セキュアエンドポイントでのID持続性の設定

内容

はじめに

アイデンティティパーシステンスとは何ですか。

- 要件
- アイデンティティパーシステンスが必要な状況
  - 仮想エンドポイントの導入
  - 物理エンドポイントの導入

ID持続性プロセスの概要

- 組織内の重複を特定する
  - 外部で使用可能なGitHubスクリプト
- 重複が作成される理由

誤ったID持続性の導入に関する一般的な問題と症状

導入のベストプラクティス

- snapvolファイルの構成
- ポータルポリシーの計画
  - コンフィギュレーション
- ゴールデンイメージの作成
  - ゴールデンイメージオーバーライドフラグ
  - ゴールデンイメージの作成手順
  - ゴールデンイメージの更新
- ゴールデンイメージコード
  - ゴールデンイメージのセットアップスクリプト
  - ゴールデンイメージの起動スクリプト

AWSワークスペースプロセス

VMware Horizonの重複に関する問題

- 不要な構成/変更
- スクリプトの方法論
- VMware Horizonの設定

重複するエントリの削除

はじめに

このドキュメントでは、Cisco Secure Endpoint Identity Persistence(IDS)機能を確認する方法について説明します。

アイデンティティパーシステンスとは何ですか。

ID永続性は、仮想環境またはコンピュータのイメージ再作成時に一貫したイベントログを維持できるようにする機能です。ConnectorをMACアドレスまたはホスト名にバインドすると、新しい仮想セッションが開始されたり、コンピュータが再イメージ化されるたびに新しいコネクタレコ

ードが作成されないようにできます。この機能は、特に非永続的なVMおよびラボ環境に対して設計されており、従来のワークステーションおよびサーバのセットアップでは有効にしないでください。

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Endpointsポータルへのアクセス
- Cisco TACに連絡して、組織内でアイデンティティパーシステンス機能を有効にする必要があります。
- Identity Persistenceは、Windowsオペレーティングシステム(OS)でのみサポートされています

アイデンティティパーシステンスが必要な状況

アイデンティティパーシステンスは、コネクタの初期登録時にセキュアエンドポイントを識別し、その特定のコネクタのMACアドレスやホスト名などのアイデンティティパラメータに基づいて既知のエントリと照合する、セキュアエンドポイントの機能です。この機能を実装すると、正しいライセンス数を維持できるだけでなく、最も重要な点として、非永続システムで履歴データを適切に追跡できるようになります。

仮想エンドポイントの導入

仮想環境でのID保持の最も一般的な用途は、非永続的な仮想デスクトップインフラストラクチャ(VDI)の導入です。VDIホストデスクトップ環境は、エンドユーザの要求またはニーズに応じて導入されます。これには、VMware、Citrix、AWS AMI Golden Image Deploymentなどのさまざまなベンダーが含まれます。

永続的VDI（ステートフルVDIとも呼ばれる）は、各ユーザのデスクトップが独自にカスタマイズ可能で、あるセッションから別のセッションに「持続」する設定です。このタイプの仮想導入では、Identity Persistenceの機能は必要ありません。これは、これらのマシンが定期的に再イメージ化されることはないためです。

セキュアエンドポイントのパフォーマンスと対話する可能性のあるすべてのソフトウェアと同様に、仮想デスクトップアプリケーションでは、機能を最大化し、影響を最小限に抑えるために、除外の可能性について評価する必要があります。

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

物理エンドポイントの導入

セキュアエンドポイントの物理マシンでのID持続性の導入に適用できるシナリオは2つあります。

- Secure Endpointコネクタが事前にインストールされたゴールデンイメージを使用して物理エンドポイントを導入または再イメージ化する場合は、Goldenimageフラグを有効にする必

要があります。アイデンティティパーシステンスは、再イメージ化されたマシンのインスタンスでの重複を回避するために使用できますが、必須ではありません。

- ゴールデンイメージを含む物理エンドポイントを導入または再イメージ化し、後でセキュアエンドポイントコネクタをインストールする場合、Identity Persistenceを使用して、再イメージ化されたマシンのインスタンスでの重複を回避できますが、これは必須ではありません。

ID持続性プロセスの概要

1. コネクタは、policy.xmlファイル内のトークンを使用してダウンロードされ、クラウド側の該当するポリシーに関連付けられます。
2. コネクタがインストールされ、トークンがlocal.xmlに保存されます。コネクタは、対象のトークンを使用してポータルにPOST要求を行います。
3. クラウド側では、次の順序で動作します。
   a.コンピュータはID同期ポリシー設定のポリシーを確認します。これがない場合、登録は通常どおり行われます。
   b.ポリシー設定に応じて、Registrationはホスト名またはMACアドレスについて既存のデータベースをチェックします。
   ビジネス全体：設定に応じて、すべてのポリシーでホスト名またはMACの一致がチェックされます。一致したオブジェクトGUIDが記録され、エンドクライアントマシンに送り返されます。次に、クライアントマシンはUUIDを引き受け、以前に一致したホストのグループ/ポリシー設定を引き受けます。これは、インストールされたポリシー/グループ設定を上書きします。
   ポリシー全体：トークン はクラウド側のポリシーと一致し、そのポリシー内でのみ同じホスト名またはMACアドレスを持つ既存のオブジェクトを検索します。存在する場合はUUIDと見なされます。そのポリシーに関連付けられた既存のオブジェクトがない場合は、新しいオブジェクトが作成されます。注：他のグループ/ポリシーに関連付けられた同じホスト名に対して重複が存在する可能性があります。
   c.トークンの欠落（以前の登録、導入方法の誤りなど）が原因でグループ/ポリシーに一致するものがない場合、コネクタはbusinessタブのデフォルトのコネクタグループ/ポリシーセットに該当します。グループ/ポリシーの設定に基づいて、一致するすべてのポリシー（ビジネス全体）、問題のあるポリシーのみ（ポリシー全体）、またはまったく一致しない（なし）ことを確認しようとします。 このことを念頭に置いて、トークンの問題が発生した場合にマシンが正しく同期するように、デフォルトグループを必要なID同期設定を含むグループに設定することを推奨します。

組織内の重複を特定する

外部で使用可能なGitHubスクリプト

重複するUUIDを検索します：https://github.com/CiscoSecurity/amp-04-find-duplicate-guids

重複が作成される理由

重複が見られる原因となる可能性がある一般的なインスタンスがいくつかあります。

1. VDIプールで次の手順を実行した場合：

- 非永続的VM/VDIでの初期導入は、ID永続性を無効にして行われます（たとえば、ゴールデンイメージを使用）。
- クラウド内でポリシーが更新され、Identity Persistenceが有効になります。日中はエンドポイントでポリシーが更新されます。
- マシンは更新/再イメージ化され（同じゴールデンイメージを使用）、元のポリシーはアイデンティティパーシステンスなしでエンドポイントに戻されます。
- ポリシーはローカルにID持続性を持たないため、登録サーバは以前のレコードをチェックしません。
- このフローの結果、重複が発生します。

2.ユーザは、ポリシーでID永続性が有効になっている元のゴールデンイメージを1つのグループに導入し、セキュアエンドポイントポータルからエンドポイントを別のグループに移動します。その後、「moved-to」グループに元のレコードが含まれますが、VMが再イメージ化/再展開されると、元のグループに新しいコピーが作成されます。

✎ 注：これは重複を引き起こす可能性のあるすべてのシナリオのリストではなく、最も一般的なシナリオの一部です。

誤ったID持続性の導入に関する一般的な問題と症状

ID持続性の実装が正しくない場合、次の問題や症状が発生する可能性があります。

- コネクタシート数が正しくない
- 誤った結果が報告される
- デバイストラジェクトリデータの不一致
- 監査ログ内でのマシン名のスワップ
- コネクタはコンソールからランダムに登録および登録解除されます
- コネクタがクラウドに正しくレポートされない
- UUIDの重複
- マシン名の重複
- データの不整合
- 再構成後にコンピューターが既定のビジネスグループ/ポリシーに登録される

- ポリシーでアイデンティティパーシステンスを有効にして手動で展開する。

– ポリシーでID永続性が有効になっているコマンドラインスイッチを使用してエンドポイントを手動で展開し、後でエンドポイントをアンインストールして、別のグループ/ポリシーのパッケージを使用して再インストールを試みると、エンドポイントは自動的に元のポリシーに切り替わります。

- SFCログからの出力で、ポリシーの切り替えが1 ~ 10秒以内に自動的に行われたことが示されます。

```
(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
```

別のグループに属するコネクタをインストールしようとすると、もう1つの副作用が発生します。ポータルに、コネクタが正しいグループに割り当てられているものの、元のポリシーが「間違った」ことが表示されます

これは、ID持続性(ID SYNC)の動作の仕組みによるものです。

ID SYNCを使用しない場合、コネクタが完全にアンインストールされるか、再登録コマンドラインスイッチを使用してアンインストールされます。アンインストールの場合は新しい作成日とコネクタGUIDが表示され、再登録コマンドの場合は新しいコネクタGUIDのみが表示されます。ただし、使用できないID SYNCでは、ID SYNCは古いGUIDとDATEで上書きされます。ホストを「同期」する方法です。

この問題が確認された場合は、ポリシーの変更を通じて修正を実装する必要があります。影響を受けるエンドポイントを元のグループ/ポリシーに戻し、ポリシーが同期されていることを確認する必要があります。次に、エンドポイントを目的のグループ/ポリシーに戻します

導入のベストプラクティス

snapvolファイルの構成

VDIインフラストラクチャにアプリケーションボリュームを使用する場合は、snapvol.cfg設定に次の設定変更を行うことをお勧めします

次の除外をsnapvol.cfgファイルに実装する必要があります。

Paths:

- 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

レジストリキー：

- HKEY_LOCAL_MACHINE\SOFTWARE\Immunet保護
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Immunet保護
- 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

x64システムで、次を追加します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Immunet保護
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstal
  護

参照:

- 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

ポータルポリシーの計画

セキュアエンドポイントポータルでID持続性を実装する際に従う必要があるベストプラクティスの一部を次に示します。

1.分離を容易にするために、Identity Persistenceエンドポイントには個別のポリシー/グループを使用することを強くお勧めします。

2.エンドポイントの分離を使用して、侵害の発生時にコンピュータをグループに移動するアクションを実装する場合。宛先グループでは、ID持続性も有効にする必要があり、VDIコンピュータでのみ使用する必要があります。

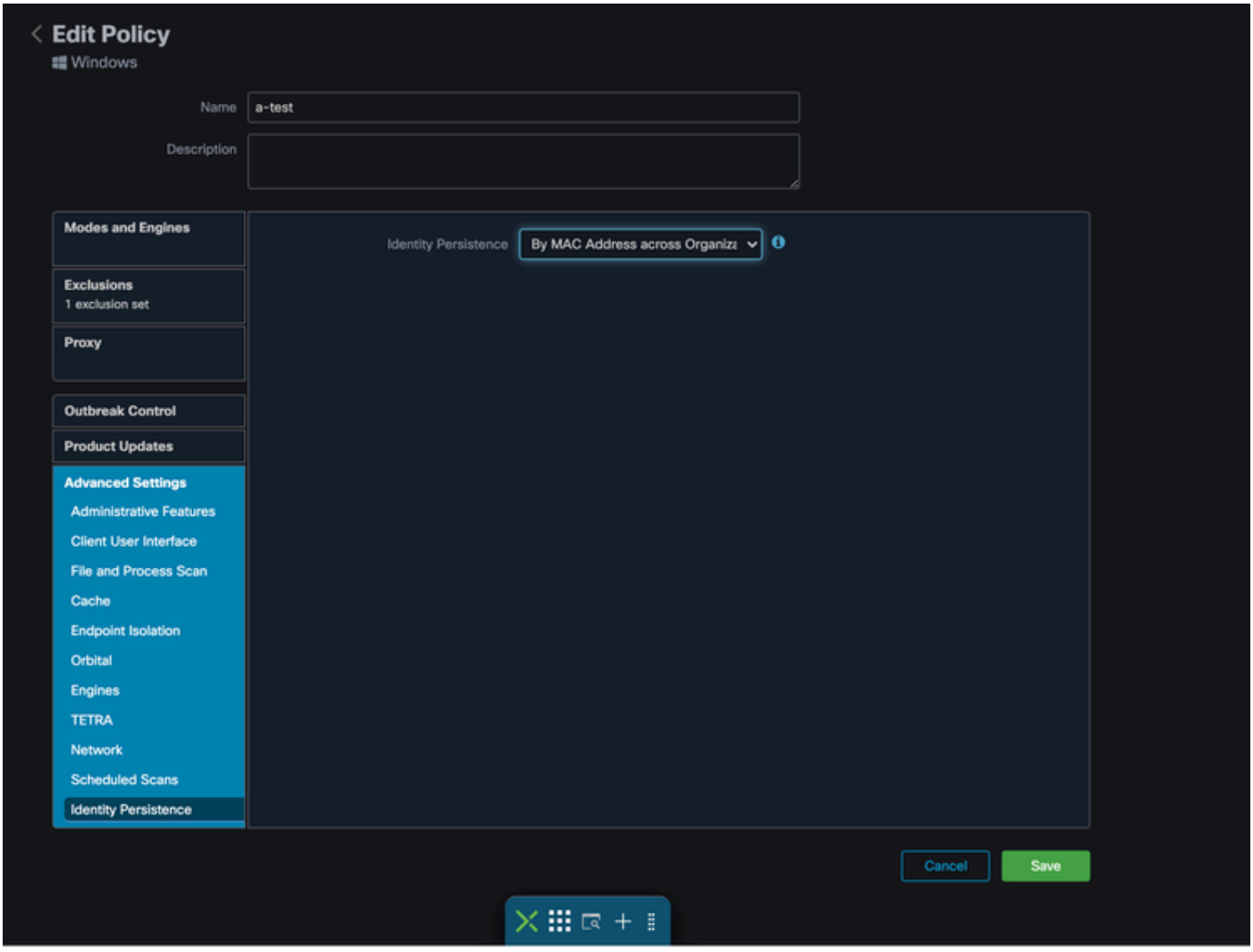
3.組織の設定でデフォルトのグループ/ポリシーのID持続性を有効にすることは、すべてのポリシーでID持続性が有効になっており、設定のスコープが「組織間」である場合を除き、推奨されません。

