Configura persistenza identità in endpoint sicuro

Sommario

Introduzione

In questo documento viene descritto come controllare la funzionalità Cisco Secure Endpoint Identity Persistence.

Che cos'è Persistenza identità?

Persistenza identità è una funzionalità che consente di mantenere un registro eventi coerente negli ambienti virtuali o quando viene ricreata l'immagine dei computer. È possibile associare un connettore a un indirizzo MAC o a un nome host in modo che non venga creato un nuovo record

del connettore ogni volta che viene avviata una nuova sessione virtuale o che viene ricreata l'immagine di un computer. Questa funzionalità è progettata specificamente per ambienti VM e Lab non persistenti e non deve essere abilitata per le configurazioni di workstation e server tradizionali.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso al portale Cisco Secure Endpoints
- Per abilitare la funzione Identity Persistence nella tua organizzazione, devi contattare Cisco TAC.
- Persistenza identità supportata solo nel sistema operativo Windows

Quando è necessaria la persistenza dell'identità?

La persistenza delle identità è una funzionalità degli endpoint sicuri che consente di identificare gli endpoint sicuri al momento della registrazione iniziale del connettore e di confrontarli con le voci note in precedenza in base a parametri di identità quali l'indirizzo MAC o il nome host per il connettore specifico. L'implementazione di questa funzione non solo contribuisce a mantenere un numero di licenze corretto, ma soprattutto consente di tenere traccia in modo corretto dei dati cronologici sui sistemi non persistenti.

Distribuzione degli endpoint virtuali

L'utilizzo più comune per la persistenza delle identità nelle distribuzioni virtuali è la distribuzione VDI (Virtual Desktop Infrastructure) non persistente. Gli ambienti desktop host VDI vengono implementati su richiesta o necessità dell'utente finale. tra cui VMware, Citrix, AWS AMI Golden Image Deployment e così via.

La VDI persistente, chiamata anche 'VDI stateful', è una configurazione in cui il desktop di ogni singolo utente è personalizzabile in modo esclusivo e "persistente" da una sessione all'altra. Questo tipo di distribuzione virtuale non richiede la funzionalità di persistenza delle identità, in quanto queste macchine sono progettate per non essere sottoposte regolarmente a re-imaging.

Come per tutto il software che potrebbe interagire con le prestazioni dell'endpoint sicuro, le applicazioni desktop virtuali devono essere valutate per eventuali esclusioni al fine di ottimizzare le funzionalità e ridurre al minimo l'impatto.

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

Distribuzione degli endpoint fisici

Per la distribuzione di Identity Persistence sui computer fisici degli endpoint sicuri possono essere applicati due scenari:

- Quando si distribuisce o si ricrea un'immagine di un endpoint fisico con un'immagine finale con il connettore Secure Endpoint preinstallato, è necessario abilitare il flag Goldenimage. Identity Persistence può essere utilizzato per evitare la duplicazione in istanze di macchine con re-imaging, ma non è richiesto.

- Quando si distribuisce o si ricrea un'immagine dell'endpoint fisico con un'immagine finale e successivamente si installa il connettore Secure Endpoint, è possibile utilizzare la persistenza delle identità per evitare la duplicazione nelle istanze dei computer sottoposti a re-imaging, ma questa operazione non è necessaria.

Panoramica sul processo di persistenza delle identità

1. Il connettore viene scaricato con un token nel file policy.xml, che lo collega al criterio in questione sul lato cloud.
2. Il connettore viene installato, memorizzando il token in local.xml, e il connettore effettua una richiesta POST al portale con il token in questione.
3. Il lato cloud presenta questo ordine di operazioni:
   a. Il computer controlla il criterio per la configurazione del criterio di sincronizzazione ID. In caso contrario, la registrazione avviene normalmente.
   b. A seconda delle impostazioni dei criteri, la funzione di registrazione verifica se il nome host o l'indirizzo MAC sono presenti nel database esistente.
      Per tutte le aziende:Tutti i criteri vengono controllati per verificare la corrispondenza su nome host o MAC, a seconda dell'impostazione. Il GUID dell'oggetto corrispondente viene registrato e inviato nuovamente al computer client finale. Il computer client assume quindi l'UUID e le impostazioni di gruppo/criterio dell'host precedentemente corrispondente. In questo modo vengono ignorate le impostazioni dei criteri o dei gruppi installate.
      Nei criteri: il token corrisponde al criterio sul lato cloud e cerca un oggetto esistente con lo stesso nome host o indirizzo MAC solo ALL'INTERNO di tale criterio. Se ne esiste uno, presuppone l'UUID. Se al criterio non è associato alcun oggetto esistente, verrà creato un nuovo oggetto. Nota: possono esistere duplicati per lo stesso nome host associato ad altri gruppi/criteri.
   c. Se non è possibile trovare una corrispondenza con un gruppo/criterio a causa di un token mancante (registrato in precedenza, una procedura di distribuzione non valida e così via), il connettore ricade nel gruppo/criterio predefinito del connettore impostato nella scheda business. In base all'impostazione del gruppo/criterio, tenta di esaminare tutti i criteri per una corrispondenza (nell'azienda), solo il criterio in questione (nel criterio) o nessuno (nessuno). In questo contesto, si consiglia di impostare il gruppo predefinito in modo che contenga le impostazioni di sincronizzazione degli ID desiderate, in modo che i computer eseguano correttamente la sincronizzazione in caso di problemi di token.

Identificazione dei duplicati nell'organizzazione

Script GitHub disponibili esternamente

Trovare gli UUID duplicati: https://github.com/CiscoSecurity/amp-04-find-duplicate-guids

Motivi per cui vengono creati duplicati

Esistono alcune istanze comuni che possono causare la visualizzazione di duplicati nella parte finale:

1. Se sono stati seguiti questi passaggi mentre il pool VDI:

- La distribuzione iniziale su una VM/VDI non persistente viene eseguita con la persistenza dell'identità disabilitata (ad esempio, utilizzare un'immagine finale).
- Il criterio viene aggiornato nel cloud per abilitare la persistenza delle identità, che durante il giorno la aggiorna nell'endpoint.
- I computer vengono aggiornati/ricreati con la stessa immagine finale, che quindi riporta il criterio originale sull'endpoint senza persistenza dell'identità.
- Il criterio localmente non dispone di Identity Persistence, quindi il server di registrazione non controlla i record precedenti.
- Questo flusso genera duplicati.

2. L'utente distribuisce l'immagine finale originale con Persistenza identità abilitata nel criterio in un gruppo e quindi sposta un endpoint in un altro gruppo dal portale degli endpoint protetti. Il record originale viene quindi inserito nel gruppo "spostato in", ma vengono create nuove copie nel gruppo originale quando le VM vengono nuovamente immesse/reinstallate.

✎ Nota: non si tratta di un elenco esaustivo di scenari che potrebbero causare duplicati, ma alcuni dei più comuni.

Problemi/sintomi comuni con distribuzione non corretta della persistenza dell'identità

Un'implementazione non corretta di Identity Persistence può causare i seguenti problemi/sintomi:

- Conteggio dei sedili del connettore non corretto
- Risultati segnalati non corretti
- Mancata corrispondenza dei dati della traiettoria dispositivo
- Scambi di nomi di computer nei registri di controllo
- I connettori si registrano ed eliminano la registrazione casualmente dalla console
- I connettori non segnalano correttamente al cloud
- Duplicazione UUID
- Duplicazione nome computer
- Incoerenza dei dati
- I computer vengono registrati nel business group/criterio predefinito dopo la ricomposizione

- Distribuzione manuale con Persistenza identità abilitata nel criterio.

- Se si distribuisce l'endpoint manualmente tramite l'opzione della riga di comando con Persistenza identità già abilitata nel criterio e successivamente si disinstalla l'endpoint e si prova a reinstallare con un pacchetto di un gruppo o di un criterio diverso, l'endpoint tornerà

automaticamente al criterio originale.

