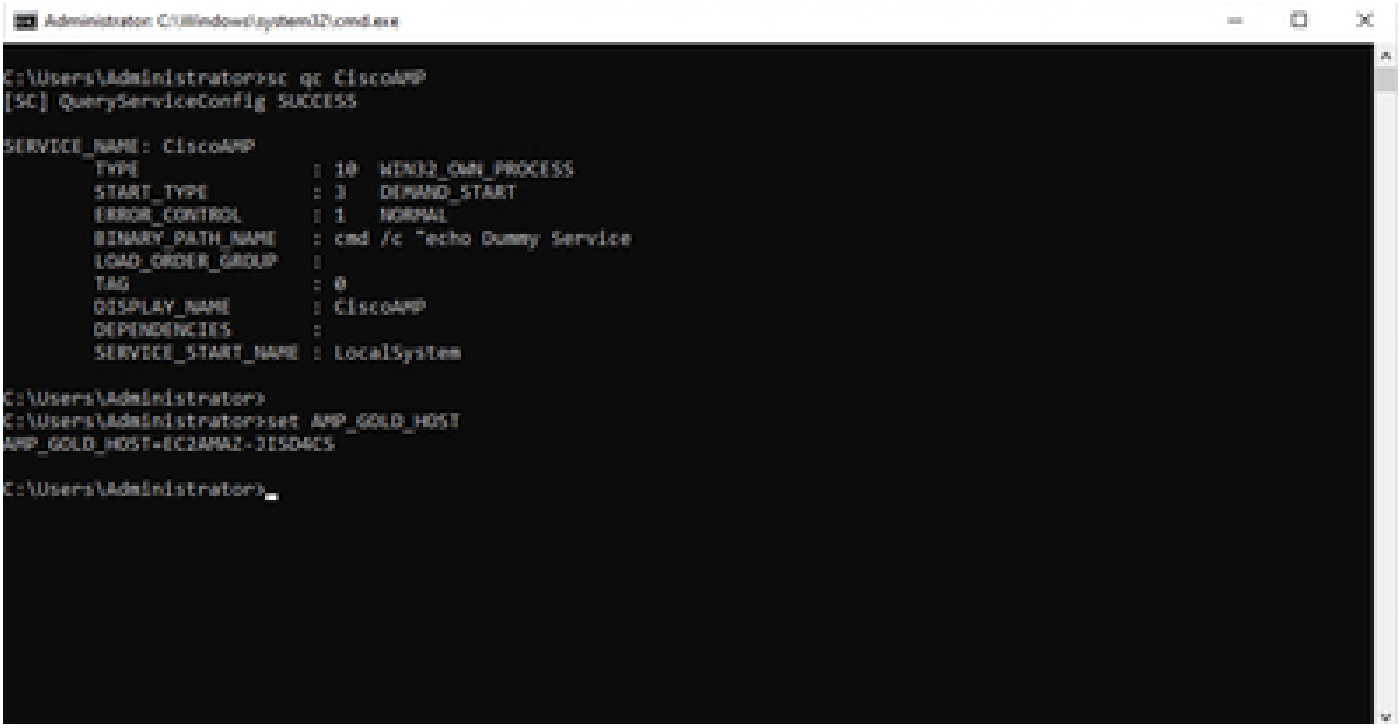
Nota: estos dos scripts permiten iniciar el servicio Cisco AMP en entornos de máquina virtual clonados. Al configurar correctamente la imagen Golden y utilizar los scripts de inicio, se garantiza que Cisco Secure Endpoint se ejecute en todas las máquinas virtuales clonadas con la configuración correcta.

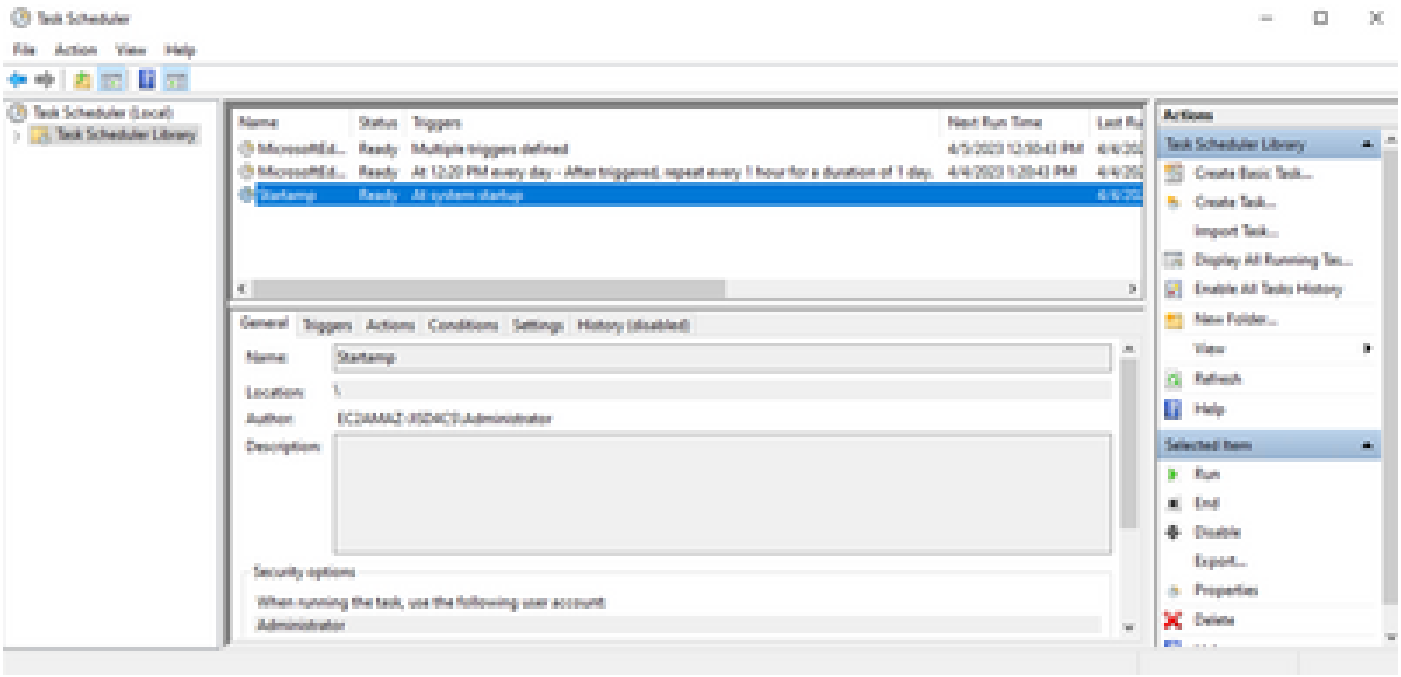
Proceso de AWS Workspace

Esta solución consta de un script de 'configuración' ejecutado en la imagen dorada antes de la clonación y un script de 'inicio' que se ejecuta en cada máquina virtual clonada durante el inicio del sistema. El objetivo principal de estos scripts es garantizar la configuración adecuada del servicio al tiempo que se reduce la intervención manual. Estas dos secuencias de comandos permiten iniciar el servicio Cisco Secure Endpoint en entornos de máquina virtual clonados. Al configurar correctamente la imagen Golden y utilizar los scripts de inicio, se garantiza que el conector de Cisco Secure Endpoint se ejecute en todas las máquinas virtuales clonadas con la configuración correcta

Refiérase a la sección Código de Script de Configuración de Imagen Dorada y Código de Script de Inicio de Imagen Dorada para obtener el código de script necesario para implementar la Imagen Dorada en AWS Workspace.

