Secure Endpoint op AWS-werkruimten - Opstartscripts en Setup-scripts voor Golden Images

Inhoud

Inleiding

Deze oplossing bestaat uit een 'Setup' script uitgevoerd op de Golden Image voorafgaand aan het klonen en een 'Startup' script dat draait op elke gekloonde virtuele machine tijdens het opstarten van het systeem. De primaire doelstelling van deze scripts is om de juiste configuratie van de service te verzekeren en tegelijkertijd de handmatige tussenkomst te verminderen.

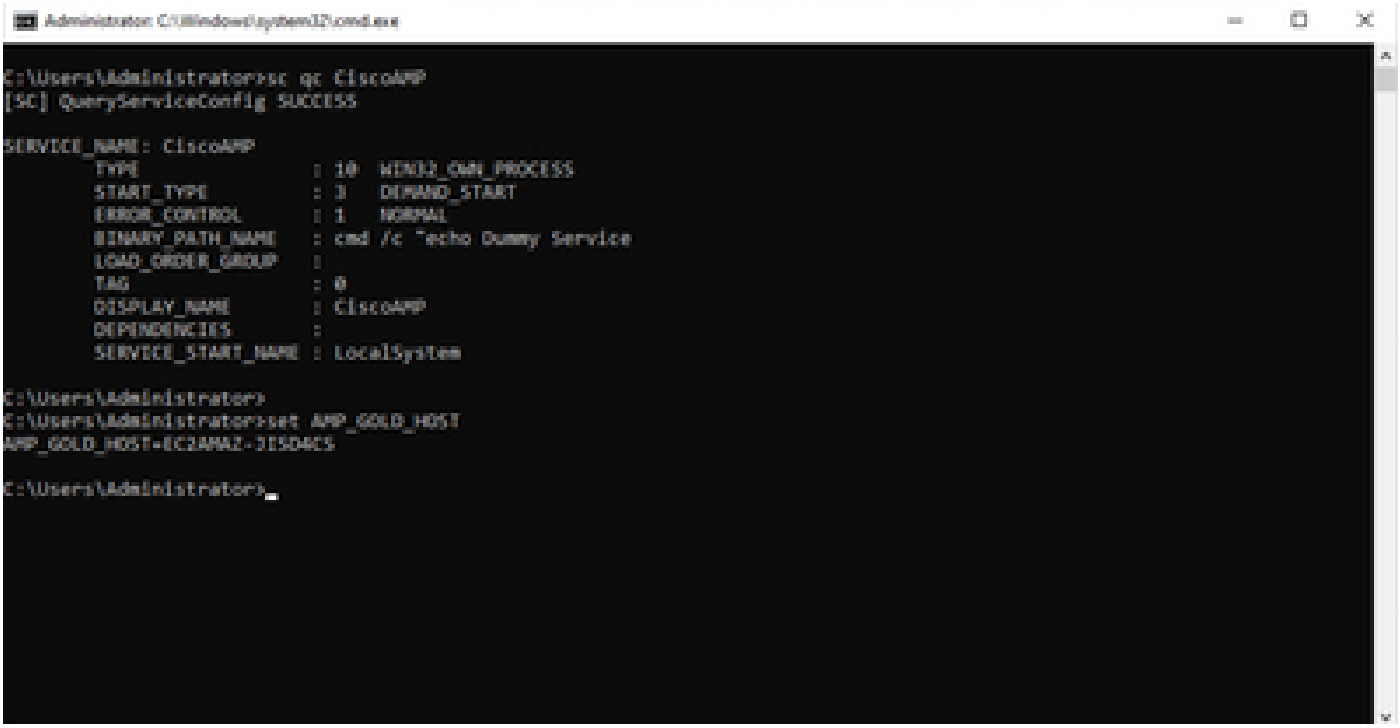
Instellingsscripts

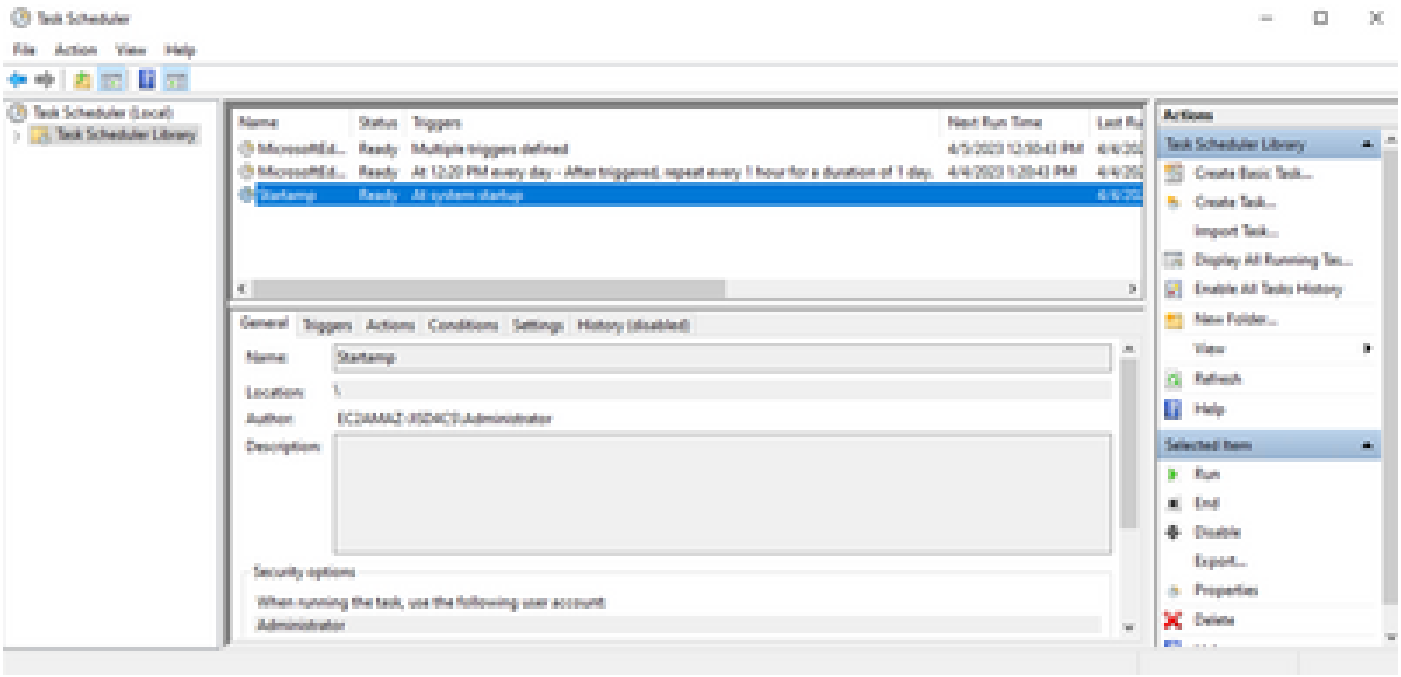
Script-beschrijving instellen

Het eerste script, 'Setup', wordt uitgevoerd op de Golden Image voordat het wordt gekloond. Het moet slechts één keer handmatig worden uitgevoerd. Het belangrijkste doel is om initiële configuraties vast te stellen waarmee het volgende script correct kan functioneren op de gekloonde virtuele machines. Deze configuraties omvatten:

- De opstart van de Cisco Advanced Malware Service handmatig wijzigen om automatische start te voorkomen.
- Een geplande taak maken die het volgende script uitvoert (Startup) bij het opstarten van het systeem met de hoogste rechten.
- Een variabele voor de systeemomgeving maken met de naam "AMP_GOLD_HOST" waarin de hostnaam van de Golden Image wordt opgeslagen. Dat zou door het Startup script worden gebruikt om te kijken of we de wijzigingen moeten terugdraaien

Na het uitvoeren van het Setup Script kunnen we verifiëren dat de configuratie wijzigingen is geïmplementeerd





Aangezien wij deze actie in het gouden beeld uitvoerden zullen alle nieuwe instanties deze configuratie hebben en zullen het StartupScript bij opstarten uitvoeren.

Scriptcode instellen

```
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
```

De scriptcode van de instelling is vrij simpel:

Lijn 2: Verandert het opstarttype van de malware-beveiligingsdienst in handleiding.

Lijn 5: Maakt een nieuwe omgevingsvariabele genaamd "AMP_GOLD_HOST" en slaat de hostnaam van de huidige computer erin op.

