AWS Workspaces의 보안 엔드포인트 - 골든 이미지 시작 및 설정 스크립트

목차

소개

이 솔루션은 복제 전에 골든 이미지에서 실행되는 '설치' 스크립트와 시스템 시작 중에 복제된 각 가상 머신에서 실행되는 '시작' 스크립트로 구성됩니다. 이러한 스크립트의 주요 목적은 수동 작업을 줄이면서 서비스의 올바른 구성을 보장하는 것입니다.

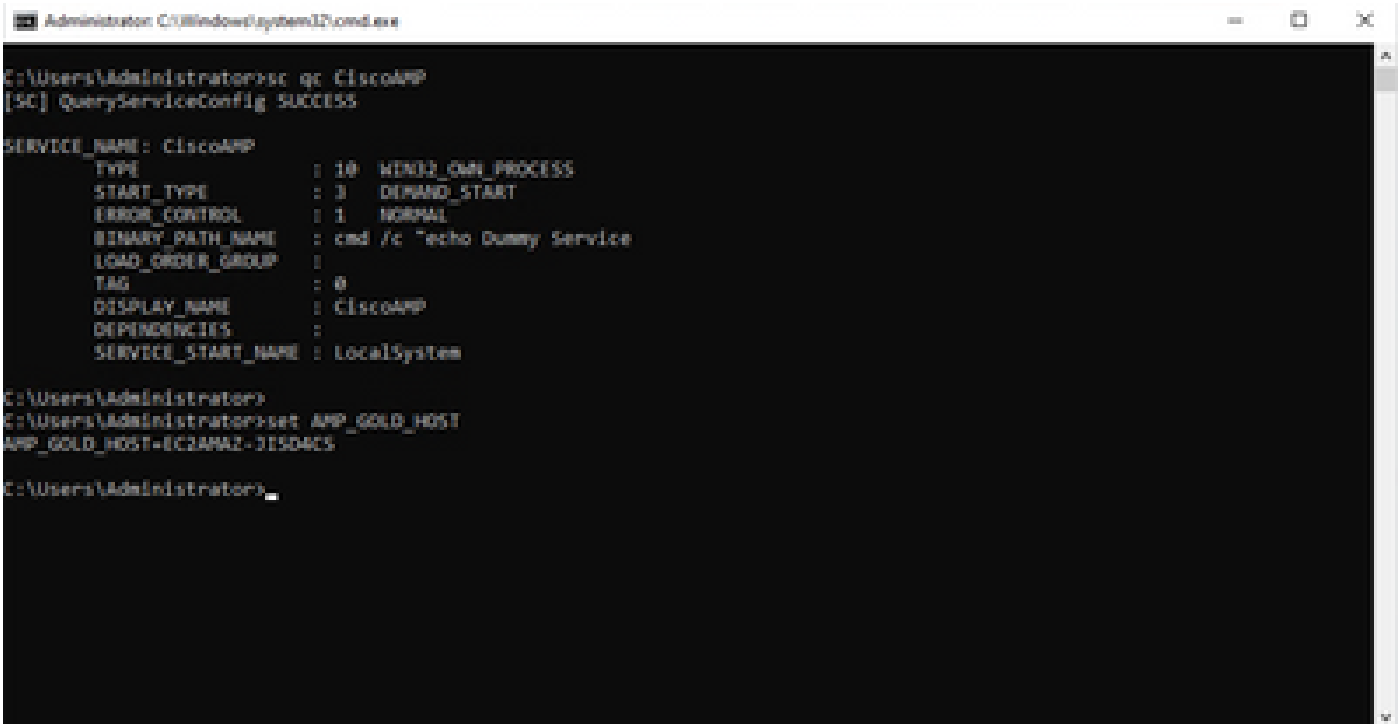
설치 스크립트

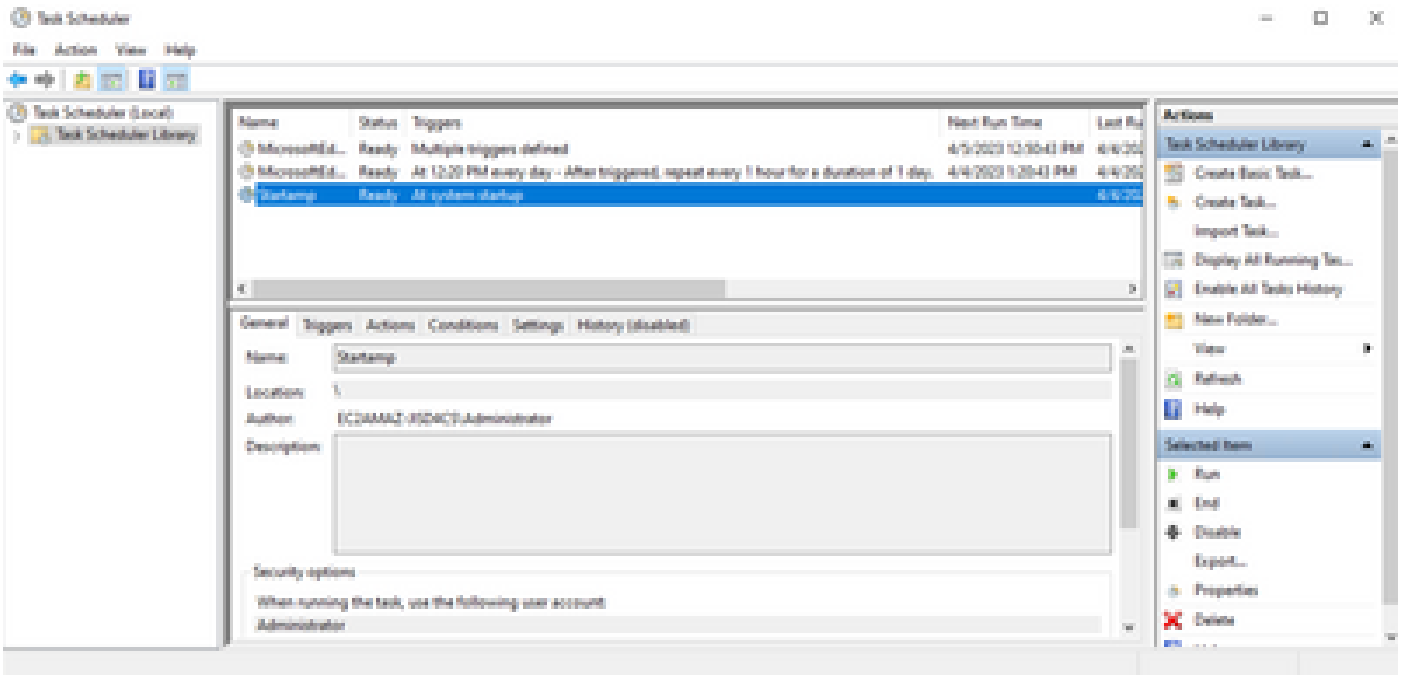
설치 스크립트 설명

첫 번째 스크립트인 'Setup'은 복제 전에 골든 이미지에서 실행됩니다. 한 번만 수동으로 실행해야 합니다. 주요 목적은 다음 스크립트가 복제된 가상 머신에서 올바르게 작동할 수 있도록 하는 초기 컨피그레이션을 설정하는 것입니다. 이러한 컨피그레이션에는 다음이 포함됩니다.

- Cisco AMP 서비스 시작을 수동으로 변경하여 자동 시작을 방지합니다.
- 최고 권한을 가진 시스템 시작 시 다음 스크립트(시작)를 실행하는 예약 작업 생성
- 골든 이미지의 호스트 이름을 저장하는 "AMP_GOLD_HOST"라는 시스템 환경 변수를 생성합니다. 이는 Startup 스크립트에서 변경 사항을 되돌려야 하는지 확인하는 데 사용됩니다

설치 스크립트를 실행한 후 컨피그레이션 변경 사항이 성공적으로 구축되었는지 확인할 수 있습니다





골든 이미지에서 이 작업을 수행했으므로 모든 새 인스턴스는 이 컨피그레이션을 갖게 되며 시작 시 시작 스크립트를 실행합니다.

설치 스크립트 코드

```
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
```

설치 스크립트 코드는 매우 간단합니다.

행 2: 악성코드 차단 서비스의 시작 유형을 manual로 변경합니다.

행 5: "AMP_GOLD_HOST"라는 새 환경 변수를 만들고 현재 컴퓨터의 호스트 이름을 저장합니다.

행 9: "Startamp"라는 이름의 예약된 작업을 만듭니다. 이 작업은 시스템 시작 중에 비밀번호 없이 가장 높은 권한으로 지정된 'Startamp' 스크립트를 실행합니다.

