Configurer la persistance des identités dans Secure Endpoint

Table des matières

Introduction

Ce document décrit comment passer en revue la fonctionnalité Cisco Secure Endpoint Identity Persistence.

Qu'est-ce que la persistance identitaire ?

La persistance des identités est une fonctionnalité qui vous permet de maintenir un journal des

événements cohérent dans les environnements virtuels ou lorsque les ordinateurs sont recréés en image. Vous pouvez lier un connecteur à une adresse MAC ou à un nom d'hôte de sorte qu'un nouvel enregistrement de connecteur ne soit pas créé chaque fois qu'une nouvelle session virtuelle est démarrée ou qu'un ordinateur est recréé. Cette fonctionnalité est spécialement conçue pour les environnements de machines virtuelles et de travaux pratiques non persistants. La méthode recommandée est le nom d'hôte dans l'ensemble de l'entreprise et activez la fonctionnalité sur les stratégies dans lesquelles vous souhaitez synchroniser les identités.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès au portail Cisco Secure Endpoints
- Vous devez contacter le centre d'assistance technique Cisco pour qu'il active la fonction de persistance de l'identité dans votre entreprise.
- La persistance de l'identité est uniquement prise en charge sur le système d'exploitation Windows

Quand Avez-Vous Besoin De Persistance D'Identité ?

La persistance de l'identité est une fonctionnalité sur les terminaux sécurisés qui permet d'identifier les terminaux sécurisés au moment de l'enregistrement initial du connecteur et de les comparer à des entrées connues précédemment en fonction de paramètres d'identité tels que l'adresse MAC ou le nom d'hôte pour ce connecteur spécifique. La mise en oeuvre de cette fonctionnalité permet non seulement de conserver un nombre de licences correct, mais surtout de suivre correctement les données historiques sur les systèmes non persistants.

Déploiement de terminaux virtuels

L'utilisation la plus courante de la persistance de l'identité dans les déploiements virtuels est le déploiement d'une infrastructure de bureau virtuel (VDI) non persistante. Les environnements de bureau hôtes VDI sont déployés en fonction des demandes ou des besoins des utilisateurs finaux. Cela inclut différents fournisseurs tels que VMware, Citrix, AWS AMI Golden Image Deployment, etc.

L'interface VDI persistante, également appelée « VDI avec état », est une configuration dans laquelle le bureau de chaque utilisateur est personnalisable de manière unique et « persiste » d'une session à l'autre. Ce type de déploiement virtuel n'a pas besoin de la fonctionnalité de persistance d'identité, car ces machines ne sont pas conçues pour être ré-imagées régulièrement.

Comme pour tous les logiciels susceptibles d'interagir avec les performances du point d'extrémité sécurisé, les applications de bureau virtuel doivent être évaluées afin de détecter d'éventuelles exclusions, afin d'optimiser les fonctionnalités et de minimiser l'impact.

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

Déploiement des terminaux physiques

Deux scénarios peuvent s'appliquer au déploiement de la persistance d'identité sur les machines physiques des terminaux sécurisés :

- Lorsque vous déployez ou réinstallez un terminal physique avec une image dorée avec le connecteur Secure Endpoint préinstallé, l'indicateur Goldenimage doit être activé. La persistance de l'identité peut être utilisée pour éviter la duplication dans les instances de machines recréées, mais elle n'est pas requise.

- Lorsque vous déployez ou réinstallez un point de terminaison physique avec une image dorée et installez ultérieurement le connecteur Secure Endpoint, la persistance de l'identité peut être utilisée pour éviter la duplication dans les instances de machines recréées en image, mais elle n'est pas requise.

Généralités sur le processus de persistance des identités

1. Le connecteur est téléchargé avec un jeton dans le fichier policy.xml, qui le relie à la stratégie en question du côté du cloud.
2. Le connecteur est installé, stockant le jeton dans local.xml, et le connecteur envoie une requête POST au portail avec le jeton en question.
3. Le côté cloud suit cet ordre d'opération :
   a. L'ordinateur vérifie la stratégie pour la configuration de la stratégie de synchronisation d'ID. Sans cela, l'enregistrement s'effectue normalement.
   b. En fonction des paramètres de stratégie, Registration recherche le nom d'hôte ou l'adresse MAC dans la base de données existante.
      Dans l'ensemble de l'entreprise : toutes les stratégies sont vérifiées pour une correspondance sur le nom d'hôte ou l'adresse MAC, selon le paramètre. Le GUID d'objet correspondant est noté et renvoyé à l'ordinateur client final. L'ordinateur client prend alors l'UUID et les paramètres de groupe/stratégie de l'hôte correspondant précédemment. Ceci remplace les paramètres de stratégie/groupe installés.
      Dans la stratégie : le jeton correspond à la stratégie du côté du cloud et recherche un objet existant avec le même nom d'hôte ou la même adresse MAC DANS cette stratégie uniquement. S'il en existe un, il prend l'UUID. Si aucun objet existant n'est lié à cette stratégie, un nouvel objet est créé. Remarque : des doublons peuvent exister pour le même nom d'hôte lié à d'autres groupes/stratégies.
   c. Si une correspondance ne peut pas être établie avec un groupe/une stratégie en raison d'un jeton manquant (précédemment enregistré, pratique de déploiement incorrecte, etc.), le connecteur tombe dans le groupe/la stratégie de connecteur par défaut défini sous l'onglet Entreprise. En fonction du paramètre du groupe/de la stratégie, il tente de vérifier toutes les stratégies pour une correspondance (dans l'entreprise), uniquement la stratégie en question (dans l'ensemble de la stratégie) ou aucune stratégie du tout (aucune). Dans cet esprit, il est généralement conseillé de placer votre groupe par défaut pour qu'il contienne les paramètres de synchronisation d'ID souhaités afin que les ordinateurs se synchronisent correctement en cas de problème de jeton.

Identifier les doublons dans votre entreprise

Scripts GitHub disponibles en externe

Rechercher les UUID dupliqués : https://github.com/CiscoSecurity/amp-04-find-duplicate-guids

Raisons de la création de doublons

Quelques instances courantes peuvent provoquer l'affichage de doublons à votre extrémité :

1. Si ces étapes ont été suivies pendant le pool VDI :

- Le déploiement initial sur une VM/VDI non persistante est effectué avec la persistance d'identité désactivée (utilisez une image dorée par exemple).
- La stratégie est mise à jour dans le cloud pour que la persistance de l'identité soit activée, ce qui permet de la mettre à jour sur le terminal pendant la journée.
- Les ordinateurs sont actualisés/recréés (ils utilisent la même image dorée), ce qui ramène la stratégie d'origine sur le terminal sans persistance de l'identité.
- La stratégie localement n'a pas de persistance d'identité, de sorte que le serveur d'enregistrement ne vérifie pas les enregistrements précédents.
- Ce flux génère des doublons.

2. L'utilisateur déploie l'image dorée d'origine avec la persistance de l'identité activée dans la stratégie dans un groupe, puis déplace un terminal vers un autre groupe à partir du portail Secure Endpoints. L'enregistrement d'origine est alors placé dans le groupe « déplacé vers », puis de nouvelles copies sont créées dans le groupe d'origine lorsque les machines virtuelles sont redimensionnées/redéployées.

Remarque : cette liste n'est pas exhaustive et ne contient que quelques-uns des scénarios les plus courants.

Problèmes/symptômes courants avec un déploiement de persistance d'identité incorrect

Une implémentation incorrecte de la persistance de l'identité peut provoquer les problèmes/symptômes suivants :

- Nombre de sièges de connecteur incorrect
- Résultats rapportés incorrects
- Discordance des données de trajectoire des périphériques
- Échanges de noms de machine dans les journaux d'audit
- Les connecteurs s'enregistrent et se désenregistrent de manière aléatoire à partir de la console
- Les connecteurs ne communiquent pas correctement sur le cloud
- Duplication UUID

- Duplication du nom de machine
- Incohérence des données
- Les ordinateurs s'enregistrent auprès de la stratégie/groupe professionnel par défaut après recomposition

- Déploiement manuel avec la persistance d'identité activée sur la stratégie.

- Si vous déployez le point de terminaison manuellement via le commutateur de ligne de commande avec la persistance d'identité déjà activée dans la stratégie, puis que vous désinstallez le point de terminaison ultérieurement et que vous essayez de réinstaller le package avec un autre groupe/stratégie, le point de terminaison bascule automatiquement vers la stratégie d'origine.

- Sortie des journaux SFC montrant le commutateur de stratégie seul avec en 1-10sec

```
(167656, +0 ms) Dec 14 11:37:17 [1308]: Util::VerifyOsVersion: ret 0
(167656, +0 ms) Dec 14 11:37:17 [1308]: ERROR: ETWEnableConfiguration::IsETWEnabled: ETW not 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
```

L'autre effet secondaire si vous essayez d'installer un connecteur qui appartient à un autre groupe. Vous verrez dans le portail que le connecteur est attribué au groupe correct mais avec une stratégie d'origine « incorrecte »

Cela est dû à la façon dont la persistance de l'identité (ID SYNC) fonctionne.

Sans ID SYNC une fois que le connecteur est complètement désinstallé ou en utilisant le commutateur de ligne de commande de ré-enregistrement. Vous devriez voir une nouvelle date de création et un nouveau GUID de connecteur en cas de désinstallation ou juste un nouveau GUID de connecteur en cas de commande de réenregistrement. Cependant, avec ID SYNC qui n'est pas possible ID SYNC remplace avec l'ancien GUID et DATE. C'est ainsi que nous 'synchronisons' l'hôte.

Si ce problème est observé, le correctif doit être mis en oeuvre par le biais de la modification de stratégie. Vous devrez replacer le ou les terminaux affectés dans le groupe/la stratégie d'origine et vous assurer que la stratégie est synchronisée. Ensuite, replacez le ou les terminaux dans le groupe/la stratégie souhaité(s)

Meilleures pratiques de déploiement

Configurer le fichier snapvol

Si vous utilisez des volumes d'applications pour votre infrastructure VDI, il est recommandé d'apporter ces modifications de configuration à votre configuration snapvol.cfg

Ces exclusions doivent être implémentées dans le fichier snapvol.cfg :

Chemins :

- 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

Clés de registre :

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

Sur les systèmes x64, ajoutez les éléments suivants :

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Immunet Protéger
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstal Protéger

Références:

- 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

Planification de stratégie de portail

Voici quelques-unes des meilleures pratiques qui doivent être suivies lorsque vous mettez en oeuvre la persistance de l'identité sur le portail Secure Endpoint :

1. Il est fortement recommandé d'utiliser des stratégies/groupes distincts pour les terminaux de persistance de l'identité afin de faciliter la ségrégation.

2. Si vous prévoyez d'utiliser l'isolation des points de terminaison et d'implémenter l'action Déplacer l'ordinateur vers le groupe en cas de compromission. La persistance de l'identité doit également être activée pour le groupe de destination et ne doit être utilisée que pour les ordinateurs VDI.

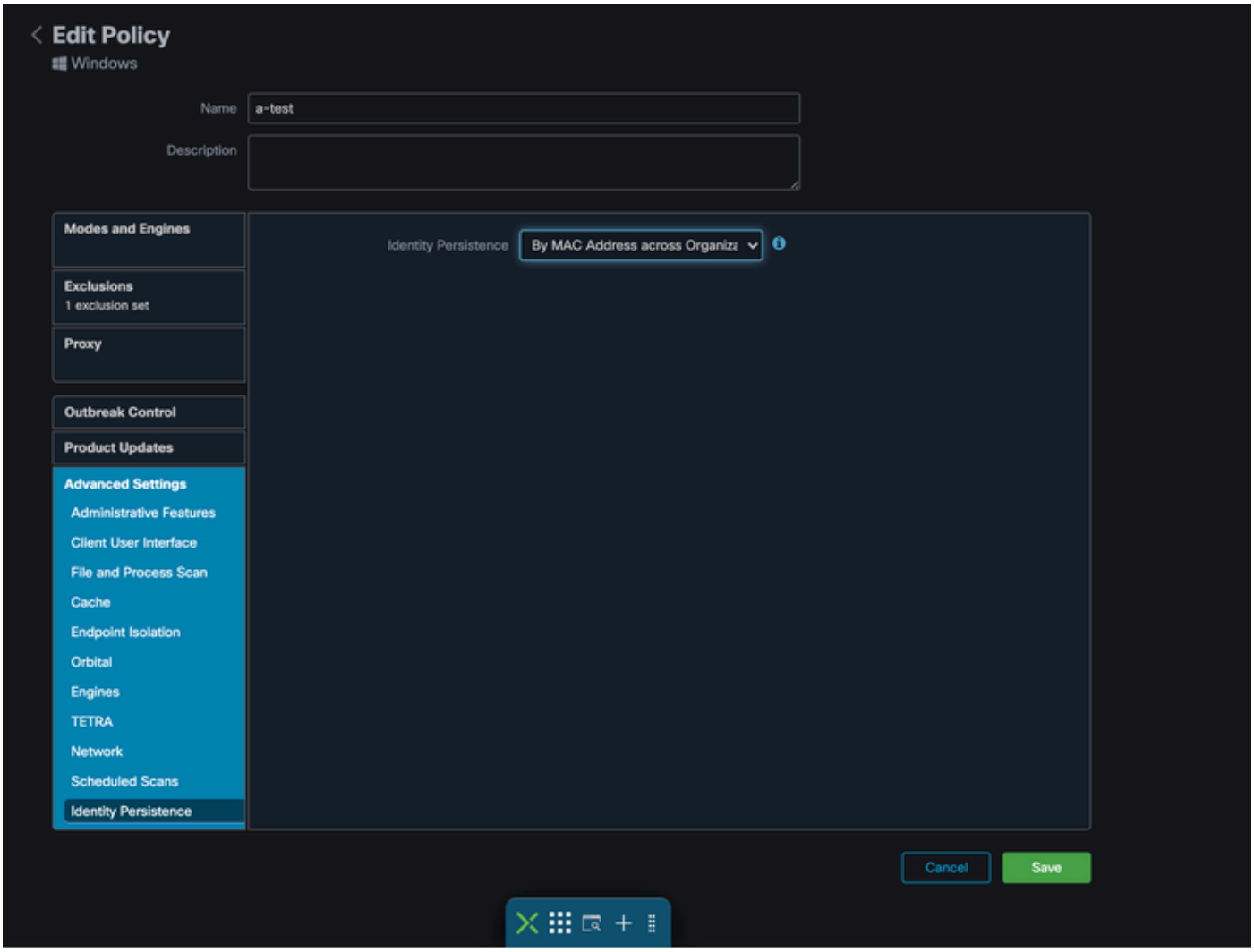
3. Il n'est pas recommandé d'activer la persistance de l'identité sur le groupe/la stratégie par défaut sur les paramètres de votre organisation, sauf si la persistance de l'identité a été activée sur toutes les stratégies avec l'étendue des paramètres sur l'ensemble de l'organisation.

