ASA/PIX:CLI를 사용하여 장애 조치 쌍의 소프트웨어 이미지를 업그레이드하는 방법

목차

소개

이 문서에서는 Cisco ASA 5500 Series Adaptive Security Appliances 장애 조치 쌍에서 소프트웨어 이미지를 업그레이드하기 위해 CLI를 사용하는 방법에 대해 설명합니다.

참고: ASDM(Adaptive Security Device Manager)은 7.0에서 7.2로 보안 어플라이언스 소프트웨어를 직접 업그레이드(또는 다운그레이드)하거나 ASDM 소프트웨어를 5.0에서 5.2로 직접 업그레이드(또는 다운그레이드)하는 경우 작동하지 않습니다.증분 순서로 업그레이드(또는 다운그레이드)해야 합니다.

ASA에서 ASDM 및 소프트웨어 이미지를 업그레이드하는 방법에 대한 자세한 내용은 PIX/ASA를 참조하십시오.ASDM 또는 CLI 컨피그레이션을 사용하여 소프트웨어 이미지 업그레이드 예

참고: 다중 컨텍스트 모드에서는 copy tftp **flash** 명령을 사용하여 모든 컨텍스트에서 PIX/ASA 이미지를 업그레이드하거나 다운그레이드할 수 없습니다.System Exec 모드에서만 지원됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA(Adaptive Security Appliance) 버전 7.0 이상
- Cisco ASDM 버전 5.0 이상

참고: ASDM에서 ASA를 구성하는 방법에 대한 자세한 내용은 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 컨피그레이션은 Cisco PIX 500 Series Security Appliance Software 버전 7.0 이상에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

장애 조치 쌍에 대해 제로 다운타임 업그레이드 수행

장애 조치 컨피그레이션의 두 유닛에는 동일한 주(첫 번째 번호) 및 부(두 번째 번호) 소프트웨어 버전이 있어야 합니다.그러나 업그레이드 프로세스 중에 유닛의 버전 패리티를 유지할 필요는 없습니다.각 유닛에서 실행되는 소프트웨어에 대해 다른 버전을 사용할 수 있으며 장애 조치 지원을 계속 유지할 수 있습니다.장기적인 호환성 및 안정성을 보장하려면 가능한 한 빨리 두 유닛을 동일한 버전으로 업그레이드하는 것이 좋습니다.

3가지 유형의 업그레이드를 사용할 수 있습니다.다음과 같습니다.

1. **Maintenance Release**(유지 보수 릴리스) - 부 릴리스의 모든 유지 보수 릴리스에서 다른 유지 보수 릴리스로 업그레이드할 수 있습니다.예를 들어 7.0(1)에서 7.0(4)으로 업그레이드할 수 있습니다. 먼저 그 사이에 유지 보수 릴리스를 설치할 필요가 없습니다.
2. **Minor Release**(부 릴리스) - 부 릴리스에서 다음 부 릴리스로 업그레이드할 수 있습니다.부 릴리스는 건너뛸 수 없습니다.예를 들어 7.0에서 7.1로 업그레이드할 수 있습니다. 7.0에서 7.2로 직접 업그레이드하는 것은 다운타임 없는 업그레이드에 지원되지 않습니다.먼저 7.1로 업그레이드해야 합니다.
3. **Major Release**(주 릴리스) - 이전 버전의 마지막 부 릴리스에서 다음 주 릴리스로 업그레이드할 수 있습니다.예를 들어 7.9가 7.x 릴리스의 마지막 부 버전인 경우 7.9에서 8.0으로 업그레이드할 수 있습니다.

액티브/스탠바이 장애 조치 컨피그레이션 업그레이드

액티브/스탠바이 장애 조치 컨피그레이션에서 2개의 유닛을 업그레이드하려면 다음 단계를 완료합

니다.

1. 두 유닛에 새 소프트웨어를 다운로드하고 boot system 명령을 사용하여 로드할 새 이미지를 지정합니다.자세한 내용은 CLI를 사용하여 소프트웨어 이미지 및 ASDM 이미지 업그레이드를 참조하십시오.
2. 아래와 같이 액티브 유닛에서 failover reload-standby **명령**을 입력하여 새 이미지를 부팅하려면 스탠바이 유닛을 다시 로드합니다.
   ```
   active#failover reload-standby
   ```
3. 스탠바이 유닛이 재로드를 완료하고 스탠바이 준비 상태에 있는 경우 액티브 유닛에서 액티브 유닛에 no failover active **명령**을 입력하여 액티브 유닛을 스탠바이 유닛으로 장애 조치를 강제로 실행합니다.
   ```
   active#no failover active
   ```

