Endpoint seguro no AWS Workspaces - Scripts de inicialização e configuração para Golden Images

Contents

Introdução

Esta solução consiste em um script 'Setup' executado na Imagem de ouro antes da clonagem e um script 'Startup' executado em cada máquina virtual clonada durante a inicialização do sistema. O principal objetivo desses scripts é garantir a configuração adequada do serviço e, ao mesmo tempo, reduzir a intervenção manual.

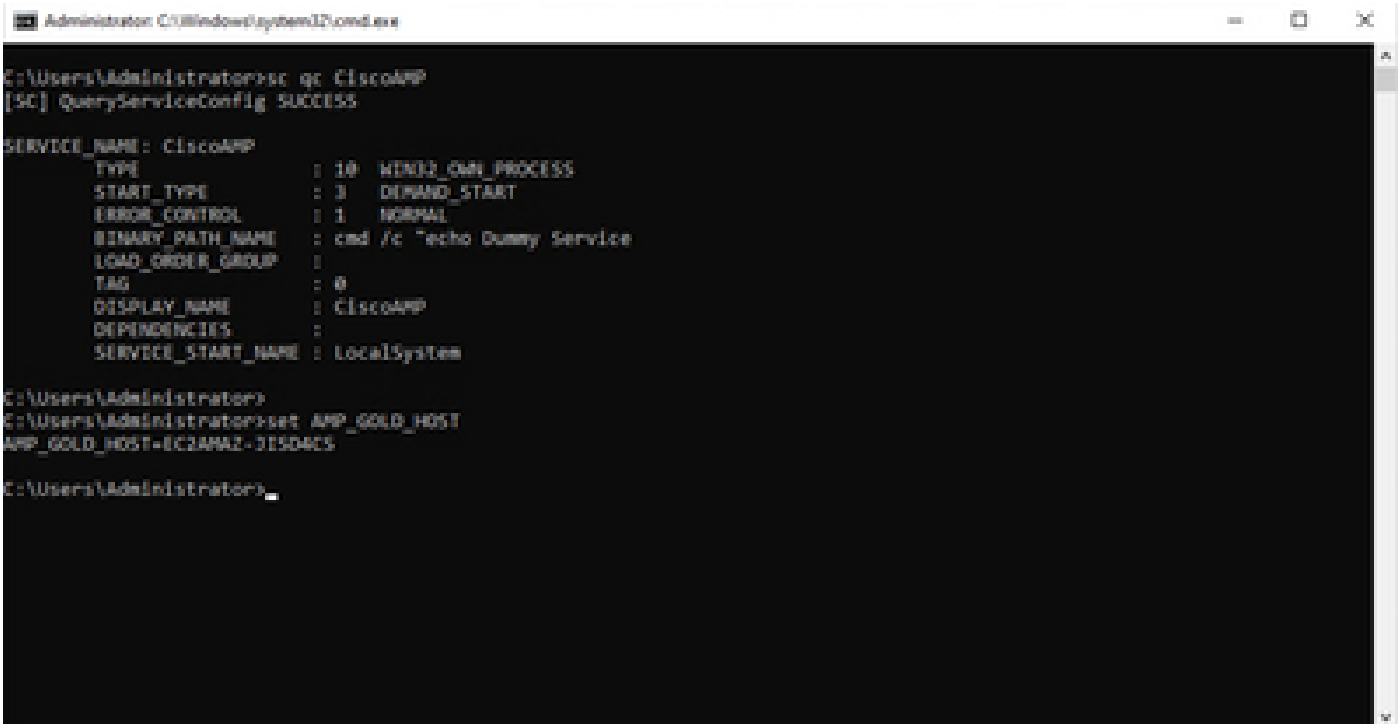
Script de configuração

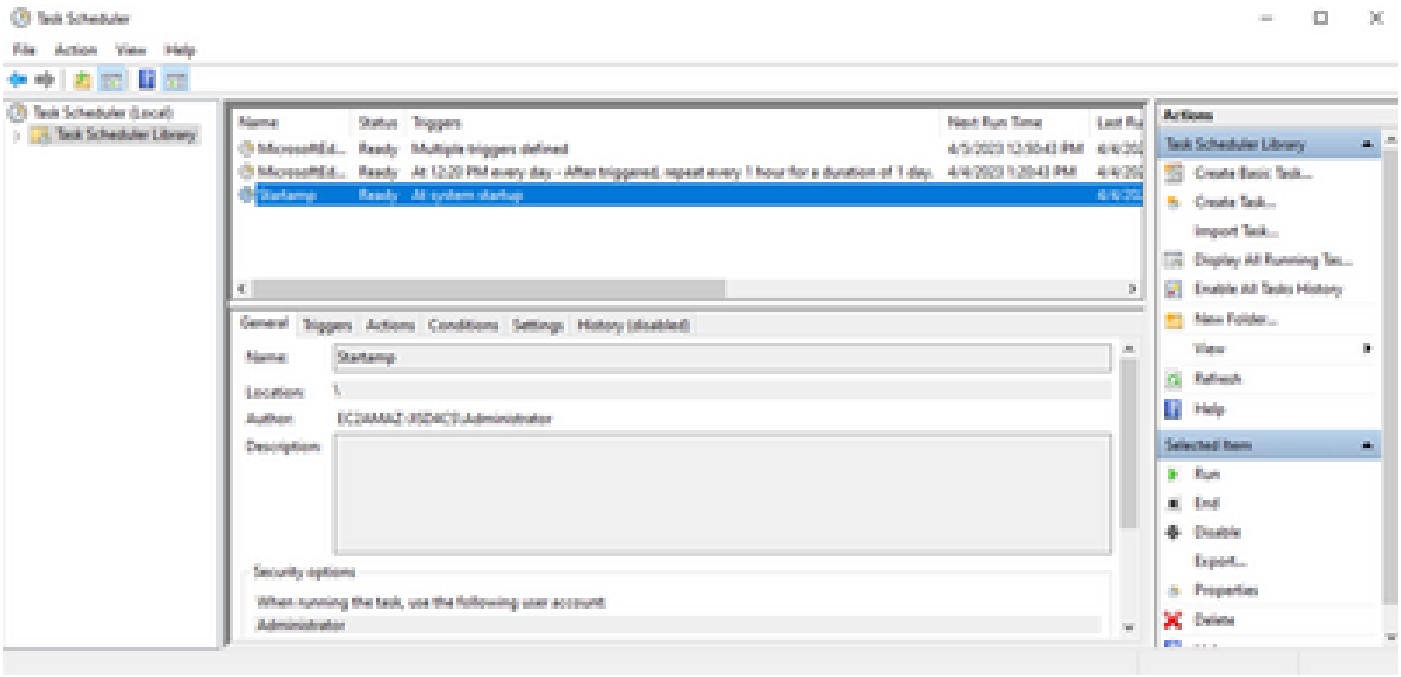
Descrição do script de instalação

O primeiro script, 'Setup', é executado na Imagem Dourada antes de ser clonado. Ele deve ser executado manualmente apenas uma vez. Seu principal objetivo é estabelecer configurações iniciais que permitirão que o seguinte script funcione corretamente nas máquinas virtuais clonadas. Essas configurações incluem:

- Alterar a inicialização do serviço Cisco AMP para manual para evitar a inicialização automática.
- Criando uma tarefa agendada que executa o seguinte script (Inicialização) na inicialização do sistema com os privilégios mais altos.
- Criar uma variável de ambiente de sistema chamada "AMP_GOLD_HOST" que armazena o nome de host da Golden Image. Isso seria usado pelo script de inicialização para verificar se temos que reverter as alterações

Após executar o script de instalação, podemos verificar se as alterações de configuração foram implantadas com êxito





Como executamos essa ação na imagem de ouro, todas as novas ocorrências terão essa configuração e executarão o script de inicialização na inicialização.

Configurar código de script

```
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
```

O código do script de instalação é bastante simples:

Linha 2: Altera o tipo de inicialização do serviço de proteção contra malware para manual.

Linha 5: Cria uma nova variável de ambiente chamada "AMP_GOLD_HOST" e salva o nome de host do computador atual nela.

