在安全终端中配置身份持久性

目录

简介

什么是身份持久性？

- 要求
- 何时需要身份持久性？
  - 虚拟终端部署
  - 物理终端部署

身份持久性流程概述

- 识别组织中的重复项
  - 外部可用的GitHub脚本
- 创建重复项的原因

身份持久性部署不正确的常见问题/症状

部署最佳实践

- 配置snapvol文件
- 门户策略规划
  - 配置
- 黄金映像创建
  - 金色图像覆盖标志
  - 黄金映像创建步骤
  - 更新黄金映像
- 金色图像代码
  - 黄金映像设置脚本
  - 黄金映像启动脚本

AWS Workspace流程

VMware Horizon复制问题

- 不再需要配置/更改
- 脚本方法
- VMware Horizon配置

删除重复条目

简介

本文档介绍如何通过思科安全终端身份持久性功能。

什么是身份持久性？

身份持久化功能允许您在虚拟环境中或计算机重新映像时维护一致的事件日志。您可以将连接器绑定到MAC地址或主机名，这样就不会在每次启动新的虚拟会话或重新映像计算机时都创建新的连接器记录。此功能专为非持久VM和实验室环境设计，不能为传统工作站和服务器设置启用。

要求

Cisco 建议您了解以下主题：

- 访问思科安全终端门户
- 您需要联系思科TAC，让他们在您的组织中启用身份持久功能。
- 仅Windows操作系统(OS)支持身份持久性

何时需要身份持久性？

身份持久性是安全终端上的功能，它有助于在初始连接器注册时识别安全终端，并根据特定连接器的MAC地址或主机名等身份参数将它们与先前已知条目进行匹配。此功能的实施不仅有助于保持正确的许可证数量，而且最重要的是，它允许对非持久系统上的历史数据进行正确的跟踪。

虚拟终端部署

在虚拟部署中，身份持久性最常见的是非持久虚拟桌面基础设施(VDI)部署。VDI主机桌面环境根据最终用户的请求或需求进行部署。这包括不同的供应商，如VMware、Citrix、AWS AMI Golden Image Deployment等。

持续VDI（通常也称为“有状态VDI”）是一种设置，其中每个用户的桌面可唯一自定义，并且从一个会话“持续”到另一个会话。此类虚拟部署不需要身份持久性的功能，因为这些计算机不会定期重新映像。

与可能与安全终端性能交互的所有软件一样，需要对虚拟桌面应用进行可能的例外评估，以最大限度地提高功能并最大程度地减小影响。

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

物理终端部署

有两种方案可用于在安全终端物理计算机上部署身份持久性：

- 在部署或重新映像具有预安装安全终端连接器的黄金映像的物理终端时，必须启用Goldenimage标志。身份持久性可用于避免重新映像计算机实例中的重复，但并非必需。
- 当您使用金牌映像部署或重新映像物理终端并在以后安装安全终端连接器时，可以使用身份持久性，以避免在重新映像计算机的实例中出现重复，但不需要这样做。

身份持久性流程概述

1. 连接器将通过policy.xml文件中的令牌下载，这会将其绑定回云端上的相关策略。
2. 安装连接器，将令牌存储在local.xml中，并且连接器使用有问题的令牌向门户发出POST请求。
3. 云端按照以下操作顺序进行：
   a.计算机检查ID同步策略配置的策略。否则，注册将正常进行。

b.根据策略设置，“注册”会检查现有数据库的主机名或MAC地址。
跨业务：根据设置，会检查所有策略在主机名或MAC上的匹配项。会记录匹配的对象GUID并将其发送回终端客户机。然后，客户端计算机采用UUID并承担以前匹配的主机的任何组/策略设置。这将覆盖安装的策略/组设置。
跨策略：令牌 匹配云端的策略，并仅在该策略内查找具有相同主机名或MAC地址的现有对象。如果存在，则采用UUID。如果没有与该策略关联的现有对象，将创建一个新对象。注意：相同的主机名可能与其他组/策略相关联。
c.如果由于缺少令牌（之前注册、部署实践不佳等）而无法与组/策略进行匹配，则连接器将归入“业务”选项卡下设置的默认连接器组/策略。根据组/策略的设置，它会尝试审核匹配的所有策略（跨业务）、仅相关策略（跨策略），或完全无（无）。 考虑到这一点，通常建议将默认组设置为包含其所需的ID同步设置的组，以便计算机在出现令牌问题时正确进行同步返回。

识别组织中的重复项

外部可用的GitHub脚本

查找重复的UUID:https://github.com/CiscoSecurity/amp-04-find-duplicate-guids

创建重复项的原因

有一些常见实例可能导致在您的终端上看到重复项：

1.如果在VDI池期间执行了以下步骤：

- 在非持久VM/VDI上的初始部署是在禁用身份持久性的情况下完成的（例如，使用金牌图像）。
- 在云中更新策略以启用身份持久性，在白天，身份持久性会在终端上更新策略。
- 计算机将刷新/重新映像（使用相同的金色映像），然后将原始策略重新放置到终端上，而不使用身份持久性。
- 本地策略没有身份持久性，因此注册服务器不会检查以前的记录。
- 此流程会生成重复项。

2.用户在一个组中的策略中部署启用了身份持久性的原始黄金映像，然后从安全终端门户将终端移动到另一个组。然后，它会将原始记录放在“移动到”组中，但是当重新映像/重新部署虚拟机时，会在原始组中创建新副本。

注意：这不是可能引起重复问题的详尽场景列表，而是一些最常见的场景。

身份持久性部署不正确的常见问题/症状

不正确的身份持久性实施可能导致以下问题/症状：

- 连接器底座计数不正确
- 不正确报告的结果
- 设备轨迹数据不匹配
- 审核日志中的计算机名称交换

- 连接器从控制台随机注册和注销
- 连接器无法正确向云报告
- UUID复制
- 计算机名称重复
- 数据不一致
- 重组后计算机注册到默认业务组/策略

- 在策略上启用身份持久性的情况下手动部署。

— 如果通过命令行交换机手动部署终端，并且已经在策略中启用了身份持久性，然后卸载该终端并尝试使用来自不同组/策略的软件包重新安装，则终端将自动切换回原始策略。

- SFC日志的输出，显示在1-10秒内自行启用策略交换机

```
(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
```

如果您尝试安装属于不同组的连接器，还会出现其他副作用。您将在门户中看到，连接器被分配到正确的组，但原始策略错误

这是因为身份持久性(ID SYNC)的工作方式。

一旦连接器完全卸载或使用re-register命令行开关，则没有ID SYNC。在卸载时应看到新的创建日

期和连接器GUID，在重新注册命令时应只看到新的连接器GUID。但是，对于ID SYNC，不可能使用旧GUID和日期进行ID SYNC覆盖。这就是我们“同步”主机的方式。

如果发现此问题，必须通过策略更改进行修复。您需要将受影响的终端移回原始组/策略，并确保策略同步。然后将终端移回所需的组/策略

部署最佳实践

配置snapvol文件

如果您将App Volumes用于VDI基础结构，建议您对snapvol.cfg配置进行这些配置更改

这些排除项必须实施到snapvol.cfg文件中:

路径：

- 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

注册表项：

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

在x64系统上，添加以下内容：

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Immunet保护
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstal
  护

参考资料:

- 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

门户策略规划

以下是您在安全终端门户上实施身份持久性时必须遵循的一些最佳实践：

1.强烈建议为身份持久性终端使用单独的策略/组，以简化分离。

2.如果计划使用终端隔离并实施“危害时将计算机移动到组”操作。目标组还必须启用身份持久性，且只能用于VDI计算机。

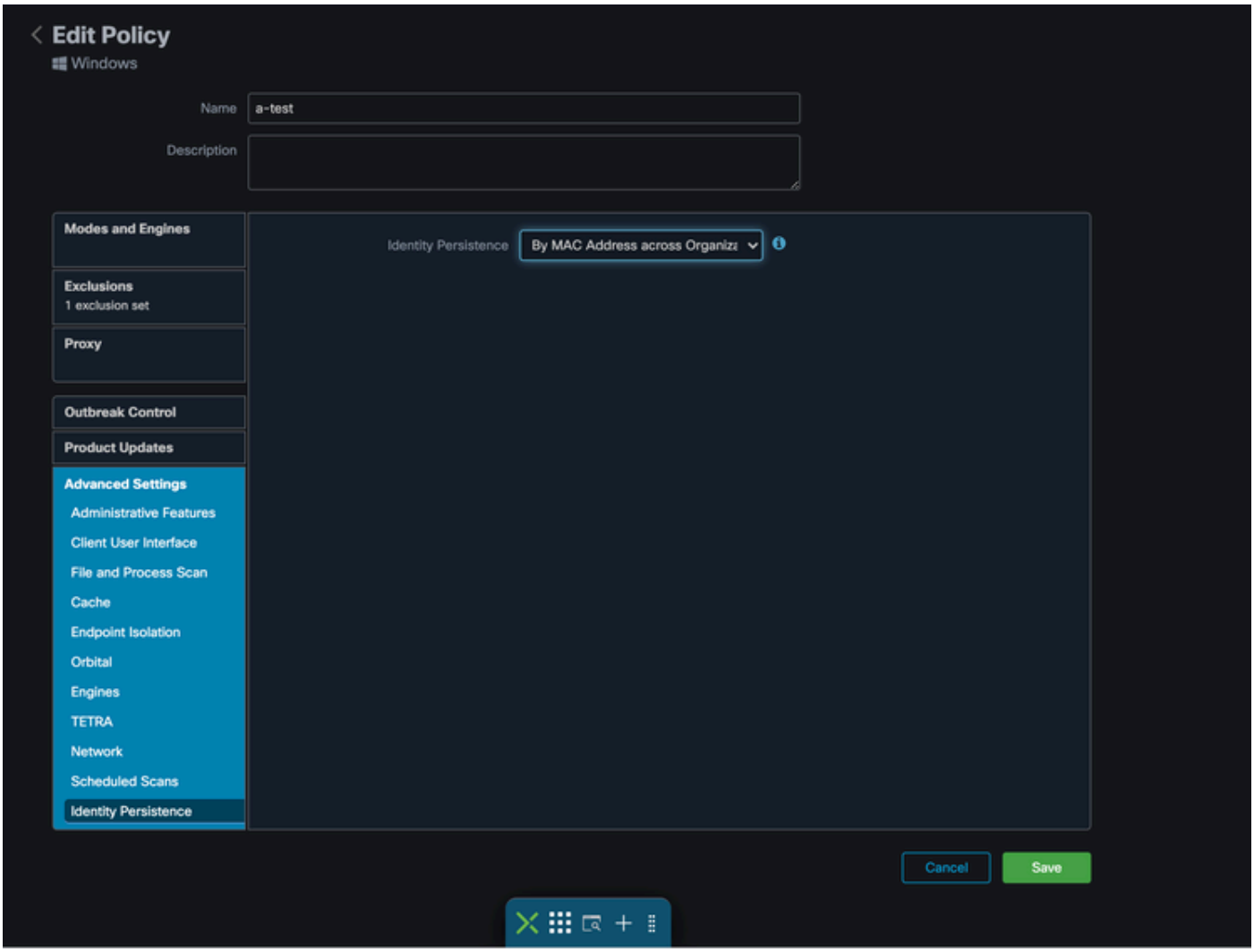
3.建议不要在组织设置上的默认组/策略上启用身份持久性，除非已在所有策略中启用身份持久性，且设置范围为跨组织。