Configuration

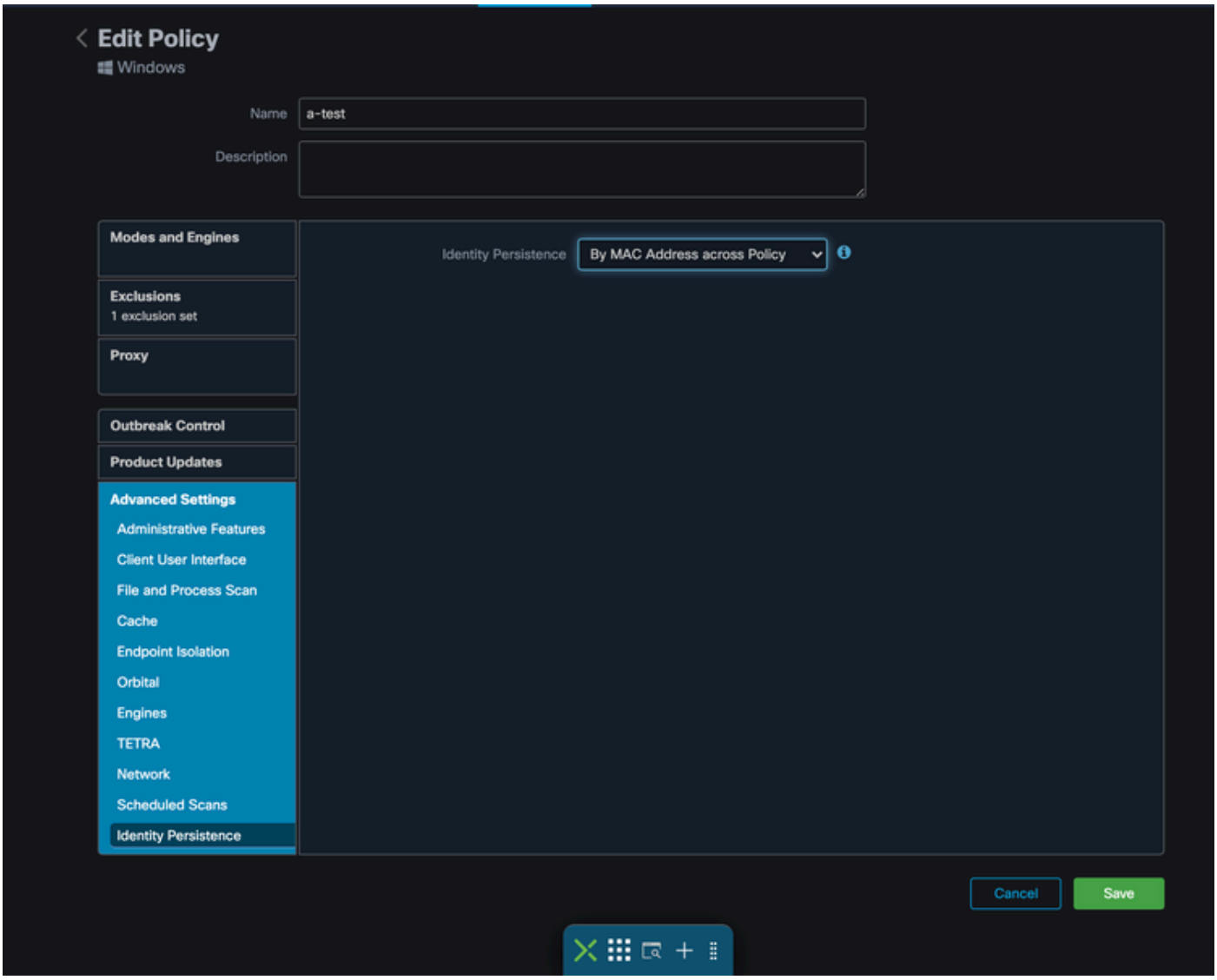
Suivez ces étapes afin de déployer le connecteur Secure Endpoint avec la persistance d'identité :

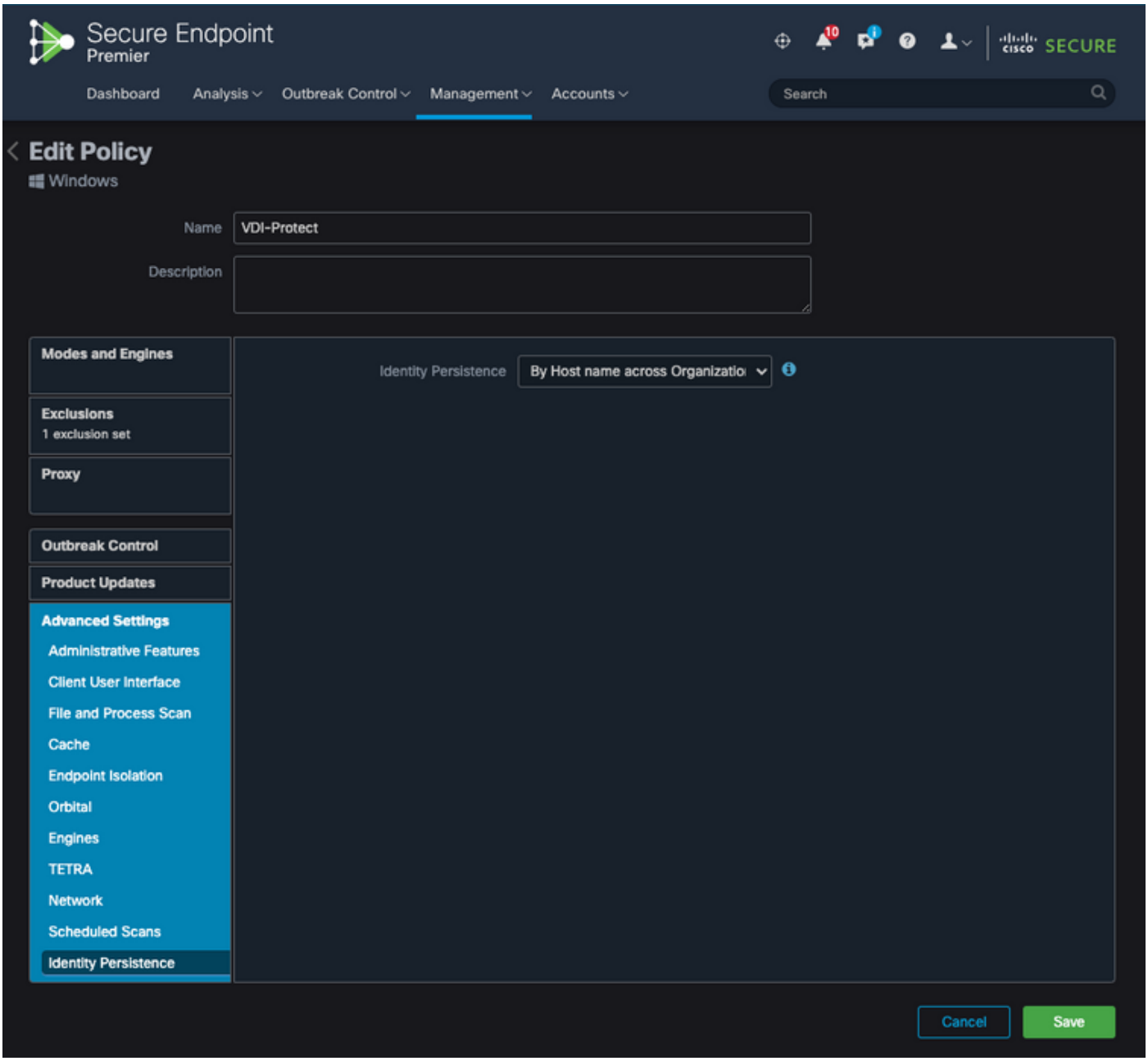
Étape 1. Appliquez le paramètre Persistance de l'identité souhaité à vos stratégies :

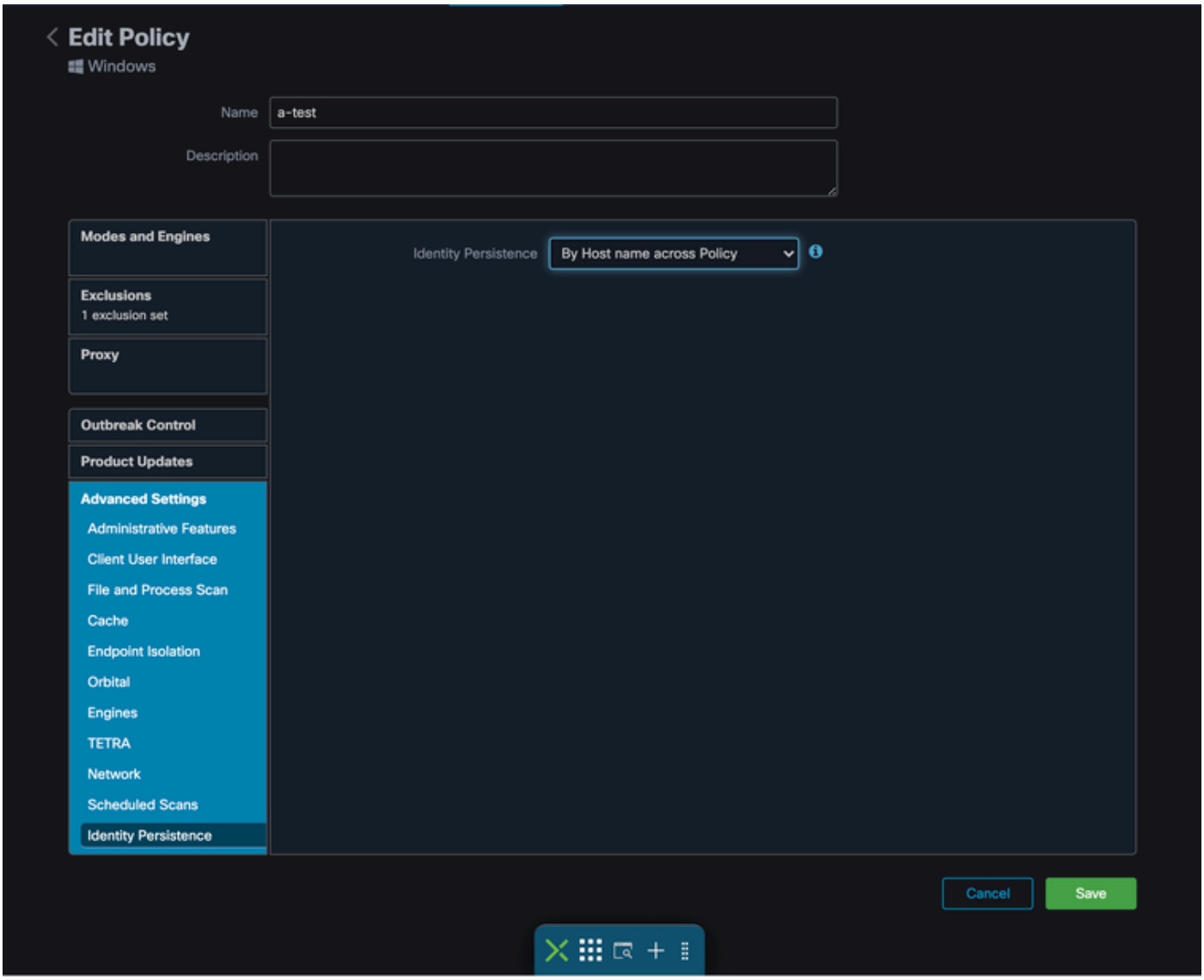
- Dans le portail Secure Endpoint, accédez à Management > Policies.
- Sélectionnez la stratégie sur laquelle vous souhaitez activer la persistance de l'identité, puis cliquez sur Modifier.
- Accédez à l'onglet Paramètres avancés, puis cliquez sur l'onglet Persistance d'identité en bas.
- Sélectionnez la liste déroulante Persistance de l'identité et choisissez l'option la plus adaptée à votre environnement. Reportez-vous à cette image.


