ASA/PIX: 투명 모드에서 액티브/액티브 장애 조치 구성

목차

소개

장애 조치 컨피그레이션에는 전용 장애 조치 링크 및 선택적으로 상태 기반 장애 조치 링크를 통해 서로 연결된 두 개의 동일한 보안 어플라이언스가 필요합니다. 특정 장애 조치 조건이 충족되는지 확인하기 위해 활성 인터페이스 및 유닛의 상태가 모니터링됩니다. 이러한 조건이 충족되면 장애 조치가 발생합니다.

보안 어플라이언스는 두 가지 장애 조치 컨피그레이션을 지원합니다.

- 액티브/액티브 장애 조치
- 액티브/스탠바이 장애 조치

각 장애 조치 컨피그레이션에는 장애 조치를 확인하고 수행하는 고유한 방법이 있습니다. 액티브/액티브 장애 조치를 사용하면 두 유닛 모두 네트워크 트래픽을 전달할 수 있습니다. 이렇게 하면 네트워크에서 로드 밸런싱을 구성할 수 있습니다. 액티브/액티브 장애 조치는 다중 컨텍스트 모드에서 실행되는 유닛에서만 사용할 수 있습니다. 액티브/스탠바이 장애 조치의 경우 한 유닛만 트래픽을 전달하고 다른 유닛은 스탠바이 상태로 대기합니다. 액티브/스탠바이 장애 조치는 단일 또는 다중 컨텍스트 모드에서 실행되는 유닛에서 사용할 수 있습니다. 두 장애 조치 구성 모두 상태 저장 또는 상태 비저장(일반) 장애 조치를 지원합니다.

투명 방화벽은 *와이어* 또는 *스텔스 방화벽*과 같은 역할을 *하는 레이어* 2 방화벽이며 연결된 디바이스에 대한 라우터 홉으로 보이지 않습니다. 보안 어플라이언스는 내부 및 외부 포트에서 동일한 네트워크를 연결합니다. 방화벽은 라우팅 홉이 아니므로 기존 네트워크에 투명 방화벽을 쉽게 도입할 수 있습니다. IP를 재구성할 필요가 없습니다. 기본 라우팅 방화벽 모드 또는 투명 방화벽 모드에서 실행되도록 Adaptive Security Appliance를 설정할 수 있습니다. 모드를 변경할 때 Adaptive Security Appliance는 두 모드 모두에서 지원되지 않는 명령이 많으므로 컨피그레이션을 지웁니다. 이미 채워진 컨피그레이션이 있는 경우 모드를 변경하기 전에 이 컨피그레이션을 백업해야 합니다. 새 컨피그레이션을 생성할 때 이 백업 컨피그레이션을 참조할 수 있습니다. 투명 모드의 방화벽 어플라이언스 컨피그레이션에 대한 자세한 내용은 투명 방화벽 컨피그레이션 예를 참조하십시오.

이 문서에서는 ASA 보안 어플라이언스에서 투명 모드에서 액티브/액티브 장애 조치를 구성하는 방법에 대해 중점적으로 설명합니다.

참고: 다중 컨텍스트 모드에서 실행되는 유닛에서는 VPN 장애 조치가 지원되지 않습니다. VPN 장애 조치는 **액티브/스탠바이 장애 조치** 컨피그레이션에만 사용할 수 있습니다.

Cisco에서는 장애 조치에 관리 인터페이스를 사용하지 않는 것이 좋습니다. 특히 보안 어플라이언스가 한 보안 어플라이언스에서 다른 보안 어플라이언스로 연결 정보를 지속적으로 전송하는 상태 저장 장애 조치에는 이 인터페이스를 사용하지 않는 것이 좋습니다. 장애 조치를 위한 인터페이스는 일반 트래픽을 전달하는 인터페이스와 최소 용량이 같아야 하며, ASA 5540의 인터페이스는 기가비트이지만 관리 인터페이스는 FastEthernet 전용입니다. 관리 인터페이스는 관리 트래픽에만 사용하도록 설계되고 management0/0으로 지정됩니다. 그러나 **management-only** 명령을 사용하여 모든 인터페이스를 관리 전용 인터페이스로 구성할 수 있습니다. 또한 Management 0/0의 경우 관리 전용 모드를 비활성화하여 인터페이스가 다른 인터페이스처럼 트래픽을 전달할 수 있도록 할 수 있습니다. **management-only** 명령에 대한 자세한 내용은 Cisco Security Appliance 명령 참조 버전 8.0을 참조하십시오.

이 컨피그레이션 가이드는 ASA/PIX 7.x Active/Standby 기술을 간략하게 소개하는 샘플 컨피그레

이션을 제공합니다. 이 기술을 기반으로 한 이론에 대한 자세한 내용은 ASA/PIX 명령 참조 설명서를 참조하십시오.

사전 요구 사항

요구 사항

하드웨어 요구 사항

장애 조치 컨피그레이션의 두 유닛에는 동일한 하드웨어 컨피그레이션이 있어야 합니다. 동일한 모델이어야 하며 인터페이스 수와 유형이 동일해야 하며 동일한 양의 RAM이 있어야 합니다.

참고: 두 유닛에는 동일한 크기의 플래시 메모리가 필요하지 않습니다. 장애 조치 컨피그레이션에서 플래시 메모리 크기가 다른 유닛을 사용하는 경우, 플래시 메모리가 작은 유닛에 소프트웨어 이미지 파일 및 컨피그레이션 파일을 수용할 충분한 공간이 있는지 확인하십시오. 그렇지 않으면 플래시 메모리가 큰 유닛에서 플래시 메모리가 작은 유닛으로 컨피그레이션 동기화에 실패합니다.

소프트웨어 요구 사항

장애 조치 컨피그레이션의 두 유닛은 운영 모드(라우팅 또는 투명, 단일 또는 다중 컨텍스트)여야 합니다. 주(첫 번째 번호) 및 부(두 번째 번호) 소프트웨어 버전이 동일해야 하지만, 업그레이드 프로세스 내에서 다른 버전의 소프트웨어를 사용할 수 있습니다. 예를 들어, 한 유닛을 버전 7.0(1)에서 버전 7.0(2)으로 업그레이드하고 장애 조치가 활성 상태로 유지되도록 할 수 있습니다. Cisco에서는 장기적인 호환성을 보장하기 위해 두 유닛을 모두 동일한 버전으로 업그레이드할 것을 권장합니다.

장애 조치 쌍에서 소프트웨어를 업그레이드하는 방법에 대한 자세한 내용은 *Cisco Security Appliance Command Line Configuration Guide, Version 8.0*의 Performing Zero Downtime Upgrades for Failover Pairs 섹션을 참조하십시오.

라이센스 요구 사항

ASA 보안 어플라이언스 플랫폼에서 하나 이상의 유닛에 **제한(UR) 라이센스가** 있어야 합니다.