配置

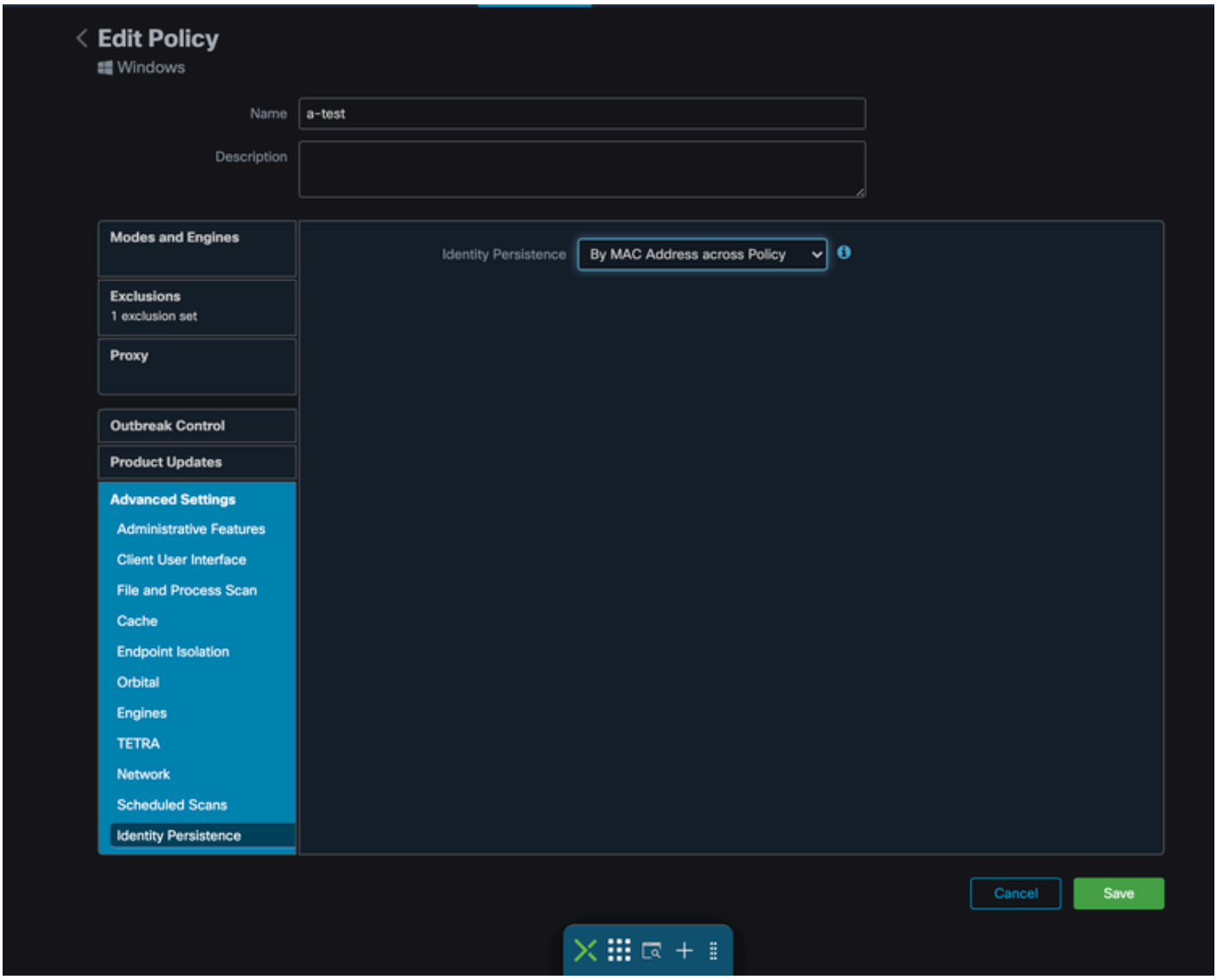
按照以下步骤部署具有身份持久性的安全终端连接器：

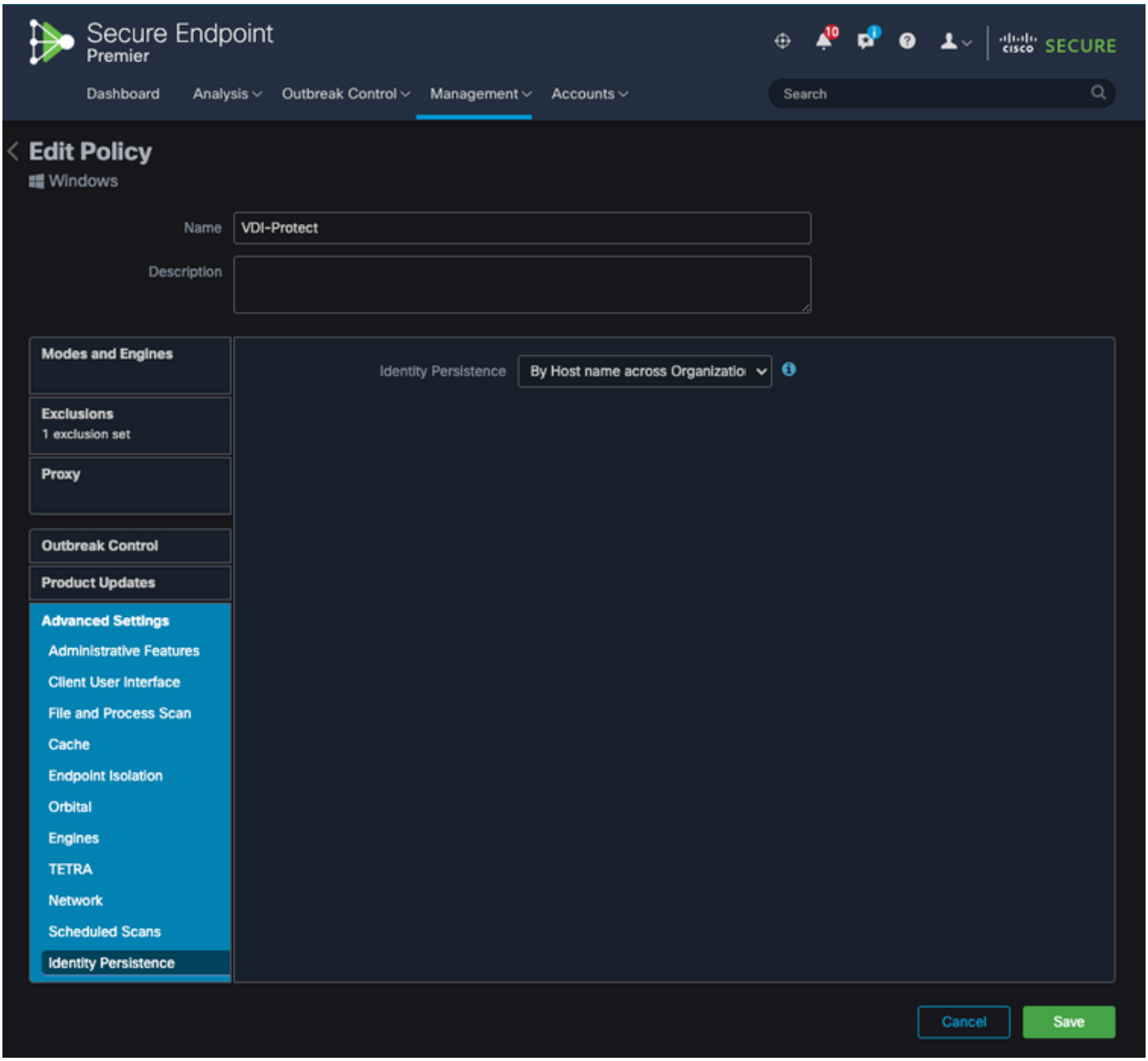
步骤1:将所需的身份持久性设置应用于策略：

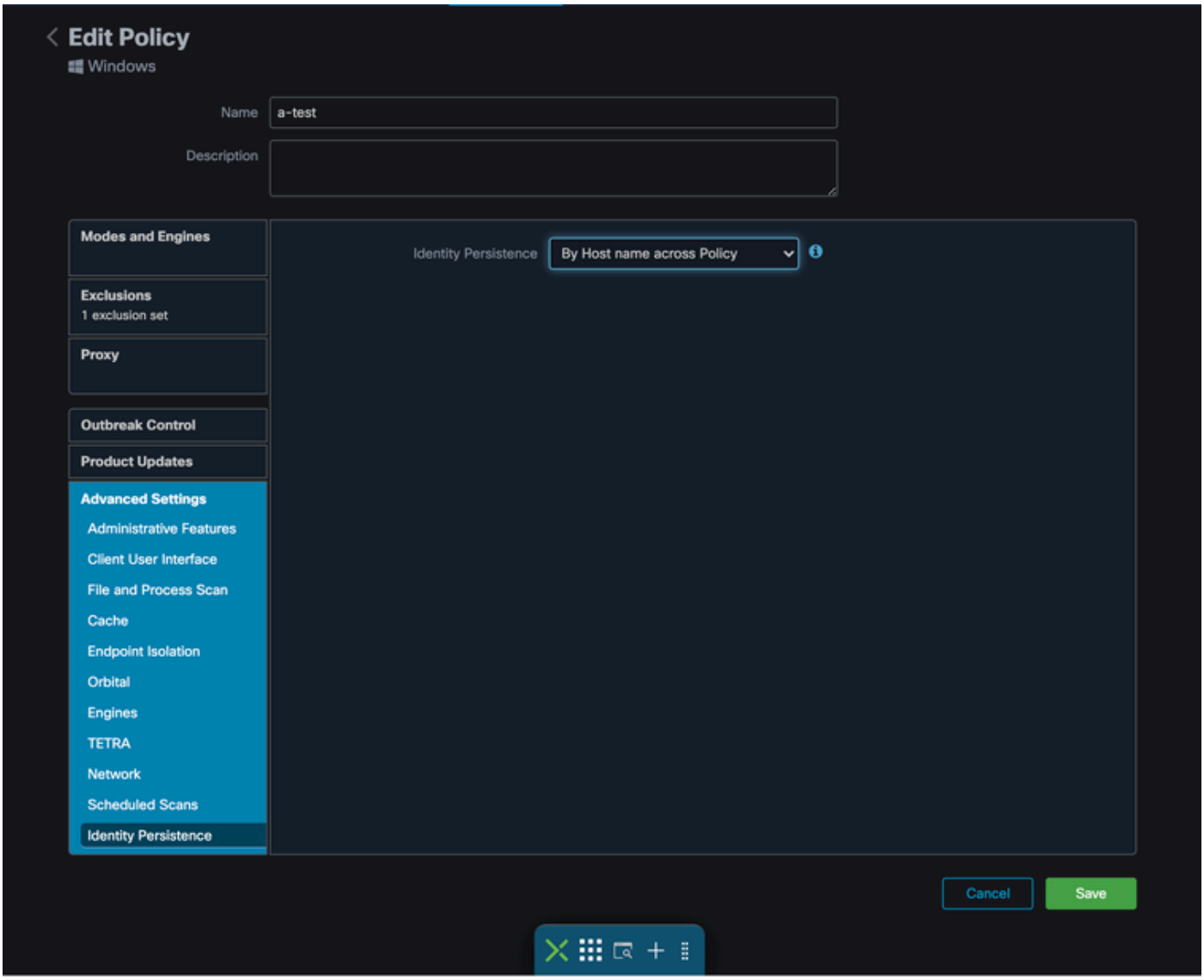
- 在安全终端门户中，导航到管理>策略。
- 选择要启用身份持久性的所需策略，然后单击Edit。
- 导航到Advanced Settingstab，然后点击底部的Identity Persistence选项卡。
- 选择Identity Persistence下拉列表，然后选择对您的环境最有意义的选项。请参阅此图。