Lijn 9: Maakt een geplande taak genaamd "Startamp" die het gespecificeerde 'Startup' script uitvoert tijdens het opstarten van het systeem met de hoogste rechten, zonder dat er een wachtwoord nodig is.

Opstartscripts

Beschrijving opstartscripts

Het tweede script, 'Startup', draait op elk systeem startup op de gekloonde virtuele machines. Het belangrijkste doel is om te controleren of de huidige machine de hostnaam van de 'Golden Image' heeft:

- Als de huidige machine de Gouden Afbeelding is, wordt geen actie ondernomen en het manuscript beëindigt. AMP blijft actief bij het opstarten van het systeem omdat we de geplande taak onderhouden.
- Als de huidige machine NIET de 'Gouden' afbeelding is, worden de wijzigingen die door het eerste script zijn aangebracht, gereset:
  - De opstartconfiguratie van de Cisco AMP-service wijzigen in automatisch.
  - De Cisco Advanced Malware Protection-service starten.
  - Verwijderen van de "AMP_GOLD_HOST" omgevingsvariabele.
  - Verwijderen van de geplande taak die het opstartscript uitvoert en het script zelf verwijderen.

Scriptcode instellen

```
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
```

Lijn 2: Vergelijkt de huidige hostnaam met de opgeslagen "AMP_GOLD_HOST" waarde; als ze hetzelfde zijn, springt het script naar hetzelfde "zelfde" label, anders springt het naar het "niet zelfde" label.

Lijn 4-6: Wanneer het "zelfde"etiket wordt bereikt, doet het script niets aangezien het nog steeds de Gouden Beeld is en gaat verder naar het "uitgang"etiket.

Lijn 8-16: Als het "niet zelfde"etiket wordt bereikt, voert het script de volgende acties uit:

- Verandert het opstarttype van de malware-beveiligingsdienst naar automatisch.
- Start de malware-beveiligingsservice.
- Verwijdert de "AMP_GOLD_HOST" omgevingsvariabele.
- Verwijdert de geplande taak met de naam "Startamp"

Conclusie

Deze twee scripts maken het opstarten van Cisco AMP-services in gekloonde virtuele machinemilieu's mogelijk. Door het Golden Image correct te configureren en de opstartscripts te gebruiken, zorgt deze ervoor dat het Cisco AMP op alle gekloonde virtuele machines met de juiste configuratie wordt uitgevoerd

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.