Después de ejecutar el archivo de comandos de configuración, podemos comprobar que los cambios de configuración se han implementado correctamente.





Dado que realizamos esta acción en la imagen dorada, todas las nuevas instancias tendrán esta configuración y ejecutarán el Script de inicio al inicio.

Problemas de duplicación de VMware Horizon

Con VMware Horizon, pudimos identificar que las máquinas virtuales secundarias cuando se crean se reinician varias veces como parte del proceso de composición de Horizon. Esto provoca problemas, ya que los servicios de terminales seguros se activan cuando las VM secundarias no están preparadas (no tienen asignado el nombre NetBios final/correcto). Esto provoca más problemas, ya que el terminal seguro se confunde y, por tanto, el proceso se interrumpe. Para evitar este problema, se nos ocurrió una solución para esta incompatibilidad con Horizon Process

y esto implica la implementación de los scripts adjuntos en la máquina virtual Golden Image y el uso de la funcionalidad de script posterior a la sincronización para VMware Horizon: https://docs.vmware.com/en/VMware-Horizon/2103/published-desktops-applications.pdf.

Ya no se necesitan cambios o configuraciones

- Ya no es necesario desinstalar y volver a instalar Secure Endpoint si desea realizar cambios en la imagen Golden después de la primera implementación.
- No es necesario establecer Secure Endpoint Service en Inicio retrasado.

Metodología de script

A continuación se incluyen ejemplos de los scripts.

- Archivo de Comandos de Configuración de Golden Image: Este archivo de comandos debe implementarse una vez que se haya instalado el conector de Secure Endpoint, como se ha descrito anteriormente, con los indicadores como se ha documentado anteriormente. Este script modificó el servicio de Secure Endpoint a Inicio manual y guarda el nombre de host Golden Image como una variable de entorno para su referencia en el siguiente paso.

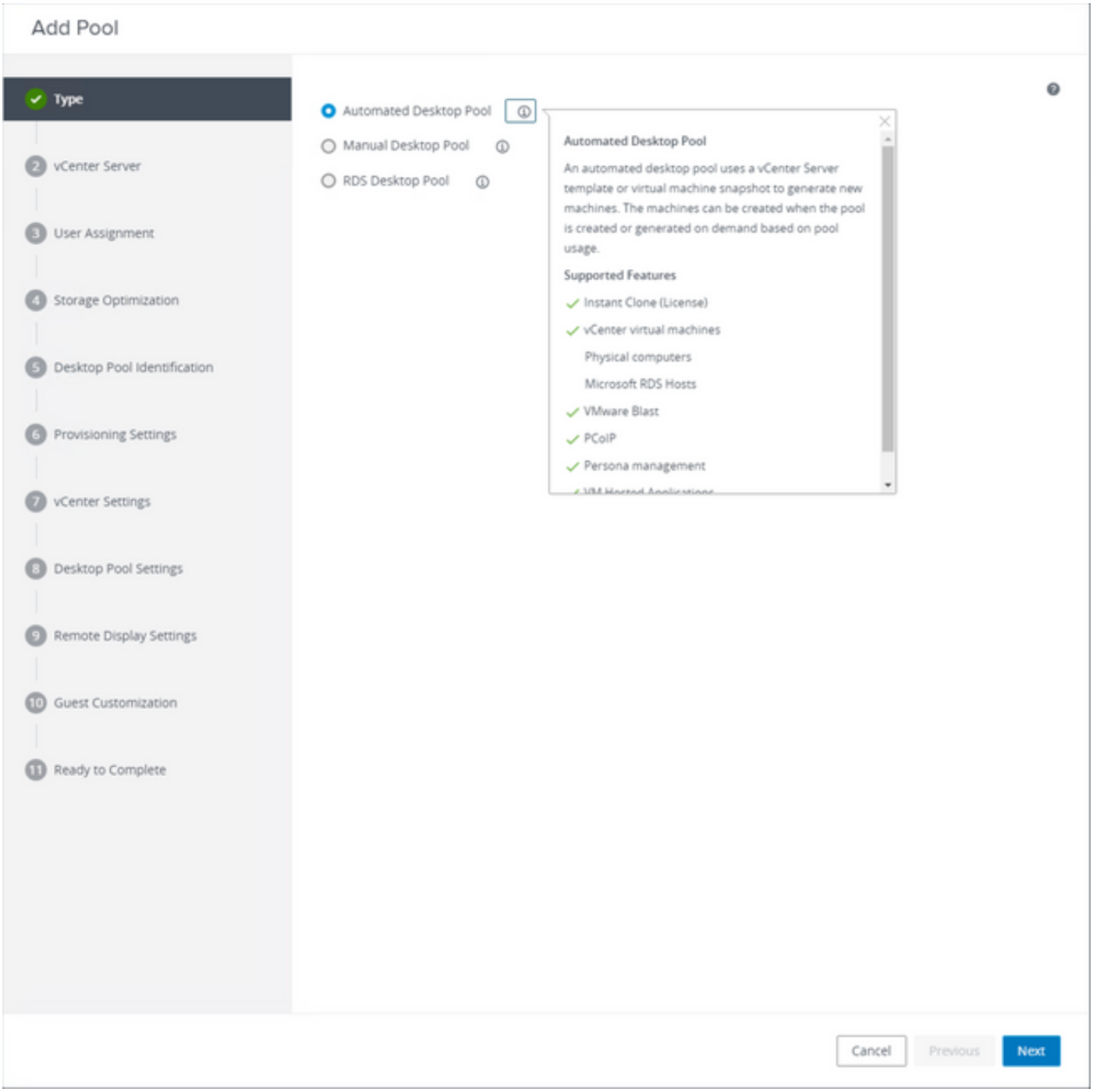
- Script de inicio de imagen dorada: Este script es una comprobación lógica en la que coincidimos el nombre de host de las VM clonadas (secundarias) con el almacenado en el paso anterior para asegurarnos de identificar cuándo la VM clonada (secundarias) obtiene un nombre de host que no es la VM de imagen dorada (que sería el nombre de host final de la máquina) y, a continuación, se inicia el servicio de terminales seguros y se cambia a Automático. También se quita la variable de entorno de la secuencia de comandos mencionada anteriormente. Normalmente, esto se implementa mediante los mecanismos disponibles en la solución de implementación, como VMware. En VMware, puede utilizar parámetros posteriores a la sincronización: https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-E177899E-023D-4E61-B058-AFE3822158AA.html De forma similar para AWS, puede utilizar Scripts de inicio de forma similar: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-windows-user-data.html.

