

Secure Endpoint on AWS Workspaces - Startup and Setup scripts for Golden Images

Contents

Introduction

This solution consists of a 'Setup' script executed on the Golden Image prior to cloning and a 'Startup' script that runs on each cloned virtual machine during system startup. The primary objective of these scripts is to ensure the proper configuration of the service while reducing manual intervention.

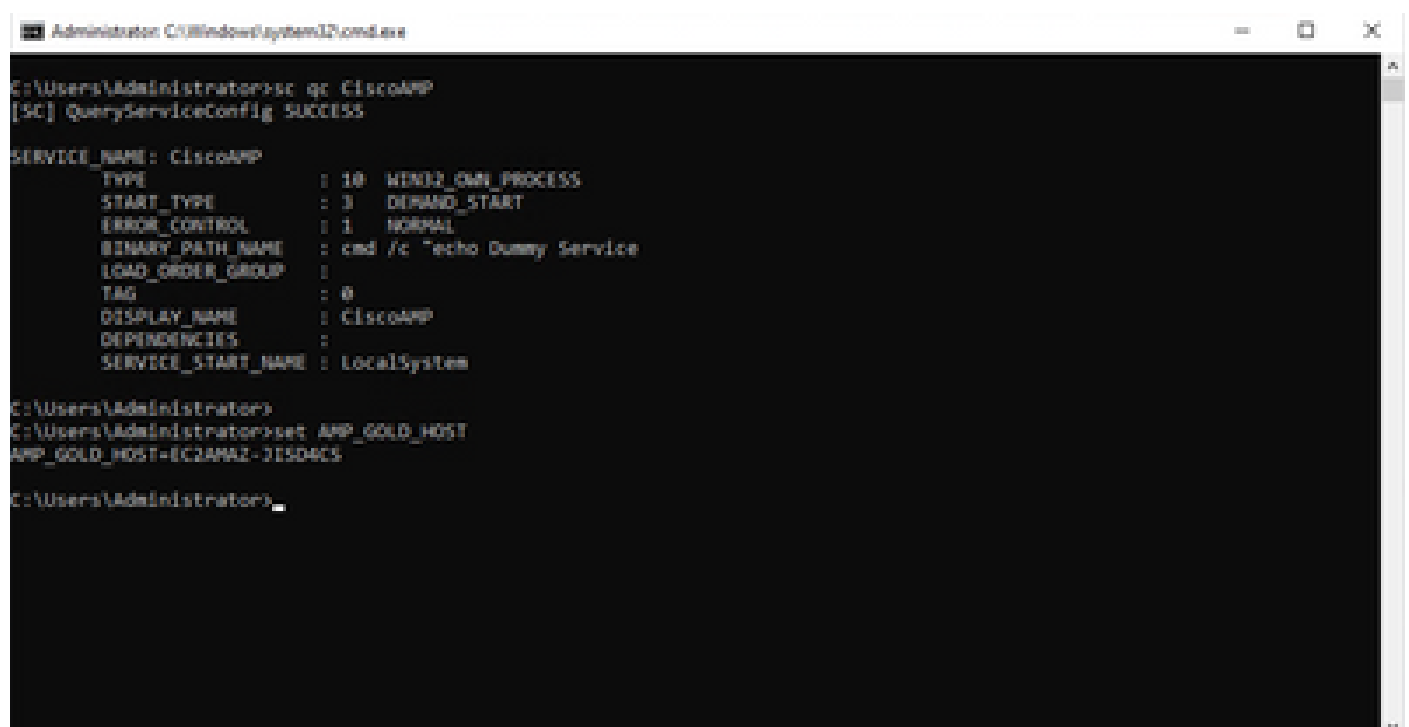
Setup Script

Setup Script Description

The first script, 'Setup', is executed on the Golden Image before cloning it. It has to be manually executed just **one time**. Its main purpose is to establish initial configurations that will allow the following script to function correctly on the cloned virtual machines. These configurations include:

- Changing the Cisco AMP service startup to manual to avoid auto-start.
- Creating a scheduled task that executes the following script (Startup) at system startup with highest privileges.
- Creating a system environment variable called "AMP_GOLD_HOST" that stores the hostname of the Golden Image. That would be use by the Startup script to verify if we have to revert the changes

After execute the Setup Script we can verify that the configuration changes has been succesfully deployed

