Secure Endpoint sur les espaces de travail AWS - Scripts de démarrage et de configuration pour Golden Images

Table des matières

Introduction

Cette solution se compose d'un script de configuration exécuté sur l'image d'or avant le clonage et d'un script de démarrage qui s'exécute sur chaque machine virtuelle clonée pendant le démarrage du système. L'objectif principal de ces scripts est de garantir la configuration correcte du service tout en réduisant les interventions manuelles.

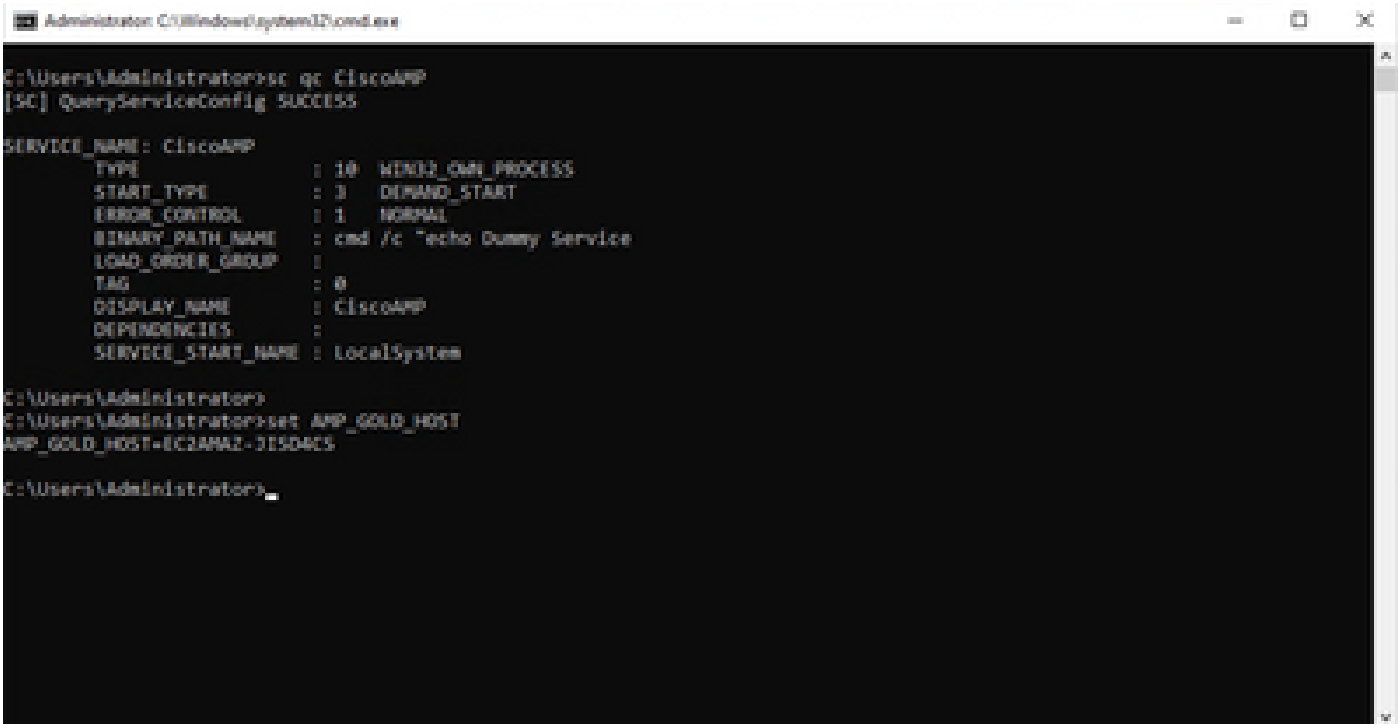
Script de configuration

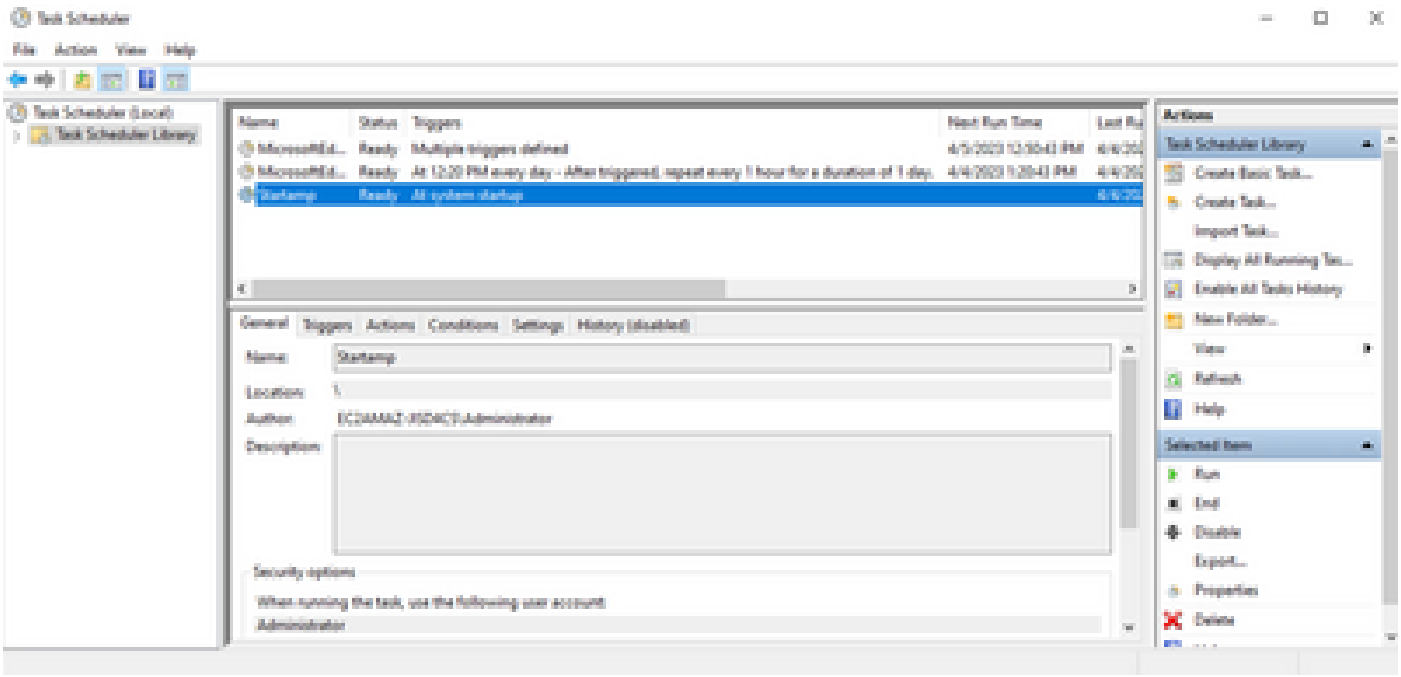
Description du script de configuration

Le premier script, 'Setup', est exécuté sur l'image d'or avant de la cloner. Il doit être exécuté manuellement une seule fois. Son objectif principal est d'établir des configurations initiales qui permettront au script suivant de fonctionner correctement sur les machines virtuelles clonées. Ces configurations incluent :

- Remplacer le démarrage du service Cisco AMP par manuel pour éviter le démarrage automatique.
- Créer une tâche planifiée qui exécute le script suivant (Démarrage) au démarrage du système avec les privilèges les plus élevés.
- Création d'une variable d'environnement système appelée « AMP_GOLD_HOST » qui stocke le nom d'hôte de l'image Golden. Il est utilisé par le script de démarrage pour vérifier si nous devons annuler les modifications

Après avoir exécuté le script de configuration, nous pouvons vérifier que les modifications de configuration ont été correctement déployées





Puisque nous avons effectué cette action dans l'image dorée, toutes les nouvelles instances auront cette configuration et exécuteront le script de démarrage au démarrage.

Code script de configuration

```
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
```

Le code du script de configuration est assez simple :

Ligne 2 : Modifie le type de démarrage du service de protection contre les programmes malveillants en manuel.

Ligne 5 : Crée une nouvelle variable d'environnement appelée « AMP_GOLD_HOST » et y enregistre le nom d'hôte de l'ordinateur actuel.