Configuración de VMware Horizon

1. La máquina virtual Golden Image está preparada y todas las aplicaciones necesarias para la implementación inicial del grupo están instaladas en la máquina virtual.
2. Se instala un punto final seguro con esta sintaxis de línea de comandos para incluir el indicador goldenimage. Por ejemplo, <ampinstaller.exe> /R /S /goldenimage 1. Tenga en cuenta que el indicador de imagen dorada garantiza que el servicio de terminal seguro no se ejecute hasta que se produzca un reinicio, lo que es fundamental para que este proceso funcione correctamente. Consulte https://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-endpoints/118587-technote-fireamp-00.html
3. Después de Secure Endpoint Installation, ejecute primero el script VMWareHorizonAMPSetup.bat en la máquina virtual Golden Image. Básicamente, este script cambia el Servicio de terminal seguro a Inicio manual y crea una Variable de entorno

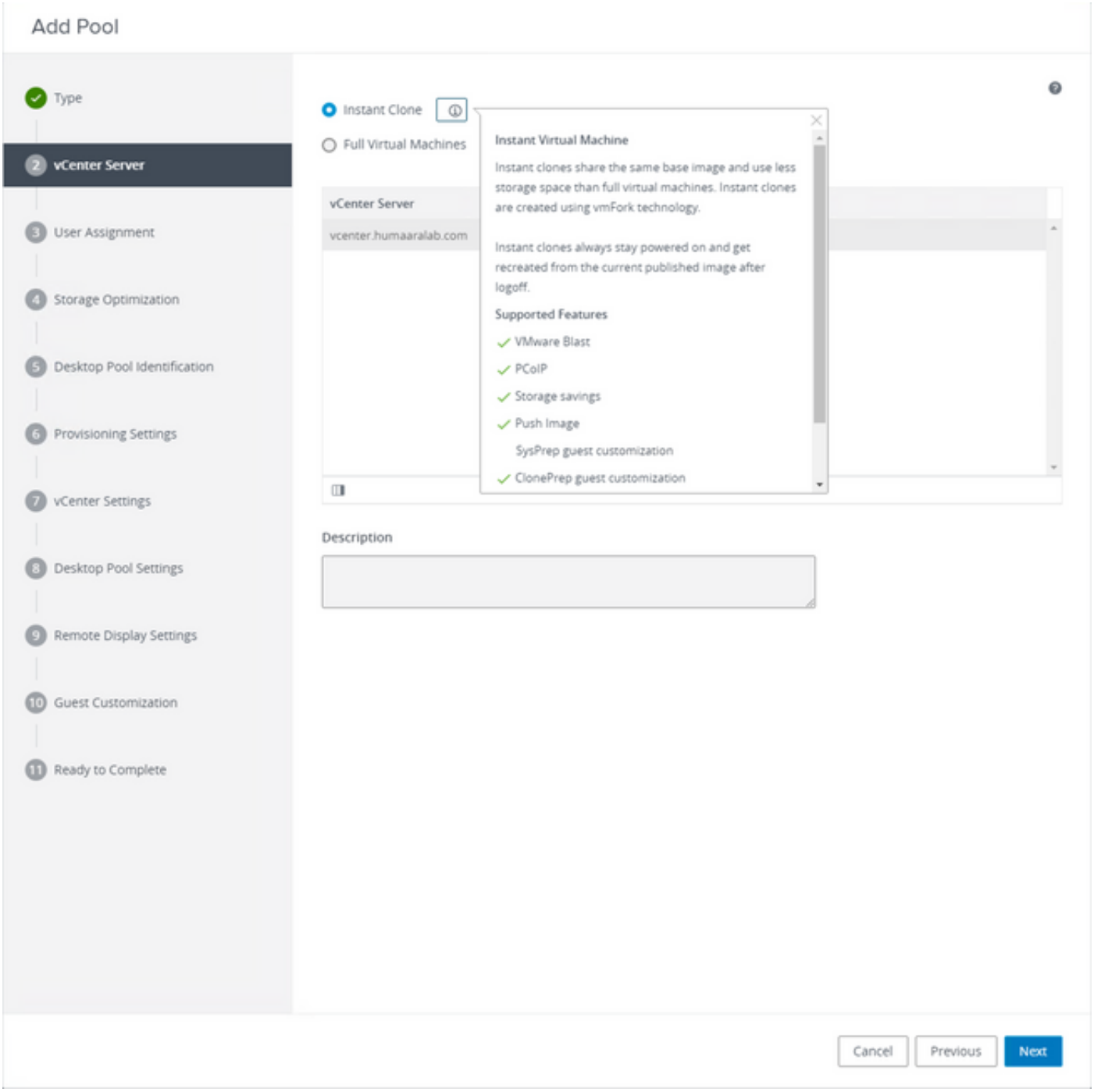
que almacena el Golden Image Hostname para su uso posterior.

4. Debe copiar VMWareHorizonAMPStartup.bat en una ruta universal en la máquina virtual Golden Image como "C:\ProgramData" ya que se utilizaría en los pasos posteriores.
5. La máquina virtual Golden Image ahora se puede apagar y el proceso de composición se puede iniciar en VMware Horizon.
6. Esta es la información paso a paso sobre su aspecto desde la perspectiva de VMware Horizon:



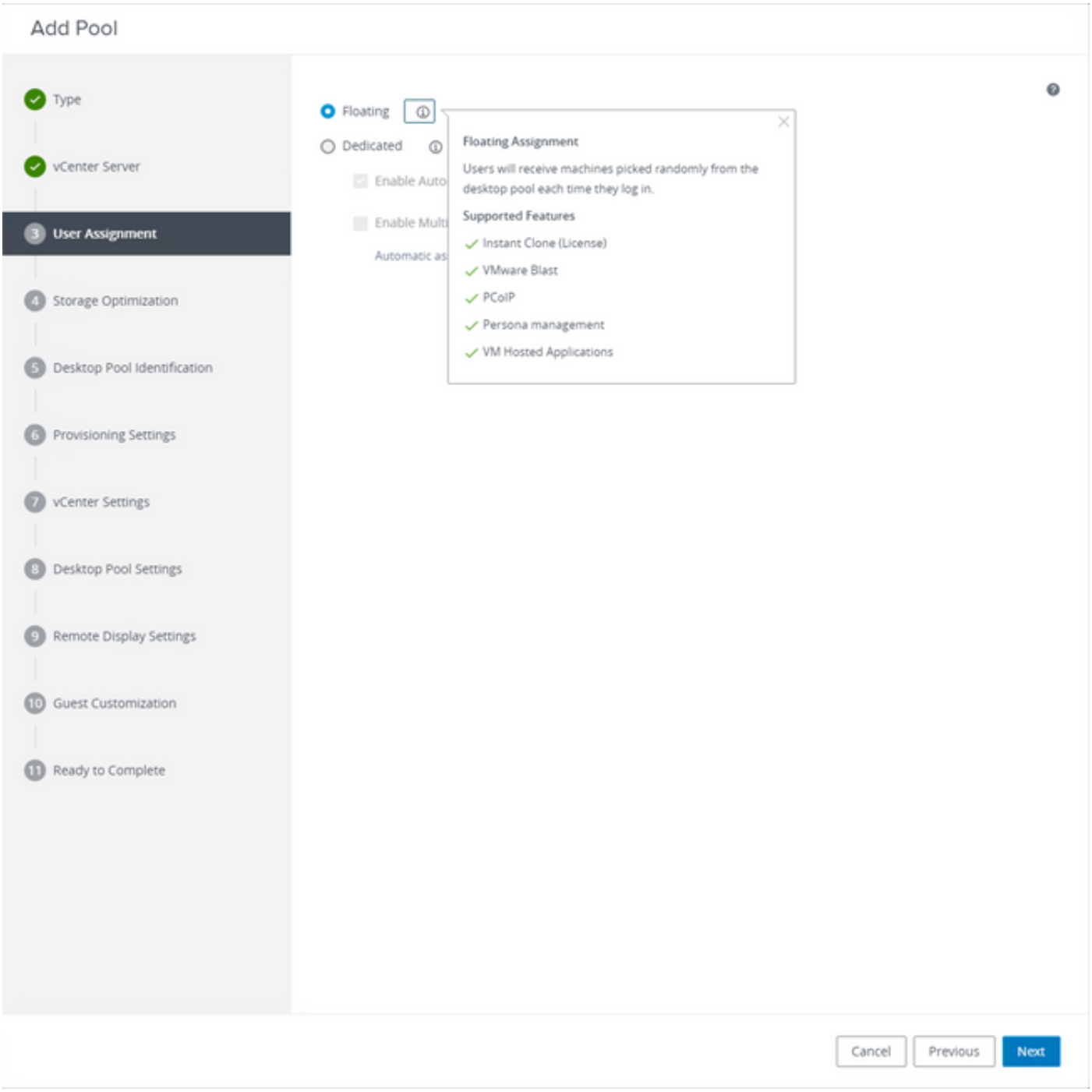
Selección de "Conjunto de escritorios automatizado"