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

测试 — 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



有五个选项可供您选择。

- 请注意，功能未启用。在任何情况下，连接器UUID都不会与新连接器安装同步。每次新安装都会生成新的计算机对象。
- 按跨业务的MAC地址：新的或更新的安装会查找具有相同MAC地址的最新连接器记录，以便将以前的历史数据与新的注册同步。此设置查看所有业务记录

  将身份同步设置为除None以外值的所有策略之间。连接器可以更新其策略，以便反映先前的安装（如果它与新的安装不同）。

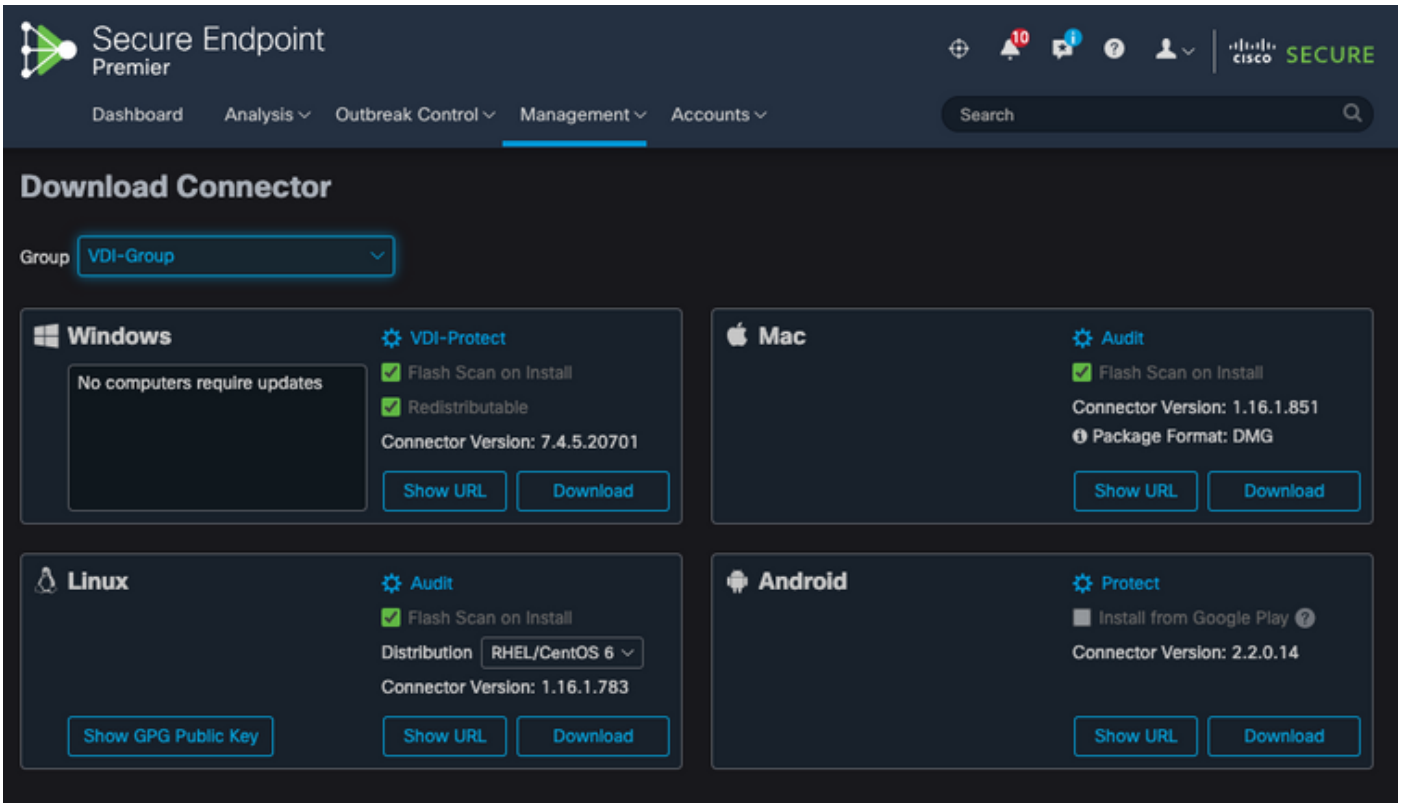
- 跨策略按MAC地址：新的或更新的安装会查找具有相同MAC地址的最新连接器记录，以便将以前的历史数据与新的注册同步。此设置仅查看与部署中使用的策略相关的记录。如果连接器以前未在此策略中安装，但以前在其他策略中处于活动状态，则可以创建重复项。
- 按跨业务的主机名：新的或刷新的安装会查找具有相同主机名的最新连接器记录，以便将以前的历史数据与新的注册同步。此设置将查看所有业务记录，无论其他策略中的身份持久性设置如何，并且连接器可以更新其策略，以反映先前的安装（如果与新安装不同）。主机名包括FQDN，因此，如果连接器经常在网络之间移动（如笔记本电脑），则可能会发生重复。
- 按跨策略的主机名：新的或刷新的安装会查找具有相同主机名的最新连接器记录，以便将以前的历史数据与新的注册同步。此设置仅查看与用于部署的策略相关的记录。如果连接器以前未

在此策略中安装，但以前在其他策略中处于活动状态，则可以创建重复项。主机名包括FQDN，因此，如果连接器经常在网络之间移动（如笔记本电脑），也可能会发生重复。

注意：如果选择使用身份持久性，思科建议您跨业务或策略使用By Hostname。一台计算机有一个主机名，但可以有多个MAC地址，而且许多虚拟机可以克隆MAC地址。

第二步：下载安全终端连接器。

- 导航到管理>下载连接器。
- 为在第1步中编辑的策略选择组。
- 单击Windows Connector的“下载”，如图所示。



第三步：将连接器部署到终端。

- 您现在可以使用下载的连接器在终端上手动安装安全终端（现已启用身份持久性）。
- 否则，您也可以使用金牌图像（请参阅图像）部署连接器

注意：您需要选择可再发行的安装程序。这是一个约57 MB（大小因新版本而异）的文件，包含32位和64位安装程序。要在多台计算机上安装连接器，可以将此文件放在网络共享上，或相应地将其推送到所有计算机。安装程序包含用作安装配置文件的policy.xml文件。

黄金映像创建

创建用于VDI克隆流程的金牌映像时，请遵循供应商文档（VMware、Citrix、AWS、Azure等）中的最佳实践指南。

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

由于您已经确定了VMware，AWS合成流程在虚拟机配置完成之前多次重新启动克隆（子级虚拟机），这会导致安全终端注册流程出现问题，因为此时克隆（子级虚拟机）没有分配最终/正确的主机名，导致克隆（子级虚拟机）使用Golden Image主机名并注册到安全终端云。这会中断克隆过程并导致问题。

这不是安全终端连接器进程的问题，但与克隆进程和安全终端注册不兼容。为了防止出现此问题，我们确定了要在克隆过程中实施的一些更改，这些更改有助于解决这些问题。

这些更改需要在黄金映像VM上实施，然后才会冻结映像进行克隆

1.在安装安全终端时，请始终在金色映像上使用Goldenimage标志。

2.实施Golden Image Setup Script和Golden Image Startup Script部分，以查找仅在克隆（子VM）上实施最终主机名时才会帮助打开终端服务的脚本。有关详细信息，请参阅VMware Horizon复制问题部分。

金色图像覆盖标志

使用安装程序时，用于黄金图像的标志是/goldenimage 1。

金色图像标志可防止连接器在基础图像上启动和注册；因此，在图像的下一个开始处，连接器处于由分配给它的策略所配置的功能状态。

有关其他标志的信息，您可以使用，请参阅本文。

使用安装程序时，用于金色图像的新标志为/goldenimage [1|0]

0 — 默认值 — 此值不会触发golden image选项，并且其运行方式与安装程序运行时完全没有该选项一样。安装时请勿跳过初始连接器注册和启动。

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

1 — 安装为黄金映像。这是与标志一起使用的典型选项，也是唯一的预期用途。跳过初始连接器注册和在安装时启动。

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

黄金映像创建步骤

最佳实践是最后安装连接器，以准备Golden Image。

1. 根据您的要求准备Windows映像；安装除连接器之外的所有必需软件和配置Windows映像。
2. 安装Cisco Secure Endpoint连接器。

使用/goldenimage 1标志向安装程序指示这是黄金映像部署。

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

3.实施脚本逻辑（如果需要），如下文所述

4.完成安装

5.冻结您的黄金形象

安装金牌映像后，系统已预装，安全终端已安装/goldenimageflag，主机已准备好冻结和分发。克隆主机启动后，安全终端会启动并注册到云。配置连接器无需执行其他操作，除非您要对策略或主机进行更改。如果在金色映像完成注册后进行了更改，则必须重新启动该过程。 该标志防止连接器在基础图像上启动和注册。在映像的下一个开始处，连接器将处于为其分配的策略所配置的功能状态。

注意：如果黄金映像在您可以冻结VM之前注册到Secure EndpointCloud，则建议在Golden Image VM上卸载并重新安装Secure Endpoint，然后再次冻结VM，以防止注册和重复连接器问题。在此卸载过程中，建议不要修改安全终端的任何注册表值。

更新黄金映像

在需要更新金牌图像以保留未注册连接器时，有两个选项。

推荐的流程

1. 卸载连接器。
2. 安装主机更新/升级。
3. 使用金色图像标志在金色图像处理之后重新安装连接器。
4. 如果执行了此过程，则主机不应启动连接器。
5. 冻结图像。
6. 在启动克隆之前，验证黄金映像未注册到门户以防止不需要的重复主机。

替代流程

1. 确保主机没有连接到Internet以防止连接器注册。
2. 停止连接器服务。
3. 安装更新.
4. 更新完成后，冻结映像
5. 需要防止连接器注册，以防止出现重复主机。当您删除连接时，会阻止其向云注册连接。此外，被停止的连接器会一直保持该状态，直到下次重新启动为止，这允许克隆注册为唯一主机。

6. 在启动克隆之前，验证黄金映像未注册到门户以防止不需要的重复主机。

金色图像代码

此部分包括代码片段，可帮助支持金色图像处理，并有助于在实施身份持久性时防止连接器重复。

黄金映像设置脚本

安装脚本说明

第一个脚本“设置”在克隆黄金映像之前在黄金映像上执行。只需手动执行一次。其主要目的是建立初始配置，以允许以下脚本在克隆虚拟机上正确运行。这些配置包括：

- 将思科安全终端服务启动更改为手动以避免自动启动。
- 创建在系统启动时以最高权限执行以下脚本（启动）的计划任务。
- 创建名为“AMP_GOLD_HOST”的系统环境变量，以存储Golden Image的主机名。启动脚本将使用此命令来验证我们是否必须恢复更改

设置脚本代码

```
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 /
```

安装脚本代码非常简单：

第2行：将恶意软件防护服务的启动类型更改为手动。

第5行：创建名为“AMP_GOLD_HOST”的新环境变量，并在其中保存当前计算机的主机名。

第9行：创建名为“Startamp”的计划任务，该任务在系统启动期间以最高权限运行指定的“Startup”脚本，无需密码。

黄金映像启动脚本

启动脚本说明

第二个脚本“启动”在克隆虚拟机的每个系统启动上运行。其主要目的是检查当前计算机是否具有“Golden Image”的主机名：

- 如果当前计算机是黄金映像，则不执行任何操作，脚本将结束。由于我们维护了计划任务，因

此安全终端将在系统启动时继续运行。

- 如果当前计算机不是“Golden”映像，则会重置第一个脚本所做的更改：
  - 将思科安全终端服务启动配置更改为自动。
  - 正在启动思科安全终端服务。
  - 删除“AMP_GOLD_HOST”环境变量。
  - 删除执行启动脚本的计划任务，并删除脚本本身。