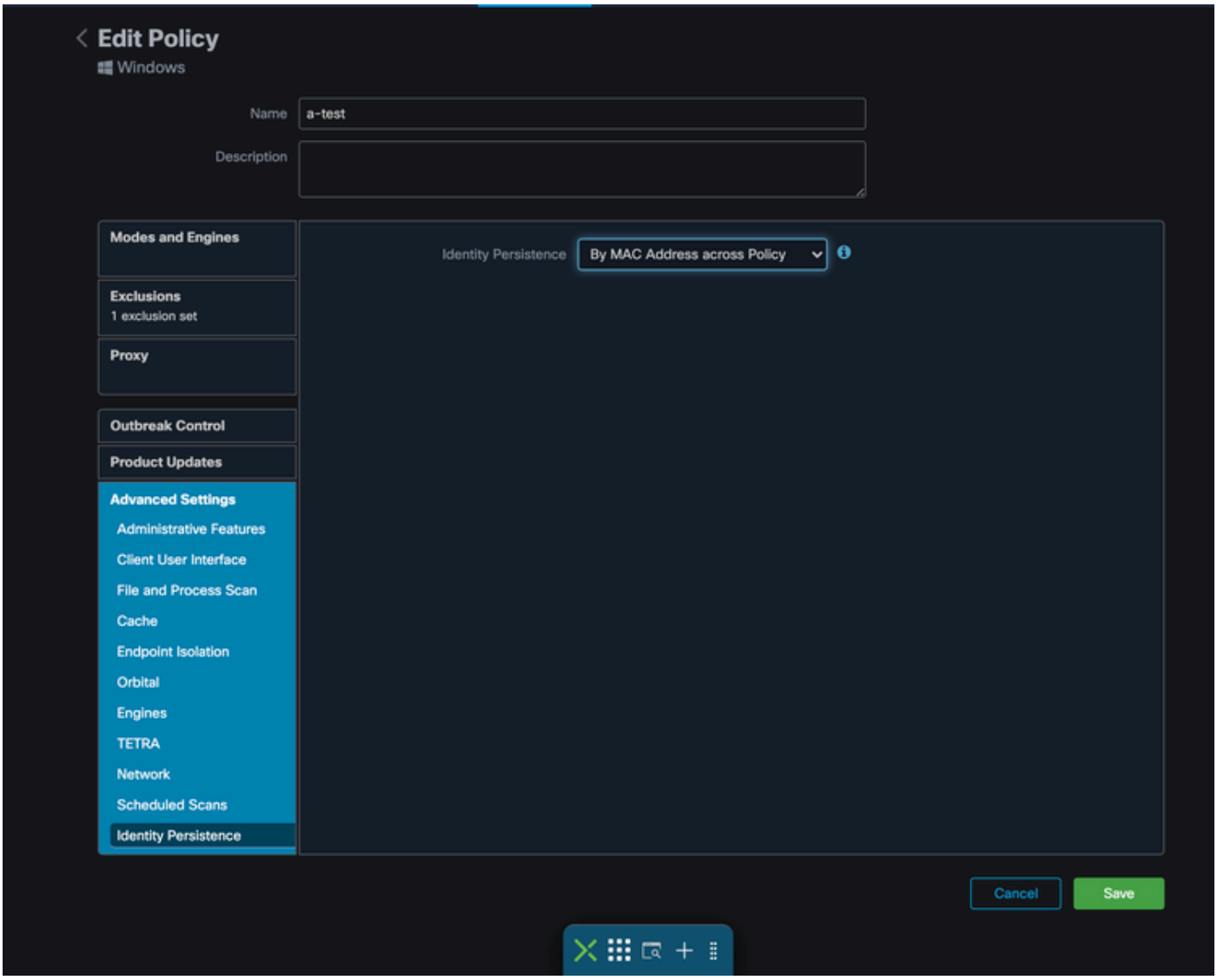
コンフィギュレーション

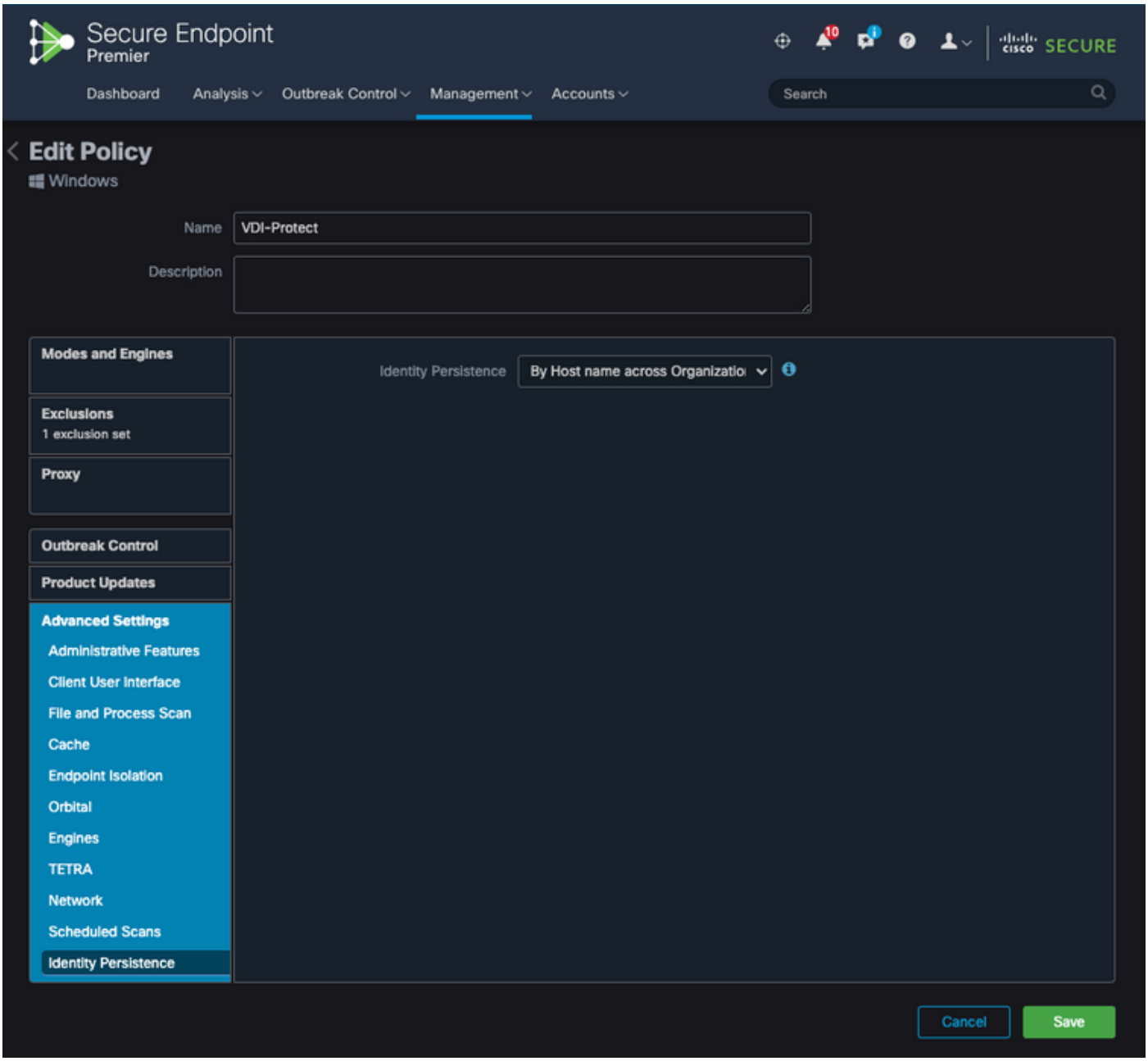
Identity Persistenceを使用してセキュアエンドポイントコネクタを導入するには、次の手順に従います。

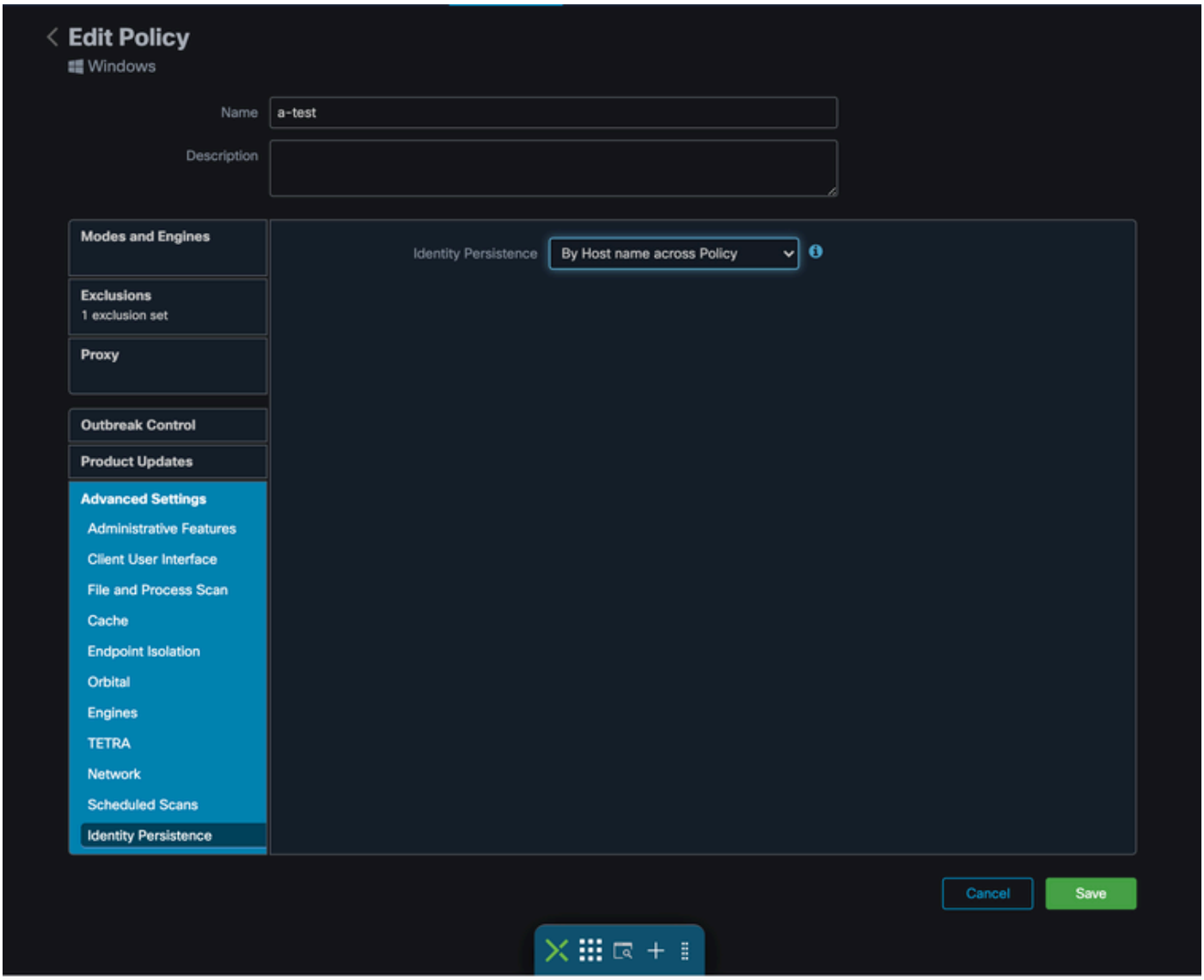
ステップ 1：必要なID持続性の設定をポリシーに適用します。

- セキュアエンドポイントポータルで、Management > Policiesの順に移動します。
- アイデンティティパーシステンスを有効にするポリシーを選択し、Editをクリックします。
- Advanced Settingsタブに移動し、下部にあるIdentity Persistenceタブをクリックします。
- 「ID持続性」ドロップダウンを選択し、環境に最も適したオプションを選択します。次の図を参照してください。




