

在安全端點中配置身份永續性

目錄

[簡介](#)

[什麼是身份永續性？](#)

[需求](#)

[何時需要身份永續性？](#)

[虛擬終端部署](#)

[物理終端部署](#)

[身份永續性流程概述](#)

[識別組織中的重複項](#)

[外部可用的GitHub指令碼](#)

[建立重複項的原因](#)

[身份永續性部署不正確的常見問題/症狀](#)

[部署最佳實踐](#)

[配置snapvol檔案](#)

[門戶策略規劃](#)

[組態](#)

[金色影像創作](#)

[金色影像覆蓋標誌](#)

[黃金映像建立步驟](#)

[更新金色影像](#)

[金色影像代碼](#)

[Golden Image設定指令碼](#)

[Golden Image啟動指令碼](#)

[AWS Workspace流程](#)

[VMware Horizon重複問題](#)

[不再需要配置/更改](#)

[指令碼方法](#)

[VMware Horizon配置](#)

[刪除重複條目](#)

簡介

本文檔介紹如何通過思科安全端點身份永續性功能。

什麼是身份永續性？

身份永續功能允許您在虛擬環境中或電腦重新映像時維護一致的事件日誌。您可以將聯結器繫結到MAC地址或主機名，這樣就不會每次啟動新的虛擬會話或重新映像電腦時都建立一個新的聯結器記錄。此功能專為非永續性VM和實驗室環境設計，不能為傳統的工作站和伺服器設定啟用。

需求

思科建議您瞭解以下主題：

- 對思科安全終端門戶的訪問
- 您需要聯絡Cisco TAC，讓他們在您的組織中啟用身份永續性功能。
- 只有Windows作業系統(OS)支援身份永續性

何時需要身份永續性？

身份永續性是安全端點上的功能，它有助於在初始聯結器註冊時識別安全端點，並根據特定聯結器的MAC地址或主機名等身份引數，將它們與先前已知條目進行匹配。該功能的實施不僅有助於保持正確的許可證數量，而且最重要的是，能夠正確跟蹤非永續性系統上的歷史資料。

虛擬終端部署

在虛擬部署中，標識永續性最常見的是非永續性虛擬案頭基礎設施(VDI)部署。VDI主機案頭環境根據終端使用者的請求或需求進行部署。這包括不同的供應商，如VMware、Citrix、AWS AMI Golden Image Deployment等。

持續VDI (也通常稱為「有狀態VDI」) 是一種設定，其中每個使用者的案頭可唯一自定義，並在一個會話到另一個會話「持續」。這種型別的虛擬部署不需要身份永續性功能，因為這些電腦不會定期重新映像。

與可能與安全端點效能互動的所有軟體一樣，虛擬案頭應用程式需要評估可能的例外情況，以便最大限度地提高功能並最大程度地減小影響。

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

物理終端部署

有兩種方案可用於在安全終端物理電腦上部署身份永續性：

- 在部署或重新映像具有黃金映像且預安裝了安全終端聯結器的物理終端時，必須啟用Goldenimage標誌。身份永續性可用於避免重映像電腦中的重複，但並非必需的。
- 當您使用金色映像部署或重新映像物理終結點，並在以後安裝安全終結點聯結器時，可以使用身份永續性來避免在重新映像電腦的情況下發生重複，但不需要這樣做。

身份永續性流程概述

1. 聯結器將使用policy.xml檔案中的令牌下載，該令牌將聯結器繫結回雲端有問題的策略。
2. 安裝聯結器，將令牌儲存在local.xml中，並且聯結器使用有問題的令牌向入口發出POST請求。
3. 雲端會經歷以下操作順序：
 - a. 電腦將檢查ID同步策略配置的策略。否則，註冊將正常進行。

b.根據策略設定，「註冊」將檢查現有資料庫的主機名或MAC地址。

跨業務：根據設定，將檢查所有策略在主機名或MAC上的匹配項。會記下匹配的對象GUID，並將其傳送回終端客戶機。然後，客戶端電腦採用UUID並採用以前匹配的主機的任何組/策略設定。這將覆蓋安裝的策略/組設定。

跨策略：令牌 匹配雲端的策略，並僅在該策略內查詢具有相同主機名或MAC地址的現有對象。如果存在，則採用UUID。如果不存在與該策略關聯的現有對象，則會建立一個新對象。注意：對於與其他組/策略關聯的相同主機名，可能存在重複項。

c.如果由於缺少令牌（以前註冊、部署實踐不佳等）而無法與組/策略匹配，則聯結器將歸入「業務」頁籤下設定的預設聯結器組/策略。根據組/策略的設定，它會嘗試檢查匹配的所有策略（跨業務），僅檢查相關策略（跨策略），或根本不檢查任何策略（無）。考慮到這一點，通常建議將預設組設定為包含其所需的ID同步設定的組，以便在出現令牌問題時電腦能夠正確重新同步。

識別組織中的重複項

外部可用的GitHub指令碼

查詢重複的UUID:<https://github.com/CiscoSecurity/amp-04-find-duplicate-guids>

建立重複項的原因

有一些常見例項可能導致在您的終端上看到重複項：

1.如果在VDI池期間執行了以下步驟：

- 在非永續性VM/VDI上完成初始部署時禁用了身份永續性（例如，使用golden映像）。
- 在雲中更新策略以啟用身份永續性，在白天，身份永續性會在終端上更新。
- 電腦將刷新/重新映像（使用相同的金色映像），然後將原始策略重新放置到終端上，而無需身份永續性。
- 本地策略沒有身份永續性，因此註冊伺服器不會檢查以前的記錄。
- 此流程將產生重複項。

2.使用者將策略中啟用了身份永續性的原始黃金映像部署到一個組中，然後將一個終端從安全終端門戶移動到另一個組。然後，它會將原始記錄放在「移動到」組中，但是當重新映像/重新部署虛擬機器時，它會在原始組中建立新副本。



注意：這不是可能引起重複的方案的詳盡清單，而是一些最常見的方案。

身份永續性部署不正確的常見問題/症狀

不正確的身份永續性實現可能導致以下問題/症狀：

- 聯結器座位數不正確
- 不正確的報告結果
- 裝置軌跡資料不匹配
- 審計日誌中的電腦名稱交換

- 連結器從控制檯隨機註冊和註銷
 - 連結器無法正確向雲報告
 - UUID複製
 - 電腦名稱重複
 - 資料不一致
 - 重組後電腦註冊到預設業務組/策略
- 在策略上啟用身份永續性的情況下手動部署。

— 如果通過命令列開關手動部署終結點，並且已經在策略中啟用了身份永續性，然後解除安裝該終結點並嘗試使用不同組/策略的軟體包重新安裝，則終結點將自動切換回原始策略。

— 顯示1到10秒內策略交換機自身的SFC日誌輸出

```
(167656, +0 ms) Dec 14 11:37:17 [1308]: Util::VerifyOsVersion: ret 0
(167656, +0 ms) Dec 14 11:37:17 [1308]: ERROR: ETWEnableConfiguration::IsETWEnabled: ETW not initialized
(167656, +0 ms) Dec 14 11:37:17 [1308]: UiPublisher::PublishPolicyInfo: Name -UTMB-WinServer-Protect 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
```

如果您嘗試安裝屬於不同組的連結器，則會產生另一個副作用。您將在門戶中看到，連結器被分配到正確的組，但原始策略為「錯誤」

這是因為身份永續性(ID SYNC)的工作方式。

一旦連結器完全解除安裝或使用re-register命令列開關，則沒有ID SYNC。在解除安裝時應看到新

的建立日期和聯結器GUID，在重新註冊命令時應只看到新的聯結器GUID。但是，對於ID SYNC，不可能使用舊GUID和DATE進行ID SYNC覆蓋。這就是我們「同步」主機的方式。