참고: 추가 기능 및 혜택을 얻으려면 장애 조치 쌍의 라이센스를 업그레이드해야 할 수 있습니다. 자세한 내용은 장애 조치 쌍의 라이센스 키 업그레이드를 참조하십시오.

참고: 장애 조치에 참여하는 두 보안 어플라이언스의 라이센스 기능(예: SSL VPN 피어 또는 보안 컨텍스트)은 동일해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 7.x 버전 이상의 ASA Security Appliance

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 다음 하드웨어 및 소프트웨어 버전과 함께 사용할 수도 있습니다.

- 7.x 버전 이상의 PIX Security Appliance

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

액티브/액티브 장애 조치

이 섹션에서는 액티브/스탠바이 장애 조치에 대해 설명하며 다음 항목을 포함합니다.

액티브/액티브 장애 조치 개요

액티브/액티브 장애 조치는 다중 컨텍스트 모드의 보안 어플라이언스에서만 사용할 수 있습니다. 액티브/액티브 장애 조치 컨피그레이션에서는 두 보안 어플라이언스가 네트워크 트래픽을 전달할 수 있습니다.

액티브/액티브 장애 조치에서는 보안 어플라이언스의 보안 컨텍스트를 장애 조치 그룹으로 나눕니다. 장애 조치 그룹은 단순히 하나 이상의 보안 컨텍스트로 구성된 논리적 그룹입니다. 보안 어플라이언스에 최대 2개의 장애 조치 그룹을 생성할 수 있습니다. 관리 컨텍스트는 항상 장애 조치 그룹 1의 멤버입니다. 할당되지 않은 모든 보안 컨텍스트는 기본적으로 장애 조치 그룹 1의 멤버입니다.

장애 조치 그룹은 액티브/액티브 장애 조치에서 장애 조치를 위한 기본 유닛을 구성합니다. 인터페이스 장애 모니터링, 장애 조치 및 액티브/스탠바이 상태는 유닛이 아닌 장애 조치 그룹의 모든 속성입니다. 액티브 장애 조치 그룹이 실패하면 스탠바이 상태로 변경되고 스탠바이 장애 조치 그룹은 액티브 상태가 됩니다. 액티브 상태가 되는 장애 조치 그룹의 인터페이스는 장애 조치 그룹에서 실패한 인터페이스의 MAC 및 IP 주소를 가정합니다. 스탠바이 상태가 된 장애 조치 그룹의 인터페이스는 스탠바이 MAC 및 IP 주소를 인수합니다.

참고: 유닛에서 장애 조치 그룹이 실패하는 것은 유닛이 실패했음을 의미하지 않습니다. 유닛에는 여전히 트래픽을 전달하는 다른 장애 조치 그룹이 있을 수 있습니다.

기본/보조 상태 및 활성/대기 상태

액티브/스탠바이 장애 조치에서와 같이 액티브/액티브 장애 조치 쌍의 한 유닛은 기본 유닛으로, 다른 유닛은 보조 유닛으로 지정됩니다. 액티브/스탠바이 장애 조치와 달리, 이 지정은 두 유닛이 동시에 시작될 때 액티브 유닛이 되는 것을 나타내지 않습니다. 대신 기본/보조 지정에서는 두 가지 작업을 수행합니다.

- 쌍을 동시에 부팅할 때 실행 중인 컨피그레이션을 제공하는 유닛을 결정합니다.
- 유닛이 동시에 부팅될 때 각 장애 조치 그룹이 활성 상태로 표시되는 유닛을 결정합니다. 컨피

그레이션의 각 장애 조치 그룹은 기본 또는 보조 유닛 기본 설정으로 구성됩니다. 두 장애 조치 그룹 모두 쌍의 단일 유닛에서 액티브 상태에 있고, 스탠바이 상태의 장애 조치 그룹이 포함된 다른 유닛을 구성할 수 있습니다. 그러나 더 일반적인 컨피그레이션에서는 각 장애 조치 그룹에 서로 다른 역할 환경 설정을 할당하여 각 장애 조치 그룹을 다른 유닛에서 액티브 상태로 만들고 디바이스 전체에 트래픽을 분산하는 것이 좋습니다.**참고:** 보안 어플라이언스는 로드 밸런싱 서비스를 제공하지 **않습니다**. 로드 밸런싱은 보안 어플라이언스로 트래픽을 전달하는 라우터에서 처리해야 합니다.

각 장애 조치 그룹이 활성화되는 유닛은 아래와 같이 결정됩니다.

- 피어 유닛을 사용할 수 없는 동안 유닛이 부팅되면 두 장애 조치 그룹 모두 유닛에서 액티브 상태가 됩니다.
- 피어 유닛이 활성 상태일 때(두 장애 조치 그룹이 모두 활성 상태인 경우) 유닛이 부팅될 경우, 장애 조치 그룹은 다음 중 하나가 발생할 때까지 장애 조치 그룹의 기본 또는 보조 기본 설정에 관계없이 액티브 유닛에서 액티브 상태로 유지됩니다.장애 조치가 발생합니다.**no failover active** 명령을 사용하여 장애 조치 그룹을 다른 유닛에 수동으로 강제 적용합니다preempt 명령을 사용하여 장애 조치 그룹을 구성했으므로 유닛이 사용 가능하게 되면 장애 조치 그룹이 기본 유닛에서 자동으로 액티브 상태가 됩니다.
- 두 유닛이 동시에 부팅되면 컨피그레이션이 동기화된 후 각 장애 조치 그룹이 기본 유닛에서 액티브 상태가 됩니다.

디바이스 초기화 및 컨피그레이션 동기화

컨피그레이션 동기화는 장애 조치 쌍 부팅 시 하나 또는 두 유닛 모두 발생할 때 발생합니다. 다음과 같이 컨피그레이션이 동기화됩니다.

- 피어 유닛이 활성 상태일 때(두 장애 조치 그룹 모두 활성 상태) 유닛이 부팅될 경우 부팅 유닛은 부팅 유닛의 기본 또는 보조 지정에 관계없이 실행 중인 컨피그레이션을 얻기 위해 액티브 유닛에 접속합니다.
- 두 유닛이 동시에 부팅되면 보조 유닛에서는 기본 유닛에서 실행 중인 컨피그레이션을 가져옵니다.

복제가 시작되면 컨피그레이션을 전송하는 유닛의 보안 어플라이언스 콘솔에 `"Beginning configuration replication: Sending to mate,"` 및 완료 시 보안 어플라이언스는 `"End Configuration Replication to mate"` 메시지를 표시합니다. 복제 과정에서 컨피그레이션을 전송하는 유닛에 입력된 명령은 피어 유닛에 제대로 복제되지 않으며, 컨피그레이션을 수신하는 유닛에 입력된 명령을 수신한 컨피그레이션에 의해 덮어쓸 수 있습니다. 컨피그레이션 복제 프로세스 중에 장애 조치 쌍의 유닛 중 하나에서 명령을 수행하지 마십시오. 컨피그레이션의 크기에 따라 복제가 몇 초에서 몇 분 정도 걸릴 수 있습니다.