   참고: 스탠바이 유닛이 Standby Ready(스탠바이 준비) 상태인지 확인하려면 show failover **명령**을 사용합니다.
4. reload **명령**을 입력하여 이전 액티브 유닛(이제 새 스탠바이 유닛)을 다시 로드합니다.
   ```
   newstandby#reload
   ```
5. 새 스탠바이 유닛이 재로드를 완료하고 스탠바이 준비 상태에 있으면 failover active **명령**을 입력하여 원래 액티브 유닛을 액티브 상태로 되돌립니다.
   ```
   newstandby#failover active
   ```

이렇게 하면 액티브/스탠바이 장애 조치 쌍을 업그레이드하는 프로세스가 완료됩니다.

액티브/액티브 장애 조치 컨피그레이션 업그레이드

액티브/액티브 장애 조치 컨피그레이션에서 두 유닛을 업그레이드하려면 다음 단계를 완료합니다.

1. 두 유닛에 새 소프트웨어를 다운로드하고 boot system 명령을 사용하여 로드할 새 이미지를 지정합니다.자세한 내용은 CLI를 사용하여 소프트웨어 이미지 및 ASDM 이미지 업그레이드를 참조하십시오.
2. 기본 유닛의 시스템 실행 공간에 failover active **명령**을 입력하여 기본 유닛에서 두 장애 조치 그룹을 모두 활성으로 설정합니다.
   ```
   primary#failover active
   ```
3. 보조 유닛을 다시 로드하여 기본 유닛의 **시스템 실행 공간**에 failover reload-standby **명령**을 입력하여 새 이미지를 부팅합니다.
   ```
   primary#failover reload-standby
   ```
4. 보조 유닛의 재로드가 완료되고 두 장애 조치 그룹이 해당 유닛의 대기 준비 상태에 있는 경우, 기본 유닛의 시스템 실행 공간에서 no failover active **명령**을 사용하여 보조 유닛에서 두 장애 조치 그룹을 모두 활성으로 설정합니다.
   ```
   primary#no failover active
   ```

   참고: 두 장애 조치 그룹이 보조 유닛에서 Standby Ready 상태임을 확인하려면 show failover 명령**을** 사용합니다.
5. 두 장애 조치 그룹 모두 기본 유닛의 Standby Ready 상태에 있는지 확인한 다음 reload **명령**을 사용하여 기본 유닛을 다시 로드합니다.
   ```
   primary#reload
   ```

6. 장애 조치 그룹이 preempt 명령으로 구성된 경우 **선점 지연**이 경과한 후 지정된 유닛에서 자동으로 액티브 상태가 됩니다.장애 조치 그룹이 preempt 명령으로 구성되지 않은 경우 **failover active group 명령**을 사용하여 지정된 유닛에서 액티브 상태로 되돌릴 수 있습니다.

문제 해결

%ASA-5-720012:(VPN-Secondary) 스탠바이 유닛(또는) %ASA-6-720012에서 IPSec 장애 조치(failover) 런타임 데이터를 업데이트하지 못했습니다.(VPN-unit) 스탠바이 유닛에서 IPsec 장애 조치 런타임 데이터를 업데이트하지 못했습니다.

문제

Cisco ASA(Adaptive Security Appliance)를 업그레이드하려고 할 때 다음 오류 메시지 중 하나가 나타납니다.

```
%ASA-5-720012:(VPN-Secondary)   IPSec      .

%ASA-6-720012:(VPN-unit)   IPsec      .
```

솔루션

이러한 오류 메시지는 정보 관련 오류입니다.메시지는 ASA 또는 VPN의 기능에 영향을 주지 않습니다.

이러한 메시지는 대기 유닛에서 해당 IPsec 터널이 삭제되었기 때문에 VPN 장애 조치 하위 시스템이 IPsec 관련 런타임 데이터를 업데이트할 수 없는 경우에 나타납니다.이를 해결하려면 액티브 유닛에서 wr **standby** 명령을 실행합니다.

이러한 행동을 해결하기 위해 두 개의 버그가 제출되었습니다.이러한 버그가 수정된 ASA의 소프트웨어 버전으로 업그레이드할 수 있습니다.자세한 내용은 Cisco 버그 ID CSCtj58420(등록된 고객만 해당) 및 CSCtn56517(등록된 고객만 해당)을 참조하십시오.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco Adaptive Security Device Manager
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems