Secure Endpoint on AWS Workspaces – ゴールデンイメージのスタートアップおよびセットアップスクリプト

内容

はじめに

このソリューションは、クローニング前にゴールデンイメージで実行される「セットアップ」スクリプトと、システムの起動中にクローニングされた各仮想マシンで実行される「スタートアップ」スクリプトで構成されます。これらのスクリプトの主な目的は、手動による介入を減らしながらサービスを適切に設定することです。

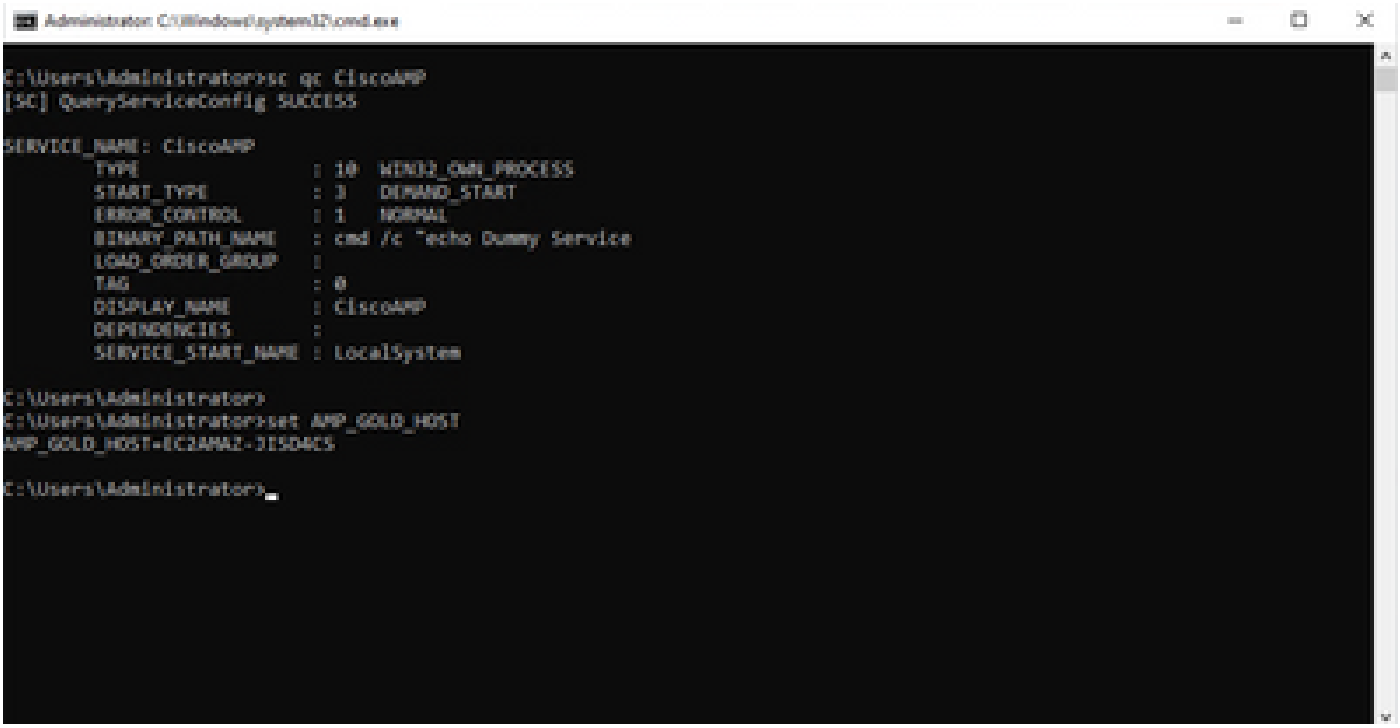
セットアップ スクリプト

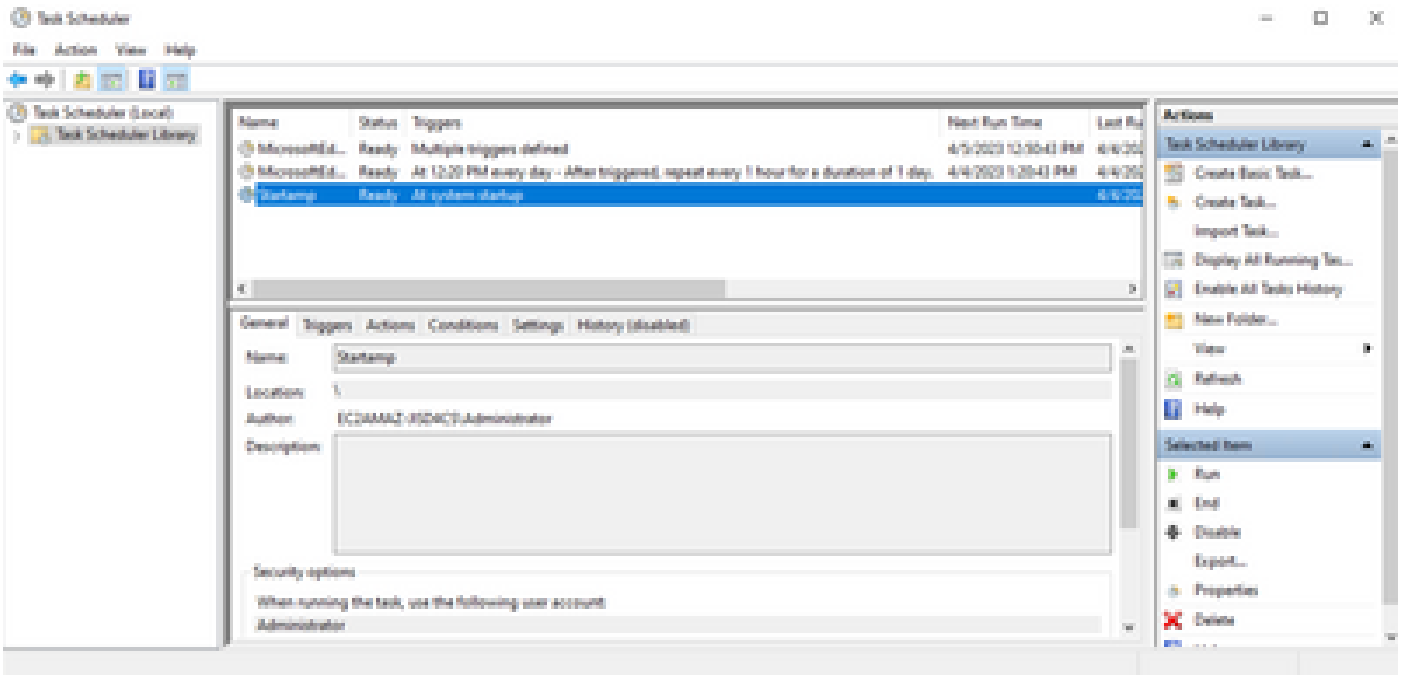
セットアップスクリプトの説明

最初のスクリプト「Setup」は、ゴールデンイメージを複製する前に実行されます。これは1回だけ手動で実行する必要があります。主な目的は、クローンされた仮想マシン上で次のスクリプトが正しく動作するように初期設定を行うことです。設定には次のものがあります。

- Cisco AMPサービスのスタートアップを手動に変更して、自動起動を回避する。
- システムの起動時に、最高の権限で次のスクリプト(Startup)を実行するスケジュールタスクを作成します。
- ゴールデンイメージのホスト名を保存する「AMP_GOLD_HOST」というシステム環境変数を作成します。これは、変更を元に戻す必要があるかどうかを確認するために、スタートアップスクリプトによって使用されます

セットアップスクリプトを実行すると、設定変更が正常に導入されたことを確認できます





ゴールデンイメージでこのアクションを実行したので、すべての新しいインスタンスにこの設定が含まれ、スタートアップ時にスタートアップスクリプトが実行されます。

セットアップスクリプトコード

```
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
```

セットアップスクリプトコードは非常に単純です。

行2:マルウェア防御サービスの起動タイプを手動に変更します。

5行目：「AMP_GOLD_HOST」という新しい環境変数を作成し、現在のコンピュータのホスト名をその環境変数に保存します。

行9:システムの起動時に、パスワードを必要とせずに最高の特権で指定の「Startup」スクリプトを実行する「Startamp」という名前のスケジュールタスクを作成します。