如果發現此問題，則必須通過策略更改進行修復。您需要將受影響的終端移回原始組/策略，並確保策略同步。然後將終端移回所需的組/策略

部署最佳實踐

配置snapvol檔案

如果您將App Volumes用於VDI基礎結構，建議您對snapvol.cfg配置進行這些配置

這些排除項必須實施到snapvol.cfg檔案中：

路徑：

- C:\Program Files\Cisco\AMP
- C:\ProgramData\Cisco
- C:\Windows\System32\drivers
- C:\Windows\System32\drivers\ImmuneNetNetworkMonitor.sys
- C:\Windows\System32\drivers\immunetprotect.sys
- C:\Windows\System32\drivers\immunetselfprotect.sys
- C:\Windows\System32\drivers\ImmuneNetUtilDriver.sys
- C:\Windows\System32\drivers\trufos.sys

登錄檔項：

- HKEY_LOCAL_MACHINE\SOFTWARE\ImmuneNet Protect
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ImmuneNet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\ImmuneNetProtectDriver
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ImmuneNetSelfProtectDriver
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Trufos

在x64系統上，新增以下內容：

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ImmuneNet保護
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\保護

參考資料：

- <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>

門戶策略規劃

以下是在安全終端門戶上實施身份永續性時必須遵循的一些最佳實踐：

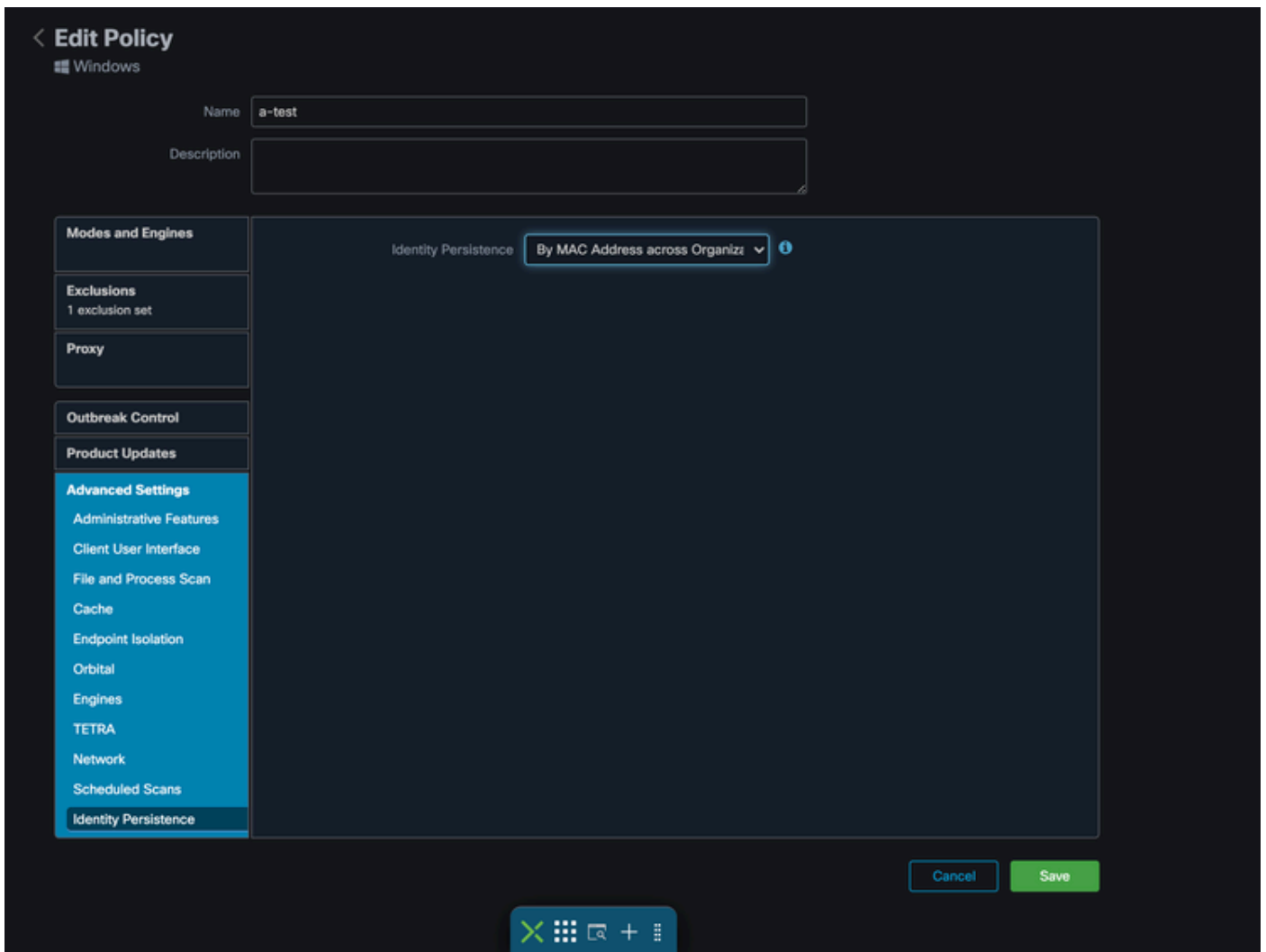
- 1.強烈建議為身份永續性終結點使用單獨的策略/組，以簡化隔離。
- 2.如果計畫使用終端隔離並實施「危害時將電腦移動到組」操作。目標組還必須啟用身份永續性，且只能用於VDI電腦。
- 3.建議不要在組織設定上的預設組/策略上啟用身份永續性，除非已啟用「跨組織所有策略」(Across Organization as as settings scope)中的身份永續性。

組態

按照以下步驟部署具有身份永續性的安全終端聯結器：

步驟 1.將所需的身份永續性設定應用於策略：

- 在安全終端門戶中，導航到管理>策略。
- 選擇要啟用身份持續性的所需策略，然後按一下編輯。
- 導航到Advanced Settings頁籤，然後按一下底部的Identity Persistence頁籤。
- 選擇Identity Persistence下拉選單，然後選擇最適合您的環境的選項。請參閱此圖。