- Output dei log SFC che mostrano l'opzione di criterio in modo autonomo con 1-10 sec

```
(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'altro effetto collaterale se si prova a installare un connettore che appartiene a un gruppo diverso. Nel portale verrà visualizzato che il connettore è assegnato al gruppo corretto ma con criteri originali "errati"

Ciò è dovuto al funzionamento di Identity Persistence (ID SYNC).

Senza ID SYNC una volta che il connettore è stato disinstallato completamente o utilizzando l'opzione della riga di comando re-register. In caso di disinstallazione o di semplice GUID del nuovo connettore, in caso di comando di nuova registrazione, verranno visualizzati la nuova data di creazione e il GUID del connettore. Tuttavia, con ID SYNC che non è possibile, ID SYNC viene sovrascritto con il GUID e la DATA precedenti. È così che si sincronizza l'host.

Se il problema si verifica, è necessario implementare la correzione tramite la modifica dei criteri. È necessario spostare gli endpoint interessati di nuovo nel gruppo o nei criteri originali e verificare che i criteri siano sincronizzati. Spostare quindi gli endpoint nel gruppo o nei criteri desiderati

Procedure ottimali per l'installazione

Configura file snapvol

Se si utilizzano volumi di applicazioni per l'infrastruttura VDI, è consigliabile apportare le modifiche di configurazione alla configurazione di snapvol.cfg

Queste esclusioni devono essere implementate nel file snapvol.cfg:

Percorsi:

- 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

Chiavi del Registro di sistema:

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

Sui sistemi x64, aggiungere quanto segue:

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

Riferimenti:

- 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

Pianificazione criteri portale

Di seguito sono riportate alcune delle procedure ottimali da seguire quando si implementa Identity Persistence sul portale degli endpoint sicuri:

1. Si consiglia di utilizzare criteri/gruppi separati per gli endpoint di persistenza dell'identità per semplificare la segregazione.

2. Se si intende utilizzare l'isolamento degli endpoint e implementare l'azione Sposta computer in gruppo in caso di compromissione. Il gruppo di destinazione deve inoltre avere la persistenza delle identità abilitata e deve essere utilizzato solo per i computer VDI.

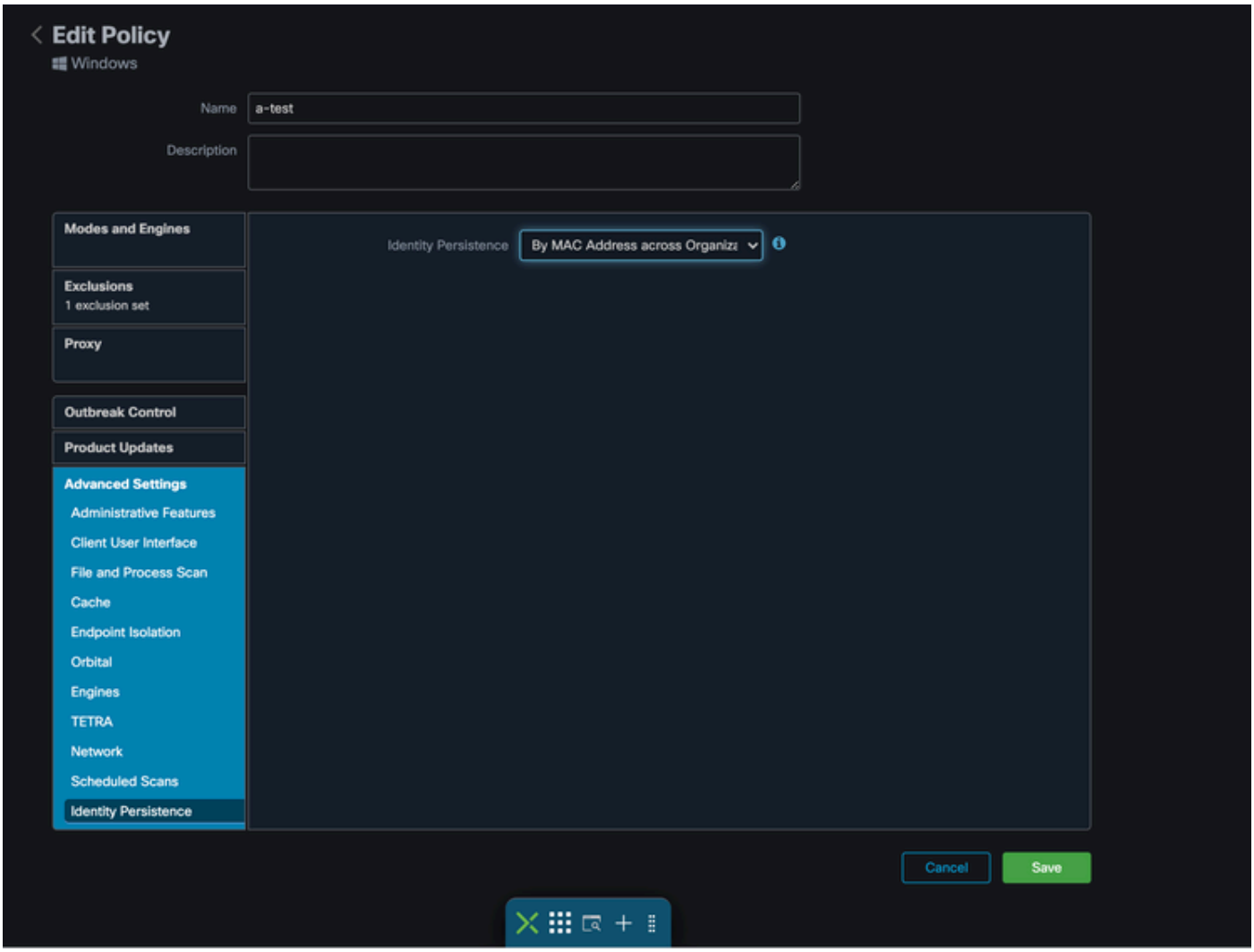
3. Non è consigliabile abilitare la persistenza delle identità nel gruppo/criterio predefinito per le impostazioni dell'organizzazione, a meno che non sia stata abilitata l'opzione Persistenza delle identità in tutti i criteri con l'opzione In tutta l'organizzazione come ambito delle impostazioni.

Configurazione

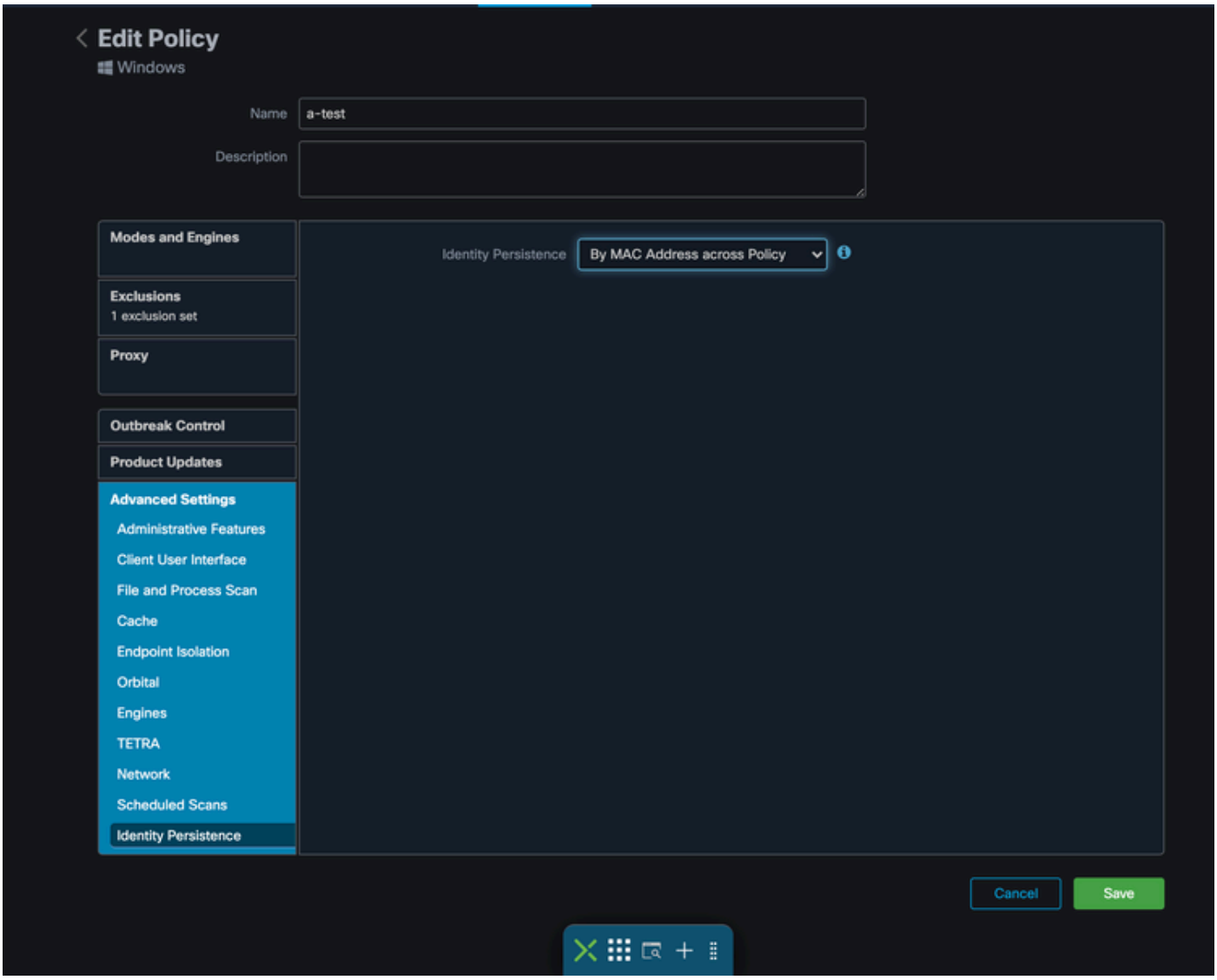
Per distribuire il connettore di endpoint sicuro con persistenza dell'identità, eseguire la procedura seguente:

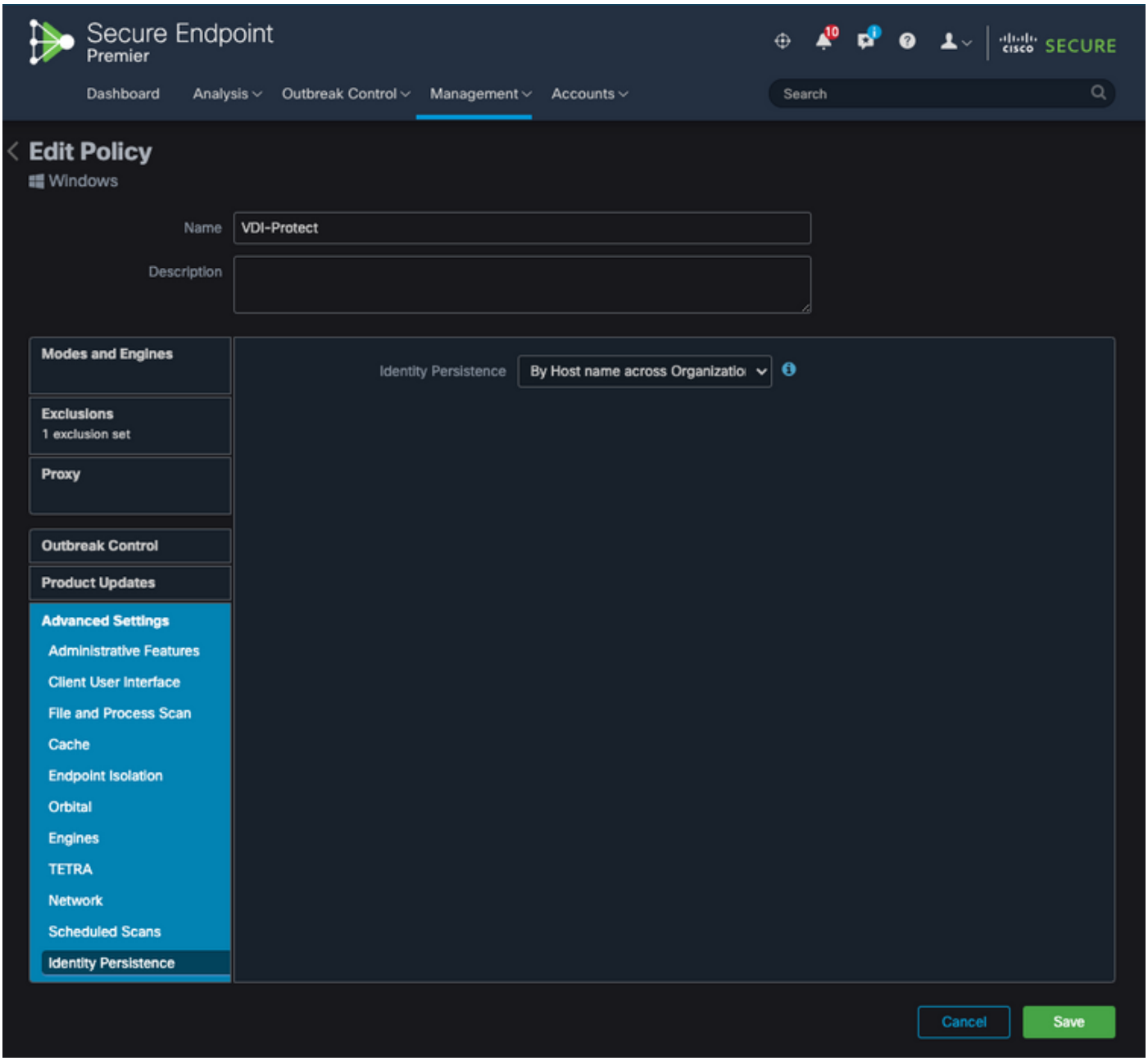
Passaggio 1. Applicare ai criteri l'impostazione di Persistenza identità desiderata:

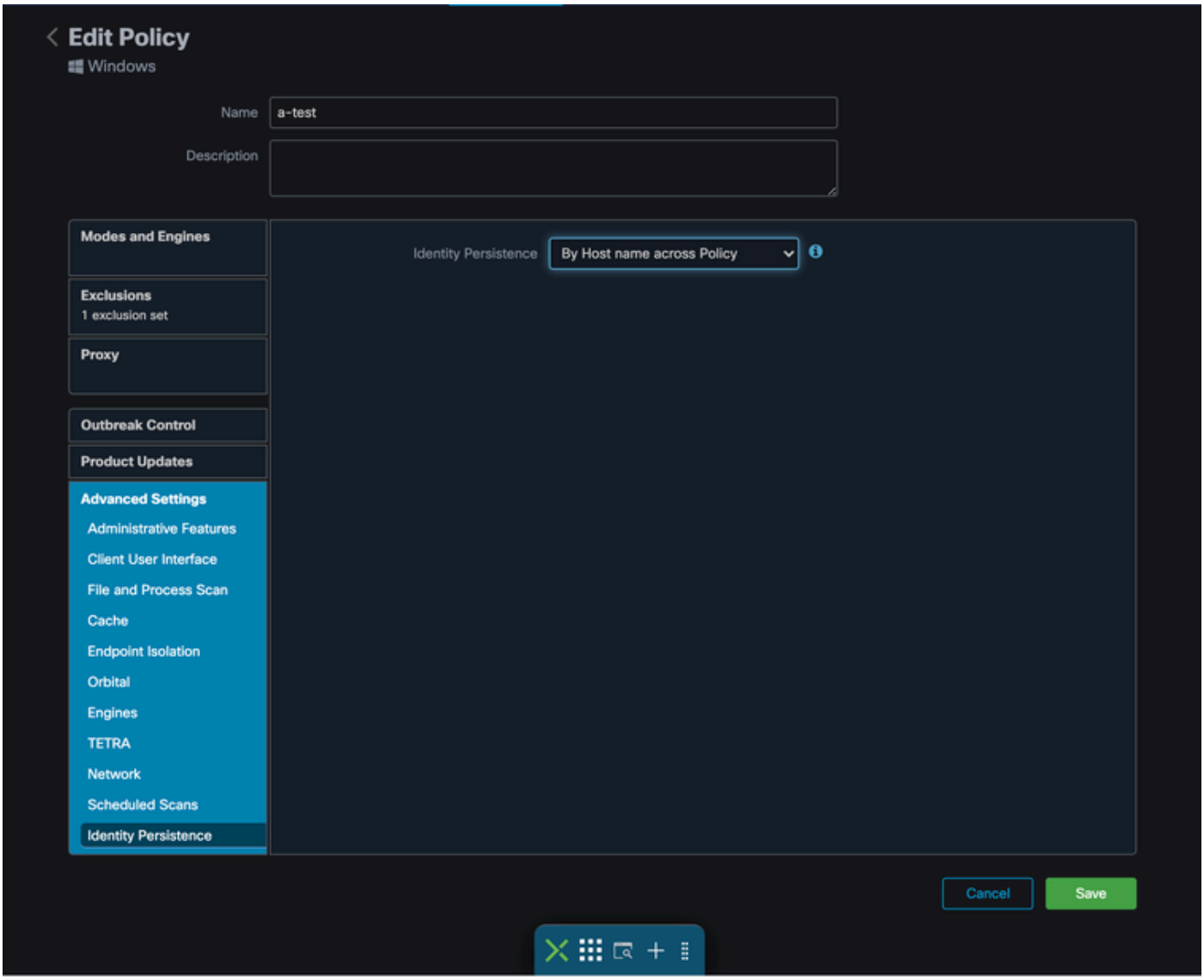
- Nel portale Secure Endpoint, passare a Gestione > Criteri.
- Selezionare il criterio desiderato per il quale si desidera attivare la persistenza delle identità, quindi fare clic su Modifica.
- Passare alla scheda Impostazioni avanzate, quindi fare clic sulla scheda Persistenza identità nella parte inferiore.
- Selezionare l'elenco a discesa Persistenza identità e scegliere l'opzione più appropriata per l'ambiente in uso. Fare riferimento a questa immagine.


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



È possibile scegliere tra cinque opzioni.

- Notare che l'opzione Feature non è attivata. Gli UUID dei connettori non sono sincronizzati con le nuove installazioni dei connettori in nessuna circostanza. Ogni nuova installazione genera un nuovo oggetto computer.
- Per indirizzo MAC in azienda: le installazioni nuove o aggiornate cercano il record Connector più recente con lo stesso indirizzo MAC per sincronizzare i dati cronologici precedenti con la nuova registrazione. Questa impostazione consente di esaminare tutti i record aziendali

  in tutti i criteri dell'organizzazione con Sincronizzazione identità impostata su un valore diverso da Nessuno. Il Connettore può aggiornare i propri criteri in modo che riflettano l'installazione precedente, se diversa da quella nuova.

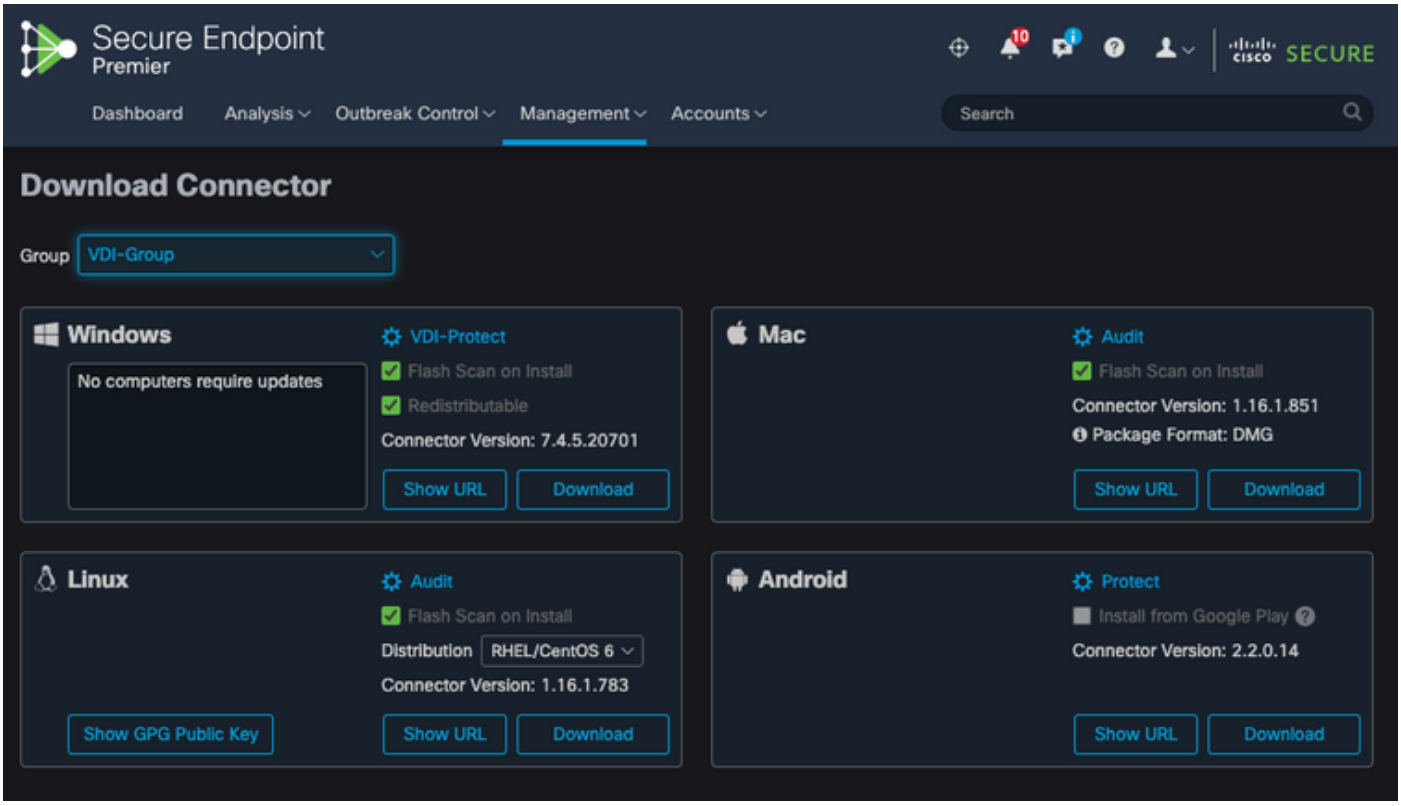
- Per indirizzo MAC nei criteri: le installazioni nuove o aggiornate cercano il record Connector più recente con lo stesso indirizzo MAC per sincronizzare i dati cronologici precedenti con la nuova registrazione. Questa impostazione consente di eseguire una ricerca solo nei record associati al criterio utilizzato nella distribuzione. Se il Connettore non è stato precedentemente installato in questo criterio, ma era precedentemente attivo in un altro criterio, può creare duplicati.

- Per nome host in azienda: le installazioni nuove o aggiornate cercano il record Connector più recente con lo stesso nome host per sincronizzare i dati cronologici precedenti con la nuova registrazione. Questa impostazione esegue una ricerca in tutti i record aziendali, indipendentemente dalle impostazioni di Persistenza identità di altri criteri e Connector può aggiornare i propri criteri in modo da riflettere l'installazione precedente, se diversa dalla nuova. Il nome host include il nome di dominio completo (FQDN) in modo che possano verificarsi duplicati se il connettore si sposta regolarmente tra le reti (come un portatile).
- Per nome host nei criteri: le installazioni nuove o aggiornate cercano il record Connector più recente con lo stesso nome host per sincronizzare i dati cronologici precedenti con la nuova registrazione. Questa impostazione consente di eseguire una ricerca solo nei record associati al criterio utilizzato per la distribuzione. Se il Connettore non è stato precedentemente installato in questo criterio, ma era precedentemente attivo in un altro criterio, può creare duplicati. Il nome host include il nome di dominio completo (FQDN), in modo che possano verificarsi duplicati anche se il connettore si sposta regolarmente tra le reti (come un laptop).

Nota: se si sceglie di utilizzare Persistenza identità, Cisco consiglia di utilizzare Per nome host in Business o Policy. Un computer ha un nome host ma può avere più indirizzi MAC e molte VM clonano gli indirizzi MAC.

Passaggio 2. Scaricare Secure Endpoint Connector.

- Selezionare Gestione > Scarica connettore.
- Selezionare il gruppo per il criterio modificato nel passaggio 1.
- Fare clic su Download per Windows Connector, come illustrato nell'immagine.



Passaggio 3. Distribuire il connettore agli endpoint.

- È ora possibile utilizzare il connettore scaricato per installare manualmente l'endpoint sicuro (con Persistenza identità abilitata) sugli endpoint.
- In caso contrario, è possibile distribuire il connettore utilizzando un'immagine dorata (vedere immagine)

Nota: selezionare il programma di installazione ridistribuibile. Si tratta di un file di circa 57 MB (le dimensioni possono variare a seconda delle versioni più recenti) che contiene i programmi di installazione a 32 e a 64 bit. Per installare il connettore su più computer, è possibile inserire il file in una condivisione di rete o inserirlo in tutti i computer. Il programma di installazione contiene un file policy.xml utilizzato come file di configurazione per l'installazione.