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

Test - 123


Edit Policy
Windows
Name
a-test
Description
Modes and Engines
Exclusions
1 exclusion set
Proxy
Outbreak Control
Product Updates
Advanced Settings
Administrative Features
Client User Interface
File and Process Scan
Cache
Endpoint Isolation
Orbital
Engines
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



Vous avez le choix entre cinq options.

- Notez que la fonctionnalité n'est pas activée. Les UUID de connecteur ne sont en aucun cas synchronisés avec les nouvelles installations de connecteur. Chaque nouvelle installation génère un nouvel objet machine.
- Par adresse MAC dans l'entreprise : les installations nouvelles ou actualisées recherchent l'enregistrement Connector le plus récent qui a la même adresse MAC afin de synchroniser les données historiques précédentes avec la nouvelle inscription. Ce paramètre examine tous les enregistrements d'entreprise

  dans toutes les stratégies de l'organisation pour lesquelles la synchronisation des identités est définie sur une valeur autre que None. Le connecteur peut mettre à jour sa stratégie pour refléter l'installation précédente si elle diffère de la nouvelle.

- Par adresse MAC dans la stratégie : les installations nouvelles ou actualisées recherchent l'enregistrement Connector le plus récent qui a la même adresse MAC afin de synchroniser les données historiques précédentes avec le nouvel enregistrement. Ce paramètre examine uniquement les enregistrements associés à la stratégie utilisée dans le déploiement. Si le connecteur n'était pas installé précédemment dans cette stratégie mais était déjà actif dans

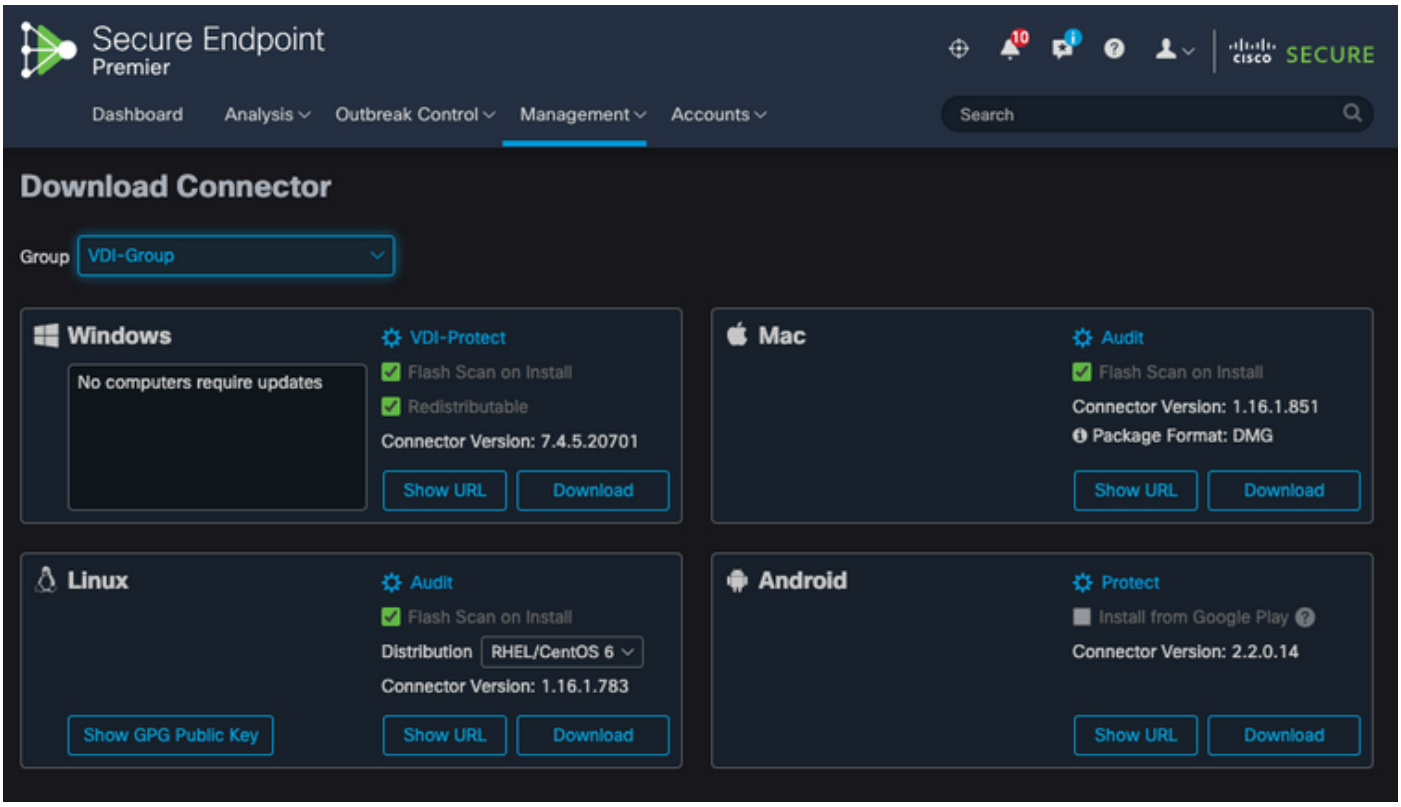
une autre, il peut créer des doublons.

- Par nom d'hôte dans l'entreprise : les installations nouvelles ou actualisées recherchent l'enregistrement Connector le plus récent ayant le même nom d'hôte afin de synchroniser les données historiques précédentes avec le nouvel enregistrement. Ce paramètre parcourt tous les enregistrements de l'entreprise, quels que soient les paramètres de persistance des identités définis dans d'autres stratégies et le connecteur peut mettre à jour sa stratégie pour refléter l'installation précédente si elle diffère de la nouvelle. Le nom d'hôte inclut le nom de domaine complet (FQDN), de sorte que des doublons peuvent se produire si le connecteur se déplace régulièrement entre les réseaux (comme un ordinateur portable).
- Par nom d'hôte dans la stratégie : les installations nouvelles ou actualisées recherchent l'enregistrement Connector le plus récent qui a le même nom d'hôte afin de synchroniser les données historiques précédentes avec le nouvel enregistrement. Ce paramètre examine uniquement les enregistrements associés à la stratégie utilisée pour le déploiement. Si le connecteur n'était pas installé précédemment dans cette stratégie mais était déjà actif dans une autre, il peut créer des doublons. Le nom d'hôte inclut le nom de domaine complet (FQDN), de sorte que les doublons peuvent également se produire si le connecteur se déplace régulièrement entre les réseaux (comme un ordinateur portable).

Remarque : si vous choisissez d'utiliser la persistance de l'identité, Cisco vous suggère d'utiliser Par nom d'hôte dans l'entreprise ou la politique. Une machine a un nom d'hôte, mais peut avoir plusieurs adresses MAC et de nombreuses machines virtuelles clonent les adresses MAC.

Étape 2. Téléchargez le connecteur Secure Endpoint Connector.

- Accédez à Management > Download Connector.
- Sélectionnez le groupe correspondant à la stratégie que vous avez modifiée à l'étape 1.
- Cliquez sur Télécharger pour le Connecteur Windows comme illustré dans l'image.



Étape 3. Déployez le connecteur sur les terminaux.

- Vous pouvez maintenant utiliser le connecteur téléchargé pour installer manuellement Secure Endpoint (avec la persistance de l'identité activée) sur vos terminaux.
- Sinon, vous pouvez également déployer le connecteur à l'aide d'une image dorée (voir image)

Remarque : vous devez sélectionner le programme d'installation redistribuable. Il s'agit d'un fichier d'environ 57 Mo (la taille peut varier selon les versions récentes) qui contient les programmes d'installation 32 bits et 64 bits. Afin d'installer le connecteur sur plusieurs ordinateurs, vous pouvez placer ce fichier sur un partage réseau ou le pousser vers tous les ordinateurs en conséquence. Le programme d'installation contient un fichier policy.xml utilisé comme fichier de configuration pour l'installation.

Création d'image dorée

Suivez les directives des meilleures pratiques du document du Fournisseur (VMware, Citrix, AWS, Azure, etc.) lorsque vous créez une image d'or à utiliser pour le processus de clonage VDI.

Par exemple, le processus VMware Golden Image : [https://docs.vmware.com/en/VMware-Horizon/2106/virtual-desktops/GUID-D9C46AEF-1C41-4711-BF9E-84362EBE6ABF.html.](https://docs.vmware.com/en/VMware-Horizon/2106/virtual-desktops/GUID-D9C46AEF-1C41-4711-BF9E-84362EBE6ABF.html)

Comme vous avez identifié VMware, le processus de composition AWS redémarre les machines virtuelles clonées (machines virtuelles enfant) plusieurs fois avant la finalisation de la configuration de la machine virtuelle. Cela entraîne des problèmes avec le processus d'enregistrement du point de terminaison sécurisé, car à ce moment-là, les machines virtuelles clonées (machines virtuelles

enfant) n'ont pas les noms d'hôte finaux/corrects attribués et cela entraîne l'utilisation du nom d'hôte de l'image dorée par les machines virtuelles clonées (machines virtuelles enfant) et l'enregistrement sur le cloud du point de terminaison sécurisé. Cela interrompt le processus de clonage et entraîne des problèmes.

Il ne s'agit pas d'un problème lié au processus du connecteur Secure Endpoint, mais d'une incompatibilité avec le processus de clonage et l'enregistrement Secure Endpoint. Afin d'éviter ce problème, nous avons identifié quelques changements à mettre en oeuvre dans le processus de clonage qui aident à résoudre ces problèmes.

Il s'agit des modifications qui doivent être implémentées sur la machine virtuelle Golden Image avant que l'image ne soit figée pour être clonée

1. Utilisez toujours le drapeau Goldenimage sur l'image d'or au moment de l'installation de Secure Endpoint.

2. Mettez en oeuvre le script de configuration Golden Image et le script de démarrage Golden Image pour trouver les scripts qui aideraient à activer le service de point de terminaison seulement quand nous avons un nom d'hôte final mis en oeuvre sur les machines virtuelles clonées (machines virtuelles enfant). Reportez-vous à la section Problèmes de duplication VMware Horizon pour plus de détails.

Indicateur de remplacement d'image dorée

Lorsque vous utilisez le programme d'installation, l'indicateur à utiliser pour les images dorées est /goldenimage 1.

L'indicateur d'image dorée empêche le connecteur de démarrer et de s'enregistrer sur l'image de base ; ainsi, au prochain démarrage de l'image, le connecteur est dans l'état fonctionnel dans lequel il a été configuré par la stratégie qui lui a été attribuée.

Pour plus d'informations sur les autres indicateurs, vous pouvez utiliser, veuillez consulter cet article.

Lorsque vous utilisez le programme d'installation, le nouvel indicateur à utiliser pour les images dorées est /goldenimage [1|0]

0 - Valeur par défaut : cette valeur ne déclenche pas l'option d'image dorée et fonctionne comme si le programme d'installation était exécuté sans l'option. N'ignorez pas l'enregistrement et le démarrage du connecteur initial lors de l'installation.

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

1 - Installation en tant qu'image dorée. C'est l'option typique utilisée avec l'indicateur et c'est la seule utilisation prévue. Ignore l'enregistrement initial du connecteur et le démarrage lors de l'installation.

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

Étapes de création d'image dorée

Il est recommandé d'installer le connecteur en dernier pour la préparation de l'image dorée.

1. Préparez l'image système Windows selon vos besoins ; installez tous les logiciels et configurations requis pour l'image système Windows, à l'exception du connecteur.
2. Installez le connecteur Cisco Secure Endpoint.

Utilisez l'indicateur/goldenimage 1afin d'indiquer à l'installateur qu'il s'agit d'un déploiement d'image dorée.

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

3. Implémentez la logique de script (si nécessaire) comme décrit ici

4. Installation complète

5. Gelez votre image dorée

Une fois que les applications ont été installées sur l'image d'or, que le système a été préparé et que le terminal sécurisé a été installé avec l'indicateur/goldenimageflag, l'hôte est prêt à être figé et distribué. Une fois l'hôte cloné démarré, Secure Endpoint démarre et s'enregistre sur le cloud. Aucune autre action n'est requise en ce qui concerne la configuration du connecteur, sauf si vous souhaitez apporter des modifications à la stratégie ou à l'hôte. Si des modifications sont apportées après l'enregistrement de l'image dorée, ce processus doit être redémarré. L'indicateur empêche le connecteur de démarrer et de s'enregistrer sur l'image de base. Au prochain démarrage de l'image, le connecteur sera dans l'état fonctionnel dans lequel il a été configuré par la stratégie qui lui a été attribuée.