Linha 9: Cria uma tarefa programada denominada "Startamp" que executa o script 'Startup' especificado durante a inicialização do sistema com os privilégios mais altos, sem precisar de uma senha.

Script de inicialização

Descrição do script de inicialização

O segundo script, 'Startup', é executado em cada inicialização do sistema nas máquinas virtuais clonadas. Seu principal objetivo é verificar se a máquina atual tem o nome de host da 'Imagem Dourada':

- Se a máquina atual for a imagem dourada, nenhuma ação será tomada e o script será encerrado. O AMP continuará em execução na inicialização do sistema, pois manteremos a tarefa agendada.
- Se a máquina atual NÃO for a imagem 'Dourada', as alterações feitas pelo primeiro script serão redefinidas:
  - Alterar a configuração de inicialização do serviço Cisco AMP para automática.
  - Iniciando o serviço Cisco AMP.
  - Removendo a variável de ambiente "AMP_GOLD_HOST".
  - Excluindo a tarefa agendada que executa o script de inicialização e excluindo o próprio script.

Configurar código de script

```
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
```

Linha 2: Compara o nome do host atual com o valor armazenado "AMP_GOLD_HOST"; se eles forem iguais, o script salta para o rótulo "mesmo"; caso contrário, ele salta para o rótulo "não igual".

Linha 4-6: Quando o rótulo "mesmo" é alcançado, o script não faz nada, uma vez que ainda é a Imagem Dourada e prossegue para o rótulo "saída".

Linha 8-16: se o rótulo "notsame" for alcançado, o script executa as seguintes ações:

- Altera o tipo de inicialização do serviço de proteção contra malware para automático.
- Inicia o serviço de proteção contra malware.
- Remove a variável de ambiente "AMP_GOLD_HOST".
- Exclui a tarefa agendada chamada "Carimbo"

Conclusão

Esses dois scripts permitem a inicialização do serviço Cisco AMP em ambientes de máquina virtual clonados. Ao configurar corretamente a imagem Golden e usar os scripts de inicialização, ele garante que o Cisco AMP seja executado em todas as máquinas virtuais clonadas com a configuração correta

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.