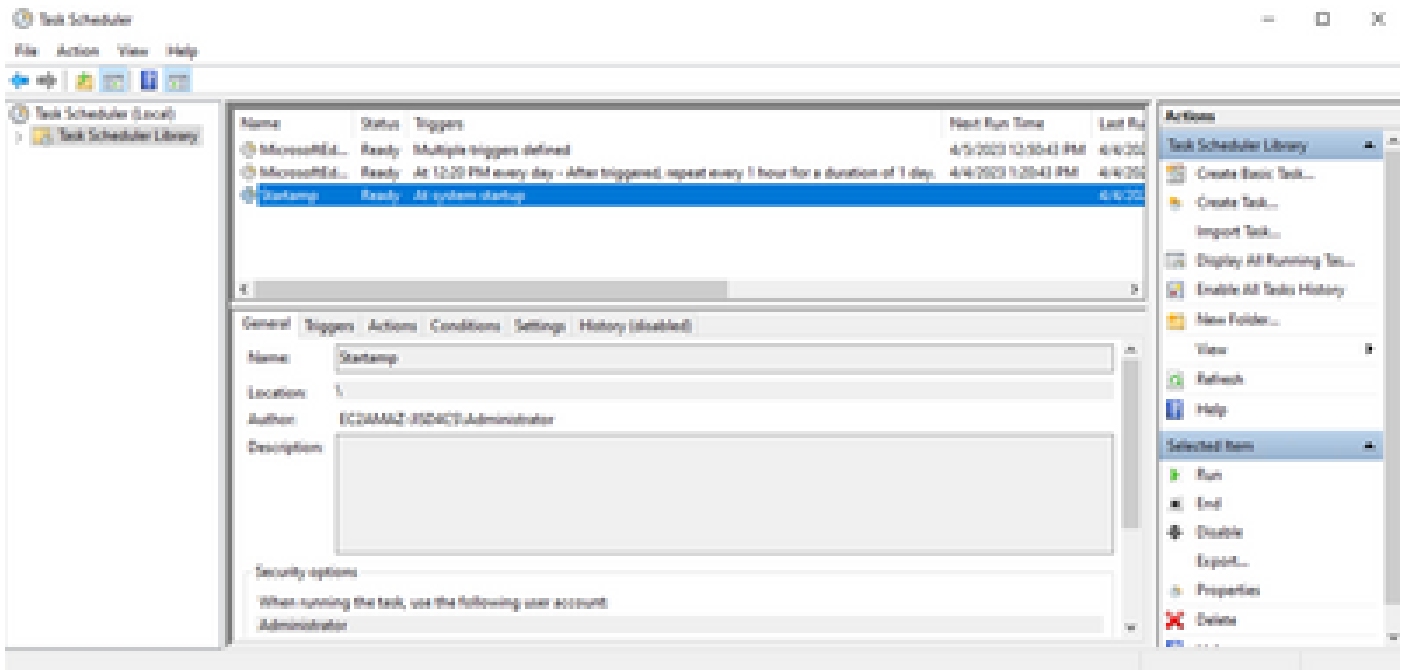


```
Administrator C:\Windows\system32\cmd.exe
C:\Users\Administrator>sc qc CiscoAMP
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: CiscoAMP
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 3   DEMAND_START
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : cmd /c "echo Dummy Service"
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : CiscoAMP
        DEPENDENCIES        :
        SERVICE_START_NAME  : LocalSystem

C:\Users\Administrator>
C:\Users\Administrator>set AMP_GOLD_HOST
AMP_GOLD_HOST=EC2AMAZ-31504CS

C:\Users\Administrator>
```



Since we performed this action in the golden image all the new instances will have this configuration and will execute the Startup Script at startup.

Setup script code

```
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
```

The Setup script code is quite straightforward:

Line 2: Changes the startup type of the malware protection service to manual.

Line 5: Creates a new environment variable called "AMP_GOLD_HOST" and saves the current computer's hostname in it.

Line 9: Creates a scheduled task named "Startamp" that runs the specified 'Startup' script during system startup with the highest privileges, without needing a password.

Startup Script

Startup Script Description

The second script, 'Startup', runs on each system startup on the cloned virtual machines. Its main purpose is

to check if the current machine has the hostname of the 'Golden Image':

- If the current machine is the Golden image, no action is taken and the script ends. AMP will continue running at system startup since we maintain the scheduled task.
- If the current machine is NOT the 'Golden' image, the changes made by the first script are reset:
 - Changing the Cisco AMP service startup configuration to automatic.
 - Starting the Cisco AMP service.
 - Removing the "AMP_GOLD_HOST" environment variable.
 - Deleting the scheduled task that executes the startup script and deleting the script itself.

Setup script code

```
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
```

Line 2: Compares the current hostname with the stored "AMP_GOLD_HOST" value; if they are the same, the script jumps to the "same" label, otherwise, it jumps to the "notsame" label.

Line 4-6: When the "same" label is reached, the script does nothing since it is still the Golden Image and proceeds to the "exit" label.

Line 8-16: If the "notsame" label is reached, the script performs the following actions:

- Changes the startup type of the malware protection service to automatic.
- Starts the malware protection service.
- Removes the "AMP_GOLD_HOST" environment variable.
- Deletes the scheduled task named "Startamp"

Conclusion

These two scripts allow the Cisco AMP service startup in cloned virtual machine environments. By properly configuring the Golden image and using the startup scripts, it ensures that the Cisco AMP runs on all cloned

virtual machines with the correct configuration