启动脚本代码

```
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
```

第2行：将当前主机名与存储的“AMP_GOLD_HOST”值进行比较；如果它们相同，则脚本跳至“相同”标签，否则跳至“不相同”标签。

第4-6行：当到达“相同”标签时，脚本不会执行任何操作，因为它仍然是“黄金图像”，并继续进入“退出”标签。

第8-16行：如果到达“notsame”标签，脚本将执行以下操作：

- 将恶意软件防护服务的启动类型更改为自动。
- 启动恶意软件防护服务。
- 删除“AMP_GOLD_HOST”环境变量。
- 删除名为“Startamp”的计划任务

注意：请注意，TAC不正式支持本文档中包含的脚本。

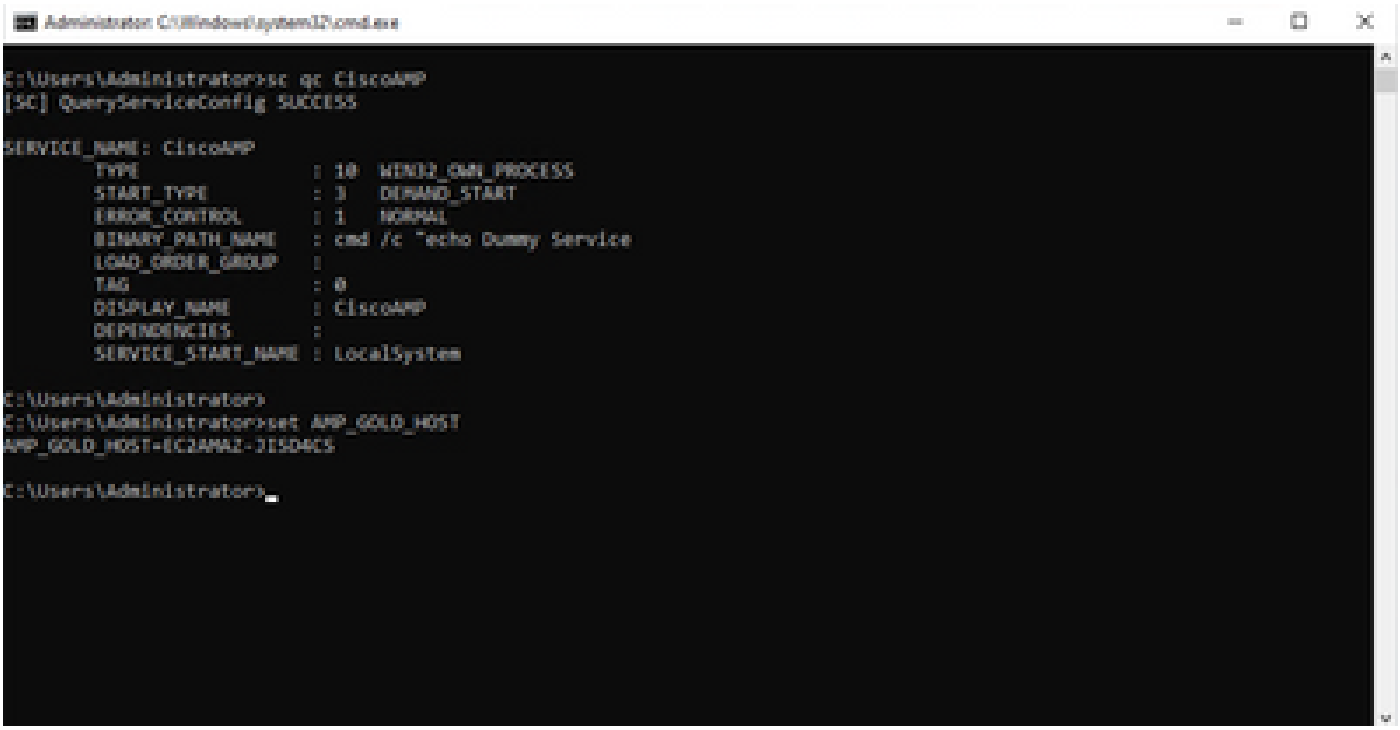
注意：这两个脚本允许在克隆虚拟机环境中启动Cisco AMP服务。通过正确配置黄金映像并使用启动脚本，它可确保思科安全终端在所有克隆虚拟机上以正确配置运行。

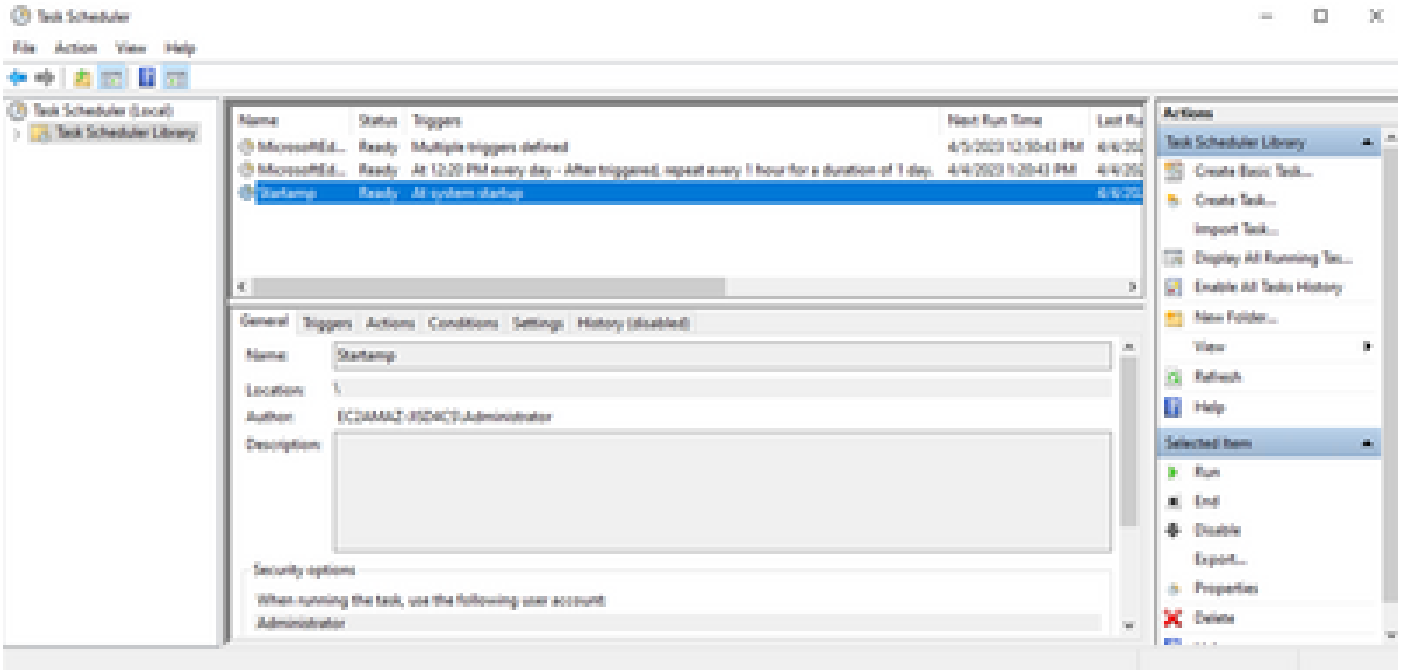
AWS Workspace流程

此解决方案包括克隆之前在金牌映像上执行的“设置”脚本和在系统启动期间在每个克隆虚拟机上运行的“启动”脚本。这些脚本的主要目标是确保正确配置服务，同时减少手动干预。这两个脚本允许在克隆虚拟机环境中启动思科安全终端服务。通过正确配置黄金映像和使用启动脚本，它可确保Cisco安全终端连接器在所有克隆虚拟机上以正确配置运行

有关在AWS Workspace上实施Golden Image所需的脚本代码，请参阅Golden Image Setup Script Code和Golden Image Startup Script Code部分。

执行设置脚本后，我们可以验证配置更改已成功部署。





由于我们在黄金映像上执行了此操作，所有新实例都将具有此配置，并在启动时执行启动脚本。

VMware Horizon复制问题

使用VMware Horizon，我们可以确定，作为Horizon合成过程的一部分，在创建子虚拟机时会多次重新引导它们。这会导致以下问题：当子VM未准备就绪时，安全终端服务启用（它们没有分配最终/正确的NetBios名称）。这会导致安全终端出现更多问题，从而导致流程中断。为避免遇到此问题，我们针对此与Horizon进程的不兼容性提出了一种解决方案，其中包括在Golden Image VM上实施附加的脚本，并使用VMware Horizon的同步后脚本功能：https://docs.vmware.com/en/VMware-Horizon/2103/published-desktops-applications.pdf。

不再需要配置/更改

- 如果要在首次部署后对金牌映像进行任何更改，则不再需要卸载并重新安装安全终端。
- 无需将安全终端服务设置为延迟启动。

脚本方法

下面提供了脚本示例。

- Golden Image Setup Script：必须按照之前所述安装安全终端连接器以及前面所述的标记实施此脚本。此脚本将Secure Endpoint服务修改为手动启动，并将Golden Image Hostname另存为环境变量，以供下一步参考。

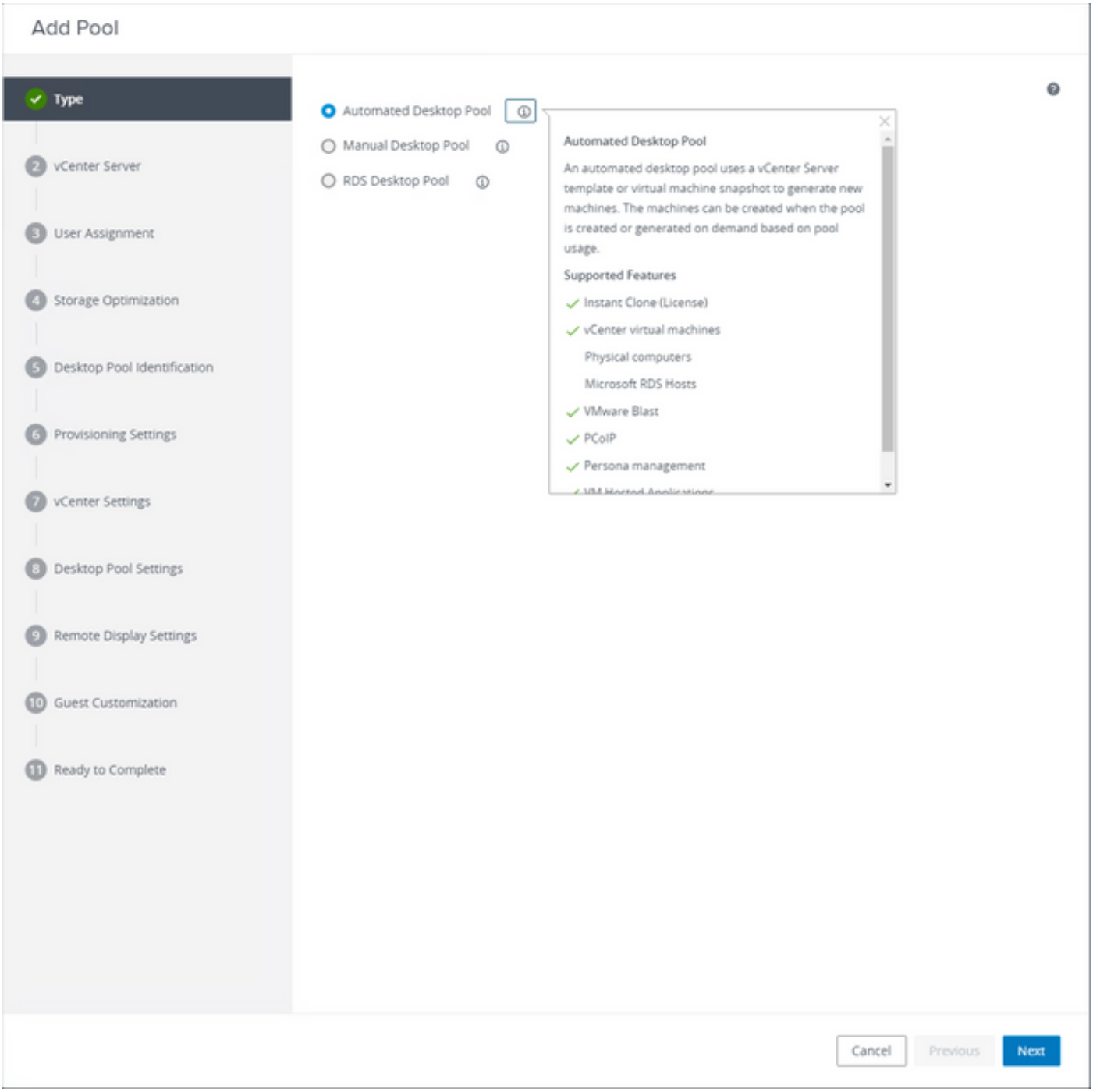
- Golden Image启动脚本：此脚本是一个逻辑检查，其中我们将克隆（子）虚拟机的主机名与前一步中存储的主机名进行匹配，以确保我们确定克隆（子）虚拟机何时获取除Golden Image VM以外的任何主机名（即计算机的最终主机名），然后启动安全终端服务并将其更改为“自动”。您也可以从前面提到的脚本中删除环境变量。这通常是通过使用部署解决方案（如VMware）提供的机制实现的。在VMware上，您可以使用同步后参数：https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-E177899E-023D-4E61-B058-AFE3822158AA.html 对于AWS，您也可以以类似的方式使用启动脚本：https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-windows-user-data.html。