Remarque : si l'image d'or est enregistrée sur le cloud Secure Endpoint avant que vous ne puissiez figer la machine virtuelle, il est recommandé de désinstaller et de réinstaller Secure Endpoint sur la machine virtuelle Golden Image, puis de figer à nouveau la machine virtuelle pour empêcher l'enregistrement et les problèmes de connecteur en double. Il n'est pas recommandé de modifier les valeurs du Registre pour Secure Endpoint dans le cadre de ce processus de désinstallation.

Mettre à jour l'image dorée

Vous avez deux options lorsque vous devez mettre à jour une image dorée afin de conserver un

connecteur non enregistré.

Processus recommandé

1. Désinstallez le connecteur.
2. Installer les mises à jour/mises à niveau de l'hôte.
3. Réinstallez le connecteur après le processus d'image dorée à l'aide des indicateurs d'image dorée.
4. L’hôte ne doit pas démarrer le connecteur si le processus est suivi.
5. Gelez l'image.
6. Avant de lancer des clones, vérifiez que l'image d'or ne s'est pas enregistrée sur le portail pour empêcher les hôtes dupliqués indésirables.

Processus alternatif

1. Assurez-vous que l'hôte n'a aucune connectivité à Internet pour empêcher l'enregistrement du connecteur.
2. Arrêtez le service de connexion.
3. Installer les mises à jour
4. Geler l'image une fois les mises à jour terminées
5. Le connecteur ne doit pas être enregistré afin d’empêcher la duplication des hôtes. Lorsque vous supprimez la connectivité, cela l'empêche d'accéder au cloud pour s'y inscrire. En outre, le connecteur en cours d'arrêt conserve cet état jusqu'au prochain redémarrage, ce qui permet aux clones de s'enregistrer en tant qu'hôtes uniques.
6. Avant de lancer des clones, vérifiez que l'image d'or ne s'est pas enregistrée sur le portail pour empêcher les hôtes dupliqués indésirables.

Code image doré

Cette section contient les extraits de code qui peuvent aider à prendre en charge le processus Golden Image et à empêcher les doublons de connecteur lors de la mise en oeuvre de la persistance d'identité.

Script de configuration Golden Image

Description du script de configuration

Le premier script, 'Setup', est exécuté sur l'image d'or avant de la cloner. Il doit être exécuté manuellement une seule fois. Son objectif principal est d'établir des configurations initiales qui permettront au script suivant de fonctionner correctement sur les machines virtuelles clonées. Ces configurations incluent :

- Remplacer le démarrage du service Cisco Secure Endpoint par manuel pour éviter le démarrage automatique.
- Créer une tâche planifiée qui exécute le script suivant (Démarrage) au démarrage du système avec les privilèges les plus élevés.
- Création d'une variable d'environnement système appelée « AMP_GOLD_HOST » qui

stocke le nom d'hôte de l'image Golden. Il est utilisé par le script de démarrage pour vérifier si nous devons annuler les modifications

Code script de configuration

```
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 /
```

Le code du script de configuration est assez simple :

Ligne 2 : Modifie le type de démarrage du service de protection contre les programmes malveillants en manuel.

Ligne 5 : Crée une nouvelle variable d'environnement appelée « AMP_GOLD_HOST » et y enregistre le nom d'hôte de l'ordinateur actuel.

Ligne 9 : Crée une tâche planifiée nommée « Startamp » qui exécute le script « Startup » spécifié au démarrage du système avec les privilèges les plus élevés, sans avoir besoin d'un mot de passe.

Script de démarrage Golden Image

Description du script de démarrage

Le deuxième script, « Démarrage », s'exécute à chaque démarrage du système sur les machines virtuelles clonées. Son objectif principal est de vérifier si la machine actuelle a le nom d'hôte de l'« image dorée » :

- Si la machine actuelle est l'image d'or, aucune action n'est entreprise et le script se termine. Secure Endpoint continuera à s'exécuter au démarrage du système puisque nous maintenons la tâche planifiée.
- Si la machine actuelle n'est PAS l'image 'Golden', les modifications apportées par le premier script sont réinitialisées :
    - Remplacement automatique de la configuration de démarrage du service Cisco Secure Endpoint.
    - Démarrage du service Cisco Secure Endpoint.
    - Suppression de la variable d'environnement « AMP_GOLD_HOST ».
    - Suppression de la tâche planifiée qui exécute le script de démarrage et suppression du script lui-même.

Code de script de démarrage

```
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
```

Ligne 2 : compare le nom d'hôte actuel avec la valeur stockée "AMP_GOLD_HOST" ; s'ils sont identiques, le script passe à la "même" étiquette, sinon, il passe à la "différente" étiquette.

Ligne 4-6 : Lorsque la « même » étiquette est atteinte, le script ne fait rien puisqu'il s'agit toujours de l'image d'or et passe à l'étiquette « exit ».

Ligne 8-16 : si l'étiquette « not same » est atteinte, le script effectue les actions suivantes :

- Modifie le type de démarrage du service de protection contre les programmes malveillants en automatique.
- Démarre le service de protection contre les programmes malveillants.
- Supprime la variable d'environnement « AMP_GOLD_HOST ».
- Supprime la tâche planifiée nommée « Startamp »

Remarque : veuillez noter que les scripts contenus dans ce document ne sont pas officiellement pris en charge par le TAC.

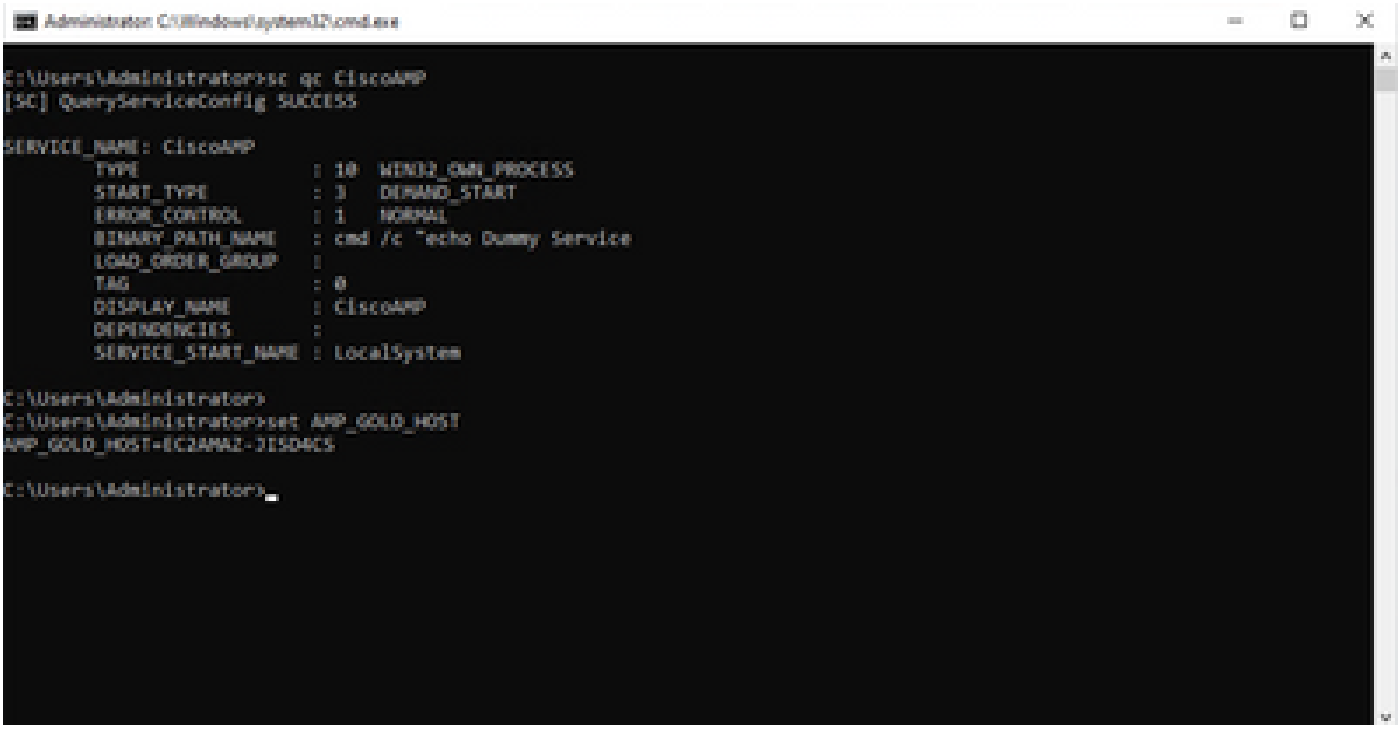
Remarque : ces deux scripts permettent le démarrage du service Cisco AMP dans les environnements de machines virtuelles clonées. En configurant correctement l'image Golden et en utilisant les scripts de démarrage, il s'assure que Cisco Secure Endpoint s'exécute sur toutes les machines virtuelles clonées avec la configuration correcte.

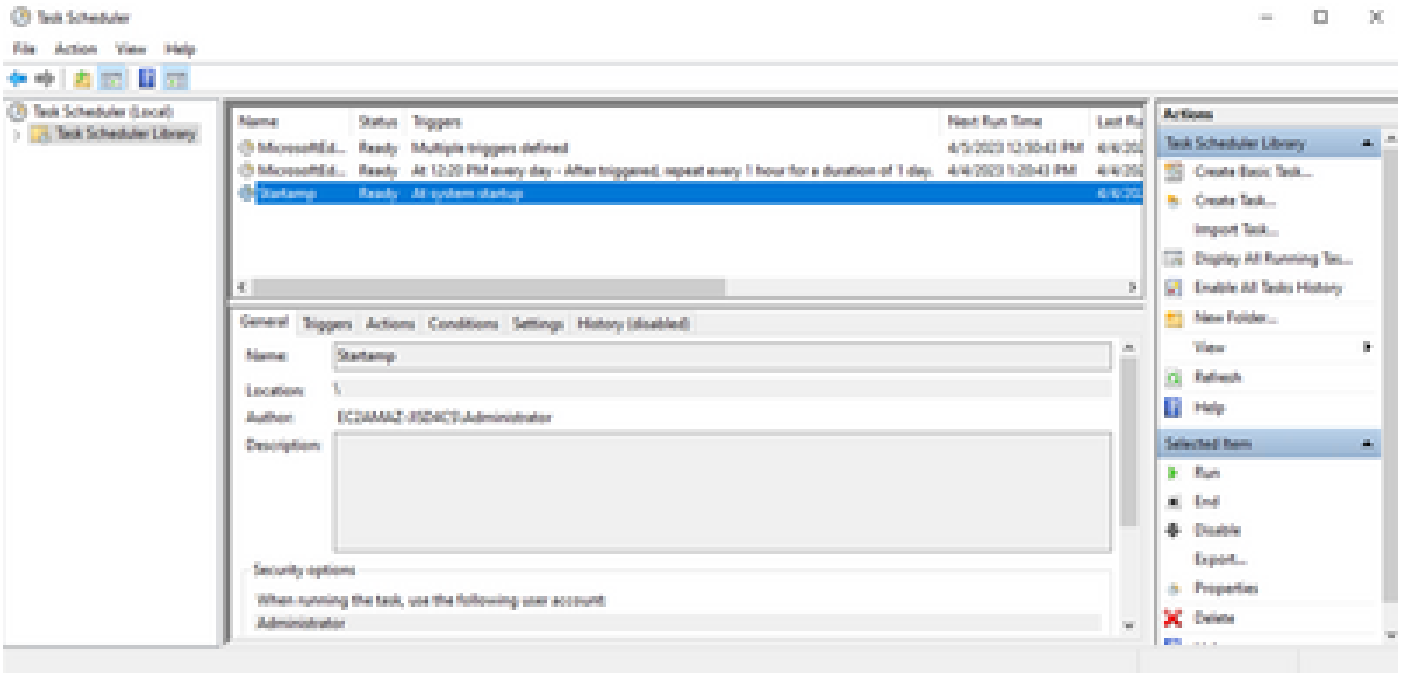
Processus AWS Workspace

Cette solution se compose d'un script de configuration exécuté sur l'image d'or avant le clonage et d'un script de démarrage qui s'exécute sur chaque machine virtuelle clonée pendant le démarrage du système. L'objectif principal de ces scripts est de garantir la configuration correcte du service tout en réduisant les interventions manuelles. Ces deux scripts permettent le démarrage du service Cisco Secure Endpoint dans des environnements de machines virtuelles clonées. En configurant correctement l'image Golden et en utilisant les scripts de démarrage, il garantit que le connecteur Cisco Secure Endpoint s'exécute sur toutes les machines virtuelles clonées avec la configuration correcte

Référez-vous à la section Code de script de configuration de Golden Image et Code de script de démarrage de Golden Image pour le code de script requis pour implémenter Golden Image sur AWS Workspace.