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



5つのオプションから選択できます。

- 機能が有効になっていないことに注意してください。コネクタのUUIDは、どのような状況でも新しいコネクタのインストールと同期されません。新しいインストールのたびに、新しいマシンオブジェクトが生成されます。
- ビジネス間のMACアドレスによる方法：新規または更新されたインストールでは、以前の履歴データと新しい登録を同期するために、同じMACアドレスを持つ最新のコネクタレコードが検索されます。この設定では、すべてのビジネスレコードが検索されます

  アイデンティティー同期が「なし」以外の値に設定されている組織内のすべてのポリシーに対して適用されます。コネクタは、以前のインストールが新しいインストールと異なる場合は、ポリシーを更新して以前のインストールを反映できます。

- ポリシーを越えたMACアドレス：新規または更新されたインストールでは、以前の履歴データと新しい登録を同期するために、同じMACアドレスを持つ最新のコネクタレコードが検索されます。この設定は、展開で使用されるポリシーに関連付けられたレコードのみを参照します。コネクタがこのポリシーで以前にインストールされていなくても、別のポリシーで以前にアクティブになっていた場合は、重複が作成される可能性があります。
- ビジネス間のホスト名：新規または更新されたインストールでは、以前の履歴データと新し

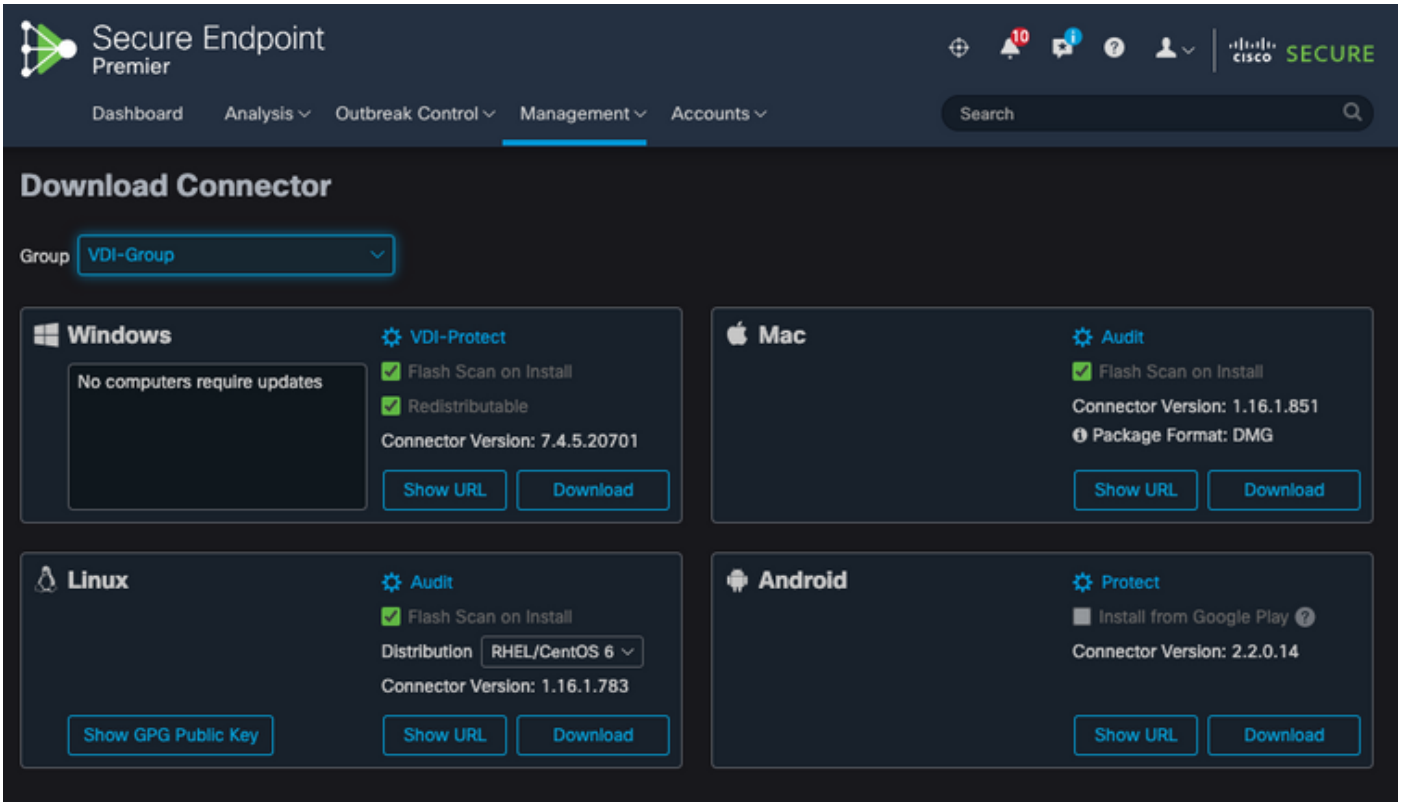
い登録を同期するために、同じホスト名を持つ最新のコネクタレコードが検索されます。この設定は、他のポリシーのID永続性設定に関係なく、すべてのビジネスレコードを調べ、以前のインストールが新しいものと異なる場合は、コネクタはそのポリシーを更新して以前のインストールを反映できます。ホスト名にはFQDNが含まれるため、コネクタがネットワーク間（ラップトップなど）を定期的に移動する場合は重複が発生する可能性があります。

- ポリシーをまたがるホスト名：新規または更新されたインストールでは、以前の履歴データと新しい登録を同期するために、同じホスト名を持つ最新のコネクタレコードが検索されます。この設定は、展開に使用されたポリシーに関連付けられたレコードのみを参照します。コネクタがこのポリシーで以前にインストールされていなくても、別のポリシーで以前にアクティブになっていた場合は、重複が作成される可能性があります。ホスト名にはFQDNが含まれるため、コネクタがネットワーク間（ラップトップなど）で定期的に移動する場合にも重複が発生する可能性があります。

注：アイデンティティパーシステンスを使用する場合は、ビジネスまたはポリシー全体でホスト名別を使用することを推奨します。マシンにはホスト名が1つありますが、複数のMACアドレスを持つことができ、多くのVMがMACアドレスを複製します。

ステップ 2：セキュアエンドポイントコネクタをダウンロードします。

- Management > Download Connectorの順に移動します。
- ステップ1で編集したポリシーのグループを選択します。
- 図に示すように、Windows ConnectorのDownloadをクリックします。



ステップ 3：コネクタをエンドポイントに導入します。

- ダウンロードしたコネクタを使用して、Secure Endpoint（Identity Persistenceを有効にし

た状態）をエンドポイントに手動でインストールできるようになりました。
- それ以外の場合は、ゴールデンイメージを使用してコネクタを導入することもできます（図を参照）

注：再頒布可能インストーラを選択する必要があります。これは、32ビットと64ビットの両方のインストーラを含む約57 MB（サイズは新しいバージョンによって異なる場合があります）のファイルです。コネクタを複数のコンピュータにインストールするには、このファイルをネットワーク共有に配置するか、または必要に応じてすべてのコンピュータにプッシュします。インストーラには、インストール用の設定ファイルとして使用されるpolicy.xmlファイルが含まれています。

ゴールデンイメージの作成

VDIクローニングプロセスに使用するゴールデンイメージを作成する場合は、ベンダーのドキュメント（VMware、Citrix、AWS、Azureなど）のベストプラクティスガイドラインに従ってください。

たとえば、VMware Golden Image Process:https://docs.vmware.com/en/VMware-Horizon/2106/virtual-desktops/GUID-D9C46AEF-1C41-4711-BF9E-84362EBE6ABF.htmlです。

VMwareを特定したため、AWS構成プロセスはVM構成の終了前にクローン（子VM）を複数回再起動します。これにより、クローン（子VM）に最終的なホスト名が割り当てられず、クローン（子VM）がゴールデンイメージホスト名を使用してセキュアエンドポイントクラウドに登録されるため、セキュアエンドポイント登録プロセスに問題が発生します。これにより、クローン作成プロセスが中断され、問題が発生します。

これは、セキュアエンドポイントコネクタプロセスの問題ではなく、クローニングプロセスおよびセキュアエンドポイント登録との互換性の問題です。この問題を回避するために、クローン作成プロセスに実装する必要がある変更をいくつか確認しました。この変更は、これらの問題の解決に役立ちます。

以下は、イメージをフリーズしてクローンを作成する前に、ゴールデンイメージVMに実装する必要がある変更です

1.セキュアエンドポイントのインストール時には、常にゴールデンイメージのGoldenimageフラグを使用してください。

2.「ゴールデンイメージ設定スクリプト」および「ゴールデンイメージ起動スクリプト」セクションを実装し、クローン（子VM）に最終ホスト名が実装されている場合にのみエンドポイントサービスをオンにするのに役立つスクリプトを見つけます。詳細については、「VMware Horizon Duplication Issues」のセクションを参照してください。

ゴールデンイメージオーバーライドフラグ

インストーラを使用する場合、ゴールデンイメージに使用するフラグは/goldenimage 1です。

ゴールデンイメージフラグは、ベースイメージでのコネクタの開始と登録を禁止します。したが

って、イメージの次の開始時に、コネクタは、割り当てられたポリシーによって構成された機能状態にあります。

その他のフラグの詳細については、この記事を参照してください。

インストーラを使用する場合、ゴールデンイメージに使用する新しいフラグは/goldenimage [1|0]です

0 – デフォルト値 – この値はゴールデンイメージオプションをトリガーせず、オプションなしでインストーラが実行されたかのように動作します。インストール時に初期コネクタの登録と起動をスキップしないでください。

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

1 – ゴールデンイメージとしてインストールします。これはフラグとともに使用される一般的なオプションで、予想される唯一の使用方法です。インストール時にコネクタの初期登録とスタートアップをスキップします。

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

ゴールデンイメージの作成手順

コネクタは、ゴールデンイメージの準備のために最後に取り付けることをお勧めします。

1. Windowsイメージを要件に合わせて準備し、必要なソフトウェアと、コネクタ以外のWindowsイメージの構成をすべてインストールします。
2. Cisco Secure Endpointコネクタをインストールします。

/goldenimage 1フラグを使用して、これがゴールデンイメージの展開であることをインストーラに示します。

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

3.ここで説明されているスクリプトロジック（必要な場合）を実装します

4.インストールの完了

5.ゴールデンイメージをフリーズする

ゴールデンイメージにアプリケーションがインストールされ、システムが準備され、セキュア工

ンドポイントが/goldenimageflagを使用してインストールされた後、ホストをフリーズして配布する準備が整います。複製されたホストが起動すると、Secure Endpointが起動し、クラウドに登録されます。ポリシーまたはホストに変更を加える場合を除き、コネクタの設定に関してこれ以上の操作は必要ありません。ゴールデンイメージの登録が完了した後に変更が行われた場合は、このプロセスを再起動する必要があります。 このフラグは、コネクタがベースイメージ上で開始および登録されるのを防ぎます。イメージの次の起動時に、コネクタは、割り当てられたポリシーによって設定された機能状態になります。

注：ゴールデンイメージがSecure EndpointCloudに登録された後でVMをフリーズする場合は、ゴールデンイメージVM上のSecure Endpointをアンインストールして再インストールし、登録とコネクタの重複の問題を防ぐためにVMを再びフリーズすることをお勧めします。このアンインストール処理の一環として、Secure Endpointのレジストリ値を変更することは推奨されません。