VMware Horizon配置

1. Golden Image VM已预装，且池初始部署所需的所有应用均已安装在VM上。
2. 安全终端将使用此命令行语法安装，以包含goldenimage标志。例如，<ampinstaller.exe> /R /S /goldenimage 1。请注意，黄金映像标志可确保安全终端服务在重新启动之前不会运行，重新启动对于此流程正常运行至关重要。请参阅 https://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-endpoints/118587-technote-fireamp-00.html
3. 安装安全终端后，首先在Golden Image VM上执行VMWareHorizonAMPSetup.bat脚本。实质上，此脚本将安全终端服务更改为手动启动，并创建存储黄金映像主机名的环境变量供以后使用。
4. 您需要将VMWareHorizonAMPStartup.bat复制到Golden Image VM上的通用路径，如

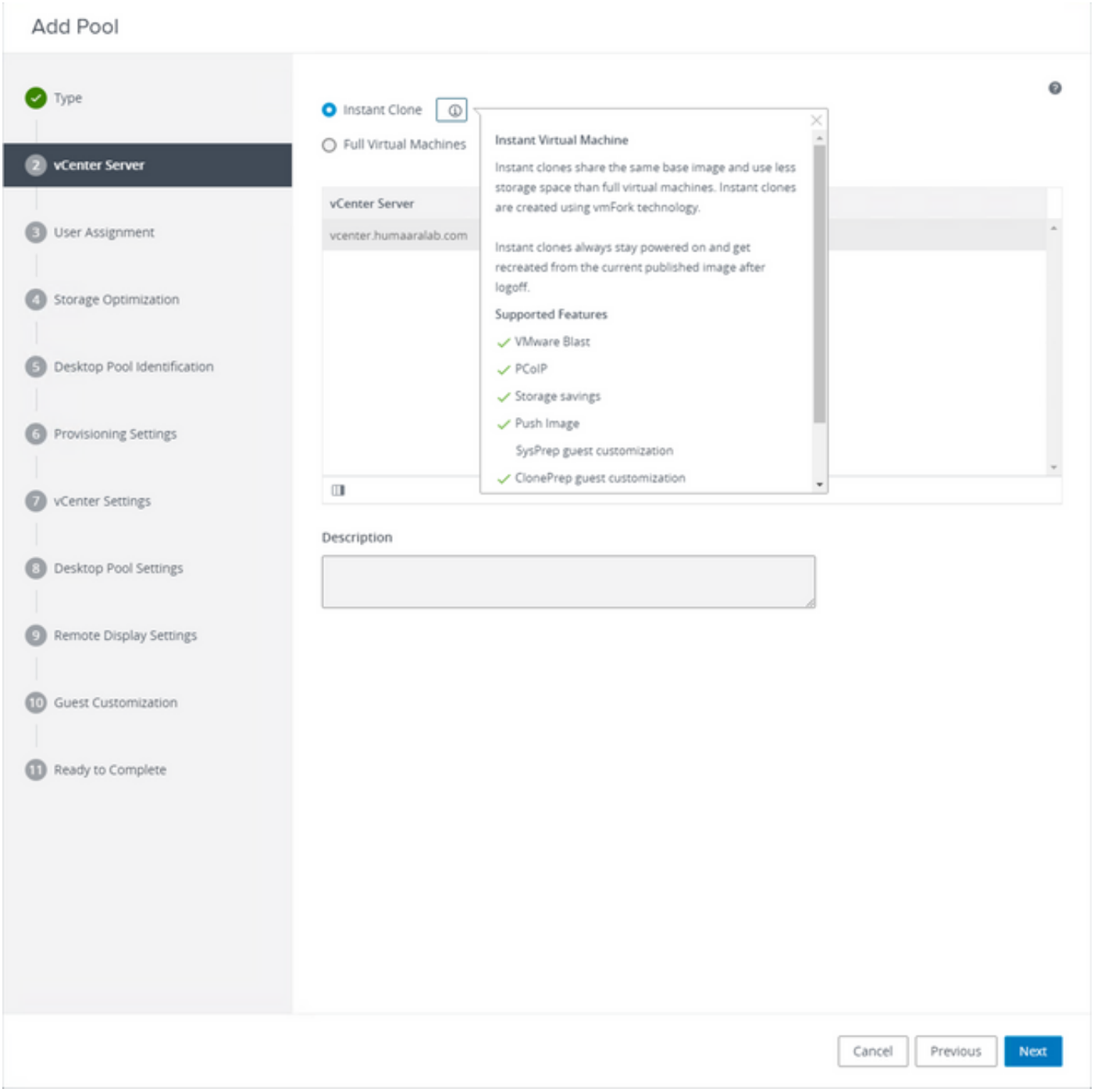
“C:\ProgramData”，因为后面的步骤中将使用此路径。

5. 黄金映像VM现在可关闭，并且组合过程可在VMware Horizon上启动。
6. 下面是从VMware Horizon角度来看它的逐步显示信息：



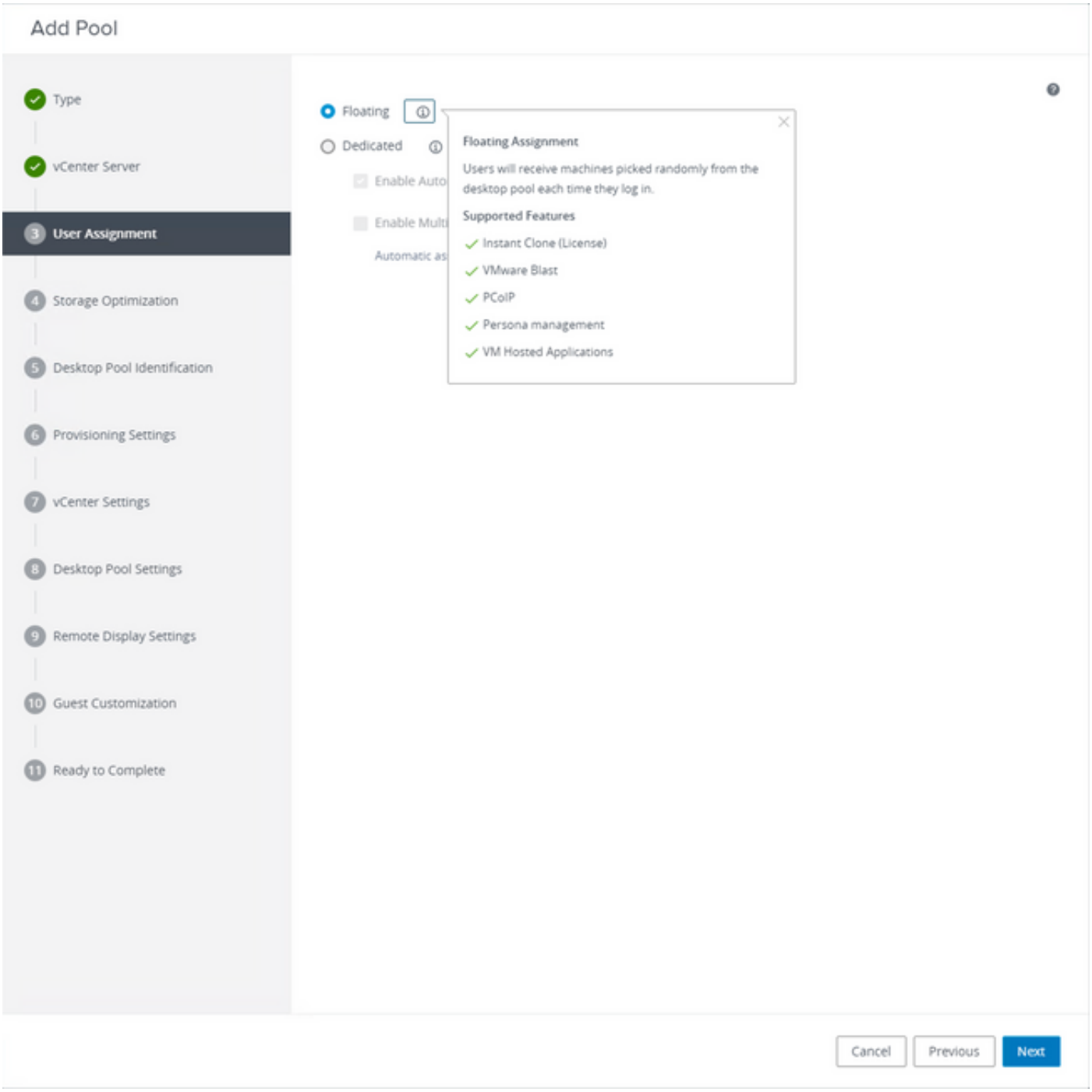
选择“Automated Desktop Pool”