컨피그레이션을 수신하는 유닛에서는 컨피그레이션이 실행 중인 메모리에만 존재합니다. 동기화 후 컨피그레이션을 플래시 메모리에 저장하려면 액티브 상태의 장애 조치 그룹 1이 있는 유닛의 시스템 실행 공간에 **write memory all** 명령을 입력합니다. 이 명령은 피어 유닛에 복제되며 플래시 메모리에 컨피그레이션을 계속 씁니다. **all** 키워드를 이 명령과 함께 사용하면 시스템 및 모든 컨텍스트 컨피그레이션이 저장됩니다.

참고: 외부 서버에 저장된 시작 컨피그레이션은 네트워크를 통해 유닛에서 액세스할 수 있으며 각 유닛에 대해 별도로 저장할 필요가 없습니다. 또는 기본 유닛의 디스크에서 외부 서버로 컨텍스트 컨피그레이션 파일을 복사한 다음, 유닛이 다시 로드될 때 사용 가능한 보조 유닛의 디스크에 복사할 수 있습니다.

명령 복제

두 유닛이 모두 실행되면 다음과 같이 명령이 한 유닛에서 다른 유닛으로 복제됩니다.

- 보안 컨텍스트 내에 입력된 명령은 보안 컨텍스트가 활성 상태에 나타나는 유닛에서 피어 유닛으로 복제됩니다.**참고:** 해당 유닛이 속한 장애 조치 그룹이 해당 유닛의 활성 상태인 경우 컨텍스트는 유닛의 활성 상태로 간주됩니다.
- 시스템 실행 영역에 입력된 명령은 장애 조치 그룹 1이 활성 상태인 유닛에서 장애 조치 그룹 1이 대기 상태인 유닛으로 복제됩니다.
- 관리 컨텍스트에 입력된 명령은 장애 조치 그룹 1이 활성 상태인 유닛에서 장애 조치 그룹 1이 대기 상태인 유닛으로 복제됩니다.

모든 컨피그레이션 및 파일 명령(**copy, rename, delete, mkdir, rmdir** 등)이 복제되며 이러한 경우는 예외입니다. **show, debug, mode, firewall** 및 **failover lan unit** 명령은 복제되지 않습니다.

명령 복제가 발생할 수 있는 적절한 유닛에 명령을 입력하지 않으면 컨피그레이션이 동기화되지 않습니다. 이러한 변경 사항은 다음에 초기 컨피그레이션 동기화가 발생할 때 손실될 수 있습니다.

write standby 명령을 사용하여 동기화되지 않은 컨피그레이션을 재동기화할 수 있습니다. 액티브/**쓰기 대기** 액티브 장애 조치의 경우 **write standby** 명령은 다음과 같이 동작합니다.

- 시스템 실행 공간에 **write standby** 명령을 입력하면 보안 어플라이언스의 모든 보안 컨텍스트에 대한 시스템 컨피그레이션 및 컨피그레이션이 피어 유닛에 기록됩니다. 여기에는 대기 상태의 보안 컨텍스트에 대한 컨피그레이션 정보가 포함됩니다. 액티브 상태의 장애 조치 그룹 1이 있는 유닛의 시스템 실행 영역에서 명령을 입력해야 합니다.**참고:** 피어 유닛의 활성 상태에 보안 컨텍스트가 있는 경우 write standby 명령을 사용하면 해당 컨텍스트를 통한 활성 연결이 종료됩니다. **write standby** 명령을 입력하기 전에 컨피그레이션을 제공하는 유닛에서 failover **active** 명령을 사용하여 해당 유닛에서 모든 컨텍스트가 활성 상태인지 확인합니다.
- 보안 컨텍스트에서 **write standby** 명령을 입력하면 보안 컨텍스트에 대한 컨피그레이션만 피어 유닛에 기록됩니다. 보안 컨텍스트가 활성 상태로 표시되는 유닛의 보안 컨텍스트에서 명령을 입력해야 합니다.

복제된 명령은 피어 유닛에 복제될 때 플래시 메모리에 저장되지 않습니다. 실행 중인 컨피그레이션에 추가됩니다. 두 유닛의 플래시 메모리에 복제된 명령을 저장하려면 변경한 유닛에서 **write memory** 또는 copy running-**config startup-config** 명령을 사용합니다. 이 명령은 피어 유닛에 복제되고 컨피그레이션이 피어 유닛의 플래시 메모리에 저장되도록 합니다.

장애 조치 트리거

액티브/액티브 장애 조치에서는 다음 이벤트 중 하나가 발생하는 경우 유닛 레벨에서 장애 조치를 트리거할 수 있습니다.

- 장치에 하드웨어 오류가 있습니다.
- 장치에 전원 오류가 있습니다.
- 장치에 소프트웨어 오류가 있습니다.
- no failover **active** 또는 **failover active** 명령이 시스템 실행 공간에 입력됩니다.

다음 이벤트 중 하나가 발생하면 장애 조치 그룹 레벨에서 장애 조치가 트리거됩니다.

- 그룹에 너무 많은 모니터링된 인터페이스가 실패합니다.
- no failover **active group group_id** 또는 **failover active group group_id** 명령이 입력되었습니다.

장애 조치 작업

액티브/액티브 장애 조치 컨피그레이션에서는 시스템이 아닌 장애 조치 그룹 기준으로 장애 조치가 발생합니다. 예를 들어, 기본 유닛에서 두 장애 조치 그룹을 모두 활성으로 지정하고 장애 조치 그룹 1이 실패하면, 장애 조치 그룹 2는 기본 유닛에서 액티브 상태로 유지되고 장애 조치 그룹 1은 보조 유닛에서 액티브 상태가 됩니다.

참고: 액티브/액티브 장애 조치를 구성할 때 두 유닛의 결합된 트래픽이 각 유닛의 용량 내에 있는지 확인합니다.

이 표에서는 각 실패 이벤트에 대한 장애 조치 작업을 보여 줍니다. 각 오류 이벤트에 대해 정책, 장애 조치 발생 여부, 활성 장애 조치 그룹에 대한 작업 및 대기 장애 조치 그룹에 대한 작업이 제공됩니다.

