Secure Endpoint auf AWS Workspaces - Startup- und Setup-Skripte für Golden Images

Inhalt

Einleitung

Diese Lösung besteht aus einem Setup-Skript, das vor dem Klonen auf dem Golden Image ausgeführt wird, und einem Startup-Skript, das während des Systemstarts auf jedem geklonten virtuellen System ausgeführt wird. Das Hauptziel dieser Skripte besteht darin, die ordnungsgemäße Konfiguration des Services sicherzustellen und gleichzeitig die Anzahl manueller Eingriffe zu reduzieren.

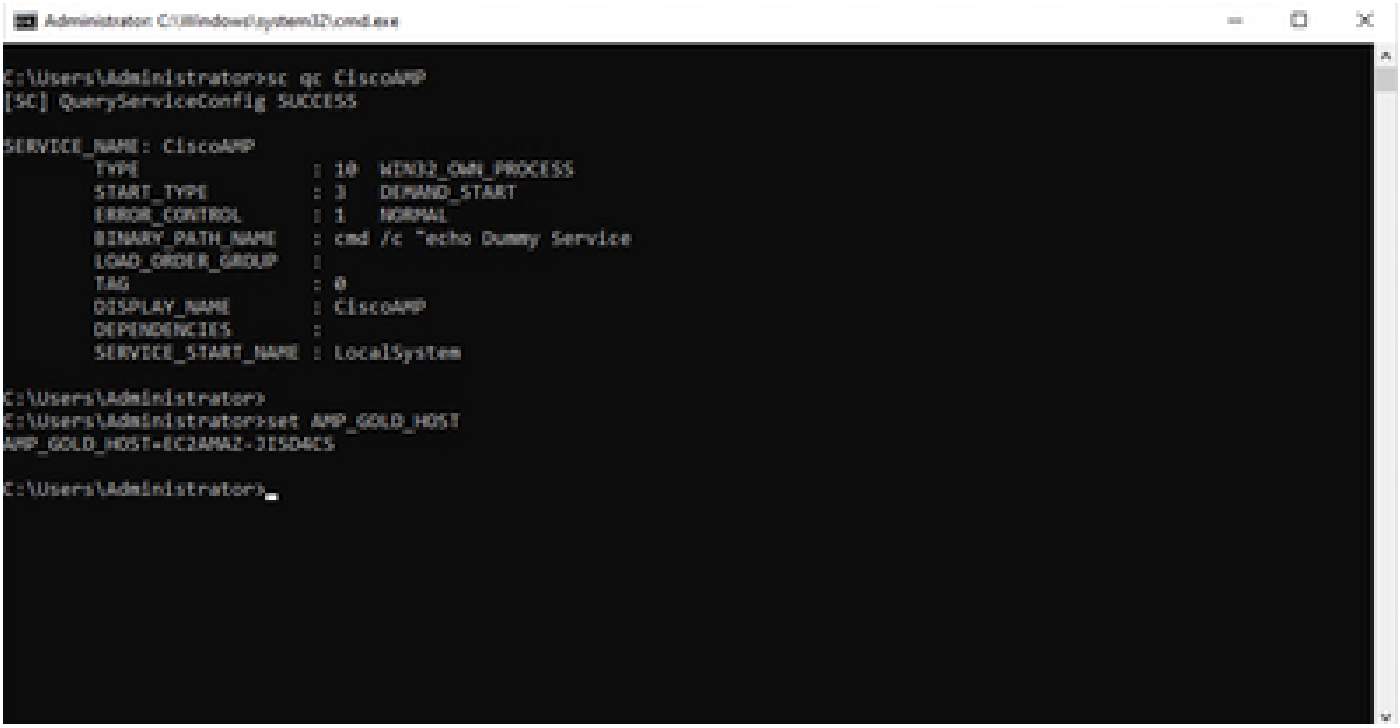
Einrichtungsskript

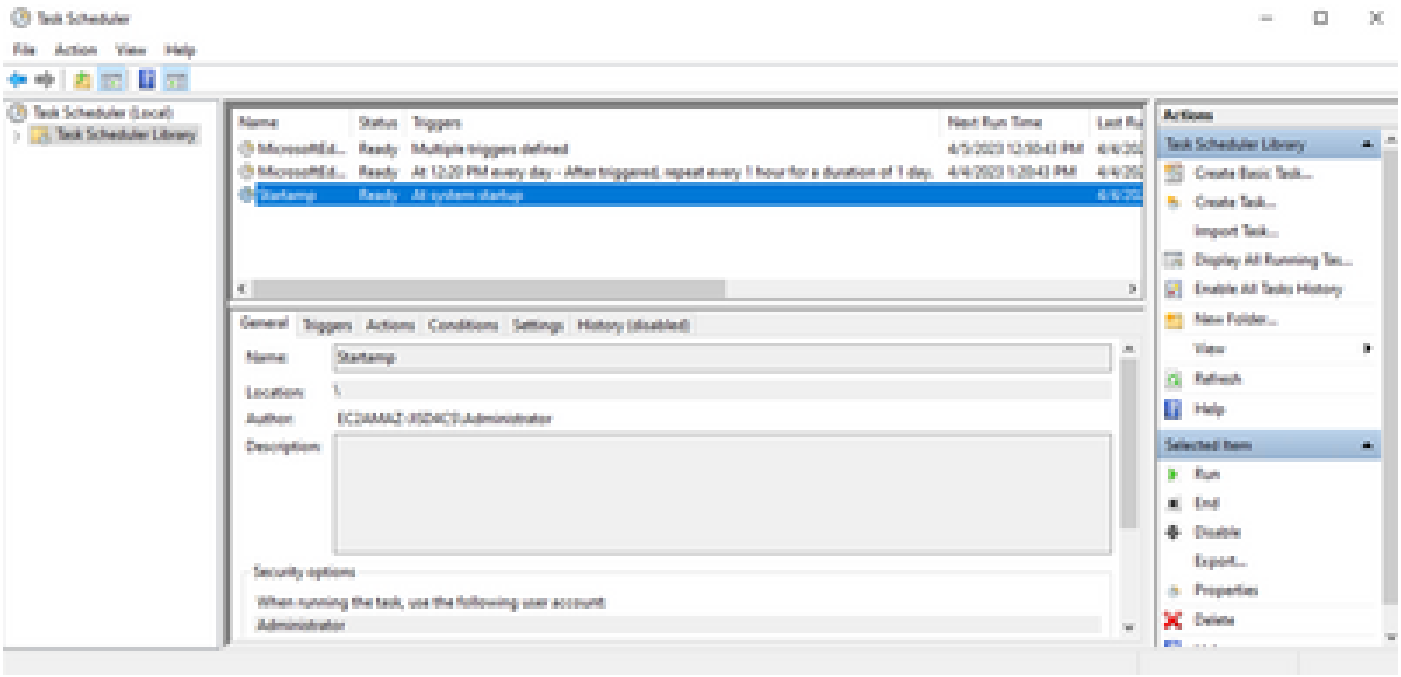
Beschreibung des Einrichtungsskripts

Das erste Skript, 'Setup', wird auf dem Golden Image ausgeführt, bevor es geklont wird. Es muss nur einmal manuell ausgeführt werden. Sein Hauptzweck besteht darin, Anfangskonfigurationen festzulegen, die es dem folgenden Skript ermöglichen, auf den geklonten virtuellen Maschinen ordnungsgemäß zu funktionieren. Diese Konfigurationen umfassen:

- Ändern Sie den Start des Cisco AMP-Dienstes in manuell, um einen automatischen Start zu vermeiden.
- Erstellen einer geplanten Aufgabe, die das folgende Skript (Startup) beim Systemstart mit den höchsten Berechtigungen ausführt
- Erstellen einer Systemumgebungsvariable mit der Bezeichnung "AMP_GOLD_HOST", in der der Hostname des Golden Image gespeichert wird. Das Startup-Skript prüft, ob die Änderungen rückgängig gemacht werden müssen.

Nach der Ausführung des Setup-Skripts können wir überprüfen, ob die Konfigurationsänderungen erfolgreich bereitgestellt wurden.





Da wir diese Aktion im Golden Image durchgeführt haben, haben alle neuen Instanzen diese Konfiguration und führen das Startskript beim Start aus.

Setup-Skriptcode

```
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
```

Der Setup-Skriptcode ist recht einfach:

Zeile 2: Ändert den Starttyp des Malware-Schutzdienstes in "Manuell".

Zeile 5: Erstellt eine neue Umgebungsvariable mit dem Namen "AMP_GOLD_HOST" und speichert den Hostnamen des aktuellen Computers darin.