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



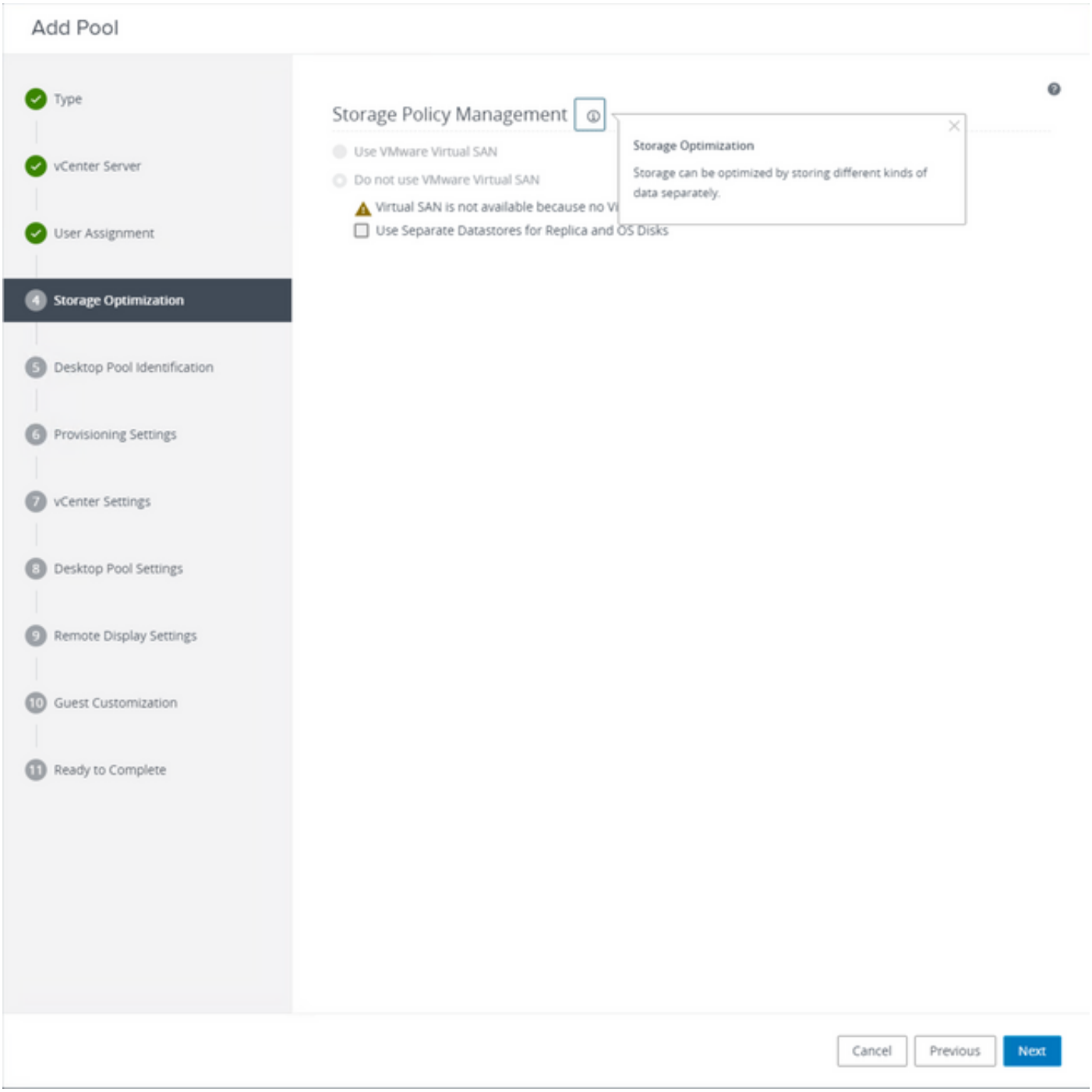
选择“即时克隆”

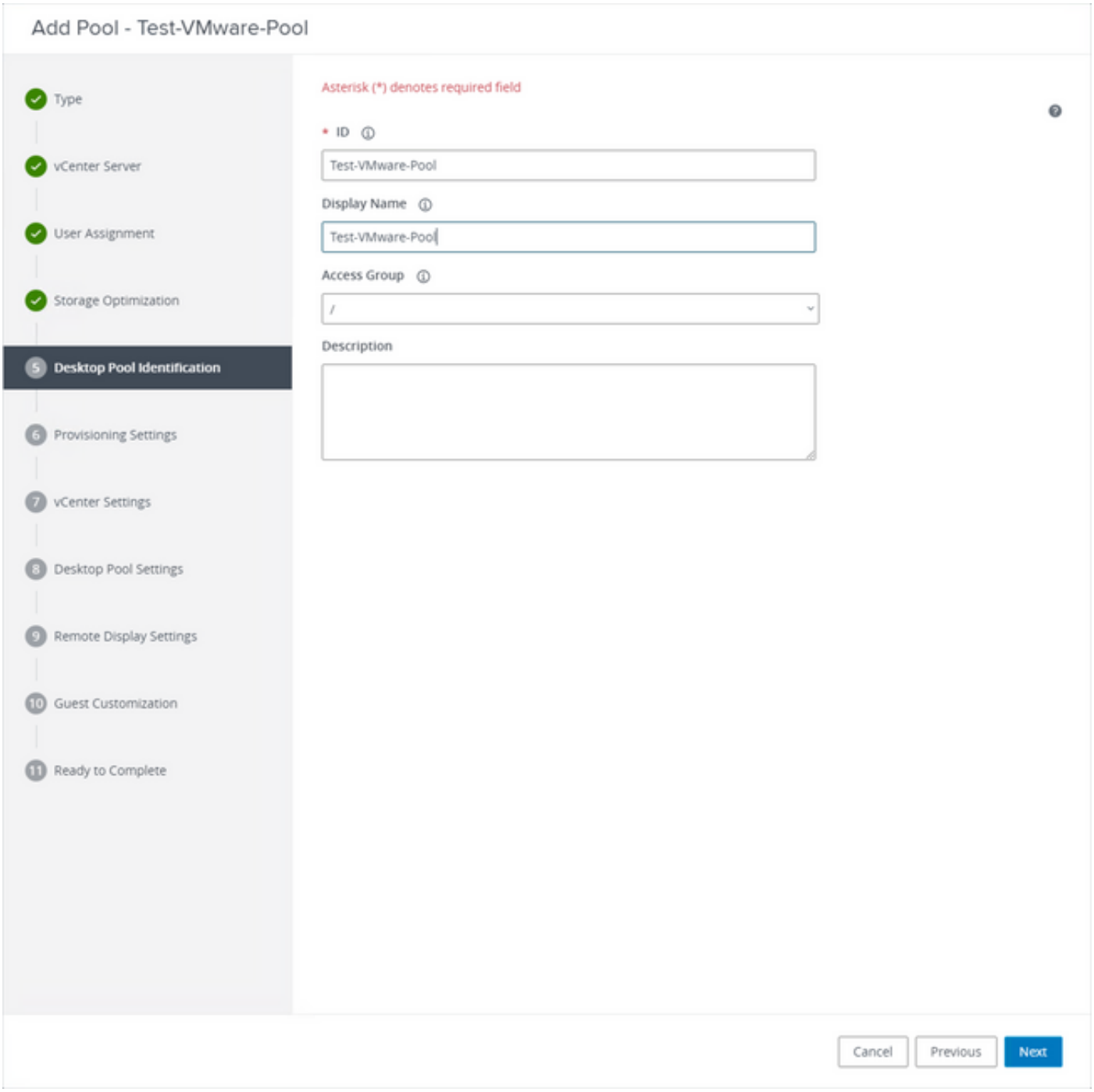
请参阅：https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-D7C0150E-18CE-4012-944D-4E9AF5B28347.html