실패 이벤트	정책	활성 그룹 작업	대기 그룹 작업	참고
유닛에 전원 또는 소프트웨어 장애 발생	장애 조치	스탠바이 마크 실패	대기 상태가 됩니다. 활성으로 실패 표시	장애 조치 쌍의 유닛에 장애가 발생하면 해당 유닛의 모든 활성 장애 조치 그룹은 실패로 표시되고 피어 유닛에서 액티브 상태가 됩니다.
임계값을 초과하는 활성 장애 조치 그룹에서 인터페이스 오류 발생	장애 조치	활성 그룹을 실패한 것으로 표시	활성 상태가 됨	없음
임계값을 초과하는 스탠바이 장애 조치 그룹에서 인터페이스 오류 발생	장애 조치 없음	작업 없음	대기 그룹을 실패한 것으로 표시	스탠바이 장애 조치 그룹이 실패한 것으로 표시될 경우, 액티브 장애 조치 그룹은 인터페이스 장애 조치 임계값을 넘은 경우에도 장애 조치를 시도하지 않습니다.
이전에 활성 장애 조치 그룹 복구	장애 조치 없음	작업 없음	작업 없음	preempt 명령을 사용하여 구성하지 않는 한 장애 조치 그룹은 현재 유닛에서 활성 상태로 유지됩니다.
시작 시 장애 조치 링크 실패	장애 조치 없	활성 상태가 됨	활성 상태가 됨	시작 시 장애 조치 링크가 다운되면 두 유닛의 두 장애 조치 그룹 모두 액티브 상태가 됩니다.

	음			
상태 저장 장애 조치 링크 실패	장애 조치 없음	작업 없음	작업 없음	상태 정보가 오래되고 장애 조치가 발생하면 세션이 종료됩니다.
작업 중 장애 조치 링크에 실패했습니다.	장애 조치 없음	해당 없음	해당 없음	각 유닛은 장애 조치 인터페이스를 실패한 것으로 표시합니다. 장애 조치 링크가 다운된 동안에는 유닛에서 스탠바이 유닛으로 장애 조치할 수 없으므로 최대한 빨리 장애 조치 링크를 복원해야 합니다.

일반 및 상태 기반 장애 조치

보안 어플라이언스는 두 가지 유형의 장애 조치(일반 및 상태 저장)를 지원합니다. 이 섹션에서는 다음 항목을 다룹니다.

- 일반 장애 조치
- 상태 기반 장애 조치

일반 장애 조치

장애 조치가 발생하면 모든 활성 연결이 삭제됩니다. 클라이언트는 새 활성 유닛이 인계될 때 연결을 다시 설정해야 합니다.

상태 기반 장애 조치

상태 저장 장애 조치가 활성화되면 활성 유닛은 연결 당 상태 정보를 대기 유닛에 지속적으로 전달합니다. 장애 조치가 발생하면 새 액티브 유닛에서 동일한 연결 정보를 사용할 수 있습니다. 지원되는 최종 사용자 애플리케이션은 동일한 통신 세션을 유지하기 위해 다시 연결할 필요가 없습니다.

스탠바이 유닛에 전달되는 상태 정보에는 다음이 포함됩니다.

- NAT 변환 테이블
- TCP 연결 상태
- UDP 연결 상태
- ARP 테이블
- 레이어 2 브리지 테이블(투명 방화벽 모드에서 실행되는 경우)
- HTTP 연결 상태(HTTP 복제가 활성화된 경우)
- ISAKMP 및 IPSec SA 테이블
- GTP PDP 연결 데이터베이스

상태 저장 장애 조치가 활성화된 경우 스탠바이 유닛에 전달되지 않는 정보에는 다음이 포함됩니다.

- HTTP 연결 테이블(HTTP 복제가 활성화된 경우 제외)

- 사용자 인증(uauth) 테이블
- 라우팅 테이블
- 보안 서비스 모듈에 대한 상태 정보

참고: 활성 Cisco IP SoftPhone 세션 내에서 장애 조치가 발생하면 통화 세션 상태 정보가 대기 유닛에 복제되므로 통화가 활성 상태로 유지됩니다. 통화가 종료되면 IP SoftPhone 클라이언트가 통화 관리자와의 연결이 끊어집니다. 이는 스탠바이 유닛에 CTIQBE 끊기 메시지에 대한 세션 정보가 없기 때문에 발생합니다. IP SoftPhone 클라이언트가 특정 기간 내에 Call Manager로부터 응답을 받지 못하면 Call Manager에 연결할 수 없는 것으로 간주하여 자체적으로 등록을 취소합니다.

장애 조치 컨피그레이션 제한 사항

다음 유형의 IP 주소로 장애 조치를 구성할 수 없습니다.

- DHCP를 통해 얻은 IP 주소
- PPPoE를 통해 얻은 IP 주소
- IPv6 주소

또한 다음과 같은 제한 사항이 적용됩니다.

- 상태 기반 장애 조치는 ASA 5505 Adaptive Security Appliance에서 지원되지 않습니다.
- 액티브/액티브 장애 조치는 ASA 5505 Adaptive Security Appliance에서 지원되지 않습니다.
- ASA 5505 Adaptive Security Appliance에서 Easy VPN Remote가 활성화된 경우 장애 조치를 구성할 수 없습니다.
- VPN 장애 조치는 다중 컨텍스트 모드에서 지원되지 않습니다.

지원되지 않는 기능

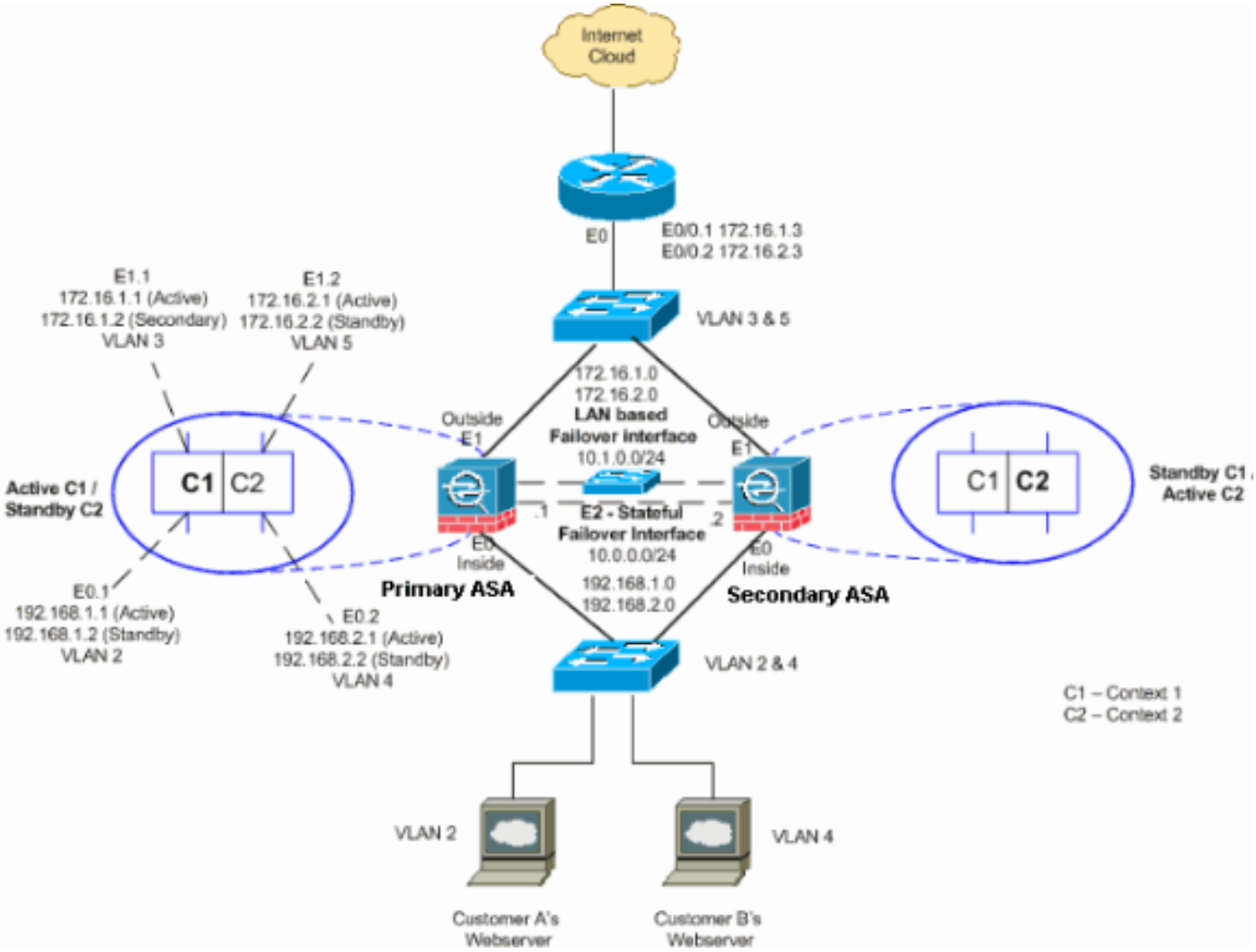
다중 컨텍스트 모드에서는 다음 기능을 지원하지 않습니다.