Creazione di immagini dorate

Quando si crea un'immagine finale da utilizzare per il processo di duplicazione di VDI, attenersi alle linee guida sulle procedure ottimali riportate nel documento del fornitore (VMware, Citrix, AWS, Azure e così via).

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

Una volta identificato il VMware, il processo di composizione AWS riavvia le VM clonate (VM figlio) più volte prima della finalizzazione della configurazione della VM, causando problemi con il processo di registrazione degli endpoint sicuri, in quanto attualmente alle VM clonate (VM figlio) non sono stati assegnati i nomi host finali/corretti e ciò fa sì che le VM clonate (VM figlio) utilizzino il nome host dell'immagine dorata e si registrino nel cloud di endpoint sicuri. Questo interrompe il processo di duplicazione e causa problemi.

Questo non è un problema con il processo di connessione dell'endpoint sicuro, ma è incompatibile con il processo di duplicazione e con la registrazione dell'endpoint sicuro. Per prevenire questo problema, abbiamo identificato alcune modifiche da implementare nel processo di duplicazione che aiutano a risolvere questi problemi.

Queste sono le modifiche che devono essere implementate sulla VM Golden Image prima che l'immagine venga bloccata per essere duplicata

1. Utilizzare sempre il flag Goldenimage sull'immagine dorata al momento dell'installazione di Secure Endpoint.

2. Implementare la sezione Golden Image Setup Script e la sezione Golden Image Startup Script per trovare gli script che consentirebbero di attivare il servizio Endpoint solo quando viene implementato un nome host finale nelle VM clonate (VM figlio). Per ulteriori informazioni, fare riferimento alla sezione Problemi di duplicazione orizzonte VMware.

Flag di sostituzione immagine dorata

Quando si utilizza il programma di installazione, il flag da utilizzare per le immagini dorate è /goldenimage 1.

Il flag golden image impedisce l'avvio e la registrazione del connettore sull'immagine di base. All'avvio successivo dell'immagine, il connettore si trova nello stato funzionale in cui è stato configurato dal criterio assegnato.

Per informazioni su altri contrassegni, è possibile utilizzare, vedere questo articolo.

Quando si utilizza il programma di installazione, il nuovo flag da utilizzare per le immagini golden è /goldenimage [1|0]

0 - Valore predefinito - questo valore non attiva l'opzione golden image e funziona come se il programma di installazione fosse stato eseguito senza l'opzione. Non ignorare la registrazione iniziale del connettore e l'avvio durante l'installazione.

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

1 - Installare come immagine dorata. Si tratta dell'opzione tipica utilizzata con il contrassegno ed è l'unico utilizzo previsto. Ignora la registrazione iniziale del connettore e l'avvio durante l'installazione.

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

Passi per la creazione di immagini dorate

È buona norma installare l'ultimo connettore per la preparazione dell'immagine dorata.

1. Preparare l'immagine Windows in base alle proprie esigenze; installare tutto il software e le configurazioni necessarie per l'immagine Windows, ad eccezione del connettore.
2. Installare il connettore Cisco Secure Endpoint.

Utilizzare il flag /goldenimage 1 per indicare all'installatore che si tratta di una distribuzione di immagini dorate.

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

3. Implementare la logica dello script (se necessario) come descritto di seguito

4. Completare l'installazione

5. Bloccare l'immagine dorata

Dopo l'installazione delle applicazioni, il sistema viene preparato e Secure Endpoint viene installato con/goldenimageflag, l'host è pronto per essere bloccato e distribuito. Una volta avviato l'host clonato, Secure Endpoint si avvia e si registra nel cloud. Non sono necessarie ulteriori azioni per la configurazione del connettore a meno che non si desideri apportare modifiche al criterio o all'host. Se vengono apportate modifiche dopo che l'immagine finale ha completato la registrazione, è necessario riavviare il processo. L'indicatore impedisce l'avvio e la registrazione del connettore sull'immagine di base. Al successivo avvio dell'immagine, il connettore sarà nello stato funzionale in cui è stato configurato dal criterio assegnato.

 Nota: se l'immagine dorata viene registrata su Secure Endpoint Cloud prima di poter bloccare la VM, si consiglia di disinstallare e reinstallare Secure Endpoint sulla VM dell'immagine dorata e quindi bloccare nuovamente la VM per evitare problemi di registrazione e duplicazione del connettore. Non è consigliabile modificare i valori del Registro di sistema per Secure Endpoint durante il processo di disinstallazione.

Aggiornare l'immagine dorata

Sono disponibili due opzioni quando è necessario aggiornare un'immagine dorata per mantenere un connettore non registrato.

Processo consigliato

1. Disinstallare il connettore.
2. Installare gli aggiornamenti dell'host.
3. Reinstallare il connettore dopo il processo dell'immagine dorata utilizzando i flag dell'immagine dorata.
4. L'host non deve avviare il connettore se il processo viene seguito.
5. Bloccare l'immagine.
6. Prima di eseguire lo spin-up dei duplicati, verificare che l'immagine finale non sia stata registrata nel portale per impedire la presenza di host duplicati indesiderati.

Processo alternativo

1. Verificare che l'host non disponga di connettività a Internet per impedire la registrazione del connettore.
2. Arrestare il servizio connettore.
3. Installare gli aggiornamenti.
4. Blocca l'immagine al termine degli aggiornamenti
5. Per evitare la duplicazione degli host, è necessario impedire la registrazione del connettore. Quando si rimuove la connettività, non è possibile eseguire la registrazione nel cloud. Inoltre, il connettore in fase di arresto lo manterrà in tale stato fino al successivo riavvio, consentendo ai duplicati di registrarsi come host univoci.
6. Prima di eseguire lo spin-up dei duplicati, verificare che l'immagine finale non sia stata

registrata nel portale per impedire la presenza di host duplicati indesiderati.

Golden Image Code

Questa sezione è costituita dai frammenti di codice che supportano il processo Golden Image e consentono di evitare duplicati dei connettori durante l'implementazione di Identity Persistence.

Script di impostazione immagine dorata

Descrizione script di installazione

Il primo script, 'Setup', viene eseguito sull'immagine d'oro prima di clonarla. Deve essere eseguito manualmente solo una volta. Il suo scopo principale è quello di stabilire configurazioni iniziali che consentano il corretto funzionamento del seguente script sulle macchine virtuali clonate. Queste configurazioni includono:

- Modifica dell'avvio del servizio Cisco Secure Endpoint in manuale per evitare l'avvio automatico.
- Creazione di un'operazione pianificata che esegue lo script seguente (Avvio) all'avvio del sistema con i privilegi più elevati.
- Creazione di una variabile di ambiente di sistema denominata "AMP_GOLD_HOST" in cui è memorizzato il nome host dell'immagine d'oro. Viene utilizzato dallo script di avvio per verificare se è necessario annullare le modifiche

Imposta codice script