ゴールデンイメージの更新

未登録のコネクタを保持するためにゴールデンイメージを更新する必要がある場合は、2つのオプションがあります。

推奨されるプロセス

1. コネクタをアンインストールします。
2. ホストの更新またはアップグレードをインストールします。
3. ゴールデンイメージフラグを使用して、ゴールデンイメージの処理の後でコネクタを再インストールします。
4. このプロセスに従う場合、ホストはコネクタを起動すべきではありません。
5. イメージをフリーズします。
6. クローンを作成する前に、不要な重複ホストを防ぐために、ゴールデンイメージがポータルに登録されていないことを確認してください。

代替プロセス

1. コネクタが登録されないように、ホストがインターネットに接続できないことを確認します。
2. コネクタサービスを停止します。
3. 更新プログラムをインストールします。
4. 更新が完了したらイメージをフリーズする
5. 重複ホストが発生しないようにするには、コネクタの登録を防止する必要があります。接続を削除すると、クラウドへの登録にアクセスできなくなります。また、停止されるコネクタは、次のリブートまでコネクタの状態を維持し、クローンを一意のホストとして登録できるようにします。
6. クローンを作成する前に、不要な重複ホストを防ぐために、ゴールデンイメージがポータルに登録されていないことを確認してください。

ゴールデンイメージコード

このセクションは、ゴールデンイメージプロセスのサポートに役立つコードスニペットで構成され、ID持続性の実装時にコネクタの重複を防止するのに役立ちます。

ゴールデンイメージのセットアップスクリプト

セットアップスクリプトの説明

最初のスクリプト「Setup」は、ゴールデンイメージを複製する前に実行されます。これは一度だけ手動で実行する必要があります。主な目的は、クローン仮想マシン上で次のスクリプトが正しく機能するように初期設定を行うことです。次のような設定が含まれます。

- Cisco Secure Endpointサービスのスタートアップを手動に変更して、自動起動を回避する。
- 次のスクリプトを実行するスケジュールされたタスクを、システム起動時に最高の権限で作成します(Startup)。
- ゴールデンイメージのホスト名を格納する「AMP_GOLD_HOST」というシステム環境変数を作成します。これは、変更を元に戻す必要があるかどうかを確認するために起動スクリプトで使用されます

セットアップスクリプトコード

```
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 /
```

セットアップスクリプトコードは非常に単純です。

品目2:マルウェア防御サービスの起動タイプを手動に変更。

5行目：「AMP_GOLD_HOST」という新しい環境変数を作成し、現在のコンピュータのホスト名をその環境変数に保存します。

9行目：システムの起動時に、パスワードを必要とせずに、最高の特権で指定された「Startup」スクリプトを実行する「Startamp」という名前のスケジュールタスクを作成します。

ゴールデンイメージの起動スクリプト

起動スクリプトの説明

2番目のスクリプト「Startup」は、複製された仮想マシン上の各システム起動時に実行されます。主な目的は、現在のマシンが「ゴールデンイメージ」のホスト名を持っているかどうかを確認

することです。

- 現在のマシンがゴールデンイメージの場合、アクションは実行されず、スクリプトは終了します。スケジュールされたタスクが維持されるため、セキュアエンドポイントはシステムの起動時に実行を続行します。
- 現在のマシンが「Golden」イメージでない場合、最初のスクリプトによる変更はリセットされます。
  - Cisco Secure Endpointサービススタートアップ設定を自動に変更する。
  - Cisco Secure Endpointサービスを開始しています。
  - 「AMP_GOLD_HOST」環境変数を削除しています。
  - 起動スクリプトを実行するスケジュール済みタスクを削除し、スクリプト自体を削除します。

起動スクリプトコード

```
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
```

2行目：現在のホスト名と保存されている「AMP_GOLD_HOST」値を比較します。これらが同じ場合、スクリプトは「同じ」ラベルにジャンプします。同じ場合は、「同じ」ラベルにジャンプします。

行4-6:「same」ラベルに到達すると、スクリプトは何も行いません。これは、まだゴールデンイメージであるためです。「exit」ラベルに進みます。

行8-16:「notsame」ラベルに到達すると、スクリプトは次のアクションを実行します。

- Malware Protectionサービスのスタートアップの種類を自動に変更します。
- マルウェア防御サービスを開始します。
- 環境変数「AMP_GOLD_HOST」を削除します。
- 「Startamp」という名前のスケジュールタスクを削除します。

注：このドキュメントに記載されているスクリプトは、TACによって正式にサポートされているわけではありません。

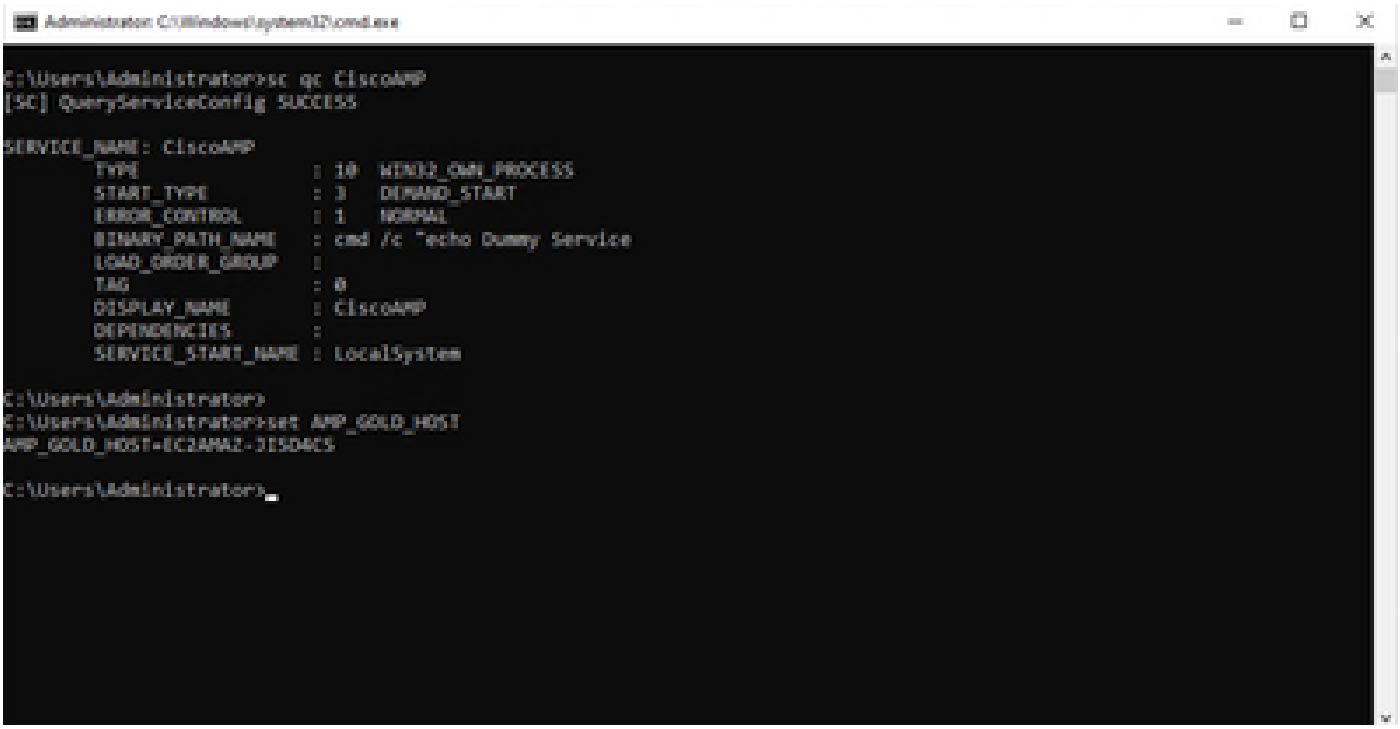
注：この2つのスクリプトにより、クローン仮想マシン環境でCisco AMPサービスを起動できます。ゴールデンイメージを適切に設定し、起動スクリプトを使用することで、Cisco Secure Endpointが正しい設定を持つすべてのクローン仮想マシンで確実に実行されます。

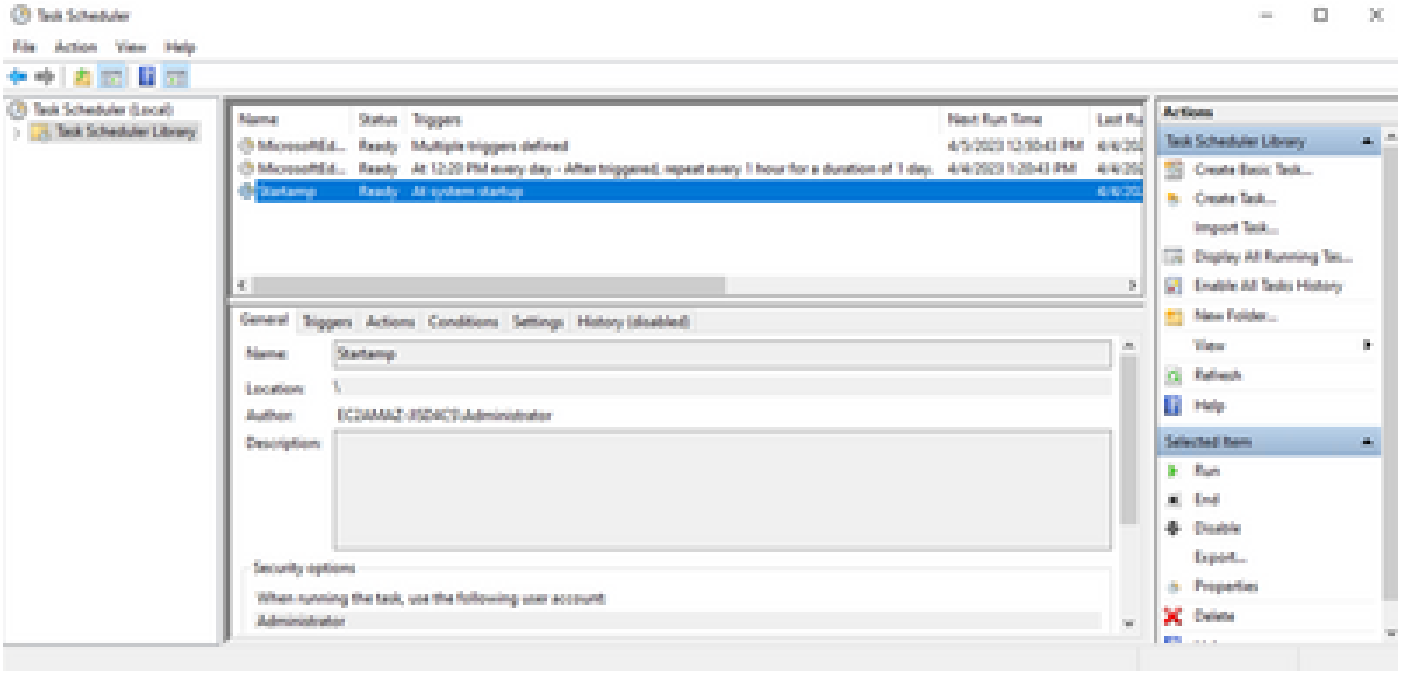
AWSワークスペースプロセス

このソリューションは、クローニング前にゴールデンイメージで実行される「セットアップ」スクリプトと、システムの起動時にクローニングされた各仮想マシンで実行される「スタートアップ」スクリプトで構成されます。これらのスクリプトの主な目的は、手動による介入を減らしながらサービスを適切に設定することです。この2つのスクリプトにより、クローン仮想マシン環境でのCisco Secure Endpointサービスの起動が可能になります。ゴールデンイメージを適切に設定し、起動スクリプトを使用することで、Cisco Secure Endpoint Connectorが、正しい設定を持つすべてのクローン仮想マシン上で確実に実行されます

AWS Workspaceにゴールデンイメージを実装するために必要なスクリプトコードについては、「ゴールデンイメージのセットアップスクリプトコード」および「ゴールデンイメージのスタートアップスクリプトコード」のセクションを参照してください。

セットアップスクリプトを実行した後、設定変更が正常に導入されたことを確認できます。





ゴールデンイメージでこのアクションを実行したので、すべての新しいインスタンスにこの設定が適用され、起動時に起動スクリプトが実行されます。

VMware Horizonの重複に関する問題

VMware Horizonでは、子VMマシンの作成時に、Horizon作成プロセスの一環として子VMマシンが何度も再起動されることを確認できました。これにより、子VMの準備ができていない（最終または正しいNetBios名が割り当てられていない）ときに、セキュアエンドポイントサービスが有効になるという問題が発生します。これにより、セキュアエンドポイントが混乱し、プロセスが中断するという問題が発生します。この問題が発生しないように、Horizon Processとの非互換性に対するソリューションを開発しました。このソリューションでは、ゴールデンイメージVMに添付スクリプトを実装し、VMware Horizonの同期後スクリプト機能を使用します。
https://docs.vmware.com/en/VMware-Horizon/2103/published-desktops-applications.pdf