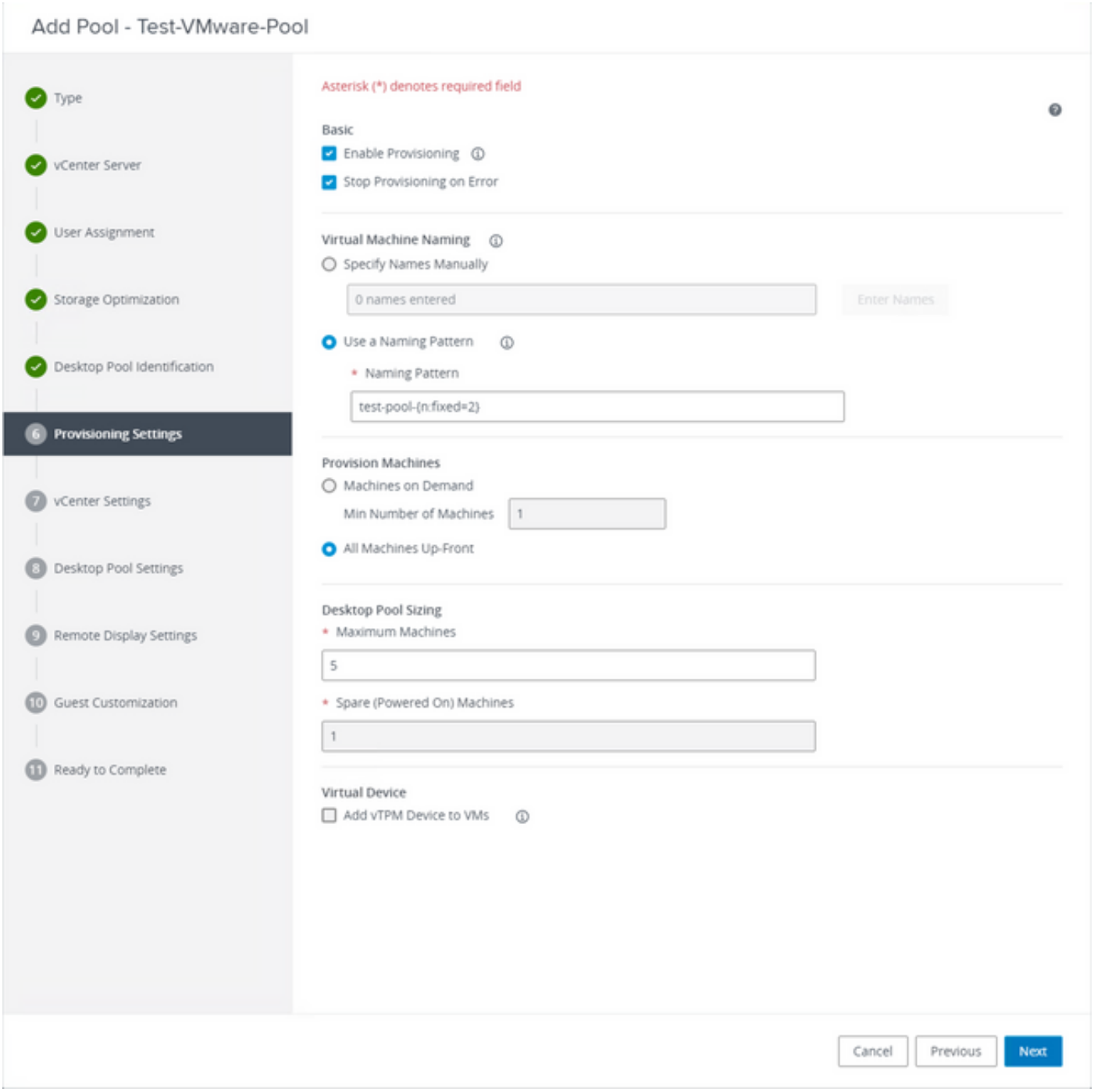
选择“浮动”类型

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

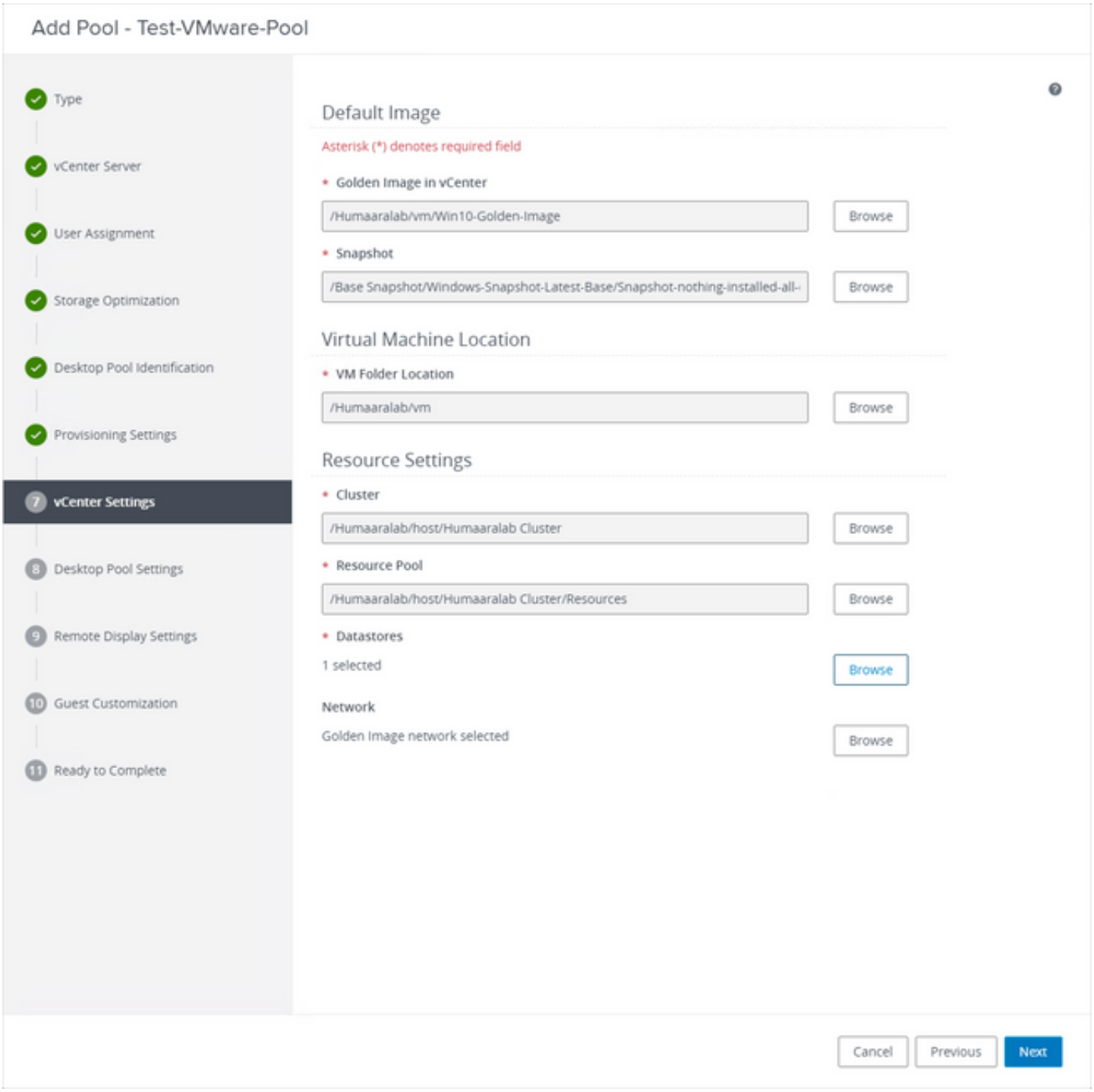

Add Pool
Type
vCenter Server
User Assignment
4 Storage Optimization
5 Desktop Pool Identification
6 Provisioning Settings
7 vCenter Settings
8 Desktop Pool Settings
9 Remote Display Settings
10 Guest Customization
11 Ready to Complete
Storage Policy Management
Use VMware Virtual SAN
Do not use VMware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


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

桌面池名称

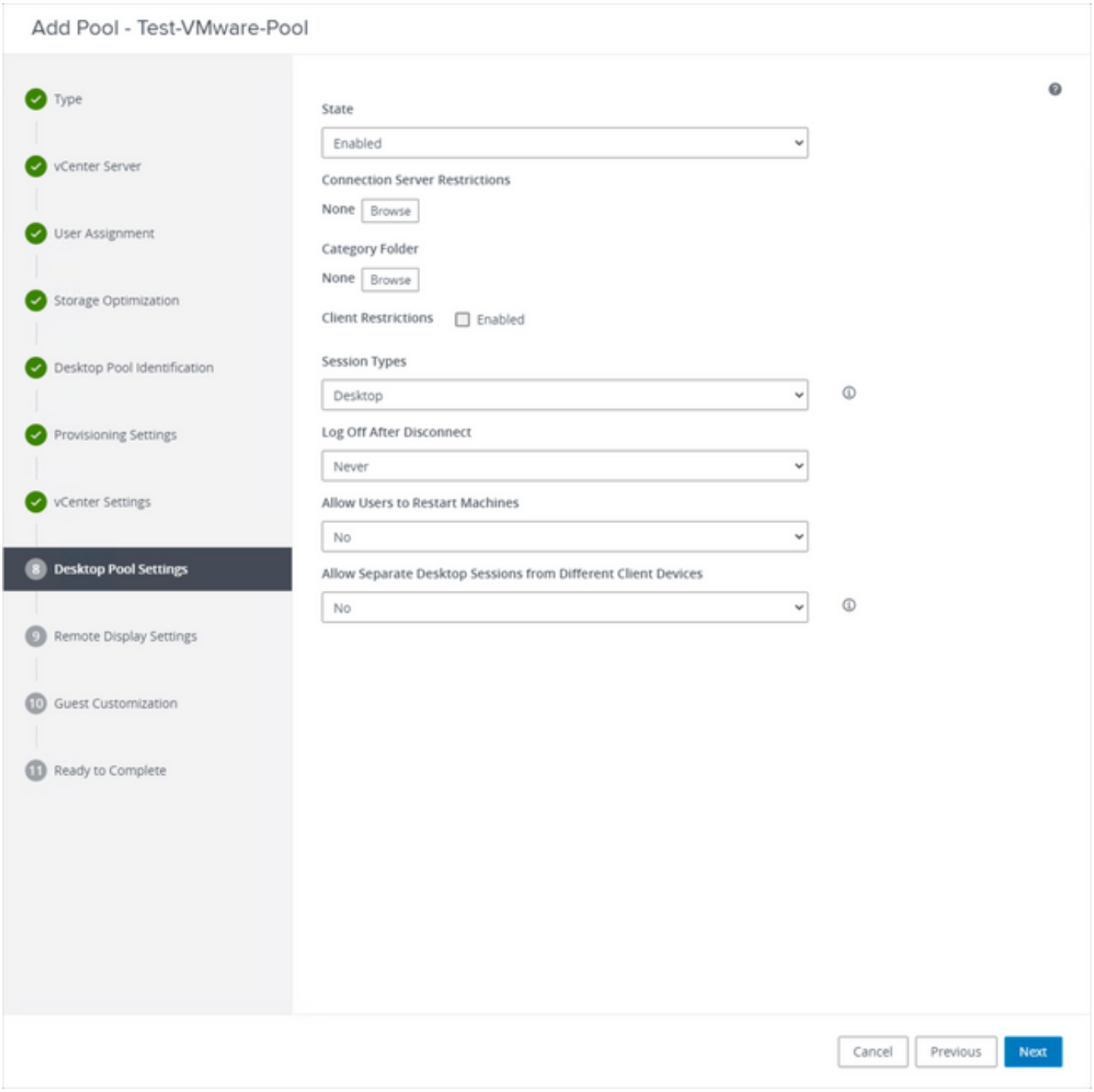


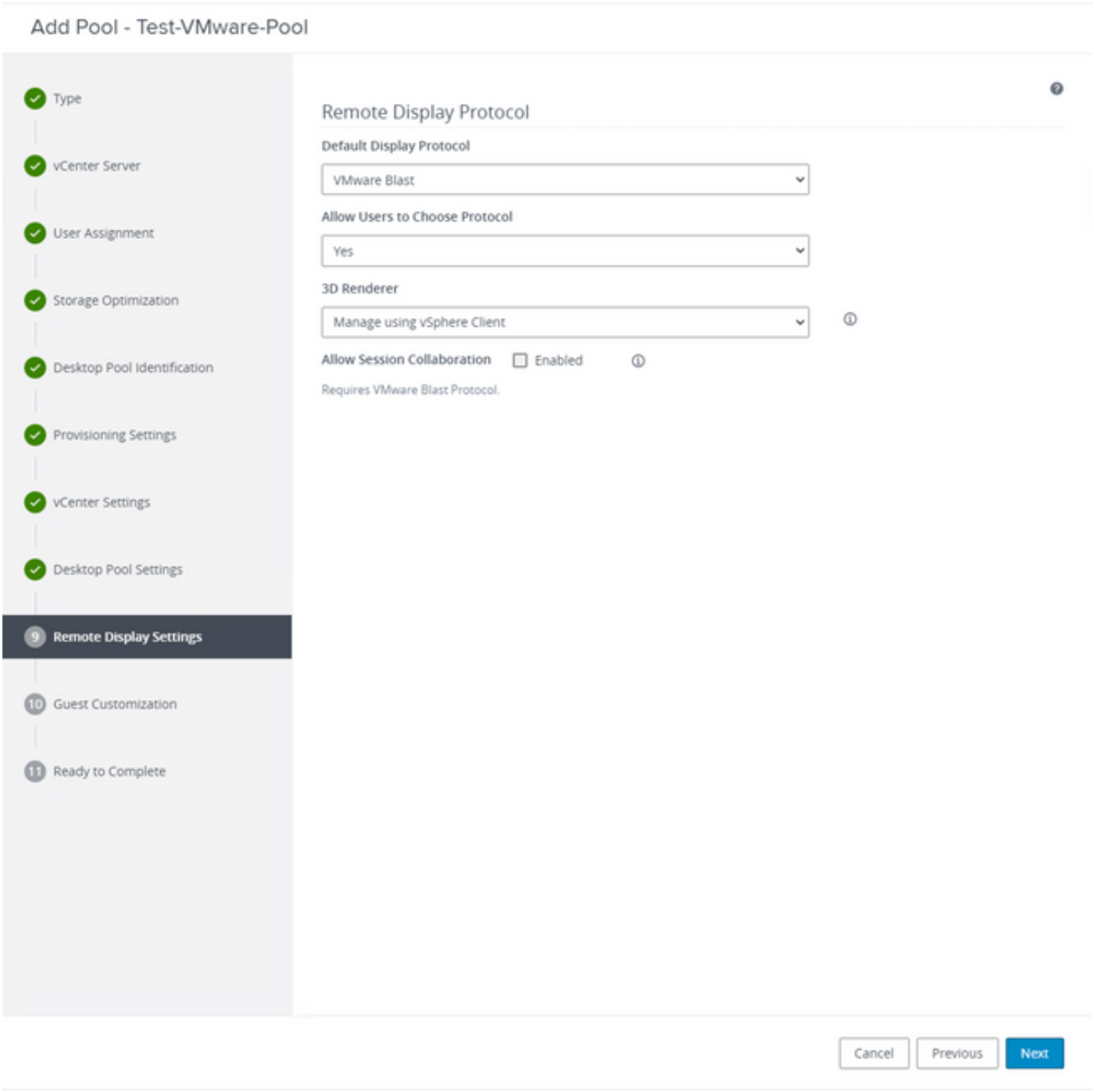
VMware Horizon命名模式：https://docs.vmware.com/en/VMware-Horizon/2103/virtual-desktops/GUID-26AD6C7D-553A-46CB-B8B3-DA3F6958CD9C.html