< Edit Policy

Windows

Name

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

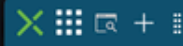
Scheduled Scans

Identity Persistence

Identity Persistence ⓘ

Cancel

Save





< Edit Policy

🏠 Windows

Name

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

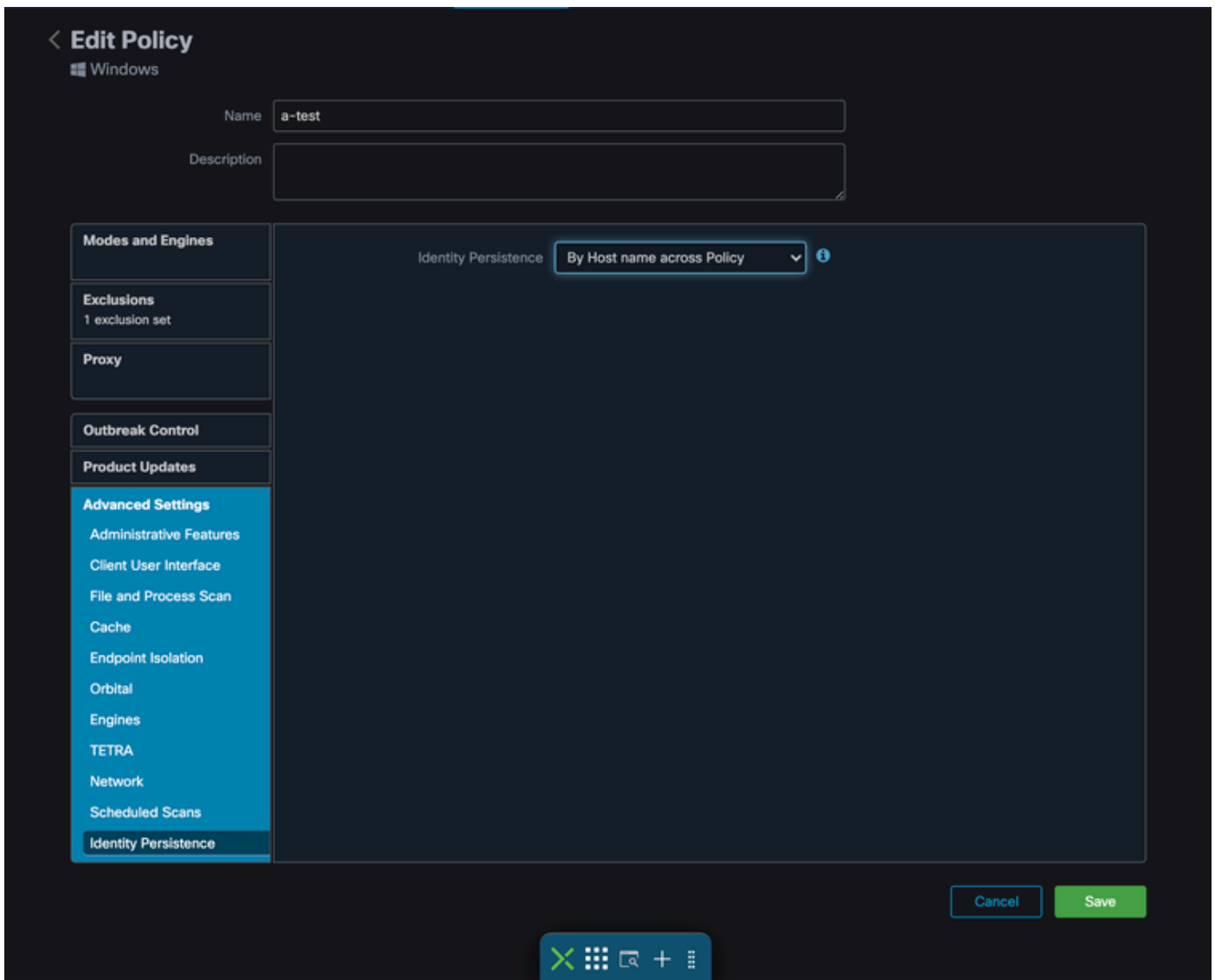
Scheduled Scans

Identity Persistence

Identity Persistence ⓘ

Cancel

Save




有五個選項可供您選擇。

- 請注意，功能未啟用。在任何情況下，聯結器UUID都不會與新聯結器安裝同步。每次新安裝都會生成新的電腦對象。
- 按跨業務的MAC地址：新的或更新的安裝查詢具有相同MAC地址的最新聯結器記錄，以便將以前的歷史資料與新註冊同步。此設定檢視所有業務記錄

將身份同步設定為非零值的組織中的所有策略之間。如果聯結器不同於新安裝，則聯結器可以更新其策略以反映以前的安裝。

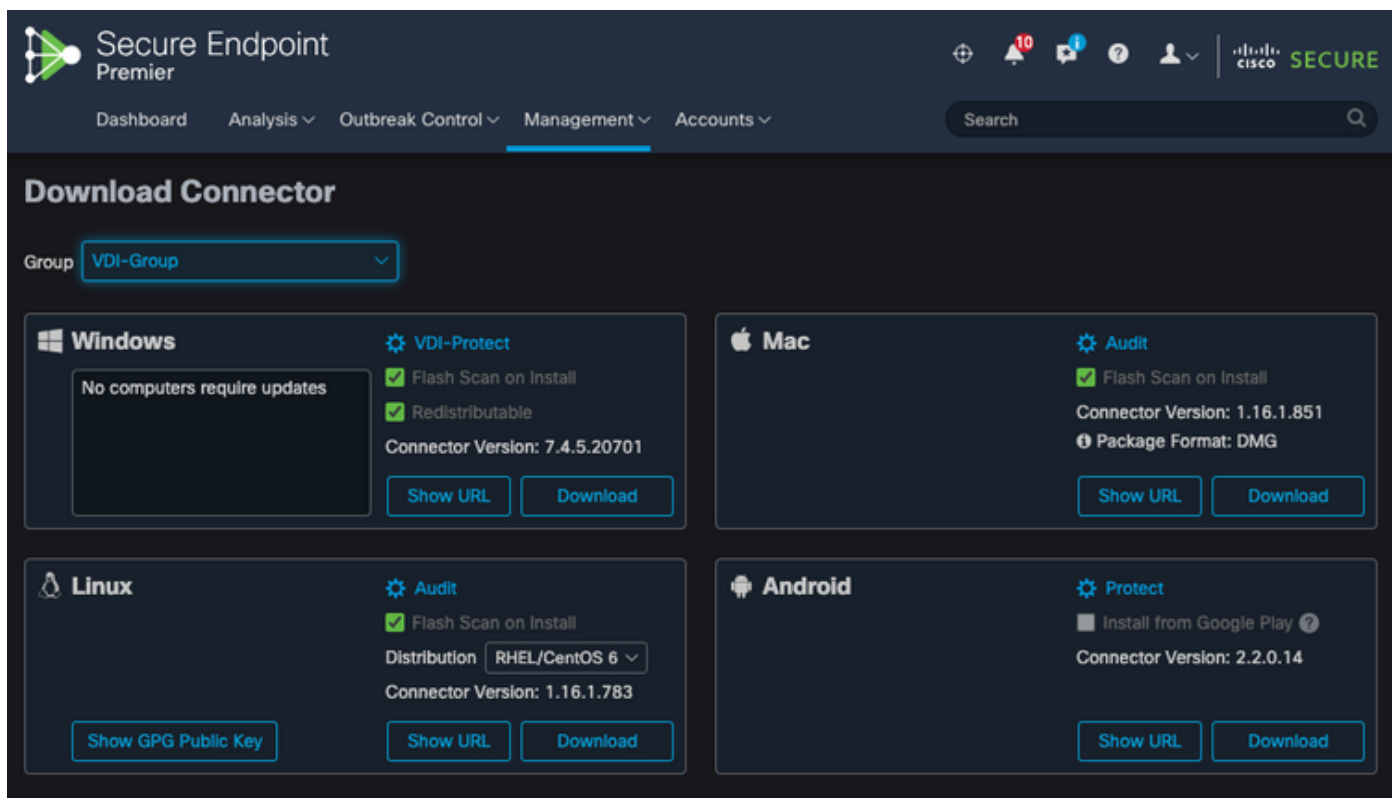
- 跨策略按MAC地址：新的或刷新的安裝將查詢具有相同MAC地址的最新聯結器記錄，以便將以前的歷史資料與新的註冊同步。此設定僅檢視與部署中使用的策略相關聯的記錄。如果聯結器以前未安裝在此策略中，但以前在其他策略中處於活動狀態，則可以建立重複項。
- 按跨業務的主機名：新的或刷新的安裝將查詢具有相同主機名的最新聯結器記錄，以便將以前的歷史資料與新註冊同步。此設定將檢視所有業務記錄，無論其他策略中的身份永續性設定如何。如果以前的安裝與新安裝不同，聯結器可以更新其策略以反映以前的安裝。主機名包括 FQDN，因此，如果聯結器經常在網路之間（如筆記型電腦）移動，就會發生重複項。
- 跨策略按主機名：新的或刷新的安裝將查詢具有相同主機名的最新聯結器記錄，以便將以前的歷史資料與新的註冊同步。此設定僅檢視與用於部署的策略關聯的記錄。如果聯結器以前未安

裝在此策略中，但以前在其他策略中處於活動狀態，則可以建立重複項。主機名包括 FQDN，因此，如果聯結器經常在網路之間（如筆記型電腦）移動，也可能會發生重複。

 注意：如果選擇使用身份永續性，思科建議您跨業務或策略使用按主機名。一台電腦有一個主機名，但可以有多個MAC地址，並且許多虛擬機器克隆該MAC地址。

步驟 2. 下載安全端點聯結器。

- 導覽至 Management > Download Connector。
- 為步驟1中編輯的策略選擇組。
- 按一下「Windows Connector」的「Download」，如下圖所示。




The screenshot shows the 'Download Connector' page in the Secure Endpoint Premier interface. The 'Group' is set to 'VDI-Group'. There are four connector cards:

- Windows:** VDI-Protect, Flash Scan on Install, Redistributable, Connector Version: 7.4.5.20701. Buttons: Show URL, Download.
- Mac:** Audit, Flash Scan on Install, Connector Version: 1.16.1.851, Package Format: DMG. Buttons: Show URL, Download.
- Linux:** Audit, Flash Scan on Install, Distribution: RHEL/CentOS 6, Connector Version: 1.16.1.783. Buttons: Show GPG Public Key, Show URL, Download.
- Android:** Protect, Install from Google Play, Connector Version: 2.2.0.14. Buttons: Show URL, Download.