不要な構成/変更

- 最初の展開後にゴールデンイメージを変更する場合は、Secure Endpointをアンインストールして再インストールする必要はありません。
- セキュアエンドポイントサービスを遅延開始に設定する必要はありません。

スクリプトの方法論

スクリプトの例は次のとおりです。

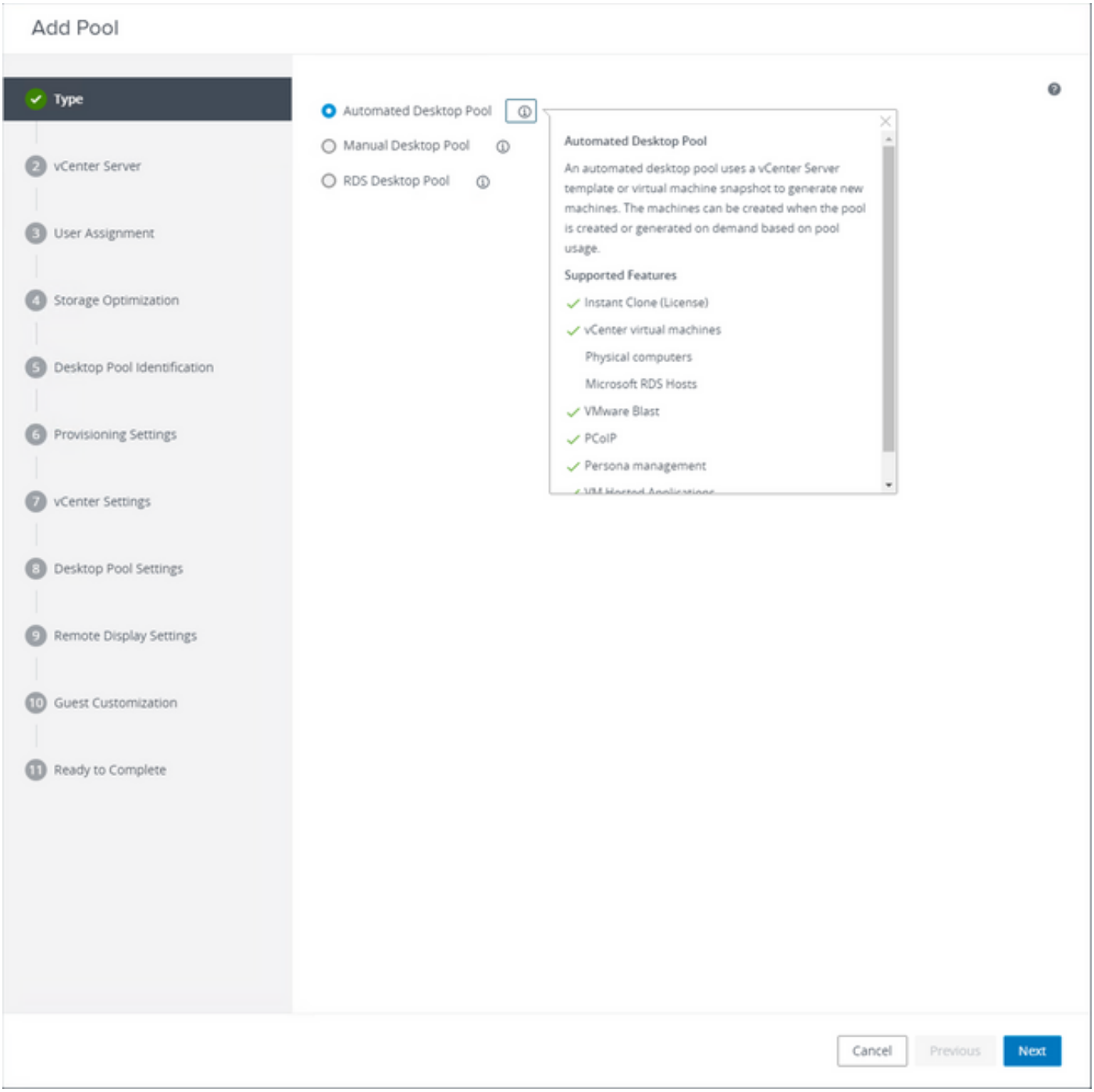
- Golden Image Setupスクリプト：このスクリプトは、前述のフラグを使用してセキュアエンドポイントコネクタをインストールした後に実装する必要があります。このスクリプトは、セキュアエンドポイントサービスを手動開始に変更し、次の手順で参照できるようにゴールデンイメージのホスト名を環境変数として保存します。

- ゴールデンイメージ起動スクリプト：このスクリプトは、クローン（子）VMのホスト名を

前の手順で保存したホスト名と一致させる論理的なチェックです。これにより、クローン（子）VMがゴールデンイメージVM以外のホスト名（マシンの最終ホスト名）を取得したことを確認し、Secure Endpoint Serviceを起動して自動に変更します。また、前述のスクリプトから環境変数を削除します。これは通常、VMwareなどの導入ソリューションで使用可能なメカニズムを使用して実装されます。VMwareでは、同期後のパラメータ https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-E177899E-023D-4E61-B058-AFE3822158AA.html を使用できます。AWSでも同様に、https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-windows-user-data.htmlのようにスタートアップスクリプトを使用できます。

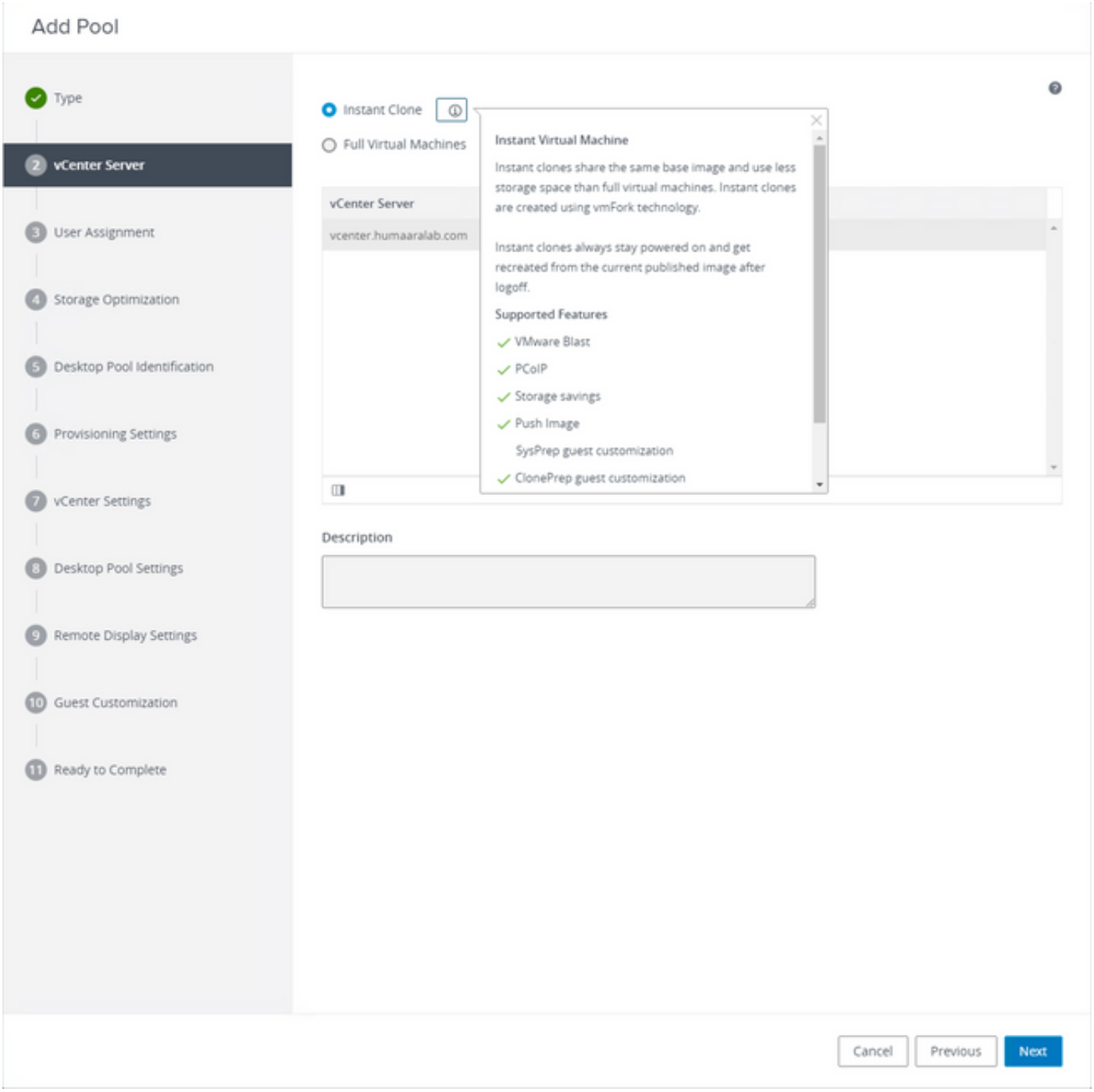
VMware Horizonの設定

1. ゴールデンイメージVMが準備され、プールの初期導入に必要なすべてのアプリケーションがVMにインストールされます。
2. セキュアエンドポイントは、次のコマンドライン構文を使用してインストールされ、goldenimageフラグが含まれます。たとえば、<ampinstaller.exe> /R /S /goldenimage 1のようになります。ゴールデンイメージフラグは、このプロセスが正常に動作するために重要なリブートまでセキュアエンドポイントサービスが実行されないことを保証します。https://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-endpoints/118587-technote-fireamp-00.html を参照してください。
3. セキュアエンドポイントのインストール後、最初にゴールデンイメージVMでVMWareHorizonAMPSetup.batスクリプトを実行します。基本的に、このスクリプトはセキュアエンドポイントサービスを手動開始に変更し、後で使用するためにゴールデンイメージホスト名を保存する環境変数を作成します。
4. VMWareHorizonAMPStartup.batをゴールデンイメージVM上のユニバーサルパス(C:\ProgramDataなど)にコピーする必要があります。これは、後の手順で使用します。
5. ゴールデンイメージVMをシャットダウンし、VMware Horizonで構成プロセスを開始できるようになりました。
6. これは、VMware Horizonの観点から見た手順の詳細な情報です。



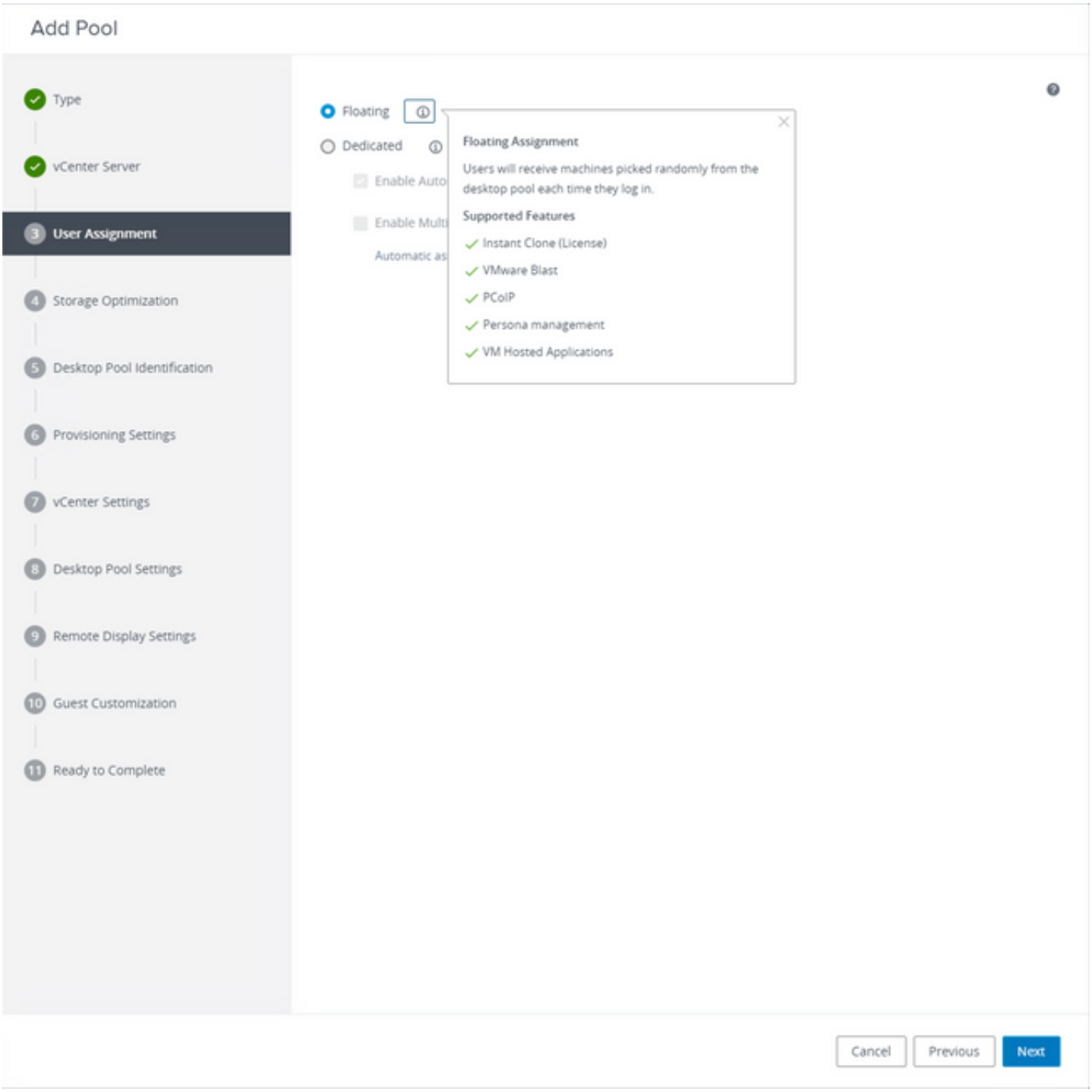
「Automated Desktop Pool」の選択

https://docs.vmware.com/en/VMware-Horizon/2106/virtual-desktops/GUID-6C3AB7F3-0BCF-4423-8418-30CA19CFC8FC.htmlを参照してください。