起動スクリプト

起動スクリプトの説明

2番目のスクリプト「Startup」は、クローニングされた仮想マシン上の各システムの起動で実行されます。主な目的は、現在のマシンが「ゴールデンイメージ」のホスト名を持っているかどうかを確認することです。

- 現在のマシンがゴールデンイメージの場合、アクションは実行されず、スクリプトは終了します。スケジュールされたタスクを維持するため、AMPはシステムの起動時に実行を継続します。
- 現在のマシンが「Golden」イメージでない場合、最初のスクリプトによる変更はリセットされます。
  - Cisco AMPサービスのスタートアップ設定を自動に変更します。
  - Cisco AMPサービスを開始しています。
  - 「AMP_GOLD_HOST」環境変数を削除しています。
  - 起動スクリプトを実行するスケジュールされたタスクを削除し、スクリプト自体を削除します。

セットアップスクリプトコード

```
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
```

行2：現在のホスト名と保存されている「AMP_GOLD_HOST」の値を比較します。これらが同じである場合、スクリプトは「same」ラベルにジャンプし、異なる場合は「notsame」ラベルにジャンプします。

行4-6:「same」ラベルに到達すると、スクリプトはゴールデンイメージのままであるため何も行わず、「exit」ラベルに進みます。

行8-16:「notsame」ラベルに到達すると、スクリプトによって次のアクションが実行されます。

- Malware Protectionサービスのスタートアップの種類を自動に変更します。
- マルウェア対策サービスを開始します。
- 環境変数「AMP_GOLD_HOST」を削除します。
- 「Startamp」という名前のスケジュールタスクを削除します。

結論

この2つのスクリプトにより、クローニングされた仮想マシン環境でCisco AMPサービスを起動できます。ゴールデンイメージを適切に設定し、起動スクリプトを使用することで、Cisco AMPはクローンされたすべての仮想マシン上で正しく設定された状態で動作します

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。