```
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 /
```

Il codice dello script di installazione è molto semplice:

Riga 2: modifica il tipo di avvio del servizio di protezione dal malware in manuale.

Riga 5: crea una nuova variabile di ambiente denominata "AMP_GOLD_HOST" in cui salva il nome host del computer corrente.

Riga 9: crea un'attività pianificata denominata "Startamp" che esegue lo script di avvio specificato durante l'avvio del sistema con i privilegi più elevati, senza richiedere una password.

Script di avvio con immagine dorata

Descrizione script di avvio

Il secondo script, 'Avvio', viene eseguito a ogni avvio del sistema nelle macchine virtuali clonate. Il suo scopo principale è quello di controllare se la macchina attuale ha il nome host dell'immagine d'oro:

- Se il computer corrente è l'immagine dorata, non viene eseguita alcuna azione e lo script termina. L'esecuzione di Secure Endpoint continuerà all'avvio del sistema poiché l'attività pianificata viene mantenuta.
- Se il computer corrente NON è l'immagine 'Golden', le modifiche apportate dal primo script vengono reimpostate:
    - Impostazione della configurazione di avvio del servizio Cisco Secure Endpoint su automatica.
    - Avvio del servizio Cisco Secure Endpoint.
    - Rimozione della variabile di ambiente "AMP_GOLD_HOST".
    - Eliminazione dell'attività pianificata che esegue lo script di avvio ed eliminazione dello script stesso.

Codice script di avvio