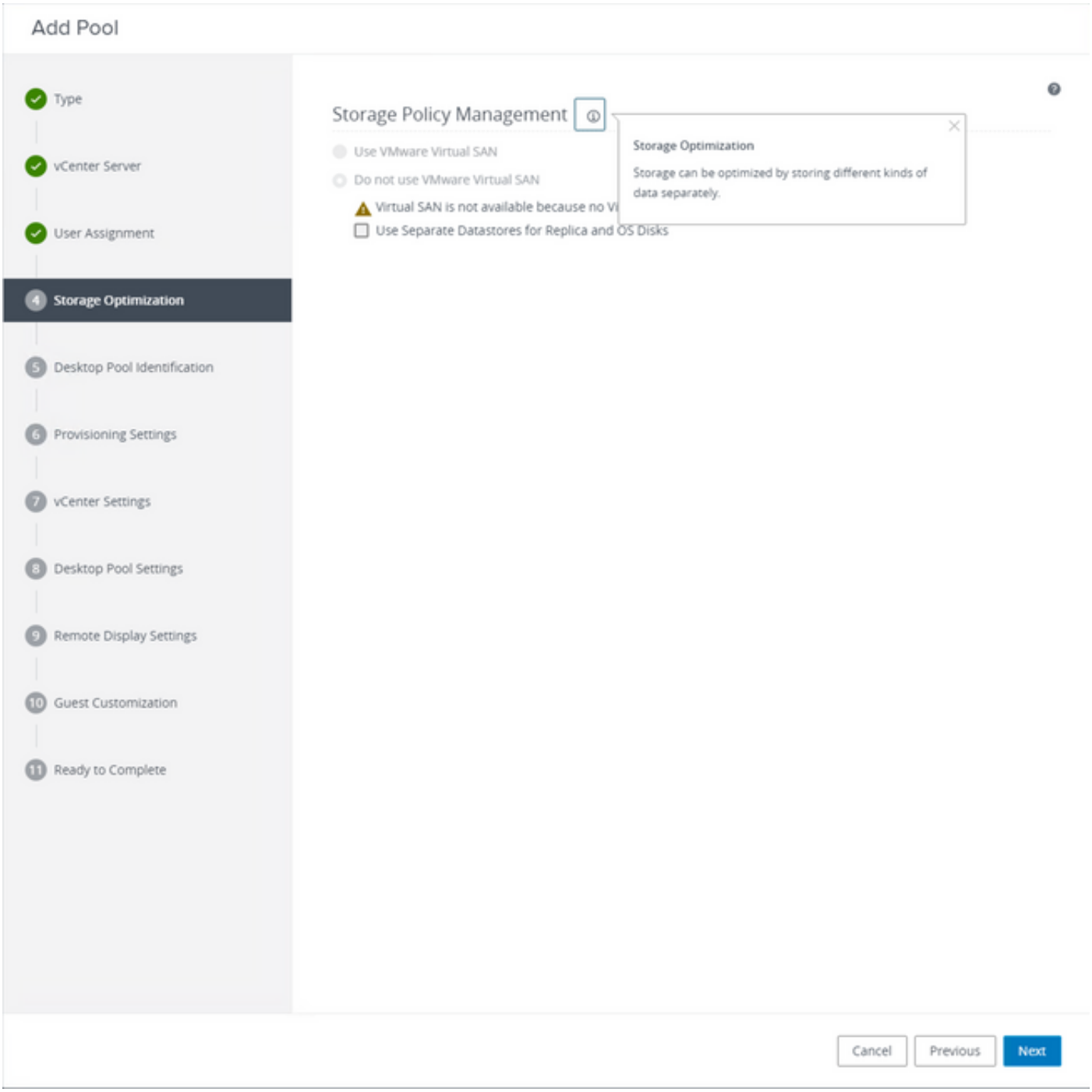
「インスタント・クローン」の選択

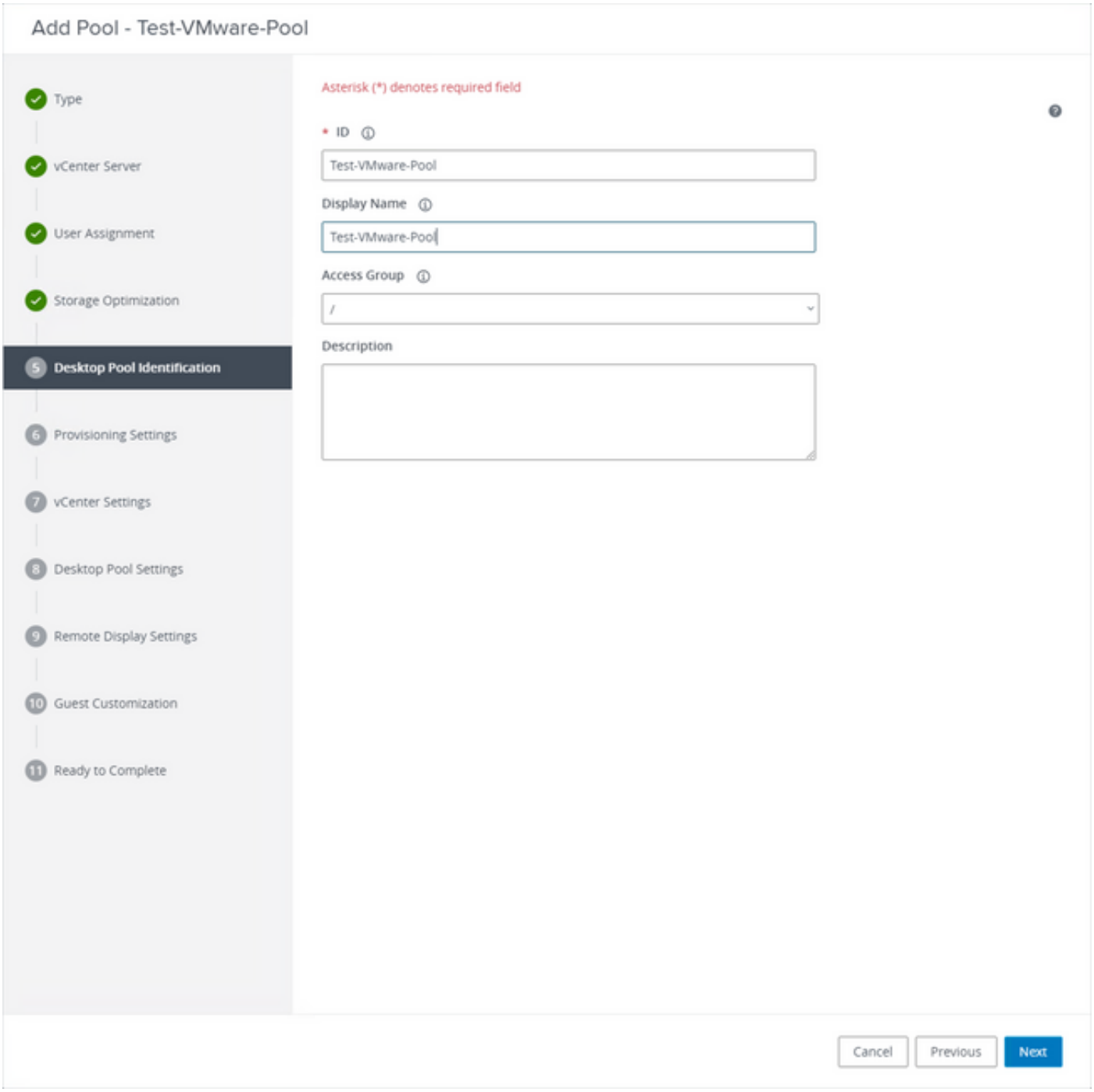
https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-D7C0150E-18CE-4012-944D-4E9AF5B28347.htmlを参照してください。



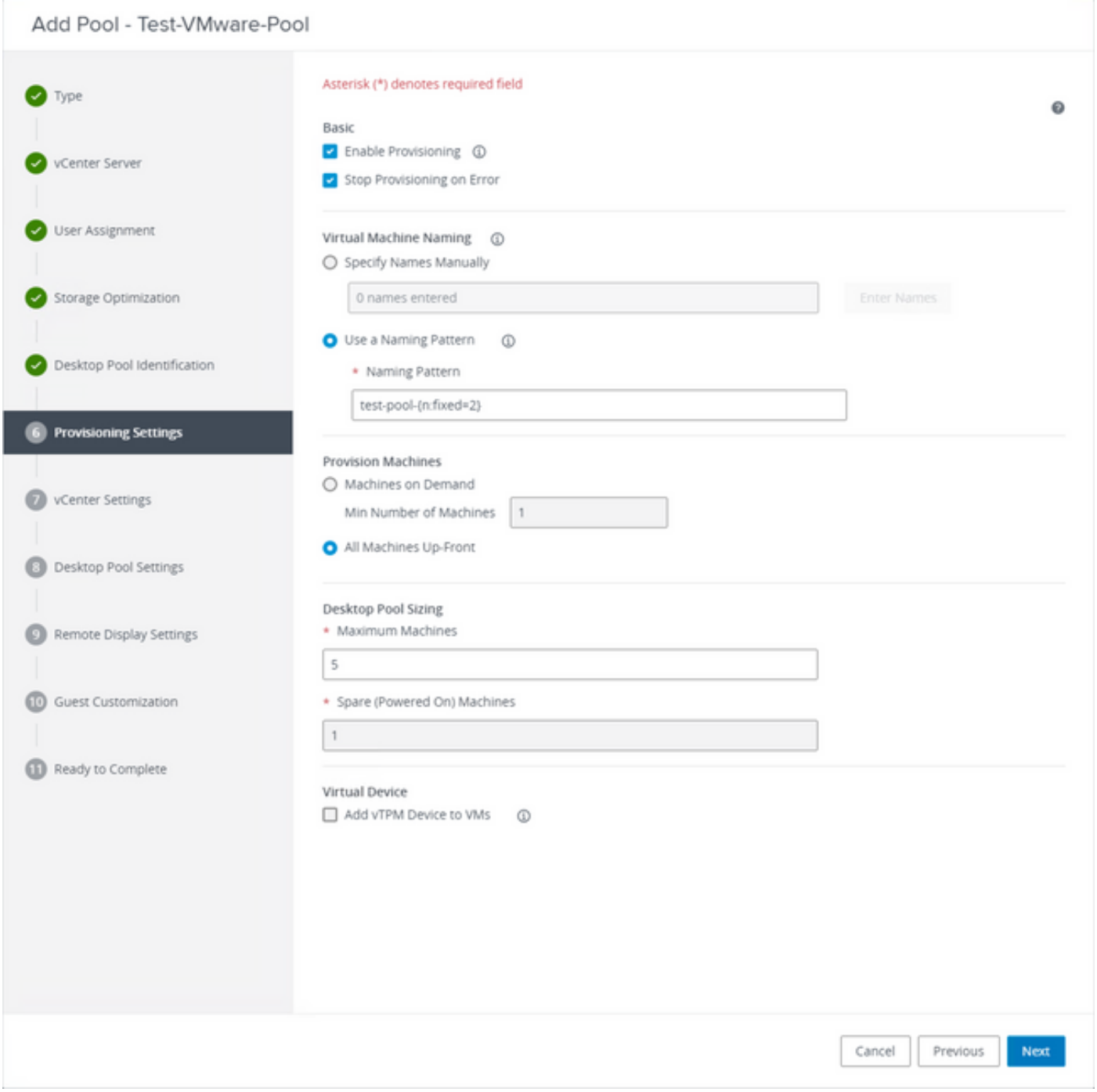
「フローティング」タイプの選択

https://docs.vmware.com/en/VMware-Horizon-Cloud-Service-on-IBM-Cloud/21.1/horizoncloudhosted.deploy/GUID-34C260C7-A63E-452E-88E9-6AB63DEBB416.htmlを参照してください。