Zeile 9: Erstellt eine geplante Aufgabe mit dem Namen "Startamp", die das angegebene Startskript während des Systemstarts mit den höchsten Berechtigungen ausführt, ohne dass ein Kennwort erforderlich ist.

Startskript

Beschreibung des Startskripts

Das zweite Skript, 'Startup', wird bei jedem Systemstart auf den geklonten virtuellen Maschinen ausgeführt. Sein Hauptzweck ist es zu überprüfen, ob der aktuelle Rechner den Hostnamen des 'Golden Image' hat:

- Wenn das aktuelle System das Goldene Bild ist, wird keine Aktion ausgeführt und das Skript wird beendet. AMP wird beim Systemstart weiterhin ausgeführt, da wir den geplanten Task verwalten.
- Wenn der aktuelle Rechner NICHT das 'Goldene' Bild ist, werden die vom ersten Skript vorgenommenen Änderungen zurückgesetzt:
  - Ändern der Startkonfiguration des Cisco AMP-Diensts in "Automatisch"
  - Starten des Cisco AMP-Dienstes
  - Die Umgebungsvariable "AMP_GOLD_HOST" wird entfernt.
  - Löschen der geplanten Aufgabe, die das Startskript ausführt, und Löschen des Skripts selbst.

Setup-Skriptcode

```
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
```

Zeile 2: Vergleicht den aktuellen Hostnamen mit dem gespeicherten "AMP_GOLD_HOST"-Wert; wenn beide identisch sind, springt das Skript zur Bezeichnung "same", andernfalls zur Bezeichnung "notsame".

Zeile 4-6: Wenn das "gleiche" Label erreicht ist, tut das Script nichts, da es immer noch das Goldene Bild ist und geht zum "exit" Label.

Zeile 8-16: Wenn die Bezeichnung "notsame" erreicht ist, führt das Skript die folgenden Aktionen aus:

- Ändert den Starttyp des Malware-Schutzdiensts in "Automatisch".
- Startet den Malware-Schutzdienst.
- Entfernt die Umgebungsvariable "AMP_GOLD_HOST".
- Löscht den geplanten Task "Startamp"

Schlussfolgerung

Diese beiden Skripts ermöglichen den Start des Cisco AMP-Service in geklonten Umgebungen mit virtuellen Systemen. Durch die ordnungsgemäße Konfiguration des Golden Image und die Verwendung der Startskripts wird sichergestellt, dass Cisco AMP auf allen geklonten virtuellen Systemen mit der richtigen Konfiguration ausgeführt wird

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.