步驟 3. 將聯結器部署到終端。

- 現在，您可以使用下載的聯結器在端點上手動安裝安全端點（此時啟用了身份永續性）。
- 否則，也可以使用金色影象部署聯結器（請參見影象）

 注意：您需要選擇可再發行的安裝程式。這是一個~57 MB（大小因新版本而異）的檔案，其中包含32位和64位安裝程式。若要在多台電腦上安裝聯結器，可以將此檔案放在網路共用上，或者相應地將其推送到所有電腦。安裝程式包含一個用作安裝配置檔案的policy.xml檔案。

金色影像創作

建立用於VDI克隆流程的黃金映像時，請遵循供應商文檔（VMware、Citrix、AWS、Azure等）中的最佳實踐指南。

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

由於您已經識別了VMware，AWS合成流程在最終確定虛擬機器配置之前多次重新啟動克隆（子虛擬機器），這將導致安全終端註冊流程出現問題，因為此時克隆（子虛擬機器）沒有分配最終/正確的主機名，導致克隆（子虛擬機器）使用黃金映像主機名並註冊到安全終端雲。這會中斷克隆過程並引起問題。

這不是安全終結點聯結器進程的問題，而是與克隆進程和安全終結點註冊不相容的問題。為了防止出現此問題，我們確定了要在克隆過程中實施的一些更改，這些更改有助於解決這些問題。

這些是需要在凍結映像以克隆之前在Golden Image VM上實施的更改

1. 安裝安全端點時，始終在Golden Image上使用Goldenimage標誌。
2. 實施Golden Image Setup Script和Golden Image Startup Script部分，以查詢僅在克隆（子VM）上實施最終主機名時才會幫助開啟終端服務的指令碼。有關詳細資訊，請參閱VMware Horizon複製問題部分。

金色影象覆蓋標誌

使用安裝程式時，用於黃金映像的標誌是/goldenimage 1。

金色影象標誌防止聯結器在基礎影象上啟動和註冊；因此，在影象的下一個開始時，聯結器處於被分配給它的策略配置為所處於的功能狀態。

有關其他標誌的資訊，您可以使用[使用，請參閱本文。](#)

使用安裝程式時，用於黃金映像的新標誌為/goldenimage [1|0]

0 — 預設值 — 該值不會觸發golden image選項，並且其運行方式與安裝程式未使用該選項時的運行方式一樣。安裝時不要跳過初始聯結器註冊和啟動。

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

1 — 安裝為黃金映像。這是與標誌一起使用的典型選項，也是唯一預期的用法。跳過初始聯結器註冊和在安裝時啟動。

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

黃金映像建立步驟

最佳實踐是最後安裝聯結器，以準備Golden Image。

1. 根據您的要求準備Windows映像；安裝除Windows聯結器之外的所有所需軟體和配置。
2. 安裝思科安全終端聯結器。

使用/goldenimage 1標誌向安裝程式指示這是黃金映像部署。


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

3. 實施指令碼邏輯（如果需要），如下文[所述](#)

4. 完成安裝

5. 凍結您的黃金形象

在安裝了Golden Image應用程式、預裝了系統且安裝了帶有/goldenimagelag的Secure Endpoint後，主機已準備好凍結和分發。克隆主機啟動後，安全終端將啟動並註冊到雲。配置聯結器不需要執行進一步的操作，除非您要對策略或主機進行更改。如果在金色映像完成註冊後進行了更改，則必須重新啟動該過程。該標誌防止聯結器在基礎影象上啟動和註冊。在映像的下一個開始處，聯結器將處於為其分配的策略所配置的功能狀態。

 註：如果在您可以凍結VM之前向Secure EndpointCloud註冊了Golden Image，則建議在Golden Image VM上解除安裝並重新安裝安全終結點，然後再次凍結該VM，以防止註冊和重複聯結器問題。建議不要在此解除安裝過程中修改安全終結點的任何登錄檔值。

更新金色影象

當需要更新金色影象以保留未註冊的聯結器時，有兩個選項。

推薦的流程

1. 解除安裝聯結器。
2. 安裝主機更新/升級。
3. 使用金色影象標誌在金色影象處理之後重新安裝聯結器。
4. 如果按照該過程，主機不應啟動聯結器。
5. 凍結影象。
6. 在旋轉克隆之前，請確認黃金映像未註冊到門戶以防止不需要的重複主機。

替代流程

1. 確保主機沒有連線到Internet以防止聯結器註冊。
2. 停止聯結器服務。
3. 安裝更新。
4. 更新完成後，凍結映像
5. 需要防止聯結器註冊，以防止出現重複的主機。當您刪除連線時，會阻止它連線到雲進行註冊。此外，被停止的聯結器會一直保持該狀態，直到下次重新啟動為止，這允許克隆註冊為唯一

主機。

6. 在旋轉克隆之前，請確認黃金映像未註冊到門戶以防止不需要的重複主機。

金色影象代碼

此部分包括代碼片段，這些代碼片段有助於支援金色影象處理，並且有助於在實施身份永續性時防止連結器重複。

Golden Image設定指令碼

安裝指令碼說明

第一個指令碼「設定」在克隆之前在黃金映像上執行。只需手動執行一次。其主要目的是建立初始配置，以允許以下指令碼在克隆虛擬機器上正確運行。這些配置包括：

- 將思科安全端點服務啟動更改為手動以避免自動啟動。
- 建立在系統啟動時以最高許可權執行以下指令碼（啟動）的計畫任務。
- 建立名為「AMP_GOLD_HOST」的系統環境變數，以儲存Golden Image的主機名。啟動指令碼將使用此命令來驗證我們是否必須恢復更改

設定指令碼代碼

```
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 /
```

安裝指令碼代碼非常簡單：

第2行：將惡意軟體防護服務的啟動型別更改為手動。

第5行：創建名為「AMP_GOLD_HOST」的新環境變數，並將當前電腦的主機名儲存在該變數中。

第9行：創建名為「Startamp」的計畫任務，該任務在系統啟動期間以最高許可權運行指定的「Startup」指令碼，無需密碼。

Golden Image啟動指令碼

啟動指令碼說明

第二個指令碼「啟動」在克隆虛擬機器的每個系統啟動上運行。其主要目的是檢查當前電腦是否具有「Golden Image」的主機名：

- 如果當前電腦是黃金影像，則不執行任何操作，指令碼結束。由於我們維護計畫任務，安全終結點將在系統啟動時繼續運行。
- 如果當前電腦不是「Golden」映像，則會重置第一個指令碼所做的更改：
 - 將思科安全端點服務啟動配置更改為自動。
 - 正在啟動思科安全端點服務。
 - 正在刪除「AMP_GOLD_HOST」環境變數。
 - 刪除執行啟動指令碼的計畫任務，並刪除指令碼本身。