- 동적 라우팅 프로토콜보안 컨텍스트는 고정 경로만 지원합니다. 다중 컨텍스트 모드에서는 OSPF 또는 RIP를 활성화할 수 없습니다.
- VPN
- 멀티캐스트

LAN 기반 액티브/액티브 장애 조치 구성

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



이 섹션에서는 이더넷 장애 조치 링크를 사용하여 액티브/액티브 장애 조치를 구성하는 방법에 대해 설명합니다. LAN 기반 장애 조치를 구성할 때 보조 디바이스가 기본 디바이스에서 실행 중인 컨피그레이션을 가져오려면 먼저 보조 디바이스를 부트스트랩하여 장애 조치 링크를 인식해야 합니다.

참고: 크로스오버 이더넷 케이블 대신 기본 유닛과 보조 유닛 간에 전용 스위치를 사용하는 것이 좋습니다.

이 섹션에는 다음과 같은 항목이 포함되어 있습니다.

- 기본 유닛 컨피그레이션
- 보조 유닛 컨피그레이션

기본 유닛 컨피그레이션

액티브/액티브 장애 조치 컨피그레이션에서 기본 유닛을 구성하려면 다음 단계를 완료하십시오.

1. 아직 수행하지 않은 경우 각 데이터 인터페이스(라우팅 모드), 관리 IP 주소(투명 모드) 또는 관리 전용 인터페이스에 대해 활성 및 대기 IP 주소를 구성합니다. 대기 IP 주소는 현재 대기 유닛인 보안 어플라이언스에서 사용됩니다. 활성 IP 주소와 동일한 서브넷에 있어야 합니다.각 컨텍스트 내에서 인터페이스 주소를 구성해야 합니다. contexts를 전환하려면 changeto context 명령을 사용합니다. 명령 프롬프트가 hostname/context(config-if)#으로 변경됩니다. 여기서 context는 현재 컨텍스트의 이름입니다. 투명 방화벽 모드에서는 각 컨텍스트에 대한

관리 IP 주소를 입력해야 합니다.**참고:** 전용 상태 기반 장애 조치 인터페이스를 사용하는 경우 상태 기반 장애 조치 링크에 대한 IP 주소를 구성하지 마십시오. 장애 조치 **인터페이스 ip** 명령을 사용하여 나중에 전용 상태 기반 장애 조치 인터페이스를 구성합니다.

```
hostname/context(config-if)#ip address active_addr netmask standby standby_addr
```

이 예에서는 기본 ASA의 context1에 대한 외부 인터페이스가 다음과 같이 구성됩니다.

```
ASA/context1(config)#ip address 172.16.1.1 255.255.255.0
                                    standby 172.16.1.2
```

Context2의 경우:

```
ASA/context2(config)#ip address 192.168.2.1 255.255.255.0
                                    standby 192.168.2.2
```

라우팅된 방화벽 모드 및 관리 전용 인터페이스의 경우 이 명령은 각 인터페이스에 대한 인터페이스 컨피그레이션 모드에서 입력됩니다. 투명 방화벽 모드에서는 명령이 전역 컨피그레이션 모드에서 입력됩니다.

2. 시스템 실행 영역에서 기본 장애 조치 매개변수를 구성합니다.(PIX 보안 어플라이언스에만 해당) LAN 기반 장애 조치를 활성화합니다.

```
hostname(config)#failover lan enable
```

유닛을 기본 유닛으로 지정합니다.

```
hostname(config)#failover lan unit primary
```

장애 조치 링크를 지정합니다.

```
hostname(config)#failover lan interface if_name phy_if
```

이 예에서는 인터페이스 이더넷 3을 LAN 기반 장애 조치 인터페이스로 사용합니다.

```
ASA(config)#failover lan interface LANFailover ethernet3
```

if_name 인수는 phy_if 인수로 지정한 인터페이스에 논리 이름을 할당합니다. phy_if 인수는 Ethernet1과 같은 물리적 포트 이름 또는 이전에 생성한 Ethernet0/2.3 등의 하위 인터페이스가 될 수 있습니다. ASA 5505 Adaptive Security Appliance에서 phy_if는 VLAN을 지정합니다. 이 인터페이스는 다른 용도로 사용해서는 안 됩니다(선택적으로 상태 저장 장애 조치 링크 제외).장애 조치 링크 활성 및 대기 IP 주소를 지정합니다.

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

이 예에서는 10.1.0.1을 액티브 IP 주소로, 10.1.0.2은 장애 조치 인터페이스에 대해 스탠바이 IP 주소로 사용합니다.

```
ASA(config)#failover interface ip LANFailover
      10.1.0.1 255.255.255.0 standby 10.1.0.2
```

대기 IP 주소는 활성 IP 주소와 동일한 서브넷에 있어야 합니다. 스탠바이 IP 주소 서브넷 마스크를 식별할 필요가 없습니다. 장애 조치 링크 IP 주소 및 MAC 주소는 장애 조치 시 변경되지 않습니다. 활성 IP 주소는 항상 기본 유닛에 있고 대기 IP 주소는 보조 유닛에 유지됩니다.