```
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
```

Riga 2: confronta il nome host corrente con il valore "AMP_GOLD_HOST" memorizzato; se sono uguali, lo script passa alla "stessa" etichetta, altrimenti passa all'etichetta "non uguale".

Riga 4-6: quando viene raggiunta la "stessa" etichetta, la sceneggiatura non fa nulla poiché è ancora l'immagine d'oro e procede verso l'etichetta di "uscita".

Riga 8-16: se viene raggiunta l'etichetta "notsame", lo script esegue le azioni seguenti:

- Imposta il tipo di avvio automatico del servizio di protezione dal malware.
- Avvia il servizio di protezione dal malware.
- Rimuove la variabile di ambiente "AMP_GOLD_HOST".
- Elimina l'attività pianificata denominata Startamp.

Nota: gli script contenuti in questo documento non sono ufficialmente supportati da TAC.

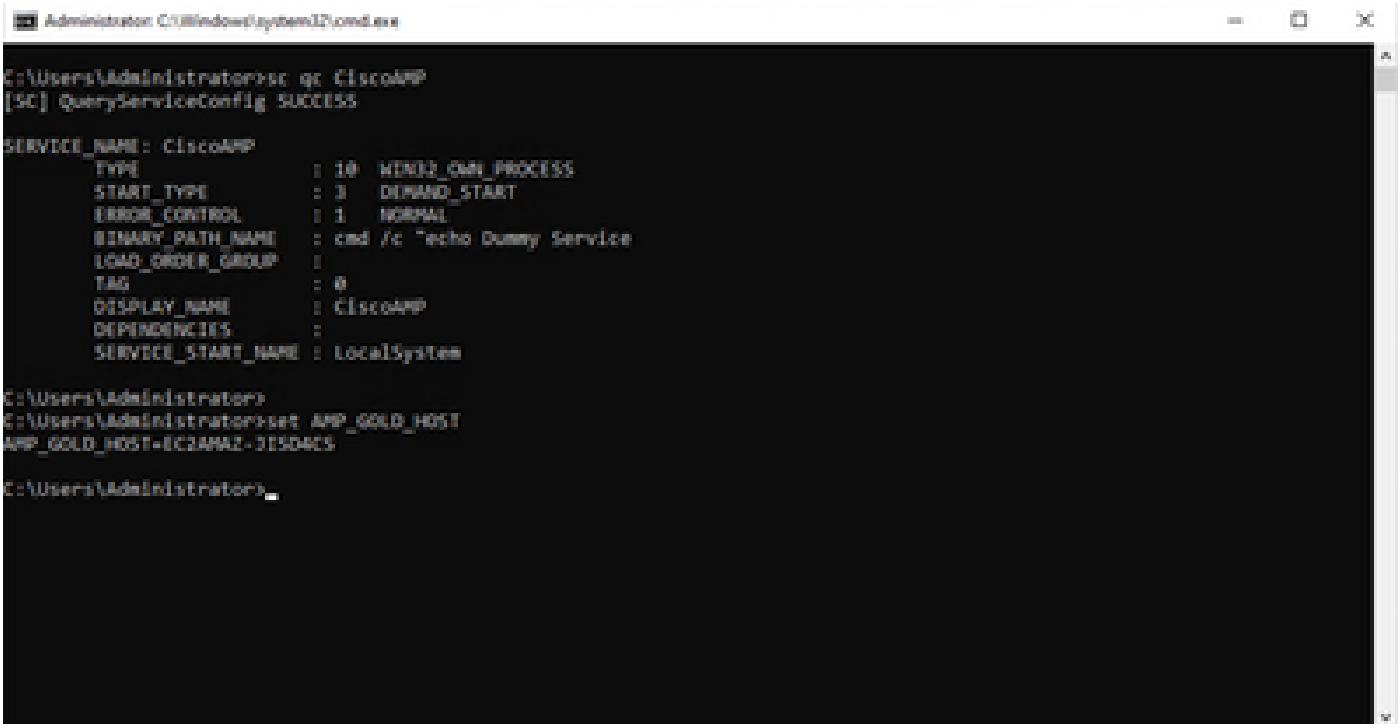
Nota: questi due script consentono l'avvio del servizio Cisco AMP in ambienti di macchine virtuali clonati. Configurando correttamente l'immagine Golden e utilizzando gli script di avvio, garantisce che Cisco Secure Endpoint venga eseguito su tutte le macchine virtuali clonate con la configurazione corretta.

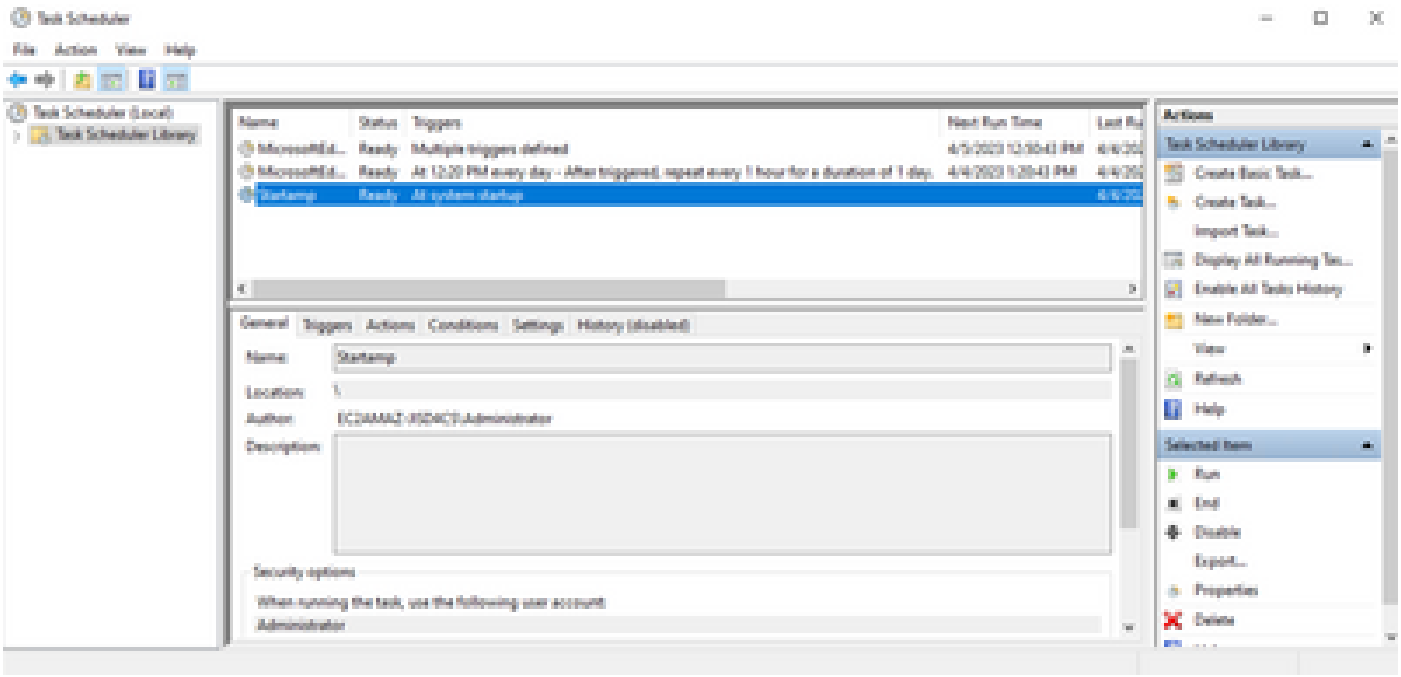
Processo AWS Workspace

Questa soluzione è costituita da uno script di installazione eseguito sull'immagine finale prima della clonazione e da uno script di avvio eseguito su ogni macchina virtuale clonata durante l'avvio del sistema. L'obiettivo principale di questi script è quello di garantire la corretta configurazione del servizio, riducendo al contempo gli interventi manuali. Questi due script consentono l'avvio del servizio Cisco Secure Endpoint in ambienti di macchine virtuali clonati. Configurando correttamente l'immagine Golden e utilizzando gli script di avvio, garantisce che il connettore Cisco Secure Endpoint venga eseguito su tutte le macchine virtuali clonate con la configurazione corretta

Fare riferimento alle sezioni Golden Image Setup Script Code e Golden Image Startup Script Code per il codice di script richiesto per l'implementazione di Golden Image su AWS Workspace.

Dopo aver eseguito lo script di installazione, è possibile verificare che le modifiche alla configurazione siano state distribuite correttamente.