Après avoir exécuté le script de configuration, nous pouvons vérifier que les modifications de configuration ont été correctement déployées.





Puisque nous avons effectué cette action sur l'image dorée, toutes les nouvelles instances auront cette configuration et exécuteront le script de démarrage au démarrage.

Problèmes de duplication VMware Horizon

Avec VMware Horizon, nous avons pu identifier que les machines virtuelles enfant lors de leur création sont redémarrées plusieurs fois dans le cadre du processus de composition d'Horizon. Cela entraîne des problèmes lorsque les services Secure Endpoint sont activés lorsque les machines virtuelles enfant ne sont pas prêtes (le nom NetBios final/correct ne leur est pas attribué). Cela entraîne d'autres problèmes avec Secure Endpoint devenant confus et donc les ruptures de processus. Pour éviter ce problème, nous avons trouvé une solution à cette incompatibilité avec le processus Horizon. Cela implique la mise en oeuvre des scripts joints sur la machine virtuelle Golden Image et l'utilisation de la fonctionnalité de script de post-synchronisation pour VMware Horizon : [https://docs.vmware.com/en/VMware-Horizon/2103/published-desktops-applications.pdf.](https://docs.vmware.com/en/VMware-Horizon/2103/published-desktops-applications.pdf)

Configuration/modifications inutiles

- Vous n'avez plus besoin de désinstaller et de réinstaller Secure Endpoint si vous souhaitez apporter des modifications à l'image d'or après le premier déploiement.
- Il n'est pas nécessaire de définir le service Secure Endpoint sur Démarrage différé.

Méthodologie de script

Vous trouverez ci-dessous des exemples de scripts.

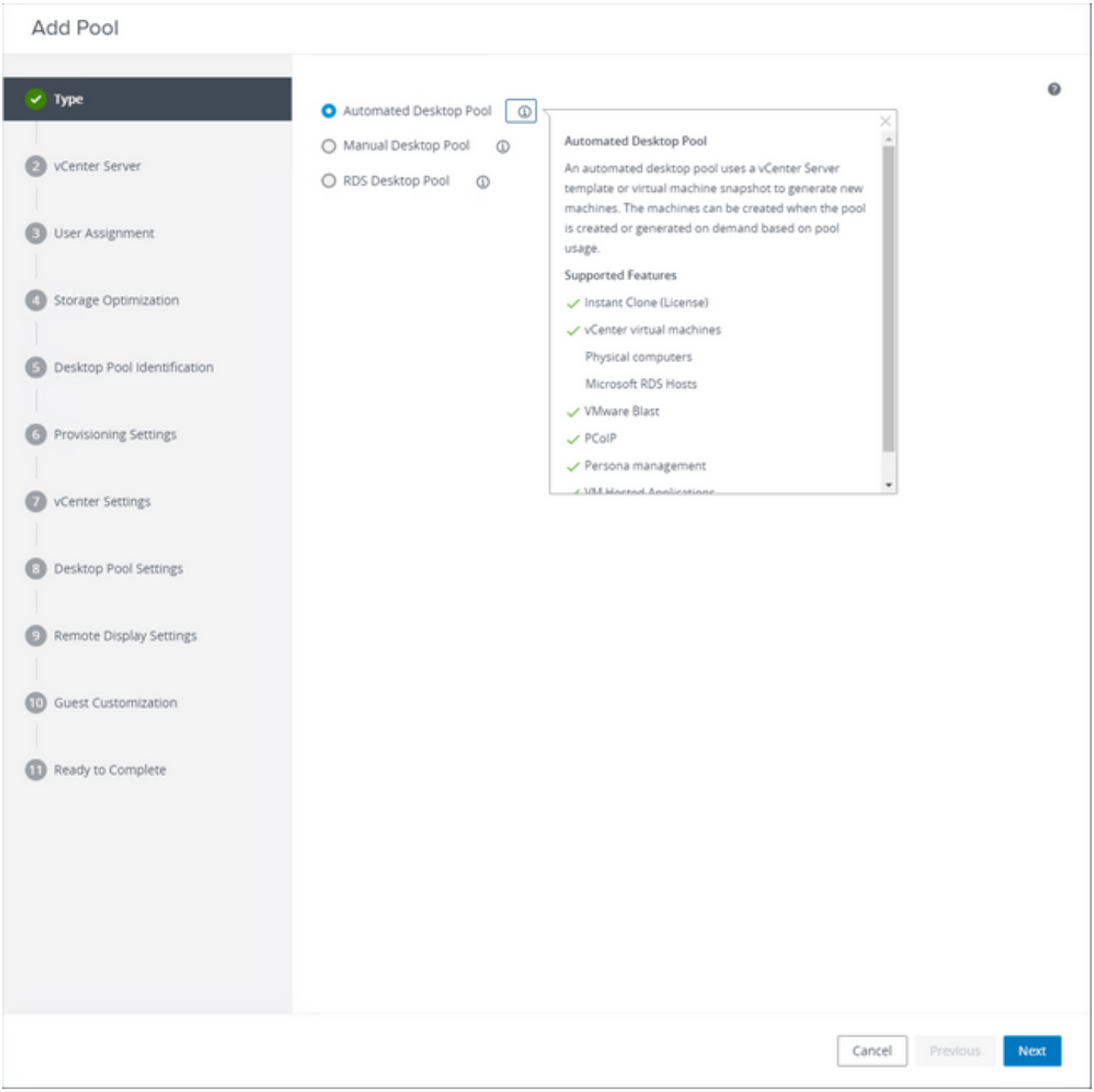
- Script de configuration Golden Image : ce script doit être implémenté une fois que le connecteur Secure Endpoint est installé comme décrit précédemment avec les indicateurs comme documenté précédemment. Ce script a modifié le service Secure Endpoint en

Démarrage manuel et enregistre le nom d'hôte Golden Image en tant que variable d'environnement pour référence à l'étape suivante.

- Script de démarrage d'image d'or : ce script est une vérification logique où nous faisons correspondre le nom d'hôte sur les machines virtuelles clonées (enfant) à celui stocké à l'étape précédente pour nous assurer que nous identifions quand la machine virtuelle clonée (enfant) obtient un nom d'hôte qui est autre que la machine virtuelle d'image d'or (qui serait le nom d'hôte final pour la machine), puis vous allez de l'avant et démarrez le service de point de terminaison sécurisé et changez cela pour être automatique. Vous supprimez également la variable d'environnement du script mentionné précédemment. Ceci est normalement mis en oeuvre à l'aide des mécanismes disponibles dans la solution de déploiement comme VMware. Sur VMware, vous pouvez utiliser les paramètres de post-synchronisation : https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-E177899E-023D-4E61-B058-AFE3822158AA.html De même pour AWS, vous pouvez utiliser les scripts de démarrage de la même manière : https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-windows-user-data.html.

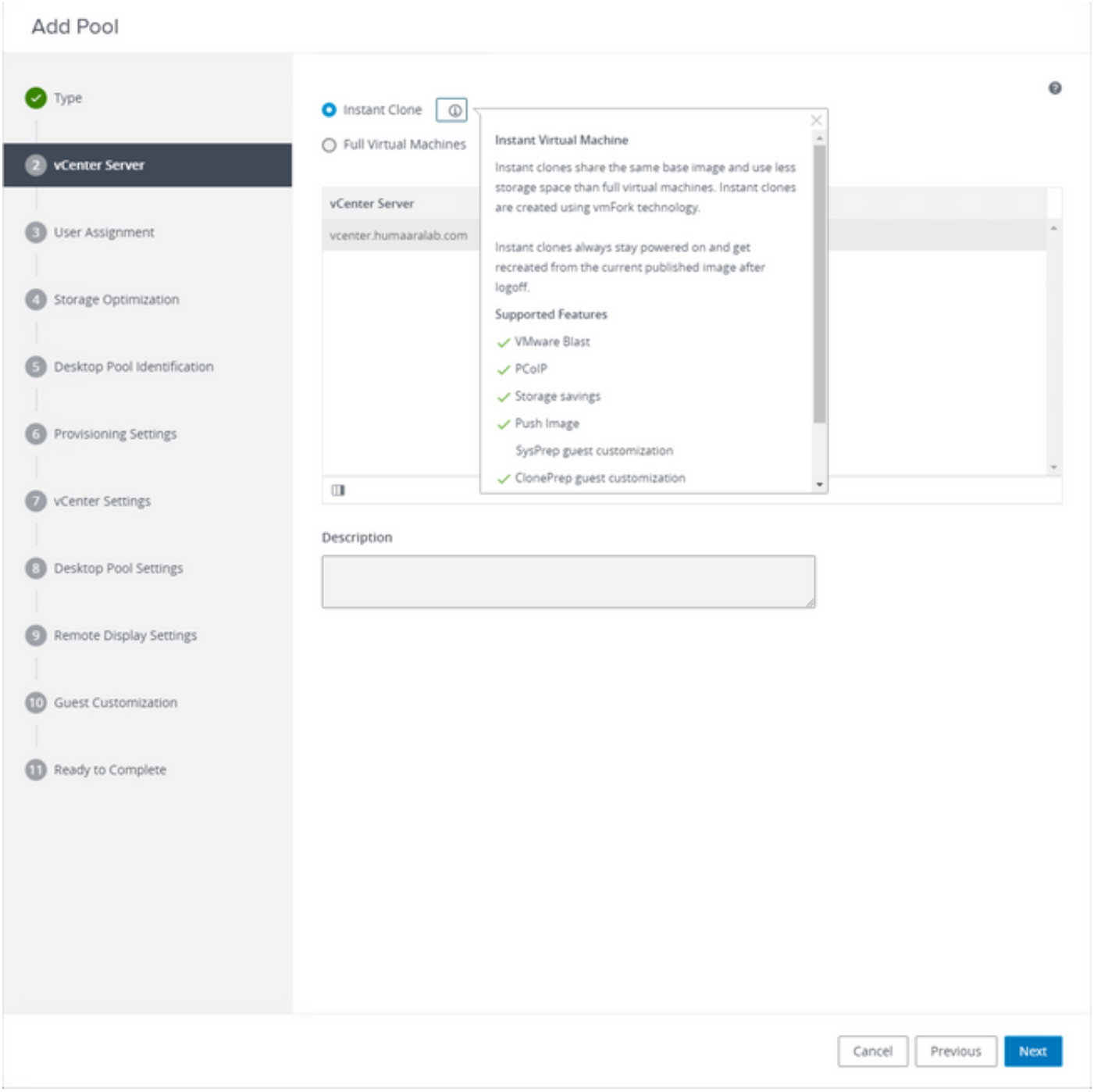
Configuration de VMware Horizon

1. La machine virtuelle Golden Image est préparée et toutes les applications requises pour le déploiement initial du pool sont installées sur la machine virtuelle.
2. Un terminal sécurisé est installé avec cette syntaxe de ligne de commande pour inclure l'indicateur goldenimage. Par exemple, <ampinstaller.exe> /R /S /goldenimage 1. Veuillez noter que l'indicateur d'image dorée garantit que le service Secure Endpoint ne s'exécute pas avant un redémarrage qui est essentiel pour que ce processus fonctionne correctement. Reportez-vous à la page https://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-endpoints/118587-technote-fireamp-00.html
3. Après l'installation de Secure Endpoint, exécutez d'abord le script VMWareHorizonAMPSetup.bat sur la machine virtuelle Golden Image. Ce script remplace essentiellement le service Secure Endpoint par Manual Start et crée une variable d'environnement qui stocke le nom d'hôte Golden Image pour une utilisation ultérieure.
4. Vous devez copier le fichier VMWareHorizonAMPStartup.bat vers un chemin d'accès universel sur la machine virtuelle d'image dorée comme "C:\ProgramData" comme cela sera utilisé dans les étapes ultérieures.
5. La machine virtuelle Golden Image peut maintenant être arrêtée et le processus de composition peut être lancé sur VMware Horizon.
6. Voici des informations détaillées sur ce à quoi il ressemble du point de vue de VMware Horizon :