보조 유닛 컨피그레이션

LAN 기반 액티브/액티브 장애 조치를 구성할 때 장애 조치 링크를 인식하려면 보조 유닛을 부트스트랩해야 합니다. 이렇게 하면 보조 유닛이 기본 유닛에서 실행 중인 컨피그레이션과 통신하고 수신할 수 있습니다.

액티브/액티브 장애 조치 컨피그레이션에서 보조 유닛을 부트스트랩하려면 다음 단계를 완료하십시오.

1. (PIX 보안 어플라이언스에만 해당) LAN 기반 장애 조치를 활성화합니다.
   hostname(config)#**failover lan enable**

2. 장애 조치 인터페이스를 정의합니다. 기본 유닛에 사용한 것과 동일한 설정을 사용합니다.장애 조치 인터페이스로 사용할 인터페이스를 지정합니다.
   hostname(config)#**failover lan interface** *if_name phy_if*

   ASA(config)#failover lan interface LANFailover ethernet3
   if_name 인수는 phy_if 인수로 지정한 인터페이스에 논리 이름을 할당합니다. phy_if 인수는 Ethernet1과 같은 물리적 포트 이름 또는 이전에 생성한 Ethernet0/2.3 등의 하위 인터페이스가 될 수 있습니다. ASA 5505 Adaptive Security Appliance에서 phy_if는 VLAN을 지정합니다.장애 조치 링크에 액티브 및 스탠바이 IP 주소를 할당합니다.
   hostname(config)#**failover interface ip** *if_name ip_addr* **mask standby** *ip_addr*

   ASA(config)#**failover interface ip LANFailover 10.1.0.1**
   255.255.255.0 standby 10.1.0.2

   참고: 장애 조치 인터페이스를 구성할 때 기본 유닛에서 입력한 것과 동일하게 이 명령을 입력합니다.대기 IP 주소는 활성 IP 주소와 동일한 서브넷에 있어야 합니다. 스탠바이 주소 서브넷 마스크를 식별할 필요가 없습니다.인터페이스를 활성화합니다.
   hostname(config)#**interface***phy_if*
   hostname(config-if)#**no shutdown**

3. 이 유닛을 보조 유닛으로 지정합니다.
   hostname(config)#**failover lan unit secondary**

   참고: 이 단계는 이전에 별도로 구성하지 않은 경우 기본 유닛이 보조로 지정되므로 선택 사항입니다.
4. 장애 조치를 활성화합니다.
   hostname(config)#**failover**

   장애 조치를 활성화하면 활성 유닛은 실행 중인 메모리의 컨피그레이션을 스탠바이 유닛으로 전송합니다. 컨피그레이션이 동기화되면 Beginning configuration **replication**(컨피그레이션 **복제 시작**) 메시지가 **표시됩니다. Sending to mate and End Configuration Replication to mate to mate(짝짓기 및 종료 컨피그레이션 복제**로 보내기)가 활성 유닛 콘솔에 나타납니다.**참고:** 먼저 기본 디바이스에서 failover 명령을 실행한 다음 보조 디바이스에서 실행합니다. 보조 디바이스에서 failover 명령을 실행하면 보조 디바이스에서 즉시 기본 디바이스에서 컨피그레이션을 가져오고 자신을 *대기*로 설정합니다. 기본 ASA는 작동 상태를 유지하고 트래픽을 정상적으로 전달하며 자신을 *활성* 디바이스로 표시합니다. 이 시점부터 활성 디바이스에서 장애가 발생할 때마다 대기 디바이스가 활성 상태로 표시됩니다.
5. 실행 중인 컨피그레이션이 복제를 완료한 후 이 명령을 입력하여 컨피그레이션을 플래시 메모리에 저장합니다.
   hostname(config)#**copy running-config startup-config**

6. 필요한 경우 기본 유닛에서 활성 상태인 장애 조치 그룹을 보조 유닛의 액티브 상태로 강제 적용합니다. 보조 유닛에서 장애 조치 그룹을 강제로 액티브 상태로 만들려면 기본 유닛의 시스

템 실행 공간에 이 명령을 입력합니다.

```
hostname#no failover active group group_id
```

group_id 인수는 보조 유닛에서 활성화하려는 그룹을 지정합니다.

구성

이 문서에서는 다음 구성을 사용합니다.

기본 ASA - Context1 컨피그레이션

```
ASA/context1(config)#show running-config
: Saved
:
ASA Version 7.2(3)




!
hostname context1
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside_context1
 nameif inside
 security-level 100
!--- Configure the active and standby IP's for the
logical inside !--- interface of the context1. ip
address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
interface outside_context1
 nameif outside
 security-level 0
!--- Configure the active and standby IP's for the
logical outside !--- interface of the context1. ip
address 172.16.1.1 255.255.255.0 standby 172.16.1.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.1.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.1.1 192.168.1.5 netmask
255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
```

```
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh timeout 5
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:00000000000000000000000000000000
: end
```

기본 ASA - Context2 컨피그레이션

```
ASA/context2(config)#show running-config
: Saved
:
ASA Version 7.2(3)




!
hostname context2
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside_context2
 nameif inside
 security-level 100
!--- Configure the active and standby IP's for the
logical inside !--- interface of the context2. ip
address 192.168.2.1 255.255.255.0 standby 192.168.2.2
!
interface outside_context2
 nameif outside
 security-level 0
!--- Configure the active and standby IP's for the
```

```
logical outside !--- interface of the context2. ip
address 172.16.2.1 255.255.255.0 standby 172.16.2.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.2.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.2.1 192.168.2.5 netmask
255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.2.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh timeout 5
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:00000000000000000000000000000000
: end
```

기본 ASA

```
ASA(config)#show running-config
```

```
: Saved
:
ASA Version 7.2(3) <system>
!
 !--- Use the firewall transparent command !--- in
global configuration mode in order to !--- set the
firewall mode to transparent mode.

firewall transparent
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
no mac-address auto
!
interface Ethernet0
!
interface Ethernet0.1
 vlan 2
!
interface Ethernet0.2
 vlan 4
!
interface Ethernet1
!
interface Ethernet1.1
 vlan 3
!
interface Ethernet1.2
 vlan 5
!
!--- Configure "no shutdown" in the stateful failover
interface as well as !--- LAN Failover interface of both
Primary and secondary ASA/PIX. interface Ethernet2
description STATE Failover Interface
!
interface Ethernet3
 description LAN Failover Interface
!
interface Ethernet4
 shutdown
!
interface Ethernet5
 shutdown
!
class default
  limit-resource All 0
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
!

ftp mode passive
pager lines 24
failover
failover lan unit primary
!--- Command to assign the interface for LAN based
failover failover lan interface LANFailover Ethernet3
!--- Configure the Authentication/Encryption key
failover key *****
failover link stateful Ethernet2
!--- Configure the active and standby IP's for the LAN
based failover failover interface ip LANFailover
10.1.0.1 255.255.255.0 standby 10.1.0.2
failover interface ip stateful 10.0.0.1 255.255.255.0
standby 10.0.0.2
```

```
failover group 1
failover group 2
  secondary
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
  config-url flash:/admin.cfg
!

context context1
  allocate-interface Ethernet0.1 inside_context1
  allocate-interface Ethernet1.1 outside_context1
  config-url flash:/context1.cfg
  join-failover-group 1
!

context context2
  allocate-interface Ethernet0.2 inside_context2
  allocate-interface Ethernet1.2 outside_context2
  config-url flash:/context2.cfg
  join-failover-group 2
!

prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

보조 ASA