Poiché questa azione è stata eseguita sull'immagine finale, tutte le nuove istanze avranno questa configurazione ed eseguiranno lo script di avvio all'avvio.

Problemi di duplicazione orizzonte VMware

Con VMware Horizon, siamo stati in grado di identificare che le macchine virtuali secondarie, quando vengono create, vengono riavviate più volte come parte del processo di composizione di Horizon. Ciò causa problemi quando i servizi endpoint protetti vengono abilitati quando le VM figlio non sono pronte (non dispongono del nome NetBios finale/corretto). In questo modo, si creano ulteriori problemi con l'endpoint sicuro che diventano confusi e quindi il processo si interrompe. Per evitare di incorrere in questo problema, abbiamo trovato una soluzione per questa

incompatibilità con Horizon Process che prevede l'implementazione degli script allegati sulla VM Golden Image e l'utilizzo della funzionalità di script post-sincronizzazione per VMware Horizon: https://docs.vmware.com/en/VMware-Horizon/2103/published-desktops-applications.pdf.

Configurazione/modifiche non più necessarie

- Non è più necessario disinstallare e reinstallare Secure Endpoint se si desidera apportare modifiche all'immagine finale dopo la prima distribuzione.
- Non è necessario impostare il servizio Endpoint protetto su Avvio ritardato.

Metodologia script

Di seguito sono riportati alcuni esempi di script.

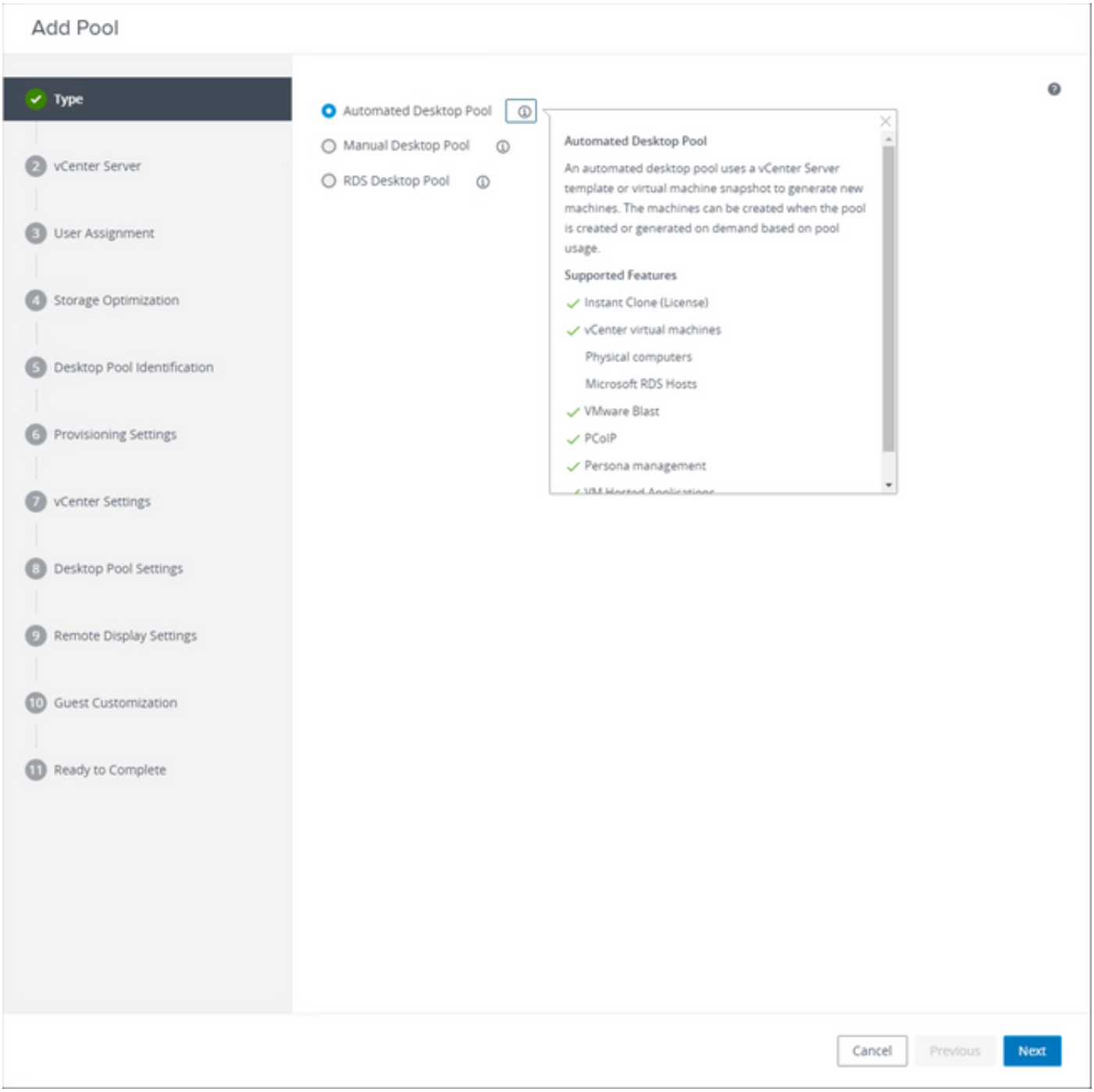
- Script di impostazione immagine dorata: questo script deve essere implementato una volta installato il connettore Secure Endpoint come descritto in precedenza con i flag come documentato in precedenza. Questo script ha modificato il servizio Secure Endpoint in Manual Start e salva il nome host dell'immagine dorata come variabile di ambiente come riferimento nel passaggio successivo.

- Script di avvio con immagine d'oro: questo script è un controllo logico in cui il nome host delle VM clonate (figlie) viene confrontato con quello memorizzato nel passaggio precedente per garantire che venga identificato quando la VM clonata (figlie) ottiene un nome host diverso da quello della VM con immagine d'oro (che sarebbe il nome host finale per la macchina) e quindi si avvia il servizio Endpoint protetto e lo si imposta su Automatico. È inoltre possibile rimuovere la variabile di ambiente dallo script indicato in precedenza. Questo viene generalmente