AWS工作空间上的安全终端 — 黄金映像的启动和设置脚本

目录

简介

此解决方案包括克隆之前在金牌映像上执行的“设置”脚本和在系统启动期间在每个克隆虚拟机上运行的“启动”脚本。这些脚本的主要目标是确保正确配置服务，同时减少手动干预。

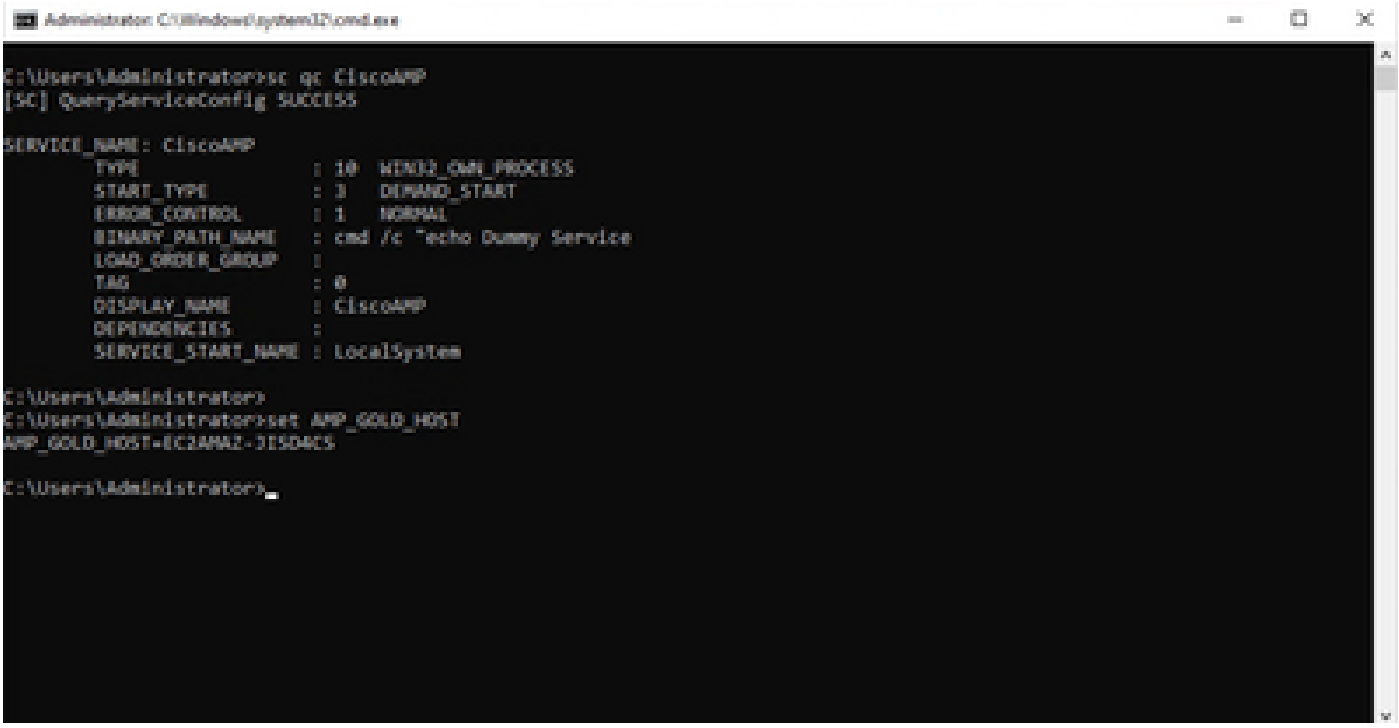
设置脚本

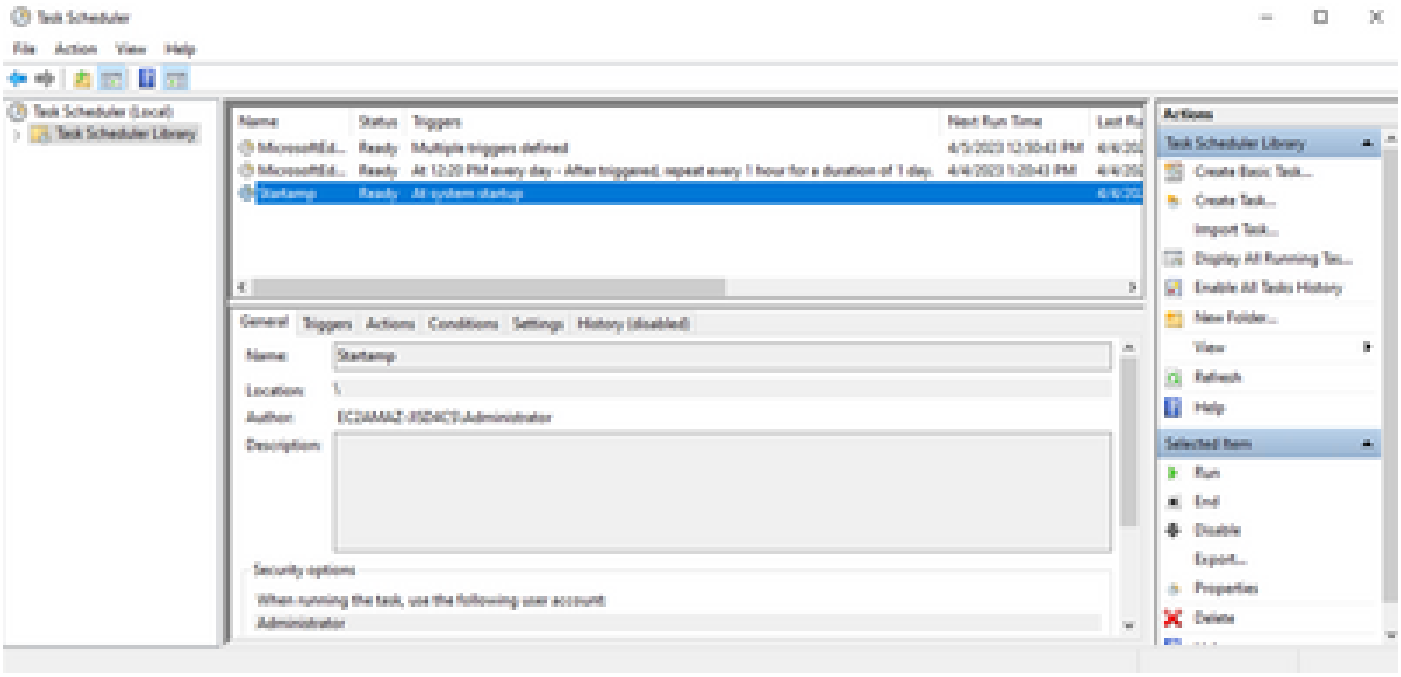
安装脚本说明

第一个脚本“设置”在克隆黄金映像之前在黄金映像上执行。只需手动执行一次。其主要目的是建立初始配置，以允许以下脚本在克隆虚拟机上正确运行。这些配置包括：

- 将Cisco AMP服务启动更改为手动以避免自动启动。
- 创建在系统启动时以最高权限执行以下脚本（启动）的计划任务。
- 创建名为“AMP_GOLD_HOST”的系统环境变量，以存储Golden Image的主机名。启动脚本将使用此命令来验证我们是否必须恢复更改

执行设置脚本后，我们可以验证配置更改已成功部署





由于我们是在金色映像中执行此操作的，因此所有新实例都将具有此配置，并将在启动时执行启动脚本。

设置脚本代码

```
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
```

安装脚本代码非常简单：

第2行：将恶意软件防护服务的启动类型更改为手动。

第5行：创建名为“AMP_GOLD_HOST”的新环境变量，并在其中保存当前计算机的主机名。

第9行：创建名为“Startamp”的计划任务，该任务在系统启动期间以最高权限运行指定的“Startup”脚本，无需密码。