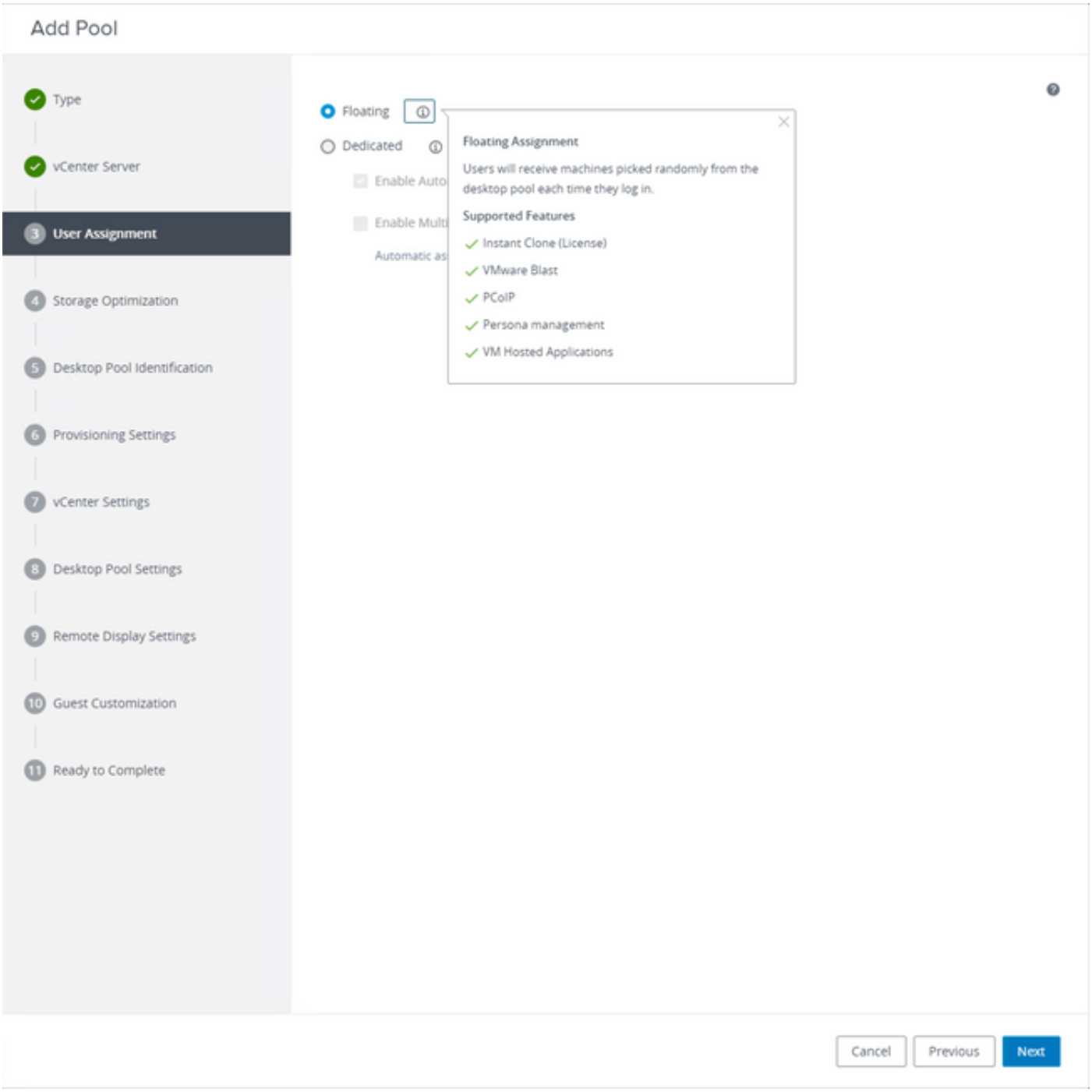
Sélection de « Pool de bureaux automatisés »

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



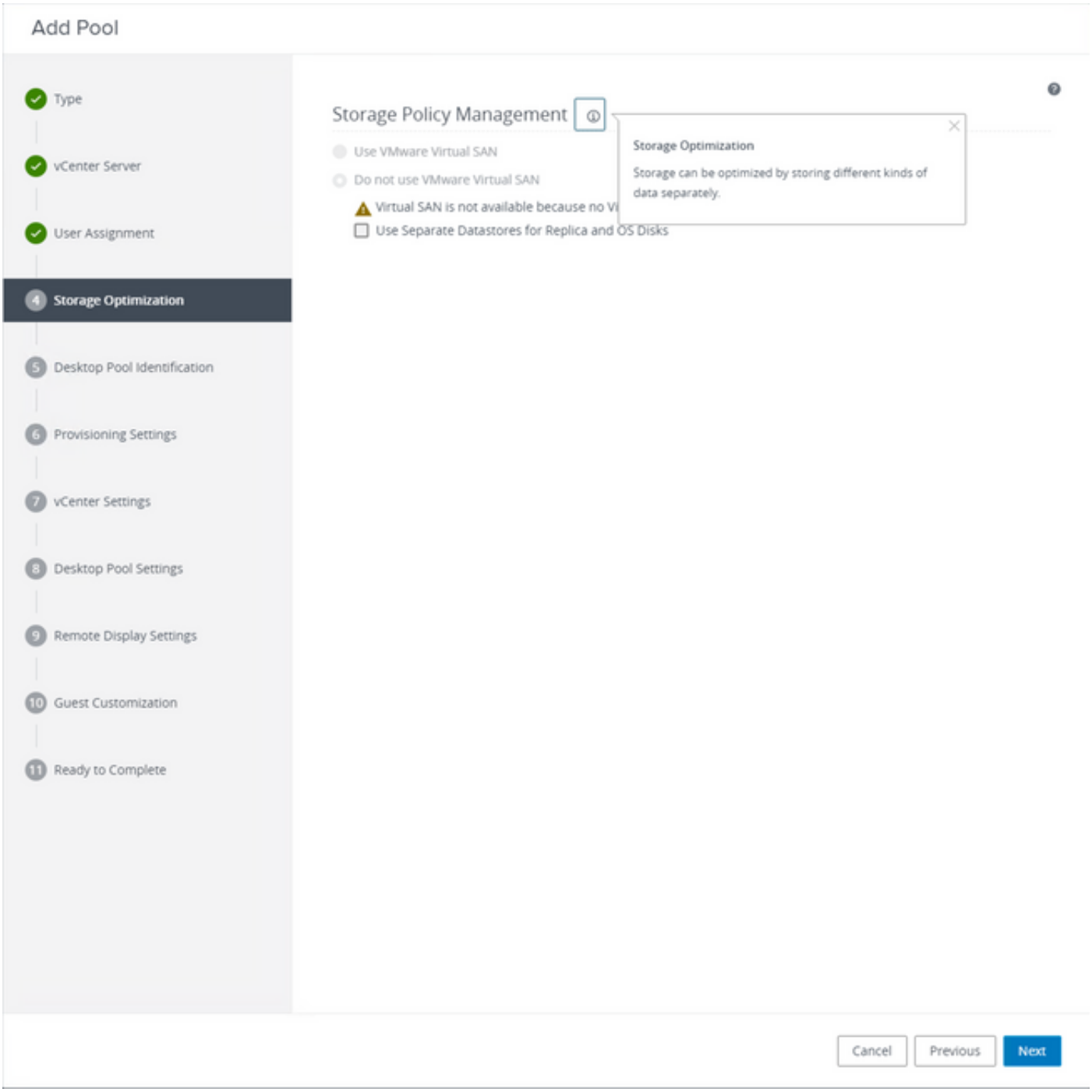
Sélection de « Clones instantanés »

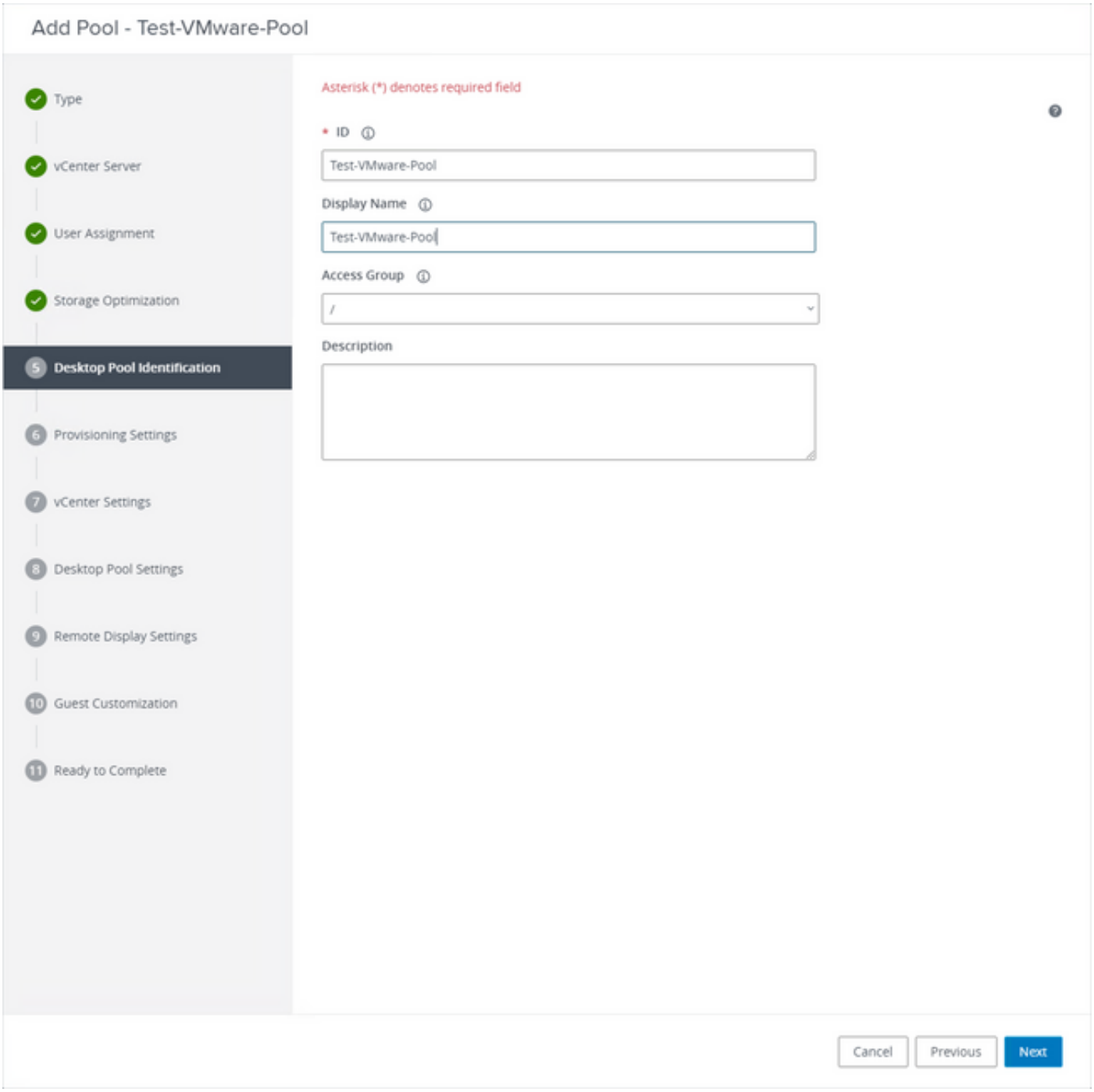
Reportez-vous à : https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-D7C0150E-18CE-4012-944D-4E9AF5B28347.html



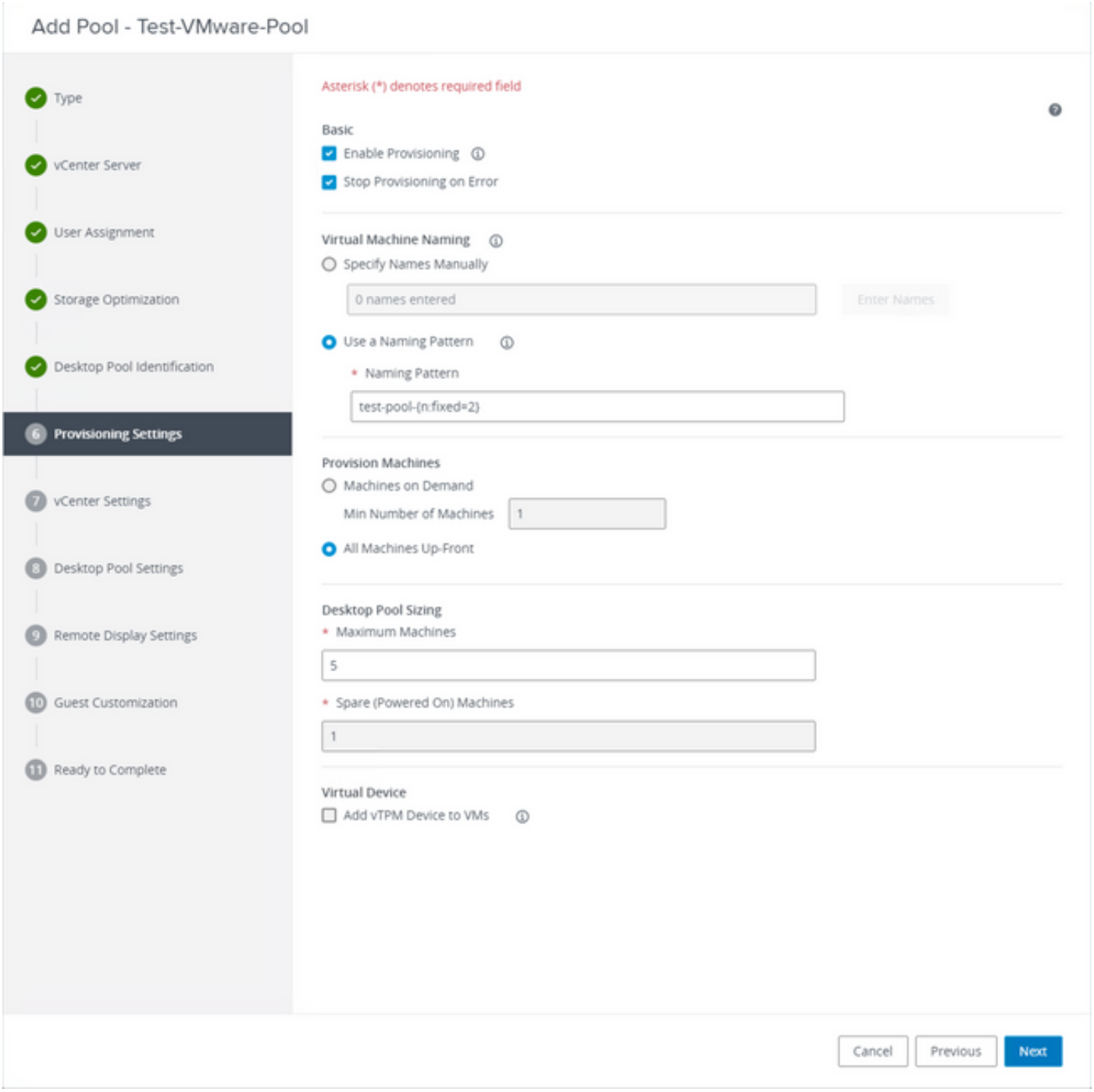
Sélection du type "Flottant"