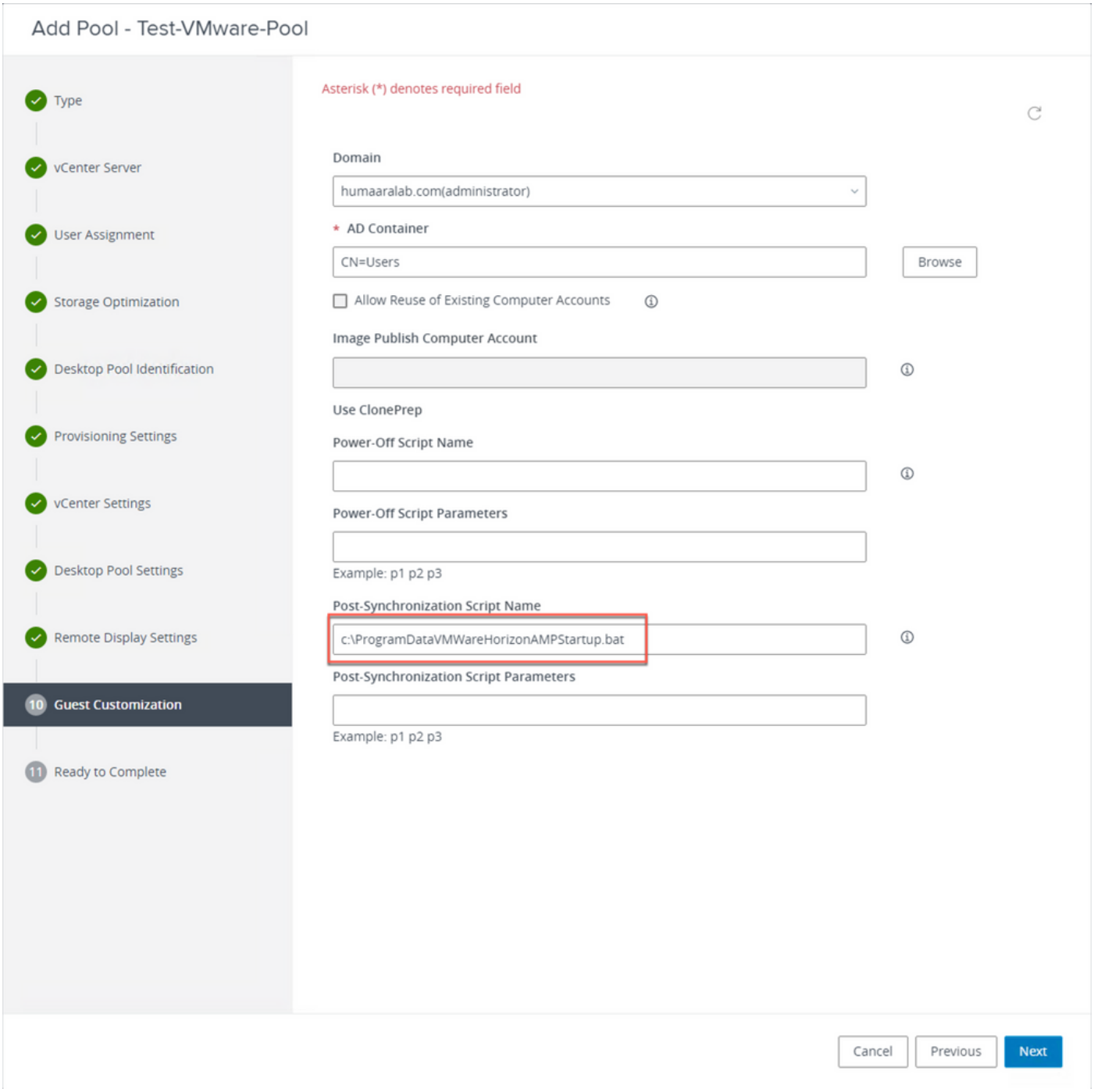


Golden Image：这是实际的Golden Image VM。

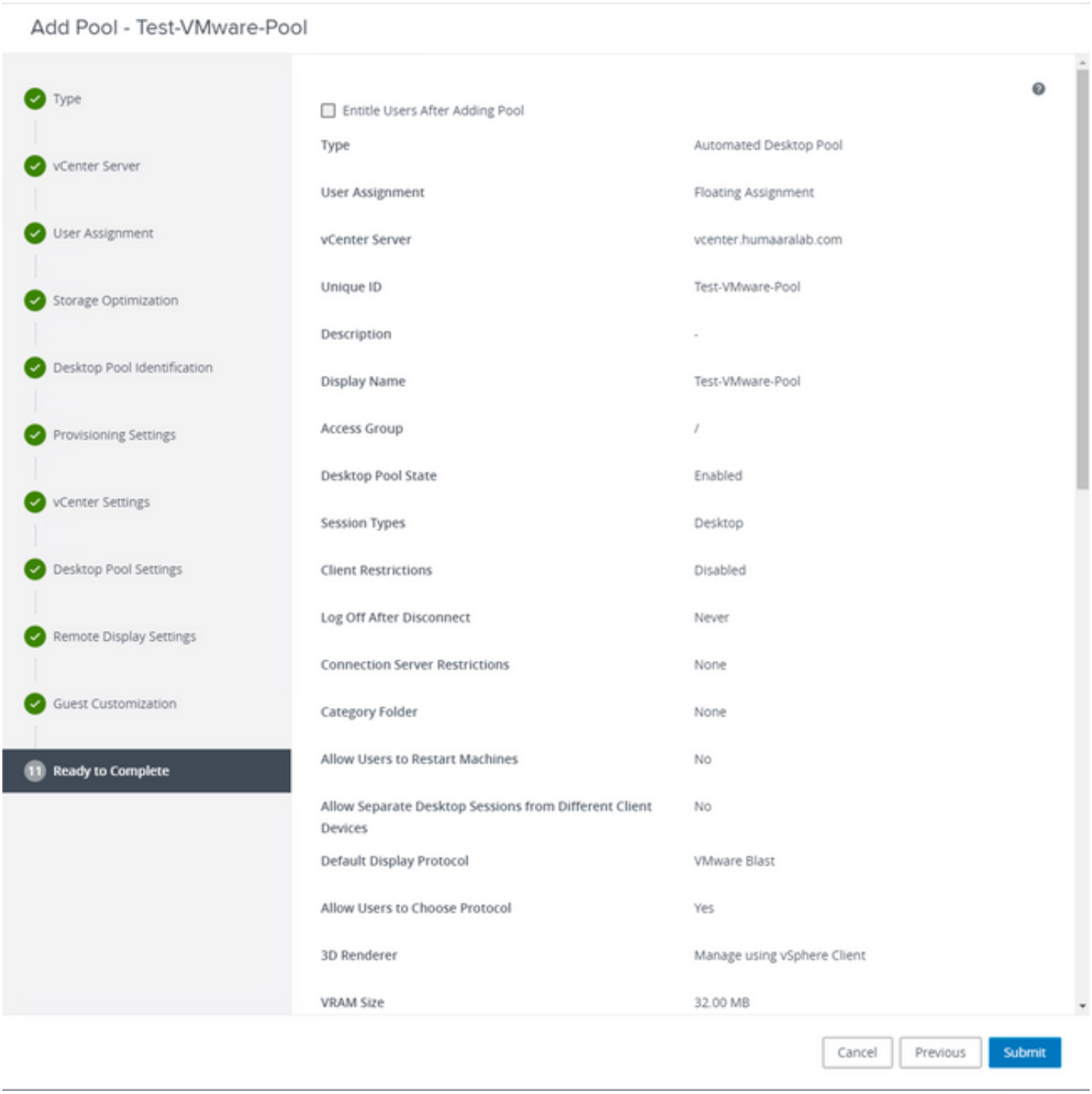
快照：这是要用于部署子虚拟机的映像。这是使用任何更改更新金色图像时更新的值。其余部分是特定于VMware环境的设置。


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.如前所述，向导中的步骤10用于设置脚本路径。



8.完成并提交VMware Horizon后，VMware Horizon将开始创建子级虚拟机。

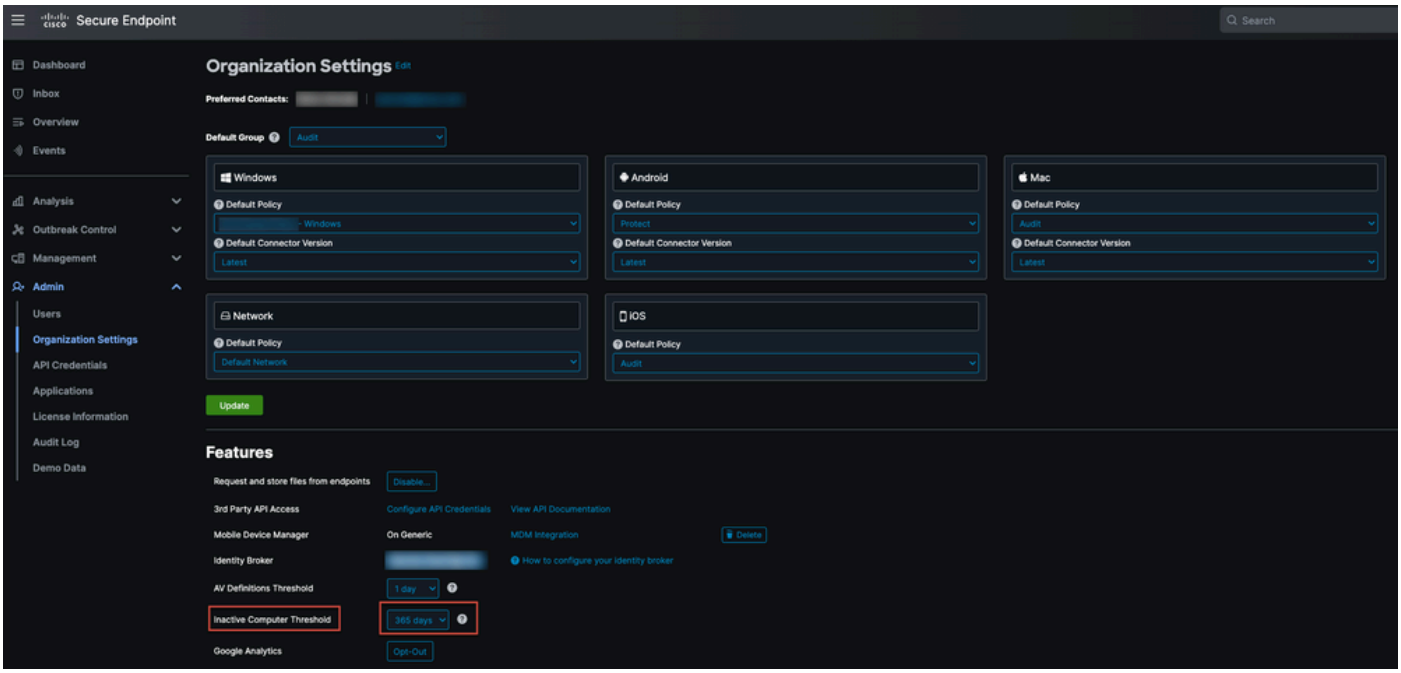
注意：有关这些步骤的信息，请参阅VMware指南，但这些步骤不言自明。

删除重复条目

有多种方法可用于删除连接器重复项：

1.利用安全终端门户上的自动删除功能删除重复（非活动）条目：

您可以在Admin > Organization Settings下找到此设置



非活动计算机阈值允许您指定连接器在未从“计算机管理”(Computer Management)页面列表中移除之前可以进入思科云的天数。默认设置为90天。非活动计算机将仅从列表中删除，并且它们生成的任何事件将保留在您的安全终端组织中。如果连接器再次签入，计算机将重新显示在列表中。

2.使用可用的协调工作流程：https://ciscosecurity.github.io/sxo-05-security-workflows/workflows/secure-endpoint/0056-remove-inactive-endpoints

3.使用外部可用脚本删除过时/旧的UUID:https://github.com/CiscoSecurity/amp-04-delete-stale-guids

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。