implementato utilizzando i meccanismi disponibili nella soluzione di installazione, ad esempio VMware. In VMware è possibile utilizzare i parametri di post-sincronizzazione: https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-E177899E-023D-4E61-B058-AFE3822158AA.html Analogamente, per AWS è possibile utilizzare gli script di avvio in modo simile: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-windows-user-data.html.

Configurazione orizzonte VMware

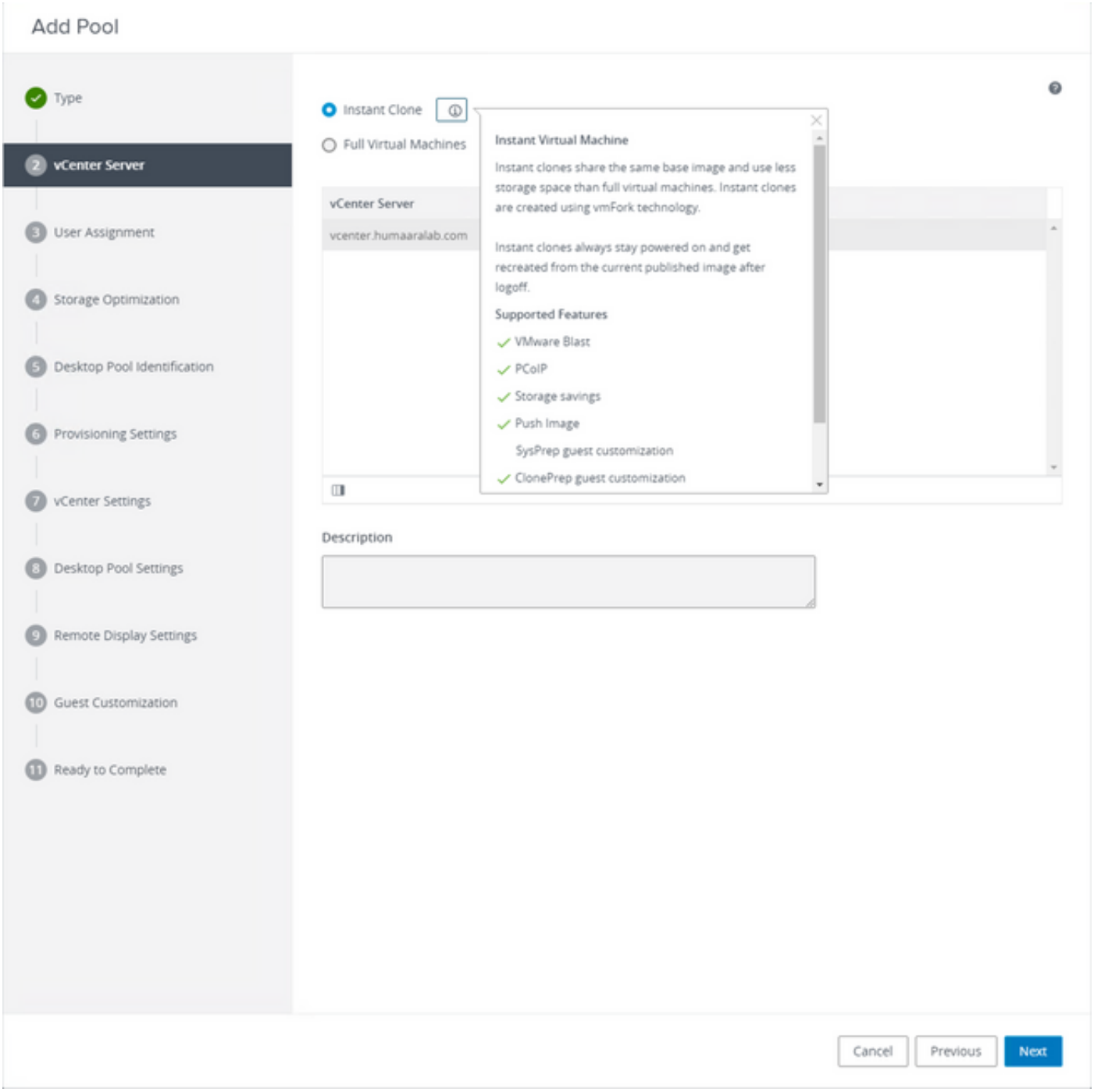
1. Golden Image VM viene predisposto e tutte le applicazioni necessarie per la distribuzione iniziale del pool vengono installate sulla VM.
2. Con questa sintassi della riga di comando viene installato un endpoint sicuro che include il flag goldenimage. Ad esempio, <ampinstaller.exe> /R /S /goldenimage 1. Il flag Golden Image assicura che il servizio Secure Endpoint non venga eseguito fino al riavvio, fondamentale per il corretto funzionamento del processo. Fare riferimento a https://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-endpoints/118587-technote-fireamp-00.html
3. Dopo l'installazione dell'endpoint sicuro, eseguire prima lo script VMWareHorizonAMPSetup.bat sulla VM Golden Image. In sostanza, questo script imposta il servizio Secure Endpoint su Manual Start e crea una variabile di ambiente che memorizza il nome host dell'immagine dorata per un utilizzo successivo.

4. È necessario copiare il file VMWareHorizonAMPStartup.bat in un percorso universale sulla VM Golden Image, ad esempio "C:\ProgramData", in quanto verrà utilizzato nei passaggi successivi.
5. La VM Golden Image può ora essere chiusa e il processo di composizione può essere avviato su VMware Horizon.
6. Ecco le informazioni dettagliate su come appare dalla prospettiva VMware Horizon:



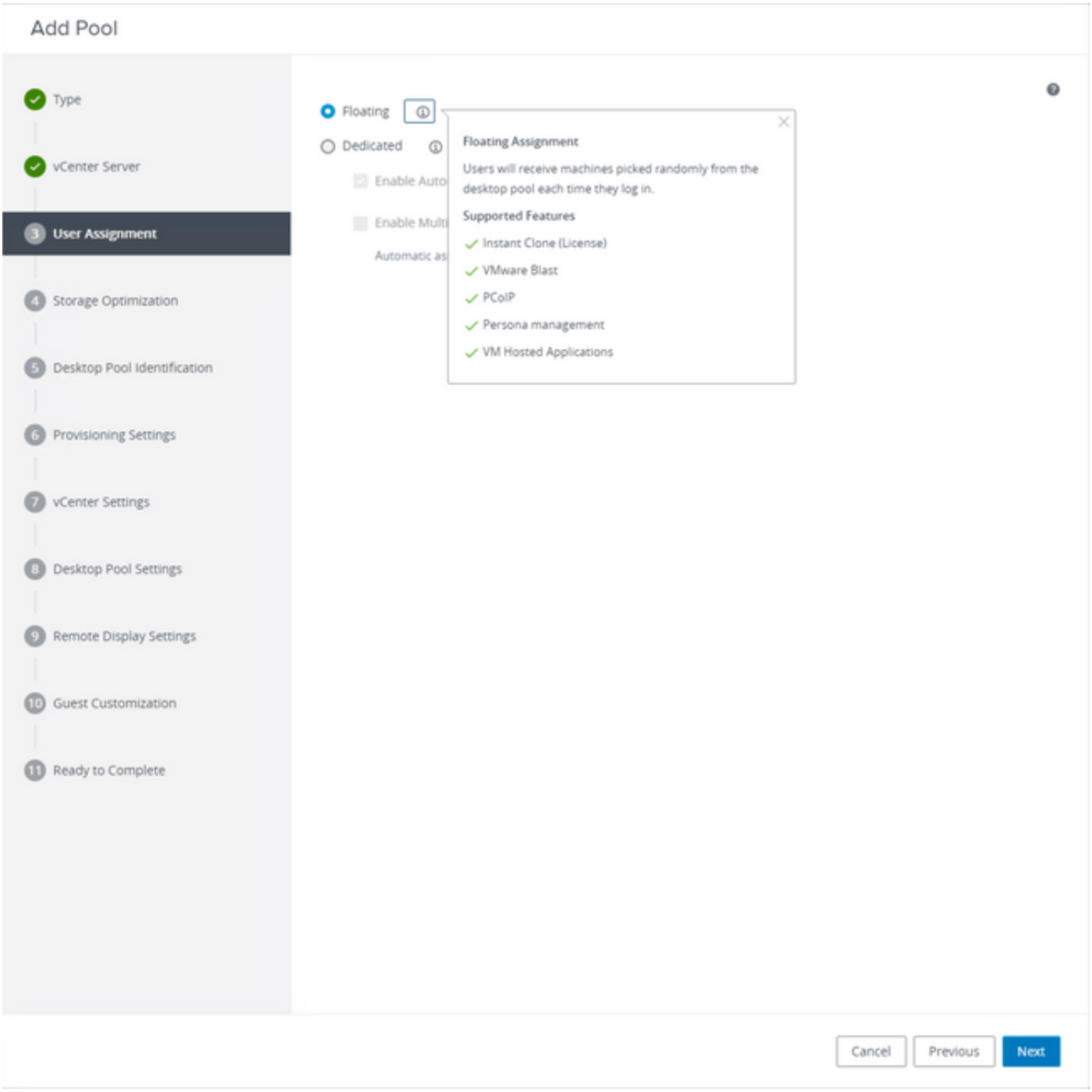
Selezione di "Pool di desktop automatico"

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



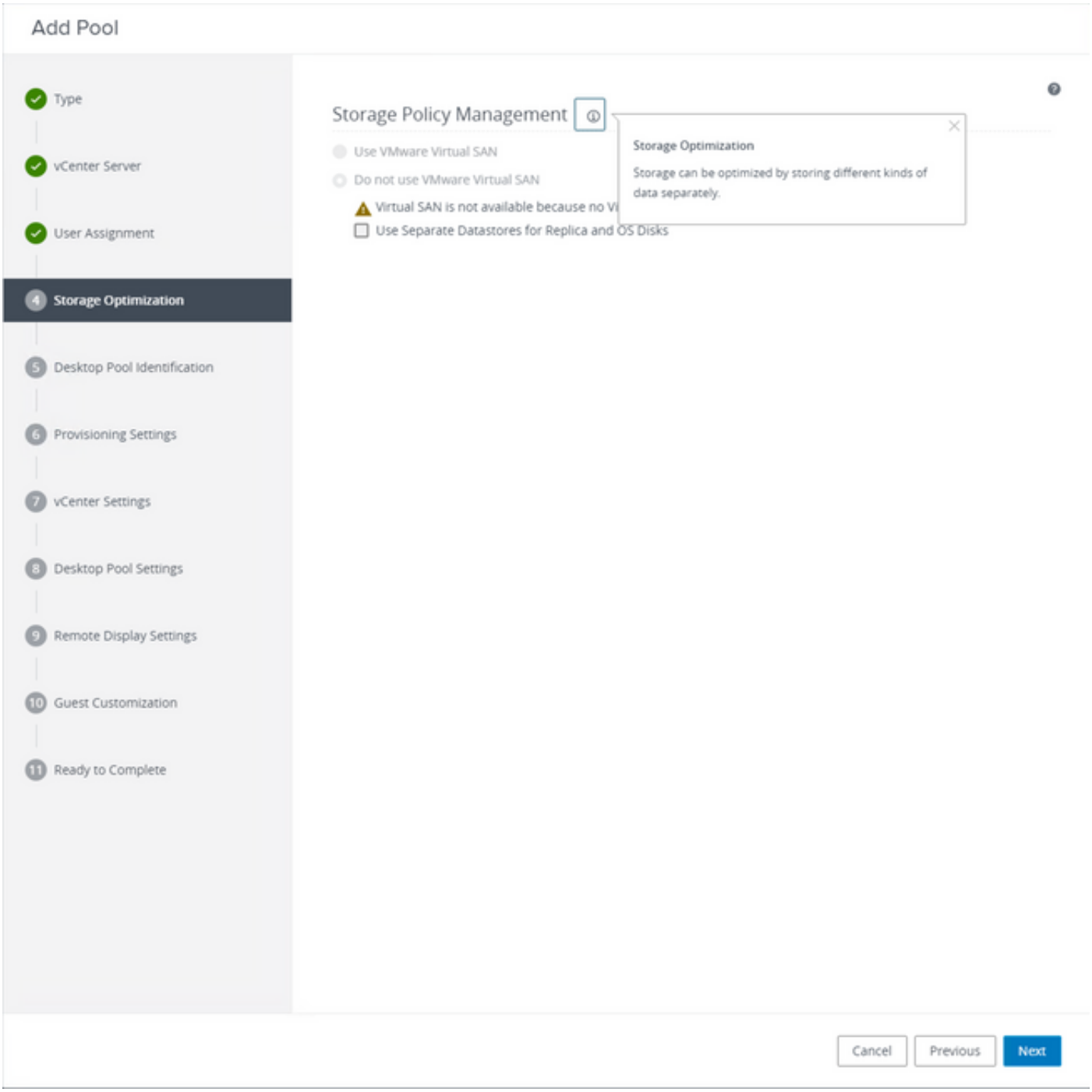
Selezione di "Cloni istantanei"

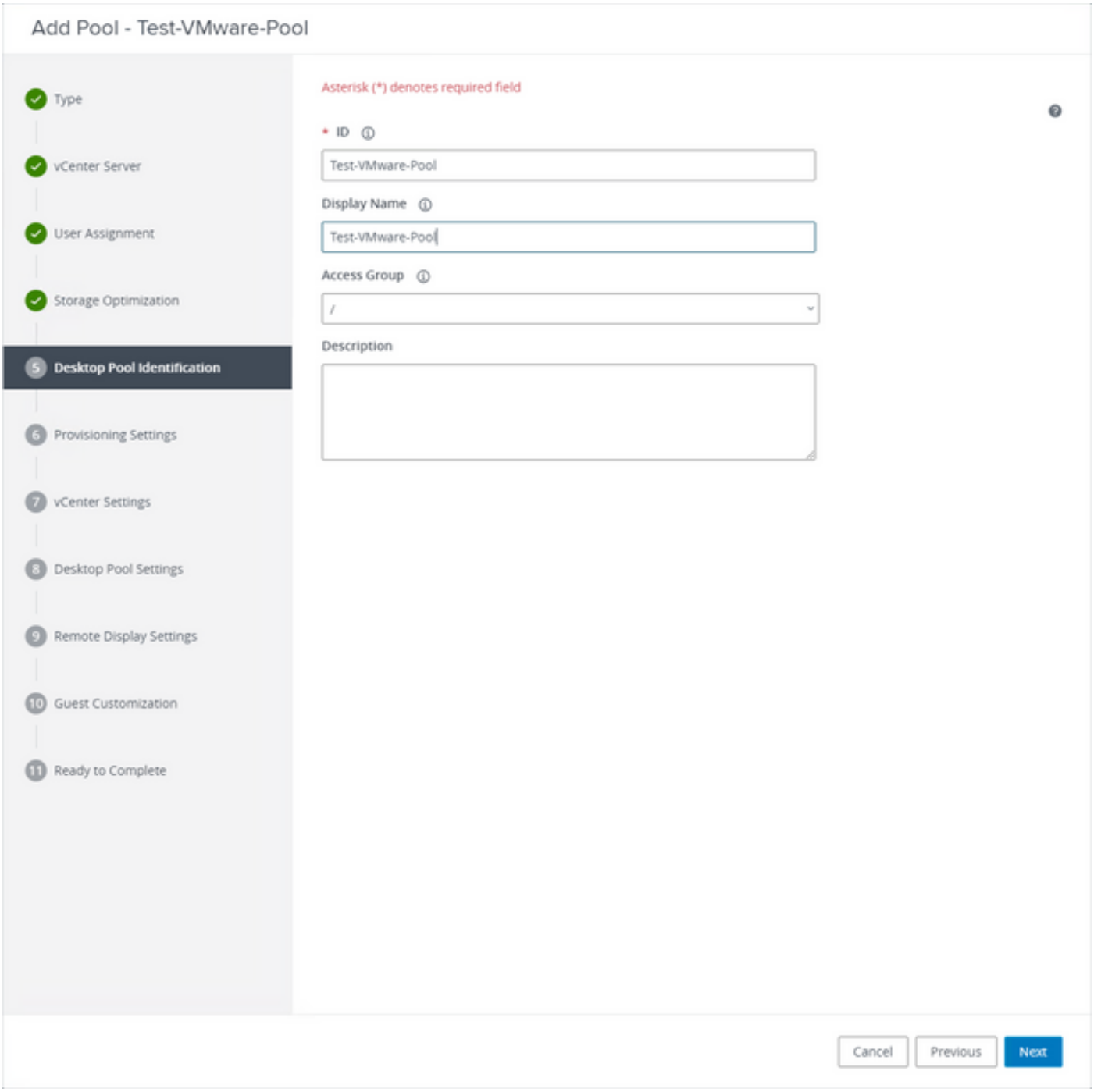
Fare riferimento a: https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-D7C0150E-18CE-4012-944D-4E9AF5B28347.html



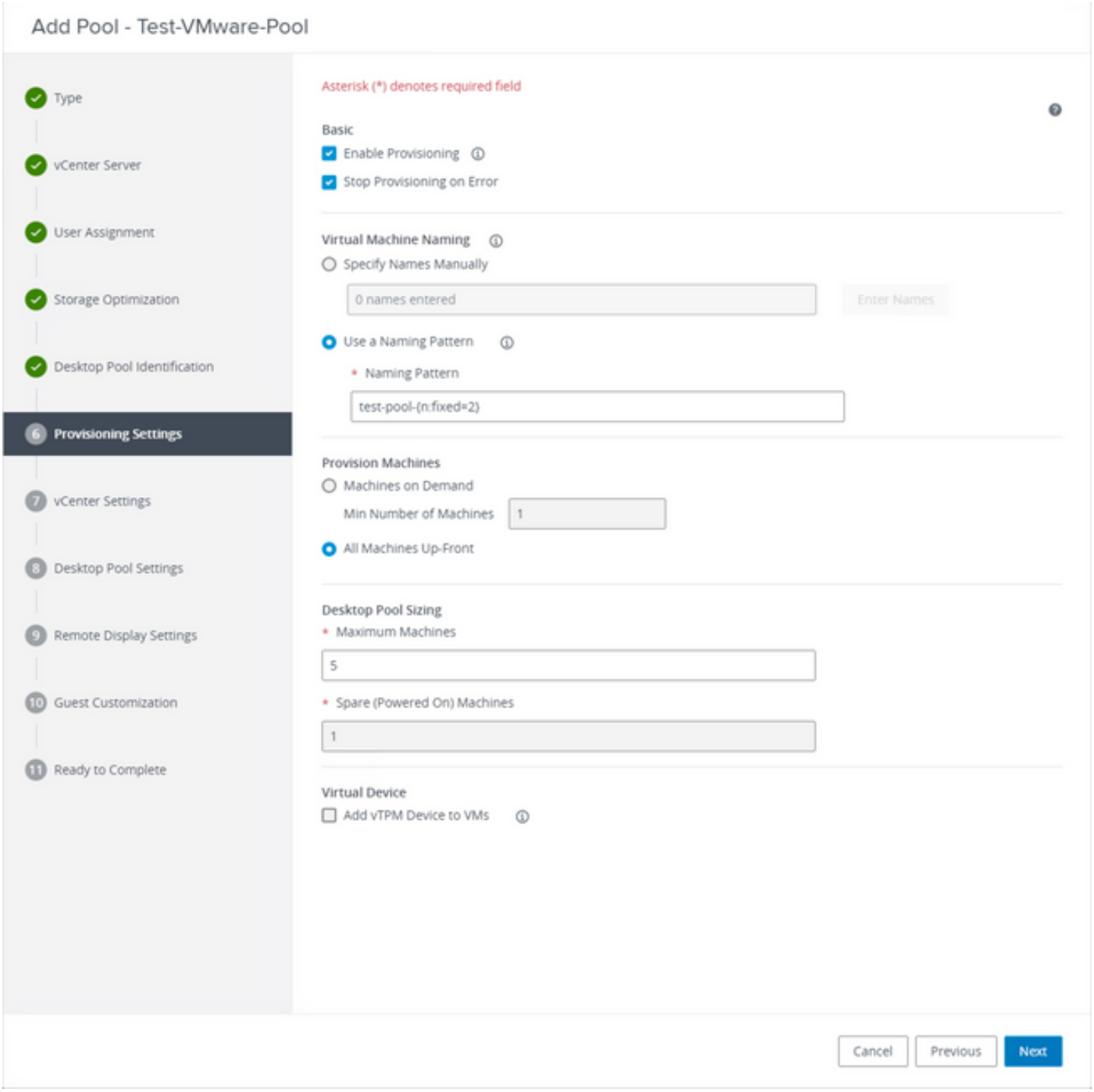
Selezione del tipo "Mobile"

Fare riferimento a: 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