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

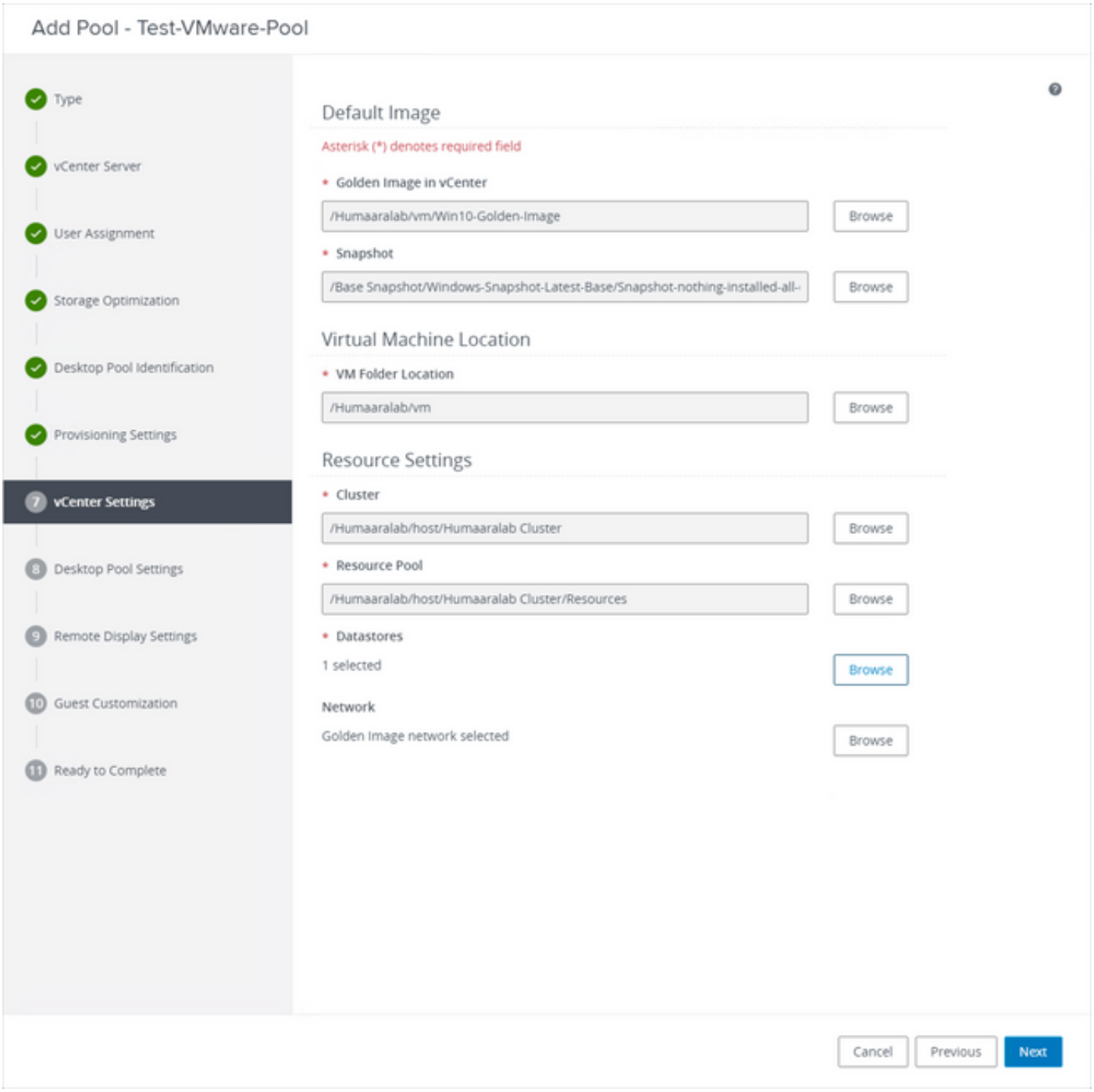

Add Pool
Type
vCenter Server
User Assignment
4 Storage Optimization
5 Desktop Pool Identification
6 Provisioning Settings
7 vCenter Settings
8 Desktop Pool Settings
9 Remote Display Settings
10 Guest Customization
11 Ready to Complete
Storage Policy Management
Use VMware Virtual SAN
Do not use VMware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



Noms des pools de bureaux

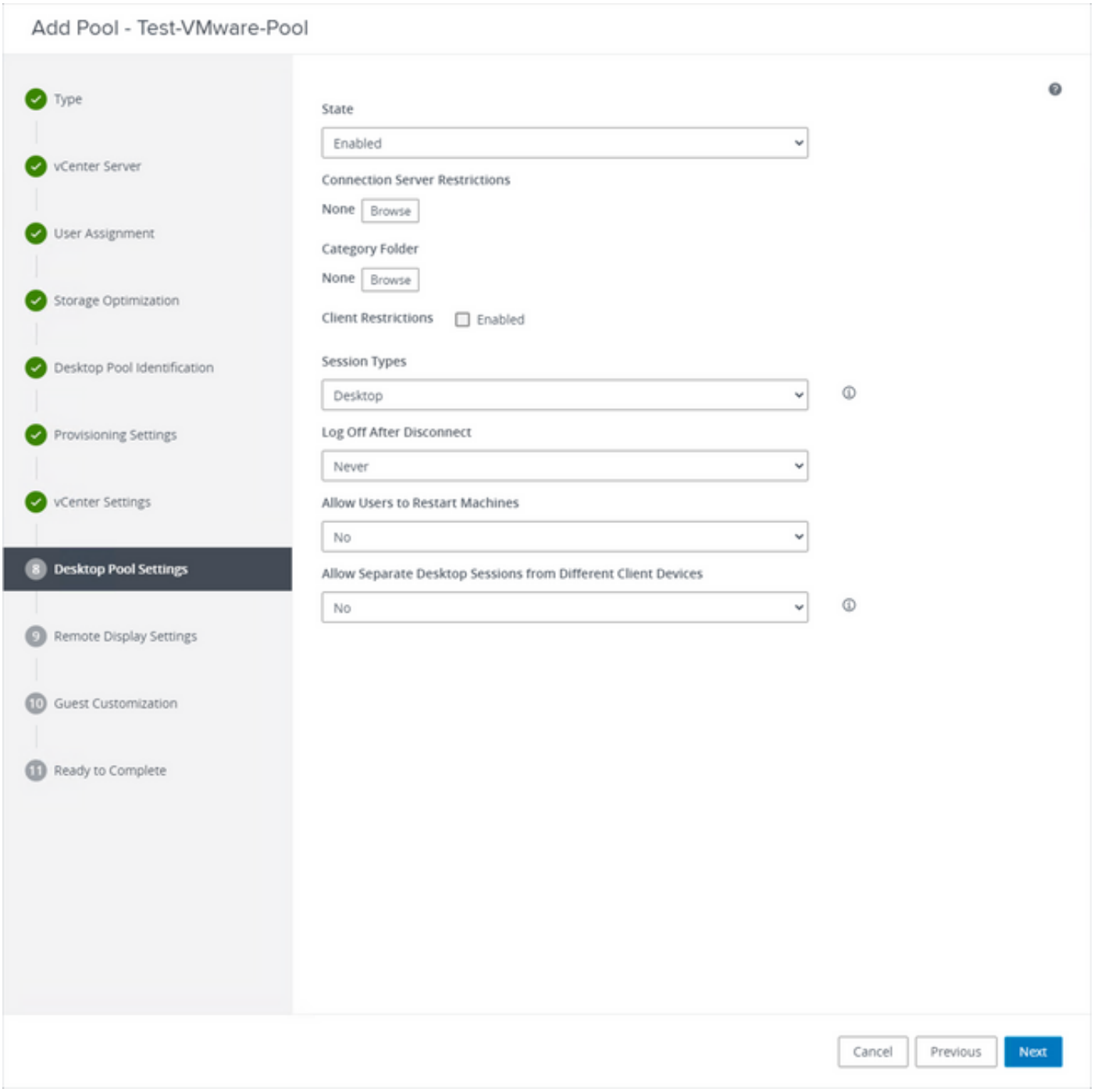


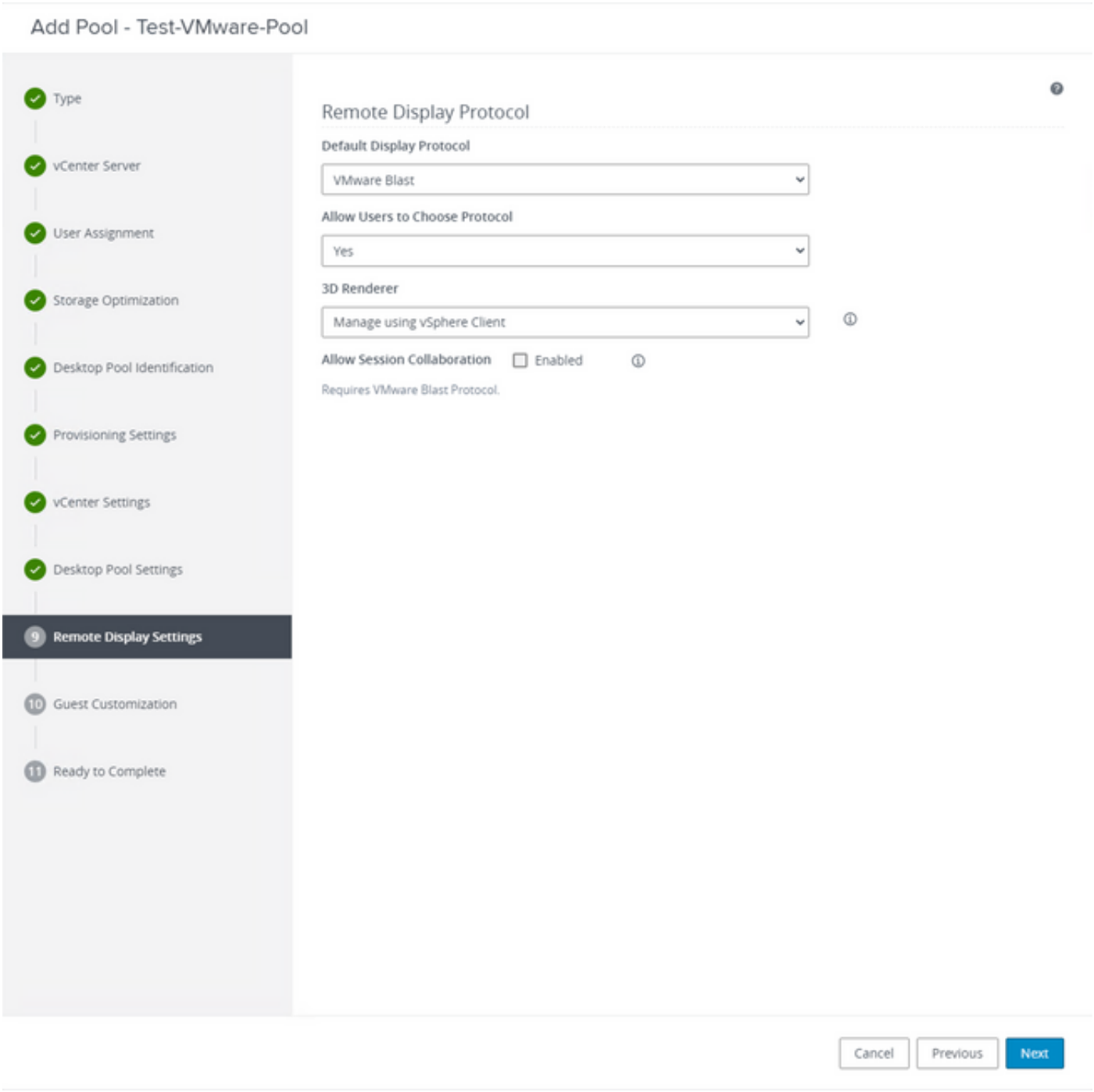
Modèle de dénomination VMware Horizon : https://docs.vmware.com/en/VMware-Horizon/2103/virtual-desktops/GUID-26AD6C7D-553A-46CB-B8B3-DA3F6958CD9C.html