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



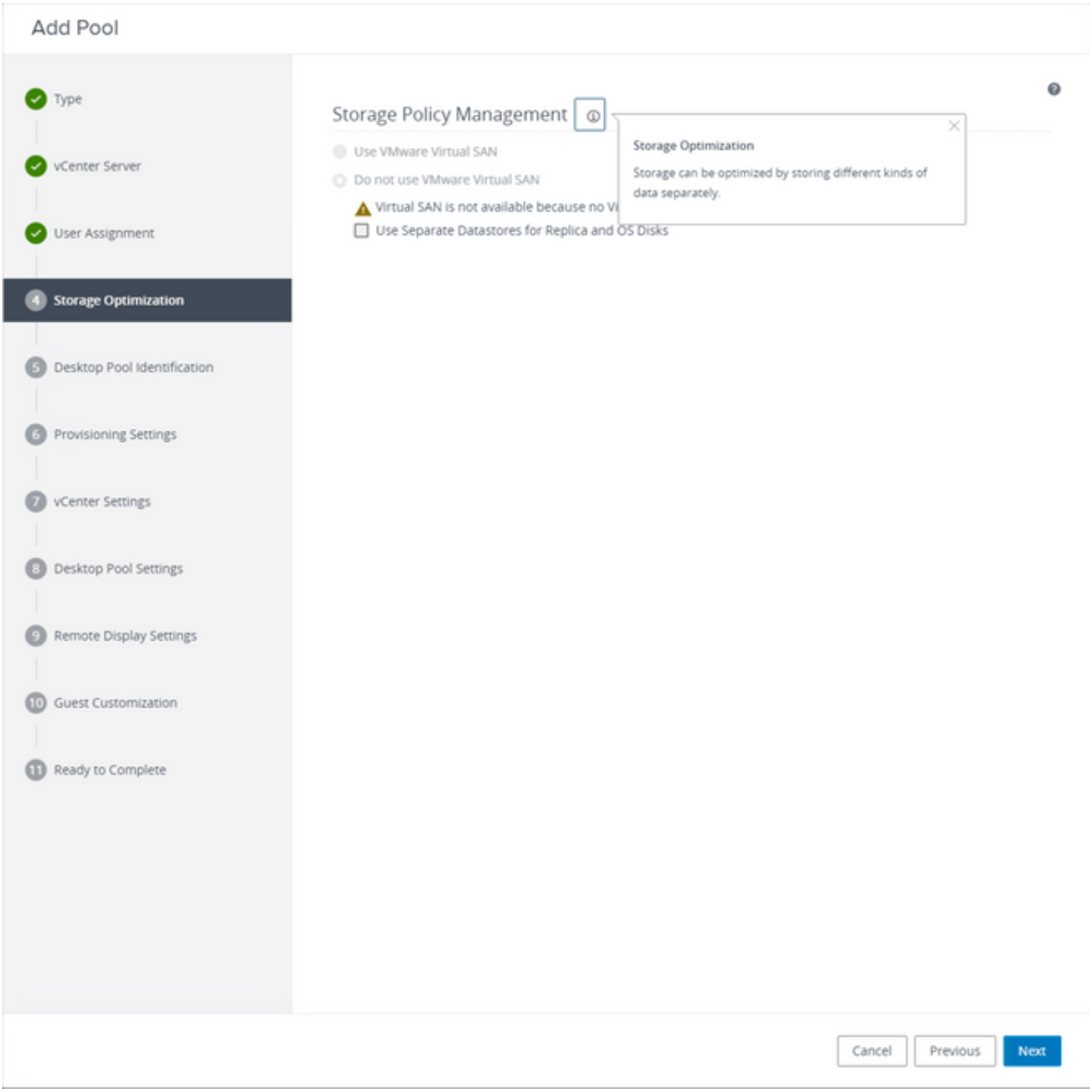
Selección de "Clones instantáneos"

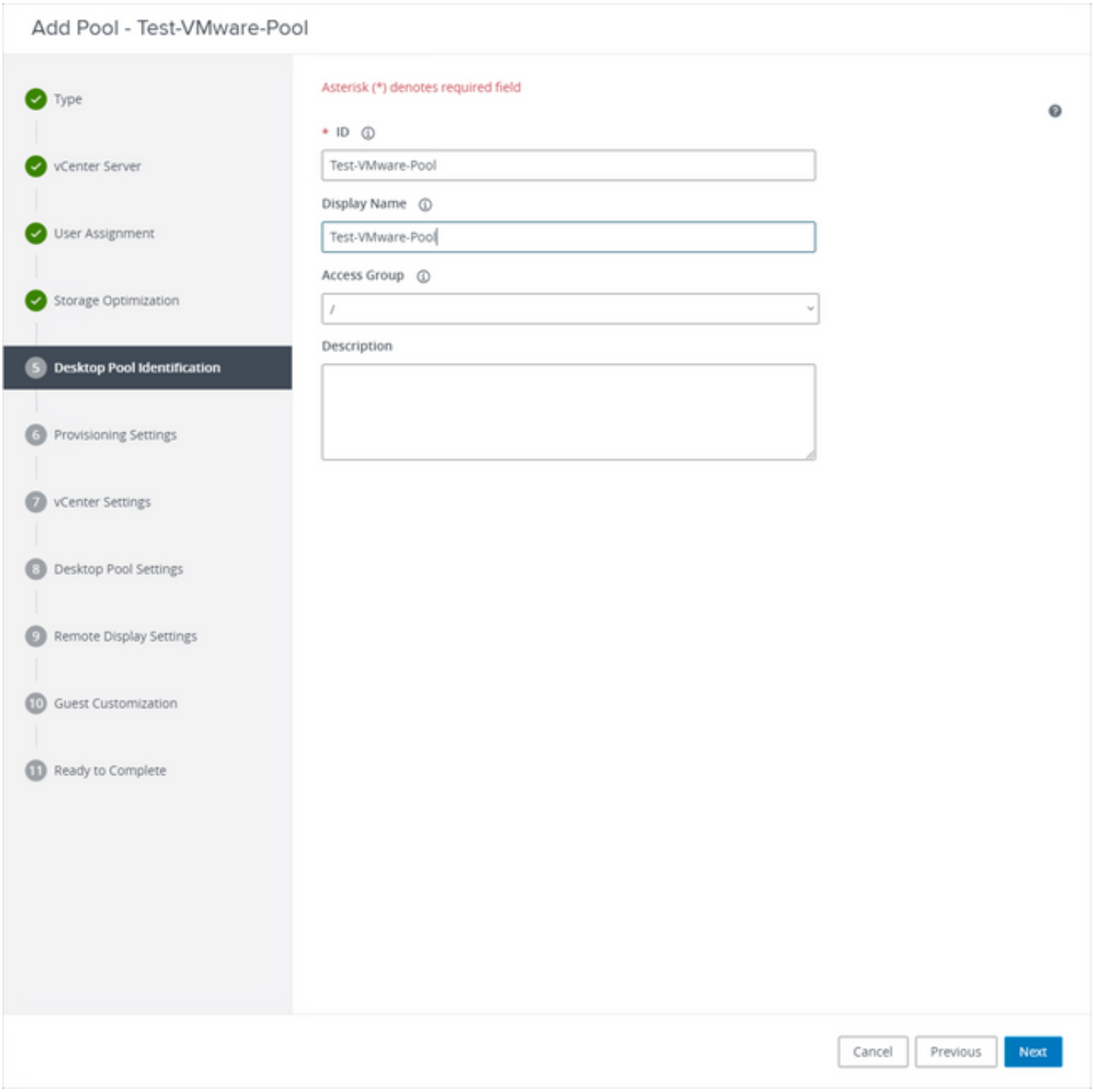
Consulte: https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-D7C0150E-18CE-4012-944D-4E9AF5B28347.html