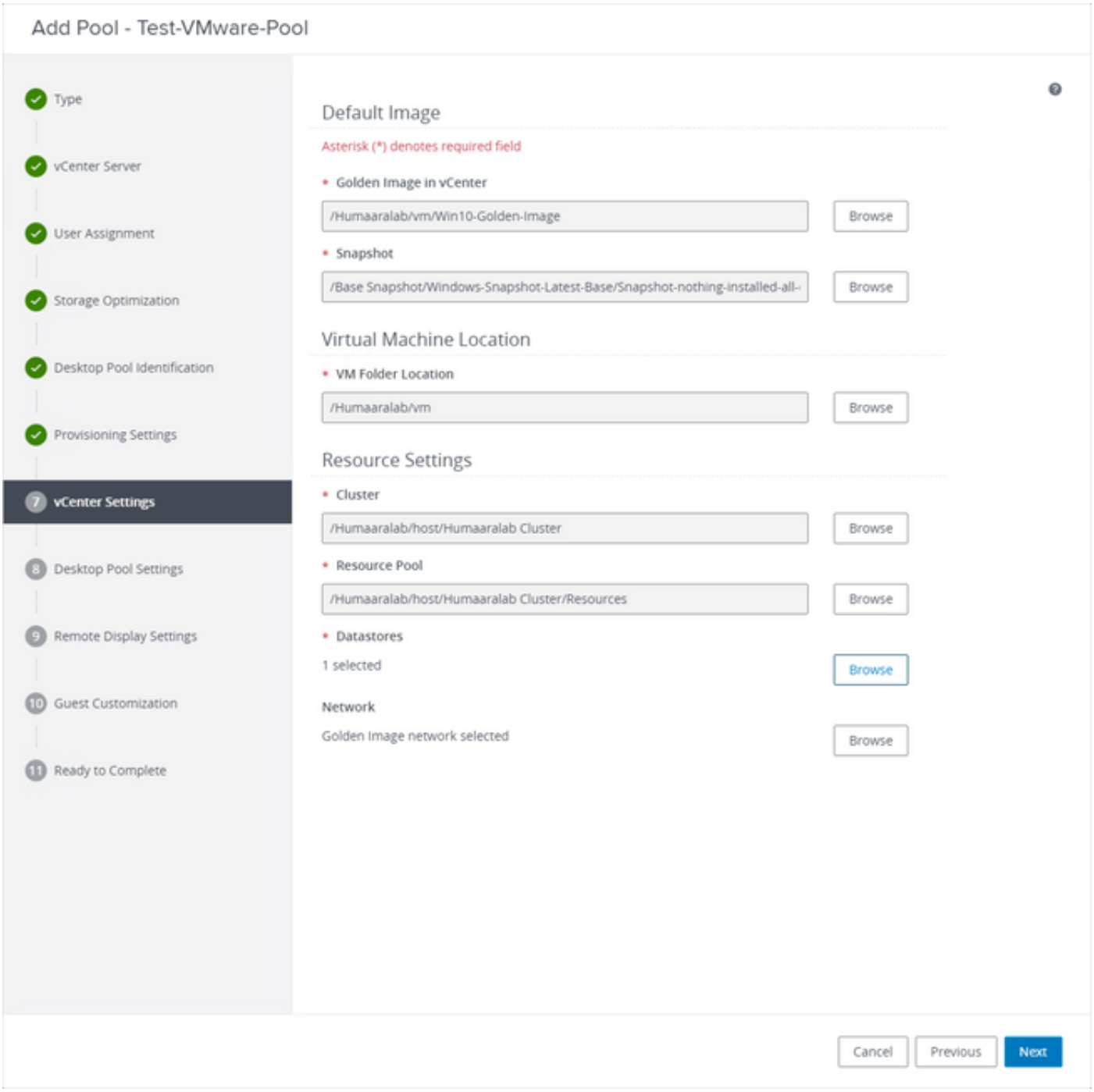

Add Pool
Type
vCenter Server
User Assignment
4 Storage Optimization
5 Desktop Pool Identification
6 Provisioning Settings
7 vCenter Settings
8 Desktop Pool Settings
9 Remote Display Settings
10 Guest Customization
11 Ready to Complete
Storage Policy Management
Use VMware Virtual SAN
Do not use VMware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

デスクトッププール名

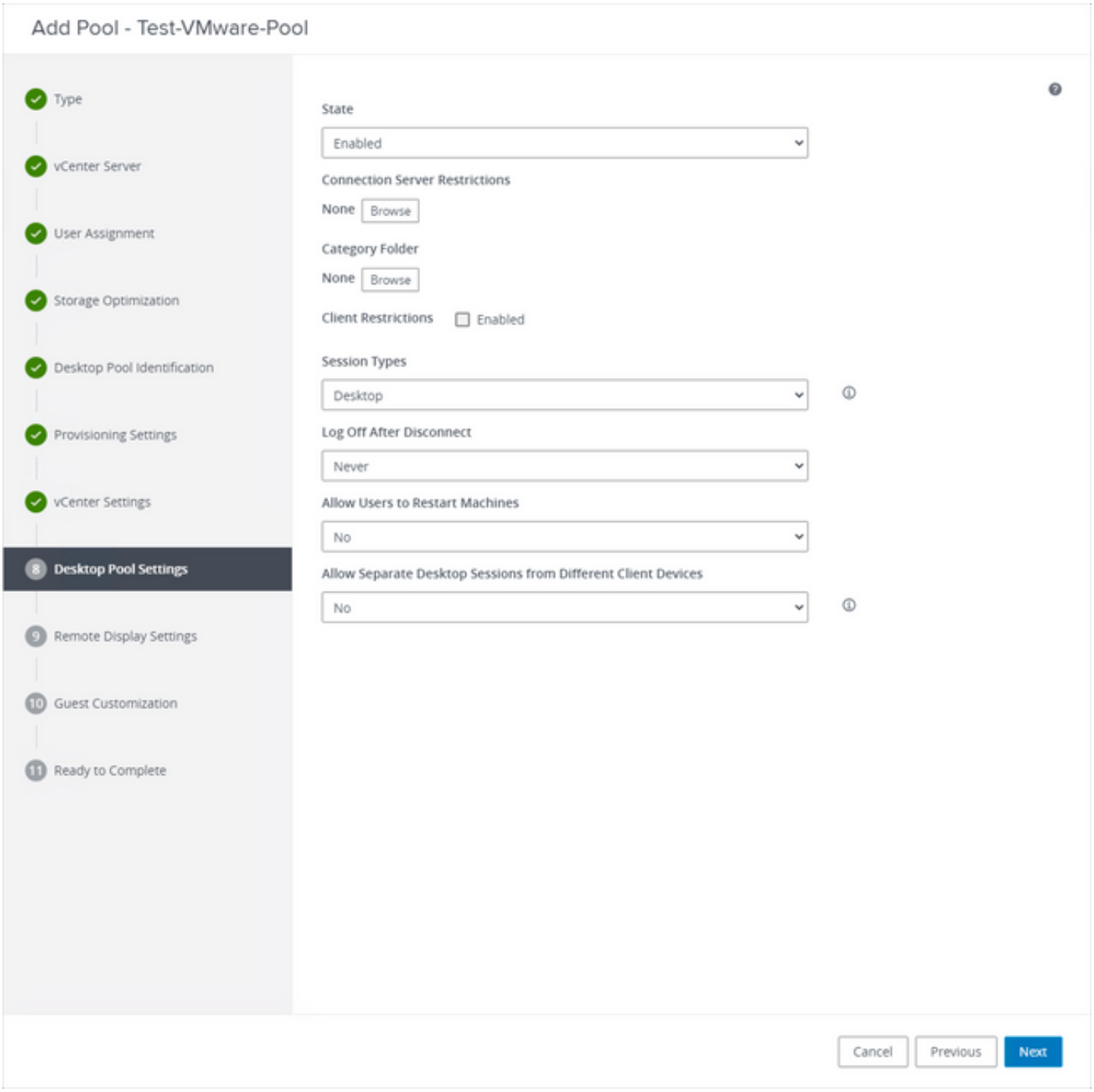


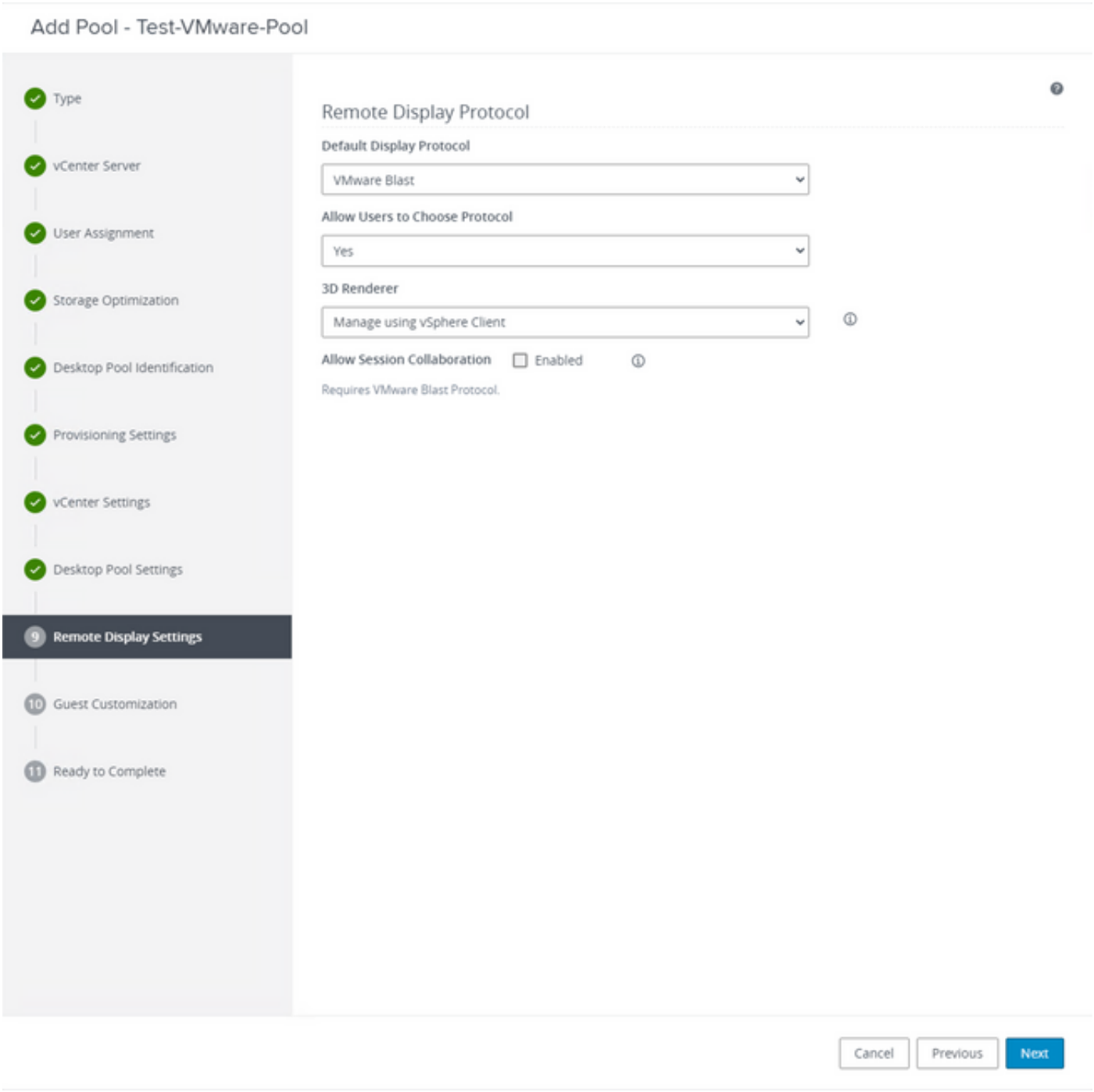
VMware Horizonの命名パターン：https://docs.vmware.com/en/VMware-Horizon/2103/virtual-desktops/GUID-26AD6C7D-553A-46CB-B8B3-DA3F6958CD9C.html