啟動指令碼代碼

```
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：將當前主機名與儲存的「AMP_GOLD_HOST」值進行比較；如果它們相同，則指令碼跳至「相同」標籤，否則跳至「notsame」標籤。

第4-6行：當到達「相同」標籤時，指令碼不會執行任何操作，因為它仍是黃金影像，並繼續進入「退出」標籤。

第8-16行：如果達到「notsame」標籤，指令碼將執行以下操作：


- 將惡意軟體防護服務的啟動型別更改為自動。
- 啟動惡意軟體防護服務。
- 刪除「AMP_GOLD_HOST」環境變數。
- 刪除名為「Startamp」的計畫任務



注意：請注意，TAC未正式支援本文檔中包含的指令碼。



注意：這兩個指令碼允許在克隆虛擬機器環境中啟動Cisco AMP服務。通過正確配置

 Golden映像和使用啟動指令碼，可確保思科安全終端在所有克隆虛擬機器上以正確配置運行。

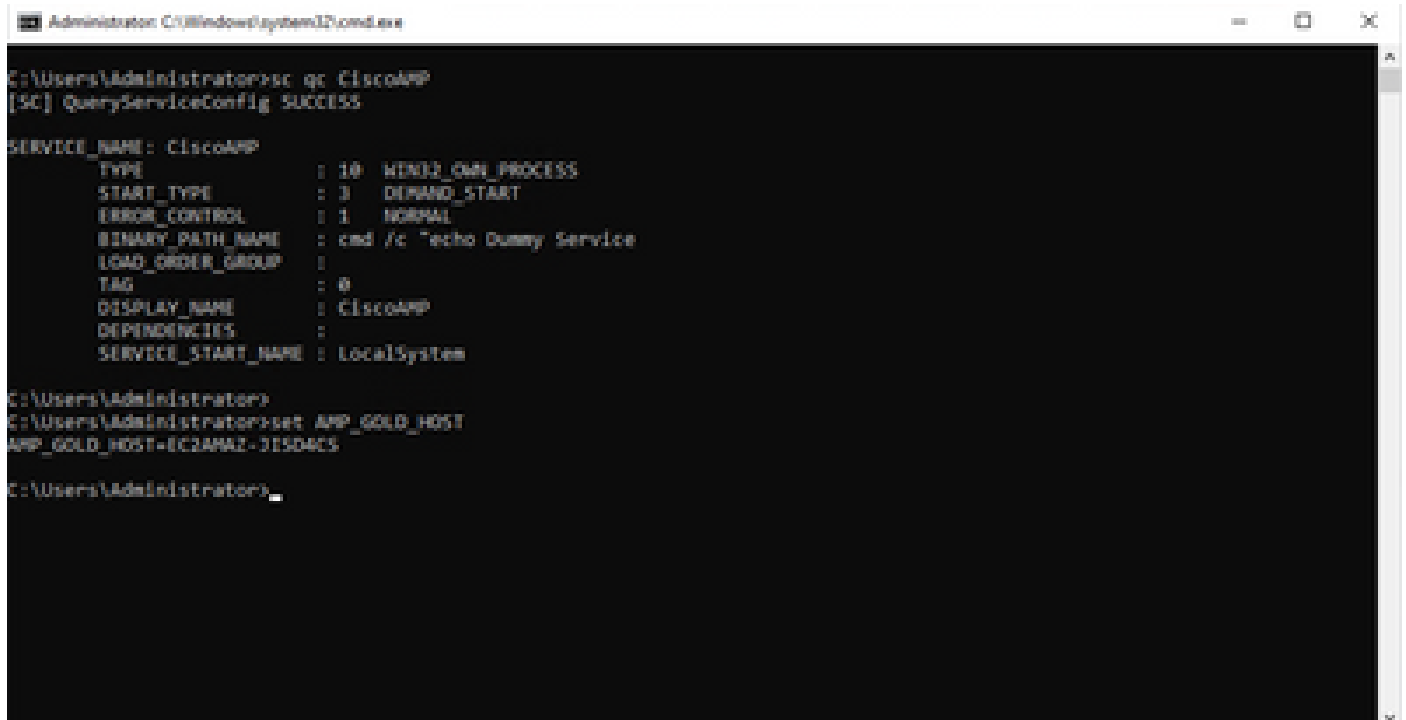
。

AWS Workspace 流程

此解決方案包括克隆之前在金色映像上執行的「Setup」指令碼和在系統啟動期間在每個克隆虛擬機器上運行的「Startup」指令碼。這些指令碼的主要目標是確保正確配置服務，同時減少手動干預。這兩個指令碼允許在克隆虛擬機器環境中啟動思科安全終端服務。通過正確配置Golden映像和使用啟動指令碼，它可以確保思科安全終端聯結器在所有克隆虛擬機器上以正確配置運行。

有關在AWS Workspace上實施Golden Image所需的指令碼代碼，請參閱Golden Image設定指令碼代碼和Golden Image啟動指令碼代碼部分。

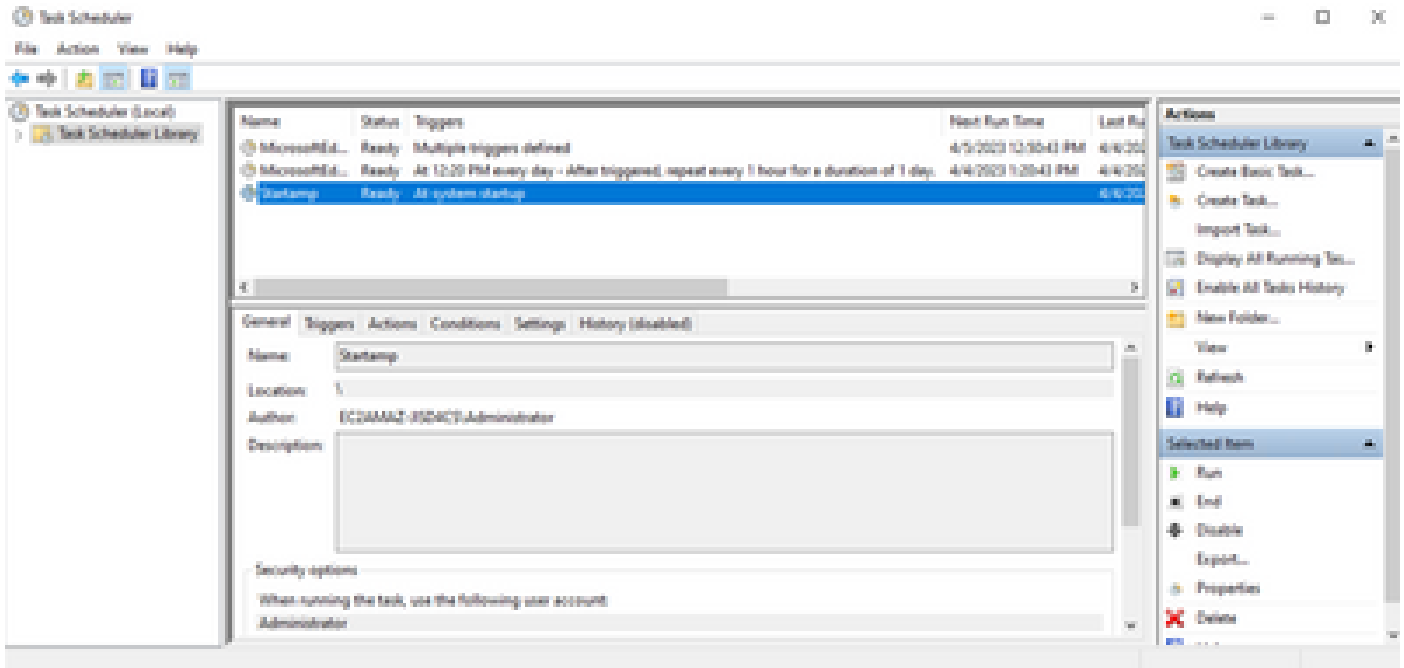
執行安裝指令碼後，我們可以驗證配置更改是否已成功部署。



