Secure Endpoint su AWS Workspaces - Script di avvio e configurazione per Golden Images

Sommario

Introduzione

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.

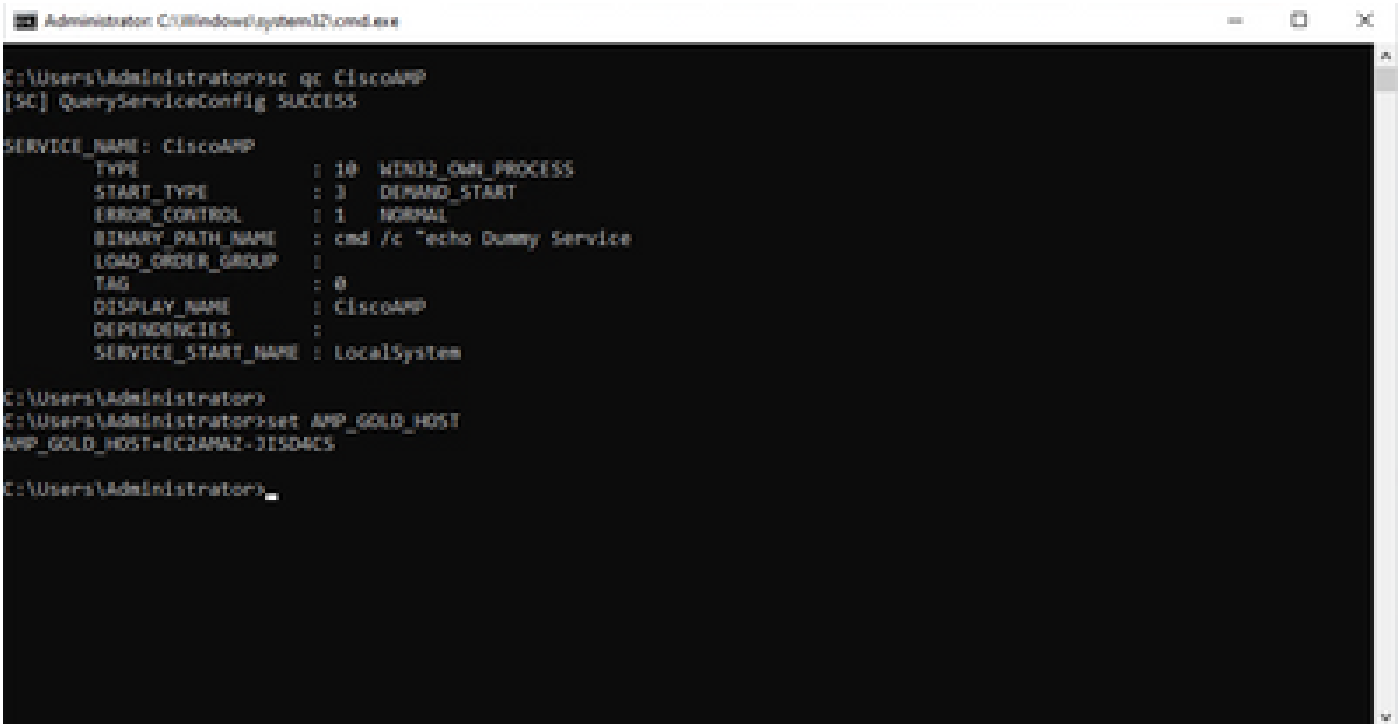
Script di installazione

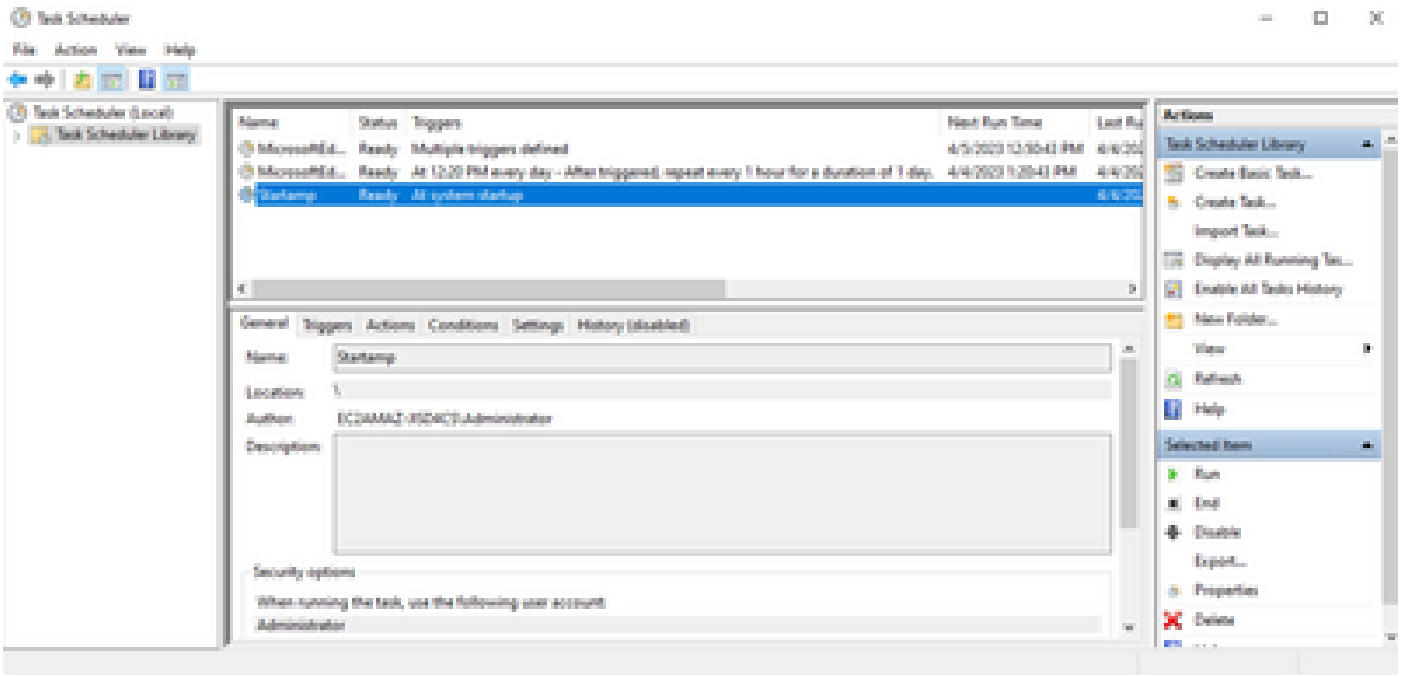
Descrizione script di installazione

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:

- Impostazione dell'avvio manuale del servizio Cisco AMP 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. Questa opzione viene utilizzata dallo script di avvio per verificare se è necessario annullare le modifiche

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 nell'immagine finale, tutte le nuove istanze avranno questa configurazione ed eseguiranno lo script di avvio all'avvio.

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\chmilbur\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

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. AMP continuerà l'esecuzione all'avvio del sistema poiché viene mantenuta l'operazione pianificata.
- 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 AMP su automatico.
  - Avvio del servizio Cisco AMP.
  - Rimozione della variabile di ambiente "AMP_GOLD_HOST".
  - Eliminazione dell'attività pianificata che esegue lo script di avvio ed eliminazione dello script stesso.

Imposta codice script

```
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.

Conclusioni

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, l'AMP di Cisco viene eseguito su tutte le macchine virtuali clonate con la configurazione corretta

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).