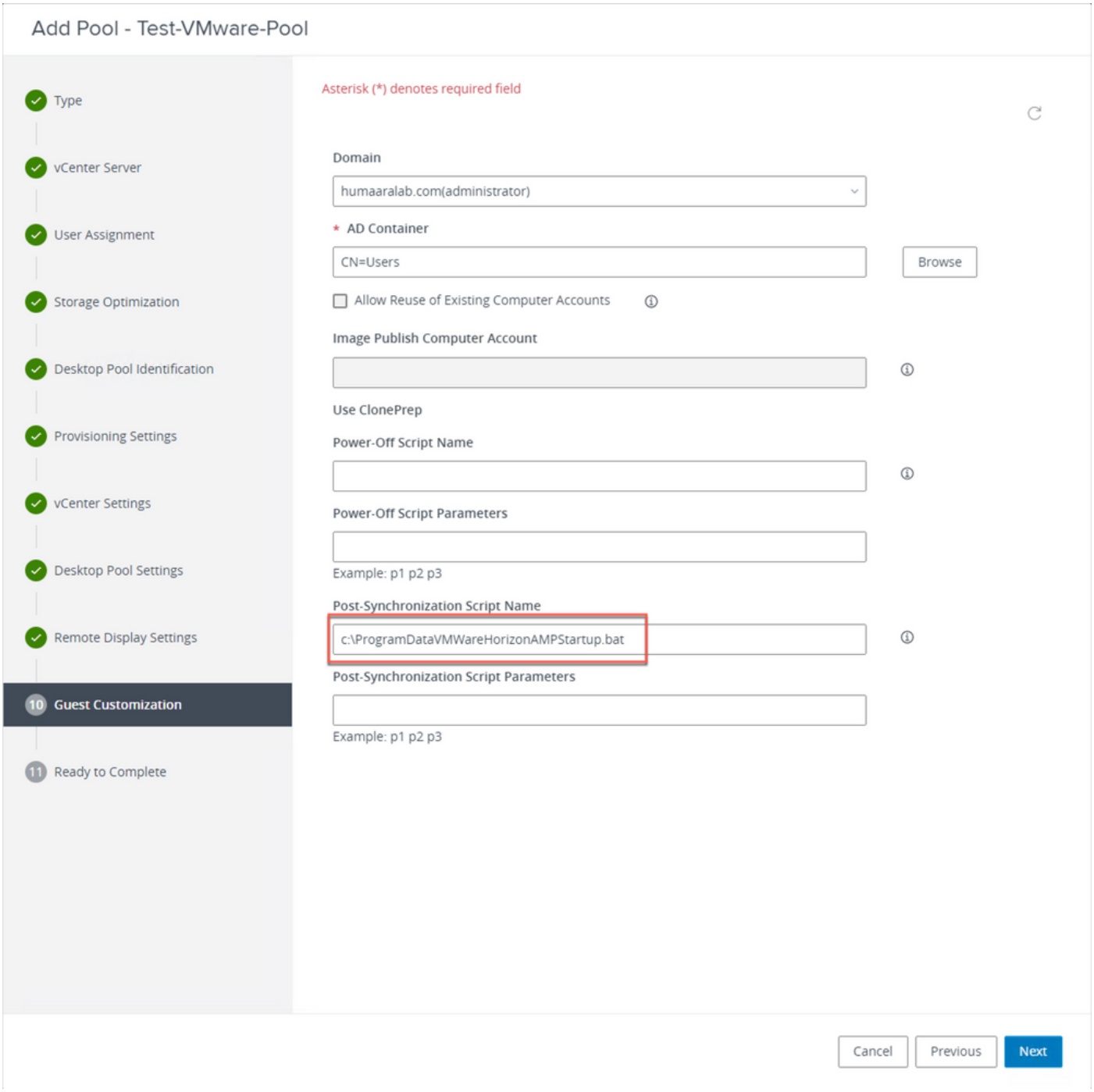


ゴールデンイメージ：これは実際のゴールデンイメージVMです。

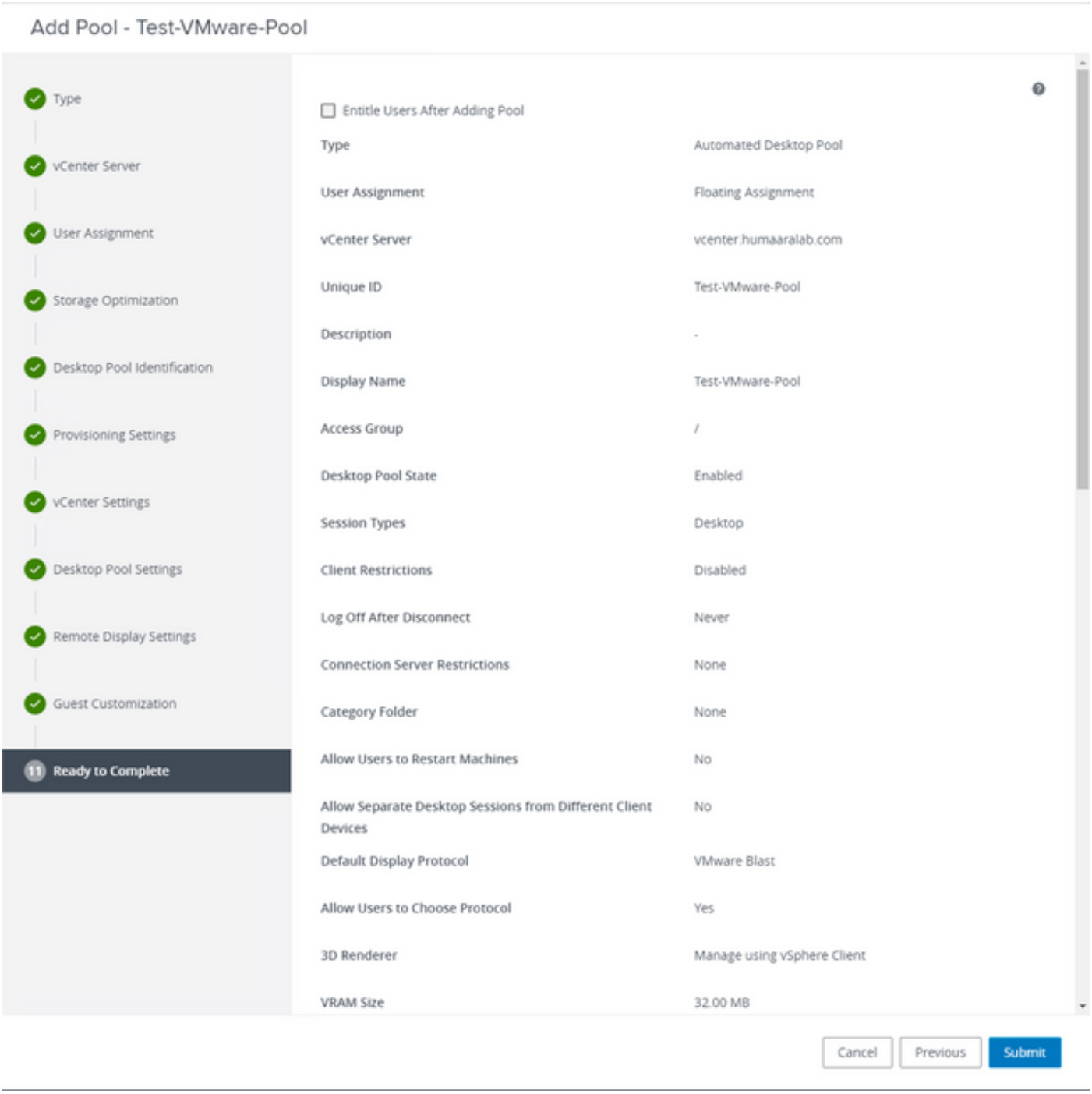
スナップショット：子VMを導入するために使用するイメージです。この値は、変更を加えてゴールデンイメージを更新すると更新されます。その他は、VMware環境固有の設定の一部です。


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.前述のとおり、ウィザードのステップ10.でスクリプトパスを設定します。



8.完了して送信すると、VMware Horizonが構成を開始し、子VMが作成されます。

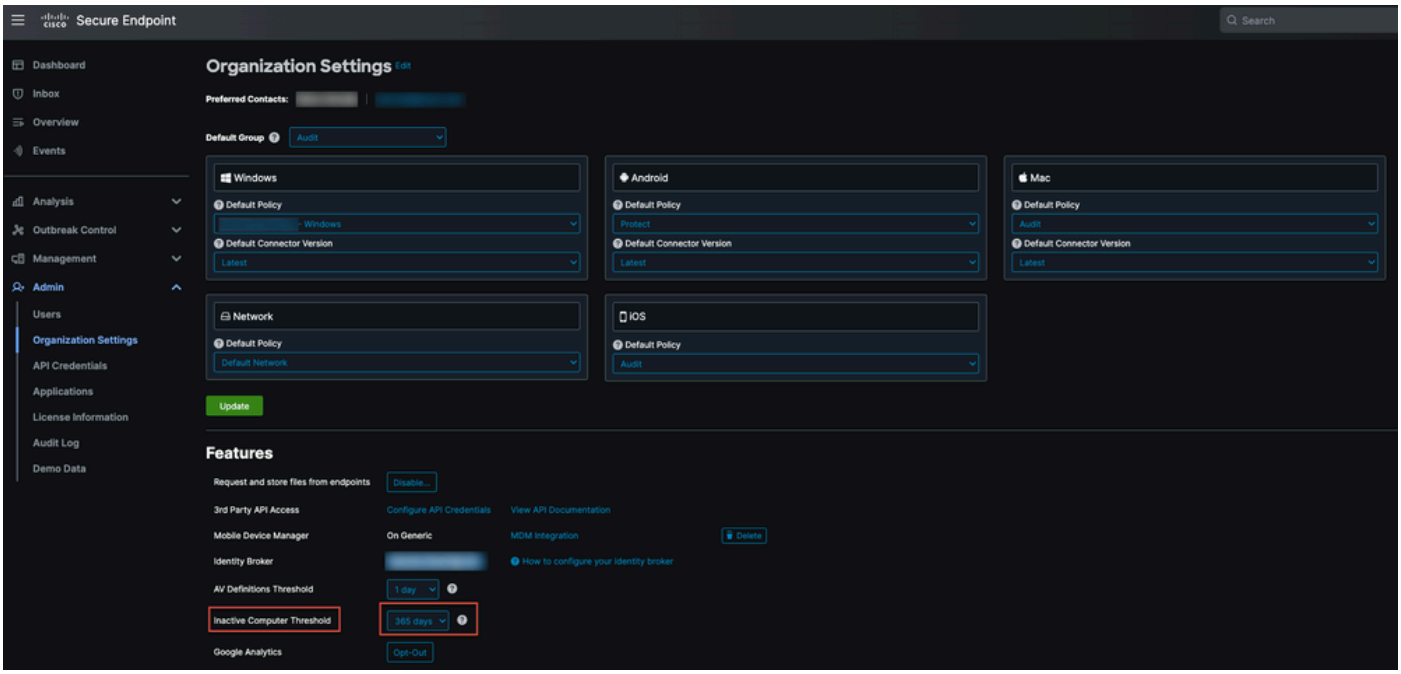
注：これらの手順の詳細については、VMwareのガイドを参照してください。手順については説明を参照してください。

重複するエントリの削除

コネクタの重複エントリを削除する方法がいくつかあります。

1.セキュアエンドポイントポータルの自動削除機能を使用して、重複した（非アクティブな）エントリを削除します。

この設定は、Admin > Organization Settingsにあります



非アクティブコンピュータしきい値では、コネクタがコンピュータ管理ページのリストから削除されるまでの日数を、シスコクラウドへのチェックインなしで指定できます。デフォルト設定は90日です。非アクティブなコンピューターは一覧からのみ削除され、それらのコンピューターによって生成されるすべてのイベントはセキュリティで保護されたエンドポイント組織に残ります。コネクタが再びチェックインすると、コンピュータがリストに再び表示されます。

2.利用可能なオーケストレーションワークフローの利用：https://ciscosecurity.github.io/sxo-05-security-workflows/workflows/secure-endpoint/0056-remove-inactive-endpoints

3.外部で利用可能なスクリプトを使用して、古い/古いUUIDを削除します。
https://github.com/CiscoSecurity/amp-04-delete-stale-guids

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。