```
Administrator C:\Windows\system32\cmd.exe
C:\Users\Administrator>sc qc CiscoAMP
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: CiscoAMP
        TYPE               : 10  WINDLL_OWN_PROCESS
        START_TYPE           : 3   DEMAND_START
        ERROR_CONTROL        : 1   NORMAL
        BINARY_PATH_NAME     : cmd /c "echo Dummy Service"
        LOAD_ORDER_GROUP    :
        TAG                  : 0
        DISPLAY_NAME        : CiscoAMP
        DEPENDENCIES         :
        SERVICE_START_NAME  : LocalSystem

C:\Users\Administrator>
C:\Users\Administrator>set AMP_GOLD_HOST
AMP_GOLD_HOST=EC2AMAZ-31504CS
C:\Users\Administrator>
```

由於我們在golden image上執行此操作，因此所有新例項都將具有此配置，並在啟動時執行啟動指令碼。

VMware Horizon重複問題

使用VMware Horizon，我們能夠確定在建立子級虛擬機器時，作為Horizon合成過程的一部分，會多次重新引導這些虛擬機器。這會導致以下問題：當子VM未準備就緒時（它們沒有分配最終/正確的NetBios名稱）啟用安全終端服務。這會導致安全終端出現更多問題，從而導致進程中斷。為了避免出現此問題，我們針對與Horizon Process的不相容性提出了一個解決方案，其中包括在Golden Image VM上實施附加的指令碼，並為VMware Horizon使用同步後指令碼功能

：<https://docs.vmware.com/en/VMware-Horizon/2103/published-desktops-applications.pdf>。

不再需要配置/更改

- 如果要在首次部署後對Golden Image進行任何更改，則不再需要解除安裝並重新安裝安全終結點。
- 無需將安全終端服務設定為延遲啟動。

指令碼方法

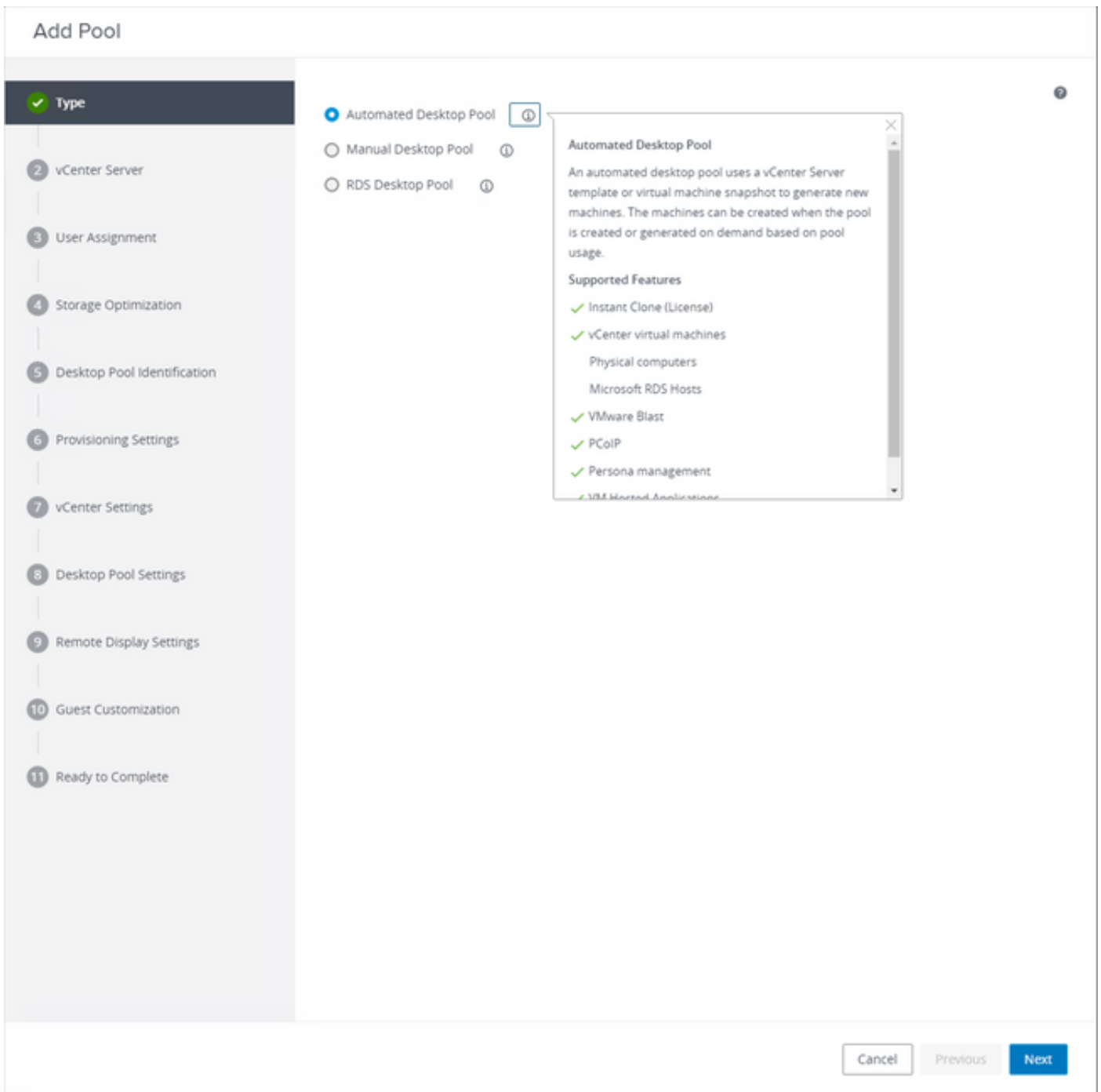
指令碼的示例可以在下面找到。

- Golden Image Setup Script：必須按照之前所述安裝安全終端聯結器後實施此指令碼，並且使用前面所述的標誌。此指令碼將Secure Endpoint服務修改為手動啟動，並將Golden Image主機名儲存為環境變數，以供下一步參考。
- Golden Image啟動腳本：此指令碼是一個邏輯檢查，其中我們將已克隆（子）虛擬機器上的主機名與上一步中儲存的主機名進行匹配，以確保我們識別何時已克隆（子）虛擬機器獲取的主機名是除Golden Image VM以外的任何名稱（該主機名將是電腦的最終主機名），然後啟動安全終端服務並將其更改為「自動」。也可以從前面提到的指令碼中刪除環境變數。這通常通

過使用部署解決方案（如VMware）中提供的機制來實現。在VMware上，您可以使用同步後引數：<https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-E177899E-023D-4E61-B058-AFE3822158AA.html> 對於AWS，您可以以類似的方式使用Startup Scripts：<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-windows-user-data.html>。

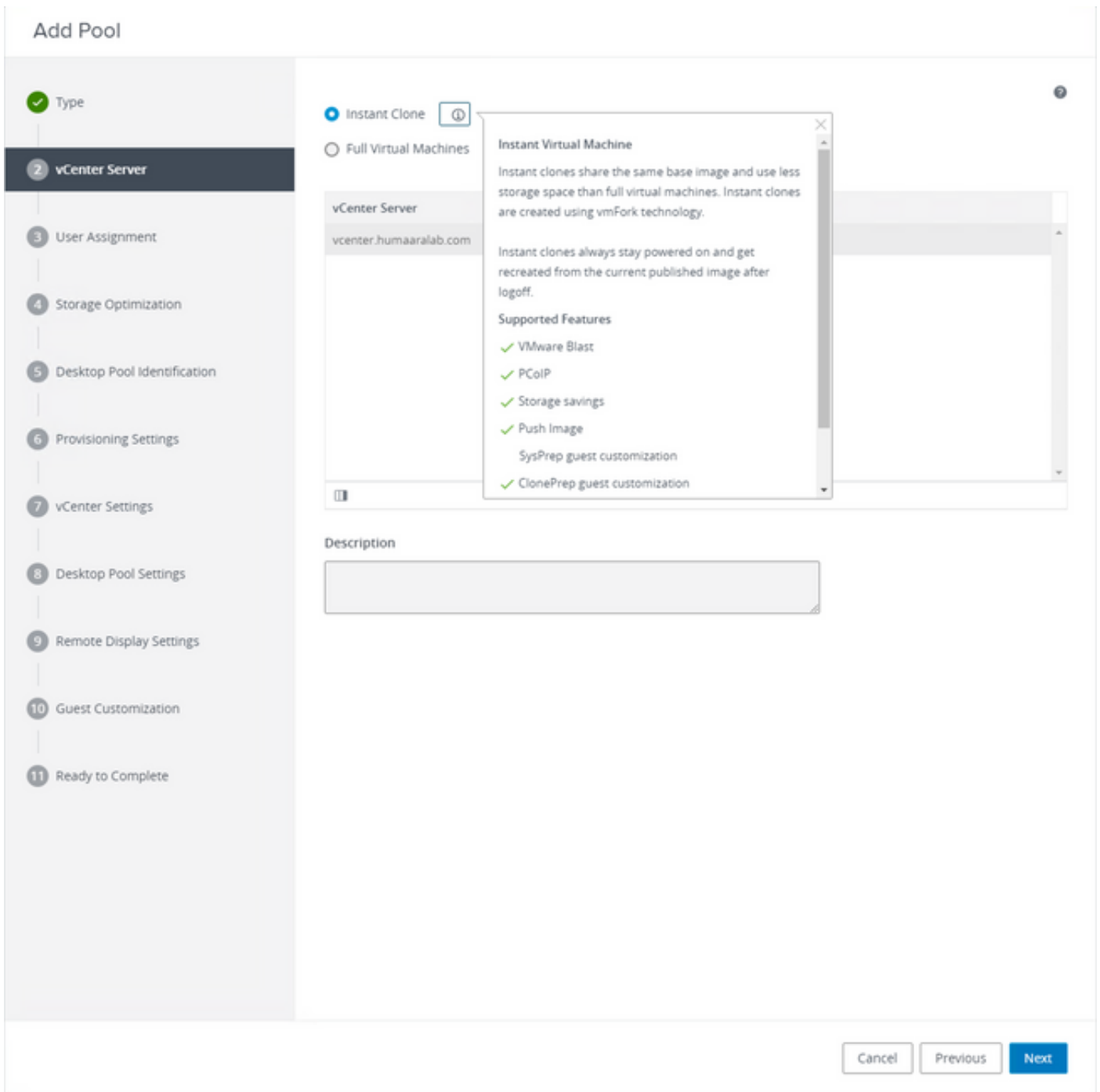
VMware Horizon配置

1. Golden Image VM已預裝，並且池初始部署所需的所有應用程式都安裝在VM上。
2. 安全終結點隨此命令列語法一起安裝，以包括goldenimage標誌。例如，`<amp;installer.exe> /R /S /goldenimage 1`。請注意，金色映像標誌可確保安全終端服務在重新啟動之前不會運行，而重新啟動對於此過程正常運行至關重要。請參閱 <https://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-endpoints/118587-technote-fireamp-00.html>