Nomi pool di desktop



Modello di denominazione orizzonte VMware: https://docs.vmware.com/en/VMware-Horizon/2103/virtual-desktops/GUID-26AD6C7D-553A-46CB-B8B3-DA3F6958CD9C.html

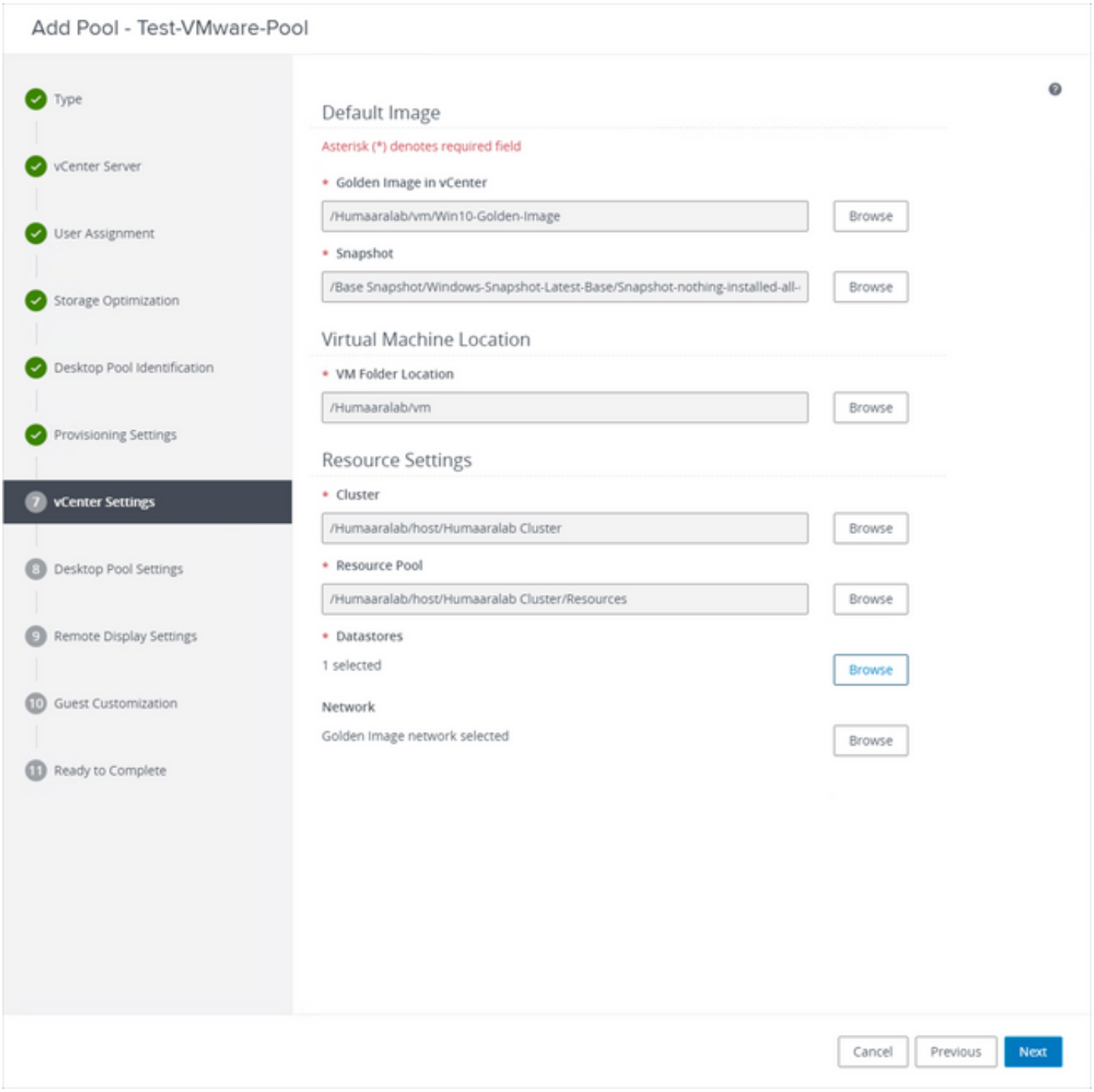
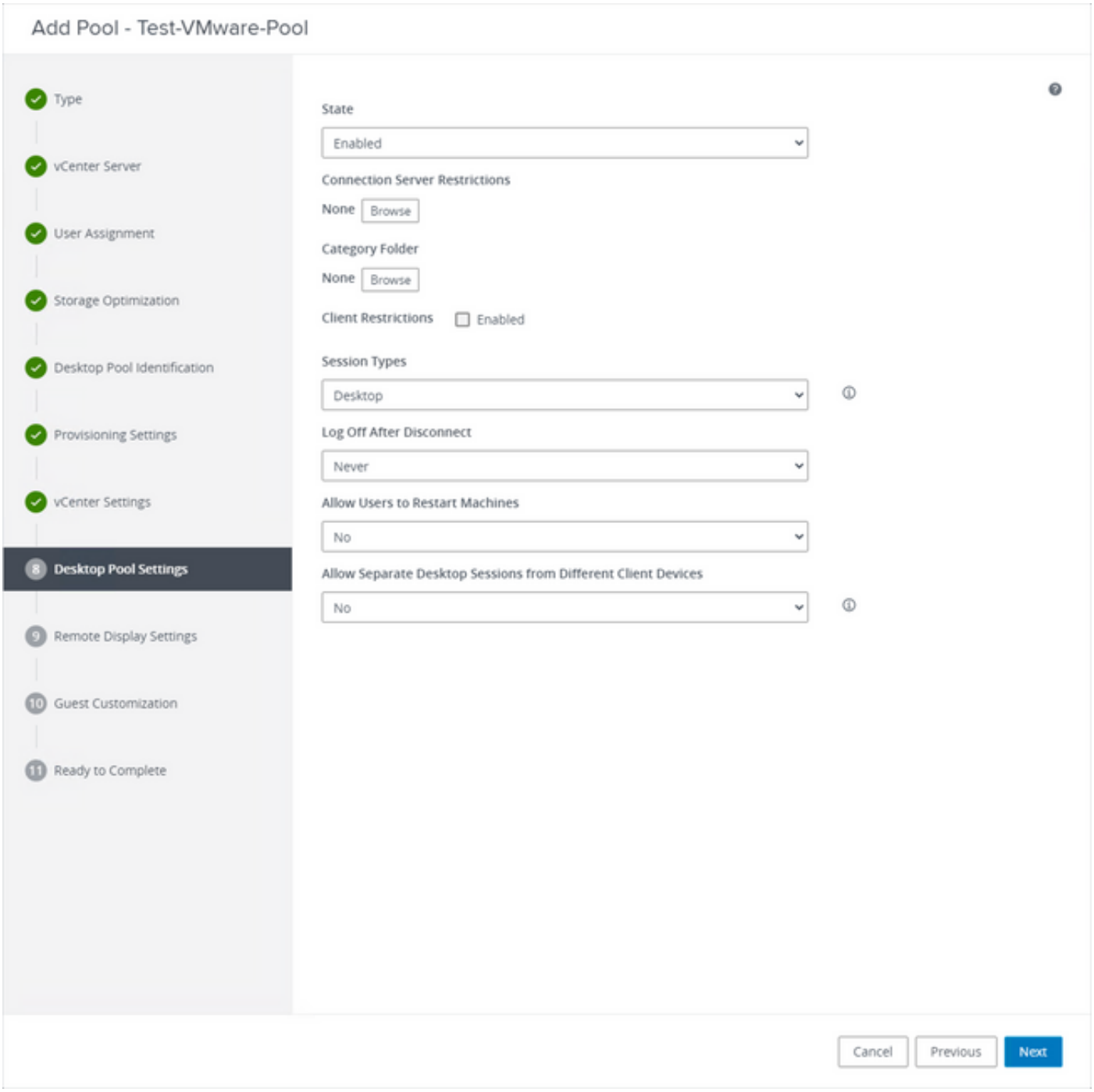
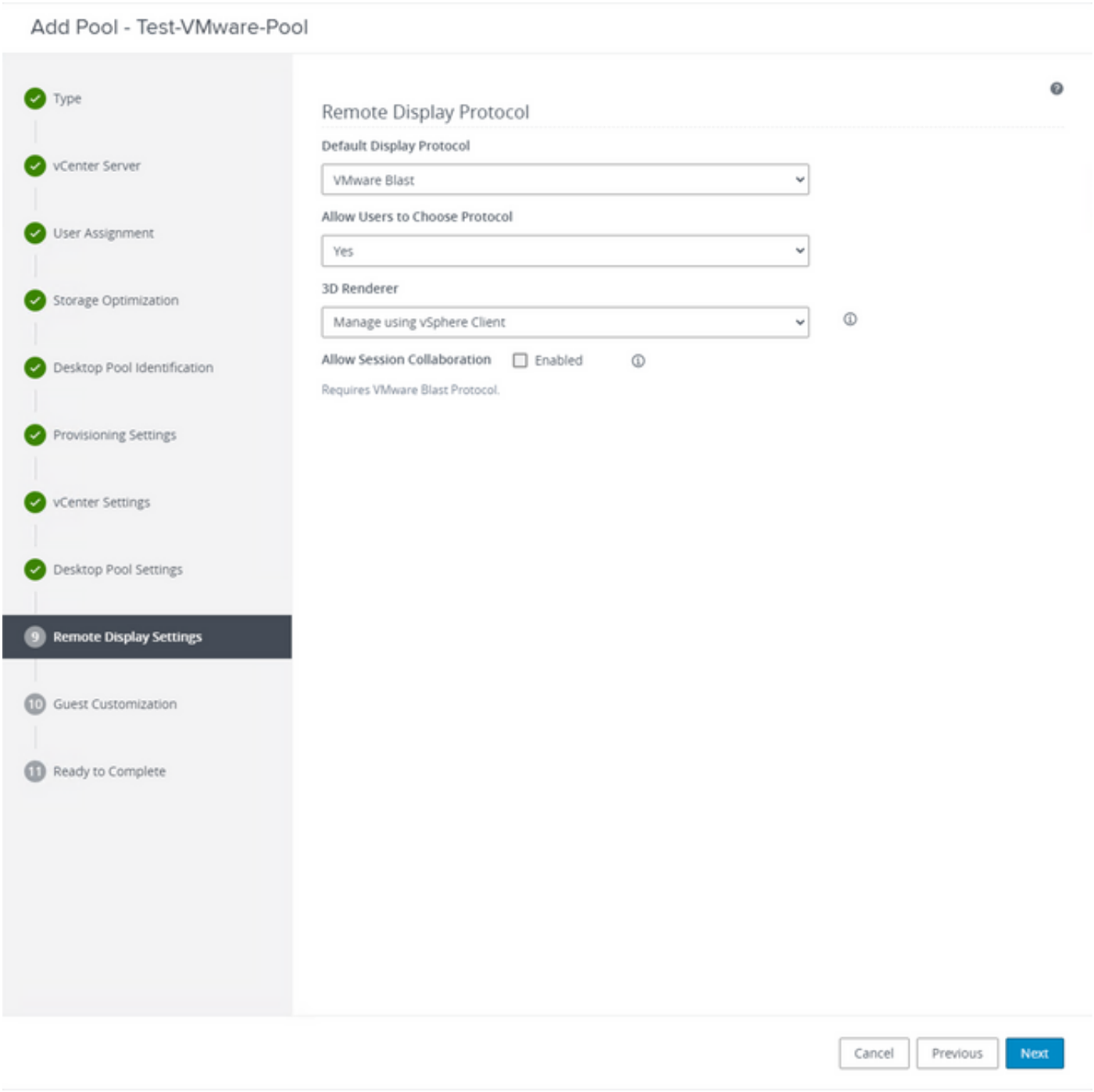
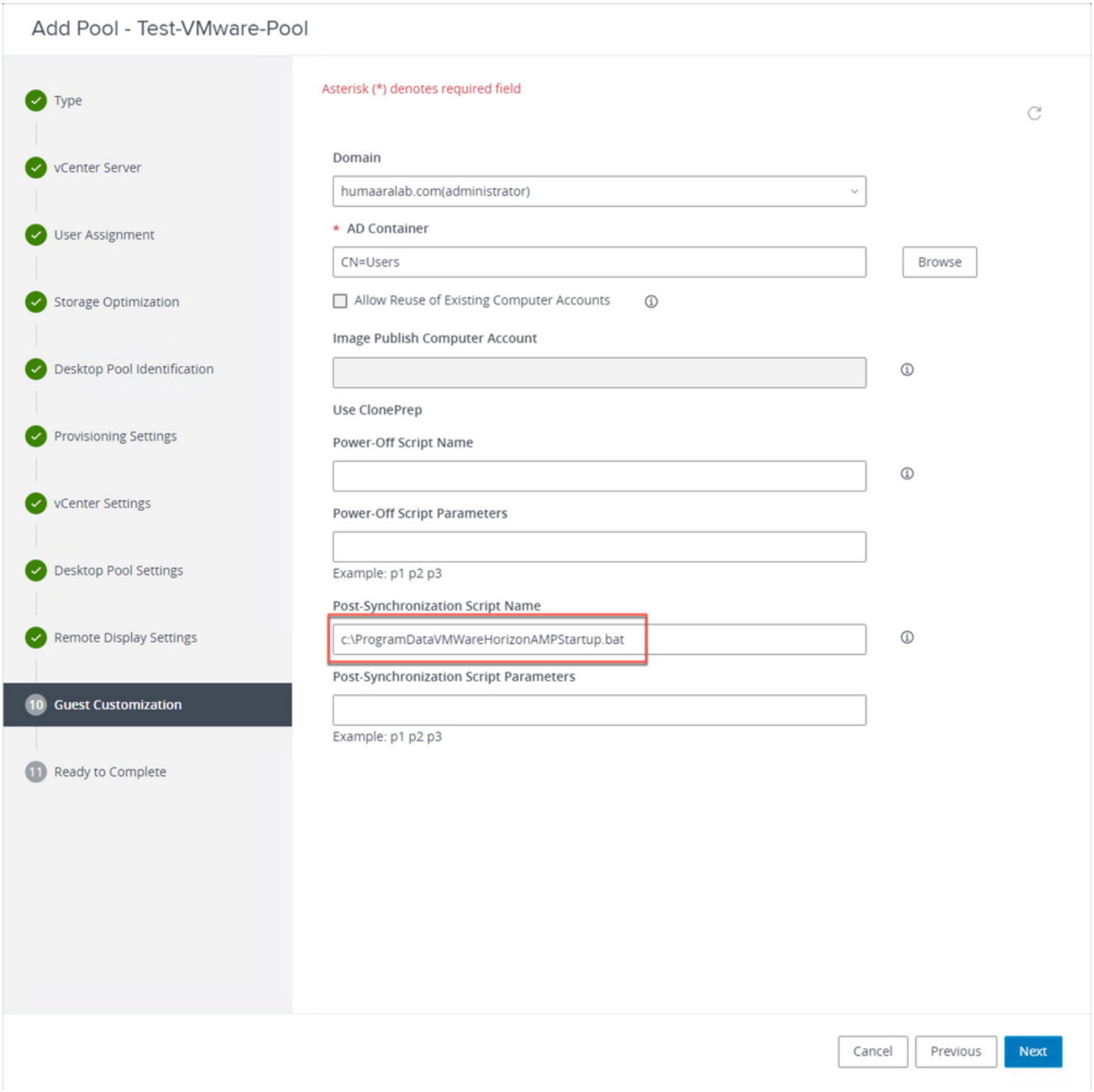


Immagine d'oro: questa è l'immagine d'oro effettiva VM.

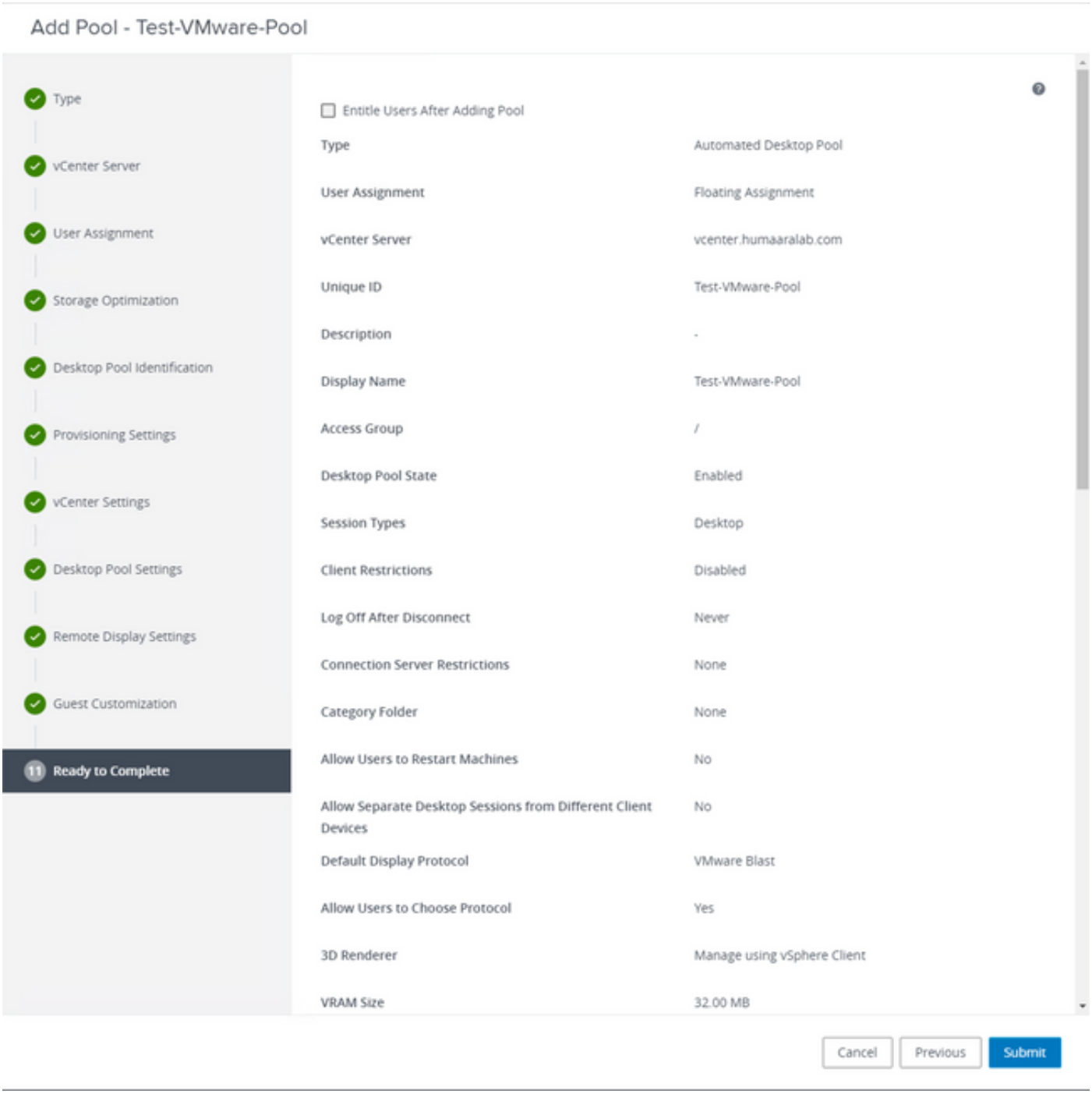
Istantanea: questa è l'immagine che si desidera utilizzare per distribuire la VM figlio. Questo è il valore che viene aggiornato quando si aggiorna l'Immagine d'oro con qualsiasi modifica. Le altre sono alcune delle impostazioni specifiche dell'ambiente VMware.


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. Come accennato in precedenza, il Passaggio 10. nella procedura guidata è il punto in cui è stato impostato il percorso dello script.



8. Una volta completata e inoltrata, VMware Horizon inizia la composizione e le VM figlio vengono create.

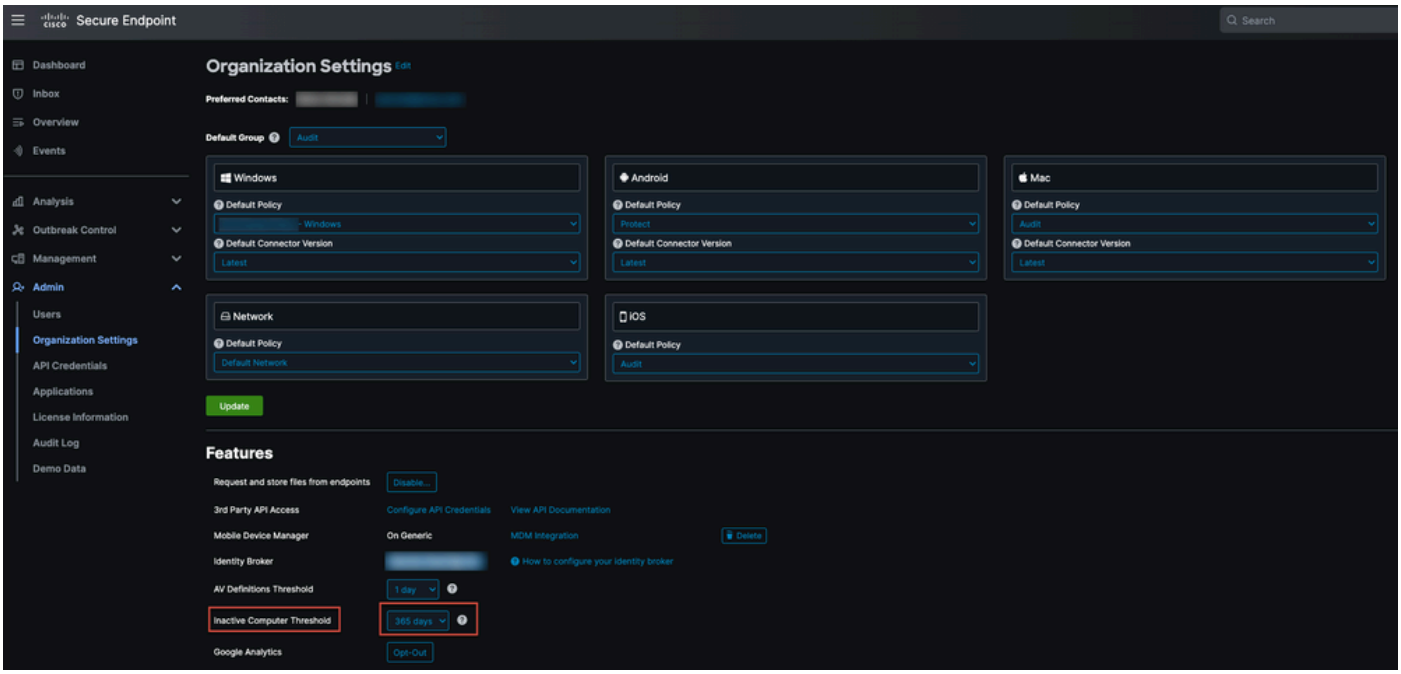
Nota: per informazioni su questi passaggi, consultare la guida di VMware, che tuttavia è di immediata comprensione.

Rimozione di voci duplicate

È possibile rimuovere le voci duplicate del connettore in alcuni modi:

1. Utilizzare la funzione di rimozione automatica sul portale degli endpoint sicuri per rimuovere le voci duplicate (inattive):

Questa impostazione è disponibile in Amministrazione > Impostazioni organizzazione



La Soglia computer inattivo consente di specificare per quanti giorni un connettore può passare senza effettuare il check-in nel cloud Cisco prima di essere rimosso dall'elenco della pagina Gestione computer. L'impostazione predefinita è 90 giorni. I computer inattivi verranno rimossi solo dall'elenco e tutti gli eventi generati rimarranno nell'organizzazione dell'endpoint sicuro. Il computer verrà nuovamente visualizzato nell'elenco se il connettore viene nuovamente archiviato.

2. Utilizzare i workflow di orchestrazione disponibili: https://ciscosecurity.github.io/sxo-05-security-workflows/workflows/secure-endpoint/0056-remove-inactive-endpoints

3. Utilizzare lo script disponibile esternamente per rimuovere gli UUID obsoleti/obsoleti: https://github.com/CiscoSecurity/amp-04-delete-stale-guids

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).