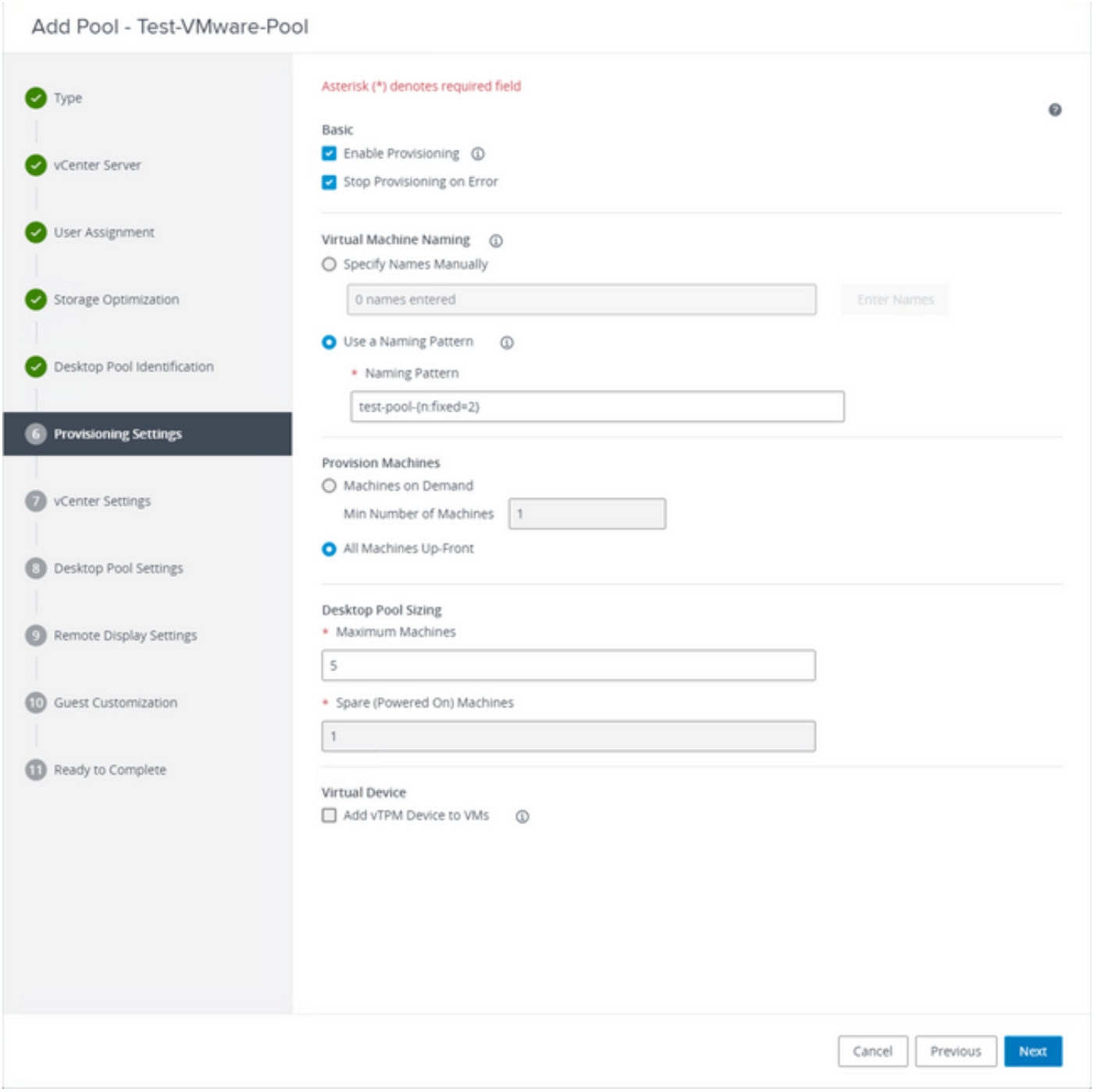
Selección del tipo "Flotante"