3. 安裝安全終端後，首先在Golden Image VM上執行VMWareHorizonAMPSetup.bat指令碼。實質上，此指令碼將安全端點服務更改為手動啟動，並建立環境變數，該變數儲存黃金映像主機名以供以後使用。
4. 您需要將VMWareHorizonAMPStartup.bat複製到Golden Image VM上的通用路徑，如「C:\ProgramData」，因為稍後將使用此方法。
5. Golden Image VM現在可以關閉，並且組合過程可以在VMware Horizon上啟動。
6. 從VMware Horizon的角度來看，這是有關其樣式的逐步資訊：



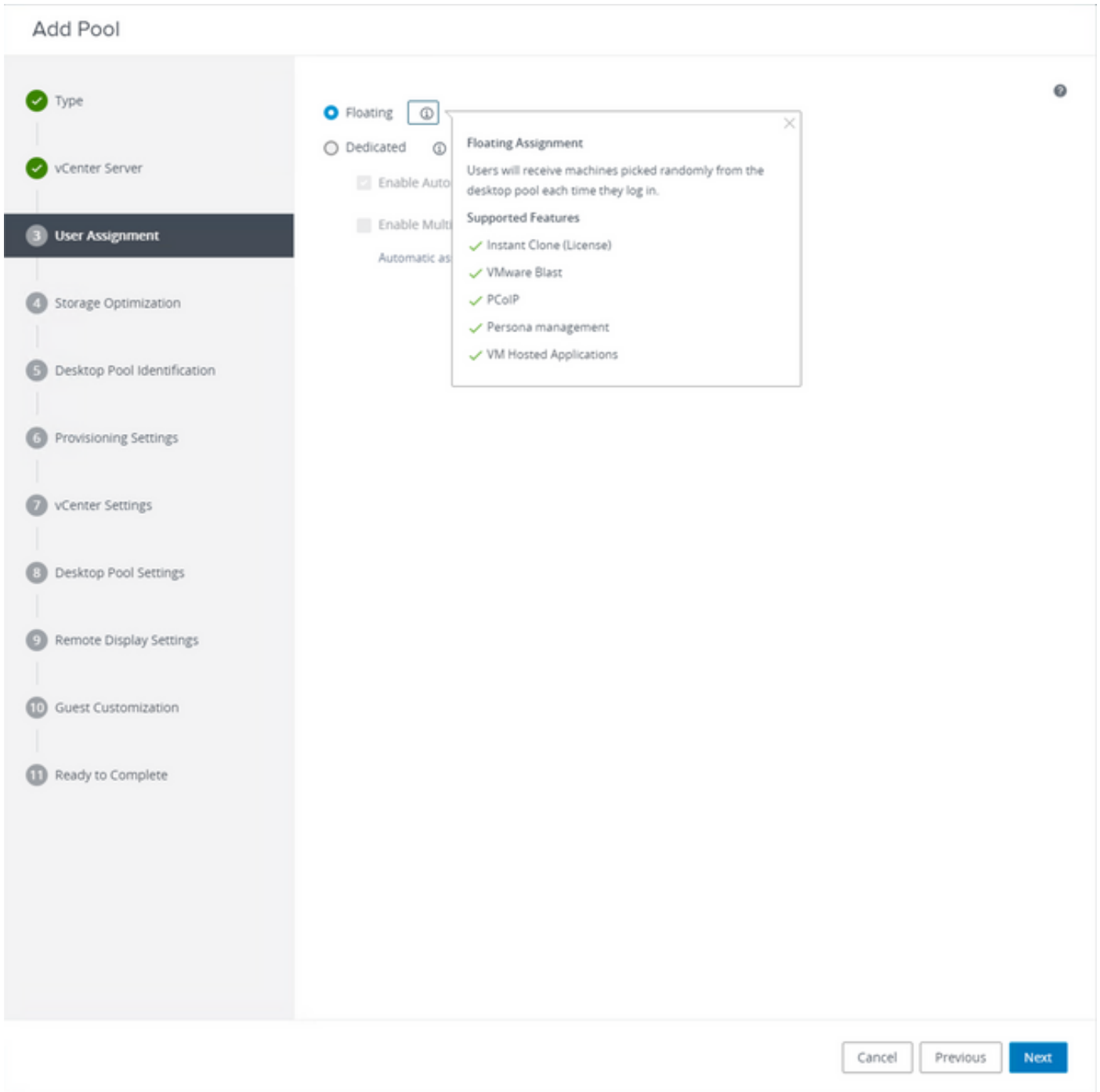
選擇「Automated Desktop Pool」

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



選擇「即時克隆」

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



選擇「浮動」型別

請參閱：<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 ⓘ

Display Name ⓘ

Access Group ⓘ

Description

Cancel

Previous

Next

案頭池名稱

Add Pool - Test-VMware-Pool

Asterisk (*) denotes required field

Basic

Enable Provisioning ⓘ

Stop Provisioning on Error

Virtual Machine Naming ⓘ

Specify Names Manually

0 names entered

Use a Naming Pattern ⓘ

* Naming Pattern

test-pool-(n.fixed=2)

Provision Machines

Machines on Demand

Min Number of Machines

All Machines Up-Front

Desktop Pool Sizing

* Maximum Machines

* Spare (Powered On) Machines

Virtual Device

Add vTPM Device to VMs ⓘ

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

Add Pool - Test-VMware-Pool

- Type
- vCenter Server
- User Assignment
- Storage Optimization
- Desktop Pool Identification
- Provisioning Settings
- 7 vCenter Settings**
- 8 Desktop Pool Settings
- 9 Remote Display Settings
- 10 Guest Customization
- 11 Ready to Complete

Default Image

Asterisk (*) denotes required field

- Golden Image in vCenter
- Snapshot

Virtual Machine Location

- VM Folder Location

Resource Settings

- Cluster
- Resource Pool
- Datstores
1 selected
- Network
Golden Image network selected

Golden Image : 這是實際的Golden Image VM。

快照 : 這是要用於部署子VM的映像。這是使用任何更改更新Golden Image時更新的值。其餘是一些特定於VMware環境的設定。

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

Category Folder

None

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

Add Pool - Test-VMware-Pool

Asterisk (*) denotes required field

10 Guest Customization

11 Ready to Complete

Domain: humaaralab.com(administrator)

* AD Container: CN=Users [Browse]

Allow Reuse of Existing Computer Accounts ⓘ

Image Publish Computer Account ⓘ

