Secure Endpoint on AWS Workspaces - Scripts de inicio y configuración para Golden Images

Contenido

Introducción

Esta solución consta de un script de 'configuración' ejecutado en la imagen dorada antes de la clonación y un script de 'inicio' que se ejecuta en cada máquina virtual clonada durante el inicio del sistema. El objetivo principal de estos scripts es garantizar la configuración adecuada del servicio al tiempo que se reduce la intervención manual.

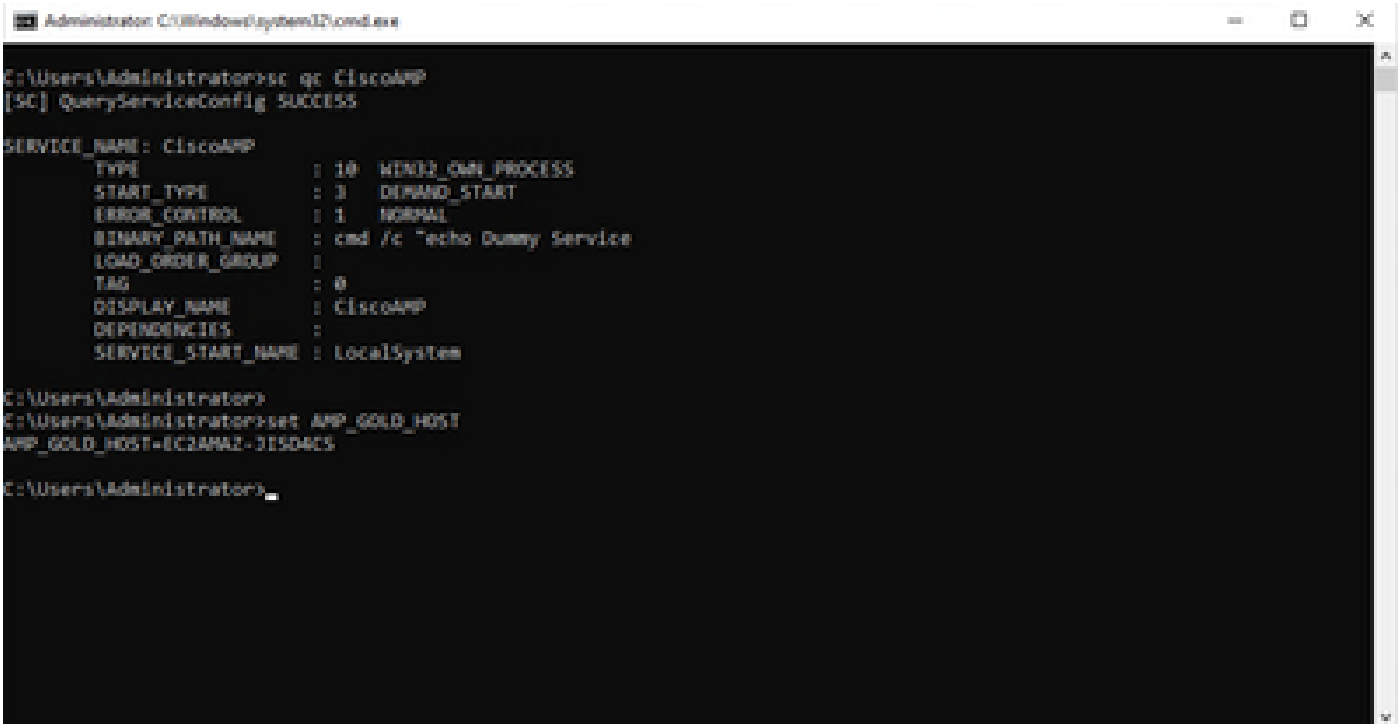
Script de configuración

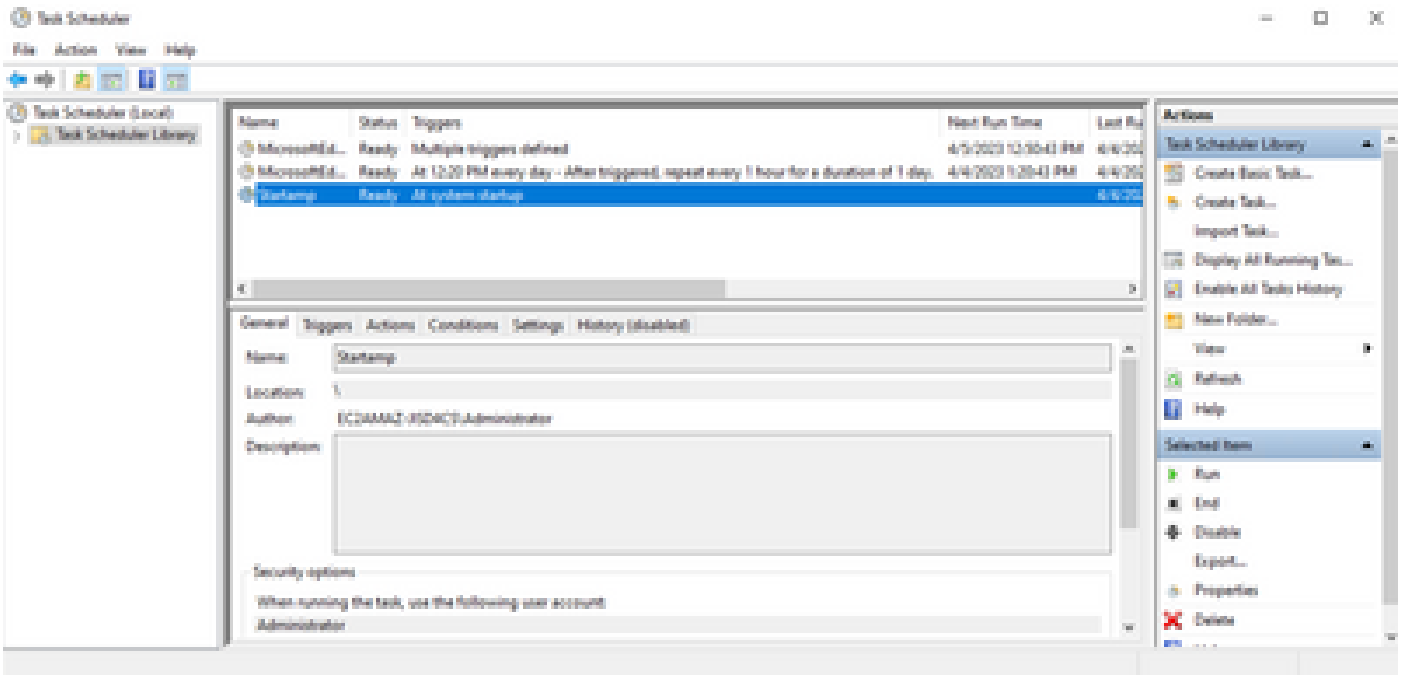
Descripción del script de configuración

El primer script, 'Setup', se ejecuta en la imagen dorada antes de clonarla. Tiene que ser ejecutado manualmente solo una vez. Su objetivo principal es establecer configuraciones iniciales que permitan que el siguiente script funcione correctamente en las máquinas virtuales clonadas. Estas configuraciones incluyen:

- Cambio del inicio del servicio de Cisco AMP a manual para evitar el inicio automático.
- Crear una tarea programada que ejecute el siguiente script (Inicio) al iniciar el sistema con los privilegios más altos.
- Creación de una variable de entorno del sistema denominada "AMP_GOLD_HOST" que almacena el nombre de host de la imagen dorada. El script de inicio lo utilizaría para comprobar si tenemos que revertir los cambios

Después de ejecutar el script de configuración, podemos verificar que los cambios de configuración se hayan implementado correctamente





Dado que realizamos esta acción en la imagen dorada, todas las nuevas instancias tendrán esta configuración y ejecutarán el Script de inicio al inicio.

Código de script de configuración

```
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
```

El código de la secuencia de comandos de configuración es bastante sencillo:

Línea 2: cambia el tipo de inicio del servicio de protección frente a malware a manual.

Línea 5: Crea una nueva variable de entorno denominada "AMP_GOLD_HOST" y guarda en ella el nombre de host del ordenador actual.