```
ASA#show running-config

failover
failover lan unit secondary
failover lan interface LANFailover Ethernet3
failover key *****
failover interface ip LANFailover 10.1.0.1 255.255.255.0
standby 10.1.0.2
```

다음을 확인합니다.

show failover 명령 사용

이 섹션에서는 show failover 명령 출력에 대해 설명합니다. 각 유닛에서 **show failover** 명령을 사용하여 장애 조치 상태를 확인할 수 있습니다.

기본 ASA

```
ASA(config-subif)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: LANFailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
```

```
Version: Ours 7.2(3), Mate 7.2(3)
Group 1 last failover at: 06:12:45 UTC Jan 17 2009
Group 2 last failover at: 06:12:43 UTC Jan 17 2009

  This host:    Primary
  Group 1       State:          Active
                Active time:    359610 (sec)
  Group 2       State:          Standby Ready
                Active time:    3165 (sec)

                  context1 Interface inside (192.168.1.1): Normal
                  context1 Interface outside (172.16.1.1): Normal
                  context2 Interface inside (192.168.2.2): Normal
                  context2 Interface outside (172.16.2.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    3900 (sec)

                  context1 Interface inside (192.168.1.2): Normal
                  context1 Interface outside (172.16.1.2): Normal
                  context2 Interface inside (192.168.2.1): Normal
                  context2 Interface outside (172.16.2.2): Normal

Stateful Failover Logical Update Statistics
        Link : stateful Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         48044      0          48040      1
        sys cmd         48042      0          48040      1
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         2          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       72081
        Xmit Q:         0       1       48044
```

보조 ASA

```
ASA(config)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: LANFailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Group 1 last failover at: 06:12:46 UTC Jan 17 2009
Group 2 last failover at: 06:12:41 UTC Jan 17 2009

  This host:    Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    3975 (sec)
```

```
                  context1 Interface inside (192.168.1.2): Normal
                  context1 Interface outside (172.16.1.2): Normal
                  context2 Interface inside (192.168.2.1): Normal
                  context2 Interface outside (172.16.2.1): Normal

  Other host:   Primary
  Group 1       State:          Active
                Active time:    359685 (sec)
  Group 2       State:          Standby Ready
                Active time:    3165 (sec)

                  context1 Interface inside (192.168.1.1): Normal
                  context1 Interface outside (172.16.1.1): Normal
                  context2 Interface inside (192.168.2.2): Normal
                  context2 Interface outside (172.16.2.2): Normal

Stateful Failover Logical Update Statistics
        Link : stateful Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         940        0          942        2
        sys cmd         940        0          940        2
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          2          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1419
        Xmit Q:         0       1       940
```

상태를 확인하려면 **show failover state** 명령을 사용합니다.

기본 ASA

```
ASA(config)#show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
    Group 1    Active         None
    Group 2    Standby Ready  None
Other host -   Secondary
    Group 1    Standby Ready  None
    Group 2    Active         None

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

보조 유닛

```
ASA(config)#show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Standby Ready  None
    Group 2    Active         None
Other host -   Primary
```

```
    Group 1     Active         None
    Group 2     Standby Ready  None

====Configuration State===
        Sync Done - STANDBY
====Communication State===
        Mac set
```

장애 조치 유닛의 IP 주소를 확인하려면 **show failover interface 명령을** 사용합니다.

기본 유닛

```
ASA(config)#show failover interface
        interface stateful Ethernet2
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.1
                Other IP Address : 10.0.0.2
        interface LANFailover Ethernet3
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.1
                Other IP Address : 10.1.0.2
```

보조 유닛

```
ASA(config)#show failover interface
        interface LANFailover Ethernet3
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.2
                Other IP Address : 10.1.0.1
        interface stateful Ethernet2
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.2
                Other IP Address : 10.0.0.1
```

모니터링되는 인터페이스 보기

모니터링되는 인터페이스의 상태를 보려면 단일 컨텍스트 모드에서 글로벌 컨피그레이션 모드 `show monitor-interface` 명령을 입력합니다. 다중 컨텍스트 모드에서 컨텍스트 내에서 `show monitor-interface`를 입력합니다.

참고: 특정 인터페이스에서 상태 모니터링을 활성화하려면 글로벌 컨피그레이션 모드에서 **monitor-interface 명령**을 사용합니다.

monitor-interface <*if_name***>**

기본 ASA

```
ASA/context1(config)#show monitor-interface
        This host: Secondary - Active
                Interface inside (192.168.1.1): Normal
                Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Interface inside (192.168.1.2): Normal
                Interface outside (172.16.1.2): Normal
```

보조 ASA

```
ASA/context1(config)#show monitor-interface
        This host: Secondary - Standby Ready
                Interface inside (192.168.1.2): Normal
                Interface outside (172.16.1.2): Normal
        Other host: Secondary - Active
                Interface inside (192.168.1.1): Normal
                Interface outside (172.16.1.1): Normal
```

참고: 장애 조치 IP 주소를 입력하지 않으면 **show failover** 명령이 IP 주소에 대해 0.0.0.0으로 표시되고 인터페이스의 모니터링은 상태로 유지됩니다. 장애 조치가 작동하려면 장애 조치 IP 주소를 설정해야 합니다. 장애 조치의 여러 상태에 대한 자세한 내용은 장애 조치 표시 를 참조하십시오.

실행 중인 컨피그레이션에서 장애 조치 명령 표시

실행 중인 컨피그레이션에서 failover 명령을 보려면 다음 명령을 입력합니다.

```
hostname(config)#show running-config failover
```

모든 failover 명령이 표시됩니다. 다중 컨텍스트 모드에서 실행되는 유닛의 경우 시스템 실행 공간 `show running-config failover` 명령을 입력합니다. show running-**config all failover** 명령을 입력하여 실행 중인 컨피그레이션에 failover 명령을 표시하고 기본값을 변경하지 않은 명령을 포함합니다.

장애 조치 기능 테스트

장애 조치 기능을 테스트하려면 다음 단계를 완료하십시오.