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

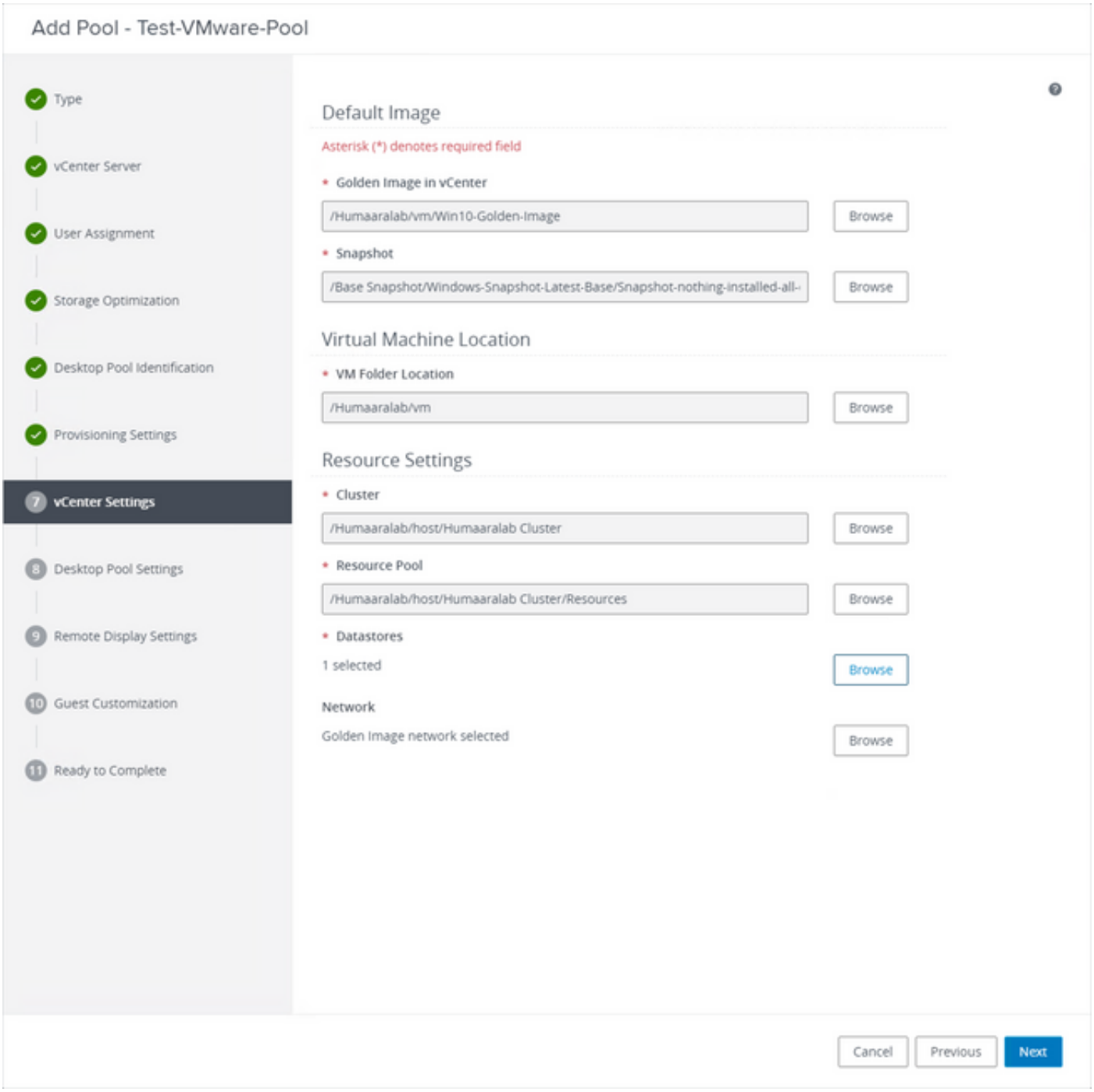

Add Pool
Type
vCenter Server
User Assignment
4 Storage Optimization
5 Desktop Pool Identification
6 Provisioning Settings
7 vCenter Settings
8 Desktop Pool Settings
9 Remote Display Settings
10 Guest Customization
11 Ready to Complete
Storage Policy Management
Use VMware Virtual SAN
Do not use VMware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