启动脚本

启动脚本说明

第二个脚本“启动”在克隆虚拟机的每个系统启动上运行。其主要目的是检查当前计算机是否具有“Golden Image”的主机名：

- 如果当前计算机是黄金映像，则不执行任何操作，脚本将结束。AMP将在系统启动时继续运行，因为我们维护了计划任务。
- 如果当前计算机不是“Golden”映像，则会重置第一个脚本所做的更改：
  - 将Cisco AMP服务启动配置更改为自动。
  - 正在启动Cisco AMP服务。
  - 删除“AMP_GOLD_HOST”环境变量。
  - 删除执行启动脚本的计划任务，并删除脚本本身。

设置脚本代码

```
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：将当前主机名与存储的“AMP_GOLD_HOST”值进行比较；如果它们相同，则脚本跳至“相同”标签，否则跳至“不相同”标签。

第4-6行：当到达“相同”标签时，脚本不会执行任何操作，因为它仍然是“黄金图像”，并继续进入“退出”标签。

第8-16行：如果到达“notsame”标签，脚本将执行以下操作：

- 将恶意软件防护服务的启动类型更改为自动。
- 启动恶意软件防护服务。
- 删除“AMP_GOLD_HOST”环境变量。
- 删除名为“Startamp”的计划任务

结论

这两个脚本允许在克隆虚拟机环境中启动Cisco AMP服务。通过正确配置黄金映像并使用启动脚本，确保Cisco AMP在所有克隆虚拟机上以正确配置运行

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。