Ligne 9 : Crée une tâche planifiée nommée « Startamp » qui exécute le script « Startup » spécifié au démarrage du système avec les privilèges les plus élevés, sans avoir besoin d'un mot de passe.

Script de démarrage

Description du script de démarrage

Le deuxième script, « Démarrage », s'exécute à chaque démarrage du système sur les machines virtuelles clonées. Son objectif principal est de vérifier si la machine actuelle a le nom d'hôte de l'« image dorée » :

- Si la machine actuelle est l'image d'or, aucune action n'est entreprise et le script se termine. AMP continuera de s'exécuter au démarrage du système puisque nous gérons la tâche planifiée.
- Si la machine actuelle n'est PAS l'image 'Golden', les modifications apportées par le premier script sont réinitialisées :
  - Modification de la configuration de démarrage du service Cisco AMP en automatique.
  - Démarrage du service Cisco AMP.
  - Suppression de la variable d'environnement « AMP_GOLD_HOST ».
  - Suppression de la tâche planifiée qui exécute le script de démarrage et suppression du script lui-même.

Code script de configuration

```
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
```

Ligne 2 : compare le nom d'hôte actuel avec la valeur stockée "AMP_GOLD_HOST" ; s'ils sont identiques, le script passe à la "même" étiquette, sinon, il passe à la "différente" étiquette.

Ligne 4-6 : Lorsque la « même » étiquette est atteinte, le script ne fait rien puisqu'il s'agit toujours de l'image d'or et passe à l'étiquette « exit ».

Ligne 8-16 : si l'étiquette « not same » est atteinte, le script effectue les actions suivantes :

- Modifie le type de démarrage du service de protection contre les programmes malveillants en automatique.
- Démarre le service de protection contre les programmes malveillants.
- Supprime la variable d'environnement « AMP_GOLD_HOST ».
- Supprime la tâche planifiée nommée « Startamp »

Conclusion

Ces deux scripts permettent le démarrage du service Cisco AMP dans les environnements de machines virtuelles clonées. En configurant correctement l'image Golden et en utilisant les scripts de démarrage, Cisco AMP s'exécute sur toutes les machines virtuelles clonées avec la configuration correcte

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.