Nombres de grupos de escritorios

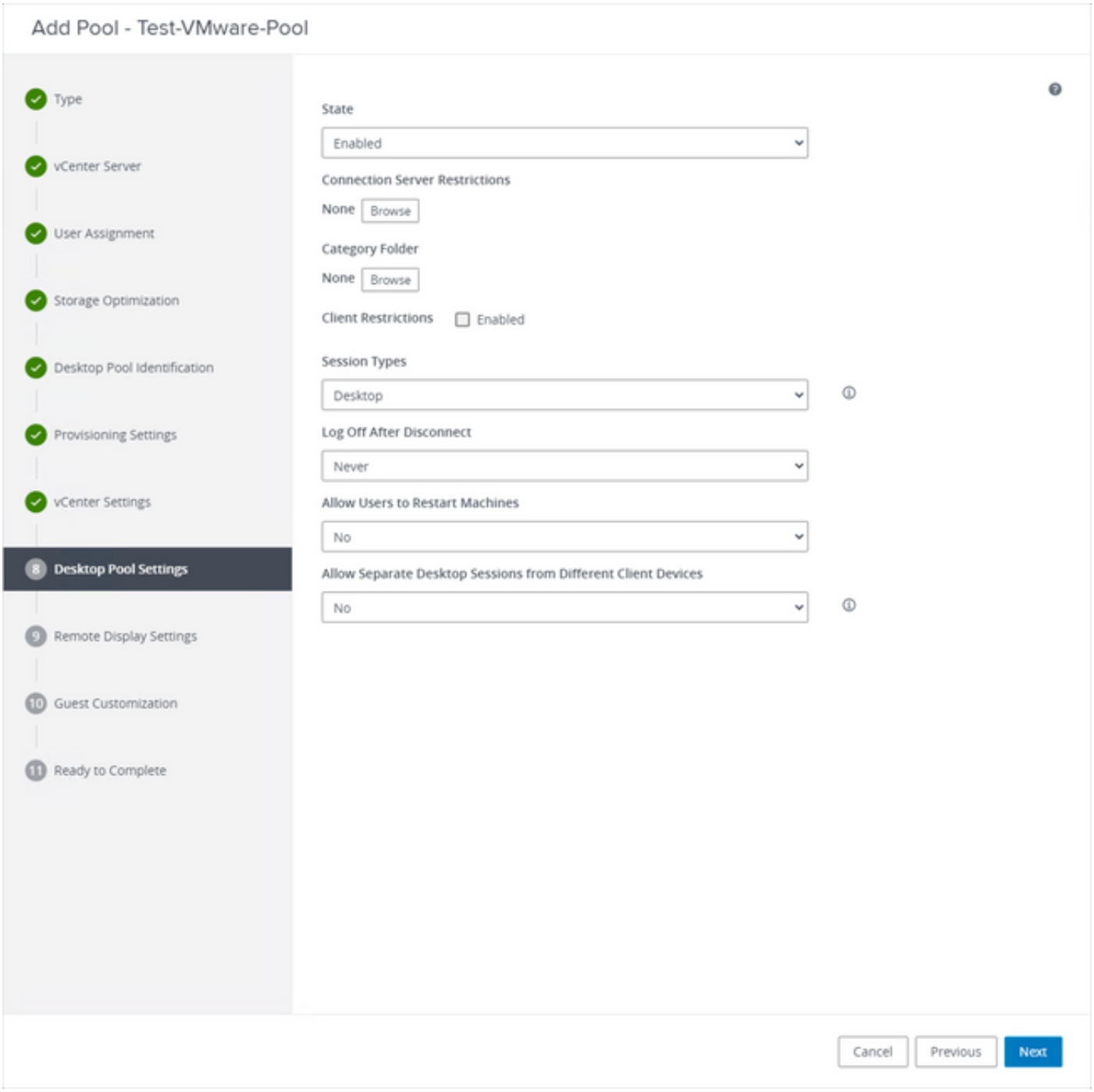


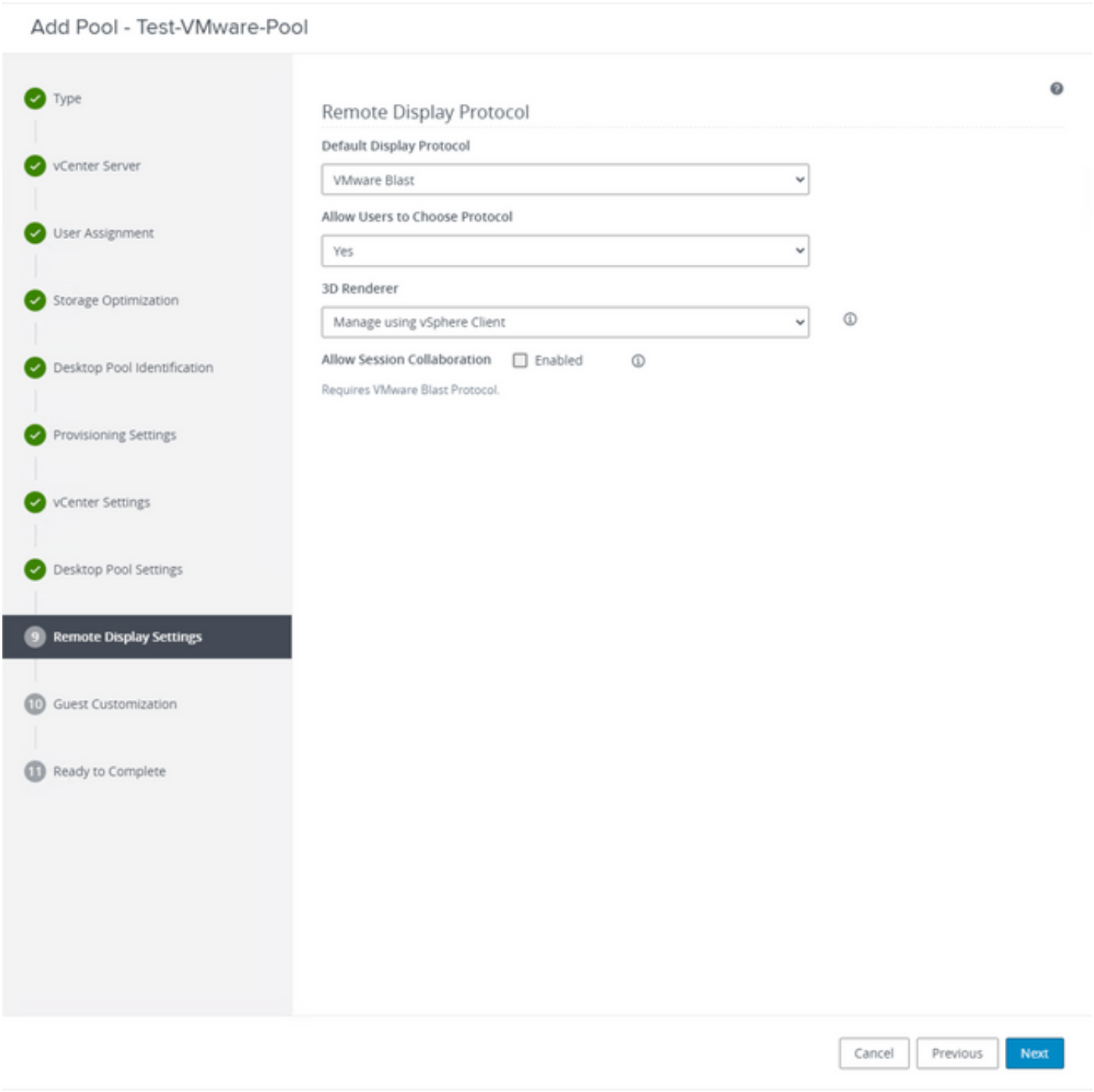
Patrón de nombres de VMware Horizon: https://docs.vmware.com/en/VMware-Horizon/2103/virtual-desktops/GUID-26AD6C7D-553A-46CB-B8B3-DA3F6958CD9C.html

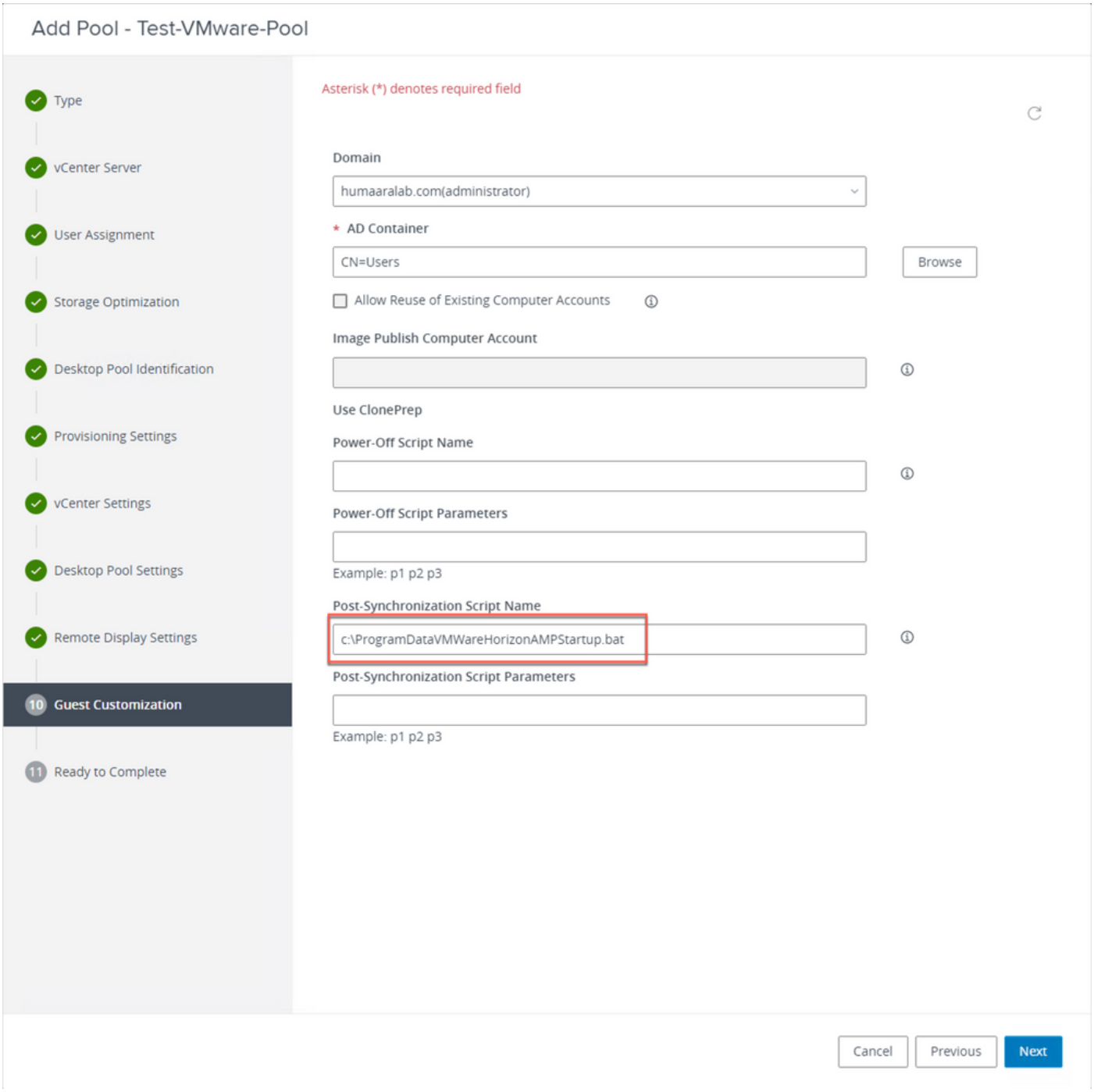


Golden Image: Esta es la máquina virtual de Golden Image.