시작 스크립트

시작 스크립트 설명

두 번째 스크립트인 'Startup'은 복제된 가상 머신의 각 시스템 시작에서 실행됩니다. 주요 목적은 현재 시스템의 호스트 이름이 '골든 이미지'인지 확인하는 것입니다.

- 현재 시스템이 골든 이미지이면 작업이 수행되지 않고 스크립트가 종료됩니다. 예약된 작업을 유지하므로 AMP는 시스템 시작 시 계속 실행됩니다.
- 현재 시스템이 '골든' 이미지가 아닌 경우 첫 번째 스크립트에서 변경한 내용이 재설정됩니다.
  - Cisco AMP 서비스 시작 컨피그레이션을 자동으로 변경
  - Cisco AMP 서비스를 시작합니다.
  - "AMP_GOLD_HOST" 환경 변수를 제거합니다.
  - 시작 스크립트를 실행하는 예약 작업을 삭제하고 스크립트 자체를 삭제합니다.

설치 스크립트 코드

```
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
```

행 2: 현재 호스트 이름을 저장된 "AMP_GOLD_HOST" 값과 비교합니다. 동일한 경우 스크립트는 "same" 레이블로 이동하고, 그렇지 않으면 "notsame" 레이블로 이동합니다.

행 4-6: "동일한" 레이블에 도달하면 스크립트는 여전히 골든 이미지이므로 아무 작업도 수행하지 않고 "종료" 레이블로 진행합니다.

행 8-16: "notsame" 레이블에 도달하면 스크립트는 다음 작업을 수행합니다.

- 악성코드 차단 서비스의 시작 유형을 automatic으로 변경합니다.
- 악성코드 차단 서비스를 시작합니다.
- "AMP_GOLD_HOST" 환경 변수를 제거합니다.
- "Startamp"라는 예약된 작업을 삭제합니다.

결론

이 두 스크립트를 사용하면 복제된 가상 머신 환경에서 Cisco AMP 서비스를 시작할 수 있습니다. Golden 이미지를 올바르게 구성하고 시작 스크립트를 사용함으로써 Cisco AMP가 올바른 컨피그레이션으로 복제된 모든 가상 머신에서 실행되도록 합니다

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.