AWS Workspaces上的安全終端 — 黃金映像的啟動和設定指令碼

目錄

簡介

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。

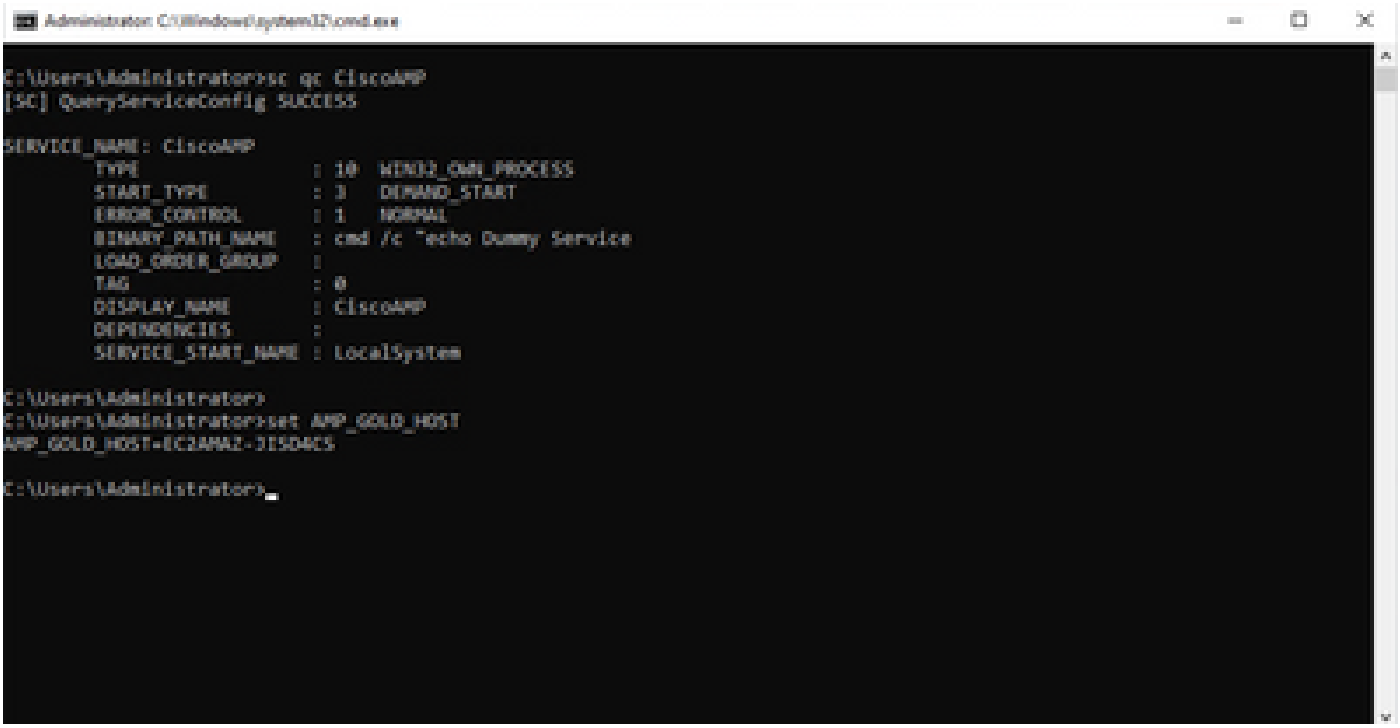
安裝指令碼

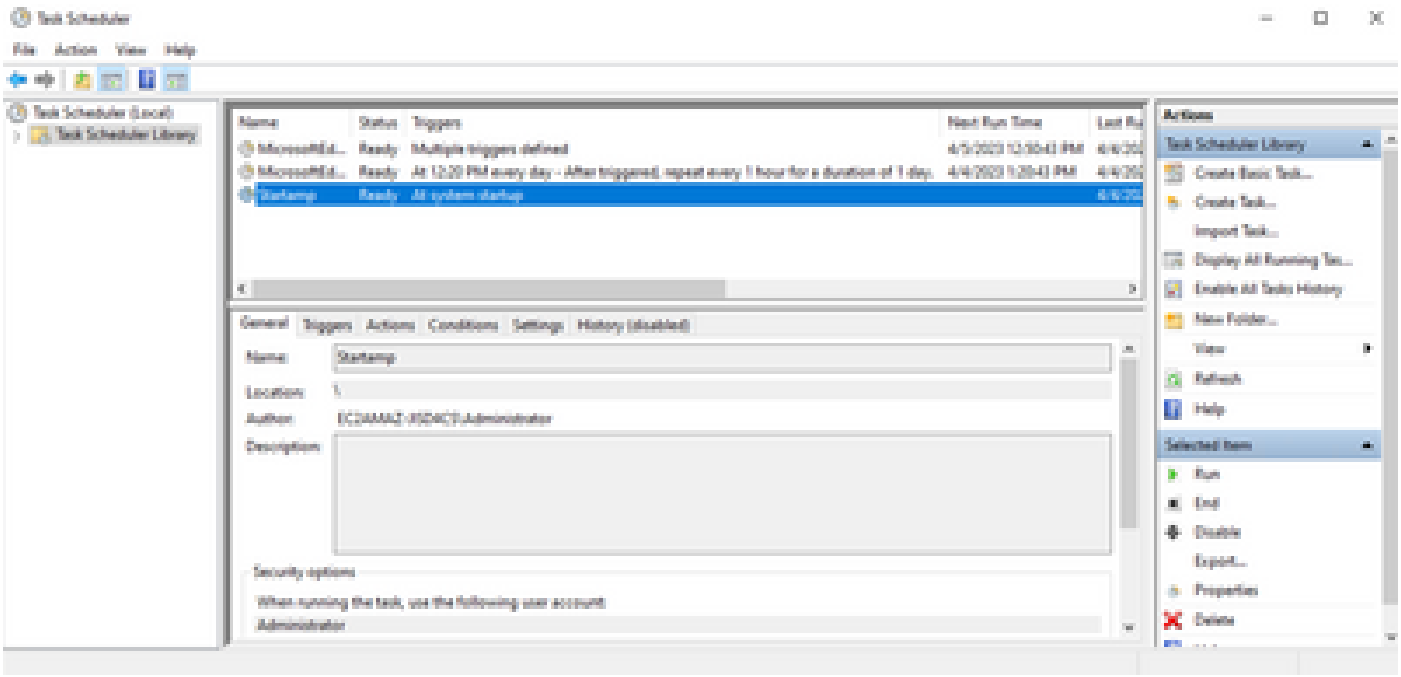
安裝指令碼說明

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Cisco AMP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

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





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

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\chmilbur\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。

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象，則不執行任何操作，指令碼結束。AMP將在系統啟動時繼續運行，因為我們維護了計畫任務。
- 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Cisco AMP服務啟動配置更改為自動。
  - 正在啟動Cisco AMP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。

設定指令碼代碼

```
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，因為它仍是黃金影象，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

結論

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，可以確保Cisco AMP在所有克隆虛擬機器上以正確配置運行

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）。