Use ClonePrep

Power-Off Script Name ⓘ

Power-Off Script Parameters

Example: p1 p2 p3

Post-Synchronization Script Name ⓘ

c:\ProgramDataVMWareHorizonAMPStartup.bat

Post-Synchronization Script Parameters

Example: p1 p2 p3

Cancel Previous Next

7.如前所述，嚮導中的步驟10是設定指令碼路徑的位置。

Add Pool - Test-VMware-Pool

<input checked="" type="checkbox"/> Type	<input type="checkbox"/> Entitle Users After Adding Pool	
<input checked="" type="checkbox"/> vCenter Server	Type	Automated Desktop Pool
<input checked="" type="checkbox"/> User Assignment	User Assignment	Floating Assignment
<input checked="" type="checkbox"/> Storage Optimization	vCenter Server	vcenter.humaaralab.com
<input checked="" type="checkbox"/> Desktop Pool Identification	Unique ID	Test-VMware-Pool
<input checked="" type="checkbox"/> Provisioning Settings	Description	-
<input checked="" type="checkbox"/> vCenter Settings	Display Name	Test-VMware-Pool
<input checked="" type="checkbox"/> Desktop Pool Settings	Access Group	/
<input checked="" type="checkbox"/> Remote Display Settings	Desktop Pool State	Enabled
<input checked="" type="checkbox"/> Guest Customization	Session Types	Desktop
11 Ready to Complete	Client Restrictions	Disabled
	Log Off After Disconnect	Never
	Connection Server Restrictions	None
	Category Folder	None
	Allow Users to Restart Machines	No
	Allow Separate Desktop Sessions from Different Client Devices	No
	Default Display Protocol	VMware Blast
	Allow Users to Choose Protocol	Yes
	3D Renderer	Manage using vSphere Client
	VRAM Size	32.00 MB

8.完成並提交後，VMware Horizon將開始進行組合，並將建立子級虛擬機器。

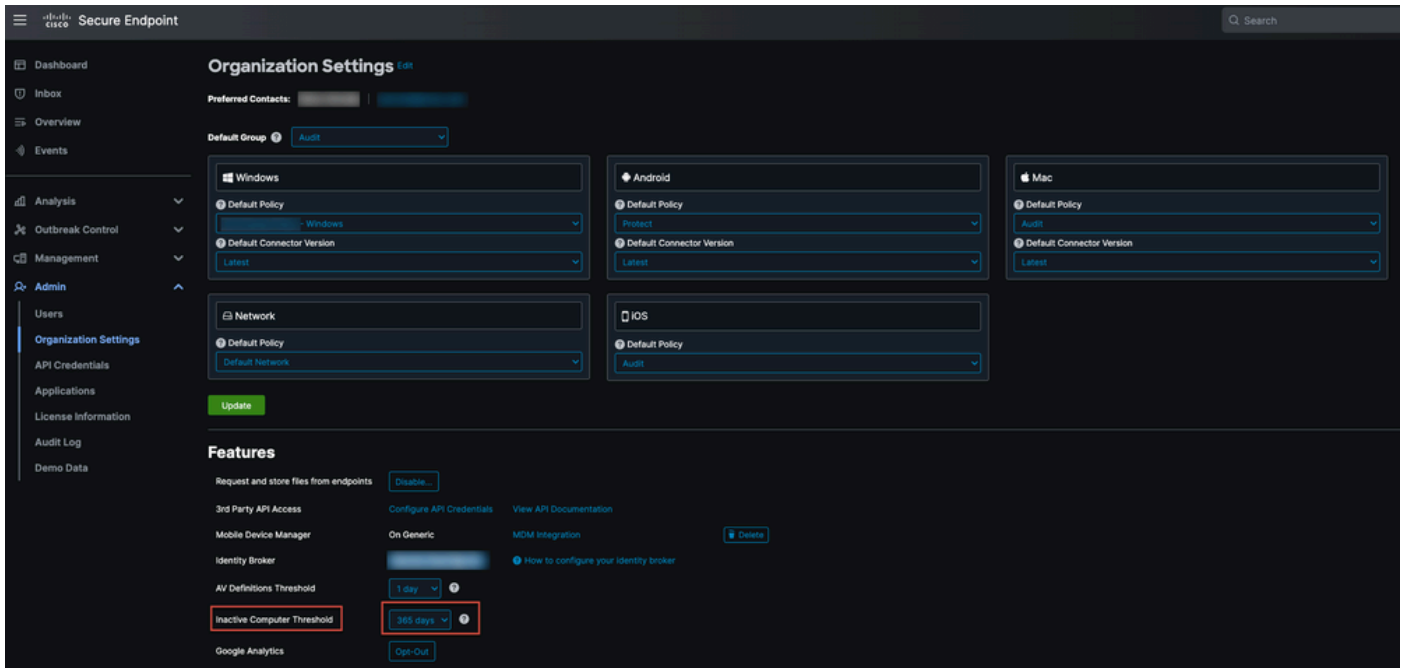
 注意：有關這些步驟的資訊，請參閱VMware指南，但這些步驟不言自明。

刪除重複條目

有多種可用方法可用來刪除連結器重複項：

1.利用安全終端門戶上的自動刪除功能刪除重複（非活動）條目：

您可以在Admin > Organization Settings下找到此設定



「非活動電腦閾值」允許您指定連結器在從「電腦管理」頁面清單中刪除之前可以離開思科雲的時間長度。預設設定為90天。非活動電腦將僅從清單中刪除，它們生成的任何事件將保留在您的安全終端組織中。如果連結器再次簽入，電腦將重新出現在清單中。

2. 利用可用的協調工作流程：<https://ciscosecurity.github.io/sxo-05-security-workflows/workflows/secure-endpoint/0056-remove-inactive-endpoints>

3. 使用外部可用指令碼刪除陳舊/舊的UUID：<https://github.com/CiscoSecurity/amp-04-delete-stale-guids>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。