Línea 9: Crea una tarea programada denominada "Startamp" que ejecuta la secuencia de comandos 'Startup' especificada durante el inicio del sistema con los privilegios más altos, sin necesidad de una contraseña.

Script de inicio

Descripción del script de inicio

El segundo script, 'Startup', se ejecuta en cada inicio del sistema en las máquinas virtuales clonadas. Su propósito principal es verificar si la máquina actual tiene el nombre de host de la 'Imagen Dorada':

- Si la máquina actual es la imagen dorada, no se realiza ninguna acción y el script finaliza. AMP seguirá ejecutándose al iniciar el sistema, ya que mantenemos la tarea programada.
- Si la máquina actual NO es la imagen 'Golden', se restablecen los cambios realizados por el primer script:
  - Cambio de la configuración de inicio del servicio Cisco AMP a automática.
  - Iniciando el servicio Cisco AMP.
  - Quitando la variable de entorno "AMP_GOLD_HOST".
  - Eliminando la tarea programada que ejecuta la secuencia de inicio y eliminando la propia secuencia de comandos.

Código de script de configuración

```
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
```

Línea 2: compara el nombre de host actual con el valor "AMP_GOLD_HOST" almacenado; si son iguales, el script salta a la etiqueta "same"; de lo contrario, salta a la etiqueta "notsame".

Línea 4-6: Cuando se llega a la etiqueta "same", el script no hace nada, ya que sigue siendo la imagen dorada y procede a la etiqueta "exit".

Línea 8-16: Si se alcanza la etiqueta "notsame", el script realiza las siguientes acciones:

- Cambia el tipo de inicio del servicio de protección frente a malware a automático.
- Inicia el servicio de protección frente a malware.
- Elimina la variable de entorno "AMP_GOLD_HOST".
- Elimina la tarea programada denominada "Startamp"

Conclusión

Estos dos scripts permiten iniciar el servicio Cisco AMP en entornos de máquina virtual clonados. Al configurar correctamente la imagen Golden y utilizar los scripts de inicio, se garantiza que Cisco AMP se ejecute en todas las máquinas virtuales clonadas con la configuración correcta

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).