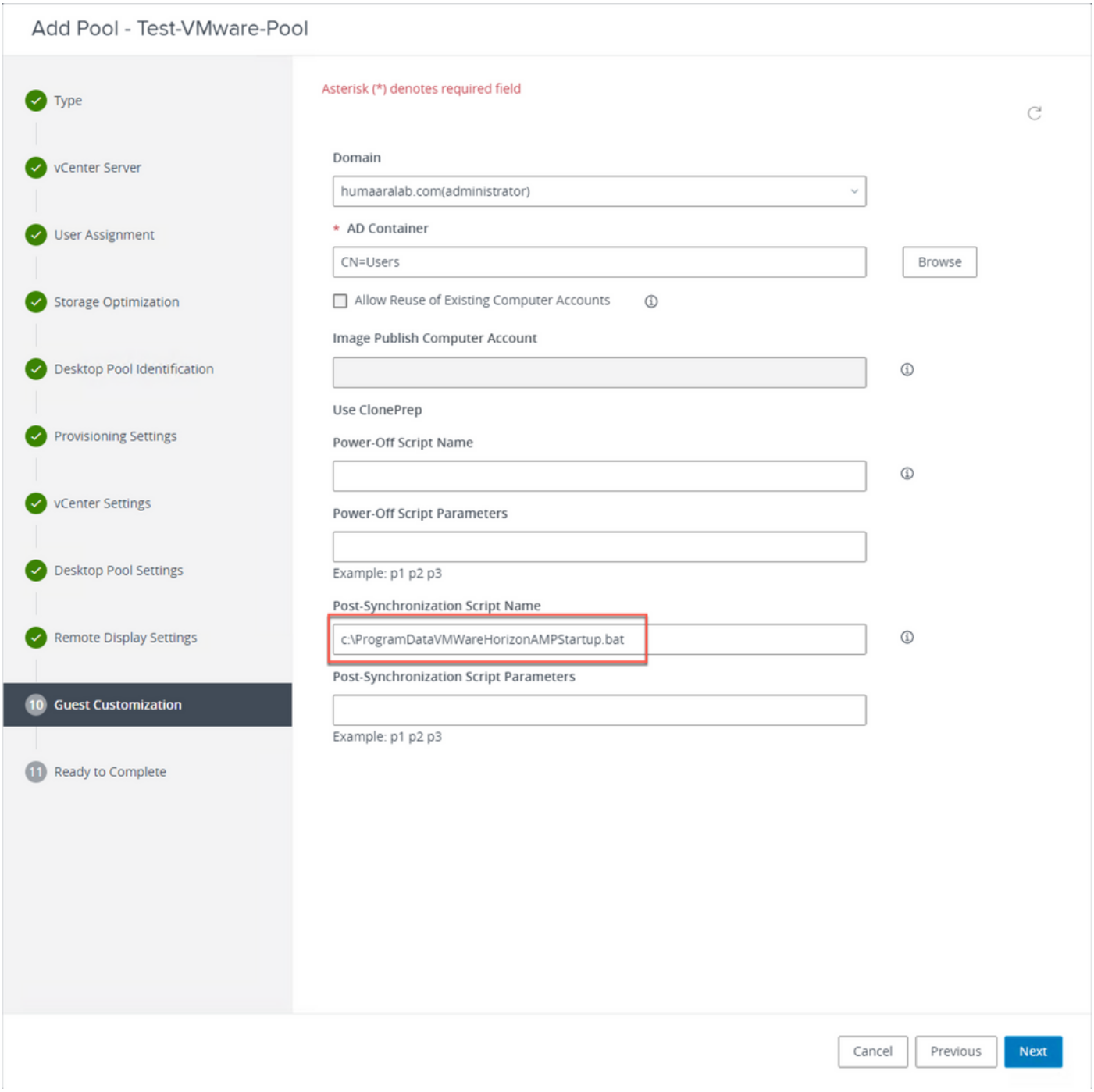


Golden Image : il s'agit de la machine virtuelle Golden Image.

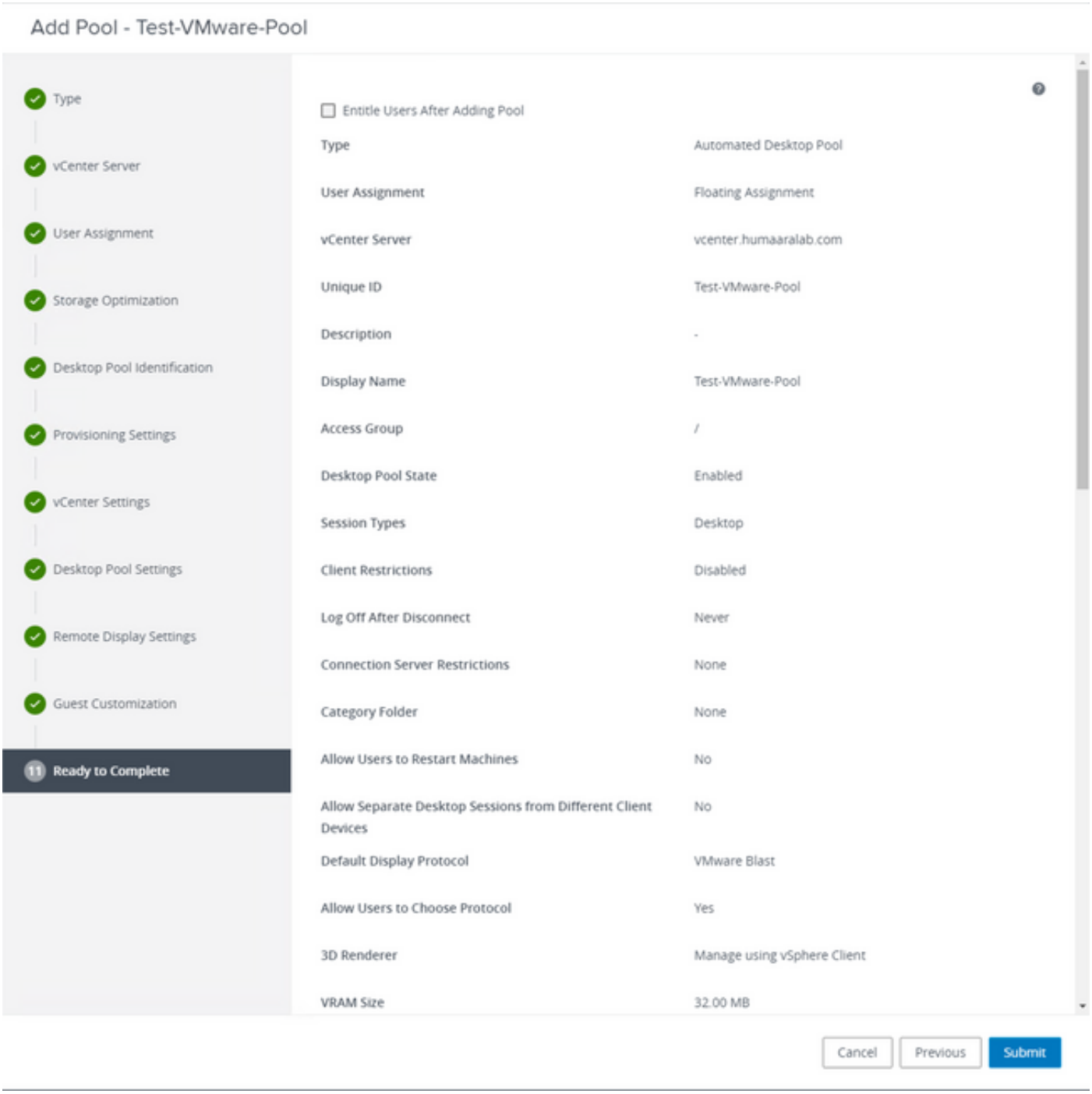
Snapshot : image que vous souhaitez utiliser afin de déployer la machine virtuelle enfant. Il s'agit de la valeur qui est mise à jour lorsque vous mettez à jour l'image d'or avec toutes les modifications. Les autres paramètres sont spécifiques à l'environnement VMware.


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. Comme mentionné précédemment, l'étape 10. de l'Assistant est l'endroit où vous définissez le chemin du script.



8. Une fois que VMware Horizon a terminé et envoyé la composition, les machines virtuelles enfant sont créées.

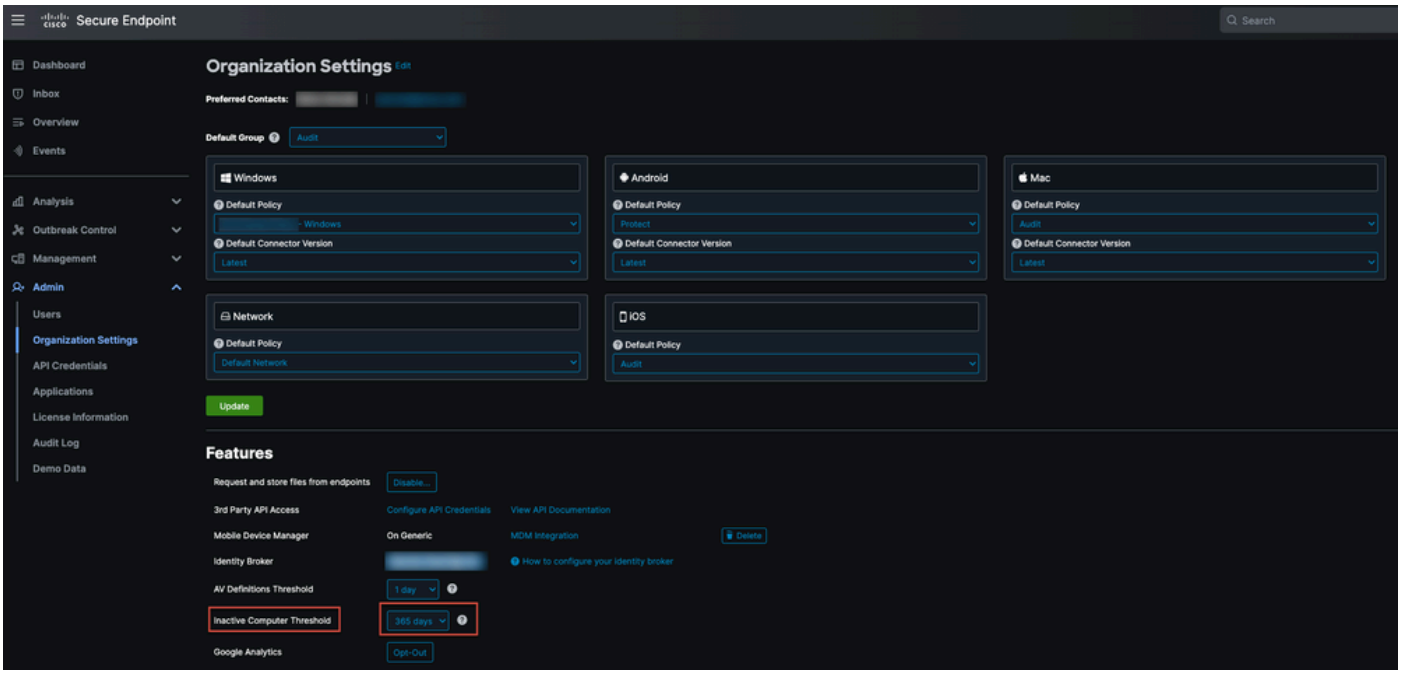
Remarque : reportez-vous au guide VMware pour obtenir des informations sur ces étapes, mais elles sont explicites.

Suppression des entrées en double

Il existe plusieurs méthodes permettant de supprimer les entrées dupliquées du connecteur :

1. Utilisez la fonction de suppression automatique sur le portail Secure Endpoint pour supprimer les entrées en double (inactives) :

Vous trouverez ce paramètre dans Admin > Paramètres de l'organisation



Le seuil de l'ordinateur inactif vous permet de spécifier le nombre de jours pendant lesquels un connecteur peut passer sans s'enregistrer dans le nuage Cisco avant d'être supprimé de la liste de la page Gestion de l'ordinateur. Le paramètre par défaut est 90 jours. Les ordinateurs inactifs seront uniquement supprimés de la liste et tous les événements qu'ils génèrent resteront dans votre organisation Secure Endpoint. L'ordinateur réapparaîtra dans la liste si le connecteur s'enregistre à nouveau.

2. Utilisez les workflows d'orchestration disponibles : https://ciscosecurity.github.io/sxo-05-security-workflows/workflows/secure-endpoint/0056-remove-inactive-endpoints

3. Utilisez le script externe pour supprimer les UUID obsolètes/anciens : https://github.com/CiscoSecurity/amp-04-delete-stale-guids

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.