1. 액티브 유닛 또는 장애 조치 그룹이 FTP를 사용하여 예상한 대로 트래픽을 전달하는지 테스트합니다(예: 다른 인터페이스의 호스트 간에 파일을 전송하려면).
2. 다음 명령을 사용하여 스탠바이 유닛에 장애 조치를 강제로 적용합니다.액티브/액티브 장애 조치의 경우 호스트를 연결하는 인터페이스가 활성 상태인 장애 조치 그룹이 있는 유닛에 이 명령을 입력합니다.
   ```
   hostname(config)#no failover active group group_id
   ```
3. 동일한 두 호스트 간에 다른 파일을 보내려면 FTP를 사용합니다.
4. 테스트가 성공하지 못한 경우 장애 조치 상태를 확인하려면 **show failover 명령**을 입력합니다.
5. 완료되면 다음 명령을 사용하여 유닛 또는 장애 조치 그룹을 활성 상태로 복원할 수 있습니다 .액티브/액티브 장애 조치의 경우 호스트를 연결하는 인터페이스가 활성 상태인 장애 조치 그룹이 있는 유닛에 이 명령을 입력합니다.
   ```
   hostname(config)#failover active group group_id
   ```

강제 장애 조치

스탠바이 유닛이 액티브 상태가 되도록 하려면 다음 명령 중 하나를 입력합니다.

장애 조치 그룹이 대기 상태에 있는 유닛의 시스템 실행 영역에서 이 명령을 입력합니다.

```
hostname#failover active group group_id
```

또는 장애 조치 그룹이 활성 상태인 유닛의 시스템 실행 공간에 이 명령을 입력합니다.

```
hostname#no failover active group group_id
```

시스템에 이 명령을 입력하면 실행 공간이 모든 장애 조치 그룹이 액티브 상태가 됩니다.

```
hostname#failover active
```

장애 조치(failover) 사용 안 함

장애 조치를 비활성화하려면 다음 명령을 입력합니다.

```
hostname(config)#no failover
```

액티브/스탠바이 쌍에서 장애 조치를 비활성화하면 재시작할 때까지 각 유닛의 액티브 및 스탠바이 상태가 유지됩니다. 예를 들어 스탠바이 유닛은 대기 모드로 유지되므로 두 유닛이 트래픽을 전달하지 않습니다. 스탠바이 유닛을 액티브 상태로 만들려면(장애 조치가 비활성화된 경우에도) Forced Failover 섹션을 참조하십시오.

액티브/액티브 쌍에서 장애 조치를 비활성화하면 장애 조치 그룹은 현재 활성 상태인 유닛에 관계없이 액티브 상태로 유지됩니다. 어떤 유닛을 선호하든 상관없습니다. 시스템 실행 공간에 **no failover** 명령을 입력할 수 있습니다.

실패한 유닛 복원

실패한 액티브/액티브 장애 조치 그룹을 오류가 발생하지 않은 상태로 복원하려면 다음 명령을 입력합니다.

```
hostname(config)#failover reset group group_id
```

오류가 발생한 유닛을 오류가 발생하지 않은 상태로 복원하면 자동으로 활성화되지 않습니다. 복원된 유닛 또는 그룹은 장애 조치(강제 또는 자연)에 의해 활성화될 때까지 스탠바이 상태로 유지됩니다. 예외는 preempt 명령으로 구성된 장애 조치 **그룹입니다**. 이전에 활성 상태였던 경우 장애 조치 그룹은 preempt 명령으로 구성된 경우 그리고 실패한 유닛이 기본 유닛인 경우 액티브 상태가 됩니다.

문제 해결

장애 조치가 발생하면 두 보안 어플라이언스는 시스템 메시지를 전송합니다. 이 섹션에서는 다음 항목을 다룹니다.

1. 장애 조치 시스템 메시지
2. 디버그 메시지
3. SNMP

장애 조치 시스템 메시지

보안 어플라이언스는 우선 순위 레벨 2에서 장애 조치와 관련된 여러 시스템 메시지를 발급하며, 이는 심각한 상태를 나타냅니다. 이러한 메시지를 보려면 Cisco Security Appliance 로깅 컨피그레이션 및 시스템 로그 메시지를 참조하여 로깅을 활성화하고 시스템 메시지에 대한 설명을 확인하십시오.

참고: 스위치오버 내에서 장애 조치가 논리적으로 종료되고 인터페이스가 실행되어 syslog **411001** 및 **411002** 메시지가 생성됩니다. 이것은 정상적인 활동입니다.

interface_name에서 mate를 사용하는 기본 장애 조치 통신

이 장애 조치 메시지는 장애 조치 쌍의 한 유닛이 더 이상 쌍의 다른 유닛과 통신할 수 없는 경우에 표시됩니다. 기본 유닛은 보조 유닛에 대해 보조 유닛으로 나열될 수도 있습니다.

(기본) interface_name에서 mate를 사용한 장애 조치 통신 손실

지정된 인터페이스에 연결된 네트워크가 올바르게 작동하는지 확인합니다.

디버그 메시지

디버그 메시지를 보려면 debug fover 명령**을** 입력합니다. 자세한 내용은 Cisco Security Appliance 명령 참조 버전 7.2를 참조하십시오.

참고: 디버깅 출력은 CPU 프로세스에 높은 우선 순위가 할당되므로 시스템 성능에 크게 영향을 줄 수 있습니다. 따라서 debug **fover** 명령만 사용하여 특정 문제를 해결하거나 Cisco 기술 지원 담당자와의 문제 해결 세션 내에서만 문제를 해결합니다.

SNMP

장애 조치를 위한 SNMP syslog 트랩을 수신하려면 SNMP 에이전트를 구성하여 SNMP 트랩을 SNMP 관리 스테이션으로 전송하고, syslog 호스트를 정의하고, Cisco syslog MIB를 SNMP 관리 스테이션으로 컴파일합니다. 자세한 내용은 Cisco **Security Appliance 명령 참조**, 버전 7.2의 **snmp-server** 및 **logging** 명령을 참조하십시오.

장애 조치 폴링 시간

장애 조치 유닛 폴링 및 대기 시간을 지정하려면 전역 컨피그레이션 모드**에서 failover polltime** 명령을 실행합니다.

failover polltime `unit msec [time]`은 hello 메시지를 폴링하여 스탠바이 유닛의 존재를 확인하는 시간 간격을 나타냅니다.

마찬가지로, failover `holdtime unit msec [time]`은 유닛이 장애 조치 링크에 대한 hello 메시지를 수신해야 하는 기간을 나타내며, 그 이후에는 피어 유닛이 실패한 것으로 선언됩니다.

자세한 내용은 장애 조치 폴링 시간을 참조하십시오.

경고: 장애 조치(failover) 메시지 암호 해독 실패.

오류 메시지:

```
Failover message decryption failure. Please make sure both units have the
same failover shared key and crypto license or system is not out of memory
```

이 문제는 장애 조치 키 컨피그레이션으로 인해 발생합니다. 이 문제를 해결하려면 장애 조치 키를 제거하고 새 공유 키를 구성하십시오.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco PIX 방화벽 소프트웨어
- FWSM(Firewall Services Module) 장애 조치 컨피그레이션
- FWSM 장애 조치 문제 해결
- Cisco Secure PIX Firewall에서 장애 조치가 작동하는 방식
- 기술 지원 및 문서 – Cisco Systems