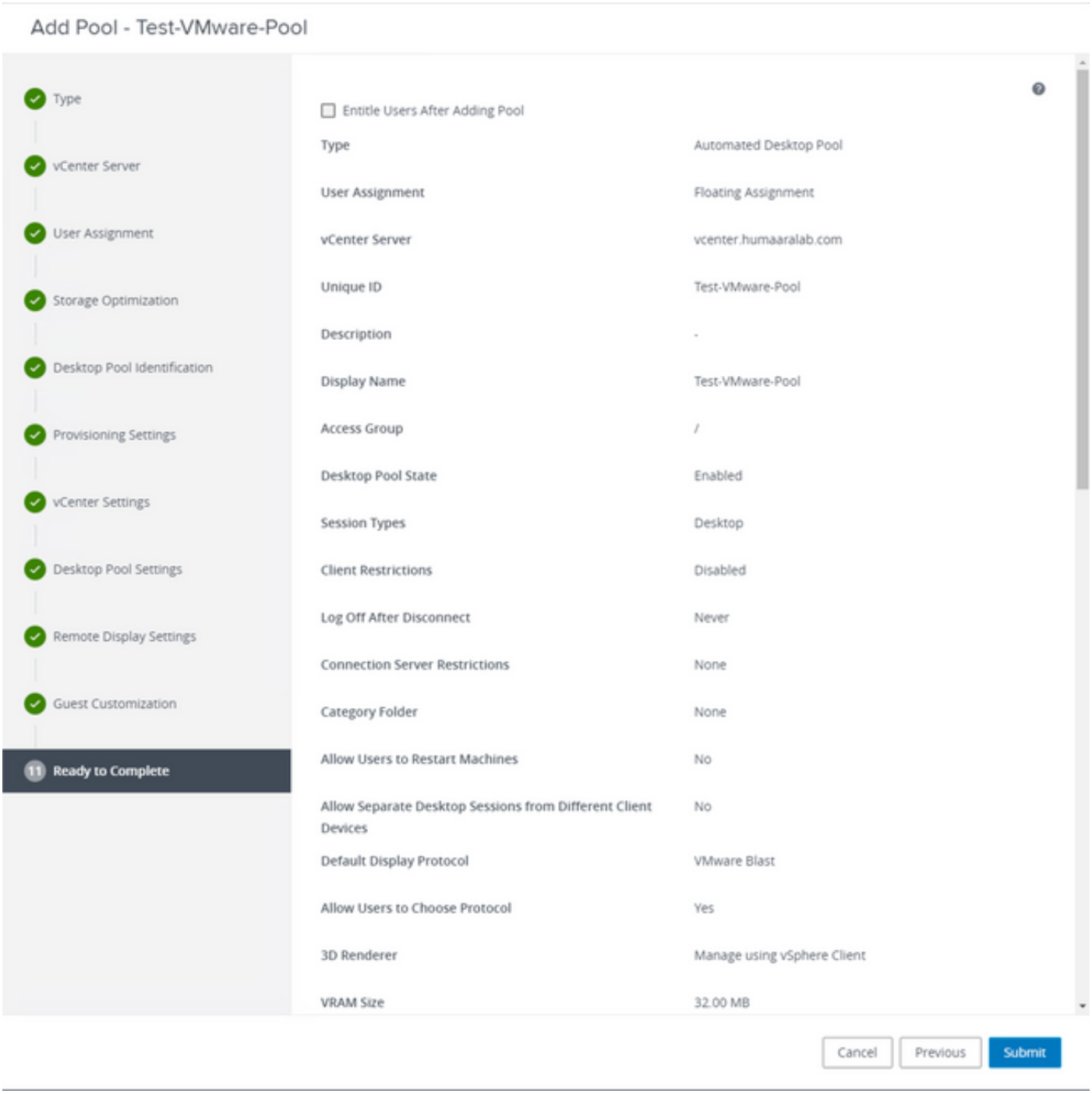
Instantánea: esta es la imagen que desea utilizar para implementar la VM secundaria. Este es el valor que se actualiza cuando se actualiza la imagen dorada con cualquier cambio. El resto son algunos de los parámetros específicos del entorno VMware.


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 se ha mencionado anteriormente, en el paso 10 del asistente es donde se define la ruta del archivo de comandos.



8. Una vez completada y enviada, VMware Horizon comienza la composición y se crean las VM secundarias.

Nota: Consulte la guía de VMware para obtener información sobre estos pasos, pero son autoexplicativos.

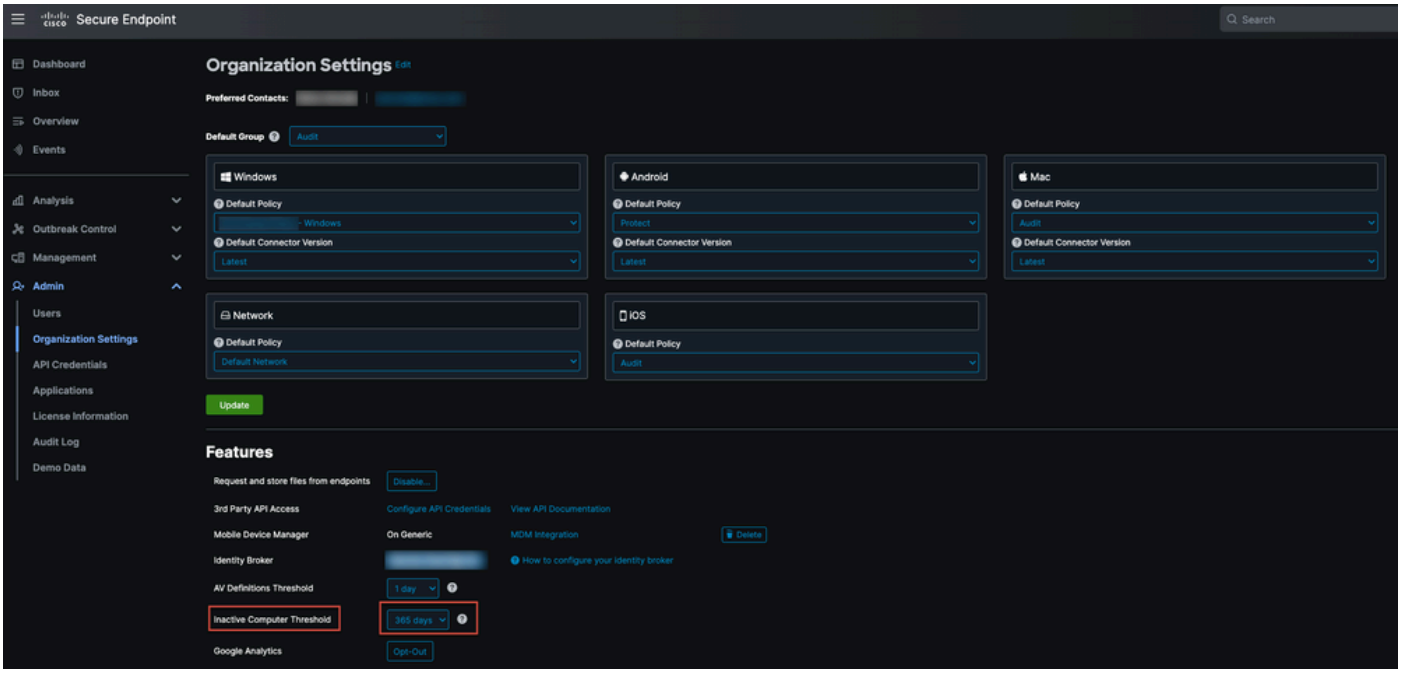
Eliminación de entradas duplicadas

Hay algunas maneras disponibles por las cuales podemos eliminar las entradas duplicadas del conector:

1. Utilice la función de eliminación automática en Secure Endpoint Portal para eliminar las

entradas duplicadas (inactivas):

Podrá encontrar esta configuración en Admin > Organization Settings .



El umbral de equipo inactivo permite especificar cuántos días puede transcurrir un conector sin protegerlo en la nube de Cisco antes de quitarlo de la lista de la página Administración de equipos. El valor predeterminado es 90 días. Los equipos inactivos sólo se quitarán de la lista y los eventos que generen permanecerán en la organización de Secure Endpoint. El equipo volverá a aparecer en la lista si el conector vuelve a protegerse.

2. Utilice los flujos de trabajo de orquestación disponibles: https://ciscosecurity.github.io/sxo-05-security-workflows/workflows/secure-endpoint/0056-remove-inactive-endpoints

3. Utilice el script disponible externamente para eliminar los UUID obsoletos/antiguos: https://github.com/CiscoSecurity/amp-04-delete-stale-guids

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).